Lucent Technologies
Bell Labs Innovations

Lucent VoIP for Enterprise

Release 2.2.1

Technical Description

255-485-006R2.2.1
Issue 1
January 2006

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Notice

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

Ordering information

The ordering number for this Information Product is as stated on the front page.

To order, use one of the following numbers:

Within the United States: Tel: 1–888–LUCENT8 (1–888–582–3688); Fax: 1–888–566–9568

Within Canada: Tel: +1 317 322 6615; Fax: +1 317 322 6359

All other countries: Tel: +1 317 322 6416; Fax: +1 317 322 6699

Technical support

For initial technical assistance, please call one of the following numbers:

North America, Central and Latin America and Asia Pacific regions:

Customer Technical Assistance Management (CTAM) center: +1 630 713 0488

Europe, Middle East and African regions:

International Customer Management Center (ICMC): +353 1692 4579

Developed by Lucent Technologies.

Developed by Lucent Technologies.

Contents

Part III: Operations, Administration, Maintenance and Provisioning aspects

16 Operations, Administration, Maintenance and Provisioning

A Supported hardware

B Lucent VoIP for Enterprise offer matrix

About this information product

Purpose

This information product describes Lucent VoIP for Enterprise. Lucent VoIP for Enterprise is a powerful and flexible solution offering VoIP services to enterprises.

The information product provides:

- An overview of the solution architecture
- A description of the different network elements and features
- Basic OAM and P information

Reason for reissue

This is the first release of this information product.

Safety information

This information product contains hazard statements for your safety. Hazard statements are given at points where safety consequences to personnel, equipment, and operation may exist. Failure to follow these statements may result in serious consequences.

Required hardware and software releases

Lucent VoIP for Enterprise is based upon the following hardware and software releases:

- BroadWorks R13.0
- APX TAOS Release 11.0
- VitalNet 9.4

Related documentation

The documentation set includes:

Title	Ordering number
Lucent VoIP for Enterprise - Release Notes R2.2.1	255-485-005R2.2.1

Title	Ordering number
Lucent VoIP for Enterprise - Technical Description R2.2.1	255-485-006R2.2.1

A documentation set is also available for the Lucent Feature Server 3000.

Related training

The following related training is available:

Course title	Course number
Lucent VoIP for Enterprise - Application Overview	AG670
Lucent VoIP for Enterprise - Application Configuration	AG671
Lucent VoIP for Enterprise - Solution Overview	AG674
Lucent VoIP for Enterprise - Solution Configuration	AG675

How to comment

To comment on this information product, go to the Online Comment Form (http://www.lucent-info.com/comments/enus/) or email your comments to the Comments Hotline (comments@lucent.com).

Part I: Introduction to Lucent VoIP for Enterprise

Overview

Purpose

This part gives an overview of the solution and explains the functions of the entities that are used in the solution.

Contents

1 Lucent VoIP for Enterprise

Overview

Purpose

This chapter provides an overview of the components that form Lucent VoIP for Enterprise and the functions that are performed by the components.

Contents

Lucent VoIP for Enterprise

Introduction

Lucent VoIP for Enterprise is a powerful, cost-effective enterprise, network-based IP telephony solution that combines reliability, flexibility and scalability to deliver extraordinary levels of communications control for next generation voice for medium to large enterprises, such as:

- Consistent feature functionality to all employees regardless of location or Customer Premises Equipment (CPE)
- Carrier-grade service and quality assurance
- Open, standards-based voice networking

It comprises all of the elements needed to provide business voice/PBX functionality and QoS transport using an IP infrastructure and standards-based protocols (SIP and MGCP).

The solution provides for the communications needs of forward-looking organizations. It combines the practicality, functionality and affordability of the traditional PBX with the power, flexibility and adaptability of IP-based networks and servers.

Scalable architecture

The solution has a scalable architecture that can support virtually unlimited numbers of end-users by linking multiple systems, deployed in a centralized or geographically dispersed architecture.

