

Communication Applications Complex  
Distributed Switching System

# Advanced Communications System

Provides a overview of product features and concepts  
of operations for the MeritVoice Advanced Communication System

January 2008



## Reference Architecture

The reference architecture depicts the logical topology of MeritVoice's Advanced Communications System (ACS). The ACS is comprised of (a) the Communication Applications Complex (CAC), (b) the Distributed Switching System (DSS), and (c) the access interfaces and methods to end-user locations.

The ACS is a best-in-class framework with network elements from Genband, Tekelec, Cisco, Conveda, Sun, etc. The ACS is geographically dispersed and integrated at Merit switching centers in multiple locations across the Great Lakes region. Interconnection with other carriers or peering partners is accomplished via comprehensive IP or PSTN connectivity.

All components and the inherent design of the ACS are built upon diversity and redundancy. Diversity provides multiple ways to accomplish the same thing e.g. termination of traffic to the PSTN. Redundancy means that the components themselves have built-in duplication at all levels (e.g. power supplies, interfaces) and also at the system level (i.e. components are deployed in pairs.) For example, the Call Agent Servers will successfully switchover when either the primary Call Agent Server becomes unavailable or the Network Switch or link to the Call Agent Server disconnects.

## Communication Applications Complex Overview

The Communication Applications Complex (CAC) contains the application servers for the Call Agents and Database Agents, servers for hosted enhanced applications (such as conferencing, unified messaging, Web Portal), gateways, and components (Session Border Controller, DTMF Proxy, and Streaming Server).

The components are standards based and best-in-class, optimized for discrete functions, quality, reliability, security, and scalability, including a pathway to a full IP Multimedia Subsystem (IMS) architecture.

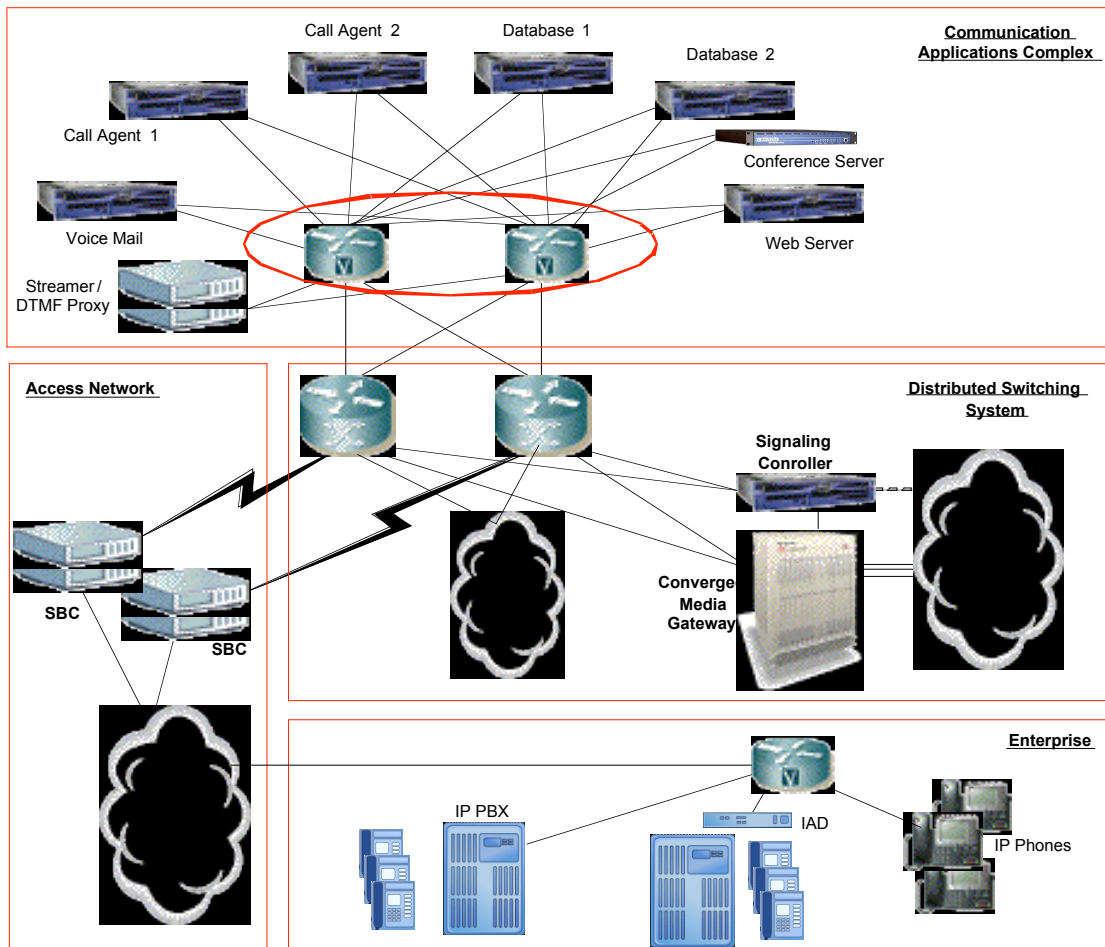


Figure 1: Advanced Communications System Logical Architecture

## Distributed Switching System Overview

The Distributed Switching System (DSS) is composed of Signaling Controllers and Media Gateways tailored to the application and traffic carrying capacity required. It also includes the Element Management System (EMS) that is used for fault and security management as well as configuration and performance monitoring.

