Network Reference for the

Avaya™ S8300 Media Server with an Avaya™ G700 Media Gateway

555-234-600
Issue 1
May 2002

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.

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.

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: Document No.555-234-600, Issue 1
May, 2002

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/

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

Purpose

This book describes the Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway in the context of converged voice and IP networks. It describes how to assess existing data and voice networks, how to design a converged network using the G700 or the expansion of an existing network, and how to implement a new or existing network with G700s.

Prerequisites

Users should have broad data networking experience with Avaya, Cisco, Nortel, 3Com, or equivalent products. A knowledge of Avaya products, particularly Definity and Cajun systems, would be beneficial. Technicians should also be familiar with standard industry safety procedures and other practices.

Intended Audience

This book is intended for Avaya technicians, business partners, network system integrators, engineers, and customers. It is specifically intended for Tier 1, Tier 2, and Tier 3 technicians, as well as network provisioning specialists. It serves as a resource for initial network planning, for on-site installation, and for help-desk reference.

Organization

- "Chapter 1, Networking Overview" describes the Avaya™ S8300 Media Server and the Avaya™ G700 Media Gateway, converged networks, the process of converting voice to IP packets, the signalling protocols used by the G700, and typical network components.
- "Chapter 2, Components and Capacities" describes the available media modules for the G700, the network interfaces supported by the G700, the system capacities for the media modules and for the G700 itself.
- "Chapter 3, Network Configurations" describes possible network configurations for the G700 with and without the Avaya™ S8300 Media Server and lists system capacities for networks using G700s.
- "Chapter 4, Network Requirements" lists minimum network requirements for such parameters as delay, jitter, packet loss, and bandwidth. It also lists minimum requirements for PCs used as softphones.
- "Chapter 5, Network Assessment" describes the Avaya Network Assessment Services for IP Telephony and general procedures for assessing an existing network and its ability to support G700s and Voice over IP.
- "Chapter 6, Network Design" discusses best practices in network design and details network design problems that may impact voice transmission using G700s.
- "Chapter 7, Network Planning" describes how to calculate the number of G700s and the number and type of media modules required to meet particular station and trunk requirements.
- "Chapter 8, Network Implementation and Management" describes how to create and effect an implementation plan for G700s. It also provides an overview of the installation process and of the tools available for device and network management.
- "Glossary" defines networking and other terms associated with the G700.

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.

Standards Compliance

The equipment in this document complies with the following standards (as applicable).

Environmental Requirements and Safety Standards

Table 1. Regulatory Compliance

Standard	Country/Region
EN60950	Western Europe
UL 1950., ULC C22.2.950	USA and Canada
Global IEC, CB /Scheme Report IEC 950	Global
AS/NZS 3260	Australia
TS001	Australia
NOM 016	Mexico
NOM 019	Mexico

Network Standards

Table 2. Network Standards

Standard	Country/Region
CSO3	Canada
FCC Part 68	USA
TBR4	Europe
TBR4 Appendix 1 for Layer 3 Testing	New Zealand
TBR12	Europe
TBR13	Europe
TBR21	Europe
TS002	Australia
TS014	Australia
TS016	Australia
TS038	Australia
JATE	Japan
NOM151	Mexico
NOM152	Mexico
HKTA 2011	Hong Kong

Table 2. Network Standards *Continued*

Standard	Country/Region
HKTA 2013	Hong Kong
HKTA 2015	Hong Kong
HKTA 2017	Hong Kong
HKTA 2018	Hong Kong
HKTA 2023	Hong Kong
HKTA 2028	Hong Kong

EMC Standards

Table 3. EMC Standards

Standard	Country/Region
FCC PART 15, Class A	USA
ICES 003, Class A	Canada
AS/NZS 3548, Class B	Australia, New Zealand
EN55022, Class B	Europe
EN55024	Europe
EN61000-3-2	Europe
EN61000-3-3	Europe
VCCI, Class B	Japan
Plug and Power Specifications	Argentina

Systems Supported

This book covers the Avaya™ S8300 Media Server with an Avaya™ G700 Media Gateway offer.

1 Networking Overview

Avaya™ S8300 Media Server and the Avaya™ G700 Media Gateway

The Avaya™ G700 Media Gateway, with an Avaya™ S8300 or S8700 Media Server, is part of the Avaya family of IP solutions designed to deliver data, voice, fax, and messaging over IP networks for businesses and organizations with 10 to 450 stations. The G700 provides a standards-based, IP communications infrastructure; it can be integrated within a variety of network configurations and provides an exceptionally cost effective, highly reliable, scalable means of integrating voice and data networks. The G700 provides the highest reliability in critical applications and unified system management.

The G700 with a media server joins the power of Avaya MultiVantage™, based on the Definity feature set, with the power of distributed switching from the Avaya™ P330 line. With an Avaya S8300 or S8700 Media Server, it provides IP PBX functionality using open standards (H.323 and H.248) and an open operating system (Linux). This solution is scalable, modular, and able to support a variety of distributed configurations. It also supports stackable, hot swappable redundant architectures.

As a Voice over IP (VoIP) system, the G700 with a media server acts as an IP PBX, a messaging server, an interface between a LAN or WAN network and a wide variety of switched voice networks, and a management resource for conferencing, tone detection and generation, messaging, call classification, audio transcoding, and other telephony functions.

A single G700 with a media server can support dozens of IP telephones and IP softphones and a number of circuit switched entities. Additional G700s can be added as needed. Systems of up to 450 lines can be controlled by an S8300 Media Server residing within a G700. An external server, such as the Avaya S8700 Media Server, provides control for larger networks incorporating G700s.

The G700 moves voice data from the traditional circuit switched telephone world to the converged packetized Voice over IP world. This takes places in two steps. First, voice travelling over conventional circuits (analog trunk, analog T/R, T1/E1, or DCP) is transferred to a Time Division Multiplexing (TDM) bus similar to the traditional Definity TDM bus. This step is performed by the G700 media modules. Second, if the signal goes to an IP endpoint, or to DCP or analog endpoints in another G700, the voice signal on the TDM bus is converted into compressed or uncompressed IP packets. The second step is accomplished by the G700 VoIP engine.

The G700 contains a VoIP engine, a Layer 2 switch, modular interface connectivity for traditional trunk and station access, and resources for performing network gateway tasks. The G700 also contains a Digital Signal Processing (DSP) resource used for providing LAN audio services, such as conferencing, tones, and announcements. The G700 supports several media modules that can be installed in the four G700 media module slots. The media modules provide connectivity options to the G700, as well as application level options such as redundancy, control, and messaging. They allow for traditional interfacing of service provider network access solutions such as T1/E1, Loop Start/Ground Start Trunks, as well as connections to

TDM based endpoints such as DCP digital phones, analog phones, and tip/ring devices. Media modules can be mixed and matched inside G700s and are hot swappable and field replaceable.

The S8300 Media Server seamlessly integrates traditional circuit switched interfaces (analog stations, analog trunks, FAX, multifunction digital stations, E1/T1 trunking, ISDN-PRI, etc.) and IP switched interfaces (IP telephones, IP trunking, H.323/H.248 compliant endpoints/gateways/MCUs). This seamless integration allows the user to evolve easily from the current circuit switched telephony infrastructures to next generation IP infrastructures without changing current equipment.

Converged Voice and Data Networks

Until recently, voice, video, and data were delivered to individuals over dedicated, single-purpose networks. A converged network brings all forms of communication together: voice, data, and video travel through a single, unified network. A converged network supports all traffic types with packet-based protocols such as ATM, Frame Relay, or IP. Of these, the dominant protocol is the Internet Protocol (IP), the protocol primarily used by the G700.

However, digital data and voice communications have different characteristics that must be reconciled within a converged network. Data traffic tends to require significant network bandwidth for short periods of time, while voice traffic demands a steady, relatively constant transmission path. Data traffic can tolerate delays, while voice transmission degrades if delayed. While TDM circuit-based networks carried voice traffic streams efficiently and reliably, they were never designed for bursts of data traffic. Early-generation data networks handled data flow effectively, but they could not guarantee the constant, real-time transmission needed by voice.

Packetized Voice over IP (VoIP) services provide a cost-effective and flexible way of building a converged network. In addition, converged networks allow for the separation of such functions as call control and switching. Each section of the converged network may use different techniques for handling data, voice, and fax. Different parts of the network traffic may use different communications standards, and the media streams need to be constantly and seamlessly reformatted. This is the exactly task of the G700.

A converged network replacing separate circuit-switched voice and packetized data networks brings with it several benefits. A single network reduces equipment, cabling, and installation costs. While the cost of traditional circuit-switching equipment has remained relatively stable over recent years, the cost of IP equipment has declined steadily. With a single network for administration, only one maintenance and management plan is required. Telephones can be added or moved from one person to another easily and quickly. As a result, operational costs are also reduced.

While IP networks may eventually replace circuit-switched networks, the two technologies will likely coexist for some time to come.

Voice over IP

VoIP is simply the ability to make telephone calls, send facsimiles, or transmit audio over IP-based data networks with a suitable quality of service (QoS) and a cost/benefit ratio superior to traditional systems. VoIP transmits voice signals in digital form in discrete packets rather than in the protocols of traditional switched circuits.

Three major factors can impact the quality of the service:

- *Delay:* Significant end-to-end delay in a voice network may result in echo and talker overlap. Echo becomes a problem when one-way network delay is more than 50 milliseconds. VoIP systems must implement some means of echo cancellation. If the round-trip delay is greater than 250 milliseconds, talker overlap--one caller stepping on the other talker's speech--is likely. For adequate quality of service, network delay between endpoints should be less than 50ms.
- *Jitter (Delay Variability):* Jitter results when data packets arrive at their destination at irregular intervals as a result of variable transmission delay over the network. To remove jitter, the VoIP engine must collect and hold data packets in a buffer long enough for the slowest packet to arrive and be played in sequence. A jitter buffer, however, adds to delay. Jitter of less than 20 ms. between endpoints is normally required.
- *Packet Loss:* Under peak network loads and periods of congestion, packets may be dropped. Because voice transmission is highly time-sensitive, normal TCP-based re-transmission schemes are not suitable. Methods to compensate for packet loss include interpolation of speech by re-playing the last packet and sending of redundant information. The maximum packet loss between network endpoints should not exceed 0.2%.

IP-TDM Connectivity

Before voice can be transmitted over an IP network, it must be digitized. Analog to digital conversion usually takes place at a rate of 8000 samples per second. The digital stream is then encoded by A-law, mu-law, or bit-rate reduction methods and finally grouped into packets for transmission. Echo-cancellation to eliminate acoustic or electronic network reflection effects also takes place upon reception. To reduce packet transmission rates, silence suppression detects when there are periods of silence and, during those times, does not transmit packets.

When the packets are received, they must be put in proper order and converted back into an analog voice signal. In addition, jitter must be removed and the effects of packet loss mitigated. Various algorithms are used to deal with jitter and packet loss. In addition, silence suppression is eliminated by adding artificial samples, often in the form of comfort noise, a random, low-level signal that gives the impression that the connection is still alive during periods of silence.

VoIP is a specific set of protocols for the transmission and reception of digital packets. In addition, the User Datagram Protocol (UDP) provides for packet error detection; although the UDP does not guarantee that packets arrive in the order they are sent. As a result, it is possible to get misordered packets which may affect voice quality. The Real-Time Protocol (RTP) numbers the packets in sequence so that they can be put

in proper sequence on the receiving side and played out from the jitter buffer at the rate at which they were originally transmitted.

Avaya™ S8300 Media Servers and Avaya™ G700 Media Gateways

A converged network brings together voice and data, but it still must interact with other networks, some of which are still circuit-switched voice networks (PSTN), others of which are data-oriented. The G700 Media Gateway translates the signals from network to network.

In general, a G700 translates signals from one type of network to another; it manages the conversion of information from a network employing one standard to a network employing a different standard. A G700 commonly has terminations for several types of networks, such as Ethernet, ATM, T1/E1 digital, or analog. It usually supports several voice codecs. A G700 requires substantial Digital Signal Processing (DSP) power and IP packet handing capacity.

In general, an S8300 Media Server directs and controls the flow of voice and data traffic in a converged network; it mediates signalling between the IP and PSTN environments. The call control functions typically performed by an S8300 include call routing, call setup and tear down, user authentication, and signalling.

H.248

The signaling protocol used between the G700 Media Gateway and its server is H.248, one of the leading standard protocols for signaling Voice Over IP. The ITU-T/IETF H.248 (MEGACO) Protocol defines communication between a G700 and its server.

A wide variety of protocol choices are available for signaling voice-over-IP, and some are already supported by Definity, including H.323, and proprietary protocols like CCMS. The G700 uses the H.248 protocol because it is an open standard and allows the G700 to operate with equipment from other vendors adhering to the same protocol.

The G700 is more than an IP to circuit-switched network gateway. It also acts as an announcement server when supported by the Avaya S8700 Media Server, provides general tone detection and generation functions, provides call classification capabilities, and hosts conferences among IP and circuit switched endpoints. All these capabilities require a protocol which is oriented toward IP connection management and IP media handling. VoIP protocols like H.323 are not suited to these tasks: they are oriented toward line or trunk signaling (e.g. “setup”, “alerting”, “connect”). There is no construct in either protocol to use a G700 for the services listed. The natural choice is H.248: it is designed specifically for the capabilities of the G700.

Shuffling

G700s implement call shuffling, a routing procedure designed to reduce Digital Signal Processor load, to reduce required IP bandwidth, and to save TDM time-slot resources. When a call is shuffled, a connection between two IP endpoints is rerouted for maximum efficiency. Without shuffling, a call is transmitted from its origination point over the IP infrastructure, through the TDM bus, and back over the IP infrastructure to its destination. With shuffling, a call passes directly from origination to destination, without passing through the TDM bus. In some instances, shuffling may require that a call passing directly from IP endpoint to IP endpoint be routed back through the TDM bus. Shuffling reduces the number of media conversion ports required and, by reducing the number of transcodings, may improve voice quality.

The end user does not have to take any action to invoke audio shuffling. The G700 will shuffle, if necessary, after a point-to-point call is established between two voice endpoints and if both endpoints are capable of handling shuffling. If the endpoints take some actions that require a tone played in the connection, the G700 will reroute the call back through the TDM bus.

The following conditions must be met for call shuffling between IP endpoints:

- Both IP endpoints must be administered to allow shuffling.
- A point-to-point voice connection must exist between two endpoints and no active call (in-use or held) exists on either endpoint which requires TDM connectivity (such as applying tones, announcement, or conferencing).
- The endpoints must be in the same LAN region or in interconnected LAN regions.
- The inter-region connection management rules must be met.
- There is at least one codec in common between the codec lists of the endpoints involved and the Internetwork region Connection Management codec list.
- The endpoints must have at least one codec in common as shown in their current codec negotiations between the endpoint and the switch.

For information on administering call shuffling, see *"Administration for Network Connectivity for Avaya MultiVantage™ Software, 555-233-504"*.

Network Components

Communication Controller Software

The Avaya™ S8300 Media Server uses the rich feature set of the Avaya MultiVantage™ software as well as administration and maintenance provisioning software. Other External Media Servers (EMS), such as an Avaya™ S8700 Media Server, also use the Avaya MultiVantage™ software.

Gateway Software

On an Avaya™ G700 Media Gateway, specific software acts as the interpreter of commands from the server to the hardware. In addition, it handles the allocation of specific resources required for call control such as time slot allocation on the TDM, VoIP resource allocation, and tone management on the resident tone generator/detector.

Maintenance of the G700 components is performed by maintenance software. This software performs startup maintenance, such as verifying that a component is fit for service and alerting the upper layers of software to the presence of the component. In addition, it performs preventive and diagnostic maintenance, and provides error and status information to the system user.

LAN Equipment and Switches

Avaya™ G700 Media Gateways can use various types of connectivity solutions and LAN equipment. Data connectivity options include 10/100 Base-T Ethernet and Cajun Expansions Modules (ATM, fiber, etc.). G700s integrate with any layer 2 switch or layer 3 router. Through the Octaplane connection, G700s can be seamlessly integrated with Avaya Cajun P330 switches, but they also operate effectively with Cisco, Nortel, 3Com, and other layer 2 switches.

Network Endpoints

The Avaya™ G700 Media Gateway is primarily designed for IP endpoints, but it can also support Definity Digital Communications Protocol (DCP) or analog endpoints. For a larger system such as the Avaya™ S8700 Media Server, the maximum number of endpoints is significantly greater.

A G700 without the S8300 can support up to 32 DCP or analog station or trunk ports. With an S8300, a G700 supports up 24 stations. The G700 provides resource support for all vintages of the IP station endpoints.

IP Telephones

The 4600-series IP telephones provide a single IP endpoint solution for all Avaya platforms. They are available in black or white and provide customers with superior audio quality over the handset and the speakerphone. The speakerphone is full-duplex and has echo cancellation. These sets come with infrared ports to support future applications and an Ethernet connection (10/100 Base T) for a telephone and PC (2-port hub). Customers also have the convenience of downloading firmware for future upgrades to keep their 4600-series sets current. The IP Telephones require Trivial File Transfer Protocol (TFTP) server software installation on the network and configuration of the customer's DHCP server. DHCP is optional. It is used on an S8300 configured as an LSP (Local Survivable Processor) so the phones receive the IP address of the S8300 when the External Media Server is not reachable.

IP Softphones

The IP Softphone provides voice communications for the remote office worker and telecommuter. When IP Softphone is installed on a PC/laptop, the user can place and receive various types of calls, and retrieve and respond to voice mail messages while away from the office. Using an intuitive GUI, the remote user, whether traveling or working from home, can access important telephony station features.

There are four types of IP Softphones available:

- The Telecommuter application is a multifunction station that runs on a PC plus a conventional telephone. It provides circuit-switched level voice quality and allows your PC/laptop to work completely as a phone.
- The Road-warrior application is a multifunction station based entirely on the PC (must have IP Softphone R1 or Softphone R2).
- The Avaya IP Agent softphone is a telecommuter application that has been configured to use the Avaya IP Agent user interface software.
- The Native H.323 IP-connected softphone runs off-the-shelf H.323 software (must have IP Softphone R1 or Softphone R2).

Analog or DCP Telephones

G700 customers have the option to use Avaya 2-wire telephones when they purchase either the Avaya MM712 and/or Avaya MM711 Media Modules. If additional power is required by adjuncts, power bricks must be provided at the endpoints.

2 Components and Capacities

Avaya™ G700 Media Gateways are designed to permit exceptional network flexibility and scalability. With the Avaya™ S8300 Media Server, a G700 can run Avaya MultiVantage™ and function as server for the network. When server functions are located elsewhere, a G700 may serve in a "survivable configuration," and take over call processing and control functions when connection to the primary server is lost.

Four media module slots allow customers to mix and match any of five media modules that allow for traditional interfacing of service provider network access solutions such as T1/E1, Loop Start/Ground Start Trunks, as well as connections to TDM based endpoints such as DCP digital phones, analog phones and tip/ring devices. This chapter provides brief descriptions of the G700 communications servers and modules followed by sections detailing G700 system capacities, network interface capacities, media module capacities, and general messaging capacities. For more complete technical descriptions of the G700 communications servers, media modules, and expansion modules, see *"Avaya MultiVantage™ Solutions Hardware Guide, 555-233-200"*.

Communications Servers

The Avaya™ G700 Media Gateway functions with the following three server options:

- S8300 Media Server
- S8300 Media Server in a local survivable configuration
- External Media Server (EMS)

Avaya™ S8300 Media Server

The Avaya™ S8300 Media Server is a Pentium™ based server complex that supports Avaya MultiVantage™ and G700 server functions for small and moderately sized systems. The S8300 has the form factor of a media module but can be installed only in the leftmost slot, labeled V1, on the G700.

The S8300 comes standard with Avaya MultiVantage™ software administration and maintenance provisioning software, a 20G Hard drive, 256 MB RAM, H.248 G700 Signaling Protocol, and a TFTP server.

Avaya™ S8300 Media Server Configured as an LSP (Local Survivable Processor)

The Avaya™ S8300 Media Server configured as an LSP (Local Survivable Processor) is identical to the S8300, with the exception that it is loaded with a slightly different version of the Avaya MultiVantage™ software. This software difference allows a G700 to operate as a "Survivable" call-processing server for remote/branch customer locations.

In the LSP configuration, the S8300 serves as an alternate server/gatekeeper for IP entities such as IP telephones and G700s. These IP entities use the LSP when they lose connectivity to their primary server. In the event that the link is broken between the remote G700 and the main processing server or LSP takes over for those telephones and other G700s connected to the remote G700. A large enterprise customer may have a main processing server, such as the Avaya S8700 Media Server, controlling multiple remote G700s configured with LSPs. The LSP will ONLY take over for those telephones connected to its remote G700.

Like the S8300, the LSP can only be into placed in the leftmost media module slot (V1). An S8300 and an S8300 in LSP mode cannot both be installed in the same G700.

External Media Server (EMS)

The G700 Media Gateway can also be controlled externally by an External Media Servers, such as an S8700.

Media Modules

Media module slots host a variety of functions ranging from Legacy analog telephony ports up to Pentium-based call server devices or sophisticated voice recognition functions for enhanced call classification support. Media modules provide connectivity options to the G700, as well as other, application-level options, such as redundancy, control, and messaging. They are hot swappable and field replaceable.

For more detailed description of the media modules, refer to *"Avaya MultiVantage™ Solutions Hardware Guide, 555-233-200"*.

Avaya™ MM712 Media Module

The Avaya MM712 Media Module allows connectivity of up to eight two-wire DCP voice terminals. (The G700 does not support 4-Wire DCP telephones.) The Digital Communications Protocol (DCP) is the Avaya proprietary signaling protocol used to interface the digital voice coming from Avaya to DEFINITY.

Avaya™ MM711 Media Module

The Avaya MM711 Media Module supports eight analog interfaces allowing CO Loop Start trunks, CO trunks Ground Start, Direct Inward Dialing (DID), wink start or immediate start trunks, and 2-wire outgoing CAMA (for E911 connectivity to the PSTN) trunks. It also includes analog tip/ring devices such as single line telephones, modems, or group 3 fax machines. Each port may be configured as either a trunk or a station.

Avaya™ MM710 Media Module

The Avaya MM710 Media Module supports a T1 and E1. ISDN PRI is optionally supported (ISDN PRI is available on T1 or E1 and is an option for which the customer may pay). It provides echo cancellation in either trunk direction. It supports trunk signaling on US and International CO trunks and tie trunks. It has a built-in Channel Service Unit (CSU), and supports u-law or A-law gain/loss control and echo cancellation.

Avaya™ MM760 Media Module

The Avaya MM760 Media Module provides an additional 64 VoIP channels with G.711 compression. Each chassis base system can support up to 64 G.711 TDM/IP simultaneous calls or 32 compression codec (G.729 or G.723) TDM/IP simultaneous calls. Call types can be mixed, so the simultaneous call capacity of the module is 64 G.711 Equivalent Calls.

An essentially non-blocking system requires an additional Avaya MM760 Media Module if more than two Avaya MM710 T1/E1 Media Modules are used in a single chassis. This provides for an additional 64 channels.

As does the VoIP engine on the motherboard, the Avaya MM760 Media Module supports RTP and RTCP interfaces, dynamic jitter buffers, DTMF detection, hybrid echo cancellation, silence suppression, and comfort noise generation.

Avaya™ Expansion Modules

Avaya™ Cascade Module (Octaplane)

Each Avaya™ P330 switch and Avaya™ G700 Media Gateway has an expansion slot at the rear for the 8Gbps Octaplane stacking fabric. The use of a separate expansion slot for the Octaplane Stacking Module means that all the front panel ports are available for network connections. The Octaplane Stackable Switching System incorporates a range of redundancy, resilience, and hot-swapping features to keep the stack operating smoothly.