Many different configurations

The solution can be deployed in many different configurations, supporting all ranges of the business spectrum. Due to its software-based architecture, the system can be configured to support a small business while growing seamlessly to support large multi-site organizations.

Capabilities

The solution comprises a number of components that provide complete support for:

- Standards-based and PBX-equivalent telephony capabilities
- Enhanced web portal interfaces to provide end user productivity gains
- Standards-based system management capabilities
- Support for standards-based third-party endpoints, firewalls and gateways

Cost effectiveness

The architecture of the solution reduces costs. Both for maintaining and using the solution.

Contributing to a cost effective solution are:

- Wide range of supported products.
  This allows the enterprise to incorporate existing products or chose the most cost-efficient product for their needs.
- Wide range of configurations.
  This allows the enterprise to chose the most cost-efficient for their needs.
- Flexibility in scaling and migration.
  This allows the enterprise to scale the solution according to business needs without losing previous equipment investment. It allows migration paths from traditional network to a next generation network based on IP when and where the enterprise needs it.
- Productivity gains for employees by offering the wide range of services.
- Centralized maintenance, mainly in the data network. This minimizes the need for maintenance and administration on multiple locations and different network types, thus lowering maintenance and operation costs.
- Carrier grade reliability minimizing down time and maintenance costs.

□

Configurations

Flexible configuration

The flexible configuration of Lucent VoIP for Enterprise allows both single-location and multi-location enterprise configurations.

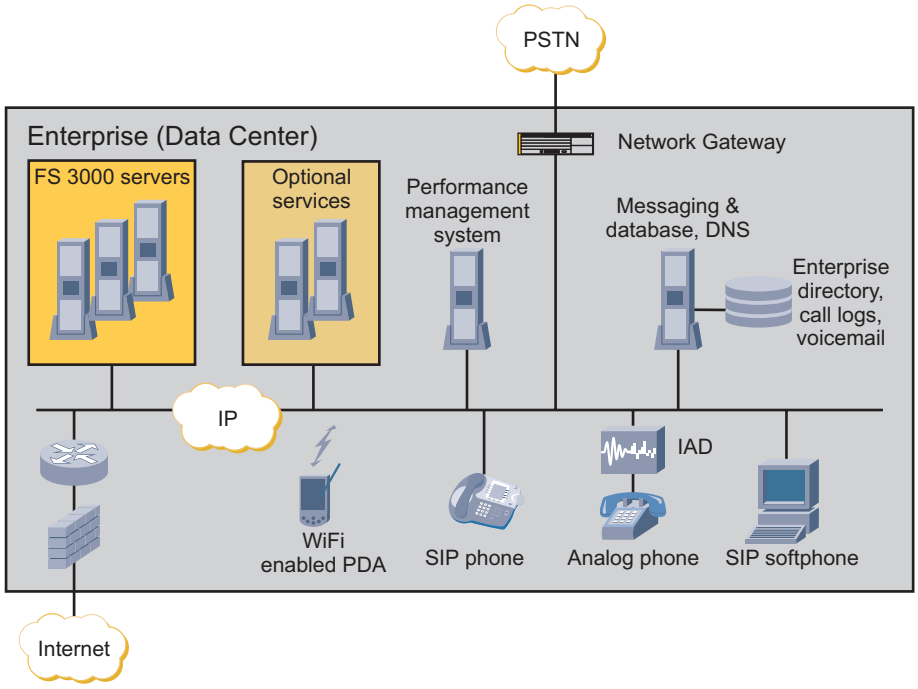
Components

The solution consists of the following main system components:

- Core Lucent Feature Server 3000 servers (containing the application, network, media server)
- Network gateways and/or Foreign Exchange Offices (FXOs)
- Session Border Controller (S/BC)
- Converged Network Applicances
- Firewalls
- Endpoints
- Performance management system
- Additional components, such as:
  - Video conferencing
  - User interfaces.
  - Element Manager Server
  - External Web server
  - Voice conferencing server
  - Call Detail Record server
  - Servers for support of messaging services