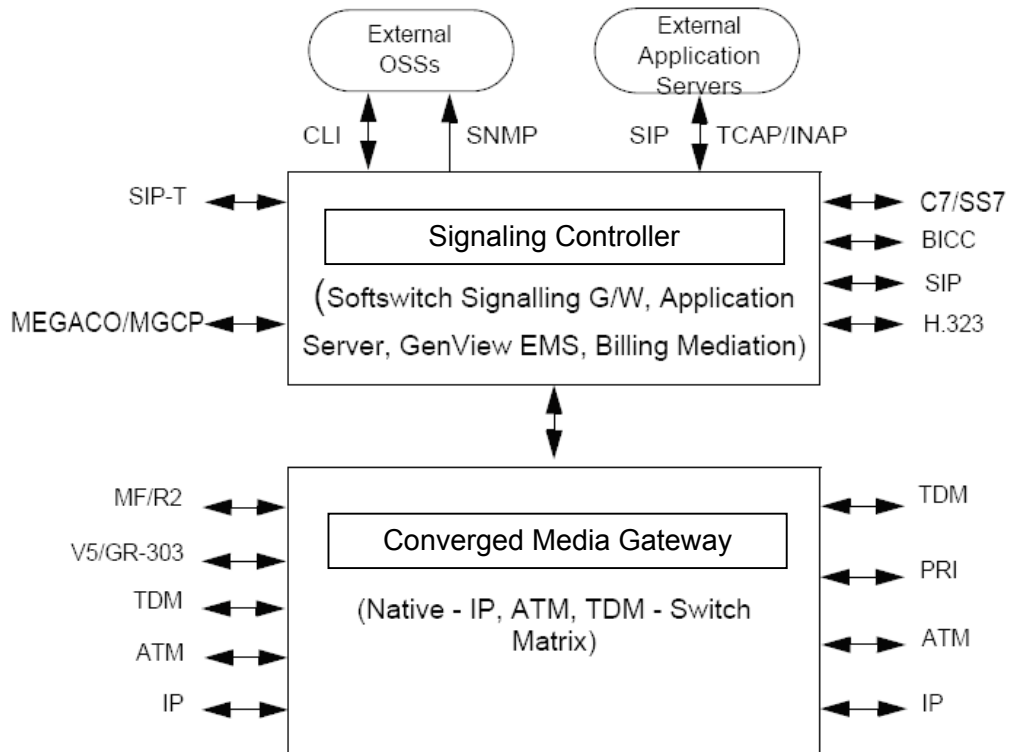
The system is a carrier-grade integrated voice and data switching solution and delivers key applications such as full feature Tandem (Class 4), Organization and Residential Voice Services (Class 5), Internet Call Diversion (ICD), Voice Over IP (VoIP), Voice over DSL (VoDSL), Voice over ATM, (VoATM), and wireless support. The system has both circuit (Time Division Multiplexing [TDM]) and packet fabric. The packet based fabric is optimized for IP and ATM while the TDM fabric provides TDM

switching.

The system also supports all of the regulatory requirements including Lawful Intercept, CALEA and Emergency calling. The system design enables a graceful migration from traditional circuit-based networks to next generation packet-based technology.

The Signaling Controller chassis hosts the media gateway controller, signaling gateway, EMS, application server, and Ethernet switches.

The Converged Media Gateway is a high-capacity, multi-fabric, multi-service platform that enables connectivity between next generation and legacy networks, whether wireless, wireline, converged or IMS. The Media Gateway scales to 60,000 ports per each chassis.



**Figure 2: Signaling Controller and Converged Media Gateway Systems (DSS)**

The ACS is a commercially proven applications service solution that delivers value-added applications over legacy and IP networks to a wide range of customers.

## Features and Functions

### Virtual Private Network

The ACS's Virtual Private Network is an advanced application that enables customer's voice services to be carried over an IP VPN. The customer that is provisioned with an IP VPN would have its own number and dialing plans, features, On-Net Routing, Outbound Flex Routing and Remote Call Forwarding access.

A customer with geographically dispersed organizations and communication needs benefit greatly from the VPN feature. The flexibility to route calls, independent of physical site location, either on-net or to a PSTN gateway for local delivery, represents significant toll charge and communication facilities cost savings.

### Organization Access

The ACS system has the ability to serve a wide range of needs from basic organization to sophisticated organization customers with reliable, full-featured voice over IP service.

Two enterprise access solutions are available:

- Organization Features
- Organization Trunking

While these access packages are described individually below, they can be implemented in combination to suit a given customers' communication requirements.

An intuitive and comprehensive systems administrator console is available to customers who wish to gain complete control and visibility over the provisioning and operations of the communications complex for their enterprise.

## Organization Features

The ACS system provides a cost-saving infrastructure that brings the power of a corporate PBX or Centrex service to enterprise customers who no longer have to invest in PBX equipment and its maintenance or deal with managing a Centrex implementation. The hosted virtual PBX or Centrex service for enterprise customers provides a comprehensive organization feature set using IP and analog phones that includes the following features:

