Avaya Communication Manager Software Based Platforms

High Availability Solutions

Avaya Media Servers and Gateways

Cheryl L. Barnes,
Bahareh Momken,
Luke Young
Members of Technical Staff, Avaya Labs

July, 2007

High Availability Solutions

Avaya Media Servers and Media Gateways *With* Avaya Communication Manager Software

Executive Summary

Companies are staking their success on reliable communications systems. With the convergence of voice and data applications running on common systems, the stakes grow higher. A communications failure could bring an entire business to a halt, with disastrous consequences. Executives and communication managers who understand what it takes to assure "high availability" will be well positioned to choose vendors who can deliver systems the enterprise can count on.

Availability is a measure of "uptime," the percentage of time that a system is performing its useful function. In voice systems, availability calculations are based on the presence of traditional "dial-tone," plus the ability of the user to make and receive calls in a desired manner. This is also true for associated applications like contact centers. .

Traditionally, "real-time" applications such as voice communication, have demanded higher availability than applications based on "store and forward" technology. As a result of this demand, the availability of soundly designed voice systems has an historic track record of 99.95% - 99.9999%. This equates to a down-time range of about 4 hours per year on the low end of the range of availability, to 32 seconds per year on the high end. In fact, this historical track record is the source of the oft-mentioned benchmark of reliability: "five nines".

The measure of success for traditional "store and forward" applications wasn't as dependent on continued availability. As long as information got to its intended destination by the time it was needed, success was achieved. It didn't matter whether the process required re-transmission of packets, or if packets experienced a temporary delay because of bandwidth optimization or other reasons. As a result of this historic difference in measure of success, systems designed for store and forward applications have not had (nor did they necessarily need) a track record of 99.999% availability. In more recent years, as customer expectations have grown, and as cost of providing bandwidth has dropped, vendors of these systems have developed ways of improving availability. Examples include server "clustering" and providing the option of redundancy for potentially critical sub-assemblies, such as power supplies, tape drives, and processing elements.

Converged infrastructures must adequately support both types of applications into the future. Real-time needs still exist and must be supported well, side by side with the store and forward applications carried over packet-based transport systems of the past.

In the Avaya Media Server and Gateway product line, Avaya has developed solutions with the strategic historical strengths of:

- applications designed to run at five nines,
  - supported by underlying service infrastructures that operate at five nines or better ,
    - which run on a variety of transport architectures
      - like circuit switching designed to operate at over six nines,
      - or packet (cell) architectures like ATM, which can run at four or five nines.

Over the decade, Avaya has introduced robust support of Internet protocol (IP)-based transport. Because the building-block architecture is cleanly implemented in the three layers just listed, flexibility in transport (including mix and match) is supported. This results in no compromise to the wide array of applications Avaya provides at the top layer. Applications like contact centers and multi-national networking work smoothly, with the same look and feel, regardless

of the underlying transport systems. As a result, enterprises can evolve toward converged infrastructures at the rate that makes sense for their business.

Avaya employs a variety of techniques to achieve this high reliability at each level. Years of applied dedication in hardware and software design have made each building block solid. Pervading all aspects is continual architectural diligence toward a consistent, logical system structure that allows an easy evolution into the future, appropriately re-using proven foundations from the past. Also pervasive is a maintenance sub-architecture which delivers built-in "intelligence" and "self-healing" abilities for systems at all levels. The software controlling Avaya Media Server systems -- Avaya Communication Manager (Avaya CM) software -- plays a central role in achieving high availability. More than 30 percent of the lines of code in this software is devoted to the maintenance subsystem. Avaya CM Software is designed to automatically and continually assess performance, detecting and correcting errors as they occur. The software incorporates component and sub-assembly self-tests, error detection/correction, system-recovery, and alarm-escalation paths. Its maintenance subsystem manages hardware operation, software processes and data relationships.

Employing the IP packet-based transport architecture allows additional reliability advantages. One example is the load-sharing and fail-over ability of the principal IP resources found in Avaya's Media Gateways:

- C-LAN (Control LAN) Circuit Module (provides TCP/IP stack processing and socket management)
- Media Processor Module and the IP Media Resources 320 (provides conversion between VoIP and TDM, where necessary, as in IP calls accessing the public-switched telephone network)
- VAL (Voice Announcements over LAN; allows recorded announcements to be stored and distributed anywhere on the LAN/WAN)

The IP architecture also allows phones to have a recovery mechanism of their own, so they can connect to alternate controllers (re-home) if the link to their primary system is broken.

For large systems, Avaya S87xx Media Servers running Avaya CM software provide server redundancy, with call- and feature- preserving fail-over, on the strength of a Linux operating system. The Avaya S8300 Media Server can further enhance redundancy by serving as local survivable processors (LSPs) within networks. LSPs can take over population segments that have been disconnected from their primary call server and provide those segments with Avaya CM Software operation until the outage resolves. Enterprise Survivable Server (ESS) can run on S87xx or S8500, and provides full CM featured back-up of the entire Enterprise if desired. Finally, the recent addition of the S8400 leverages the strength of the proven Linux operation system for small systems.

With converged infrastructures, the likelihood of mixed vendor environments is high. In addition, a converged infrastructure can involve a more distributed system. The degree of distribution will vary by situation, and will affect the overall reliability of the system. Communication Managers will need to assess their overall system reliability by understanding the nature of each building block, and how the building blocks work together. For example, a system that requires four-nines performance overall may well require individual building blocks that are close or equal to five nines (due to the combinatorial effect), and/or connections that provide alternate communication paths. Tables included in this document specify the reliability performance of Avaya Media Server and Media Gateway building blocks.

In sum, the architecture of Avaya Media Servers and Gateways makes use of many elements on each level to help assure high overall system availability, and to meet the needs of the most demanding enterprise manager.

Introduction

The purpose of this paper is to provide the reader with medium-depth insight on the subject of communication-system "availability," specifically that of Avaya Media Servers and Gateways. The discussion that follows demonstrates Avaya's long-standing diligence in hardware and software design for high performance and reliability, and demonstrates the overall architectural strength, consistency and foresight inherent in Avaya CM related products.

A brief description of "availability" and its significance to communications systems is provided, as is specific data for Avaya Media Servers and Gateways, plus historical field-performance summary data. Hardware-design considerations, software-design considerations and overall maintenance strategy are described as well.

Avaya CM software and Avaya Media Servers are designed to deliver extremely high levels of availability. Hardware and software components are constructed to minimize the impact of component, function, or data failure. The maintenance architecture incorporates a multi-faceted ability to diagnose and remedy potential causes of failure, and to enable rapid service restoration when a problem occurs.

High Availability – A Definition

The reliability of maintained systems is often expressed in terms of ***availability***. Availability is defined [1] as the percentage of time that the system is available to most of the users. The basic formula for calculating ***availability*** is:

A = MTBO/(MTBO + MTTR), where

- Mean Time Between Outage, MTBO, measures length of time between outages.
- Mean Time To Recovery, MTTR, measures the time to recover.

Table 1 shows the range of ***availability*** that is typically expected of communications systems.

Total System Availability [2]	Downtime per Year	Who Might Need This
99.99 "four nines"	53 minutes	Generally accepted as the minimum standard of acceptable down-time for business.
99.995 +	15-20 minutes	Businesses or organizations that potentially have a lot at stake on any given phone call.
99.999+ "five nines+"	5 minutes or less	Hospitals, Emergency Services, High-Performance Call Centers, Critical Government Agencies, Financial Institutions, etc.

Table 1

High Availability – General Design Considerations

When designing communications hardware and software, high availability must be incorporated from the beginning as a primary performance requirement. High availability requires dedicated design diligence at multiple layers and with several overarching objectives.

[1] For telecommunications equipment, industry-recognized specifications as documented in various IEEE publications, Bellcore / Telcordia GR 512, and MIL-HDBK-217C are most commonly used for reliability and availability characterizations. See Appendix B for more information on prediction modeling used by Avaya designers.

[2] Total system availability is made up of all hardware and software elements that can effect the intended system operation.. This is more comprehensive than hardware characterization of the processors, only.

High Availability

Design Element	Measurement
1. Failures of each component and sub-system must be infrequent.	Mean Time Between Failures (MTBF)
2. System outages must be infrequent.	Mean Time Between Outage (MTBO)
3. When there is a failure or outage, the impact must be minimized and isolated; recovery must be speedy.	Mean Time to Recovery (MTTR)
4. System collects its own performance statistics.	Various

Table 2

Not only must failures at the device or sub-assembly level be minimized, but when a failure occurs, the design itself must help alleviate the impact of the failure. For example, the design must test itself frequently, to root out problems before they become customer-affecting. The design must isolate sub-assemblies that are not functioning properly, and test them for verification. If a fault is identified, the circuit should be taken out of service, if necessary, with an alarm sent automatically to have a technician dispatched. As appropriate, the design must incorporate redundancy at the device or sub-assembly level to add reliability where it's most needed.

As an example of the extent to which maintenance architecture is intrinsic to the system design, consider that more than 30 percent of the lines of code in Avaya CM software is dedicated to system maintenance. In addition, a similar ratio of maintenance code is included in Avaya firmware that runs the circuit modules, interoperating with higher-level Avaya CM software maintenance.