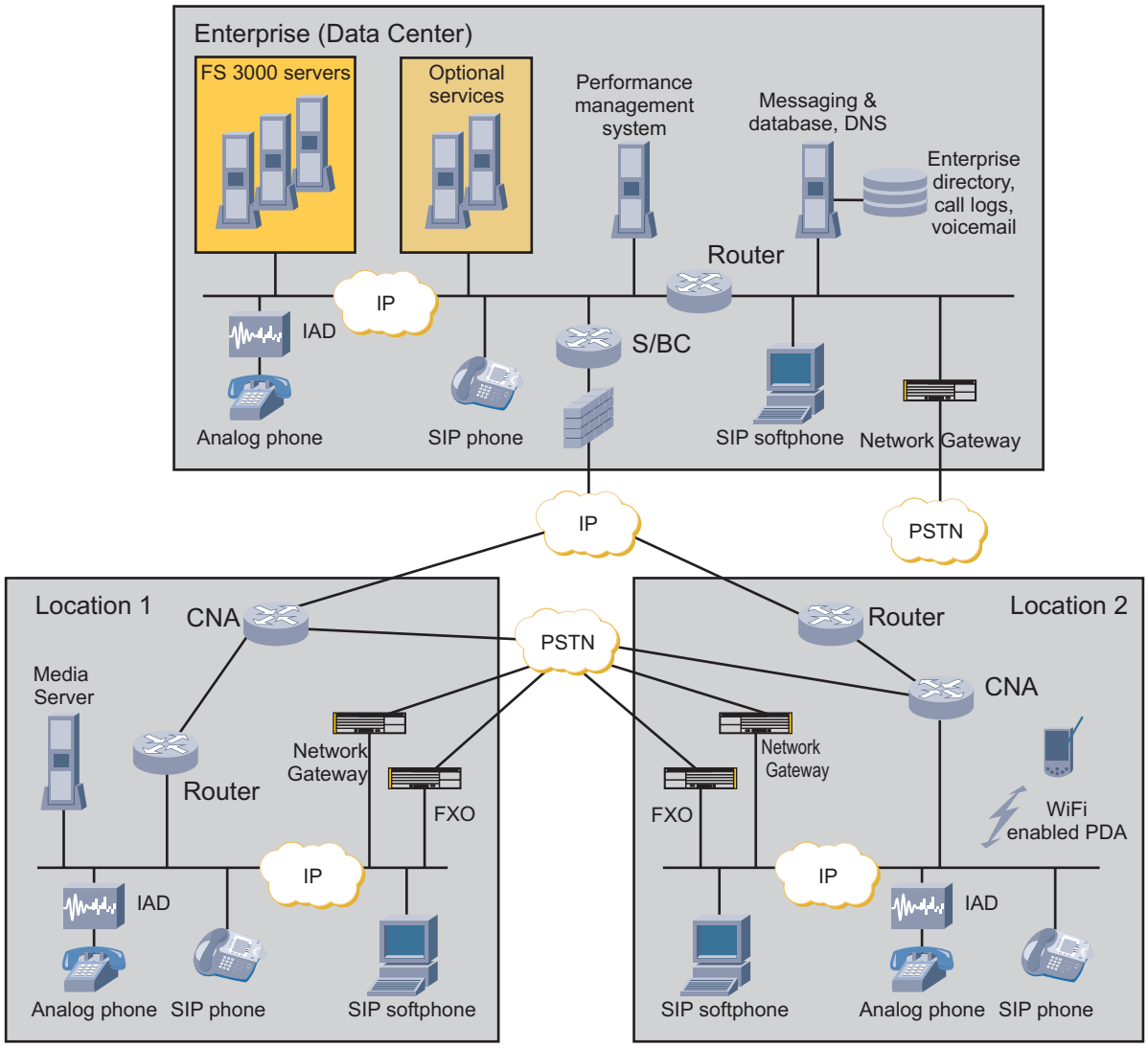
Single-location enterprise

The figure shows the single-location enterprise reference architecture:



Multi-location enterprise

The figure shows the multi-location enterprise reference architecture:



Location 1 is a remote location with a limited bandwidth connection to the data center. Location 2 is a remote location with sufficient bandwidth for voice services.