Abbreviated 2-digit Dialing	Anonymous Call Rejection
Authorization Code Calling	Billing Codes
Broadcast Paging	Call Back Queuing
Call Block (Selective Call Rejection)	Call Forward All Calls
Call Forward Busy	Call Forward No Answer
Call Forward Out of Service	Call Return
Call Screening	Call Trace
Call Waiting	Call Waiting ID
Call Waiting/Caller ID Manager	Caller ID
Caller ID Block	Class of Service
Console Assistant Application	Conference
Direct Extension Assignment	Direct Inward Dialing
Direct Outward Dialing	Directed Call Pickup
Distinctive Ring	Do Not Disturb
Emergency Number Support	Emergency Mobility Support
Forward to Voice Mail	Find Me No Answer
Group Call Pickup	Hold-on Queuing
Hold	Hunt Groups
Indicated Call Park	Intercom
Last Call Return	Meet-Me Conferencing
Multi Call Park	Music on Hold
Mute	Night Mode (After-hours Answering)
On-Net Routing	Permanent Caller ID Block Release
Phone Configurator	Priority Call
Privacy Guard	Queue/ACD
Reassign Phone	Redial
Release (End Call)	Remote Access to Call Forward
Remote Phone	Selective Call Forward
SoftPhone Application	Speed Dial
Time-of-Day Routing	Toll Bypass
Transfer, Blind & Supervised	Urgent Call
Virtual Ring	Web Portal
Voice Mail	

## Organization Trunking

The ACS solution can integrate legacy telephony customers into the IP network by providing data and telephony on the same trunk to the PSTN,

or set up legacy customers for a growth path into hosted IP telephony either as a switchover or as a gradual growth solution.

Organization trunking capability allows connections to existing key systems and PBXs using Integrated Access Devices (IADs) or gateways, including connections for IP-PBXs. Customers retain their PBX/Key System feature set, while having access to the full range of Virtual PBX features and applications.

The organization trunking functionality of the ACS allows for multiple route destinations to be defined for provisioned customer trunks. When a customer is added to the system, alternate trunk groups can be selected in the case where the connectivity to the IP PBX or the IP Gateway device is down. This feature allows an always available call completion to be achieved by providing multiple destinations for the call. Multiple main line numbers can be added to the routing allowing for overflow routing in the case of All Trunks Busy or system down scenarios. Also, multiple Auto-Attendant numbers can be provisioned, as well as multiple voice mail destinations.

### **Conferencing**

A convent and robust conferencing services system is available to provide audio and audio/video conferencing. The ACS system supports the following types of conferencing:

- On-demand or ad hoc - Users can create conferences using a web portal interface with a one-step conferencing, feature buttons, or star codes within parameters set by system administrators.
- Meet-Me - Authorized users can reserve conference ports for a specific date and time when users, who have been provided with the proper telephone numbers and passwords, can call in and join the conference.
- The multi-media assistant feature enables conferences to include video cameras.

### **Voicemail and Unified Messaging**

Traditional voice mail can be accessed from the phone or from a PC using browser based web portal. Companies can integrate voice mail, faxes, and e-mail: viewing, managing, and accessing their voice messages as part of the email environment.

### **Web Portal**

The ACS Web Portal is a browser-based application that can be accessed through the local area network or over the internet. Support is also provided for access from mobile devices. The Web Portal conveniently manages many of the ACS phone features.

Using a web browser, a user has access to an impressive array of

6productivity tools:

- Company and Personal Directories
- Call Log
- Call Screening
- Call Forwarding
- Call Control
- Customized Phone Features
- Find Me
- Audio Conference Scheduling
- Remote Phone Features (Simultaneous Ring)
- Reassign Phone
- TAPI-based Calling (for applications such as Microsoft Outlook)
- Time-of-Day Call Routing
- Voice and Unified Messaging

### **Queue/ACD**

The call queuing feature allows the ACS system to distribute incoming calls arriving at the pilot number (either DID or non-DID) to a pre-configured group of phones. If the number of calls arriving at the pilot number is less than the number of phones in the group, the calls are redirected immediately to one of the phones. If all phones in the group are busy, the incoming calls are held in a first-in-first-out queue until a phone becomes available. While a call is held in the queue, it can be connected to announcements or music-on-hold. Adding Queue lines to a phone requires that the phone have an available line appearance. It is generally recommended that phones used for agents in an ACD queue be multi-line phones capable of support multiple line appearances.

Queue/ACD offers the following features:

- Agent Membership in Multiple Queues (dependent on phone)
- Time-of-day routing
- Queue log in/out
- Multiple Announcements
- Calls in Queue Display (dependent on phone)
- Queue Overflow
- Programmable Queue Answer
  - Top-To-Bottom
  - Bottom-To-Top
  - Longest Idle (aka Universal Call Distribution)
  - Round Robin (aka Circular)

### Communication Applications Complex

Bandwidth is a limited resource which is crucial to quality of service in voice over IP service. The ACS incorporates the IPLink feature as a cost-effective alternative to re-engineering the network to provide protection against the degradation of voice quality on calls across the IP path that connects the ACS to the customer premises. The ACS system checks a system table of available bandwidth before a call is completed and returns a busy signal if the table indicates there is not enough bandwidth available for the call. IPLink is not intended to replace quality of service strategies such as the use of TOS bytes and engineering of network links.

The ACS system is also able to allocate bandwidth differently for normal calls than for "receive-only" calls. A normal call is the one where a two-way communication is established and a receive-only call is one where there is one-way communication, such as voicemail retrieval, scheduling of a Meet-Me conference, etc.

The bandwidth of an IPLink is allocated as follows:

- **Normal** - Total bandwidth allocated to the IPLink
- **Receive-Only** - Percentage of total bandwidth that will be used for receive-only calls. Receive-only bandwidth is a subset of Normal bandwidth.