DESIGN Considerations

Hardware Considerations

Tables 3 and 4 demonstrate that circuit modules and sub-assemblies used in Avaya's CM related hardware platforms are extraordinarily reliable relative to the information-technology industry in general. This is not by accident. Avaya's heritage of achieving critical or "five nines+" availability results from holistic ownership of design, manufacture and lifetime support (stemming from an initial vision that's now been refined by tens of billions of hours of user experience). Avaya's living principles that enable this include:

- Highly effective knowledge and execution of "Design for Manufacture, Installation, Reliability and Serviceability":
  - End-to-end quality control executed thoroughly from electrical-device vendor partnerships through every stage of the assembly process. The highest quality is pushed to the earliest step of the process possible. Based on Deming's "zero defects and zero errors," this actually reduces overall costs substantially.[3]
  - Commonality that is leveraged at all levels:
    - *Piece -parts*. Many of the "workhorses" of the product are in their 5th to7th generation of silicon integration. This keeps Avaya on the leading edge of technology curves.
    - *Sub-assemblies*, like circuit modules. Commonality here helps customers in a myriad of ways, not the least of which is investment protection. Like the piece parts, the sub-assemblies are also in their 5th – 7th level of renewal and refinement.

[3] Gary Hamel, in his Leading the Revolution, speaks of the importance of "getting different" rather than "getting better." The "zero defects and zero errors" passion fostered by the Quality giant, Dr. Deming, in the 1980's was revolutionary. The prevailing notions of the times were that quality just needed to be "good enough" (obviously subjective) and that to increase quality beyond "good enough" would be cost prohibitive, with diminishing returns. The principle those notions missed is that if "causes" of quality problems are addressed, rather than "effects," then overall costs actually go down.

- *Shared designs*. Even where sub-assemblies can't be directly re-used, common designs that have been optimized for reliability over the years are reapplied in new configurations.
- *Common software*. Avaya CM software is the robust, feature-rich, field-proven software for high-reliability enterprise systems, common across Avaya's converged and traditional solutions.

➢ Server Platforms:

- *Qualification*. Server specification, selection and testing is rigorous. Requirements for RAMDISK , ECC (Error-Correcting Code), and N+1 fans as well as high reliable power supplies, as examples, are leveraged to assure high availability of the system.
    - *ECC Memory* allows single bit and double bit errors to be managed by Avaya Communication Manager software. Single bit errors are detected and corrected. Double bit errors are detected, monitored and reported. The due diligence of the surround application working with the ECC enabled platform results in robust performance of memory.
    - *RAMDISK, or memory locking*, provides protection from disk failures. It locks application and critical components in memory. Typically, any device with moving parts will degrade overall reliability. Design must accommodate failures of moving parts, while maintaining service to end-users in parallel with dispatching services. RAMDISK allows a simplex platform, like the S8500 to, to continue to provide call processing in the event of disk failure, simultaneously with alarming to services for repair/replacement. It is essential for simplex platforms to support coverage for moving parts to assure 4 9's availability.
    - *N+1 Fan Redundancy* assures that the server is operational when one fan fails. Simultaneously, the Communication Manager software alerts services so that a fan replacement can be scheduled. As with the hard drive, this coverage is essential for assuring 4 9's availability.
- *HAP (High Availability Platform).* The HAP part of Avaya CM software incorporates watchdog type monitoring of health and sanity of the applications, and the base OS, as well as critical environmental conditions. Degradation of service results in simultaneous recovery strategies as well as alarming to services if necessary. The HAP requires hardware, such as the SAMP (*Server Available Management Processor) PCI card used in the S8500 platform.* This coverage is essential to assure 4 9's availability in a simplex system.
- *Details on specific platforms are provided in later section.*

Industry Data	
Component	**Mean Time To Failure**
Logic Boards *	3 – 20 years
Disks *	1 – 50 years
ISP Server Class Power Supply***	20 – 25 years
Power (North America) *	5.2 months
LAN *	3 weeks

Avaya Platform Elements	
Component	**Mean Time To Failure**
Media Processor board **	35 years
Protocol Preprocessor board (C-LAN) **	50 years
Digital Line/Trunk boards **	72 – 77 years
Avaya Media Server Complexes	10-90+ years
Avaya (Gateway) Power Supplies **	25 – 60 years
(Industry) Power (North America) *	5.2 months
(Industry) LAN *	3 weeks

* Taken from "Microsoft High Availability Operations Guide" (see footnote [4])
** Based on numerous internal Avaya studies assessing the results of millions of user-hours [5]
*** Based on internal survey of reputable vendors
(All numbers assume 24 hours per day, 7 days per week usage.)

Tables 3, 4

As can be seen in the numbers in tables 3 & 4, the mean time between failure (MTBF) of each and every Avaya sub-assembly is World Class.

Software and Maintenance Architecture

The maintenance architecture of Avaya CM software is designed to detect and correct errors as they occur. This minimizes the number of events that cause system outages. It also quickly isolates the fault to a replaceable sub-assembly. This automatic assessment is done constantly, in the background of normal operation, so errors can be addressed early and proactively. Component self-testing, sub-assembly self-testing, error detection/correction, system recovery and alarm-escalation paths are all elements of this architecture. The system software has been designed to recover from intermittent failures and to continue providing service with a minimum of disruption. Firmware that runs each circuit module does similar tasks, working cooperatively with the system software.

The maintenance subsystem manages three categories of maintenance objects. ***Hardware maintenance objects*** are tested and, where appropriate, alarmed and removed from service by the software. The error is reported to an operations center so the object can be replaced. The second category is ***software processes***; if a process encounters trouble, it is recovered or restarted. The third category is ***data relationships***; data relationships are audited and corrected.

[4] *Microsoft® Windows NT® Product Group High Availability Operations Guide*, Microsoft Consulting Services Manufacturing and Engineering Practice; © 1999, Microsoft Corporation.

[5] Availability modeling: Bell Labs "Reliability Information Notebook" (encyclopedia-like reference of multitudes of studies of pieceparts, sub-assemblies, environmental considerations, thermal modeling and testing, system modeling, etc.), 1980 – 1990; Joyce, 1987,1988,1991, 1995; Smith, 1987; Sueper, 1991; Mooney, 1992; Lincoln, 1999; Brown, 1993; Walters, 1998; Sueper, 1998; Vicker, 1999; Walters, 1998, 1999; Barnes 2000; Momken, 2001, 2002; Numerous extracts of field data from "Expert Systems" from 1992 – present; Factory studies of failure rates and field return data: each month of each year from 1987 – 2002.

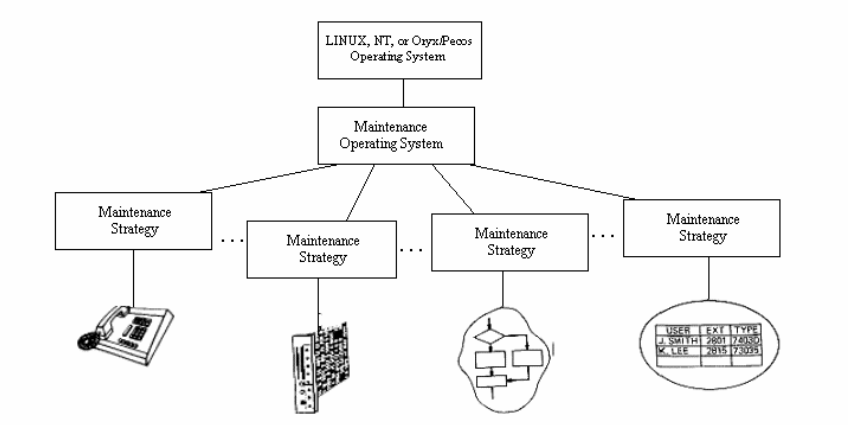


Figure 1

Avaya CM software provides its systems with remote diagnostics capability, which enables rapid troubleshooting and -- in instances when the system cannot heal itself -- maintenance. Studies have shown that most problems experienced by Avaya call-processing systems are self-corrected without impact to the customer. This sophisticated maintenance management capability makes possible the 99.99 – 99.999+ percent availability performance of Avaya CM based systems.

Software Failure Recovery

One key to rapid self-healing of software failures is the judicious use of the appropriate level of recovery. With too little action when stronger measures should be taken, the attempted recovery wastes time and does not solve the problem. Conversely, with too much action, the recovery is unnecessarily prolonged. Figure 2 shows the spectrum of recovery levels used by Avaya CM software.

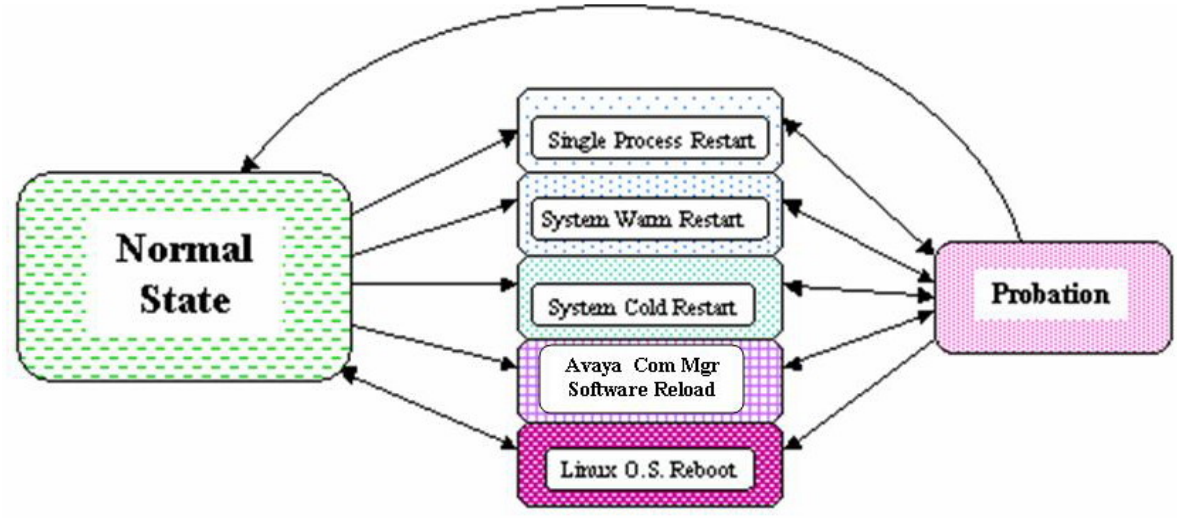


Figure 2
Software Recovery Levels

The automatic recovery levels are as follows (from mildest to strongest, which also happen to be quickest to slowest, and more frequent to less frequent):

Single Process Restarts –

Process sanity audits are performed routinely (every ten seconds or so) on many dozens of key software processes. In the event of a hung process, that single process will be restarted (no call outage will result). If a higher-level restart or three single-process restarts are needed within a sixty-second probationary period, the third single-process restart will be deemed ineffective and will instead be escalated to a system **warm restart**.