Limited bandwidth remote location

If a remote location with limited bandwidth concerns exists, then one of the media servers from the FS 3000 server pool may be located at this remote location. This reduces bandwidth requirements for 3-way calls, announcements, and voice mail access via the telephone interface.

Sufficient bandwidth remote location

If there is sufficient bandwidth available at the remote location no additional media server is required at the remote location.

Existing equipment

Individual enterprises will, however, exhibit their own architectures. To make use of the solutions, it may be necessary to perform an evaluation to see whether the data network is voice ready, or whether the existing routers and firewalls are sufficient for this new architecture.

Lucent Worldwide Services provide services that can be used to perform such validation and to recommend architectures to ensure a high quality, highly reliable VoIP service.

□

Lucent VoIP for Enterprise application services

Overview

The functionality and services of Lucent VoIP for Enterprise are provided by the Lucent Feature Server 3000 (FS 3000).

The Lucent FS 3000 provides the PBX capabilities of the solution. The servers deliver applications including:

- Hosted PBX
- IP Centrex
- Voice VPN
- Enhanced network
- Business trunking

Through any combination of these applications, enterprises can reduce telecommunication overhead costs and simplify network operations.

Reference

Refer to the Lucent FS 3000 documentation set for detailed descriptions of:

- Lucent FS 3000 applications in *BroadWorks Applications Overview*
- Lucent FS 3000 system features in *Broadworks Feature Overview*
- Lucent FS 3000 end user features in *Broadworks Service Guide*

Hosted PBX

A hosted PBX is a network-based telephony solution that provides dial tone, personal and group calling features, and web-configurable service management equivalent to IP PBX. Characteristics are:

- Offers greater deployment flexibility without the investment, maintenance, and overhead of a traditional PBX
- Can be rolled out to specific sites, or across multiple sites to replace and/or complement existing premises-based equipment.

IP Centrex

IP Centrex offers traditional calling features (for example, call forwarding, voice mail, instant conferencing) of a typical Centrex offering, often bundled with converged access.

Voice VPN

A voice VPN offers call routing policies for web-configurable enterprise private dialing plans that route site-to-site calls over private/public IP networks.

- Private dialing plans can integrate with a PBX or key system infrastructure
- Roll-out can target specific site-to-site long distance costs or drive network level voice/data convergence.

Enhanced network

Discrete enhanced features that are centralized in the network for multi-location service integration:

- Discrete feature bundles include Unified Messaging, ACD, Auto Attendant, Failover Support, and Instant Messaging
- Can be independently deployed or deployed to complement existing systems and functionality through open interfaces.

Business trunking

Business trunking provides SIP-based network services to existing PBX, IP PBX or Key Telephone Systems (KTS).

Business trunking allows providers to offer integrated access. Customer equipment for both voice and data is connected to an Integrated Access Device (IAD) which is connected to the IP-network, using T1/E1, DSL or Ethernet. IP based services can be offered without the need for enterprises to replace existing equipment.

Business trunking allows enterprises to migrate smoothly from their existing PBX and KTS systems towards a hosted PBX solution.

Modular architecture

The Lucent FS 3000 servers in the solution have a standards-based modular architecture, using common protocols and open interfaces. Depending on the size of the enterprise and the required system functionality the number of Lucent FS 3000 servers may grow.

Lucent FS 3000 server types

The system functionality is distributed across the Lucent FS 3000 servers for optimized performance:

- The *Application server* is responsible for the execution and management of enhanced personal and group services. It also includes an integrated web server.
- The *Media server* provides a host of specialized media services typically found in multiple servers, including unified messaging, conferencing, IVR, auto attendant, and network service announcements.
- The *Network server* provides network-based services, optimized resource selection, and centralized network translations and routing. It also delivers Voice VPN applications and private network gateway routing.