Bandwidth for a normal call can be allocated without any restriction as long as there is bandwidth available. The Receive-Only bandwidth of that IPLink may be allocated for a normal call. However, receive-only calls cannot use any bandwidth beyond the specified receive-only bandwidth.

#### IPLink and Emergency Calls

When the allocated bandwidth on a particular IPLink is consumed, then some calls will not be connected. However, emergency calls will always be put through.

- Emergency calls will never be disconnected because of a no-bandwidth situation.
- No attempt will be made to idle non-emergency calls to 'make room' for a emergency call

- Once a call has connected, it will not be disconnected (idled) with no bandwidth, even if the call re-negotiates to a higher bandwidth codec that would exceed the IPLink maximum of the source or destination endpoint.

## Distributed Switching System

The Signaling Controller and the Media Gateway are viewed logically as one switching unit. The two functional components form a single Distributed Switching System (DSS). The DSS provides numerous capabilities to ensure the highest quality of service for calls delivered through the system. The majority of the capabilities relate to diagnostics of internal hardware components of the system along with trunk and circuit related testing and monitoring for TDM traffic. These include diagnostic routines, tests, and status checks such as On-Demand Tone Generation, On-Demand Outpulsing Test, On-Demand Signaling Test and Remote Make Busy, Milliwatt and COT Tests, Circuit Validation Test (CVT), Echo Cancellation, and System Status. The system status tool provides the user with information about the Media Gateway, Signaling Controller, cards, facilities, and links. In addition, the workspace displays CPU and traffic information, such as CPU peak and average rates and calls per hour. To aid call monitoring the system displays a graph with the average calls per hour per 10-second intervals.

### IP Test Call Management and Performance Alarms Test

The IP Test Call Management and Performance Alarms Test allow the operator to assess the IP connectivity and QoS (Quality of Service) for the system, by using a set of diagnostics tools to identify various network problems.

The IP Test Call Management and Performance Alarms Test provide several capabilities in support of monitoring and debugging the VoIP network. Collecting summary measurements on the IP network paths between MGs, based on the RTCP (Real Time Transport Control Protocol) statistics associated with the media streams of regular VoIP calls:

- Issuing alarms when the measurements at the end of a 15- or 30-minute reporting period exceed user-configurable thresholds.
- Manually checking the IP network path between MGs
- Validating the IP connectivity between the Signaling Controller nodes and the customer's edge routers. If an IP address is not reachable, then an alarm is generated.
- The ability for the operator to execute the IP 'traceroute' command from the Signaling Controller
- Manual IP Test Call

The ACS system uses a variety of security features to protect both system and user features.

## Standard Security Features

- Administrator Login
- Web Portal Admin User
- Admin User IP Address Tracking
- Merit Command to Manually Log Out Admin Users
- Application Passwords
- Password Expiration
- Invalid Login Tracking
- Disable Reassign Phone
- Phone and Voice Mail Password Security
- Session Border Controller Security

## Session Border Controller (SBC) Security

The ACS Call Agent and Session Border Controller (SBC) software allows the hiding of the IP addresses of the Call Agents or other server related devices on the private side of the SBC from being displayed in SIP messages to endpoint devices on the public side of the SBC.

The Session Border Controller (SBC) is the interface between the private IP network and the publicly addressed IP infrastructure. To ensure maximum reliability, SBCs are deployed as redundant pairs. The ACS includes multiple redundant pairs as needed to support the end user population.

The Session Border Controller serves several purposes:

- Providing normal NAT/PAT firewall transversal functions for the ACS devices on the private LAN. That is, it hides the ACS call agents and gateways from the outside world.
- Allowing IP Phones and access gateways to function behind a customer's conventional firewall by compensating for the restrictions placed upon communication devices (such as hiding private IP addresses) in a firewall-protected environment.

- Providing fraud detection through the use of white (allowed) and black (blocked) lists of IP addresses and net masks. These lists are maintained through the Administration Application, but automatic blacklisting is available based on parameters that can be configured through the Administration Application.
- Supporting the use of static routes (a.k.a. static sessions) when a remote device does NOT send any type of boot/registration command and the device is behind a data firewall. A static route is a predefined session with a predefined destination that will not timeout, is not dependent on a boot/ register command from the device, and is "created" via the Administration Application. When a static route is configured, the Remote IP (data firewall) address will be added to the SBC's list of valid IPs.
- Providing a short circuit feature that routes the RTP stream between two user's telephones without having to route the call all the way back to the Session Border Controller. This reduces the load on the Session Border Controller and reduces traffic on the links from the customer premises to the Session Border Controller location. Additionally, calls that are short-circuited are not counted against the maximum bandwidth for the link, if the IP Link feature is being used.

In performing these functions, the Session Border Controller provides seamless signaling and RTP communication between the ACS system and IP phones, gateways and IP PBX.

The Session Border Controller operates in parallel with the data firewall to allow TFTP, SCCP, MGCP, SIP, and ICMP (ping) traffic to pass through while not allowing HTTP traffic through. The network's data firewall is responsible for passing HTTP traffic from the private to the public LAN.

## **EMS**

The EMS is the fault, configuration, performance and security management platform for DSS system. The EMS is implemented as a client-server architecture with redundant server applications. The EMS GUI clients reside on Windows based PCs and access the EMS servers via an IP network. The EMS servers also support command-line provisioning and a northbound SNMP interface for fault notifications to a Network Management System (NMS) or other support systems.