In the unlikely event that a Avaya™ P330 switch or G700 should fail, stack integrity is maintained. The broken link is bypassed and transmission continues uninterrupted. The single management IP address for the stack is also preserved for uninterrupted management and monitoring. You can also remove or replace any single unit within the stack at a time without disrupting operation or performing stack-level reconfiguration.

Avaya™ G700 Media Gateway Capacities

The Avaya™ G700 Media Gateway is designed to be used in business and organization settings with from 10 to 100 stations. A G700 can serve a maximum of 100 voice stations and 100 trunk lines. These maximum capacities are the same for a G700 with and a G700 without an S8300. The G700 supports analog, DCP, and IP station types, as well as analog, T1/E1, and IP trunks.

Single Avaya™ G700 Media Gateway with an Avaya™ S8300 Media Server

The maximum capacities for a single G700 with an S8300 installed are listed in Table 4. VoIP engine capacities for a Media Gateway equipped with an S8300 are listed in Table 5.

Table 4. Capacities of a Single Media Gateway *with* S8300 Media Server

Feature	Capacity	Constraining Factor
Media Modules	4	One of the four must be an S8300
RJ45 jacks	2	
Avaya MM712 Media Module	3	Available slots
Avaya MM711 Media Module	3	Available slots
Avaya MM710 Media Module	3	Available slots
Avaya MM760 Media Module	3	Available slots
Traditional stations	24	Number of traditional ports physically installed
IP stations	100	Defined system maximum and as limited by LAN
IP and traditional stations	100	Defined system maximum and as limited by LAN
Trunks	24 Analog	Three Avaya MM711 installed

1 of 2

Table 4. Capacities of a Single Media Gateway *with* S8300 Media Server *Continued*

Feature	Capacity	Constraining Factor
T1/E1 facilities		Three Avaya MM710 Media Modules installed
23 voice and 1 control channel per Media Module	69 T1	
31 voice and 1 control channel per Media Module	93 E1	
30 voice and 2 control channels per Media Module	90 E1	
IP trunks	100	System maximum
Touch Tone Receivers (TTR) per Media Gateway	8	Supplied by the Spitfire circuit on the G700 main board
VoIP engines per G700 (minimum)	1	Included on the main board
VoIP Engines per G700	4	One engine on main board and three additional Avaya MM760 Media Modules
DSP ports per VoIP Engine	32	
Calls requiring a TDM bus connection (traditional phone to traditional phone, or traditional phone to analog, or T1/E1)	24	Number of traditional phones that can be installed in a single G700
Announcement files	255	
Minutes of recording	30	
Simultaneous playback channels	15	
Record channels	1	
		2 of 2

Note: E1=32 is 1 control, 1 signal, and 30 voice. T1=24 in robbed-bit signaling mode. T1=23 if common channel or ISDN.

Table 5. VoIP Engine Capacities for Single Media Module *with* S8300

Feature	Number of Internal VoIP Engines				Constraining Factor
	1	2	3	4	
Simultaneous IP phone to traditional station or trunk conversations including call progress tones	32	64	96	128	VoIP engine design (Cannot be achieved simultaneously with all types of calls requiring a VoIP port)
Simultaneous IP phone to IP phone conversations with shuffling	225	225	225	225	Ability of IP phones to shuffle, performance of the LAN, and system maximum of 450 stations
Simultaneous IP Phone to IP Phone G711 conversations	64	128	192	256	Performance of the LAN and VoIP engine design
Simultaneous IP phone to IP phone 3-way conference conversations	10	21	32	42	VoIP engine design (Cannot be achieved simultaneously with all types of calls requiring a VoIP port)
Simultaneous transcoding IP phone to IP phone (from G711, G729, and G723) conversations	32	64	96	128	Volp engine design Cannot be achieved simultaneously with all types of calls requiring a VoIP port

Single Avaya™ G700 Media Gateway without an Avaya™ S8300 Media Server

The maximum capacities for a single G700 without an S8300 installed are listed in Table 6. VoIP engine capacities for a G700 equipped with an S8300 are listed in Table 7.

Table 6. Maximum Capacities of a Single G700 *without* S8300

Feature	Capacity	Constraining Factor
Media Modules	4	
RJ45 jacks	8	
S8300 configured as an LSP	1	When S8300 installed in this way, system capacities are those of a single G700 with an S8300
Avaya MM712 Media Module	4	Available slots
Avaya MM711 Media Module	4	Available slots
Avaya MM710 Media Module	4	Available slots
Avaya MM760 Media Module	4	Available slots
Traditional stations	32	Number of traditional ports physically installed
IP stations	100	Defined system maximum and as limited by LAN
IP and traditional stations	100	Defined system maximum and as limited by LAN
Trunks	32 Analog	Four Avaya MM711 installed
T1/E1 facilities		Four Avaya MM710 Media Modules installed
23 voice and 1 control channel per Media Module	92 T1	
31 voice and 1 control channel per Media Module	124 E1	
30 voice and 2 control channels per Media Module	120 E1	
IP trunks	100	System maximum
Touch Tone Receivers (TTR) per G700	8	Supplied by the Spitfire circuit on the G700 main board
VoIP engines per G700 (minimum)	1	Included on the main board
VoIP engines per G700	5	One engine on main board and four additional Avaya MM760 Media Modules
DSP ports per VoIP Engine	32	

1 of 2

Table 6. Maximum Capacities of a Single G700 *without* S8300 *Continued*

Feature	Capacity	Constraining Factor
Simultaneous calls requiring a TDM bus connection (traditional phone to traditional phone, or traditional phone to analog, or T1/E1)	32	Number of traditional phones that can be installed in a single G700
Announcement files	255	
Minutes of recording	30	
Simultaneous playback channels	15	
Record channels	1	

2 of 2

Table 7. VoIP Engine Capacities for Single Media Module *without* S8300

Feature	Number of Internal VoIP Engines					Constraining Factor
	1	2	3	4	5	
Simultaneous IP phone to traditional station or trunk conversations including call progress tones	32	64	96	128	160	VoIP engine design Cannot be achieved simultaneously with all types of calls requiring a VoIP port
Simultaneous IP phone to IP phone conversations with shuffling	225	225	225	225	225	Ability of IP phones to shuffle, performance of the LAN, and system maximum of 450 stations
Simultaneous IP Phone to IP Phone G711 conversations	64	128	192	256	320	Performance of the LAN and VoIP engine design
Simultaneous IP phone to IP phone 3-way conference conversations	10	21	32	42	53	VoIP engine design Cannot be achieved simultaneously with all types of calls requiring a VoIP port
Simultaneous transcoding IP phone to IP phone (from G711, G729, and G723) conversations	32	64	96	128	160	VoIp engine design Cannot be achieved simultaneously with all types of calls requiring a VoIP port

Network Interfaces

Sections below detail the network and voice station interfaces supported by a G700 Media Gateway.

PSTN Interfaces

G700s support the network interfaces listed in Table 8. A maximum of 100 trunks may be administered. Trunk interfaces may be mixed types, but the listed maximum limits cannot be achieved simultaneously by more than one trunk type.

Table 8. Supported PSTN Interfaces

Network Interfaces	Model Number	Maximum
Loop Start (analog facility)	MM711	100
Loop Start with ICLID	MM711	100
Ground Start (analog facility)	MM711	100
T1 Ground Start Emulation	MM710	100
T1 Loop Start Emulation	MM710	100
T1 E & M (4 signalling modes)	MM710	100
T1 DID Emulation	MM710	100

Voice Station Interfaces

G700s support the voice station interfaces listed in Table 9.

Table 9. Supported Voice Station Interfaces

Voice Station Interface	Model Number	Type
Analog	MM711	Tip/Ring See REN's in "Avaya™ G700 Media Gateway Capacities" on page 20.
DCP	MM712	2 Wire See power restrictions in "Avaya™ G700 Media Gateway Capacities" on page 20.
VoIP	MM760	G711, G723, G729 IP phones may be phantom powered following the configuration rules.

Media Module Capacities

This section lists the types of media modules available, their maximum capacities, and any restrictions on their use. The numbers reflected in this section are calculated using the Avaya™ S8300 Media Server as controlling server.

Table 10. Media Module Interfaces and Restrictions

Media Module	Network Interface	Voice Station Interface	Restrictions
S8300	None	None	One per system
MM712	None	2 wire DCP	Restricted by the number of available slots
MM711	Loop Start, Ground Start	Tip/Ring	Restricted by the number of available slots
MM710	T1/E1	None	Restricted by the number of available slots
MM760	None	None	Restricted by the number of available slots

Avaya™ MM712 Media Module

Table 11. Avaya MM712 Media Module Maximum Capacities

Feature	Capacity	Constraining Factor
Number per system	32 (without S8300) 24 (with S8300)	Available slots
DCP ports per Media Module	8	System design No restrictions on DCP set types installed

Avaya™ MM711 Media Module

Table 12. Avaya MM711 Media Module Capacities

Feature	Capacity	Constraining Factor
Number per system	32 (without S8300) 24 (with S8300)	Available slots
Analog ports per Media Module	8	No restrictions on mixing of port configurations
Touch Tone Receivers (TTR)	0	.
Incoming Caller Identification Receivers	8	
Ringer Equivalent Number (REN)	3	On a 2000 foot loop; no more than four ports ringing simultaneously; limited by line current

Avaya™ MM710 Media Module

Table 13. Avaya MM710 Media Module Capacities

Feature	Capacity	Constraining Factor
Number per system	4 (without S8300) 3 (with S8300)	Available slots
T1/E1 ports per Media Module	1	System design
Fractional T1/E1	Supported	

Avaya™ MM760 Media Module

Table 14. Avaya MM760 Media Module Capacities

Feature	Capacity	Constraining Factor
Number per system	128 (without S8300) 96 (with S8300)	Available slots
Avaya G700 Motherboard	160 (without S8300) 128 (with S8300)	

Network System Capacities

Network System Capacities for an Avaya™ G700 Media Gateway with External Media Server (EMS)

Table 15. Maximum System Capacities with an External Media Server

Feature	Capacity	Constraining Factor
G700s controlled by S8700	5	Capacity limits for G700 without S8300 apply
ASAI Links for CTI		Dependent on external server

Network System Capacities for Avaya™ G700 Media Gateways with Avaya™ S8300 Media Servers

Table 16. Maximum System Capacities for G700 with S8300 Media Server

Feature	Capacity	Constraining Factor
G700s in a stacked or distributed system	10	
G700s in stack with Octaplane cabling	10	
Avaya™ Media Modules in a stacked system	40	One of the 40 must be an S8300
S8300s	2	One S8300 required; a second may be configured as an LSP in a different G700
MM712 Media Modules	39	Available slots
MM711 Media Modules	39	Available slots
MM710 Media Modules	39	Available slots
MM760 Media Modules	39	Available slots
Traditional stations	28	Number of physical ports that can be installed

1 of 2

Table 16. Maximum System Capacities for G700 with S8300 Media Server

Feature	Capacity	Constraining Factor
IP stations	100	System limit
IP and traditional stations	100	System limit
Trunks	100	System limit
IP trunks	100	System limit
IP and traditional trunks	100	System limit
Touch Tone Receivers (TTR)	64	System limit
VoIP engines	39	Available slots
IP phones to traditional stations, analog trunks, or T1/E1 facility		VoIP engine capacities per G700
Simultaneous IP phone to IP phone conversations,		Performance of LAN and IP connections between G700s
Simultaneous IP phone to IP phone 3-way conference conversation		VoIP engine capabilities; see Table 5 on page 22 and Table 7 on page 24
Simultaneous transcoding IP phone to IP phone (from G711, G729, and G723) conversations		VoIP engine capacities per G700
Simultaneous calls requiring a TDM bus connection (traditional phone to traditional phone, or traditional phone to analog, or T1/E1 on the *same* G700)	39	Number of traditional phones that can be installed in a single G700
Simultaneous calls requiring a TDM bus connection (traditional phone to traditional phone, or traditional phone to analog, or T1/E1 on *different* G700s)	39	Number of VoIP ports on each G700
ASAI Links for CTI	1	

2 of 2

3 Network Configurations

The Avaya™ G700 Media Gateway is a highly flexible, scalable communications solution that can be incorporated in customer networks in a variety of ways. Paired with an Avaya™ switch and equipped with an Avaya™ S8300 Media Server, it can serve as a standalone gateway within a small or medium sized office. Linked to several switches, it may serve as a gateway in a large branch office networked through a WAN to a central location where the communications server resides on an S8300.

There are two general types of network configurations for the G700. In the first, Avaya MultiVantage™, resides on an External Media Server (EMS) — such as an Avaya™ S8700 Media Server — and provides call processing and network control functions, while G700s provide connectivity to lines and trunks. If AUDIX Multimedia Messaging is required, it is located with the main server.

In the second configuration, an S8300 Media Server with Avaya MultiVantage software, installed in a G700, provides call control for the network, which may incorporate other G700s without S8300s.

In both configurations, a G700 may be equipped with an S8300 configured as an LSP (Local Survivable Processor) with Avaya MultiVantage. The LSP will take over call control if connection to the main server is lost.

Office Environments

While G700 networks may be integrated in a wide variety of networks, they are particularly well suited for three business and organizational settings.

Branch Office Configurations

Branch office configurations are appropriate for remote sites with approximately 40 to 100 stations that are part of a larger enterprise network. The branch office sites are networked either through public or private LAN / PSTN networks to a large campus central office. With G700s, the branch office network becomes part of a single managed communications solution. G700s in branch offices should be equipped with Local Spare Processors so that the system will survive in the event that connection to the central office is lost.

Mid-Office Configurations

Mid-office configurations are appropriate for single sites with approximately 40 to 100 users. These sites are self-supporting and are generally not networked to a central location. These offices may be part of a larger enterprise and are networked together through such protocols as Q-Sig or DCS. Each location may have a G700 with S8300 and separate call processing, or a G700 in one location may act as server for other offices.

Small Office Configurations

Small offices may have two to twenty-five stations or more, but less than forty. The offices offer a stand-alone solution with a mixture of DCP, analog, and IP phone support. In this configuration, the G700 contains an S8300.

Avaya™ G700 Media Gateway Configurations with External Media Server (EMS)

One or more Avaya™ G700 Media Gateways can be controlled by an Avaya™ S8700 Media Server with Avaya MultiVantage through a Wide Area Network composed of devices from Avaya or another manufacturer. These configurations are appropriate to larger business and organizations with branch offices.

Avaya™ S8700 Media Server System with WAN Branch Offices (Small of Large Configuration)

As shown in Figure 1, the G700s operate in stacks with Avaya™ P330 switches through Octaplane connections. The remote local LANs may be composed of switches from other manufacturers. In this configuration also, each of the G700s may be equipped with Local Spare Processors to guarantee survivability in case connection to the central server is lost.

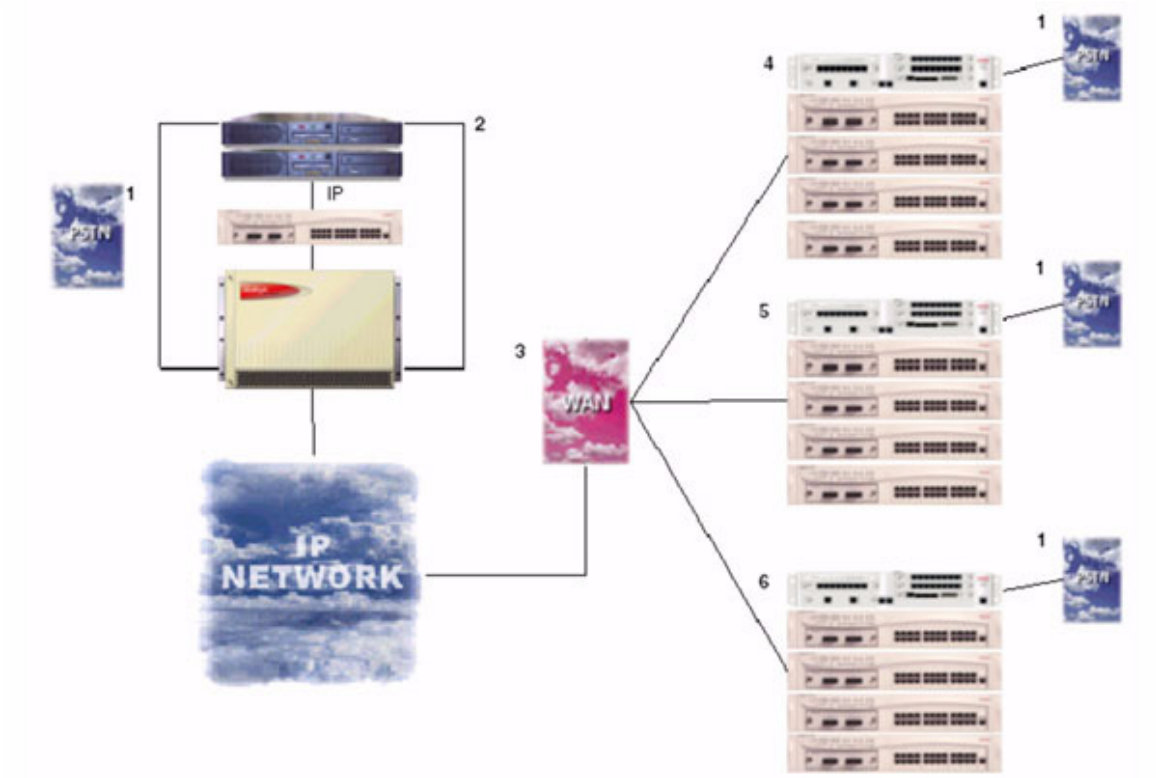


Figure 1. Avaya™ Media Gateways in Avaya™ Stacks with S8700 EMS

1) Public Service Telephone Network
2) Avaya™ S8700 Media Server with communications server in stack
3) Wide Area Network
4) G700 in Avaya switch stack at remote location A
5) G700 in Avaya switch stack at remote location B
6) G700 in Avaya switch stack at remote location C

Avaya™ G700 Media Gateway Configurations with Avaya™ S8300 Media Server

In small offices, an Avaya™ G700 Media Gateway equipped with an Avaya™ S8300 Media Server and Avaya MultiVantage, in conjunction with a Local Area Network, could serve all communications needs. Media modules could provide all the required connectivity to analog, DCP, and IP telephones and to the

PSTN. The LAN itself can either be an existing network from another manufacturer or an Avaya™ P330 linked to the G700 through the Octaplane.

Medium sized offices require a number of stacked G700s linked to an existing Local Area Network from another manufacturer or, preferably, a LAN composed of several Avaya™ P330s linked to one another and the G700 through the Octaplane.

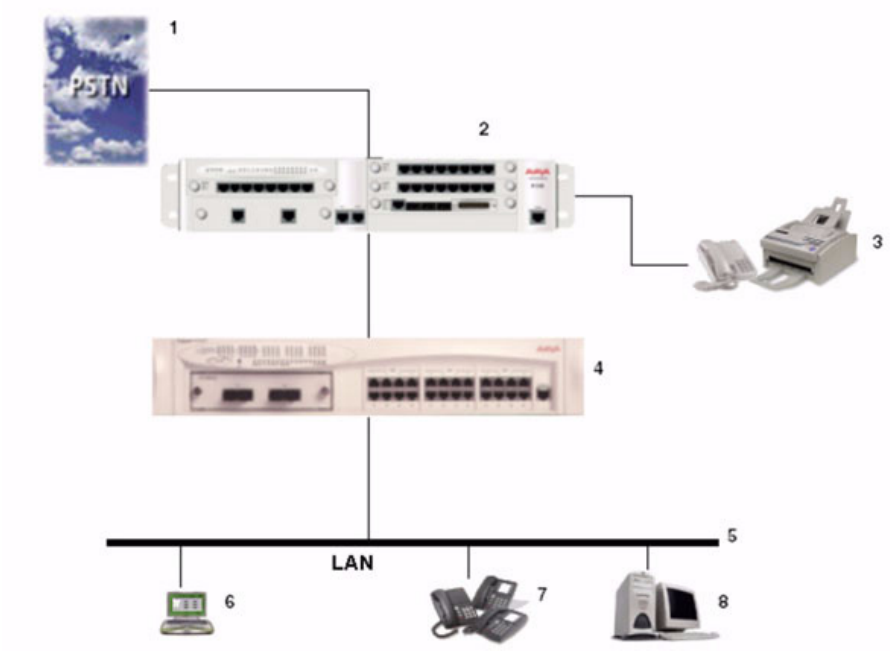
Organizations with branch offices may want to consider one, centrally located G700 with S8300 and Avaya MultiVantage networked, through a Wide Area Network, to other G700s at other locations.

Avaya™ G700 Media Gateway with LAN (Small Office Configuration)

This configuration consists of a single Avaya™ G700 Media Gateway with an Avaya™ S8300 Media Server. The three remaining open slots are occupied by media modules. The configuration also makes use of the expansion slot for a variety of expansion modules for network connectivity through ATM OC3, Gigabit ethernet (1000BaseT wire, multimode or single mode fiber), or 16 port 10/100 Ethernet, etc. In this configuration, there is a limit of 450 stations and 450 trunks.

The layer 2 switch in this configuration may be an Avaya™ P330 or an equivalent device from another manufacturer.

Figure 2. Avaya™ G700 Media Gateway with Avaya™ S8300 Media Server



1) Public Service Telephone Network
2) G700 with S8300, Avaya™ MM711 Media Module, and Avaya™ MM710 Media Module
3) Analog devices

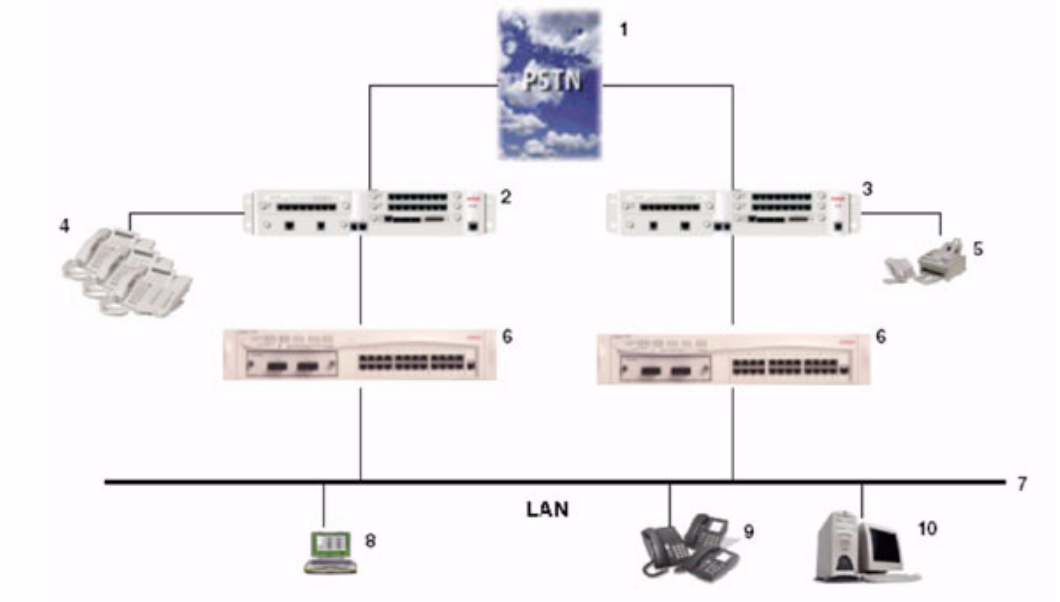
4) Layer 2 switch
5) Local Area Network
6) Administration PC
7) IP Phones (IP Telephones, IP Softphones, and IP Agents)
8) Network desktop PCs and IP softphones

Multiple Avaya™ G700 Media Gateways (Mid Office Configuration)

This configuration consists of an Avaya™ G700 Media Gateway with an Avaya™ S8300 Media Server and up to nine adjunct G700s. Each G700 has a network region assignment, as do all IP endpoints. Media module endpoints have access to system resources only in the G700 housing them. IP endpoints have access to system resources in all connected network regions, on a first region preference basis. Connectivity is specified by the Inter Region Connectivity Matrix (IRCM), which is set in system administration. The number of G700s in a given Network Region will be determined by the number of media module ports required for that region and by traffic engineering the quantity of each system resource. The limit of 100 stations and 100 trunks applies to the entire system controlled by the S8300.