Designed to operate at the enterprise data center, these servers offer the interoperability, back office capabilities, redundancy, and scalability for carrier-grade performance.

Optional servers can be added:

- Video conferencing server
- Element Manager System server
- External Web server
- Voice conferencing server
- Call Detail Record server

Messaging servers can be added to the Lucent FS 3000 to support different voice-mail applications.

□

Network gateway

Overview

The network gateway (NG) is the interface from the IP network to the PSTN. The network gateway is a carrier-class gateway that is optimized for seamless integration of dial, Voice-over-IP, fax-over-IP, virtual private network, and other IP services.

Foreign exchange office gateway

Overview

The Foreign Exchange Office (FXO) gateway provides line access to PSTN at a remote location.

The FXO can be used as an alternate backup line access to PSTN in case of failure of the network gateway or Session Border Controller. The FXO is typically installed to provide a backup to make emergency calls.

The FXO may also be used in small remote locations where a network gateway or Session Border Controller is not efficient. When only 4-8 ports for PSTN access an FXO is sufficient.

Converged network appliance

Overview

A Converged Network Appliance (CNA) is an edge device providing the demarcation point for real-time, interactive IP services. A CNA is a solution for connecting enterprise PCs and IP Phones to a private or public IP network. A CNA replaces multiple standalone systems by integrating voice-over-IP (VoIP), network security, traffic management and voice call monitoring into a low-cost, easily managed device.

Remote location configurations

A CNA is typically installed at a remote enterprise location.

Two remote location configurations are possible:

- The CNA has a E1/T1 interface, works as WAN router and provides the remote survivability function.
  The device can also work as an Application Layer Gateway (ALG), providing NAT and PAT services, and performing traffic shaping over the WAN, as well as a host of other services.
- The CNA does not have a E1/T1 interface, and is designed to reside behind the existing WAN router. The CNA provides the same set of services as a CNA that works as a WAN router.

Remote survivability

A CNA provides the remote survivability service. If at any time the CNA detects a failure of the WAN, it takes over as a SIP proxy for all new call originations. The CNA knows which devices are registered as it monitors the registration messages being sent between endpoint devices and the application servers.

Emergency services

The CNA also provides services to enable emergency services such as E911 calls.

□

Session border controller

Overview

A Session Border Controller (S/BC) is an edge device that provides a demarcation point for real-time, interactive IP services. An S/BC is the solution for connecting enterprise PCs and IP phones to a private or public IP network. The S/BC replaces multiple standalone systems by integrating VoIP, network security, traffic management and voice call quality monitoring into one device.

Supported applications

An S/BC typically support applications and functions like:

- Hosted IP telephony solutions for consumer, SOHO, and enterprises
- Service provider VoIP Network protection
- Network peering between service provider networks
- Managed enterprise IP telephony

Locations

Depending on the application and functions the S/BC supports, the S/BC is installed at an enterprise datacenter or a service provider datacenter.

□

Firewall

Overview

The firewall delivers service level-assured security, VPN, and QoS services. The firewall can be deployed in environments that range from large data centers to small offices, providing ample flexibility, availability, and scalability to meet needs across diverse applications:

- Advanced security services
- Site-to-site and remote access VPN services
- Bandwidth management services
- Secure data center web/application hosting
- Mobile data services

□

End points

Overview

The end points used in Lucent VoIP for Enterprise are the telephone devices or CPEs that an end user leverages for personal telephony needs.

These telephone devices can be:

- SIP IP phones or softphones
- Video SIP IP phones or softphones
- Wireless SIP IP phones in combination with a wireless access point
- Analog telephones in combination with a Line Gateway or Integrated Access Device (IAD)

Endpoints may support SIP, MGCP or both.

Integrated access device

The Integrated Access Device (IAD) converts the standard analog telephone signal to an internet protocol and visa versa. This allows the deployment of standard analog telephones.

□

Optional solution services

Overview

This topic describes optional services and products that are available in the solution. The services require additional hardware and software deployment in the enterprise network.