## **Security Management**

The security administration function allows a security administrator to establish and configure settings for the system. The chief functions of

11 security management include:

- Administrating the various levels of security for users
- Setting user authentication parameters
- Enforce user privileges (e.g., user group profile)
- Set system wide policy (e.g., password expiration, security log, security ID settings)
- Log query function
- Managing user passwords
- Managing user groups
- Managing user profiles

The EMS supports user authentication and authorization by requiring users to log on with a unique user ID and password. The Superuser assigns users to a user group which defines the user's role to any or all of the EMS functional areas.

This flexibility allows the system administrator to restrict users to the functional areas for which they are responsible, so that one group may be restricted to configuring office parameters and another to viewing billing parameters.

The security administration functionality also allows the system administrator to modify privileges and the status of an active group, and force a lockout of individual users, even when they are logged on to the system.

### Communication Applications Complex

Two server stacks always run the Server Call Agent. The secondary server remains in a hot standby mode, ready to take over in the event that the primary server fails for any reason. No established calls are lost during a switch over from the primary to the secondary server. All call connection information for any call is mirrored on the redundant Call Agents, ensuring carrier-grade reliability and scalability. Mirroring assures that once a call is established, it can be managed for its duration, despite the loss of either call agent. Since the “mirroring” call agent contains the call connection information for all currently active calls, it will continue to manage requests for services from these calls.

The CAC also supports redundant Database Agent stacks. The database is managed through the Master Database Agent, but is mirrored on the Secondary Database Agent, which can assume system management duties if the Primary Database Agent becomes unavailable.

The Session Border Controller (SBC) is also installed as a redundant pair with one SBC in a hot standby mode, ready to take over in the event that the primary SBC fails for any reason. Additional pairs of SBCs can be installed in a system and, depending on the endpoint capabilities, can provide a backup function in case a pair of SBCs are placed in an out-of-service condition for any reason.

The CAC network architecture also calls for redundant Ethernet switches to reduce the chance of a single point of failure disabling the entire network. Call Agent servers support dual Ethernet ports that allow for distributed connections to the Ethernet switches with automatic failover between the ports on individual Call Agent servers.

Applications that access the database (i.e., Web Portal, Console Assistant, etc.) support a connection to the second server so that when this feature is implemented the application will automatically connect to the backup Database Agent in case of an interruption of service to the primary Database Agent. This also provides for a redundant provisioning interface for the System Administration Application or customer provisioning applications.

## **Reliability Feature: Call Agent Safe Mode**

Safe mode is enabled when a Slave Call Agent Server unexpectedly loses communication with the Master Call Agent. This could happen for several reasons, such as a Master Call Agent server crash, a cable pull/disconnect, or any event that would cause an uncontrolled swap. A controlled, graceful server swap will not enable Safe Mode.

Safe Mode is enabled to protect simplex operation of the Slave processor. Safe Mode is terminated when the Master processor comes online and is fully mirrored.

The following are the characteristics of Safe Mode operation:

- Database updates are disabled. Any database changes made in the Database Agents will persist in the Administration Application database, but will not take effect in the Call Agent operating in Safe Mode. This protects system from dual swaps in the event of database corruption. When the system transitions from Safe Mode to normal operations, the database changes made during the Safe Mode duration will take effect in the Call Agents.
- The Watchdog process timeout for terminating the main VOISS process is extended when in Safe Mode to allow the simplex Call Agent extra time to complete processes and avoid trying to swap back the unavailable Call Agent. The default is 30 seconds, but can be changed through an Oats.ini setting.

## **Signaling Controller**

The Signaling Controller nodes operate as computing resources that are either available to provide service or not. For the node to be in service, it must be powered up, running the base platform, and have Ethernet connectivity to the other nodes in the system.

Application software is assigned to run on the node per the configuration database. Load-shared programs are assigned to at least two nodes for redundancy, but can be assigned to more as needed. For example, the Call Manager is frequently assigned to all nodes in the system so it can use the available CPU resources.

If a Signaling Controller node fails, the Operation Administration and Maintenance (OAM) programs coordinate the activation of the standby instance of any program that was active on that node. If just one program on the node fails, the OAM programs coordinate the activation of the standby program if that was the active instance.

While the system's Signaling Controller units are load-sharing, they also provide backup for each other. If one Signaling Controller unit fails the remaining unit assumes all call processing functions.

The power supplies within each unit provide N+1 redundancy.

Geographical redundancy of the Signaling Controller is supported for Class 4 and Class 5 applications for both VoIP and TDM. With geographical redundancy, the Signaling Controller nodes are distributed over two geographically distributed sites to protect against a total switch failure due to a catastrophic site failure.

## **Converged Media Gateway**

The Media Gateway is designed to meet telecommunications industry-standard reliability and availability expectations, including "five-nines" (99.999%) system availability, for both hardware and software components. These expectations are met by providing highly-reliable, redundant hardware and software components.

The Media Gateway chassis consists of a high-reliability midplane that provides redundant point-to-point bearer- and control-plane connectivity between interface and service card slots and their associated switching matrices. For IP bearer traffic, the midplane provides two GbE connections from each PAC card slot to every other slot in the chassis except the two SST card slots. In addition, for control traffic, there is a separate GbE connection between the PAC slots and all other chassis slots. For TDM traffic, there are 16K point-to-point TDM channels in the midplane between the SST card slots and all other chassis slots (currently, only 8K channels are utilized by the SST cards). Additionally, the midplane provides protection busses for T1 and E1 cards (one bus per chassis) and for DS-3 cards (two per chassis). The chassis also contains redundant power feeds and hot-swappable cooling fans.