In this configuration as well, the layer 2 switches may be Avaya™ P330s or equivalent devices from another manufacturer.

Figure 3. Avaya™ G700 Media Gateway with Avaya S8300 Media Server and Adjunct G700



1) Public Service Telephone Network
2) G700 with two Avaya™ MM710 and two Avaya™ MM711 Media Modules

3) G700 with S8300 and three Avaya™ MM711 Media Modules
4) IP phones (IP Telephones, IP Softphones, IP Agents)
5) Analog devices
6) Layer 2 switch
7) Local Area Network
8) Administration PC
9) IP phones (IP Telephones, IP Softphones, IP Agents)
10) Network desktop PCs and IP softphones

Avaya™ G700 Media Gateway System with Avaya™ Switch LAN (Mid Office Configuration)

More IP and analog endpoints can be served by incorporating the G700 with the S8300 in a stack of Avaya™ P330 switches and additional G700s without S8300s. Within a stack of ten elements, all joined by the Octaplane connection, there can be up to ten G700s. The limit of 100 stations and 100 trunks applies to the entire system controlled by the S8300.

Avaya™ G700 Media Gateway System with WAN (Small Office with Remote Branch)

For a small office with one or more remote branches, a G700 with an S8300 provides call control to G700s at the other location through a Wide Area Network. Routers connect the G700s to the LAN, with security provided by firewalls and VPN edge access.

For survivability in case the WAN connection is lost, the remote office G700 may be equipped with an S8300 configured as a Local Spare Processor.

4 Network Requirements

Voice over IP using Avaya™ G700 Media Gateways involves components from both the data world and the voice world. Historically, these have been markedly different worlds, with distinct network designs and protocols, implementation strategies, and support organizations.

Traditional circuit-switched voice networks dedicated their entire bandwidth to voice transmission, so signal delay was rarely an issue. They were designed to ensure "five nines" — 99.999% — reliability to support such crucial communications as 911 calls. Interactive voice traffic is sensitive to jitter and delay, but can tolerate a degree of signal loss.

Packet-switched data networks, on the other hand, are less sensitive to delay and jitter problems but cannot tolerate information loss. Data network design has focused on reliable, accurate data transmission over unreliable media, regardless of delay. Network bandwidth is shared, so congestion and delay are common but do not impair data.

Within a converged network, the factors that affect the quality of data transmission are different from those that affect voice transmission. Data is generally not degraded by delay, but voice quality suffers with even small degrees of signal delay. Packet losses can corrupt a computer file, but voice tolerates some degree of packet loss.

Implementing G700s with VoIP technology requires a data network that can identify and transmit voice packets with minimal delay, giving them priority over data packets. Some high performance data networks may not be able to support voice transmission without alterations or improvements.

For more information on Quality of Service issues, see *"Administration for Network Connectivity for Avaya MultiVantage™ Software, 555-233-504"*.

Voice Traffic Prioritizing

To support voice transmission, a network must be able to give voice data packets priority in routing over ordinary data packets. G700 Media Gateways, as well as Avaya's other products for VoIP, include several standard strategies to prioritize voice traffic. These strategies include using class of service (CoS), prioritizing ports, prioritizing services, and using IEEE 802.1p/Q to set the priority bits. These products also work with all the other popular switches and routers through open standards to provide end-to-end voice prioritization.

Class of Service (CoS) and Quality of Service (QoS)

Class of Service is a method used for queuing mechanisms to limit delay and other factors to improve Quality of Service. Most CoS strategies assign a priority level, usually 0–7 or 0-63, to a frame or packet respectively. Common CoS models include the IP TOS (Type Of Service) byte, Differentiated Services Code Point (DiffServ or DSCP) and the IEEE 802.1p/Q.

Quality of Service involves giving preferential treatment through queuing, bandwidth reservation, or other methods based on attributes of the packet, such as CoS priority. A service quality is then negotiated. Examples of QoS are Asynchronous Transfer Mode (ATM), Real Time Control Protocol P), and Multi Protocol Label Switching (MPLS).

Port Priority

One prioritization scheme assigns priority based on the User Datagram Protocol (UDP) port numbers used by voice packets. The scheme gives network priority to packets from a port range. UDP is used to transport voice through the LAN because, unlike TCP, it is not connection-based. Because voice is sensitive to delay, it is better to drop packets rather than retransmit them. So, a connectionless protocol is preferable to a connection-based protocol. G700s allow defining any port range for voice priority. Routers and data switches can use these ports to distinguish priority traffic.

Differentiated Services Code Point (DSCP)

The Differentiated Services Code Point (DSCP) prioritization scheme redefines the Type of Service (ToS) byte in the IP header by combining the first six bits into 64 possible combinations. This use of the TOS byte is still evolving, but it can be implemented now by G700s. A DSCP of 40 (101000) is suggested for the expedited forwarding of packets.

IEEE 802.1 p/Q

Another prioritization scheme is the IEEE 802.1 standard, which uses four bytes to augment the layer 2 header. The IEEE 802.1Q standard defines the open standard for VLAN tagging. Two bytes house 12 bits used to tag each frame with a VLAN identification number. The IEEE 802.1p standard uses three of the remaining bits in the 802.1Q header to assign one of eight different classes of service. G700s support adding 802.1Q bytes and setting the priority bits. The Avaya™ line of data switches can switch frames with or without these VLAN headers.

Virtual Local Area Networks (VLANs)

VLANs provide security and create smaller broadcast domains through data networks by creating virtually separated subnets. Broadcasts are a natural occurrence in most data networks from protocols used by PCs, servers, switches, and routers. Creating a separate VLAN for voice reduces the amount of broadcast traffic the telephone will receive. Separate VLANs result in more effective bandwidth utilization and reduce the server burden on endpoints by not sending irrelevant packets. VLANs, a layer 2 feature, are defined in data switches and a VLAN for voice can also be specified from a list on the switch port from the IP telephone. Separate voice and data VLANs are recommended for most customers.

Network Parameters

A converged network using one or more G700s must meet a number of requirements to ensure voice quality. VoIP applications can yield poor results on data networks that otherwise run well.

The critical factors affecting VoIP quality are delay, jitter, and packet loss. Avaya recommends these minimum network requirements:

- **Network delay:** less than 50 milliseconds between endpoints.
- **Network jitter:** less than 20 milliseconds between endpoints.
- **Network packet loss:** 0.2% or less between endpoints.

Avaya also makes these general recommendations for adequate Quality of Service:

- An appropriate Class of Service (CoS) mechanism to tag voice packets and give them priority over data packets. Switched networks should use IEEE 802.1p/Q. Routed networks should use DSCP (DiffServ Code Points). Mixed networks should use both. Port priority can also be used to enhance DiffServ and IEEE 802.1p/Q.
- A fully switched network that allows full duplex and full bandwidth for every endpoint. While VoIP applications can work in a shared network with hubs or busses, switched networks ensure higher voice quality.
- The Avaya Network Assessment Services for IP Telephony Offer from Avaya, Inc. Contact an Avaya representative or authorized dealer for information on the Offer that fully reviews and evaluates your network. For more information on the Offer, see “Avaya Network Assessment” on page 49.
- VLAN. Placing voice packets and data packets on separate VLANs (subnets) prevents data traffic from competing for the same bandwidth as voice traffic. For more information, see “Virtual Local Area Networks (VLANs)” on page 39.

Avaya urges caution with these network practices:

- Network Address Translation (NAT). Most implementations use VoIP endpoints behind NAT because H.323 messages (the protocol carrying voice information) may contain several instances of the same IP address and NAT may fail to locate and translate all of them. For more information, see “Network Address Translation (NAT)” on page 48.

- Analog Dial-Up. Converged network upstream bandwidth is limited to a maximum of 33.6 K and in most instances is less. The result is insufficient bandwidth for analog dial-up connecting two locations, which may operate at up to 56K. Some codecs and networks may provide acceptable connections, but evaluate each connection individually.
- Virtual Private Network (VPN). Significant delay is inherent in some VPN products due to encryption, decryption, and additional data encapsulation, though some hardware-based products encrypt at near wire speed and may be used. If the VPN runs over the Internet, voice quality cannot be guaranteed unless delay, jitter, and packet loss meet the requirements above. For more information, see "Virtual Private Networks (VPNs)" on page 47.

Each of these factors affecting VoIP performance and several others are discussed in more detail below.

Network Packet Delay

Packet delay is the length of time it takes a packet to traverse the network from one endpoint to another. When delay exceeds 50 milliseconds, users experience difficulties in carrying on a normal telephone conversation. Packet delay is created by every element in a network: switches, routers, cables (and the distance the packet has to travel), firewalls, and jitter buffers. The delay generated by routers depends not only on hardware, but also on configurations such as access lists, queuing methods, and transmission modes. In a private LAN environment, delay or latency can be controlled, but when the public network is involved, there are inherent delays that cannot be controlled.

Networks with more than 50 milliseconds of one-way delay between endpoints will produce inferior voice quality, though some users may elect to tolerate it.

Before you implement a G700 solution, we strongly recommend an Avaya network assessment to measure network delay and make suggestions for resolving latency issues.

Network Jitter

Jitter is a measure of the variability of delay; it is the average variation in the delivery time between packets. If the variation is greater than 20 milliseconds, jitter creates audible voice-quality problems similar to those created by high latency.

To compensate for jitter, many H.323 voice applications incorporate a jitter buffer that holds incoming packets for a specified period of time before decompression. Jitter buffers smooth packet flow, but they also add to packet delay. For best quality, jitter buffers should be dynamic or, if static, sized to twice the greatest statistical variance between packets. Buffers must also have the appropriate queue-unloading algorithm.

G700s, as well as Definity® ECS, Avaya™ S8100 Media Server, IP SoftPhone software, and IP telephones, all incorporate dynamic jitter buffers to minimize delay by reducing the jitter buffer size, as the network allows. This feature can exacerbate problems in an uncontrolled network. Delay added by jitter buffers must remain within the network jitter maximum limit.

Network topology also affects jitter. Because there are fewer collisions, a hierarchical data-switched network has less jitter than a flat hub-based network.

Between endpoints, jitter should be less than 20 milliseconds. The maximum acceptable jitter value may vary depending on the type of service the jitter buffer has in relationship to other router buffers.

Network Packet Loss

Packet loss takes place when packets are sent but not received at the final destination due to some network problem. The maximum loss of packets (or frames) between endpoints should be 0.2% or less. Several factors make this packet loss requirements somewhat variable:

- Packet loss is more noticeable for tones (other than DTMF) than for voice. The ear is less able to detect packet loss during speech (variable-pitch) than it is during a tone (consistent pitch).
- Packet loss is more noticeable when the lost packets are contiguous rather than random over a period of time.
- Packet loss is more noticeable for larger voice payloads than for smaller ones, because more voice is lost in a larger payload.

Network delay *can cause* packet loss, and it may appear the network is losing packets when in fact they have been discarded intentionally.

Tools such as the Agilent (HP) Internet Advisor, Shomiti System™ Explorer, Radcom's Prism, and others measure packet loss. For more information, see "Network Address Translation (NAT)" on page 48.

Network Packet Mis-Order

When a packet arrives out of order, it is generally discarded since it makes no sense to play it out of order. Specifically, packets are discarded when they arrive later than they can be held with their contiguous packets in the jitter buffer. Packet mis-order can occur when networks send individual packets over different routes. Network loadbalancing and re-routing due to congestion or other transient difficulties can also lead to packet mis-order.

Networks that show frequent packet mis-order problems will produce low voice quality.

Multiple Transcoding

When a voice signal is converted from analog to digital or from digital to analog, with or without compression and decompression, transcoding results in a certain degradation of quality. If calls are routed through multiple voice coders, as in the case of calls on an intermediate system routed back to a central voice mail system, they may go through multiple transcodings with an audible loss of quality.

Multiple transcoding problems may be minimized by the use of a Definity® ECS feature, DCS with Rerouting (Path Replacement). This feature detects that the call coming through the main ECS has been routed from a tandem ECS, through the main, and back out to a third switch. The system then re-routes the call directly to avoid extra transcoding. Avaya products minimize transcoding, while non-Avaya products may cause slight to excessive transcoding.

Echo Cancellation

Echo often happens when a VoIP call leaves the LAN through a mis-administered analog trunk into the PSTN. Echo can result when there is an impedance mismatch between four-wire and two wire systems. An impedance mismatch in the conversion between the TDM bus and the LAN or a headset and its adapter may also cause echo. Impedance mismatch results in an inefficient energy transfer; the energy imbalance must go somewhere and is reflected back in the form of an echo. Usually the speaker hears an echo but the receiver does not.

Echo cancellers compare the received voice with the current voice patterns. If the patterns match, the canceller cancels the echo. However, echo cancellers aren't perfect, and under some circumstances the echo may be greater than the canceller can adjust. The problem is exacerbated in VoIP systems. If the one-way trip delay between endpoints is larger than the echo canceller memory, the echo canceller can't discover the pattern to cancel.

G700s and other Avaya IP Solutions incorporate echo cancellers designed for VoIP to improve voice quality.

Silence Suppression through Voice Activity Detection (VAD)

Voice Activity Detection (VAD) monitors the received signal for voice activity. When no activity is detected for the configured period of time, the software informs the Packet Voice Protocol. This prevents the encoder output from being transported across the network when there is silence, resulting in additional bandwidth savings. This software also measures the idle noise characteristics of the telephony interface. It reports this information to the Packet Voice Protocol to relay this information to the remote end for noise generation when no voice is present. Aggressive VADs cause voice clipping and can result in poor voice quality, but the use of VAD can greatly conserve bandwidth and is therefore a very important detail to consider when planning network bandwidth – especially in the WAN (Wide Area Network). G700s and other Avaya IP solutions can employ silence suppression to preserve vital bandwidth.

Fully Duplexed or LAN Switched Network

The ideal network for transporting VoIP traffic is a network that is fully LAN switched from end-to-end because it significantly reduces or eliminates collisions. A network that has shared segments (hub-based) can result in lower voice quality due to excessive collisions.

Although there are many different brands and models of data switches available, the Avaya™ line of switches are specifically designed to enable and enhance VoIP quality throughout the network.

Codec Selection

Depending upon the bandwidth availability and required voice quality, a codec that produces compressed audio may be advisable:

- A G.711 codec produces audio uncompressed to 64 kbps
- A G.729 codec produces audio compressed to 8 kbps
- A G.723 codec produces audio compressed to approximately 6 kbps

Table 17 provides comparison of several voice quality considerations associated with some of the codecs supported by Avaya products, including the G700. It should be noted that toll-quality voice must achieve a Mean Opinion Score (MOS) of 4 or above. MOS scoring is a long-standing subjective method of measuring voice quality.

Table 17. Speech Coding Standards

Standard	Coding Type	Bit Rate (kbps)	MOS
G.711	PCM	64	4.3
G.729	CS-ACELP	8	4.0
G.723.1	ACELP	6.3	3.8
	MP-MLQ	5.3	

Bandwidth Requirements

Adequate bandwidth is crucial for successful G700 implementation. The best voice quality in both LAN and WAN environments is achieved when the customer “owns” the bandwidth, endpoint to endpoint, and can shape bandwidth to optimize voice transmission. Bandwidth not controlled by the customer, such as the Internet, cannot be optimized and will exacerbate delay, jitter, and packet loss. Avaya does not recommend using the Internet for VoIP at this time.

LAN and WAN Bandwidth Requirements

The following tables summarize common bandwidth requirements. Table 18 describes LAN bandwidth requirements for several codecs; Table 19 and Table 20 describe WAN bandwidth requirements for several codecs. Because there are so many variables, such as payload size and actual transmission rates, **all values are approximate.**

Table 18. LAN Bandwidth Requirements

Codec Type	Data Rate in Kbps	Data Bytes per 30ms voice frame	Total L2 Frame Size in Bytes	No Silence Suppressed in Kbps	One Side Silence Suppressed in Kbps	Both Sides Silence Suppressed in Kbps
G.711	64	240	298	158,93	119.20	79.47
G.729	8	30	88	46.93	35.20	23.47
G.723	5.3	20	78	41.60	31.20	20.80

Table 19. WAN Bandwidth Requirements

Codec Type	Data Rate in Kbps	Payload Size in Bytes	Full Rate PPP or FRE.12 in Kbps	PPP with CRTP in Kbps	PPP with VAD in Kbps	PPP, VAD, and CRP in Kbps
G.711	64	240	76	66	50	43
G.729	8	20	26.4	11.2	17.2	7.3
G.723.1	5.3	20	17.5	7.4	11/4	4.8

Table 20. WAN Transfer Protocol Bandwidth Requirements

Codec Type	Data Rate in Kbps	VoIP over 802.3 in Kbps	Voice over AAL-2 in Kbps	VoIP over AAL-5 in Kbps	Voice over Frame in Kbps	VoIP over Frame in Kbps
G.711	64	71,7	N/A	77.7	65.3	70.7
G.729	8	15.7	9.5	21.2	9.2	14.5
G.723	6.4	14.1	7.7	14.1	7.6	13.0

All values in Table 20 assume a 60ms voice sample.

Table 20 highlights the fact that WAN bandwidth requirements vary significantly with different protocols. The table does not take into account VAD and header compression, but they can significantly complicate bandwidth requirements.

Telecommuter System Bandwidths Requirements

A telecommuter system is commonly used in a Call Center for users working remotely. The PC and the telephone can transmit frames across the same telephone line (Road Warrior configuration), or on two lines (Telecommuter configuration). The bandwidth used by the PC for signaling is very low. However, it is difficult to express this value in bits per second due to the variability in how quickly the buttons are pressed and how many feature buttons are used during a call. Even with a 56K (V.90) modem, the upstream bandwidth is no greater than 33.6K and the downstream is anywhere from 28.8K to 53K. The speed of each connection is determined by the PSTN line conditions at the time the call is placed. Bandwidth required for signaling is almost negligible compared to the available bandwidth for voice.

Network Security Requirements

Avaya makes the following security recommendations for all networks incorporating G700s:

- All portions of the system should reside behind a firewall. Different elements of the system may reside in separate network segments, but each segment should be protected by a firewall. All network elements must have routeable addresses from segment to segment without address translation.

  When address translation must be used (e.g. to support a single Road Warrior PC logging in over a hotel's LAN, using the IP address owned by the hotel for the IPSEC packets) the VPN solution that performs address translation must support H.323 and translate the embedded IP addresses in the H.225 messages. Since encryption prevents translation at the firewall, the Road Warrior H.225 streams must not be encrypted by the endpoint or switch.

- Networks should employ switched hubs throughout. Not only does this help QoS, but it greatly reduces opportunities for eavesdropping.
- If a G700 or an IP phone is placed outside of the protected corporate network, the firewall must be opened up to allow UDP traffic to pass through as well as to allow dynamic port allocation (This weakens the firewall and is not desirable).
- Care must be taken in the installation of the TFTP server used to serve firmware to the various portions of the G700 system. TFTP is not a secure protocol. The TFTP server should be isolated so that only the minimum necessary data (e.g. IP phone firmware) is present on it and the server provides only read access to the files it serves.

IP SoftPhone Requirements

An IP SoftPhone is a software PC that simulates a telephone (Road Warrior configuration). The VoIP perceived audio/voice quality at the PC endpoint is a function of at least four factors:

- **Transducer Quality.** The quality of the speaker and microphone or headset has an impact on the reproduction of the sound.
- **Sound Card Quality.** Several parameters affect sound card quality, the most important of which is whether or not the sound card supports full-duplex operation.
- **End-to-End Delay.** A PC can be a major component of delay in a conversation. PC delay consists of the jitter buffer and sound system delays, as well as the number of other processes running and the speed of the server.
- **Speech Breakup.** Speech breakup may be the result of a number of factors: network jitter in excess of the jitter buffer size, loss of packets (due to excessive delay, etc.), aggressiveness of silence suppression, and performance bottlenecks in the PC. Lower speed PCs and those with slow hard drives may be unable to support quality sound playback and recording, which results in breaks in received or transmitted audio. When this happens, increase the server speed, increase the amount of RAM, and reduce the number of applications competing for server or hard drive resources. One notable resource consumer is the Microsoft® Find Fast program that periodically re-indexes the hard drive and consumes significant PC resources.

Other Elements Affecting VoIP Quality

Several other network factors may have an impact on voice transmission, including overall network reliability and architecture. Sections below describe those factors and make recommendations to limit the impact.

WAN Data Packet Size

Large data packets may result in added delay for VoIP packets across WAN links with limited bandwidth. Smaller VoIP packets may be held in queue while larger data packets are processed onto a WAN link. To avoid excessive delay, there may be benefit to fragmenting the larger data packets and interleaving them with the smaller voice packets. One technique is to adjust packet size by altering the Maximum Transmission Unit (MTU) size. Minimum MTU size should be no smaller than 300 bytes and no larger than 550 bytes. LAN based MTUs can be as large as 1500 bytes. However, reducing the size of the MTU will add overhead and reduce the efficiency of data applications. Other techniques, such as Multilink PPP (MPP) Link Fragmenting and Interleaving (LFI), and Frame Relay Fragmentation (FRF12) allow network managers to fragment larger packets and permit queuing mechanisms to speed the delivery of Real Time Protocol (RTP) traffic without significantly

increasing protocol overhead or reducing data efficiency. Header compression protocols like CRTP (Compressed Real Time Protocol) can and should be used between WAN links.

Virtual Private Networks (VPNs)

Virtual Private Networks are encrypted tunnels carrying packetized data between remote sites. VPNs may use private lines or the Internet via one or more Internet Service Providers (ISP). VPNs are implemented in both dedicated hardware and software, but they can also be integrated as an application to existing hardware and software packages. A common example of an integrated package is a firewall product that can provide a barrier against unauthorized intrusion, as well as perform the security features needed for a VPN session.

The encryption process can take from less than 1 millisecond to 1 second or more, at each end. VPNs represent a significant source of delay and, therefore, negatively affect voice performance. As most VPN traffic runs over the Internet and there is little control over QoS parameters for that traffic, voice signals may suffer packet loss, delay, and jitter. A VPN provider may be able to guarantee an acceptable level of service, but before implementing VoIP with a VPN, test the VPN network to make sure it meets the minimum delay, jitter, and packet loss requirements.

Frame Relay

Information transported over frame relay is subject to greater delay and jitter than data transported over ATM or point-to-point TDM circuits. In a frame relay environment, the Committed Information Rate (CIR) must be sufficient to support peak voice traffic or some threshold for voice traffic as determined by the network administrator. Then prioritize the voice traffic. One method to prioritize voice is to enable priority queuing at both ends of the frame relay link, so that voice traffic is always processed and delivered out the WAN link first.

Maintain all voice traffic within the CIR because delivery of burst traffic is not guaranteed while delivery of CIR traffic is guaranteed. Service providers will contract to meet a customer's traffic delivery requirements within the CIR through Service Level Agreements (SLAs). Carriers usually will not contract to such an extent, or at all, for burst traffic. Burst frames--frames marked Discard Eligible (DE)--are either queued until network congestion subsides, or they are discarded entirely.