System Warm Restarts –

This mechanism preserves all stable and held calls, as well as feature-activity data, throughout the brief recovery period. Processes are restarted, while maintaining call processing related data. If three warm restarts are needed within a fifteen-minute probationary period, the system warm restart will be deemed ineffective and will instead be escalated to a system **cold restart**.

System Cold Restarts –

In this recovery mechanism, processes are restarted, with some data intact, but **calls are dropped** and ports are reset, followed by a "port board activation" phase of recovery. If three cold restarts are needed within a fifteen-minute probationary period, the third system cold restart will be deemed ineffective and will instead be escalated to a software **reload**.

Avaya CM Software Reloads –

In this recovery mechanism, all **calls are dropped**, and all processes related to call processing are killed and restarted. Port-configuration data known as "translations" is re-read from disk, and (as in system cold restarts) ports are reset and port boards are activated. If three software reloads are needed within a ten-minute probationary period, the reload will be deemed ineffective and will instead be escalated to an operating system **reboot**.

Linux Operating System Reboots (applicable to S8300, S8400, S8500 and S87xx Media Servers) –

In this recovery mechanism, all **calls are dropped**, all processes are killed, and the operating system is completely rebooted. Processes are then read off disk and loaded into memory, where recovery then proceeds exactly as it does in Software reloads. If the reboot fails after a recent software upgrade, another reboot will be attempted, but from a disk partition containing the previous version of software.

In the S87xx duplicated servers, the ***server interchange*** adds graceful fault tolerance during any of the events above or in case of impending hardware failure. See the S87xx section below for more information.

Avaya S8400, S8500 and S87xx Media Servers

While all businesses require solid performance from their communications systems, some businesses may require increased levels of availability for some or all of their distributed system. To meet that need, the Avaya Media Servers and their associated Media Gateways accommodate a range of availabilities. Table 5 shows the configurations that support the range of availability. For more information, see the case studies in Appendix C.

Avaya CM System Availability [6,7]	Downtime per Year	Category	Configuration
99.99	< 53 minutes	Basic level of service.	Single Call Control Processor; Non-redundant CLAN, MedPro
99.995	< 15-20 minutes	Enhanced level of service	Single Call Control Processor; Survivable Processor back-up; N+X CLAN, MedPro
99.999+	< 5 minutes	Highest level: Hospitals, Emergency Services, High Performance Call Centers, Critical Government Agencies, Financial Institutions, etc.	Duplicated Call Control, Duplicated signaling and bearer between Port Networks

Table 5

In fiber connected configurations, the whole system was a closed system. Availability was characterized at a system level. Traditional terms, "standard", "high", and "critical" were used to categorize the levels of availability. Figures 3, 4 and 5 depict these three traditional levels. Note that Center Stage and ATM is not supported in new shipments as of Avaya Communication Manager 3.0. Nevertheless, existing installations are significant and continue to be supported.

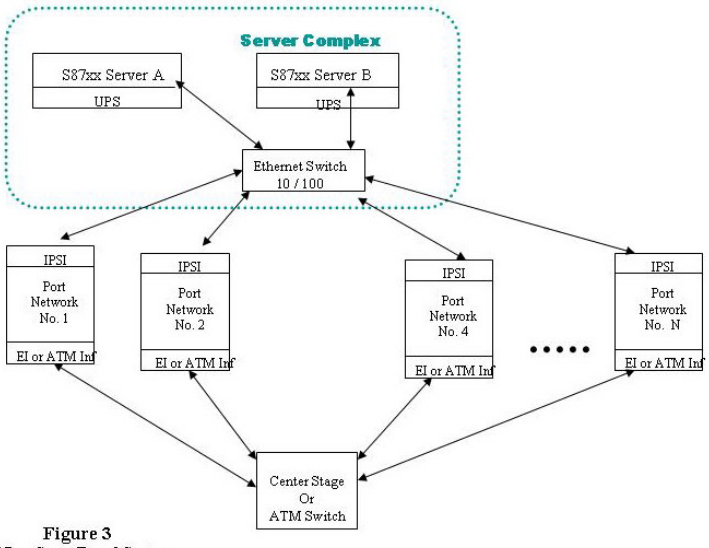


Figure 3
S87xx Sever Based System
"Duplex" or Standard Reliability

[6] This availability prediction does not include availability of the customer's data networks, PSTN contributions, or contributions due to power outages (all of which can vary depending upon implementation). Note that with "open systems," the customer must model their systems end-to-end to ensure availability that meets their objectives. In all systems depicted in this paper, the minimum numbers of data switches have been included in the analysis. Actual systems are likely to have more data switches. A conservative MTTR of 4 hours is assumed (includes travel time) but availability can be improved with reduced MTTR, if customer has on-site technician and sparing strategies. See appendix for reduced MTTR calculations.

[7] The number shown for system availability is based on server complex, as well as local and remote gateways. See appendices for breakdown of contributions.

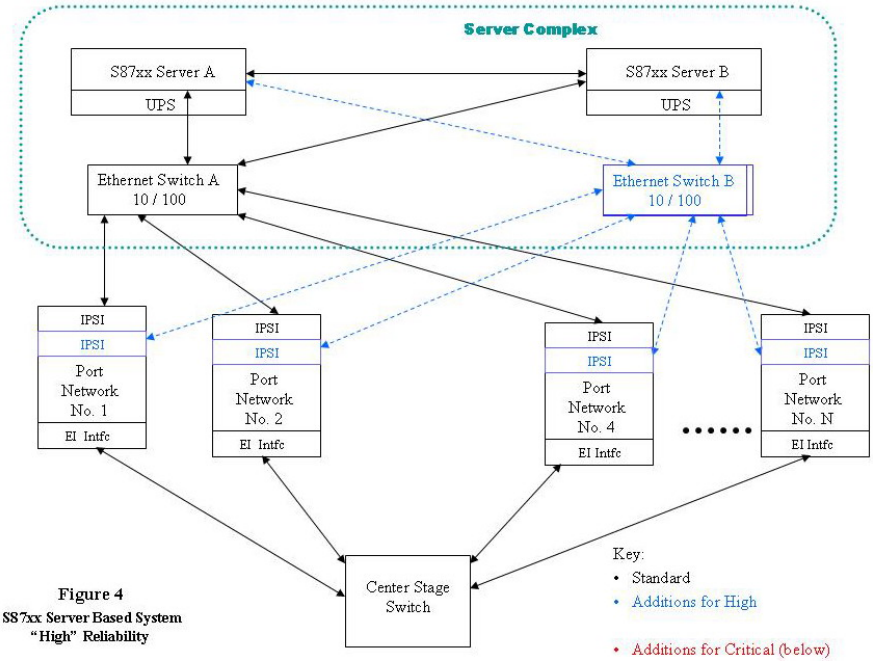


Figure 4
S87xx Server Based System
"High" Reliability

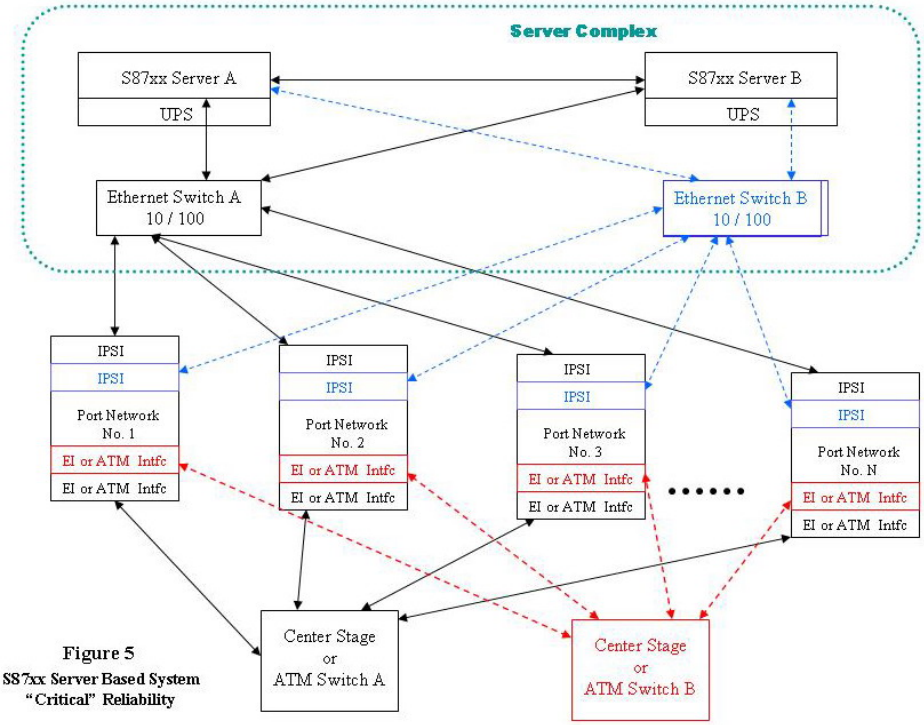


Figure 5
S87xx Server Based System
"Critical" Reliability

The Avaya S8xxx series server and associated architecture increasingly employ the data network. As of CM3.1 duplicated bearer over IP is supported in the IP Media Resource 320. This along with the duplicated signaling over IP (IPSI) result in a robust 5 9's solution (assuming a robustly designed network). The use of the data network means that the system is no longer closed, and the overall availability depends upon the underlying data network, as well as that of the Avaya Media Server and Gateways. Avaya availability and MTBF information is provided in Appendix A.