Integral with the Media Gateway chassis is the Shelf Interface (SI) unit which provides the connection points for data and clocking inputs to the chassis. The SI unit consists of two SI cards, each with 1/2 of the total SI connections on it. Thus the two cards together provide a fully redundant (dual active) set of shelf interfaces.

All of the Converged Media Gateway circuit cards are redundant, with different protection schemes depending on the card type. In addition, the Media Gateway provides protection schemes for its network interfaces.

### Communication Applications Complex

The CAC system is based on NEBS-certified Sun Netra servers taking advantage of the range of available processor speeds, memory configurations and storage capabilities to provide systems matched to anticipated needs with room for projected growth. This architectural design enables service providers to initially serve a small customer base with the flexibility to grow into a much larger capacity system of hundreds of thousands of users.

Capacity is added as demand dictates. Additional call processing, conferencing, voice messaging, PSTN gateways and other system capacities are added as the customer-installed base and revenue increases.

The Call Agent servers in the complex provide the core call processing and call control for all of the sessions routed through the system. This is a critical component that runs in an active/hot standby redundancy scheme. When server capabilities are exhausted and additional horsepower on a single redundant pair is not feasible, additional Call Agent pairs can be inserted into the system. The complex then becomes a cluster.

The Conference Server is a shared resource providing conferencing capabilities for all users. A single Conference Server can support any number of conferences up to its port maximum. To scale this conferencing resource, multiple conference servers can be supported to provide additional conferencing port capacity.

### Signaling Controller

The Signaling Controller and Converged Media Gateway system is composed of varying numbers of Gateways and Controllers depending on the applications and traffic carrying capacity required. The architecture supports scaling to over 10 million busy hour call attempts (BHCA) and close to 1 million TDM ports.

## Converged Media Gateway

The Converged Media Gateway is a high-capacity, multi-fabric, multi-service platform that enables connectivity between next generation and legacy networks, whether wireless, wireline, converged or IMS. The Gateway economically scales from a few dozen IP, ATM and TDM ports to almost 60,000 ports. Table 1 provides examples of Gateway capacities for several common configurations.

Configuration	Ports			Notes
	TDM	IP	Total	
100% T1	15,840	-	15,840	One protection group
100% E1	19,800	-	19,800	One protection group
100% DS-3	40,320	-	40,320	Two protection groups
100% OC-3	48,384	-	48,384	
100% STM-1	45,360	-	45,360	
50% OC-3 and 50% G.711	28,280	28,280	56,560	VS-8A voice server cards
	28,672	28,672	57,344	VS-8B voice server cards
50% OC-3 and 50% G.729	18,480	18,480	36,960	VS-8A voice server cards
	29,184	29,184	58,368	VS-8B voice server cards

**Table 1: Maximum Gateway System Capacity Examples**

## Communication Applications Complex

The CAC operates using industry standard protocols and RFC's/drafts. Although ACS operates using industry standards, not all handset and gateway vendors implement them the same; therefore, the ACS accommodates this by "profiling" a vendor or endpoint and uses this profile for all communications to that type of device. This ensures that multiple vendors can be connected simultaneously each utilizing their own profiles and signaling without adversely affecting other devices.

Several strategic endpoint and gateway manufacturers have been established and are tested with each release of software to ensure backwards compatibility and features across various protocols are operational.

The CAC is very flexible and can work with many handset and gateway providers in the market. If a vendor or model number is not listed in this document as being tested by Merit, certification methods are in place. The ACS provides Generic templates that can be modified to match the capabilities of a particular device.

### MGCP IAD

AudioCodesMP-102	AudioCodes MP-104
AudioCodes MP-108	AudioCodesMP-112
AudioCodes MP-114	AudioCodes MP-118
AudioCodes MP-124C	AudioCodes MP-124D
Carrier Access Adit 600	Cisco 2432
Cisco ATA-186	Cisco ATA-188
DLINK 1120M	Occam BLC 6000
Wave7 Optics LMG-B	Wave7 Optics LMG-R
World Wide Packets LE-32	World Wide Packets LE-36
Zhone Z-Edge 6100	Zhone Z-Edge 6200
Zhone MALC	Zhone 6200

### SIP IAD

Adtran TA-9xx	Arris EMTA
AudioCodes MP11X	Calix
Cisco 28XX	Cisco 26XX

Cisco 2432

Cisco ATA-188

Carrier Access 2400  
Carrier Access 3500  
GrandStream HandyTone 486  
InnoMedia 3328-2RE  
Linksys/Sipura SPA-2000  
Linksys/Sipura SPA-2002  
Linksys PAP2T  
MediaTrix 2102  
Patton SmartLink 4022

Carrier Access 3104  
DLink 3004S  
InnoMedia 6024-24  
InnoMedia 6328-2RE  
Linksys/Sipura SPA-2100  
Linksys/Sipura SPA-2102  
Linksys RT31  
Pannaway

### **SCCP Phones**

Cisco 7902	Cisco 7905	Cisco 7906
Cisco 7910	Cisco 7911	Cisco 7912
Cisco 7914 Exp Module	Cisco 7940	Cisco 7941
Cisco 7960	Cisco 7961	Cisco 7970
Cisco 7971	IP Blue SoftPhone	SpectraLink WiFi