Attendant console

An (IP) attendant console is used by front-of-house receptionists, or telephone attendants, who screen inbound calls for enterprises. Attendant consoles can offer services in a personalized way and can enhance efficiency and business processes.

Video conferencing

Video conferencing services offer the end-users video conferencing capabilities.

Advanced user interface

Advanced user interfaces provide users (end users or adminstrators) with access to multiple services and applications via one easy to use interface.

Advanced user interfaces offer:

- Access to services
- Self-management of services
- Management of users and services by administrators.

Instant Messaging

Instant Messaging services allows users to exchange text or video messages in real time.

Instant Messaging typically also allow users to:

- Share and view documents
- Define presence settngs to allow privacy
- Create friend or buddy lists and view presence information of these buddy to allow efficient communication
- Start SIP based telephone conversations.

Voice mail messaging

Voice mail messaging provides the capability for calling parties to leave messages and for users to retrieve and manage voice mail messages. The solution offers different voice mail applications for enterprises that want to migrate to a new platform.

□

Performance management system

Overview

To measure the performance of the network an optional performance management system can be added to the solution.

Purpose of performance management

The purpose of the Performance Management activity is to collect, store and distribute performance data from the Network. This data will be used to verify the grade and quality of service, availability, physical and logical configuration of the network and locate potential problems as early as possible.

Key performance indicators

The performance measurement data provides the basis for the calculation of the Key Performance Indicators (KPIs) displayed to operators on the performance management system. This data and the resulting KPIs are used to verify the load carried by the network, and the grade of service offered to improve network quality for network planning.

□

Part II: Product overview

Overview

Purpose

This part gives an overview of the products used in the solution and provides detailed information on the recommended hardware.

Contents

2 Lucent VoIP for Enterprise product overview

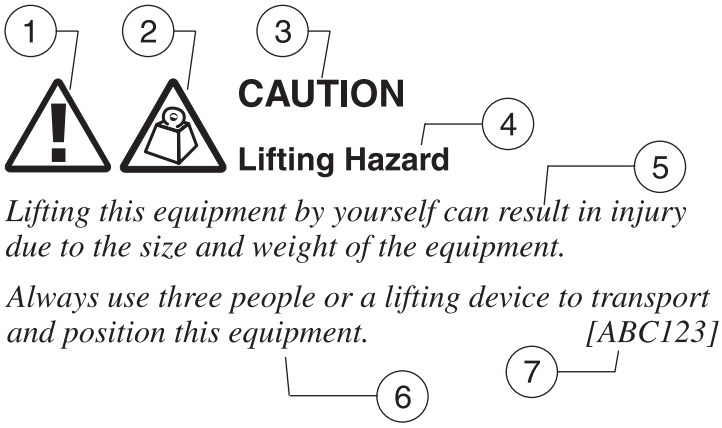
Structure of hazard statements

Overview

Hazard statements describe the safety risks relevant while performing tasks on Lucent Technologies products during deployment and/or use. Failure to avoid the hazards may have serious consequences.

General structure

Hazard statements include the following structural elements:



Item	Structure element	Purpose
1	Personal injury symbol	Indicates the potential for personal injury (optional)
2	Hazard type symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard

Item	Structure element	Purpose
4	Hazard type	Describes the source of the risk of damage or injury
5	Damage statement	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the hazard statement (optional)

Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an imminently hazardous situation (high risk) which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation (medium risk) which, if not avoided, could result in death or serious injury.
CAUTION	*When used with the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in personal injury. *When used without the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in property damage, such as service interruption or damage to equipment or other materials.

Lucent VoIP for Enterprise component suppliers

Introduction

Lucent VoIP for Enterprise supports components from various suppliers. Only the Lucent Feature Server 3000 (FS 3000) and the CNA (Edgewater EdgeMarc) have fixed suppliers. Depending on enterprise preferences, different hardware suppliers can be selected for the other network elements (see supported hardware tables in Appendix A).