Under the best circumstances, frame relay is still inherently more susceptible to delay than ATM or TDM. Even with these recommendation implemented, expect more delay over frame relay than would be present under ATM or TDM.

Network Address Translation (NAT)

VoIP does not work well with networks that use Network Address Translation (NAT) because most NAT implementations do not support H.323 protocols. The destination IP address is encapsulated in more than one header: the Q.931, H.225, and IP headers. NAT changes only the address in the IP header resulting in a mismatch that prohibits the control of calls. Avaya does suggest implementing a firewall to guard against intruders, but the firewall should not provide NAT functions for VoIP packets, unless it is Q.931 friendly like the Lucent 201 Brick.

5 Network Assessment

An Avaya™ G700 Media Gateway installation first requires an assessment and evaluation of the existing data and voice infrastructure. A network assessment normally includes network maps, a device inventory, and network baseline information.

A successfully converged network may require increased bandwidth and higher performance, particularly in the data infrastructure. The network must have adequate capacity to support the load introduced by voice traffic. Links with high peak or busy hour utilization may require upgrades. Devices that have high levels of utilization in the CPU, the backplane, or memory, or that show queuing drops and buffer misses may also require upgrades. Overall network capacity must be adequate to support voice transmission.

Avaya strongly recommends customers adopt the Avaya Basic Network Readiness Offer described below. Customers who do not avail themselves of this offer assume responsibility for all network-related problems. Avaya personnel may be required to charge a higher T&M rate if assistance is requested later, since troubleshooting will be more difficult without the assessment data.You can initiate a network assessment by contacting your Avaya representative or authorized dealer

Avaya Network Assessment

The Avaya Network Assessment Services for IP Telephony solutions consists of two phases. In the first, the Customer Infrastructure Readiness Survey (CIRS) provides a high-level evaluation of the customer's LAN/WAN infrastructure. It determines where significant network issues exist that must be dealt with prior to deploying the newly proposed IP Solution. This evaluation results in a formal CIRS Report prepared by the Converged Voice and Data Networking team.

The second phase is Network Assessment/Network Optimization (NANO), which takes information gathered from the CIRS, performs problem diagnosis and provides functional requirements for the network to implement an IP Telephony Solution.

CIRS is highly recommended in all cases, and in the case of a dealer installation it should be considered a requirement.

Customer Infrastructure Readiness Survey (CIRS)

The CIRS is a new service offer designed to provide assurance to Avaya customers that their data network is capable of supporting Voice over IP (VoIP) applications such as Definity® IP Solutions before installing the Avaya application. Working onsite with interactive questionnaires and innovative software tools, Avaya eCommunication Professional Services network engineers will perform these network readiness investigations:

- Identify all equipment in the customer's network, as well as physical and network layer information, device connections, network topology and device configurations.
- Test the customer's current network infrastructure to discover any throughput and response time issues in multi-protocol networks.
- Baseline existing application performance measures.
- Ensure that voice traffic will receive proper prioritization in the network by verifying existing prioritization schemes and recommending improvements when the existing schemes are insufficient.
- Provide a baseline to compare pre-implementation and post-implementation views of the customer's network.

Network Analysis/Network Optimization (NANO)

The Network Analysis/Network Optimization (NANO) takes information gathered from the CIRS, performs problem diagnosis and provides functional requirements for the network to implement an IP Telephony Solution. A NANO is required when the CIRS indicates that the customer's network, as it is configured, will not support the proposed IP Solution at the desired performance levels. There may be cases where a customer acknowledges in advance that their existing network has not been configured to support the addition of an IP Telephony solution and may choose to order a NANO upfront (It should be noted that the assessment will still involve two phases, requiring the CIRS to be completed as the first phase). Customers may also request a NANO to optimize their network.

The majority of NANO opportunities will be the result of a CIRS recommendation. The NANO Offer was designed to perform an in-depth network analysis, providing the functional requirements and recommendations for a network design that optimizes all available resources and any additional resources that may be required to support the IP Solution and the enterprise business needs.

The NANO offer includes scheduled on-site evaluations, traffic throughput simulation, testing of the network, analysis of the results and recommendations to resolve any network throughput issues.

Network Tools

Many tools are available to determine latency, jitter, and packet loss on IP networks. Tools fall into several categories: reactive and proactive, passive and active. Passive tools are reactive and "sniff" the network to display or capture existing (real) traffic. Active tools inject packets into the network to test network characteristics (proactive) or to stress test specific network elements. Modeling tools are also proactive because they model future "what-if" scenarios without inducing a load on the network. A partial list of these commercial tools follows.

These tools are available for purchase through their respective vendors and have been found to be very useful for diagnoses, analysis, modeling, and monitoring networks and VoIP conversations. None of these tools are specifically endorsed or explicitly warranted by Avaya Inc. They merely represents a starting list of tools that fit the active, passive, and modeling categories that are needed to properly assess networks and network products. Other tools exist that may be a better fit for your organization.

- **Shomiti Systems Explorer.** This hardware-based tool measures delay, cell loss and jitter at wire speeds from 10Mbps to 1000 Mbps and provides a seven-layer decoding of captured frames. Because it has a dedicated server for sensing traffic, results are more accurate than with software-based tools. It normally acts in passive mode by "sniffing" traffic. It can also be an active device by injecting packets into the network. Information is available at http://www.shomiti.com.
- **Ixia™ 100™ QoS Performance Tester (also the 400™ and 1600™).** This hardware-based tool is both a traffic generator and performance analyzer. It measures delay, jitter and cell loss from 10 to 1000 Mbps. It is scalable to higher speeds as it can use OC3 through OC192 for generating traffic. The results are available for pre- and post-processing by the user and the software code is open for users to customize. Information is available at http://www.ixiacom.com.
- **NetIQ™ Chariot™.** This software tool allows customized traffic generation controlled from a server between two PC endpoints. Traffic is created by selecting pre-made scripts or writing your own and represents data from the application level. Lower level (OSI layers 4, 3 and 2) traffic is also available to configure and send. Information is available at http://www.NetIQ.com.
- **Fluke® Enterprise LANmeter®.** This all-purpose hardware instrument can be used as a traffic generator and diagnostic tool, or to check Category 3 and 5 cables, simulate an endpoint, etc. It will not test fiber (yet), but it is very portable and capable of troubleshooting a LAN. Results can be viewed from a Web browser and an online database option is available. Information is available at http://www.fluke.com.
- **OPNET® IT DecisionGuru and Modeler.** OPNET produces "Cadillac" software products that will discover network elements and model the behavior of a LAN. This predictive feature is a good way to test changes to the network before implementing the actual hardware. The accuracy of results to real world experience ranges from 80 to 95 percent, which is higher than most mathematical only models because each element performs like the physical unit it represents. The code is partially open and users can create new objects or modify existing ones. This is a good proactive tool for network analysis. Information is available at http://www.opnet.com.

- **Network Associates® Sniffer® tools.** These industry-standard frame-capturing tools are very handy for examining and verifying content of OSI model layers 2, 3 and 4. They cannot measure latency or cell loss. They are portable and also analyze long-term network trends. Information is found at http://www.nai.com.

Network Infrastructure Assessment

Network topology maps, device inventories, and baseline measurements are required to determine if the existing network can support VoIP with G700s or whether upgrades are required. All links and devices must have sufficient capacity to support the network load introduced by VoIP.

LAN Assessment

A Local Area Network assessment determines whether the current network infrastructure and bandwidth will support G700 telephony with adequate voice quality or whether network upgrades are necessary. A LAN assessment gathers information in a number of categories described below.

Network Topology

In most cases, LAN infrastructure follows the standard distribution and core configuration. In smaller network environments, standard layers may be collapsed. A complete network topology map indicates the layers, devices, media, and port speeds, as well as servers, firewalls, and gateways.

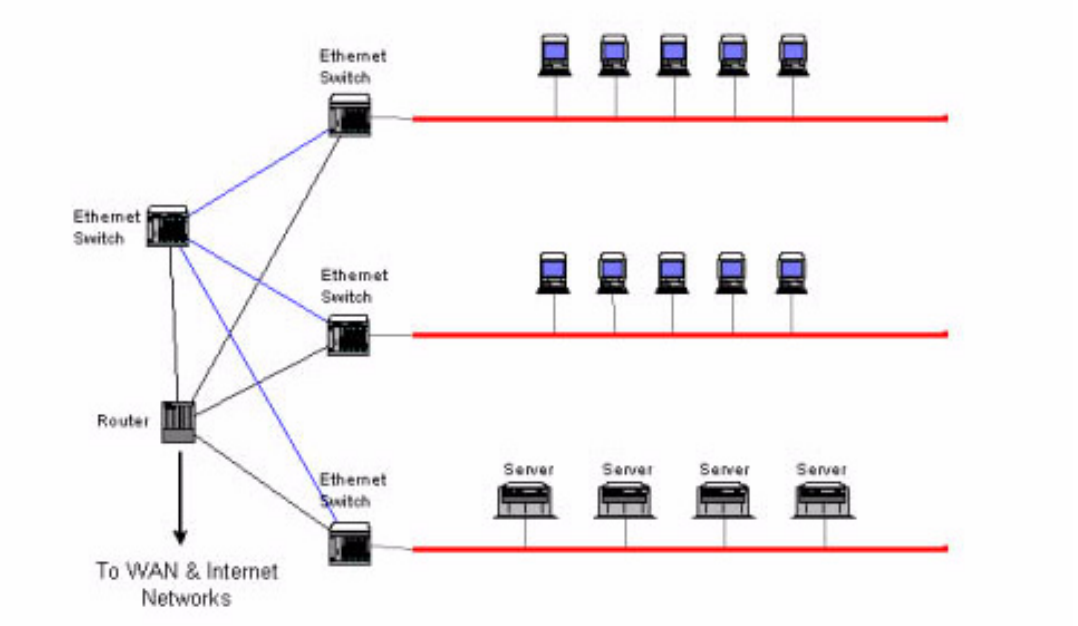


Figure 4: Sample LAN Topology Map

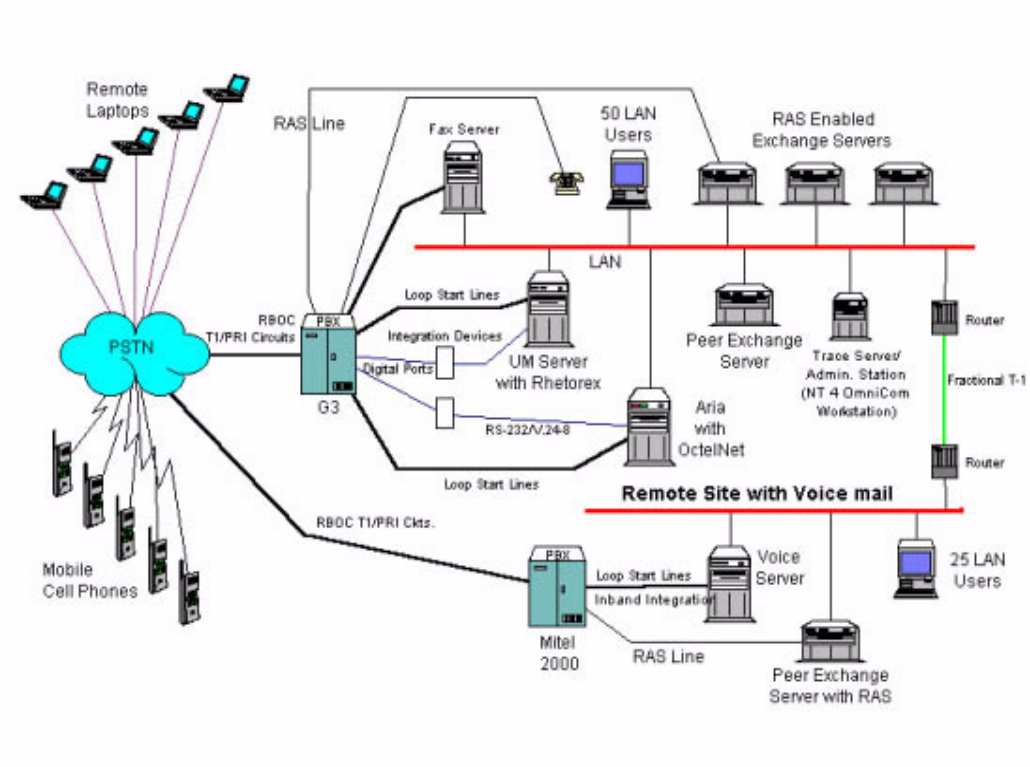


Figure 3: Sample LAN Topology Map

LAN infrastructure requires assessment in terms of the following:

- Network availability
- Network scalability
- Available average bandwidth
- Available peak or burst bandwidth
- QoS implementations
- Desktop/phone QoS
- Layer 2 and 3 convergence

Servers and Existing Gateways

LAN assessment identifies and locates all TFTP servers, DNS servers, DHCP servers, NAT gateways, firewalls, and existing gateways within the network, including any existing communication control servers. Server assessment includes level of availability, scalability, and available bandwidth.

Network Devices

An inventory of network devices by type, number deployed, software installed, and services supported can help identify potential bottlenecks in VoIP data flow. Such an inventory identifies switched and shared media, bandwidth usage, users per link, and devices per subnet.

Baseline Performance

Baseline network performance measurements include the following:

- Device average and peak CPU utilization
- Device average and peak memory utilization
- Peak backplane utilization
- Average link utilization (prefer peak hour average for capacity planning)
- Peak link utilization (prefer five minute average or smaller interval)
- Peak queue depth
- Buffer failure rates
- Average and peak voice call response times

Addressing Plan

LAN assessment includes a review of the IP addressing plan and takes into consideration core routes and subnets, route and DHCP server plans, as well as any DNS conventions in effect. The IP addressing plan review should check for duplicate IP addressing and for subnet overlap. The addressing plan must be adequate to include the new addressing required when G700s are introduced.

Protocol Implementation

LAN assessment catalogues the current network protocols to determine whether they match or can coexist with the protocols supported by G700s. Protocol analysis covers IP routing protocols, summarization methods, and routing protocol safeguards. It also takes into account HSRP configuration, VTP and VLAN configuration, and IPX, DLSW, or other required protocol services.

LAN Assessment Form

Table 21 shows a sample LAN assessment form.

Table 21. LAN Assessment

LAN Location
File Servers File and print, database or application, intranet servers

Table 21. LAN Assessment *Continued*

Terminal services Windows Terminal server or X
Internet servers DNS, TFTP, and Firewalls. PORT Filtering or NAT in use. Web, dynamic application and database servers.
Intranet servers DNS, TFTP, and Firewalls. Web, dynamic application and database servers.

Table 21. LAN Assessment *Continued*

Extranet services Detail any services offered via extranet and usage patterns.
Ethernet/Gigabit Ethernet/FDDI/Token Ring hubs and switches Show segments and head counts per segment.
Intermediate distribution facilities/wiring closets List distances for Category 3 or 5 wiring.
Segmenting via routers or switches Layer 2, layer 3, and/or VLAN. If layer 3 and/or VLAN used, attach map showing logical topology
3 of 7

Table 21. LAN Assessment *Continued*

LAN printers and fax systems
Routed protocols per segment TCP/IP, IPX/SPX, etc.
Multicast enabled on network devices Indicate if multicast is in use. Multicast mode in use. Purpose and scope of deployment.
Routing protocols per segment RIP, OSPF, etc.
Spanning Tree Indicate if Spanning Tree is in use.
4 of 7

Table 21. LAN Assessment *Continued*

Internet access for workstations Indicate number of users per segment with internet access, PORT filtering in use (if any), NAT or PAT in use.
Network operating systems on LAN UNIX, LINUX, NT4, W2000, W2000 Server, W2000 Advanced Server, OS/2, NetWare, etc.
Operating systems on LAN and desktops UNIX, LINUX, NT4, W2000 Pro, W2000 Server, OS/2, NetWare, Windows 95, Windows 98, Windows Millennium, Windows 3.1a, WFWG, etc.
Network Neighborhood Browsing Indicate whether machines are configured to make broadcasts to LAN manager 2.x clients and whether the Microsoft browsing service is enabled on server and/or client machines.
5 of 7

Table 21. LAN Assessment *Continued*

DHCP, DNS, WINS Servers List IP addresses of servers and DHCP/WINS configurations.
Network Domain Structures Define and diagram DNS name space. If NT is used, show domains and trusts.
IP addressing scheme Includes all subnets, supernets and masks.
Network management utilities in use Sniffers, SNMP/RMON/SMON based, etc. If any are in use, include recent performance data collected for the network. The data should include net available bandwidths, data loss rates, latency, and if possible jitter for each LAN and WAN segment.
6 of 7

Table 21. LAN Assessment *Continued*

SNMP Indicate if SNMP is in use, whether enabled on all network devices, and the community names.
QoS methods in use 802.1P, Diffserve, CoS Queuing, MPLS
Video conferencing equipment List manufacturer and model of any video conferencing equipment in use on the LAN.
Policy servers List any policy servers in use.
7 of 7

WAN Assessment

A WAN infrastructure analysis is necessary when G700s are located within remote or branch offices linked to one another or to a central office by a Wide Area Network. A WAN assessment gathers information in a number of categories described below.

WAN Topology

WAN infrastructure usually follows one of the following: the hub-and-spoke model; the meshed multi-site model; or a combination of the two. A network topology map indicates the WAN devices, remote LAN devices, DNS and DHCP servers, firewalls, and gateways. It also shows network interfaces and available bandwidth.

A WAN topology map makes it possible to assess network availability, topology issues that may impact voice quality, potential for expansion, and possible bandwidth limitations.

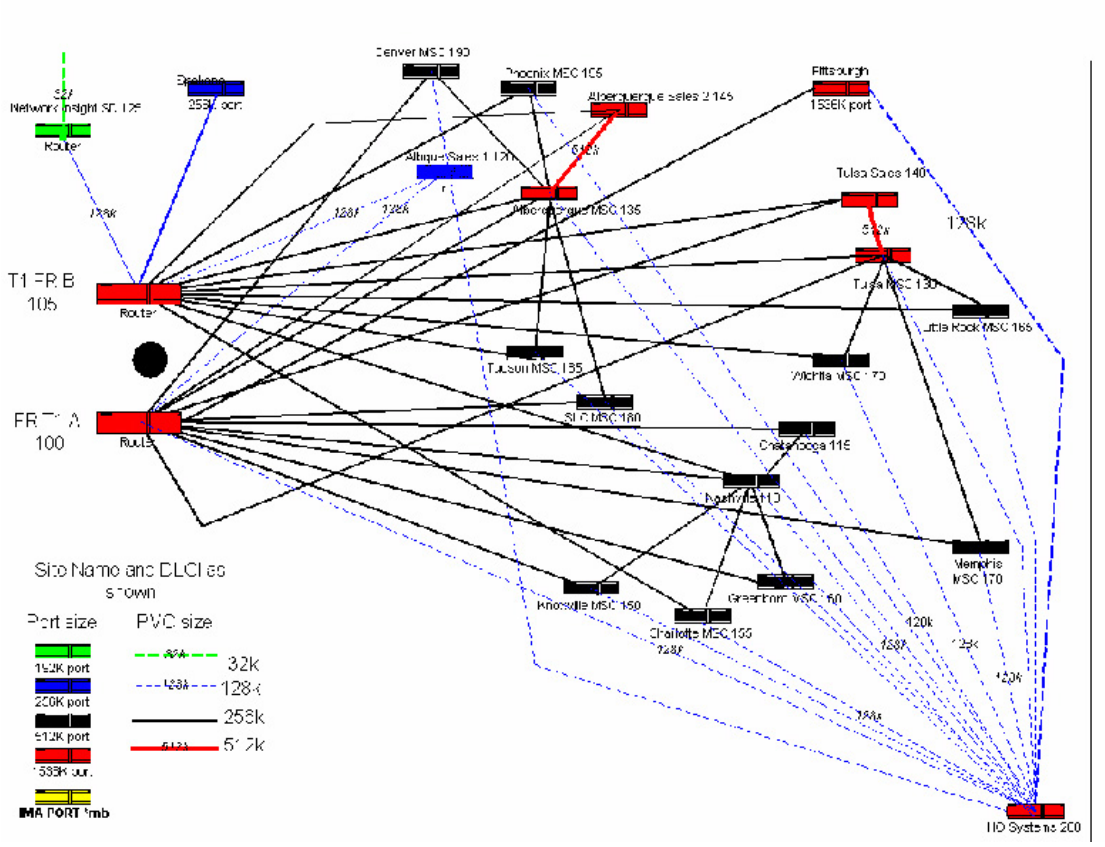


Figure 6. Sample WAN Topology Map

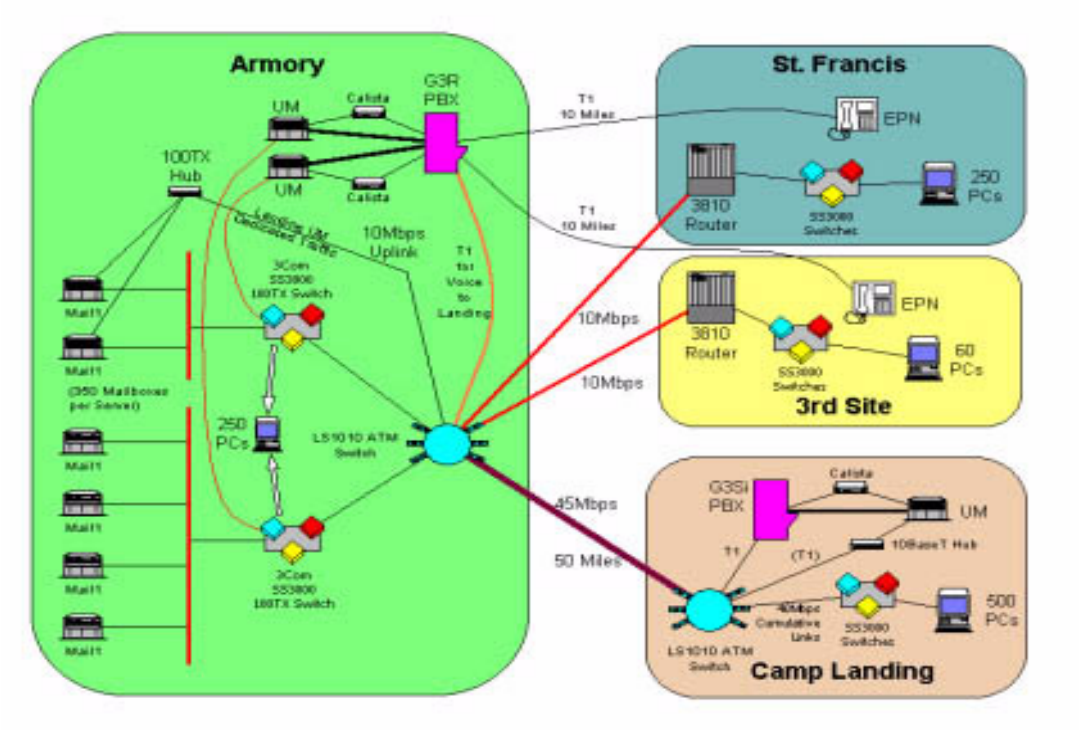


Figure 7. Sample WAN Topology Map

Servers and Gateways

WAN assessment identifies and locates all TFTP servers, DNS servers, DHCP servers, NAT gateways, firewalls, and existing gateways within the network, including any existing communication control servers. Server assessment includes scalability and available bandwidth, existing gateway support for telephony, and potential impact of WAN connection loss.