### **SIP Phones**

Cisco 7960	InnoMedia 3308 Single Line
InnoMedia 5531 Video IP Phone	GenBand SoftPhone audio
GenBand Softphone with video	GrandStream 102
LinkSys SPA-941 2 line	LinkSys SPA-941 4 line
LinkSys SPA-942 2 line	LinkSys SPA-942 4 line
LinkSys SPA-962	Polycom 601
Sipura SPA-841 2 line	Sipura SPA-841 4 line
Thomson 25631 SIP Multi-line	

### **SIP WiFi**

Hitachi Cable WIP-5000A WiFi	Linksys 300 SIP WiFi Phone
Linksys 330 SIP WiFi Phone	LinkSys WRT54GP2 WiFi IAD
Nokia E61 – Dual Mode Phone	iMATE JazJam – Dual Mode Phone
UTStarcom F-1000 WiFi Phone	

### **MGCP Phones**

Cisco 7940	Cisco 7960
Polycom SoundPoint IP400	Polycom SoundPoint IP500
SwissVoice / Vontel IP 10S	

### **PBX**

Asterisk - Open Source Telephony Platform V1.4  
Avaya - Definity  
Cisco - Call Manager 4.2

19 Cisco - Call Manager 5.1

Cisco - Call Manager Express  
Mitel - 3300  
Nortel - CS1000  
Nortel - Norstar 032 KSU  
NEC - DS2000  
NEC - DSX  
Siemens - HiCom

**Gateways**

Alcatel 5020 (SIP)	AudioCodes Mediant 2000* as T8200 (SIP)
Cisco 26XX (SIP)	Cisco 28XX (SIP)
Cisco AS5350 (SIP)	Cisco AS5400 (SIP)
Cisco AS5850 (SIP)	Cisco BTS (SIP)
Huawei C&C08 (SIP)	New Rock Trunk Gateway (SIP)
Nortel CS 2000 (SIP)	Siemens HiQ8000 (SIP)
Taqua 7000 (SIP)	Telica Plexus 9000/Compact Switch (SIP)
VegaStream 200 (SIP)	Veraz ControlSwitch (SIP)

**VoIP Peering**

Cirpack	DCI	Level3 / Sonus (Backend)
MCI / Verizon	PointOne	StarVox
Verizon		

**Other**

CosmoCom	Contact Center Solutions
Telephony@Work	Contact Center Solutions
Innovax	Contact Center Solution
Interactive Intelligence	Contact Center Solution
TeleData Technology	SIP Voice mail
UTStarCom	SIP Voice Mail
IP Unity	SIP Voice Mail
Intrado	VoIP Positioning Center
HBF Group	VoIP Positioning Center
Dash-911	VoIP Positioning Center
Kancharla [Tone]IP	VoIP Positioning Center
Brooktrout/Cantata	SIP Conferencing
Conveda	SIP Conferencing
Audiocodes IPMedia 2000	SIP Conferencing
tekVizion Labs	Certified Testing Partner
SS8 Networks Xcipio	CALEA Hardware Solution
Intelleg "Capture"	Hosted CALEA Service

Interstar Fax Server	Hosted Fax Server
TelRex / CallRex	Enterprise Call Recording
RedBox Recorders	Enterprise/Hosted Call Recording
Oak VoIP Call Recorder	Hosted Call Recording using Virtual Logger
Callis Call Recorder	Hosted Call Recording using Virtual Logger
CTI Group SmartRecord	Hosted Call Recording
Stratus "Entice"	H.323/SIP GW
Taqua 7000 Packet Cable GW	SIP/NCS Gateway
Tekelec TEKCORE CSCF	IMS CSCF
Sonus ISX CSCF	IMS CSCF
Covergin WCS	IMS FMC
Bridgeport NomadicOne	IMS FMC
HP OpenCall HSS	IMS HSS

## Signaling Controller

### Support of Legacy and Next Generation Protocols

V5, CAS, PRI, TCAP, AIN0.2, INAP CS1, ISUP, GR303  
 MEGACO, SIP, SIP-T, SIP-I, BICC, MGCP, H.323,  
 Numerous CLASS 4 and CLASS 5 features

### Regulatory Interoperability

CALEA J-STD-025A and Punch list, E911, LNP

## Converged Media Gateway

### Logical Interface Support

PRI, CAS, MF/DTMF, SS7 ISUP, GR303, V5.2

### Built-In Functionality (Regulatory, MRF)

Integrated Announcement Server, Three/Six-way Conference  
 Bridging, Tone Detection/Generation, Lawful Intercept,  
 Emergency Service, Hybrid Echo Cancellation, Adaptive Jitter  
 Buffer, Silence Suppression, Comfort Noise

### IP Routing & MPLS Enabling

Multi-path OSPF for Layer 3+ routing & control

21 MPLS RSVP-TE support for QoS

## VoIP Peering & Per Session FW/NAT for Security

### **2G/3G Wireless, UMTS, & UMA**

3GPP Mc Interface

AMR (UMTS: all rates; UMA, VoIP: 12.2 kbps), WB AMR  
(planned), EVRC, SMV (planned), CTM/TTY

3G UMTS: TFO (UMTS/PCM), TFO IPE, TrFO, CSD, 3G Iu over  
ATM (Q.2630) & Nb over IP

VoMPLS header compression over IP

HEC with VQE (ALC, time-based ANR) (planned)

### **Wireline Codecs**

G.711, G.729, G.723, T.38

## Communication Applications Complex

There are three applications that can be used to set up and configure the system.