Lucent FS 3000 servers

The Lucent FS 3000 servers are servers with application software (*BroadWorks*®) provided by *BroadSoft*®. The Lucent FS 3000 provide the main functions of the solution.

Network gateway

The recommended network gateways for the solution is the Lucent *APX*® 1000 Universal Gateway.

Supported network gateways

The gateway functionality is required for solution to function properly. The Lucent *APX*® 1000 Universal Gateway is an optional component of the offering. Depending on enterprise preferences and deployment sizing, other gateways can be deployed instead.

Refer to "Supported rack mountable trunk gateways" (p. A-9) for a list of supported gateways.

Session Border Controller

The recommended SBC for solution is the Juniper Networks VoiceFlow range of products.

Converged Network Appliance

The CNA for solution is the Edgewater EdgeMarc range of products. The CNA provides the remote survivability and emergency services capabilities in combination with the Lucent Feature Server 3000.

FXOs

For small enterprise locations or as back-up PSTN connection an FXO can be used.

Refer to "Supported FXOs" (p. A-13) for supported FXOs.

SIP phones

Refer to "Supported IP phones" (p. A-2) for supported SIP endpoints.

If a requested CPE is not listed, check whether this CPE complies to the SIP interoperability specifications specified in the *SIP Access Interface Interworking Guide*.

IADs and line gateways

Refer to "Supported integrated access devices and line gateways" (p. A-5) for the supported IADs and line gateways.

Firewalls

The recommended firewall for the solution is the Lucent VPN Firewall *Brick*®.

Alternate firewalls

The firewall functionality is required for solution to function properly. The recommended Lucent VPN Firewall *Brick*® is an optional component of the offering. As an alternate other SIP-aware firewalls can be deployed on customer request.

Network monitoring systems

The recommended network monitoring systems are:

- Lucent VitalNet

□

3 Lucent Feature Server 3000

Overview

Purpose

This chapter provides an overview of the Lucent Feature Server 3000 network communications platform and its elements.

Contents

Lucent Feature Server 3000 overview

BroadSoft

The Lucent Feature Server 3000 is based on server platforms in combination with the *BroadWorks*® software application provided by *BroadSoft*®. The servers, in combination with BroadWorks perform different roles in the architecture.

The Lucent Feature Server 3000 servers are:

- Application server
- Network server
- Media server
- Conferencing server (optional)
- Web server
- Call Detail Server (optional)
- Element Manager Server (optional).

The Lucent Feature Server 3000 also supports messaging services.

The Lucent Feature Server 3000 combines the enhanced features of an IP PBX, the reliability of Centrex, with the flexibility of open, standards-based networking. Designed to operate at the core of the network, the Lucent Feature Server 3000 delivers unmatched interoperability, back office capabilities, redundancy, and scalability for carrier-grade performance.

Reference

Refer to the Lucent FS 3000 documentation set for detailed descriptions of:

- Lucent FS 3000 applications in *BroadWorks Applications Overview*
- Lucent FS 3000 system features in *Broadworks Feature Overview*
- Lucent FS 3000 end user features in *Broadworks Service Guide*

Management interface

The CommPilot System Provider web portal provides access to all of the system monitoring, maintenance, and configuration functions of Lucent Feature Server 3000 via a web interface. System Providers can also access the provisioning and monitoring functions via a command line interface.

For details on the System Provider Web Portal see the *BroadWorks Application Server System Provider Web Interface Administration Guide*.

Accounting management

The accounting records are hosted on the Lucent Feature Server 3000. The accounting information is generated in the form of call events. The call events are atomic pieces of information generated during the calls upon call origination, termination, service invocation, and other events that may have an impact on the billing of a call. Additionally, a long duration call accounting option provides the ability to generate a separate accounting event for calls of a specified duration (for example, one day).

The Feature Server 3000 Call Detail Record (CDR) contains information about each call, including: called party, calling party, call origination time, billable call duration, call type, dialed digits (prior to any translations), and IP address of access device.

On a periodic basis, an external mediation system retrieves the accounting files from Feature Server 3000 and correlates the call events to aggregate them in call detail record that can be processed by the service provider's downstream billing system.