Network Devices

An inventory of network devices identifies the WAN and remote LAN devices, the number of each, the software implemented, the services configured, WAN and LAN media (switched and shares), and bandwidth. It also determines the degree of redundancy within the network.

Baseline Performance

Baseline network performance measurements include the following:

- Device average and peak CPU utilization
- Device average and peak memory utilization
- Link average and peak utilization
- Voice call average and peak response times
- Peak queue depth
- Buffer failures

Protocol Implementation

An assessment of WAN protocols includes the specific WAN IP protocol implementation and protocol overhead (including IPX and SNA protocol overhead), and Carrier Service subscription rates (port speed, CIR, expected performance). For VoIP data flow, carrier reliability and network quality are crucial factors.

Existing QoS Requirements

WAN assessment details existing WAN QoS requirements to determine if they are adequate for VoIP data transmission and compatible with the voice QoS required by G700s.

WAN Assessment Form

Table 22 shows a sample WAN assessment form.

Table 22. WAN Assessment

Routers List manufacturer and model for each.
Switches List manufacturer and model for each.

1 of 6

Table 22. WAN Assessment *Continued*

ISDN equipment List manufacturer and model.
ATM equipment Provide ATM circuit information.
Voice over IP equipment List manufacturer and model.
2 of 6

Table 22. WAN Assessment *Continued*

Bandwidth of site-to-site connections for data
Bandwidth of site-to-site connections for voice
PBX links across WAN Via ATM, VoIP, dedicated T1s
Frame Relay Circuits Include Committed Information Rates (CIRs), port speeds, PVCs, DLCIs
3 of 6

Table 22. WAN Assessment *Continued*

Circuit numbers of all circuits connected to WAN
Voice circuits (T1s, PRIs, Fractional Ts)
Data circuits (Frame, T1, Fractional, ISDN)
Remote Site applications run across WAN connections
Remote users gaining access to Internet through WAN
Remote PBX Extenders (like the EPN) using TCP/IP links through WAN
Remote users gaining access to database applications such as SQL, Sybase, and Oracle etc.
Remote users gaining access to non-database applications such as file shares, NT BDCs, or Multimedia applications.
Firewalls in place to the internet
List manufacturer and make
4 of 6

Table 22. WAN Assessment *Continued*

Firewalls in place between corporate WAN sites List manufacturer and make
Logical ports opened/blocked between corporate WAN sites
Circuit Service Provider contact information and circuit numbers
Busy Hour Reports for circuits from Service Provider
5 of 6

Table 22. WAN Assessment *Continued*

QoS methods in use Diffserve, CoS Queuing, MPLS
VPNs in use List manufacturer and model of gateways
6 of 6

Telephone Network Assessment

Telephone network assessment examines the existing stations, services, and features. While G700s may be implemented in networks based on Avaya products, they operate successfully in networks composed of equipment from a variety of manufacturers.

PBX and Key Systems

The telephone system in which G700s are incorporated may be a Definity® system, but it may also be a system based on PBX and key system from another manufacturer. Telephone network assessment creates an inventory list of the PBX and key system make and model, the locations, software, and release number of the software running on the PBX and key system, and the call features currently implemented. It also lists the number of analog and digital connections for each, as well as the ISDN trunks connected.

Messaging Systems

Intuity AUDIX may already be a part of the telephone network, but third-party voice and call messaging systems may also be in place. An inventory of the systems identifies the system models and vendors, their locations, hardware models, software features, and connection to the PBX.

Voice Trunking

A survey of existing voice trunking helps determine G700 requirements. The survey identifies the trunks, PSTN connectivity, and site-to-site trunking requirements.

Telephones and Telephone Features

Telephone network assessment identifies the number phones that will convert to VoIP, and the number of new stations. It also surveys the phone features, such as call holding, parking, or transfer, caller ID, and conferencing.

Dial Plan

The existing dial plan architecture helps determine the required call routing, abbreviated dialing, and route-group features for G700s. Dial Plan features analysis includes local extension dialing, emergency dialing call patterns, automatic call distribution, and call blocking, where individual groups or numbers have limited offnet access. It also lists any reserved number ranges, and describe the Long Distance PSTN Access Dial Plan.

Telephone Network Information and Dial Plan Forms

Table 23. PBX/Switch Environment

Manufacturer
Model
1 of 2
Software Release
Physical ports available
Via CLAN and Prowler cards.

Table 23. PBX/Switch Environment *Continued*

Automated Call Distribution capability in use List manufacturer. Indicate whether ACD services will be linked through Avaya solution or via co-located ACD teleset.
Third-party applications in use
Wireless handsets in use
Latest PBX traffic reports

2 of 2

Table 24. Dial Plan

Site Name	**IP Phone Dial Plan** Number of digits for dialing	**PBX Dial Plan** **Number of digits for dialing**	**PBX Gateway**	**Analog Phone Dial Plan** **Number of digits for dialing**	**Analog Gateway**

Table 25. Local Dial Plan Details for Specific Site

Site Name	Local PSTN Dial Pattern	**Local PSTN Access Code**	**Route Option** Route or block	**Outbound PSTN Gateway** Which gateway routes the dial pattern

Table 26. Long Distance Dial Plan Details for Specific Site

Site Name and Area Code(s)	Long Distance PSTN Calling Pattern	**Long Distance PSTN Access Code**	**Route Option** Route or block	**Outbound PSTN Gateway** Which gateway routes the dial pattern

Table 27. Inbound Dial Plan

Site Name	**DID or Two-stage Dialing** Specify IVR, auto-attendant	**Inbound PSTN Gateway** Specify which PSTN gateway routes incoming calls	**DID Number Range or IVR/AA Main Incoming Called Number**

Site, Power, and Cabling Assessment

The power and cabling infrastructure must be adequate to maintain and support the expanded network created by the introduction of G700s. Poor cabling as a result of substandard installation practices, poor patch cord management, or installations that are not standards-based or hierarchically structured may result in poor VoIP performance with G700s. Data center environments should show adequate available main power, UPS power, power plug compatibility, and heat dissipation.

For specific physical site requirements and power and grounding requirements, see *"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"*.

Table 28 shows a sample power requirements form.

Table 28. Power Requirements

Device	Power Requirement	Operating Voltages	Heat Dissipation
IP Telephony or Network	Watts		BTU/Hr

Table 29. Wiring Closet Power

Device	Power Requirement	Operating Voltages	Heat Dissipation
IP Telephony or Network	Watts		BTU/Hr

6 Network Design

In the early days of networking, designers used hubs to attach servers and workstations, and routers to segment the network into manageable pieces. Because of the high cost of router interfaces and the inherent limitations of shared-media hubs, network design was generally well done. In recent years, with the rise of switches to segment networks, designers could hide a number of faults in their networks and still get good performance. As a result, network design has suffered.

VoIP places new demands on the network that cannot be met by sub-optimal designs. Even with switches installed, designers must attend to industry best practices for a properly functioning voice network. Because users will not tolerate poor voice quality, administrators must implement a sound network before beginning VoIP pilots or deployments.

Best Practices Network Design

Industry best practices dictate that a network be designed for high reliability (with redundancy wherever possible), scalability, manageability, and maximum bandwidth.

Network Design

With VoIP, network design must be aimed at minimizing delay, jitter, and packet loss in a full duplex environment. Generally speaking, these concerns dictate a hierarchical network consisting of at most three layers: core, distribution, and access. Some smaller networks can collapse the functions of several layers into one device.

Core Layer

The core layer is the heart of the network. Its purpose is to forward packets as quickly as possible. It needs to be designed with high availability in mind. Generally, these high-availability features include redundant devices, redundant power supplies, redundant servers, and redundant links. Core interconnections increasingly use Gigabit Ethernet.

Distribution Layer

The distribution layer links the access layer with the core. Quality of Service features and access lists are applied at this layer. Generally, Gigabit Ethernet connects to the core and either Gigabit Ethernet or 100base-TX/FX links connect the access layer. Redundancy is important at this layer, but it is not as crucial as it is in the core.

Access Layer

The access layer connects servers and workstations. Switches at this layer are smaller, usually 24-48 ports. Desktop computers and workstations are usually connected at 10 or 100Mbps, and servers are connected at 100 Mbps or 1 Gbps. The access layer has limited redundancy. Some Quality of Service and security features are implemented in this layer.

Network Design Problems

Common network design problems can severely impact network performance and VoIP quality:

- A flat, non-hierarchical network (e.g. cascading small workgroup switches together) results in bottlenecks, as all traffic must flow across the uplinks (at maximum 1Gbps) versus traversing switch fabric (up to 256 Gbps). The greater the number of small switches (layers), the greater the number of uplinks, and the lower the bandwidth for an individual connection. Under a network of this type, voice performance quickly degrades to an unacceptable level.
- Multiple subnets on a VLAN will generate issues with broadcasts, multicasts, and routing protocol updates. It should be avoided. It will greatly impact voice performance and complicate troubleshooting issues.
- Hub-based networks create some challenges for administrators. It is advisable not to link more than four 10baseT hubs or two 100baseT hubs together. Also, the collision domain, the number of ports connected by hubs without a switch or router in between, should be kept as low as possible. Finally, the effective (half-duplex) bandwidth available on a shared collision domain is approximately 35% of the total bandwidth available.
- Too many access lists slow down a router. While they are appropriate for voice networks, care must be taken not to apply them to unnecessary interfaces. Traffic should be modeled beforehand, and access lists applied only to the appropriate interface in the appropriate direction, not all interfaces in all directions.
- Network Address Translation (NAT) does not coexist well with VoIP due to limitations in the H.323 VoIP standard. VoIP conversations rarely work across NAT boundaries. It is important to route voice streams around routers or firewalls running NAT or use a H.323 friendly NAT.
- Virtual Private Networks (VPN): VPNs present interesting challenges to VoIP implementations. First, the encryption used with VPNs adds significant latency to voice streams, adversely affecting the user experience. Second, VPNs generally run over the Internet. Because there is no control over QoS parameters for traffic crossing the Internet, voice quality may suffer due to excessive packet loss, delay, and jitter.

Recommended Platforms

Since the Avaya™ G700 Media Gateway is designed on the basis of open standard protocols, it can be incorporated in networks based on switches and routers from a variety of manufacturers. Make sure that network devices offer sufficient QoS features to ensure quality voice transmission. The following Avaya products have been designed with IP telephony in mind and will effectively support the high quality voice transmission offered by G700s.

Switches

- Avaya™ P-120 family (access-layer: 24 ports)
- Avaya™ P-130 family (access-layer: 24-48 ports)
- Avaya™P-330 family (access-layer: 24-640 ports, stackable)
- Avaya™P-550 family (access-distribution layer, up to 288 ports)
- Avaya™ P-880 family (distribution-core layer, up to 768 ports)
- Equivalent products from other manufacturers

Routers

- Avaya™ AP450 (branch office)
- Avaya™ AP1000 (central site)
- Equivalent products from other manufacturers

Network Architectures

Several basic packet network architectures can be distinguished, such as shared medium architectures, layer 2 switching architectures, router architectures, routed-switch architectures, virtual circuit-switching architectures, and circuit-emulation architectures. Each of these architectures has particular properties in terms of the ability to support real-time voice communication.

Shared Medium Network Architectures

Some of the best-known types of shared medium architectures are CSMA/CA, CSMA/CD and token (ring, bus) passing architectures. These architectures operate in layers 1 and 2 of the OSI reference model. The basic entity that is transferred across the medium is called a frame.

Both CSMA and token passing architectures maintain information sequence integrity and prevent information duplication. In both networks, the delay and jitter depends to a significant degree on the load on the medium. This is clearly a problem for VoIP networking. In CSMA architectures the jitter cannot be controlled at all. In token passing architectures the jitter can be limited by ensuring that all stations get fair access to the medium

Switch Network Architectures

Switch architectures are part of layer 2 of the OSI reference model. The packet delay and jitter through switch networks (e.g. Ethernet) can be minimized, if they provide cut-through switching and full-duplex operation. Packet sequence integrity can be maintained by preventing any loops in the switch network architecture, or by using the Spanning Tree Algorithm in Ethernet networks. Elimination of topological loops in a switch network prevents packets replication as well. By controlling the traffic load in the network, packet loss can be minimized.

Router Network Architectures

Routers are a major source of delay in packet networks as they store packets completely before they are forwarded (store-and-forward). The delay through a router network can be partially controlled by designing the network such that even the paths that give the longest transfer latency will have an acceptable delay. This promises, however, to be very difficult to ensure in network overload situations. Sequence integrity is not guaranteed in a router network, if load-balancing is activated, or when routes are updated. Packet loss is unpredictable in a router network.

Virtual Circuit-Switched Network Architectures

ATM, Frame Relay, X.25, and MPLS are examples of virtual circuit-switching networking protocols. An established circuit intrinsically guarantees that information is delivered in order and will not be replicated. Communication impairments through a physical circuit-switched network (such as a traditional TDM telephony network) are well-defined and can be bound easily by proper network design. However, packet delay, jitter, and loss impairments are not necessarily limited in a virtual circuit-switching network. Additional traffic control facilities and proper network design techniques are needed to restrict impairments.

Circuit Emulation Network Architectures

Circuit-emulation attempts to compensate for the impairments of an underlying connectionless (router/switch) network. In VoIP networks, RTP/UDP/IP circuit emulation is used to reduce jitter and to improve packet sequence integrity, at the expense of increased end-to-end delay such that packets can be played out at a regular rate and packets may be re-sequenced.

Network Technologies

For VoIP to work well, network links must be properly sized with sufficient bandwidth for voice and data traffic. Each voice call uses between 6.3 Kbps and 80 Kbps, depending on the desired codec, quality, and header compression used. G.729 is one of the most promising standards today, using 24 Kbps of bandwidth uncompressed. Interoffice bandwidth demands can be sized using traditional phone metrics such as average call volume, peak volume, and average call length.

Voice traffic must be given *absolute priority* through the network, and if links are not properly sized or queuing strategies are not properly implemented, it will become evident both with the quality and timeliness of voice and data traffic.

There are three technologies that work well with VoIP: Asynchronous Transfer Mode (ATM), Frame Relay (FR), and Point-to-Point (PPP) circuits. These technologies all have good throughput, low latency, and low jitter. ATM has the added benefit of enhanced QoS. Frame Relay and PPP links are more economical, but lack some of the traffic-shaping features of ATM.

Of the three technologies, Frame Relay is the most difficult WAN circuit to use with VoIP. Congestion in Frame Relay networks can cause frame loss, which can significantly degrade the quality of VoIP conversations. With Frame Relay, proper sizing of the Committed Information Rate (CIR) is critical. In a Frame Relay network, any traffic exceeding the CIR is marked discard eligible, and will be discarded at the carrier's option, if it experiences congestion in its switches. It is very important that voice packets not be dropped; therefore, CIR should be sized to average traffic usage. Usually, 25% of peak bandwidth is sufficient. Also, Service Level Agreements (SLA) should be established with the carrier, which defines maximum levels of delay and frame loss, and remediation should the agreed-to levels not be met.

The following sections discuss ATM, FR, PPP, and other available network technologies. Each section contains recommendations for implementing that technology when a VoIP device like the G700 is part of the network.

Ethernet

The classical Ethernet operation mode is referred to as half-duplex (HDX): at any given time, an Ethernet adapter can only transmit or receive data. A shared media Ethernet LAN has the following characteristics:

- Only one adapter can transmit at a time
- All stations contend for the same bandwidth

- Only one station can capture the bandwidth at any given time
- If more than one station has a packet to transmit, the medium access control (MAC) protocol will resolve the conflict and allow only one station to get access while the others wait

Ethernet LAN switches (also called layer 2 switches) isolate traffic from ports that are not involved in communication (provided they do not operate in broadcast mode). They also do not cause any shared medium collisions and can be very fast if they provide wire speed frame forwarding. Because they prevent medium sharing, they provide a much higher aggregate bandwidth. An additional feature that increases the throughput is full-duplex (FDX) operation: simultaneously receiving frames on the same input/output port pair. There are two types of LAN switching:

- Cut-Through Switching: The switch proceeds to transmit the frame out of the destination port right after it has received the destination address in the header.
- Store-and-Forward Switching: Before transmission of a frame out of the destination port starts, the complete frame is received by the switch.

Shared Medium Ethernet Architectures

"In a shared medium architecture, any single device producing high bandwidth traffic will likely corrupt all voice traffic."

Shared medium Ethernet hubs are still being used in networks, but shared media LAN architectures should be avoided in VoIP networks. More specifically, avoid the use of bussed architectures. Layer-1 hubs and layer-2 bridges should be avoided. Shared media hubs should be replaced with Ethernet switches. Shared media architectures permit packet collisions, and the collision rate increases when voice packets have to share the same medium with long data packets, when the occupancy of the shared medium is high, and when the network has low bandwidth.

In a shared medium architecture, any single device producing high bandwidth traffic will likely corrupt all voice traffic. Voice communication on a network initially working fine may degrade dramatically after adding such a device.

Ethernet Switches

Local Area Networks make common use of Ethernet switches. For quality VoIP transmission, use Ethernet switches with the following capacities:

- 802.1p standard allows stations to expedite frames
- 802.1Q standard supports VLANs, defines tagged frame types, and provides a way to maintain priorities across LANs
- Cut-through switching to improve frame throughput by forwarding frames as soon as their destination MAC address is read
- Full-duplex operation to minimize delay and increase throughput by allowing simultaneous transmission and reception of packets on ingress and egress port of the switch, thus significantly increasing the throughput as well
- Uni-directional port bandwidth of 100 Mbit/s
- 802.3af phantom power supply to power telephones

Ethernet Switch Networks

Ethernet switch networks should have these characteristics:

- Loops should be avoided in Ethernet switch networks
  Loops can be prevented by implementing a network topology without loops or by using the Spanning Tree Algorithm for logical loop resolution.
- The number of LAN-switches between any two endpoints should be minimized to reduce delay and jitter
  The target should be less than four in a campus environment.
- VoIP network traffic should be separated from data network traffic by locating each on separate VLANS

Internet Protocol (IP)

The Internet Protocol (IP Protocol) treats all traffic equally. Packets may be discarded on network congestion or may be re-ordered as they transit through the network. Traffic load-balancing may distribute traffic arriving on a single link over multiple output links. Route diversity causes unpredictable packet arrival times and extra delay due the need for packet re-sequencing at the destination. Higher-level data protocols such as TCP are assumed to accommodate transmission errors, jitter, and packet resequencing. Because of these characteristics, the IP protocol is called a “best-effort” protocol and by itself cannot guarantee quality of service because the service degrades as the network load of increases.

IP Routers

Follow these guidelines in implementing IP routers:

- Layer 2 IP routed switches should be used rather than pure layer 3 IP routers
  Layer 2 IP routed switches can significantly reduce the forwarding delay for real-time traffic by using cut-through switching for low-latency traffic.
- Implement multiple traffic class queues
- ImplementDiffServ traffic marking
- Voice and signalling traffic should be handled with the highest priority
- 802.3af phantom power supply should be provided to power telephones
- Deactivate traffic load balancing
  This can cause transfer delays and increase jitter.
- Deactivate UDP packet filtering
  This may prevent the forwarding of RTP voice packets.
- Packet fragmentation should be activated for non-real-time traffic on the node outputs with high link occupancy

IP Router Networks

Follow these guidelines in designing IP router networks:

- The number of traversed IP routers for VoIP packets between any two telephones should be minimized
  The target should be less than four in a campus environment. The delay through pure IP routers is in general very high since they store complete packets before they are forwarded.
- Cut-through Ethernet switches and Routed-switches should be preferred in VoIP networks, not pure IP routers
  Cut-through Ethernet switches and layer-3 routed-switches (for low latency traffic) directly forward frames/packets as soon as the destination address is captured, the routing table content is read, and the destined output link is free. This significantly minimizes the voice packet delay.
- DiffServ provisioning should assign voice signaling and bearer traffic the highest priority in the whole network
- The public Internet should not be used, because in most cases it does not meet the network performance requirements for VoIP.

Dynamic Host Configuration Protocol (DHCP) Service

Follow these guidelines for DHCP:

- Preferably, all IP telephone addresses on a LAN should be assigned by a highly reliable DHCP service
- Other processing intensive applications should not be running on the same server running the DHCP service
  Running other applications on the same server as the DHCP service may severely impact the performance of the DHCP by causing time-outs.

Frame Relay (FR)

Frame Relay is a high-performance interface for packet-switching networks. It is considered more efficient than X.25, which it is expected to replace. Frame relay technology can handle “burst” communications that have rapidly changing bandwidth requirements.

Frame Relay supports virtual circuit-switching, but the protocol is based on the assumption that the underlying physical network is reliable, and it is better to correct errors on an end-to-end basis to improve data traffic throughput. Packet forwarding is therefore faster than in X.25. The Committed Information Rate (CIR) indicates the data rate that the FR network should be able to handle without loss. To maintain the committed service of other users, the network may discard any data transmitted into the network at a rate beyond the CIR.

Frame Relay was not originally designed from the ground up to support voice service. It has no explicit way to limit jitter and loss through the network. Therefore, a reasonable quality of voice service can only be provided if the FR service provider limits the number of users on the network, and sufficient bandwidth is available on all the links between the FR switches in the network.

Follow these guidelines when implementing G700s in a FR environment:

- No more than one FR network should be used in series with one or more circuit-switching networks
- The FR service should have a sufficient committed information rate
- The service provider should guarantee a degree of service commensurate with the voice packet traffic impairments specified earlier

Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is an international ISDN high speed, high volume, packet switching transmission protocol standard that uses virtual circuit-switching technology, as well. It improves on the capabilities of Frame Relay, and offers up to 622 Mbit/s interfaces. ATM is capable of transporting efficiently a combination of voice, vide, and data. It is the only mature QoS packet based technology that has been developed from the ground up to carry both voice and data.

ATM is currently deployed most often as a connection-oriented layer 2 WAN backbone transport technology. ATM was also envisioned as an ideal technology to maintain QoS in a LAN environment, but less expensive Ethernet has been adopted on a wider scale in LAN environments. ATM can now be found in WANs as ISP transport technology and in large corporate campus environments as backbone LAN interconnect technology.

Follow these guidelines when implementing G700s in an ATM environment:

- No more than one AAL-1/ATM network should be used in series with one or more circuit-switching networks.
- AAL-1/ATM should not be used in series with VoIP networks.

Multi-Protocol Label Switching (MPLS)

Multi-Protocol Label Switching is a layer-2 (upper part) virtual circuit-switching forwarding protocol that was designed to improve packet arrival time predictability (jitter reduction), speed up packet forwarding by hardware forwarding of payloads, and solve network scalability problems by traffic engineering.

MPLS has been developed for application in (wide-area) packet networks. “Multi-Protocol” refers to the fact that the same label based forwarding principle can be applied to transport different layer 2 packet technologies such as Ethernet, ATM, PPP and Frame-Relay. Thus MPLS as a networking technology is bit rate independent. The MPLS header mappings, however, are layer 2 technology dependent. MPLS label switching allows traffic from different layer 2 technologies (such as ATM, Ethernet, and PPP) to co-reside on the same wire.

Follow these guidelines when implementing G700s in a MPLS environment:

- MPLS network should be used in series with one or more circuit-switching networks.

PPP and MLPPP

PPP is a layer-2 protocol that only runs over a duplex dedicated or switched serial links. The circuit must operate in either asynchronous or bit-synchronous serial mode, transparent to PPP link layer frames. Originally PPP was designed for simple point-to-point connections over HDLC serial links. However, PPP is now compatible with all major WAN protocols (including ISDN, X.25, FR and SONET). PPP provides facilities for link quality testing, error detection, option negotiation for the network address layer, (optional) authentication, and compression.