They are:

- System Administration Application
- Device Configurator
- Communicate Pro Console

### System Administration

The System Administration Application resides on the Database Agents and is an easy-to-use, browser-based, graphical user interface (GUI) application that enables set up, configure, and maintain the system features that are delivered to each customer site. The System Administration Application can be run from Internet Explorer or Netscape Communicator web browsers and provides setup wizards, statistics, and other administrative tools.

### Device Configurator

All configuration information required for the private network of the Session Border Controller to function properly in the system is entered through the Device Configurator.

### Communicate Pro Console

The Communicate Pro Messaging Server is accessed through a web-based interface for configuring the system on install, managing users and performing maintenance, and handling database and messaging backup and restore functions. The Server System Administration Application provides automated tools for creating and deleting user voice mail mailboxes without having to access the messaging system.

### Accessing the System Administration

The System Administration application is a Java-based application that is initially downloaded from the system web server through a link on web page accessed using the URL of the web server. Once the System Administration

application has been installed on an administrator's PC, it can be accessed from either the Java Web Start application or from an icon on the Windows desktop.

The Maintenance/Status section Comp. (Component) Status tab displays a table that monitors and troubleshoots the performance of any system component. For example, if someone reports a phone to be out-of-service, this tab to quickly determine the real-time status of the phone and the status of any components that may be associated with the phone. Or, for instance, you can monitor the current number of 911 calls on the system or even the total number of 911 calls made.

The following components can be monitored:

- 911 Component
- AMIS Component
- Announcement/Play Component
- CALEA Component
- Checking Status
- Conference Board Component
- Conference Bridge Component
- Conference Bridge Group Component
- Detailed Information
- DTMF Proxy Component
- Fanout Component
- Gateway CPE Component
- Gateway ISDN Component
- Gateway NIC Component
- Hunt Group Component
- IP Link Component
- Line Component
- Log Flat File Component
- Log Oracle Component
- Maintenance View
- Media Server Component
- Meet-Me Conference:Setup Component
- MS Conference Bridge Component
- Multi Call Park:Park Component
- NetDoctor Component
- Number Plan Component
- Outgoing Dial Component
- PBX Trunk Component
- Phone Features Component
- Phone:Hook Component
- Queue Component
- Route Point Component
- Server:Server Component
- Session Border Controller Component
- SIP Gateway Component

SIP Phone:Hook Component  
SIP Registrar/Device Component  
SIP Router/Server Component  
SIP VM Account/Play Component  
SIP VM Server Component  
SMPP Component  
SNMP Component  
Static Call Component  
Streamer Component  
Time Redirect Component  
Trunk Group Component  
VMServer:VMServer Component  
Voice Mail:Play Component

## DSS System

The EMS is required to provision, manage and operate a single system, but a single EMS server can manage up to 31 Gateway chassis.

The EMS architecture is comprised of:

- Two EMS Server and two CLI Server processes running on a pair of redundant Sun Netra Servers,
- A set of EMS Graphical User Interface (GUI) client applications running on Windows-based PCs, and
- (optionally) A set of Command Line Interface (CLI) clients running on remote (networked) hardware platforms. These clients are customer provided.

The two EMS Server processes run as an active/standby pair with the standby server maintained in a “warm” state through database updates and transaction checkpoints sent from the active server. The active EMS Server process uses SNMP-based messaging to communicate with the Converged Media Gateway nodes. FTP is used to exchange file-based data between the EMS Server processes and the Gateway nodes. Event and alarm information is exchanged using inter-process communications (IPC) messaging to insure immediate notification of faults. All OA&M data is stored in a database with synchronized copies on the two Sun Servers.

The EMS Server provides a notification service which handles the dispatching of events and alarms to registered GUI and CLI client applications.

The EMS architecture supports four external interfaces:

- EMS GUI Client - provides complete operational management of the Gateway product
- CLI Client/Server - provides complete configuration management functionality

- FTP - provides file transfer services for performance measurement data
- SNMP - provides northbound traps

The primary EMS interface is a Java-based GUI client that executes on a Windows-based PC. Multiple clients can be running on a single PC, limited only by memory and processing resources, with each client communicating with the same, or different Gateway nodes. The EMS GUI application uses socket-based TCP to communicate with the EMS Server process. Up to 100 GUI clients can simultaneously connect with a single EMS Server. All Converged Media Gateway OA&M functions are accessible through the GUI client. If a fail-over between the EMS Server processes occurs (due to the failure of the active server), the GUI clients will automatically reconnect with the new active server, making the switch transparent to the end user (with the minor exception of possibly having to re-execute an operation that is in progress at the time of the failure).

The CLI Server provides an interface through which all provisioning capabilities are accessible. This interface requires that a client application be implemented by the end customer to access this interface. This customer-provided client can be the basis of a custom machine-to-machine or man-to-machine interface (also implemented by the customer). The CLI Clients are simple Merit-based applications that act as a client to the EMS Server. The fail-over scenarios of the main EMS Server processes are transparent to CLI Servers.

Performance Measurement (PM) data is collected from the Converged Media Gateway nodes on a regular basis by the EMS Servers. PM data is written to files which can then be uploaded on a scheduled basis to a network location via FTP (both the location and schedule are provisionable). This allows a Network Management System (NMS) or traffic analysis system to receive Converged Media Gateway PM data on a routine basis without manual intervention.

The EMS Servers also provide a northbound SNMP (agent) interface for communicating with Back-Office, OSS and NMS applications. The functionality of the SNMP interface is limited to identification of the active/standby state of an EMS Server, sending of event and alarm traps and re-synch of such traps with a northbound application.