Figure 6 shows an S87xx system with full duplication of bearer and signaling over the data network.

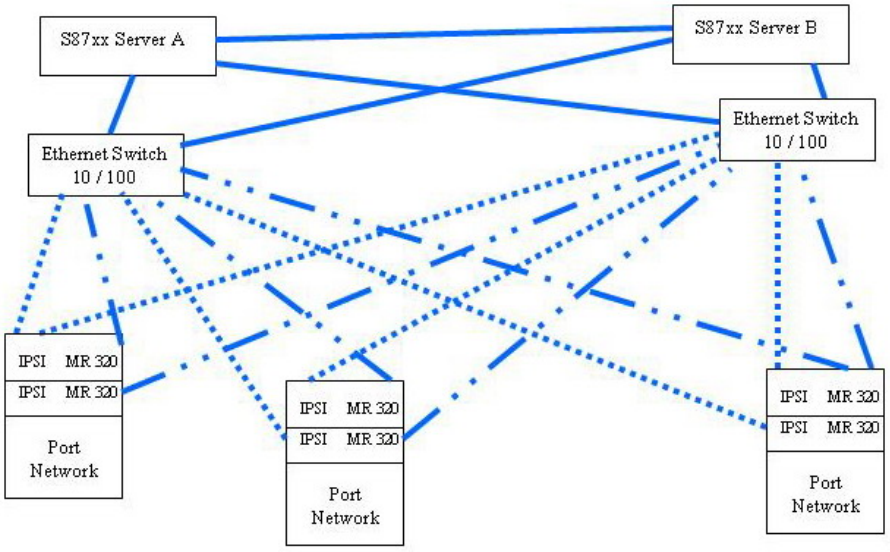
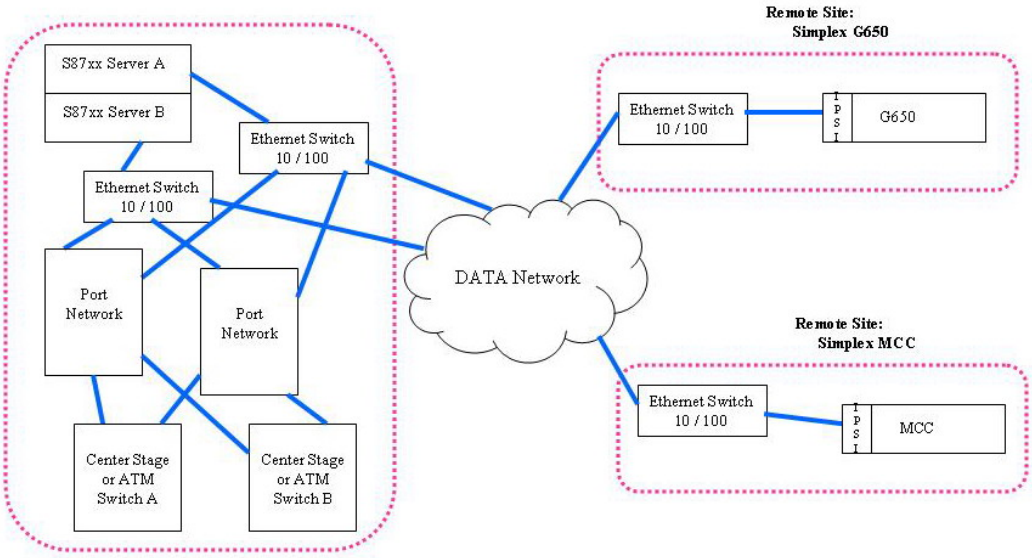


Fig. 6
S87xx Server Based System:
Duplicated Control (IPSI)
Duplicated Bearer (MR 320)

Also, beginning with Avaya Communication Manager 3.0, systems can support a mix of port network types in terms of simplex versus duplex as well as cabinet type. And, systems with traditional Center Stage equipment can be mixed with the newer architecture. This new flexibility affords a high level of investment protection. This also provides flexibility for customers to have higher availability in areas just where they need it.

Figure 7 shows a system that has both Center Stage connected port networks and IP connected port networks. This system also contains a mix of port network cabinet types, and a mix of duplicated and simplex port networks.



Main Site: Traditional
Center Stage System; Fully Duplicated

Figure 7
Mix of Port Network Types

The high-availability philosophy is scrupulously implemented in the Avaya Media Servers. Consider the following:

- Linux was selected as the Operating System (OS) for many reasons, principal of which are:
  - Access to full source code makes it possible to more rapidly fix operating system bugs.
  - Linux facilitates easy system customization to include high-availability enhancements.
  - Linux has fewer known security flaws than other operating systems, and facilitates system customization to provide further security.

- High-availability enhancements:
  - Software sanity is continuously evaluated. Any insanity (due to unexpected conditions) is detected, and, until normal operation is restored, the offending software is forced to go through escalating levels of recovery. Ultimately, with an S87xx system, the entire active software processing can switch over to a standby server.
  - Disks are partitioned to keep most of the variable information away from the invariant and to allow for automatic recovery if newly loaded software fails. In the case of S8400, Solid State Device (SSD) technology is used.
  - All event logs are proactively scanned for potential service-affecting items. If found, alarms are generated. If necessary, a service dispatch is launched.
  - Applications running on the OS are thoroughly pre-tested to assure proper performance; this OS is closed to any applications other than those provided by the manufacturer to avoid interference with operation. Alarms can be generated if any untested software is loaded on the system.
  - Eliminating the need for customers and technicians (in most cases) to access the operating system shell directly provides protection from inadvertent adverse alterations to the system.
  - Tools have been enhanced to allow secure, remote, non-stop debugging of the system as well as unattended data collection.

- S87xx highlights: Two (2) servers with a memory-shadowing link allow:
  - One processor to take over if the other fails, without dropping calls.
  - Simple duplication of all other server components (e.g. modem, disk, memory), eliminating a single point of failure.
  - Connections are preserved during upgrades.
- S8500 / Avaya Media Server running Avaya CM software:
  - Embedded remote maintenance board (SAMP) monitors the health and sanity of the Avaya Communication Manager application, and base OS, in addition to critical environmental conditions. Any degraded service results in prompt alarming to services, even if the server or OS goes down. This monitoring function will also reset the server as recovery escalation directs. The software used in theses processes is referred to as the HAP (High Availability Platform).
  - RAM DISK operation allows call processing to continue for at least 72 hours after hard disk failure. Initial degraded operation of disk generates alarms to services.
  - Redundant fans.
  - Industrial grade power supply.
- S8500 / MultiVantage Express:
  - Call processing leverages the remote maintenance board function, High Availability Platform (HAP), and RAM Disk, as listed above, to support 4 9's performance.
- S8400:
  - Proven Linux platform in a circuit pack with a TN-form factor.

        - Provides very solid upgrade path for Avaya DEFINITY® Server CSI and Avaya S8100 Media Server.
    - Embedded remote maintenance function monitors the health and sanity of the Avaya Communication Manager application, and base OS, in addition to critical environmental conditions. Any degraded service results in prompt alarming to services.
    - Solid State Device (SSD) replaces the conventional hard drive and is used for the Operating System and Communication Manager software. SSD has better availability performance than traditional hard drives because there are no moving parts.
    - Reliability comparable to, or better than, Avaya DEFINITY® Server CSI.
    - Redundant fans.
    - High grade industrial power supply.
    - Optional duplicated power supply in G650 configuration.
    - One port network is supported, and up to 5 H.248 Media Gateways.
    - LSP configuration is supported for back-up of the H.248 Media Gateways.
- All Avaya Media Servers support the following:
    - **Locally Sourced Announcements and Locally Sourced Music On Hold (MoH**) (as of CM 3.1): the same announcements and/or MoH sources can be deployed in different parts of the network. This provides back-up, while assuring the closest possible source.
    - **Automatic restoration of the most recently saved versions of translations**, following a power outage. Translations are automatically shadowed onto the standby server as well of a duplicated server pair. [Note: with Avaya™ G700 Media Gateways, translations can also be copied to Local Survivable Processors for automatic recovery in the case of network partitioning or complete central site failure.]
    - **Scheduled backups of critical system information, locally and/or at remote sites.** In an emergency, multiple copies of translations and server-configuration information are available. Saved information can be quickly restored.
    - **TTS (Time to Service)** (as of CM 4.0): reduces IP endpoint time to service, especially in cases where the system has many IP endpoints re-registering simultaneously.
    - **IP Trunk Link Bounce** (as of CM 4.0), which allows some (administrable) time for the IP network to recover before taking down the trunk. With this feature, calls would still be disrupted during the network outage, but recovery time after the outage would be minimized for network outage of typical duration.

Avaya CM Systems Survivability

Systems operation in the face of network fragmentation requires that call control back-up be distributed in the network. Avaya offers several layers of survivable call processing that can be used separately or in conjunction with each other.

For smaller locations' survivable needs, Local Spare Processor (LSP) is available with the S8300B and as of CM3.1, the S8500:

- Supports H.248 Gateways.
- Each S8300 LSP supports up to 450 users.; each S8500 LSP supports up to 2,400 users.
- (50) LSPs can be supported on single S8300 system; (250) LSPs can be supported on a single S8500 system.
- Connection preserving failover and fail-back are supported.
- Administrable choice of several auto fail-back options.

Also see the Avaya G250 Media Gateway -Standard Local Survivability (SLS) for a new low cost small branch survivable solution in the following section.