Multi-link PPP (MLPPP) has been introduced (which bundles multiple links into one logical pipe). Extra PPP links can be added to a MLPPP connection without interrupting service. Using MLPPP, each PPP link has access to the aggregate bandwidth of all links together. Packets may be transmitted across different physical links or be fragmented across multiple physical links. Like PPP, MLPPP is independent of the underlying physical network (such as ISDN, and synchronous or asynchronous technologies) MLPPP can use many different WAN network technologies (such as FR, ISDN, X.25) simultaneously for the links. MLPPP can open links as needed. Links can be closed if there is little traffic. Inverse multiplexing is used for packet transfer.

Virtual Private Networks

The following guidelines should be followed for the deployment for WAN VPN networks:

- Service Level Agreements (SLAs) with packet network operators (carriers) should include agreements about packet impairment levels, reserved bandwidth, availability (possibly to be supported by sufficient redundancy). performance monitoring feedback, and security guarantees.
- The exact SLA parameter values for packet impairments and availability should be in compliance with the overall end-to-end budget for impairment.
- Reserved bandwidth should take into account the small network growth scenarios.
- Voice security guarantees should take into account the company corporate information officer (CIO) security policies.

IP Telephones

IP/Ethernet telephones should support the following features:

- At least a G.711 encoder, though other types of encoders may be supported as well.
- Echo-cancellation with a 64 msec echo cancellation tail.
- If equipped with a single external Ethernet port, 802.1p priority and 802.1Q VLAN indication facilities.
- If equipped with multiple external network ports or extra internal ports, an Ethernet switch supporting 802.1p and 802.1Q for priority, queuing. and VLAN functionality.
- Any internal Ethernet switch should prioritize voice and signalling over data with voice and signalling at the same highest priority.
- Signalling traffic transferred over a TCP connection.
- DiffServ marking assigning the highest priority to voice signaling and bearer traffic in alignment with the DiffServ class assignments in the IP routers.
- Network-facilitated telephone power.

IP Softphones

Computers running real-time softphone voice applications should support these features:

- Softphones support the G.711, G729, and G.723 codecs.
- Echo-cancellation with an echo cancellation tail of at least 64 msec. Softphones support half-duplex to the speaker/microphone, and full duplex to the headset.
- A dynamic jitter buffer should be provided. Softphones support both dynamic and static jitter buffers. Networks should have less than 50 ms of delay, 20 ms of jitter, and 1% or less packet loss.
- Multi-media readiness. The PC should have a full duplex sound card.
- Full-duplex Ethernet network interface cards. 10/100 is sufficient. Also a 28,800 of higher modem is acceptable. VPN client software is normally required for remote connectivity.
- Good quality speakers and microphone, or a good quality headset. Headsets are recommended.
- Audio signals are sent over UDP and control signals sent over both UDP and TCP.

7 Network Planning

This chapter describes how to calculate the number of Avaya™ G700 Media Gateways and the number and type of media modules required to meet particular station and trunk requirements. The final section of the chapter provides two network configuration examples for common G700 installations. The first section provides necessary background on the impact of VoIP transmission on a network.

Network Traffic

Data Impact Calculation

Each IP frame carrying voice data has the following overhead while on an ethernet LAN link:

Table 30. Data Overhead for IP Frame

Ethernet Header	14 bytes
IP Header	20 bytes
UDP Header	8 bytes
RTP Header	12 bytes
Ethernet Trailer	12 bytes
Total	58 bytes

If layer 1 (the physical layer) is to be included in the header calculation, increase this result by 8 bytes. If 802.1 p/Q fields are included, increase by another 4 bytes.The one-way voice data rate for each of the codecs is given in kilobits per second (kbps). To convert this to bytes per 30 ms, multiply by 30/8. Add the result to the header/trailer overhead (58) to get the total frame size. For example, a G.711 64 kbps voice sample is 64 x 30/8 = 240 bytes. Dividing by the compression ratios for the other codecs yields their data bytes per 30 ms frame. Adding on 58 bytes for the header/trailer yields the total 30 ms frame size.

Table 31. Calculation of 30 ms Voice Sample IP Frames

Codec	Compression Ration	Data Bytes' 30 ms Frame	Total Frame Size (bytes)
G.711	1	240	298
G.729	8	30	88

Table 31. Calculation of 30 ms Voice Sample IP Frames *Continued*

Codec	Compression Ration	Data Bytes' 30 ms Frame	Total Frame Size (bytes)
G.723a	10	24	82
G.723b	12	20	78

To calculate the data rate of these frames, multiply by 8/30. For example, the G.711 result is

298 x 8/30 = 79.5 kbps

To determine the data rates for other frame sizes, convert the 30 ms data bytes per frame to the appropriate result, add on the header, and convert to kbps. For example, to calculate the G.711 rate for 10 ms frames, divide the 30 ms result (240) by 3, add 58, and multiply by 8/10. The result is 110.4 kbps. G.711 and G.729 frames are multiples of 10 ms. G.723 frames are multiples of 30 ms. For voice quality reasons, frames should not exceed 60 ms.

Table 32. LAN Impact of One-Way Call (kps)

Codec	Voice Sample Size					
	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	110.4	87.2	79.5	75.6	73.3	71.1
G.729	54.4	31.2	23.5	19.6	17.3	16.7
G,723a	N/A	N/A	21.9	N/A	N/A	14.1
G.723b	N/A	N/A	20.8	N/A	N/A	13.1

Grade of Service and Queuing

In the basic queuing model, service requests, such as phone calls, from traffic sources arrive at a service facility of one or more servers. The stream over time of service requests is the arrival process.

Since service facilities--TDM buses, trunk groups, and touch tone receivers--are relatively expensive, they are usually sized to grade of service (GoS) rather than to the maximum traffic possible. Grade of service is usually designated in the form "P001," which indicates that the probability of a service request finding all servers busy is 1 in 1,000 or 0.001. P01 is typical for trunk groups, P001 for port network resources, and P0001 inter port network resources.

The load associated with individual entities, such as stations or trunks, is traditionally represented in units of "Cent Call Seconds", or CCS. One CCS is 100 call seconds. The load associated with a group of entities, such as a trunk group or a TDM bus, is usually represented in Erlangs. The Erlang load is the time average number of entities busy for a given time period. The EBC calculation for the number of servers provides the GoS "buffer" required on top of the carried load in Erlangs.

Facilities are usually sized to load during the "Busy Hour". This usually means the busy hour of the year. Switching systems are usually rated by the number of busy hour calls (BHCs) they can support.

The offered load to a service facility over an interval is the mean or expected amount of time required to serve all arrivals during the interval. The carried load is the expected load the service facility will handle. The following equation usually holds:

Carried load = Offered Load x (1 - GoS).

The arrival process for telephone traffic to a switch such as a central office or PBX can typically be modeled as a Poisson Process. If the arrival process is Poisson, the time between arrivals has an exponential distribution. Queuing models with Poisson arrivals are said to be infinite source models, because the number of arrivals in service has no effect on the arrival process. Service times for arrivals are usually assumed to be exponentially distributed for telephony traffic. If blocked arrivals immediately leave and never return, the queuing model is called an “Erlang B”, or EB. If blocked arrivals always queue, and there is no queue limit, the model is called an “Erlang C” or EC. In a “Retrial” queuing, a percentage of blocked arrivals retry after an exponentially distributed period which is the same as the service time. The retrial model becomes the Erlang B if the percentage of retrials is 0.

In the EB and EC models, three numbers are significant: the load (carried or offered), the GoS, and the number of servers. Any two determine the third, and tables of these relationships are widely available, as are algorithms for computer calculation. Let EB(.) and EC(.) be the functions that return the number of servers for the Erlang B and Erlang C given the carried load and the grade of service. The following always holds:

EB(.) < EC(.)

The standard retrial tables mentioned earlier give an intermediate result, but these tables were designed for PSTN traffic. For PBX users, the time between retrials is much shorter. To account for retrials in a PBX environment, use an average:

EBC(.) = ½ EB(.) + ½ EC(.)

For low blocking levels, all of these results are approximately the same, so using a simple Erlang B is usually sufficient.

Another type of model is the finite source or “Engset” model. In this model, the arrival process is no longer Poisson. There are a finite number of traffic sources. Service times are exponential. The time between service completion and a new service request for a given source is exponential.

The Engset is used when the ratio of the number of sources to servers is small. To avoid using this model, check to make sure that the number of sources is not less than the number of servers provisioned using the EBC calculation. If so, size the facility to the number of sources.

Traffic Configuration Guidelines

Once a customer's station and trunk requirements are established, determine the number of Avaya™ Media Modules and G700s required *per network region*. This determination must also allow for Avaya™ S8300 Media Servers configured as LSPs (Local Survivable Processors).

Network regions are used to pool devices with LAN like connectivity. IP stations are assigned the network region of the communications server they used in registration. IP trunks are assigned the network region of the near end IP address of the signalling group used. Inter-region connectivity is specified by administering the inter-region connection matrix.

G700 VoIP resources cannot be shared between connected network regions. G700 resources are assigned using a round robin scheme for IP endpoints in the same region. If a request for a resource is denied by a G700, the call is dropped.

Each of the steps in the general traffic configuration procedure is detailed afterwards.

General Network Traffic Configuration

Network Traffic Configuration

Begin

1. Determine the carried load and size of each TI, EI trunk. Calculate the number of Avaya™ Media Modules required for each trunk group of each type. See "Step 1. Avaya MM710 Media Module Calculation" on page 91.
2. Determine the number and the carried load of each DCP station. Compute the number of Avaya™ MM712 Media Modules required. See "Step 2. DCP Station Calculation" on page 92.
3. Determine the carried load and size of each analog trunk group. Determine the number and the carried load of each analog station. Compute the number of Avaya™ MM711 Media Modules required for the combined pool of stations and trunks. See "Step 3. Avaya™ MM711 Media Module Calculation" on page 92.
4. Using the results of the previous three steps, calculate G.711 DSP Usage and Resources. This computation involves the percent of traffic for each codec type. For Time Slot (TS) stations and trunks, assume that all calls require IP conversion. For IP stations and trunks, this computation will require the percent of traffic that shuffles. See "Step 4. DSP Resource Calculation" on page 93.
5. Determine the number of G700s to support the Avaya™ Media Modules from Steps 1, 2, and 3. Determine the number of additional Avaya™ MM760 Media Modules required by the result of Step 3. If additional Avaya™ MM712 DCP Media Modules are required, recalculate the number of G700s. See "Step 5. Initial G700 Calculation" on page 94.
6. Given the number of G700s (initially from Step 4), determine the number of Avaya™ S8300 Media Servers configured as LSPs (Local Survivable Processors). This number will include the Avaya™ S8300 Media Server, if applicable. Recalculate the number of G700s. Repeat until the number of G700s is the same. See "Step 6. Final G700 Calculation" on page 94.

7. Check to see if there is sufficient capacity for Tone Detection. See “Step 7. Tone Detection Calculation” on page 95.
8. Check to see if there is sufficient capacity for Announcements. “Step 8. Announcement Calculation” on page 95.
9. Calculate the data network impact. See “Step 9. Data Network Impact Calculation” on page 96.

End

To simplify the guidelines, the following assumptions are made:

- All Avaya™ Media Module endpoints require PCM to IP conversion. This slightly increases the DSP load, because some Avaya™ Media Module endpoints will talk directly over the TDM bus.
- IP to IP calls always shuffle.
- Calculations are performed on a region by region basis. Summing over the regions yield system results. For R1, consolidation of resources on a network class level is ignored.
- Since the S8300 Media Server, the G700 servers, and the G700 TDMs should never be overloaded, they are not included in the configuration guidelines.

Avaya™ MM710 Media Module Calculation

For each network region, perform the following procedure.

Step 1. Avaya MM710 Media Module Calculation

Begin

1. Calculate the carried load for each trunk group for each type of trunk.

   Carried Load, in Erlangs = Number Busy Hour Calls per Group x CCS per Call / 36

2. Using an appropriate GoS method (EBC or simultaneous use), calculate the number of trunks required for each group in Step 1.
3. Calculate the number of Avaya™ Media Modules for each trunk group for each type of TS trunk.

   Number of Avaya™ Media Modules per Group = Number Trunks per Group / Trunks per Media Module (rounded up)

   Trunks per Media Module = 23 (T1 out of band), 24 (T1 in band), 30 (E1)

End

Avaya™ MM712 Media Module Calculation

For each network region, perform the following procedure.

Step 2. DCP Station Calculation

Begin

1. Calculate the carried load for DCP stations.

   Carried Load, in Erlangs = Number of Stations x Number Calls per Station x CCS per Call / 36

2. Calculate the number of Avaya™ MM712 Media Modules.

   Number of Avaya™ MM712 Media Modules = Number DCP Stations / 8 (rounded up).

End

Avaya™ MM711 Media Module Calculation

For each network region, perform the following procedure.

Step 3. Avaya™ MM711 Media Module Calculation

Begin

1. Calculate the carried load for each analog trunk group.

   Carried Load, in Erlangs = Number Busy Hour Calls per Group x CCS per Call / 36

2. Using an appropriate GOS method (EBC or simultaneous use), calculate the number of trunks required for each group in Step 1.

3. Calculate the Carried Load for Analog Stations.

   Carried Load, in Erlangs = Number of Stations x Number Calls per Station x CCS per Call / 36

4. Calculate the Number of Avaya™ MM711 Media Modules.

   Number of Avaya™ MM711 Media Modules = Total Number of Analog Trunks (Step 2) and Stations / 8 (rounded up).

End

DSP Resource Calculation

In the following calculation, fG711 = fraction of the load that is G.711, and fSHF = fraction of the IP load that shuffles.

The DSP resource calculation is complicated by the fact that IP endpoints can be assigned DSP resources in their region (or in another connected region), while TS (Time Slot) endpoints can use DSP resources only in their G700. The calculation below deals with this complexity by computing a "IP centric" result (which would be correct for an all IP endpoint region), and a "TS centric" result (which be correct for an all time slot endpoint region). The TS result yields the largest number of DSP resources. Note that 43.0 Erlangs is the P001 load for 64 servers. Either result, or an intermediate value, can be used in the next step.

For each network region, perform the following procedure.

Step 4. DSP Resource Calculation

Begin

1. Using the trunk group carried loads, calculate the trunk G.711 load for each trunk group for each type of trunk.

   For TS trunk groups, G.711 load = TS trunk group load x (2 - fG711)

   For IP trunk groups, G.711 load = Number of calls x (10 / 3600) x fSHF

   Sum over all trunk groups.

2. Using the station carried loads, calculate the station G.711 for each type of station.

   For TS stations, G.711 load = TS station load x (2 - fG711)

   For IP Stations, G.711 load = Number of Calls x (10 / 3600) x fSHF

   Sum over all stations.

3. For an IP centric region, sum the trunk and station results to get the G.711 carried load. Using an appropriate GOS method (EBC or simultaneous use), calculate the number of G.711 DSPs required.

   Number of DSP Resources = Number of G.711 DSPs / 64 (rounded up)

4. For a TS centric region, sum the trunk and station results to get the G.711 carried load.

   Number of DSP Resources = G.711 carried load / 43.0 (rounded up)

End

Initial Avaya™ G700 Media Gateway Calculation

For each network region, perform the following procedure.

Step 5. Initial G700 Calculation

Begin

1. Sum the number of Avaya™ Media Modules from Steps 1 and 2. Calculate the initial number of G700s.

   Initial number of G700s = Number of Avaya™ Media Modules / 4 (rounded up).

2. Check if initial number of G700s = Number of DSP Resources from Step 3 above. If they are not equal, increment the number of Avaya™ Media Modules by (Number of DSP Resources - Initial Number of G700s), and perform the step above again to come up with a new initial number of G700s.

End

Final G700 Calculation

For each network region, perform the following procedure.

Step 6. Final G700 Calculation

Begin

1. Given the current number of G700s, determine the number of LSPs (including, for standalone systems, the S8300).
2. Increment the number of Avaya™ Media Modules by the LSP result from the step above. Update the current number of G700s.

   Current Number of G700s = Number of Avaya™ Media Modules / 4 (rounded up).

3. Repeat the two steps above within this procedure until the number LSPs doesn't change.

Note: Avaya™ Media Modules should be distributed among the G700s in a network region using a uniform allocation scheme. In particular, the estimated G.711 equivalent carried load should not exceed 43.0 Erlangs for a G700 with no Avaya™ MM760 Media Module or 97.8 Erlangs for a G700 with one Avaya™ MM760 Media Module. (For P001 GoS, EBC(64) = 43.0, and EBC(128) = 97.8). A good rule of thumb is to require an redddddf™ MM760 Media Module in G700s with 3 Avaya™ MM710 Media Modules and to allow at most two Avaya™ MM710 Media Modules in a G700 housing an S8300 or an LSP.

Tone Detection Resource Calculation

For each network region, perform the following procedure.

Step 7. Tone Detection Calculation

Begin

1. Estimate the total carried load on the resource. To this end, sum over all call classifier and tone detection types the following:

   (Busy Hour Number of detections/classification) x (Average Hold Time [in seconds]) / 3600

2. Calculate the number of G700s required to provide Grade of Service. There are eight ports per G700, which is 2.05 Erlangs @ P001 or 3.1 Erlangs @ P01.

   Number of G700s required = (Carried Load [Step 1]) / (2.05 or 3.1), rounded up.

3. Compare this result with the G700 number from Step 5.

End

Announcement Resource Calculation

For each network region, perform the following procedure.

Step 8. Announcement Calculation

Begin

1. Estimate the total carried load on the resource. To this end, sum over all announcement types the following:

   (Busy Hour Number of announcements) x (Average Announcement Time, in seconds) / 3600

2. Calculate the number of ports required to provide Grade of Service using the carried load from the step above.

3. Calculate the number of G700s required to provide Grade of Service. There are 16 ports per G700.

   Number of G700s required = Ports Required / 16 (rounded up).

4. Compare this result with the G700 number from Step 5 or Step 6.

Note: The G700s administered for announcements count against the total system limits for announcement resources.

Data Network Impact Calculation

In this calculation, OWData is the look up result, given the codec and frame size, from "Calculation of 30 ms Voice Sample IP Frames" on page 87.

For each network region, perform the following procedure.

Step 9. Data Network Impact Calculation

Begin

1. For TS and IP station and trunk calls that send silence, compute the following:

   2 x OWData x number of calls x CCS per call / 36.

2. For TS and IP calls that suppress silence, compute the following:

   OWData x number of calls x CCS per call / 36

3. For IP calls that shuffle, divide the result from either of the steps above by 2.
4. Sum the results from all steps above to get the data impact for the region in kbps.
5. Sum the region results over all regions and divide by 1000 to get the data impact, in mbps.

End

Traffic Calculation Examples

Branch Office Configuration – 1000 Avaya™ G700 Media Gateway IP Phones

An existing Definity® system with 4000 DCP stations is being expanded to connect to a new building across town via data WAN facilities. The new building will support 1000 IP telephones, and all PSTN trunking over T1 facilities. For all phones in the existing and new facilities, the call mix is (1/3, 1/3, 1/3), with 4 calls per station and 1.5 CCS per call. Trunk and local intercom calls use G.711, while intercom across the WAN uses G.729, all with 30 ms frames. Assume all IP endpoints send silence.

Step 1. Avaya™ MM710 Media Module Calculation for PSTN Trunks

The PSTN trunk load is:

(2/3)(1000)(4)(1.5)/36 = 111.11 Erlangs

EBC(111.11) = 134 trunks for P01 grade of service. This means that 134/24 = 5.58, or six Avaya™ MM710 T1/E1 Media Modules are required.

Step 2. Avaya™ MM712 Media Module Calculation

Step 2 is not necessary in this configuration.

Step 3. Avaya™ MM711 Media Module Calculation

Step 3 is not necessary in this configuration.

Step 4. DSP Resource Calculation.

For trunk calls, the G.711 usage is 111.11 Erlangs. For intercom, we can assume that 4/5 of the calls are to the main facility over the WAN (G.729), and that 1/5 is local (G.711). We also assume all intercom calls shuffle. The intercom G.711 DSP usage is

(1/3)(1000)(4)(10/3600)(2 x 4/5 + 1 x 1/5) = 6.67 Erlangs

The total G.711 use is

111.11 + 6.67 = 117.78

The number of DSP resources required, using the more conservative, or TS centric, calculation is

(117.78/43.0) = 2.74, or 3.

Steps 5 and 6. Initial and Final G700 Calculation.

To meet the requirements of Steps 1 and 2, two configurations are possible:

- Two G700s, each with three Avaya™ MM710 T1/E1 Media Modules

  In this case, the DSP G.711 port usage is

  117.78/2 = 58.9 Erlangs

  Since this number is greater than the 43.0 Erlang design criteria, an Avaya™ MM760 Media Module is required in each of the G700s, for a total of four DSP resources, even though only three were required from the Step 2 calculation. With this configuration, there are no spare slots.

- Three G700s, each with two G700s

  Since each G700 has an embedded DSP resource, no Avaya™ MM760 Media Modules are required. There are six spares (two per G700) for future expansion.

Step 7. The Tone Detection Calculation.

Tone detectors are required on incoming PSTN trunk calls. Suppose the average hold time is 4 seconds. The total tone detector usage is

(1/3)(1000)(4)(4) / 3600 = 1.48 Erlangs

The number of G700s required is

1.48/2.05 =.72, or 1

Step 8. The Data Network Impact Calculation

Since silence is sent, an active G.711 call uses 2 x 79.5 = 159.0 Kbps, and an active G.729 uses 2 x 23.5 = 47.0 Kbps. There are 111.11 Erlangs of IP station to T1 trunk traffic, all of it G.711. There 55.56 Erlangs of IP-IP traffic, 4/5s is G.729, 1/5 is G.711, and all of it shuffles. The calculation is:

[(111.11)(159.0) +(55.6)((4/5)(47.0) + (1/5)(159.0)) / 2] / 1000 = 19.6 Mbps half duplex or 9.8 Mbps full duplex

Network Composed of Avaya™ G700 Media Gateways with IP Tie and PSTN Trunking

An enterprise has offices in five different states. Each office is to be configured to accommodate 100 DCP telephones and PSTN trunking in a stand alone system. Inter-office communication will be over H.323 tie trunks. The call mix is (1/2 enterprise, 1/4 incoming from the PSTN, and 1/4 outgoing to the PSTN), with 8 calls per hour per station and 2 CCS per call. Calls from a given station to another station in the enterprise are equally likely. Each office should have an LSP for backup. Local IP traffic is G.711, and WAN traffic is G.729, all with 30 ms frames. We can assume all IP endpoints send silence.

The following calculations are for each office.

Step 1. Avaya™ MM710 Media Module Calculation for PSTN Trunks

For each office, the PSTN trunk load is

(1/2)(100)(8)(2) / 36 = 22.22 Erlangs

EBC(22.22) = 34 trunks for P01 grade of service. This means that 34/24 = 1.42 or two Avaya™ MM710 T1/E1 Media Modules are required.

Step 2. DCP Station Avaya™ MM712 Media Module Calculation

For each office, the DCP stations will require (100/8) = 12.5 or 13 Avaya™ MM712 Media Modules. Station usage is 22.22 Erlangs.

Step 3. Avaya™ MM711 Media Module Calculation

Step 3 is not necessary in this configuration.

Step 4. The DSP Resource Calculation.

For PSTN trunk calls, the G.711 usage is 22.22 Erlangs. For enterprise intercom, assume that 4/5 of the calls are over WAN IP trunks (G.729), and that 1/5 is local (G.711). The total G.711 use is

22.22 (for PSTN trunks) + 22.22 x (1/5 + 2 x 4/5) (for enterprise intercom) = 62.16 Erlangs.