For larger locations' survivability needs, Enterprise Survivable Server (ESS) is available with S8500 or S87xx systems:

- Supports 64 Port Networks and 250 H.248 Gateways.
- Each ESS supports up to 36,000 users (of which 12,000 can be IP endpoints).
- 63 ESS servers local and/or (7) enterprise-wide up to CM3.0; 63 ESS servers local and/or enterprise-wide as of CM3.1.
- 250 LSP servers can be supported on a single system.

IF WAN Availability is:	Uptime Pay-Back with ESS / LSP		
	Minutes	Hours	Days
99%	5251	87	3 1/2
99.5%	2623	43	1 3/4
99.9%	521	8.7	
99.99%	48	0.8	

Table 6

Since WAN availability can be a serious bottleneck in overall availability, the options for local call control at remote sites is a vitally important part of the architecture. This table illustrates how much local call control uptime can be regained at remote sites by virtue of LSP or ESS back-up.

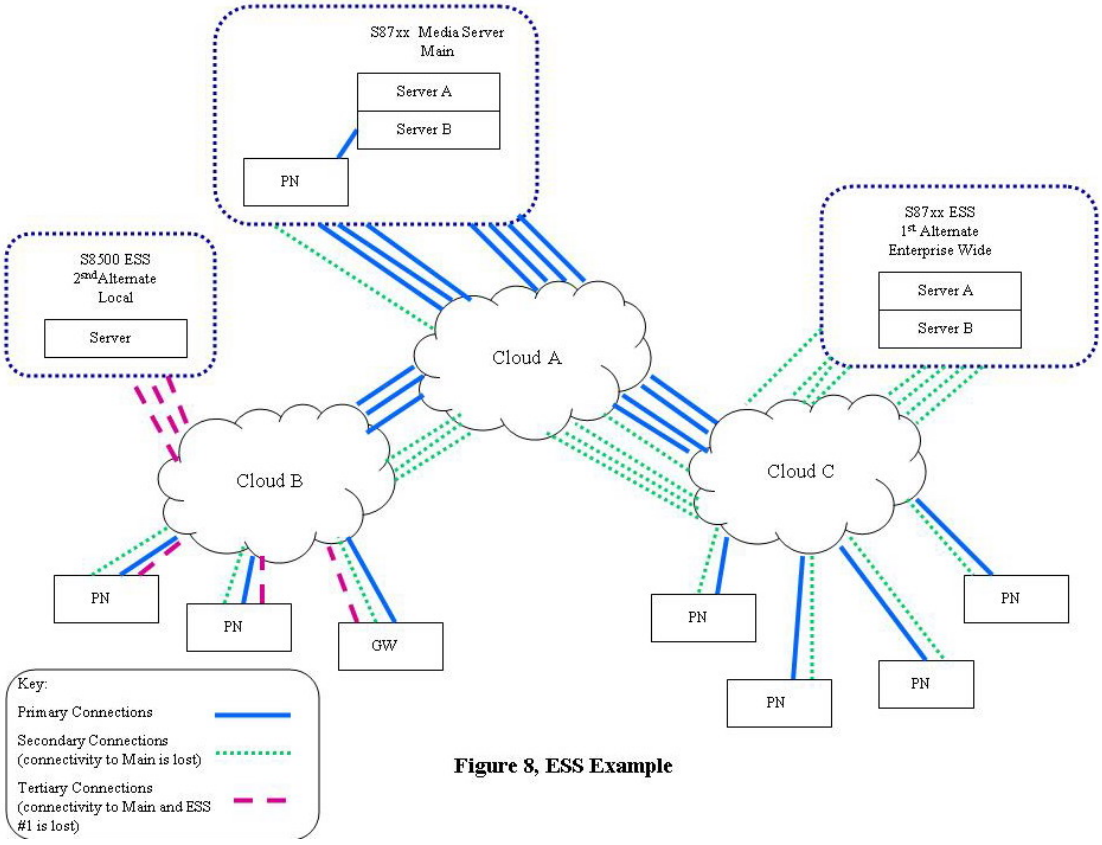


Figure 8, ESS Example

Figure 8 shows an example of a networked configuration that uses an ESS cluster to provide back up call control. Note that the first ESS cluster is set up to support the whole enterprise, should connectivity to the Main call servers be lost. The second ESS server shown here is set up for local support, should connectivity to the Main S87XX and first ESS cluster be lost. Users on "cloud B" have 3 possible connections to call control servers, and will have service even if connections are lost to the Main or first ESS cluster.

IP endpoints can be downloaded with up to 8 alternate gatekeeper addresses upon initial connection with a DHCP, and over 30 addresses upon successful registration with Communication Manager. The endpoints will re-home to other the designated gatekeepers such as CLAN's, LSP or ESS servers if connectivity to the primary is disrupted.

IP Trunk automatic fail-over (and automatic fail-back) to (and from) a traditional PSTN trunk is supported. In this configuration, the customer's system administrator sets service-quality thresholds for delay and/or packet loss. Fail-back thresholds can be set at a level more conservative than the fail-over levels to prevent unstable (thrashing) conditions. If an IP trunk is experiencing impairments that exceed the thresholds, new calls will be routed over the designated PSTN trunk, in lieu, until such time as the service quality has returned to acceptable levels.

Avaya S8300B Media Server and Branch Media Gateways

The S8300 Media Server, like the S87xx Media Server, accommodates several levels of availability performance. The S8300 Media Server is designed to provide a complementary option: Local Survivable Processing (LSP). The LSP architecture provides additional availability and survivability within a network of small-to-medium-sized offices.

Examples of the branch media gateways are: Avaya G700, Avaya G350, Avaya 250 and the Avaya 150.

This table depicts the S8300 and Branch Media Gateway availability possibilities.

System Availability [8],[9]	Downtime per Year	Who Might Need This	Configuration
99.99	53 minutes	Virtually everyone needs at least this level of service at remote sites	Single ICC (internal call controller) equipped Media Gateway per site
99.995+	< 20 minutes	Businesses or organizations that potentially have a lot at stake on any given phone call	N+1 media gateways at each site; each site has duplicate interfaces to the data networks; each IP endpoint homed to at least 2 systems run by Avaya™ CM Software (S8300LSP, or otherwise).[10] For more info see Appendix C.
Table 6			

- S8300 / branch media gateway basics:
  - **Embedded remote maintenance function** monitors the health and sanity of the Avaya Communication Manager application, and base OS, in addition to critical environmental conditions. Any degraded service results in prompt alarming to services, even if the server or OS goes down.
  - **RAM DISK** operation allows call processing to continue for at least 72 hours after hard disk failure. Initial degraded operation of disk generates alarms to services.
  - **Connection Preserving Failover and Failback:** When MG's fail-over or fail-back to any Media Server, stable calls are held up. Failback options can be immediate, or administered.
  - **Redundant fans**.
  - **Industrial grade power supply**.

- S8300 / enhancement options:
  - **LSP** and/or **ESS** for back-up call-control.
    - Up to 50 LSP servers can be supported in an S8300 System
    - The H.248 Media Gateways can be subtended off of an ESS.
    - LSP / ESS servers support the full CM feature set.
  - **Standard Local Survivability (SLS):**
    - Avaya G250 Media Gateway itself contains call very basic control ability.
      - Takes over local call control if the main server connection is lost.
      - Local outbound trunks and internal calls are supported.
      - Incoming trunk calls can be delivered to available stations.
  - **Dial-up Backup feature** provides low cost back-up support of WAN connectivity in the Avaya G250 and G350 Media Gateways.
    - This provides a backup path in case of WAN failure.

---

[8] This availability prediction does not include availability of the customer's data networks, PSTN contributions, or contributions due to power outages (all of which can vary depending upon implementation). A conservative MTTR of 4 hours is assumed (includes nominal travel time); availability can be improved with reduced MTTR, if customer has on-site technician and sparing strategies.

[9] The number shown for system availability is based on server complex, as well as local and remote gateways. See appendices for breakdown of contributions.

[10] Note that Avaya IP phones have multi-homing abilities. They can be configured to re-home to any Avaya™ CM controller. For example, in a configuration with S87xx at a main site and S8300 / G700 at remote site, the phones at the remote site could re-home to main S87xx through separate Ethernet switches. This configuration could be said to therefore provide 4 ½ -9's of availability as well.

- Call control signaling to the main server is re-routed from the WAN to the PSTN.

Availability Considerations in the Data Network

Availability of any VoIP system requires consideration of the data network as well. Data networking has evolved in an environment where 99 percent to 99.9 percent availability was considered acceptable. The quickest way to enhance this availability level is to create redundancy in the central parts of the data networks (the parts that affect many users if they fail). Cisco, for example, strongly recommends that customers who wish to implement VoIP create redundancy from the wiring-closet switches all the way through backbone structures. [11] [12]

Since redundancy of data-network elements is commonly deployed to support VoIP, the LAN interfaces from Avaya Media Server systems must be able to match this redundancy. The C-LAN (Control LAN) Protocol Preprocessor Media Processor, and the IP Media Resource 320 can all be used in N+1, or multiples (to support the same regions of users) in a shared-resource fashion.[13] IP Media Resource 320 are provisioned with 1 or 2 per system. At an MTBF of roughly 50 years each, it is not likely they will fail. In the rare event of a failure, redundant boards assigned to the same region automatically take over support of the users originally using the failed resource. More significantly, assuming redundant LAN segments are connected to each C-LAN, if one LAN segment fails, users are provided back-up service through the redundant LAN segment(s) to the alternate C-LAN(s). Up to eight "alternate gatekeeper" addresses can be downloaded to the IP telephones via either a DHCP server or the Avaya Media Server itself. The back-up boards can be local and/or remote, as long as they are on the same logical system.

For a diagram of possibilities created by this flexibility, see the case study in appendix C.

Historical Data

Constant data collection and analysis is essential not only to corroborate initial expectations, but also to continually engage in improvement cycles. Avaya Media Server systems have a sophisticated self-monitoring and reporting architecture. The information provided by the systems, together with the sophisticated databases developed for Avaya Services support, are collectively known as Avaya's "expert systems."

Avaya databases contain the history of 10's of millions of user hours, via remote reporting and other aspects of the Avaya Media Server maintenance architectures. With this data, corroboration of actual performance relative to anticipated performance can be made. Year after year, the results have verified the anticipation. The expert systems monitor system performance, initiate corrective measures when necessary, and collect data that certifies the validity of system designs and availability claims.

Conclusion

In the Avaya Media Server and Gateway architecture, the transport, services and applications layers are implemented cleanly, allowing transport infrastructure to be independent of the services and applications that run on top of it. This flexibility allows Avaya's rich heritage of features and applications to carry forward on any transport topology that a customer desires to use, including IP. This same architecture also enables easy evolution and incorporation of future enhancements. Finally, a wide array of technologies and techniques that are key to making high reliability and availability possible are robustly implemented on each architectural level, both for Avaya software and the Avaya Media Gateways and Servers powered by it. It is an architecture on which enterprises can build their business with peace of mind.

---

[11] Gene Arantowitz, Cisco Systems; "Building a Converged End to End IP Telephony Network;" VoiceCon 2001.

[12] Note that unless battery holdover is part of the design of each element and/or UPS's are used to support each element, this implementation would still be limited by the MTBF and MTTR of North American Power.

[13] The Voice Announcements over LAN board (VAL) can be used in multiples for back-up, as well.

Appendix A
Definition of Terms and General Formulas

It may be helpful to understand the terms used in technical discussions of operational robustness:

RELIABILITY is a measure that indicates time between failures occurring in a system (observable by users or not).

AVAILABILITY is a measure of the percentage of time a system or component performs its useful function for users.

OUTAGE is a measure of time the system is not performing its useful function. Useful function has to be defined based on the application required. Here, we define it as call control to users.

Reliability measures how infrequently the system fails, at any level. Availability measures the percentage of time the system is in its operational state for the user population (i.e., larger than a single failure group). In the common vernacular, "reliability" is inaccurately used to refer to both of these aspects. For clarity's sake, this discussion adheres to the precise definition. See Figure 1 for the availability range applicable to communications systems.

Availability	Downtime per year in …			
	Seconds	Minutes	Hours	Days
99.9999%	32			
99.9990%	315	5		
99.9900%	3154	53		
99.9000%	31536	526	9	
99.0000%	315360	5256	88	4

Figure 1

To assure high availability:

- Failures of each component and sub-system must be infrequent (Mean Time Between Failures, MTBF, measures length of time between failures).
- System outages must be infrequent (Mean Time Between Outage, MTBO, measures length of time between outages).
- Once there is a failure or outage, recovery must be speedy (Mean Time To Repair (or Recovery), MTTR, measures this speediness).

The actual formula for availability is:

A = MTBO/(MTBO + MTTR).

When projecting the availability of a system composed of subsystems, a model that logically equates the subsystems' availability to the total system availability is created. In turn, the availability of each subsystem is modeled based on a composite of its components.

FAILURE GROUP is the number of users affected by an outage that is going to be "counted" in the overall availability calculations. Per the Telcordia standard (footnote 1), an outage is counted as its duration multiplied by the percentage of users affected. For example: for an outage of 20 minutes affecting 10% of the users, the contribution to overall downtime is 10% X 20 minutes = 2 minutes. In the case of IP endpoints, the calculations in this document are

based on failure group sizes as low as one. This is by virtue of the dynamic assignment of CLAN and Media Processors resources (no hard connections creating a single point of failure, and assuming at least N+1 redundancy).

As another example, in the case of TDM connections, say 24 users are served by a digital Circuit Pack, TN2224. The impact may be calculated:

24 users impacted/1000 total users X outage duration.

Since the MTBF for the TN 2224 is 45 – 50 years and if an MTTR of 4 hours is assumed, then the total downtime hit from that Circuit Pack (CP) is:

24/1000 X 4.8mins/year = 0.1152 mins/year.

Now, assume that for any given call, there are at least 2 parties, and they each require a connection to a digital CP: then the CP failure rate (that could affect the call) is double the individual CP failure rate:

2 X 0.1152 mins/year = 0.2304 mins/year. (99.99996% availability)

Traditionally, this failure rate is relatively insignificant with respect to other possible causes of outages (like processors, power supplies, fans, hard drives, etc). Thus, a digital board's reliability tends not be discussed since it is so rarely a problem. The low failure contribution rate applies to the other CP's that terminate end-points as well.

Critical Sub-assemblies: These are equipment items that affect many users if they fail. In Avaya Communication Manager systems, these items are designed to last a long time. Nevertheless, they won't last forever. It's important to consider with the sales team, whether having some spares of these items on hand would be appropriate to shorten the MTTR time.

- Power supplies
- Fan assemblies
- Hard drives
- Transceivers
- IP Server Interface (IPSI) CP's
- IP Media Resource 320
- Expansion Interface (EI) CP's
- ATM Interface CP's
- CLAN's
- Media Processors
- Other as appropriate

Appendix A
Avaya Availability Analyses [14]

Avaya Availability Analysis
Avaya S8300 Media Server and H.248 Gateways

(Avaya Communication Manager Software 3.x)
(based on data as of March. 30, 2006)

Sub-System	Standard Reliability (for higher availability see footnotes [15])		
	Failure/ year	MTBO (years)	Availability
S8300 Media Server	0.118	8.5	0.99994
G150 Media Gateway	0.143	7.0	0.99993
G250 Media Gateway	0.135	7.4	0.99993
G350 Media Gateway	0.118	8.5	0.99994
G700 Media Gateway	0.149	6.7	0.99993

Avaya Availability Analysis
Avaya S8400 Media Server

(Avaya Communication Manager Software 3.x)

Sub-System	Standard Reliability		
	Failure/yr	MTBO (years)	Availability
S8400 Processor	0.0657	15.2	0.99997
G650 Media Gateway	0.131	9.0	0.99994
G650 Media Gateway w/ Dup Power	0.0613	16.3	0.99997

Table 8

* This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A hardware MTTR of 4 hours is assumed which includes travel and repair time.

[14] These are engineering estimates and are conservative; as field data is collected, the numbers will be updated. A Software allowance is included in the Availability numbers, in addition to the hardware contributions.

[15] For additional availability, (0.99995+), LSP is required to back-up ICC; N+1 media gateways at each site; each IP endpoint homed to at least 2 systems run by CM Software (S8300, or otherwise).

Avaya Availability Analysis
Avaya S8500 Media Server
(Avaya Communication Manager Software 3.x)
(based on data as of March. 30, 2006)

Sub-System	Standard Reliability		
	Failure/ year	MTBO (years)	Availability
S8500 Server Complex – Direct IPSI Connection [16]	0.1314	7.6	0.99994
G650 Media Gateway	0.131	9.0	0.99994
G650 Media Gateway w/ Dup Power	0.0613	16.3	0.99997

Table 9

***** This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

Avaya Availability Analysis
Avaya S8500 Media Server
(MultiVantage Express) [17]

Sub-System	Standard Reliability		
	Failure/ year	MTBO (years)	Availability
S8500 Server Complex – Direct IPSI Connection[18]	0.1314	7.6	0.99994
G650 Media Gateway	0.131	9.0	0.99994
G650 Media Gateway w/ Dup Power	0.0613	16.3	0.99997

Table 10

***** This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

[16] Direct IPSI connection means there is no ethernet switch between the server and its gateway. Thus, the failure rate of an ethernet switch is not additive.

[17] Applies to the call processing part of the platform only. Based on predictions as of March 30, 2006. Assumptions include use of remote maintenance board, HAP and RAMdisk.

[18] Direct IPSI connection means there is no ethernet switch between the server and its gateway. Thus, the failure rate of an ethernet switch is not additive.

Avaya Availability Analysis – S87xx

(Avaya Communication Manager Software 3.x)

(based on data as of March. 30, 2006)

Sub-System	Standard (or Duplex) Reliability			Higher Reliability		
	Failure/ year	MTBO (years)	Availability	Failure/ year	MTBO (years)	Availability
S87xx Server Complex [19]	0.1095	9.1	0.99995 /	<0.01095	>91.3	>0.999995
G650 Media Gateway - IP Connect - Simplex [20]	0.131	9.0	0.99994			
G650 Media Gateway – dup'd IPSI's [21]				0.018615	53	0.999992
G650 Media Gateway - Dup'd IPSI's and Media Processors [22]				<0.01095	>91.3	>0.999995
G650 Media Gateway - Fiber Connect [23]				<0.01095	>91.3	>0.999995
G600 Media Gateway	0.131	9.0	0.99994			

Table 11

* This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

[19] For higher reliability, the S87xx server complex is provided with duplicated servers, Ethernet switches (dedicated), and UPS's. The "duplex" reliability configuration consists of duplicated servers and a UPS for each, with a single Ethernet switch (dedicated).

[20] IP Connect system – Simplex: single IPSI per PN, simplex Media Processor.

[21] IP Connect systems (dup'd IPSI's): duplicated IPSI's per PN.

[22] Duplicated IPSI and duplicated MedPro in active/stand-by configuration.

[23] Fiber-connect systems – Duplex: duplex IPSI's and EI's .