The number of DSP resources required, using the more conservative, or TS centric, calculation is

(62.16/43.0) = 1.45 or 2

Steps 5 and 6. Initial and Final G700 Calculations

Fifteen Avaya™ Media Modules are required for T1s (2) and stations (13). This configuration then requires at least four G700s, which are more than enough to supply the number of DSPs required (2). Two more slots are required for the S8300 and the Local Spare Processor, This brings the number of G700s to five, with three spare slots.

Step 7. Tone Detection Calculation.

Tone detectors are required on all PSTN trunk calls, on intra-office intercom calls (1/5 of enterprise intercom), and on outgoing inter-office intercom calls (2/5 of enterprise intercom). The busy hour traffic load is 400 PSTN calls, and 400 enterprise intercom calls. If the average tone detector hold time is 4 seconds per call, the overall tone detector usage is

400 + 400(1/5 + 2/5)(4) / 3600 =.71 Erlangs

The total number of G700s required per office is.71/2.05 =.35 or 1.

Step 8. Data Network Impact Calculation

Since silence is sent, an active G.711 call uses 2 x 79.5 = 159.0 Kbps, and an active G.729 uses 2 x 23.5 = 47.0 Kbps. There are 22.22 Erlangs of T1 trunk traffic, all of it G.711 if converted to IP. There 22.22 Erlangs of enterprise intercom traffic, 4/5s is G.729, 1/5 is G.711, if converted to IP. To simplify, we assume 100% conversion. The calculation is

[(22.22)(159.0) +(22.22)((4/5)(47.0) + (1/5)(159.0))] / 1000 = 5.1 Mbps half duplex or 2.5 Mbps full duplex

8 Network Implementation and Management

Avaya™ G700 Media Gateway Installation

For more detailed installation and provisioning procedures information, refer to *"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"*.

Installation Options

Installation is performed by Avaya or other qualified personnel. The customer is responsible for overall site preparation, including equipment room and power requirements. The customer is also responsible for providing a floor plan, with equipment locations marked on the floor plan. This includes equipment in the equipment room, facility terminations, house wire terminations, and terminal or station locations by type of terminal. Avaya provides data collection forms and explanations of the data required. It is the customer's responsibility to provide the data required on the forms.

The are three options for provisioning and installation:

Base Installation

Base Installation is intended for distributors, dealers, and systems integrators who are well equipped to perform their own installations and are willing to assume all responsibility of ensuring that the Avaya™ S8300 Media Server is fully supported in the converged environment. Base Installation includes the placement of the hardware along with cabling, power-up of the hardware, checking system health and activating features (turn on RTUs or download license files).

Basic Installation

Basic Installation includes remote project management, standard software installation, trunk testing and loop-back test, end-user training delivered by the customer with media provided by Avaya, help desk, and a remote Toll fraud and Security Review.

Premium Installation

Premium Installation includes an on-site Project Manager, customized software, customized system software and networking translations, trunk installation and loop-back testing, training room set-up, Avaya on-site training, 7x24 hour, 365 day cutover support at no additional charge (excluding Avaya holidays), Help Desk, and an on-site Toll Fraud and Security Review.

Installation Procedures

Staging

Staging services involve the process of gathering and inspecting all equipment components, then assembling, configuring, testing, and completing an inventory of individual equipment or systems. This service is performed at an Avaya staging facility prior to the delivery and installation of the equipment at the client's site. Customer equipment is tested prior to shipment in a simulated network environment, which helps to ensure a smooth and rapid installation. Software and features are loaded and tested, components labeled and packed for shipment. Staging services reduce the time required on site to install equipment and load configurations, and assure the client that all ordered components power up and interconnect properly in a controlled environment.

On-Site Procedures

Onsite installation performed by Avaya or other authorized personnel follows this general procedure:

1. Verification of order and equipment
2. Physical installation in rack
3. Powering and grounding the device
4. Installation of media modules and, where necessary, the S8300 or S8300 in LSP mode
5. Cabling to switches, IP endpoints, or PSTN as appropriate
6. Configuring of internal server and assignment of IP addresses
7. Activation of license files
8. Device and system testing
9. Installation, configuration, and testing of Avaya MultiVantage™ on the S8300 and the S8300 configured as an LSP (Local Survivable Processor), where necessary

For detailed installation procedures and technical specifications for the G700 and associated cabling, refer to *"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"*

Avaya™ G700 Media Gateway Management

There are three aspects of G700 management:

- Device Management concerns itself with device configuration, diagnostics, and status reporting.
- Site/Network Management concerns itself with administration of the features that are provided by the calling and messaging applications, i.e. Avaya MultiVantage™ and Intuity. This is also known as configuration management and as fault and performance management. Site/Network Management may cover a single G700 system or a network of systems.
- System-wide Operations Management concerns itself with a variety of operational aspects of a system or network of systems, including such procedures as service management (initialization and recovery), software installation and upgrade, backup/restore of configuration data, and field support tools (i.e. event logging/viewing, alarm logging/viewing/resolution, and others).

Device Management

G700 device management concerns itself with such parameters as standard port settings, port security, redundancy modes, gateway alarming, and flow control.

Management of the G700 and the S8300 is performed with either of two tools: the Device Manager (DM) and the Command Line Interface (CLI). The Device Manager is a Java applet that is served from a built-in Web server, and the CLI can be accessed via a Telnet session, either remotely across the network or locally via an Ethernet NIC connected PC. In general, any operation that can be accomplished via the Device Manager can also be accomplished via the CLI. However, the converse is not true. That is, some operations can only be performed through the G700 CLI.

G700 Web Device Manager

Each G700 and communications server device in a G700 system contains a Web server in the form of an http daemon that serves HTML pages and Java applets. When the user's Web browser is pointed toward the URL corresponding to the MG or CC device, the Web server sends an initial Web page and then loads the corresponding Java device manager applet into the browser.

The Device Manager applet, once loaded and executed, uses SNMP get operations to obtain and display information regarding status of particular elements of the device. For elements of the device that can be configured, the DM provides a GUI element to allow the user to specify values and then uses SNMP set operations to configure the device.

The managed device contains an SNMP Agent that provides access to a Management Information Base (MIB). The MIB contains nodes for all elements of the device that can be configured or whose status can be displayed. The MIB definition is established in a collaborative effort between the maintenance subsystem designer and the SNMP Agent designer.

The Device Manager presents the graphic image of a stack of Avaya™ MultiService devices and allows management of the entire stack, including G700s, as a single device.

G700 Command Line Interface (CLI)

The G700 provides a Command Line Interface that provides access to all the data that is available through the Device Manager. A CLI interpreter parses the command and makes appropriate calls in the maintenance subsystem API to read or write the appropriate data.

Avaya™ MultiService Device Manager and Avaya MultiService SMON™ Manager

The Avaya™ MultiService suite of applications provides tools for device management and monitoring. See "Avaya™ MultiService and Avaya™ MultiService StandAlone (AMSA)" on page 105.

Site/Network Management

Avaya™ Site Administration

Voice feature configuration and fault and performance management is provided by Avaya™ Site Administration, which provides the full range of management functions needed to manage a G700 network.

Avaya™ Site Administration provides a forms-based administration tool, GEDI, that enables feature administration and maintenance control of the media modules in a G700, or other Definity® system. It also provides a set of "wizards" that provide simplified interfaces for common administrative tasks. In addition, it supports definition and scheduling of complex tasks. Avaya Site Administration is a Windows-based application that can be downloaded from a Web page hosted on the communications server and installed and executed on the system administrator's PC.

Avaya MultiVantage™

Avaya MultiVantage™ software can be administered and configured via the command line interface (i.e. SAT screens) or via the Avaya™ Site Administration application. The Avaya MultiVantage™ software CLI can also be accessed via a telnet session, either remotely across the network or locally via (laptop) PC that is connected to one of the network interface jacks on the G700.

Avaya™ MultiService Routing Manager and Avaya MultiService SMON™

The Avaya™ MultiService suite of applications also provides tools for site/network management and monitoring. See "Avaya™ MultiService and Avaya™ MultiService StandAlone (AMSA)" on page 105.

System-wide Operations Management

System-Wide Operation Management deals with the following procedures:

- System Initialization and Recovery
- Software Installation and Upgrade
- Configuration Backup and Restore
- Licensing and Feature Activation
- External Alarming
- Field Debugging Tools
- IP Infrastructure Management

In most cases, System-wide Operations Management takes place through one of the Network Management Systems described below.

Management Tools

All three types of system management — device management, site/network management, and system-wide operation management — are unified in a Network Management System (NMS). The G700 management capabilities are designed to work with both Avaya™ MultiService StandAlone (AMSA), HP-OpenView (HP-OV), and other management systems. Device Managers, the Site/Network Management applications, and the System-Wide Operations tools can be launched from the NMS. Applications that run on top of NMS platforms work with either CSVA or HPOV.

Avaya™ MultiService and Avaya™ MultiService StandAlone (AMSA)

Avaya™ MultiService is a comprehensive suite of SNMP-based applications that simplifies the task of managing complex enterprise networks. It allows enterprises to configure, monitor, and control the array of Avaya™ Campus products, including G700s, using a single, integrated suite of applications. This includes everything from device configuration to advanced switch monitoring and VLAN management.

Avaya™ MultiService works in two modes:

- Avaya™ MultiService over HP-OpenView mode, usually in multi-vendor and high-end installations
- Avaya™ MultiService StandAlone mode (without HP-OpenView), usually in low-end installations

G700 systems may use the Avaya™ MultiService StandAlone management infrastructure to administer and operate the system. Sometimes referred to as the Avaya Management Portal (AMP), the AMSA client acts as the launching point for the variety of tools that are provided for administering and operating the S8300 system. The AMP provides network viewing with standard and customizable filters, application launching, and trap logging and management. The AMSA server runs on a separate PC or Solaris workstation.

The AMP provides the ability to view network devices by device type (as defined in the NRF) or subnet. There is also the capability to define custom groupings of device types and have the console show customized views based on these groupings. Definity® application management and device management applications can also be launched from the AMP. These applications include Avaya Site Administration, the Avaya™ G700 Media Gateway and CC device managers, and Command Line Interfaces (CLI) via telnet. A new Avaya™ MultiService network-wide application, VoiceMaster, can also be launched from the AMP tabular. VoiceMaster provides a launch point for accessing the Avaya site administration tool.

Some of the specific CV and AMSA features are described below.

Avaya MultiService SMON™

Ordinary shared and per-port RMON tools provide only a partial view of overall traffic levels, typically one segment at a time. Avaya MultiService SMON™ Master application gives network managers complete visibility of all switched traffic in the network. Using embedded agents, Avaya MultiService SMON™ Master monitors the Ethernet and ATM switching fabric, providing a top-down view of all traffic traversing the entire network of switches.

Avaya MultiService SMON™ History

Avaya MultiService SMON™ Master's history feature permits analysis of past network performance and identification of bottlenecks. Avaya MultiService SMON™ statistics can be collected and stored for all switch ports simultaneously, allowing information to be recalled on demand.

Avaya MultiService SMON™ Alarms

The SMON Alarms function allows network managers to view occurring faults and take action on them. The alarms log generate a complete list of alarms, which can be ordered and filtered according to severity. SMON rules van be created so that alarms are created once user-specified thresholds reach a certain value.

DS-MON

DS-MON uses standard DSCP (DiffServ Code Point) information to provide display of traffic statistics for different categories of traffic in networks. QoS-enabled, DS-MON shows how much Internet traffic is receiving high priority and whether that is causing delays for delay-sensitive data such as VoIP.

ConfigMaster

ConfigMaster allows quick network setup and installation, as well as fast recovery for faulty devices. It allows downloading and uploading of full configuration data from Avaya™ Campus devices, thus eliminating configuration errors. Configurations can be uploaded from existing modules or devices and stored for later recall. These configurations can be applied to a new device or used to completely reconfigure an existing device. In addition, Configuration files can be exported to other sources such as Word or Excel for reporting and analysis. ConfigMaster also enables back up of configuration files, either automatically or upon user request. In addition, you may use it to trace any configuration changes.

ConfigMaster includes EZ2Rule—a new campuswide application that answers the need for QoS management. EZ2Rule eases configuration of QoS parameters as well as Access Control Lists for devices. It enables multiple devices to be configured with policy parameters simultaneously, ensuring accurate and consistent deployment of priorities in the network. EZ2Rule is designed for small sites with limited bandwidth resources. For the WAN environment, Avaya Policy Manager (see below) is appropriate.

UpdateMaster

UpdateMaster makes updating device software point and click easy. It downloads software to managed Avaya™ devices and performs all necessary software maintenance operations. UpdateMaster can also check the software versions currently in use against the latest versions available from the Avail Web site and recommend updates when a newer version is available.

VLANMaster

VLANMaster allows network managers to configure and monitor VLAN usage, maintain and assign VLAN numbering and naming across all campus VLANs, and follow additions and changes in the network. In addition, it validates VLAN name and tag values and number of VLANS in order to improve VLAN maintenance tasks.

Address Master

AddressMaster facilitates locating IP addresses and hosts in a network. It displays a centralized list of the hosts discovered in the network, and correlates between IP address, MAC address, and device port connectivity. AddressMaster automatically discovers duplicate IP addresses and port policy violations.

Avaya™ Policy Manager

Avaya™ Policy Manager is a software tool for managing policies on Avaya™ P550, P880, and P330 devices, as well as Cisco 2500 and 7500 systems. Avaya™ Policy Manager allows network policy management based on these features:

- Quality of Service (QoS) policies prioritize traffic and/or control delay or loss based on application or user identity.
- Access Control policies permits or denies visibility and connectivity to network resources through host application or user identity. They also provides security via permit/deny rules.
- Scheduling policies take effect at defined times and for specific domains.

Avaya™ Policy Manager policies can be either abstract or specific. Abstract policies concerning traffic flow and service apply across a network domain. Custom policies for traffic and service apply to a specific device, device interface, group of devices, or group of interfaces.

Avaya™ Policy Manager consists of a Policy Engine (server) and a Console user interface application (client). The Console application is a graphical user interface (client) that can reside on the same system as the Avaya™ Policy Manager server and/or on a remote server.

HP-OpenView (HP-OV)

HP-OpenView provides a somewhat richer set of functions than AMSA, but at a much higher cost. HP-OV is a suite of applications that offer network performance measurement and monitoring, network problem identification and resolution, node management, automated data backup, and other functions.

VoIP Monitoring Manager QoS Management

VoIP Monitoring Manager is a Quality of Service (QoS) monitoring/feedback tool that provides visual representation of the real-time operation of the network. All G700s come equipped with VoIP Monitoring Manager, which can be accessed directly or started through the Avaya™ MultiService Console.

VoIP Monitoring Manager provides data on QoS parameters related to VoIP quality in two forms:

- Through a client GUI application from the customer LAN or by remote access with historical as well as real-time data.
- By generating system traps/alarms to a Network Management System, whether to a local NMS station or to Avaya Services via INADS or to both,

While IP network level diagnostic and debugging tools (such as ping, netstat, tcpdump, and traceroute) are useful for diagnosing specific problems at a node or at a link, they are insufficient for monitoring RTP for per-call basis information. In addition, Avaya MultiVantage™ provides specific QoS techniques such as Differentiated Services, and an implementation of the IEEE Ethernet level priority 802.1 p/Q standard mainly ensures call quality. Despite these QoS techniques, IP networks can still suffer due to changes in

configuration, traffic load, and other factors. VoIP Monitoring Manager, which allows real-time monitoring of voice quality, is designed to identify these problems.

VoIP Monitoring Manager is technically a Real Time Control Protocol (RTCP) Monitor. Each participant in an IP based voice call experiences delay, jitter and various other problems associated transmission of real-time continuous data sent as packets over the data network. Each endpoint forwards the values that it is specifically seeing and publicizes the data through transmission of RTCP (Real Time Control Protocol) packets to the other IP call participants. The VoIP Monitoring Manager RTCP monitor receives the RTCP data sent by all participants in all calls and logs this data.

Specifically, the VoIP Monitoring Manager RTCP monitor performs these functions:

- Receives RTCP packets from network entities only that send or receive RTP-based VoIP media streams. The entities include IP endpoints, such as IP telephones and IP softphones, as well as VoIP engines running on G700s and Prowler boards.
- Publishes the RTCP data in the RTP MIB (plus extensions if necessary) via SNMP agent running on the server.
- Organizes that data for viewing by system administrators and services personnel.
- Provides traps/alarms related to QOS problems, based on values set by the customer.

VoIP Monitoring Manager is based on client/server architecture that allows the data collectors (servers) to be geographically distant from the front-end displays (clients). Standalone VoIP Monitoring Manager (apart from the Avaya™ MultiService Console) runs on Windows2000.

Each IP endpoint--IP telephone, IP softphone, G700, Avaya MM760 Media Module, or Prowler--reports the following information to its specific VoIP Monitoring Manager server during each session:

- IP Address
- Phone Number
- Round trip time (as defined in RFC 1889)
- Delay
- Jitter
- Packet Loss
- RTP payload type (codec used for a session)
- Communication server's IP Address

Delay, jitter, and packet loss measurements are calculated from the Sender Report (SR) and Receiver Report (RR). In return, the RTCP monitor returns the following information to IP endpoints:

- VoIP Monitoring Manager server IP Address
- UDP port number
- Transmission period (in seconds) (e.g., x RTCP packets every y seconds)
- Whether RTCP is Enabled or Disabled

VoIP Monitoring Manager Data Display

VoIP Monitoring Manager presents a graphic display of round trip time (in ms), delay, jitter, and packet loss (as a percentage of total packets transmitted). VoIP Monitoring Manager displays real-time Quality of Service parameters of RTP sessions associated with ongoing calls:

- For single IP addresses or E.164 telephone numbers, VoIP Monitoring Manager shows real-time delay, jitter, and packet loss data for ongoing RTP session at this node.
- For single IP addresses or E.164 telephone numbers, VoIP Monitoring Manager shows delay, jitter, and packet loss data for ongoing RTP sessions at this node during a specified date and time of day range.
- For pairs of IP addresses or E.164 telephone numbers, VoIP Monitoring Manager shows real-time delay, jitter, and packet loss data for ongoing RTP sessions between the pair.
- For pairs of IP addresses or E.164 telephone numbers, VoIP Monitoring Manager shows delay, jitter, and packet loss data for RTP sessions between the pair during a specified date and time of day range.

The VoIP Monitoring Manager graphic display is similar to Avaya MultiService SMON™. Users can easily access QoS measurements by specifying a phone number, an IP address, or a domain name, or they can request measurements for all endpoints. Users can obtain session measurements by specifying pairs of telephone numbers, IP addresses, or domain names, or they can request measurements for all sessions. Finally, users can obtain measurements for sessions that exceed certain delay, jitter, and/or packet loss values.

Traps and Alarms through VoIP Monitoring Manager

The VoIP Monitoring Manager RTCP Monitor, using the local SNMP agent, can generate traps to a trap collector specified through the Command Line Interface (CLI).

Alarm Configurations

Currently, there are two configurations in which the VoIP Monitoring Manager RTCP Monitor is capable of generating traps to a trap collector:

- Communications Server Based Alarming Architecture. All Linux-based communications servers can be configured so that it serves as the trap collector and provides external alarm notification. The VoIP Monitoring Manager RTCP Monitor can be configured to generate traps to the communications server's trap collector. The trap collector receives traps from RTCP Monitor along with external network devices such as G700s and Avaya™ P330 switches. The trap collector then feeds these traps into the syslog facility.
- Network Management System Based Alarming Architecture. In networks with a Network Management System (NMS), external alarm notifications are generated by an application running on the NMS called the Network Alarm Manager (NAM).

Alarm Conditions

The RTCP Monitor generates alarms on the following conditions. These types of alarms are predetermined and the conditions are configurable. The configuration includes a severity that is either “trap” or “warning”.

- VoIP Call QOS alarm: Maximum delay >= X and maximum jitter >= Y and maximum packet loss >= Z. Delay, jitter and loss are averaged over a moving window of 3 reception reports to smooth out inaccuracies in individual values. The maximum averaged values over the entire call are then compared with the alarm thresholds X, Y and Z.

  This alarm is generated if delay, jitter, packet loss, or any combination of the three exceed the specified values. If a single call triggers multiple alarms, only the first alarm is generated, and subsequent alarms are ignored.

- VoIP System QOS alarm: Total # of voip-callqos alarm warnings in the entire RTCP Monitor >= M over time interval T. If T is zero then the alarm will be generated as soon as the total # of warnings reaches the threshold M. If T is non-zero then the alarm will be checked every interval starting at the time the monitor is run.

  This alarm is generated if the total number of voip-callqos alarms recorded by the RTCP monitor exceeds the specified number within the specified time period.

- VoIP Terminal QOS trap: Total # of voip-callqos alarms from the same IP endpoint with status = “warning” >= N over time interval T. If T is zero then the alarm will be generated as soon as the total # of warnings reaches the threshold M. If T is non-zero then the alarm will be checked every interval starting at the time the monitor is run.

  This alarm is generated if the total number of voip-callqos alarms from one IP endpoint exceeds the specified number of a specified time period.

VoIP Monitoring Manager Administration

VoIP Monitoring Manager is administered using the IP Network Region SAT screens within the Definity® Administration process. For administration procedures, refer to the most recent SAT Administration documents.

Glossary

10/100. Fast Ethernet I.E.E.E. standard for 10 Mbps baseband and 100Mbps baseband over unshielded twisted-pair wire.

10Base-T. I.E.E.E standard for 10Mbs baseband over unshielded twisted-pair wire.

802.1p/802.1Q defines a layer 2 frame structure that supports VLAN identification and a QOS mechanism usually referred to as 802.1p, but the content of 802.1p is now incorporated in 802.1D.

Active Counter. In the context of Avaya G700 maintenance software, this describes the counter to be incremented to show status change for a maintenance object error.

AEC. Acoustic Echo Cancellation, a signal processing technique that significantly reduces the coupling of a received audio signal back into an active microphone.

Announcements. Recorded Messages played in telephony.

ANSI. American National Standards Institute.

Application Programming Interface (API). The programming interface between two software entities. For example, maintenance defines an API which is used as the interface between SNMP and maintenance.

ARP. Address Resolution Protocol, IETF STD 37: RFC 826.

ASAI (Adjunct/Switch Application Interface) is the protocol supported by the Definity® ECS (Enterprise Communication Server) that extends telephony features to adjuncts (computers).

ASCII. American Standard Code for Information Interchange.

ASG. Access Security Gateway.

Asynchronous Transfer Mode (ATM). ATM is a dedicated-connection switching technology that organizes digital data into 53 byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronous relative to other related cells and is queued before being multiplexing over the transmission path.

Avaya™ G700 Media Gateway. Media Gateway is also a term used in the H.248 protocol standard to identify the controlled entity in an H.248 relationship. While our G700 (the box) is an H.248 Media Gateway, the terms have different meanings. In Avaya™ G700 documentation, “Media Gateway” always refers to our box unless it’s used specifically in the context of an H.248 discussion.

Avaya™ Media Module. In Avaya™ G700, this refers to a removable, hot-pluggable circuit pack that can be inserted into one of four slots on the G700 box. They are approximately 6.25 x 11.00 inches in size, and interface to the buses on the G700 motherboard.

Avaya™ Media Module Slots. Four positions in the Avaya™ G700 Media Gateway for containing a variety of telephony interface circuits or an integrated Avaya™ S8300 Media Server. Support hot board swap. Each slot has access to one of the 8 L2 switch ports, the TDM bus and various control signals from the gateway server.