Avaya Availability Analysis

DEFINITY® Server R

(Avaya Communication Manager Software 2.x)

(based on data as of Aug.. 30, 2005)

Sub-System	Standard Reliability (Single Processor Complex)			High Reliability (Duplicated Processor Complex)			Critical Reliability (Duplicated Processor Complex)		
	Failure/ year	MTBO (years)	Availability	Failure/ year	MTBO (years)	Availability	Failure/ year	MTBO (years)	Availability
DEFINITY Server R Processor	0.153	6.5	0.99993	<0.01095	>91.3	>0.999995	<0.01095	>91.3	>0.999995
SCC1 or MCC1 Media Gateways	0.153	6.5	0.99993	0.0657	15.2	0.99997	<0.01095	>91.3	>0.999995
CSS Intf	0.1095	9.1	0.99995	0.0876	11.2	0.99996	<0.01095	>91.3	>0.999995

Table 12

* This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

Avaya Availability Analysis
DEFINITY® Server SI
(Avaya Communication Manager Software 2.x)
(based on data as of Aug.. 30, 2005)

Sub-System	Standard Reliability (single Processor Carrier)			High Reliability		
	Failure/ year	MTBO (years)	Availability	Failure/ year	MTBO (years)	Availability
DEFINITY Server SI Processor	0.219	4.6	0.9999	<0.01095	>91.3	>0.999995
SCC1 or MCC1 Media Gateways	0.153	6.5	0.99993	0.0657	15.2	0.99997

Table 13

* This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

Avaya Availability Analysis
DEFINITY® Server CSI
(Avaya Communication Manager Software 2.x)
(based on data as of Aug.. 30, 2005)

Sub-System	Standard Reliability		
	Failure/yr	MTBO (years)	Availability
DEFINITY Server CSI Processor	0.1643	6.1	0.99995
CMC1 Media Gateway	0.0657	15.2	0.99997

Table 14

* This analysis does NOT include availability of the customer's data networks, PSTN contributions, or contributions due to power outages. See further discussions below. A conservative hardware MTTR of 4 hours is assumed which includes travel and repair time.

Appendix B

Assessment Methodology:

Markov Chain Reliability Modeling is used for predicting total system hardware availability. The advantage of this technique over others (for example, the *parts count* and *combinatorial* models) is its ability in capturing the fault-tolerant aspect of the platform.[24] [25]

There are two parameters used for the mathematical modeling: individual-component failure rate, and averaged annual downtime experienced by end users due to the failure. Full system availability is assessed by determining the contribution of subsystem failure rate and downtime in the overall service provided to the end users. failure of core components such as the S87xx Servers and Ethernet Switches impacts all end users, and the downtime due to such failures is counted against the total system availability. Subsystem failures, which impact a fraction of end users, are partial outages, and the downtime due to such outages is prorated in accordance with the percentage of end users to whom service was lost.[26]

Availability Predictions Given Individual MTBF and Failure Rates

Availability of each subsystem is modeled based on a composite of its components. For each component, MTBO is calculated as the reciprocal of estimated average failure rate (FIT [27]), and a conservative average repair time (MTTR) of 4 hours is assumed to account for technician travel time. The following formula is used to measure availability of critical components.

A = MTBO/(MTBO+MTTR)

When there is duplication for the purpose of meeting higher availability, the following state-transition diagram is applied:

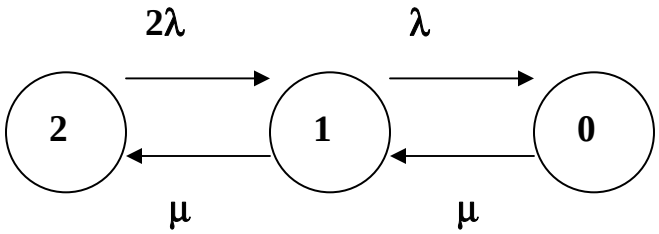


Figure 1: State Transition Diagram for Redundant Components

In Figure 1, state **2** represents both components (one in active mode and the other in standby) are operational, state **1** indicates only one is operating, and for state **0** both are in failure mode. The system is operational in both states **1** and **2**. The failure-arrival rate is associated with transitions from state **1** into state **0**. The probability of such an event happening is given by:

---

[24] Reibman, Andrew L. and Veeraraghavan, Malathi, Reliability Modeling: an Overview for System Designers, IEEE Computer, Vol 24, April 1991, pp 49-57.

[25] Boyd, Mark, *An Introduction to Markov Modeling: Concepts & Uses*, Annual Reliability and Maintainability Symposium, Anaheim, California, January 1998.

[26] Such analysis and terminology is in accordance to Hardware Reliability Parameters, Section 4, and Outage Classification Categories, Section 7.1, Bellcore GR 512, 1995.

[27] Failure in Time (FIT).

$$F = \lambda \times \mathrm{P}_1$$

$$\mathrm{P}_1 = \frac{2\lambda \times \mu}{\mu^2 + 2\lambda \times \mu + 2\lambda^2},$$

where P_1 is the probability of being in "state **1**", λ is single-component failure rate and μ is repair rate.[28]

The Avaya S87xx Server Complex Availability Analysis (this section covers hardware ONLY; Avaya CM Software is modeled separately)

To attain high availability for large systems, the Avaya S87xx Server complex consists of two paired servers. One acts as the active server, and the other is the standby. To capture modifications of memory made on the active processor, and transfer them to the standby processor's memory, the servers contain a duplication module. Memory writes are sent across a very high-speed fiber optic link for replication on the standby processor. This fiber optic cable is a key element of the duplicated Control Complex; however, since the failure rate of a cable is negligible (unless it is cut accidentally), the FIT rate of this link has not included in this analysis.

Two configurations are shown for the S87xx servers. The High and Critical configurations are designed with duplicated Servers, Ethernet Switches, and UPS. The Duplex configuration is designed with duplicated Servers and UPS and a single Ethernet Switch. Individual hardware reliability numbers are listed in Table 1.

Control Components	Mean Time Between Failure (years)	Failure/year	FIT
Server	6.025	0.166	18,947
Ethernet Switch	16.37	0.06	6,971
UPS	14.27	0.07	8,000

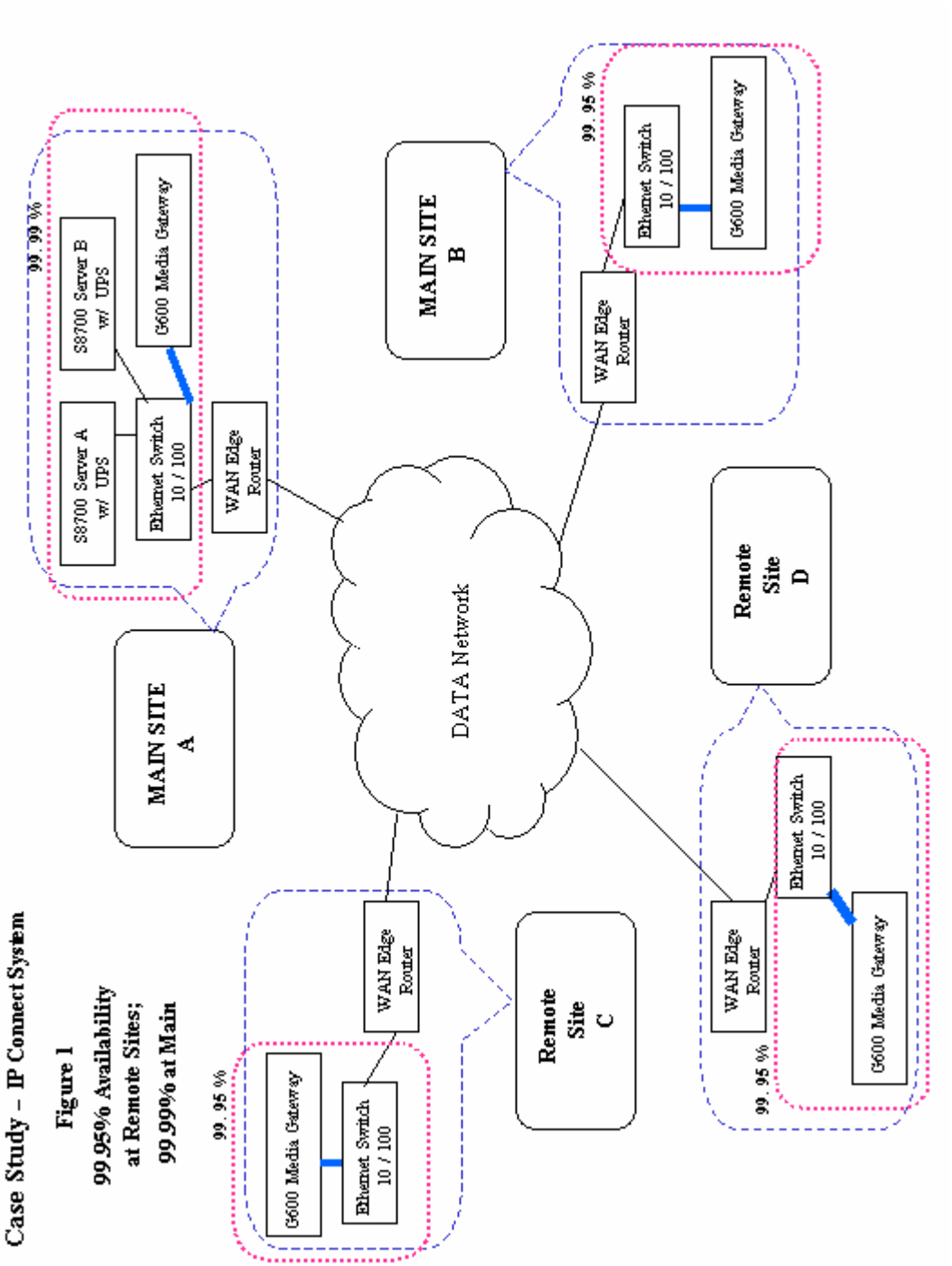
Table 10: Reliability Numbers for the Individual Control Components[29]