Avaya™ MultiService Network Manager. The network management platform developed for use with the Avaya™ product family.

Avaya™ MultiVantage. The call control application at the heart of Avaya’s Definity® and G700 Media Gateway products. Historically, this was called DEFINITY call processing.

Avaya™ Policy Manager. Software developed for the Avaya™ product line to implement policy management.

Avaya™ S8300 Media Server. The Pentium server running Linux built on an Avaya™ Media Module which runs the Avaya™ G700 applications for call control (Avaya MultiVantage™), DHCP, TFTP, HTTP, etc. This is the server used to control Avaya™ G700 in its small configurations.

Avaya™ S8700 Media Server. The open Linux server, and associated software, running Avaya MultiVantage™ software (and possibly other applications) in R11 and controlling traditional DEFINITY port networks. Its server is called the S8700 Media Server**.** When controlling an Avaya™ G700 Media Gateway, it is sometimes called an External Media Server (EMS).

BHCC. Busy Hour Call Capacity.

Border Gateway Protocol (BGP). An Internet protocol defined by RFC 1163. BGP is a TCP/IP routing protocol for inter-domain routing in large networks.

Bridge. A device that supports LAN-to-LAN communications. Bridges may be equipped to provide frame relay support to the LAN devices they serve. A frame-relay-capable bridge encapsulates LAN frames in frame relay frames and feeds those frame relay frames to a frame relay switch for transmission across the network. A frame-relay-capable bridge also receives frame relay frames from the network, strips the frame relay frame off each LAN frame, and passes the LAN frame on to the end device. Bridges are generally used to connect local area network (LAN) segments to other LAN segments or to a wide area network (WAN). They route traffic on the Level 2 LAN protocol (e.g., the Media Access Control address), which occupies the lower sub layer of the LAN OSI data link layer. See also Router.

Cascade Module. A module inserted into the back of an Avaya™ P330 family member (including the Avaya™ G700 Media Gateway), which connects the member to the Octaplane.

CCMS. Control Channel Message Set. The Media Module Manager CCMS message set and the Avaya™ G700 Media Gateway Angel CCMS message set. The message set used by the G700 Angels for control and signaling of port circuits and other G700 hardware and firmware, and for control and signaling the Media Module Manager. From the communications protocol of the same name used between DEFINITY port boards and the DEFINITY call control server (SPE).

CLAN (TN799B). Controlled-LAN. Provides TCP/IP connectivity over ethernet or PPP to adjuncts. This circuit pack in a DEFINITY port network serves as a traditional DEFINITY's network interface. It terminates IP (TCP & UDP) and relays those sockets and connections up to the traditional DEFINITY server.

CLI. Command line interface. A simple terminal interface as might be provided via telnet or a serial port providing management functions. Definity® SAT and UNIX's shell are examples.

Communications Controller (CC). The server running the Avaya MultiVantage™ application. When the CC is a Avaya™ Media Module, it's called the **Avaya™ S8300 Media Server**. In the external configuration, this is an R11 Definity® system, i.e. an Avaya™ S8700 Media Server.

Composed. This is a term defined in the H.248 standard, and describes a specific configuration where an H.248 Avaya™ G700 Media Gateway runs co-resident with its server. Occasionally this term is encountered in Avaya™ S8300 Media Server documentation to describe the G700 system controlled by an S8300, though that usage of the term "composed" is technically incorrect.

Compression. Audio coding process that reduces 64 Kbps audio streams to sub-16 Kbps rates, at the expense of delay and audio quality. Useful for transport over limited bandwidth dial-up PPP connections. Usually referred to as "CODEC" compression/ decompression. Common standard CODECs are G.723a and G.729.

CSU/DSU. A Channel Service Unit/Data Service Unit is a hardware device that in one form is about the size of an external modem. The unit converts digital data frames from the communications technology used on a local area network (LAN) into frames appropriate to a wide-area network (WAN) and vice versa. For example, if you have a Web business from your own home and have leased a digital line (perhaps a T-carrier system or fractional T-1 line) to a phone company or a gateway at an Internet service provider, you have a CSU/DSU at your end and the phone company or gateway host has a CSU/DSU at its end. The Channel Service Unit (CSU) receives and transmits signals from and to the WAN line and provides a barrier for electrical interference from either side of the unit. The CSU can also echo loopback signals from the phone company for testing purposes. The Data Service Unit (DSU) manages line control, and converts input and output between RS-232C, RS-449, or V.xx frames from the LAN and the time-division multiplexed (Time-Division Multiplexing) DSX frames on the T-1 line. The DSU manages timing errors and signal regeneration. The DSU provides a modem-like interface between the computer as Data Terminal Equipment (Data Terminal Equipment) and the CSU. CSU/DSUs are made as separate products or are sometimes part of a T-1 WAN card. A CSU/DSU's Data Terminal Equipment interface is usually compatible with the V.xx and RS-232C or similar serial interface. Manufacturers of separate unit or integrated CSU/DSUs include Adtran, Cisco, and Memotec. The CSU originated at AT&T as an interface to their nonswitched digital data system. The DSU provides an interface to the data terminal equipment (DTE) using a standard (EIA/CCITT) interface. It also provides testing capabilities.

CTI. Computer Telephony Integration.

Data Service Unit (DSU). A device designed to connect data terminal equipment to a digital phone line to allow fully digital communications. See Composed above.

DCP. Digital Communications Protocol, a proprietary digital telephone interface used on Definity®.

Definity®. Definity® describes both Avaya's flagship PBX product (hardware and software) and sometimes also the software application at the heart of the S8300 call control. That software application is now called **Avaya MultiVantage™**, though the use of the term Definity is present in many historical documents. In the context of the S8300, it almost always describes the software application, including call control software as well as maintenance and administration functions that are included with it.

Decomposed. Opposite of composed (see Composed above).

Device. This term specifically describes an entity in an Avaya™ managed network which is accessed from the Avaya™ MultiService product suite, and managed by a Java-based software entity called a **Device Manager**.

DHCP. Dynamic Host Configuration Protocol, an IETF protocol, RFCs 951, 1534, 1542, 2131 & 2132.

DiffServ: Differentiated Services (DiffServ, or DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1p tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a

packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets.

Digital Signal 1 (DS1). Primary multiplex level in North America TDM hierarchy.

DIMM. Dual In-Line Memory Modules. These are industry standard 168-pin memory modules for PC DRAM. Two DIMMs are used on TN2320.

DLCI. Data Link Connection Identifier. An identifier assigned to each data link in the LAPD protocol. It is used for routing data to its destination.

DLG. Definity LAN Gateway. This application provides the functionality of ASAI using a TCP/IP ethernet transport instead of the traditional BRI transport.

DNS. Domain Name System, a hierarchical network naming scheme. DNS servers provide a mapping of domain names to IP addresses.

DRAM. Dynamic Random Access Memory. Read/write memory which must be refreshed to maintain its contents. Used for both the MPC860 and x86 Host server on TN2320.

DS0. Digital Service, level 0, 64 kilobits per second, the worldwide standard speed for PCM digitized voice channels.

DS1: Digital signal X is a term for the series of standard digital transmission rates or levels based on DS0, a transmission rate of 64 Kbps, the bandwidth normally used for one telephone voice channel. Both the North American T-carrier system and the European E-carrier systems of transmission operate using the DS series as a base multiple. The digital signal is what is carried inside the carrier system. DS0 is the base for the digital signal X series. DS1, used as the signal in the T-1 carrier, is 24. DS0 (64 Kbps) signals transmitted using pulse-code modulation (pulse code modulation) and time-division multiplexing (Time-Division Multiplexing). DS-2 is four DS1 signals multiplexed together to produce a rate of 6.312 Mbps. DS-3, the signal in the T-3 carrier, carries a multiple of 28 DS1 signals or 672 DS0s or 44.736 Mbps. Digital signal X is based on the American National Standards Institute T1.107 guidelines. The ITU-TS guidelines differ somewhat. The following table summarizes the set of signals and relates them to the T-carrier and E-carrier systems.

DS3: DS-3, the signal in the T-3 carrier, carries a multiple of 28 DS1 signals or 672 DS0s or 44.736 Mbps.

DSP (Digital Signal Processor). Programmable device used to implement any of several signal analysis and/or conversion operations such as coding/decoding, tone detection, and echo cancellation.

DSS. Direct Station Selector, a telephone adjunct that provides additional buttons and indicators to give an attendant direct access to additional line appearances. In the S8300 Media Server, it usually identifies specifically a fifty-button adjunct that enhances the call-handling capabilities of a 4624 telephone used as an operator console.

DSU. See Composed above.

DTMF. Dual-Tone Multi-Frequency, the “touch-tones” used for in-band telephone signaling.

Duplication. The use of redundant components to improve availability. When a duplicated subsystem fails, its backup (redundant) subsystem automatically takes over.

E1. E1 (or E-1) is a European digital transmission format devised by the ITU-TS and given the name by the Conference of European Postal and Telecommunication Administration (CEPT). It's the equivalent of the North American T-carrier system format. E2 through E5 are carriers in increasing multiples of the E1 format. The E1 signal format carries data at a rate of 2.048 million bits per second and can carry 32 channels of 64 Kbps each. E1 carries at a somewhat higher data rate than T-1 (which carries 1.544 million bits per second) because, unlike T-1, it does not do bit-robbing and all eight bits per channel are used to code the signal. E1 and T-1 can be interconnected for international use.

E2. E-2 is a line that carries four multiplexed E1 signals with a data rate of 8.448 million bits per second.

E3. E3 (or E-3) carries 16 E1 signals with a data rate of 34.368 million bits per second.

E/IDE. Enhanced/Integrated Drive Electronics. Standard interface specification for hard disk drives associated with PC computer equipment. This standard interface is sometimes also called ATA-2 and/or Fast ATA. ATA is also used to denote the IDE (not enhanced) interface.

EMI. Electromagnetic Interference; Class A is typically required for business, Class B for residence.

Ephemeral Termination. In H.248 signaling, an "ephermeral" termination is used for an IP connection. For example, a connection between an analog phone on an Avaya™ g700 Media Gateway and an IP telephone would be described by an H.248 context with two terminations: a physical termination for the analog phone (which corresponds to a physical port within the G700) and an ephemeral termination for the IP telephone. The ephemeral termination includes additional information describing the IP side of the call, i.e. the codec chosen, the near end and far end IP addresses and ports, silence suppression information, frame rate (samples per IP packet), etc.

EPN. Expansion Port Network is an optional configuration of cabinets that provides increased switch capacity. It is controlled by a switch processing element that is connected to the time-division multiplexed (TDM) bus and the LAN bus of the server port network. Control is achieved by indirect connection of the EPN to the PPN via a port network link (PNL).

Ethernet L2 Switch. In the Avaya™ G700 Media Gateway and in the Avaya™ stackable switch/router family, this consists of one or more 8 port, wire-speed ASIC devices called Timpani.

Ethernet Switch. A device that provides for port multiplication by having more than one network segment.

Expansion Interface. A special slot available in the Avaya™ G700 Media Gateway and in the Avaya™ stackable line that hosts a 16 port 10/100 interface, ATM or a variety of gigabit ethernet interfaces. Note: Definity® supports a circuit pack with the same name, used for connectivity between a port network and a center stage switch. These two Expansion Interfaces are completely unrelated.

External Media Server (EMS). An external server running the Avaya MultiVantage™ application, i.e. Avaya™ S8700 Media Server, controlling Avaya™ G700 Media Gateways.

FTP. File Transfer Protocol – an Internet Protocol Standard for copying files from one computer to another.

GateKeeper (GK). GateKeeper is a term specifically defined by the H.323 standard which describes the entity performing most of the authorization, routing, and feature functionality in an H.323 system. S8300's Communication Controller (CC), being Avaya MultiVantage™ based, serves as H.323 GK for IP telephones, softphones, and trunks. The term is similar in meaning, but not quite the same as, H.248's term MGC. Our CC is both an MGC and a GK. See the standards documents for more details.

Gateway. In networking, a combination of hardware and software that links two different types of networks. The Avaya™ G700 Media Gateway is an entity on the network that links the circuit switched network (analog, DCP phones, E1/T1 trunks, etc) to the packet based network (LAN). The Avaya™ G700 provides service circuits (tones, audio mixers) and conversion resources for traversing legacy telephony and IP network domains with voice-oriented bearer and signaling information.

GQPB. Guaranteed Quality of service Packet Bus - Provides for very small packets at extremely consistent intervals with minimum delay—Highly optimized for voice traffic - Strikingly similar to a TDM Bus.

H.248. The ITU standard for communication between a gateway server and an Avaya™ G700 Media Gateway.

H.323. ITU standard for switched multimedia communication between a LAN-based multimedia endpoint and a gatekeeper.

HTML. Hypertext Markup Language, the syntax used to format pages for the World Wide Web.

HTTP. Hypertext Transfer Protocol, the protocol used to request and transmit pages on the World Wide Web.

HTTPS. Secure Hypertext Transfer Protocol.

IDE. Generic PC standard for interconnection of media devices to the PC motherboard.

IEEE. Institute of Electrical and Electronics Engineers, an organization that, among other things, produces standards applicable to LAN equipment.

Initialization and Administration System (INADS). A software tool used by Avaya Services personnel located at the Technical Service Center (TSC) to initialize, administer, and troubleshoot customer communications systems remotely.

Integrated Services Digital Network (ISDN). A message oriented signaling scheme used for call setup as well as provision for passing supplementary services across network links.

IntServ: A method for an end system to actively signal packet-handling requests into the service provider network.

IP (Internet protocol). The Internet standard protocol that defines the Internet datagram as the unit of information passed across the Internet and provides the basis for the Internet connectionless, best-effort (unreliable) packet delivery service. IP provides the functions of routing and switching the datagram based on the network address contained within the IP header. IP includes ICMP control and error message protocol as an integral part.

IPSec: IPSec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSec will be especially useful for implementing virtual private network and for remote user access through dial-up connection to private networks. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers. IPSec provides Authentication Header (AH), which essentially allows authentication of the sender of data. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

IPSI. IP Server Interface (Definity® TN 2312 Circuit Pack) that provides for Clock generation and synchronization, tone generation and detection, and Port Network AA functionality.

IrDA. Infrared Data Association, an industry association that has produced a set of standard infrared interface specifications.

IT: IT (information technology) is a term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived). It's a convenient term for including both telephony and computer technology in the same word. It is the technology that is driving what has often been called "the information revolution."

L2TP: Layer 2 Tunneling Protocol; IETF standard for Layer 2 tunneling for remote access. (Note: Point-to-Point Tunneling Protocol (PPTP), another RAS tunneling protocol—but not an IETF standard—was an earlier protocol, focused on Microsoft)

LAN. Local Area Network.

Layer 2 Switch. An IP component, which takes packets and streams and statically reroutes them to another port on the layer two switch based on the destination MAC address.

Layer 3 Switch. An IP component, which takes packets and streams and dynamically reroutes them to another port on the layer three switch based on the IP address of the packet or stream. IP Routering is a layer-3 functionality.

Line Gateway. An Avaya™ G700 Media Gateway without any IP phones.

Local Survivable Processor (LSP). A configuration of the S8300 Media Server used to provide redundancy of the Avaya MultiVantage™ application. In the LSP configuration, the server acts as an alternate server/gatekeeper for IP entities such as IP telephones and Avaya™ G700 Media Gateways. These IP entities will use the LSP when they lose connectivity to their primary server.

MAC. Media Access Control. A general reference to the low-level hardware protocols used to access a particular network. The term MAC address is often used as a synonym for physical address.

MGCP. Media Gateway Control Protocol, a protocol designed for use by Gatekeepers to control Gateways. It was written primarily by Cisco, Nortel and Bellcore (now Telcordia Technologies). In the IETF, it was superseded by the Megaco protocol, which was unified with the ITU's H.248 (formerly H.gcp).

MODEM. MOdulator-DEModulator.

NAT: Network address translation. Some firewall devices will perform a NAT function, so that many IP addresses within an Intranet can be used internally without colliding with public IP addresses on the Internet. Only when IP entities require service outside the firewall will a public IP address be allocated by the NAT device. The IP address is translated private to/from public IP by the NAT device.

OC-3: The Synchronous Optical Network (Synchronous Optical Network) includes a set of signal rate multiples for transmitting digital signals on optical fiber. The base rate (OC-1) is 51.84 Mbps. OC-2 runs at twice the base rate, OC-3 at three times the base rate, and so forth. Planned rates include OC-1, OC-3 (155.52 Mbps), OC-12 (622.08 Mbps), and OC-48 (2.488 Gbps). asynchronous transfer mode makes use of some of the Optical Carrier levels.

Octaplane. This is the marketing name for the capability (and related Hardware) to bundle stackable components using a proprietary 8 GB bus into a larger logical switch which is presented as a single network element to system management. Wired in a ring configuration, providing redundancy and re-routing should one of the boxes need to be replaced or added in a hot system.

PCI. Peripheral Component Interconnect. A local bus technology that allows SCSI host adapters, video cards, and other peripherals to send data directly to and receive data directly from the CPU.

PPN. Processor Port Network is a Definity® configuration of cabinets that houses the control complex (SPE) of the system and port interfaces.

Primary Rate Interface (PRI). Defined as having a bandwidth of 1.544 Mbps which is divided into twentyfour 64 Kbps channels plus an 8 Kbps framing channel.

Prowler. Internal name for the TN2302AP IP Media Processor Definity® circuit pack that replaced the TN802B IP Interface as of Definity® R8.3. It's also the starting point for the design of our Avaya™ G700 VoIP engine

PSA (Personal Station Access). Definity® feature. Personal Station Access makes it possible for selected users to change the current station (with its features and capabilities), associated with a particular compatible switch port, to another compatible station with different features and capabilities.

PSTN. Public Switched Telephone Network.

Pulse Code Modulation (PCM). A process in which a signal is sampled, and the magnitude of each sample with respect to a fixed reference is quantized and converted by coding to a digital signal.

QoS: On the Internet and in other networks, Quality of Service (QoS) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Transmitting this kind of content dependably is difficult in public networks using ordinary "best effort" protocols.

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by Ascend and other network product companies and is a proposed IETF standard.

RJ45. Registered Jack 45 is a single-line jack for digital transmission over 4-pair ordinary phone wire.

RMON (Remote Monitoring). is a standard monitoring specification for shared Ethernet and Tokenring media defined in RFC 1757. RMON enables various network monitors and console systems to exchange network-monitoring data. The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information. RMON has two levels:

- RMON-I analyzes the MAC layer
- RMON-II analyzes the upper layers (layer 3 and above)

Router. A device that supports LAN-to-LAN communications. Routers may be equipped to provide frame relay support to the LAN devices they serve. A frame-relay-capable router encapsulates LAN frames in frame relay frames and feeds those frame relay frames to a frame relay switch for transmission across the network. A frame-relay-capable router also receives frame relay frames from the network, strips the frame relay frame off each frame to product the original LAN frame, and passes the LAN frame on to the end device. Routers connect multiple LAN segments to each other or to a WAN. Routers route traffic on the Level 3 LAN protocol (e.g., the Internet Protocol address). See also Composed.

RTCP. Real Time Control Protocol, contained in IETF RFC 1889.

RTOS. Real Time Operating System.

RTP. Real Time Protocol, IETF RFC 1889

RYON. Roll Your Own NT. The TN795 circuit pack used by DEFINITY ONE.

SAT. System Access Terminal. The craftsperson interface into the system for administrative and maintenance functions.

SLA: A Service Level Agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish. Many Internet service providers (Internet service provider) provide their customers with an SLA. More recently, IS departments in major enterprises have adopted the idea of writing a Service Level Agreement so that services for their customers (users in other departments within the enterprise) can be measured, justified, and perhaps compared with those of outsourcing network providers. Some metrics that SLAs may specify include:

- What percentage of the time services will be available
- The number of users that can be served simultaneously
- Specific performance benchmark to which actual performance will be periodically compared
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems
- Dial-in access availability
- Usage statistics that will be provided

SMON (Switched Monitoring). Technology which is an extension of RMON Standard. SMON adds to the RMON capabilities in following ways.

"Device SMON" is an extension of RMON-I that provides additional tools and features for monitoring in a "local" switch environment.

"AnyLayer SMON" extends RMON-II that provides a "global" view of traffic flow in a network with multiple switches.

SMON collects and displays data in Real time. SMON is capable of providing:

- A global view of traffic for all switches on the network
- An over all view of traffic passing through a specific switch
- Detailed data about the hosts transmitting packets through a switch
- An analysis of traffic passing through each port connected through a switch
- A view of traffic between various hosts connected to a switch

SMT. System Management Terminal. An administration device for System 85 which is similar to the MAAP. The SMT provides limited administration capability to the customer.

SNMP: Simple Network Management Protocol (SNMP, IETF STD 15 (RFC 1157) and RFCs 1441, 1905 and 1906) is the industry standard protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SPE. Switch Processing Element. A collective term which embraces all "control" circuit packs in the server of a traditional Definity® switch.

Survivable CC. Another name for a Local Survivable Processor.

System Access Terminal (SAT). is the primary interface into the Definity® system for administrative and maintenance functions. It is also a primary interface into the Avaya™ S8300 Media Server system.

T1: The T1 (or T-1) carrier is the most commonly used digital line in the United States, Canada, and Japan. In these countries, it carries 24 pulse code modulation (pulse code modulation) signals using Time-Division Multiplexing at an overall rate of 1.544 megabit per second.

T3: 44.736 Mbps

TCP. Transmission Control Protocol, a connection-oriented transport-layer protocol, IETF STD 7: RFC 793. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TDM (Time division multiplexing). A switching technique of splitting a large bandwidth into many small channels in the time domain, called timeslots.

TFTP. Trivial File Transfer Protocol – an Internet Protocol Standard. See IETF STD 33: RFCs 1350, 2347, 2348, 2349.

TOS. Type Of Service, one of the fields in an IP packet header, also used by DiffServ.

Tunneling: Relative to the Internet, tunneling is using the Internet as part of a private secure network. The "tunnel" is the particular path that a given company message or file might travel through the Internet.

UDP. User Datagram Protocol, a connectionless transport-layer protocol, IETF STD 6: RFC 768.

URL. Uniform Resource Locator. Specifies the location of Web pages, files, and scripts for a variety of administrative purposes.

USB. Universal Serial Bus, a higher-speed (than EIA-232D) serial interface designed primarily for adding peripherals to personal computers. e.g., printers, modems, keyboard, and mouse

V.35: The trunk interface between a network access device and a packet network at data rates greater than 19.2 Kbps. V.35 may use the bandwidths of several telephone circuits as a group.

VLAN. Virtual LAN, a term used for networks whose traffic can be segregated independent of physical LAN connectivity. 802.1Q framing can support VLAN operation.

VoIP Monitoring Manager. VoIP Monitoring Manager adds to the RMON/SMON capabilities for VoIP call level monitoring. VoIP Monitoring Manager is capable of displaying both Real time data as well as historical data.

VoIP: (voice over IP - that is, voice delivered using the Internet Protocol) is a term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this means sending voice information in digital form in discrete packet rather than in the traditional circuit-committed protocols of the public switched telephone network (public switched telephone network). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

VPN: A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both extranet and wide-area intranet. Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Microsoft, 3Com, and several other companies have developed the Point-to-Point Tunneling Protocol (PPTP), and Microsoft has extended Windows NT to support it. VPN software is typically installed as part of a company's firewall server.

WAN. Wide Area Network.

WSP (WAN Spare Processor). A redundancy configuration supported by Definity®, which provides service to elements in a Definity® network across an ATM infrastructure. WSPs may be placed in various places in the customer's network to provide reliable service in cases where the ATM network fails.