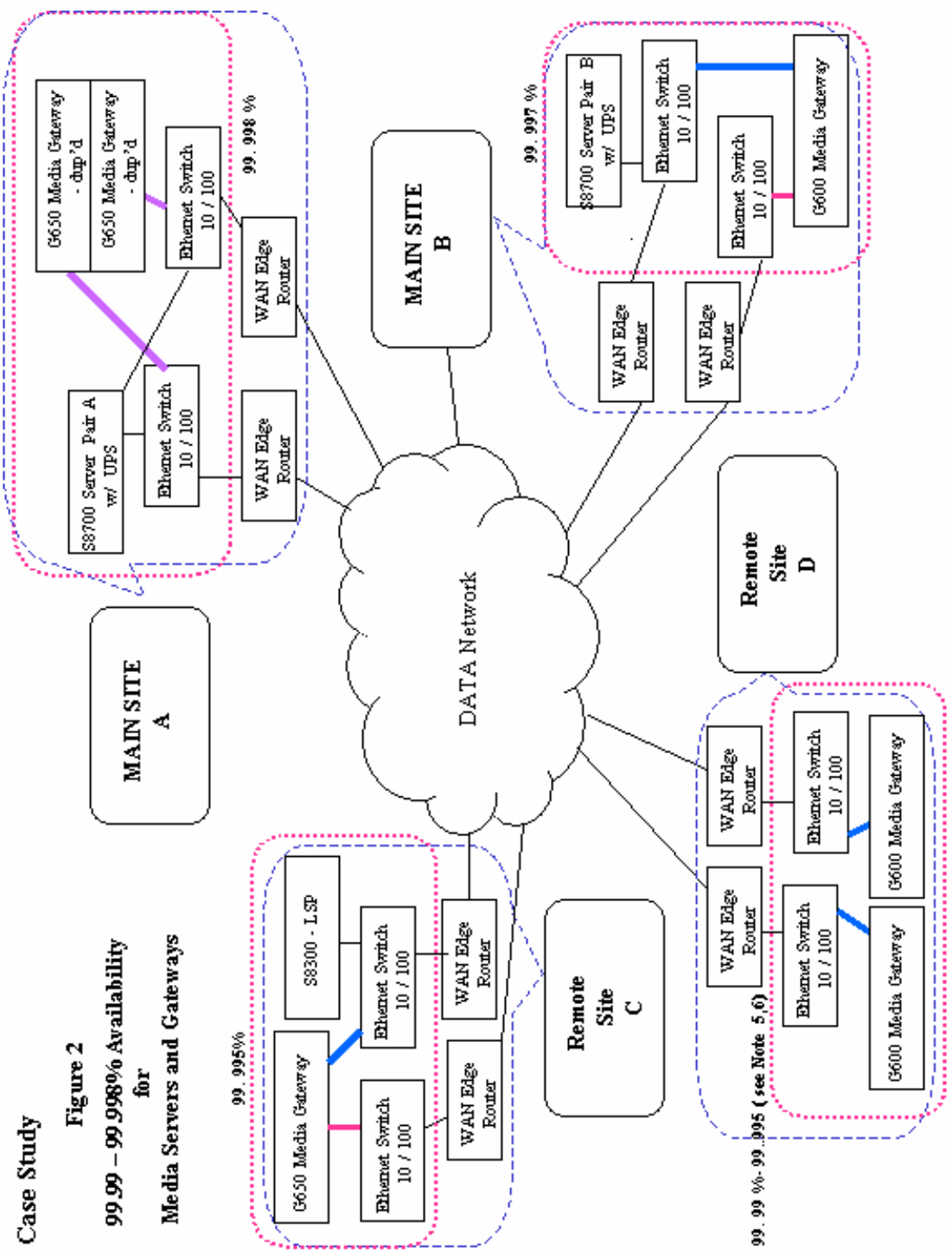
The MTBF listed for the server is the MTBF calculation of the Intel SRTR1 Server. The calculation includes four fans, power supply, motherboard, processor memory, front panel, PCI riser, hard disk and CD-ROM.
The MTBF listed for the Ethernet Switch is the reliability number provided for the Cajun P333, which is the recommended Ethernet switch for the private control network. [30]

[28] Markov Reliability Model normally assumes when in state 0, there will be 2μ repair time, which implies service is applied on both components simultaneously.
[29] Server MTBF is provided by Mike Ross, Ethernet Switch and UPS MTBF is listed in S87XX Architecture, COMPAS ID 74848.

[30] Momken, COMPAS ID 86557.

Appendix C



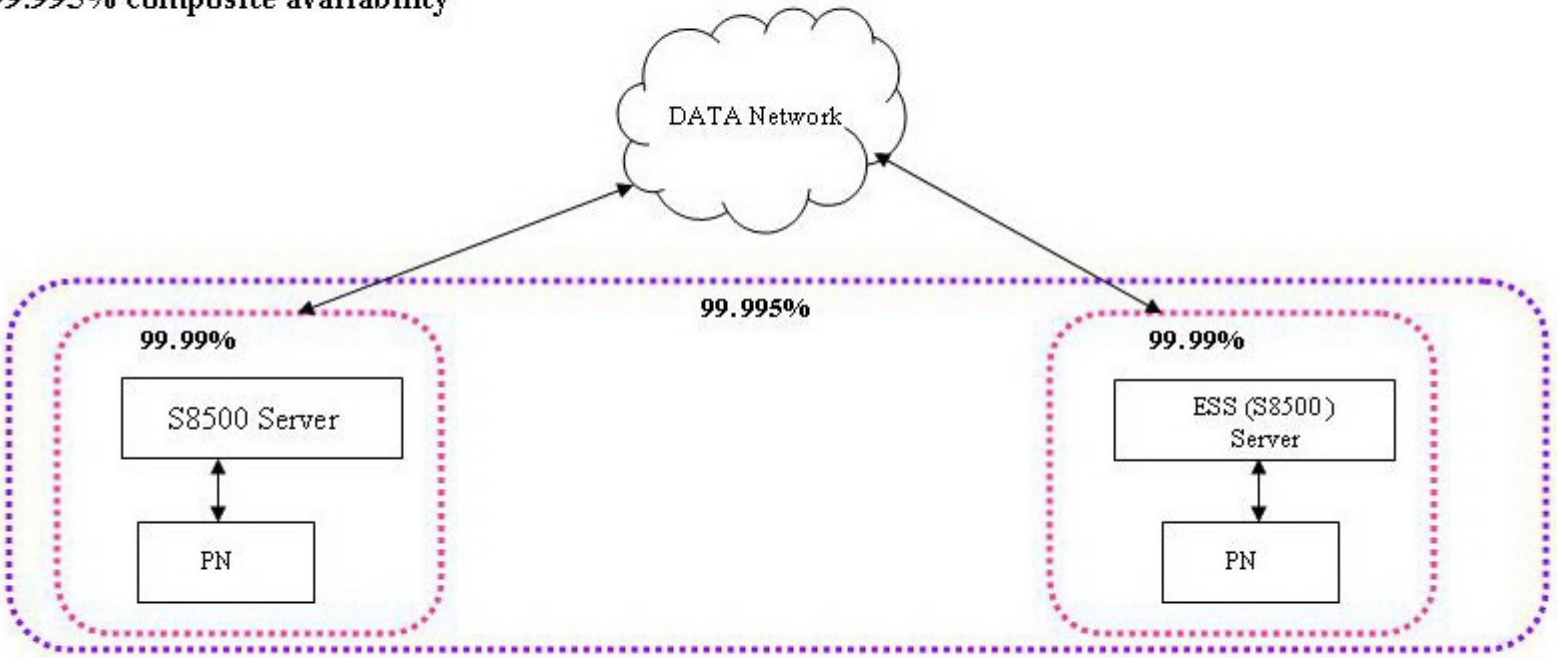


Case Study

Figure 3

99.99% availability at each S8500 sites;

99.995% composite availability



Each S8500 Server has its own availability. ESS-S8500 provides back-up in case of failure of the primary server. The combined availability is higher than the individual availabilities. The combined availability is also dependent on network robustness between the main server and the ESS.

Notes:

1. All availability calculations assume a MTTR (mean time to repair) of 4 hours.
2. Availabilities shown in the diagram refer to parts of the systems surrounded in pink dotted lines.
3. The server pair (and Software) at Main Site A has availability = 99.9995+. This added with the numbers for associated UPS's and directly connected enet switches result in 99.99% for the ***complex*** (outlined in pink).
4. To achieve 4 9's at remote site:.
   a) Assure that each gateway has both IPSI/CLAN/Med Proc links to enet switch; AND separate CLAN/Med Proc. Link that can be routed to a duplicate (or back-up) WAN link.

      or

      Employ modern techniques such as HSRP and VRRP allows dynamic re-routing if a router (or WAN circuit) fails.

   b) Assure that every IP Phone has at least 3 valid gatekeeper addresses that do not depend on the same WAN link (or at least have WAN link back-up).
5. To achieve availability approaching 5 9's at remote site: (note that 99.997 = 15 mins downtime per year).
   a) Provide some source of call control at the site (can be an LSP), for each site needing critical reliability
   b) Provide a secondary source for call control either at same site, or from a remote site.
   c) Assure that every IP Phone has at least 3 valid gatekeeper addresses that do not depend on the same WAN link (or at least have WAN link back-up). At least one address should be to a remote call controller.
   d) The S8700 should have two ingress points to the data network
   e) assure duplicated IPSI/CLAN/Med Proc links that take advantage of duplicated (or back-up) WAN links.
   f) duplicated data networks needed.
2. Blue lines indicate IPSI/CLAN/Media Processor Links.
3. Pink lines indicate CLAN/Media Processor links.
4. Trunks to outside world should be spread across at least three sites.