For more information on accounting management see the *BroadWorks Application Server System Provider Web Interface Administration Guide* and the *CDR Interface Specification*.

□

Lucent Feature Server 3000 services

Purpose

This topic provides a brief overview of services that are offered by the Lucent Feature Server 3000.

This is not intended to give a full description of all available services.

Reference

For detailed information on services, features and applications refer to:

- *Broadworks Service Guide*
- *Broadworks Feature Overview*
- *BroadWorks Applications Overview*

Types of services

The Lucent Feature Server 3000 offers the following services:

- User services
  These services are assigned to specific users on the system and are used, managed, and configured by the user.
- Group services
  These services apply to groups of users.
  Group services can be categorized as:
  - Virtual services
    These services are assigned to a group and make use of a virtual user that performs some action upon receiving a call.
  - Multi-user services
    These services are assigned to a group and enable functionality that involves selected users in the group.
  - Group services
    These services provide functionality that applies to all users in a group.
- Messaging services
  These services provide users with the ability to send, receive, and manage services.
- Service provider and enterprise services
  These services provide capabilities specific to the service provider administrator and the enterprise administrator.

User services

Examples of services are:

Service	Description
Alternate Numbers (Multiple Numbers per User)	Allows a user to have up to ten alternate phone numbers in addition to the user's main phone number. Distinctive ring patterns and call waiting tone can be assigned for each alternate number.
Anonymous Call Rejection	Enables a user to reject calls from anonymous parties who have explicitly restricted their identities.
Blind Call Transfer	Enables a user to transfer a call before or after the call is answered, without consulting with the transferred to party.
Call Forwarding services Flavors include: • Call Forwarding Always • Call Forwarding Busy • Call Forwarding No-Answer • Call Forwarding Remote Access • Call Forwarding Selective	Enables a user to automatically redirect all incoming calls to another destination.
Call Trace (Customer Originated Trace)	Enables the recipient of an obscene, harassing, or threatening call to request that it be automatically traced by dialing a feature access code after the call.
Call Transfer services	Enables a user to transfer a caller to another party.
Calling Line ID services Services include: • Calling Line ID Delivery (Persistent and Per Call) • Calling Line ID Blocking (Persistent and Per Call) • Calling Line ID Restriction Override	Enables users to manage calling line IDs.
CommPilot	Enables a user to use a web-based tool for service invocation and call control.

Service	Description
Push To Talk	Allows a user to call another station, where the system requests that the destination station automatically answer.

Group services

Examples of services are:

Service	Description
Account Code	Allows the users to assign certain calls to specified accounts, for tracking purposes.
Attendant Console	Enables a user (for example, a receptionist) to monitor a configurable set of users in his/her business group.
Calling Plan	Allows the administrator to restrict the type of calls users can make and receive.
Conferencing	Allows administrators and users to create, configure, and manage multi-party conferences hosted on the BroadWorks Conference Server.
Hunt Groups	Allows incoming calls to a central phone number to be distributed among the members of that group according to a hunting policy.
Music On Hold	Allows an administrator to set up and maintain an audio or video source that can be broadcasted to held parties in various scenarios (Call Park, Call Hold, and Call Centers).

Messaging services

Examples of services are:

Service	Description
Third-Party Voice Mail Support	Facilitates the support and integration of an external voice mail platform.

Service	Description
Voice Messaging • Personal • Group • Service Provider	Provides voice messaging services to groups and persons and allows administrator to manage the services.
Voice Portal	Provides an interactive voice response (IVR) application that can be called by members of the group from any phone, to manage their services and voice mailbox, or to change their pass code.

Service provider and enterprise services

Examples of services are:

Service	Description
Business Trunking	Provides a new a “Trunk Group”, used to serve PBX-type customer premises equipment.
Call Processing Policies	Provides explicit control of certain call processing behavior.
Large Enterprise Support	Allows a customer to better model, administer, and manage large multi-site enterprises.

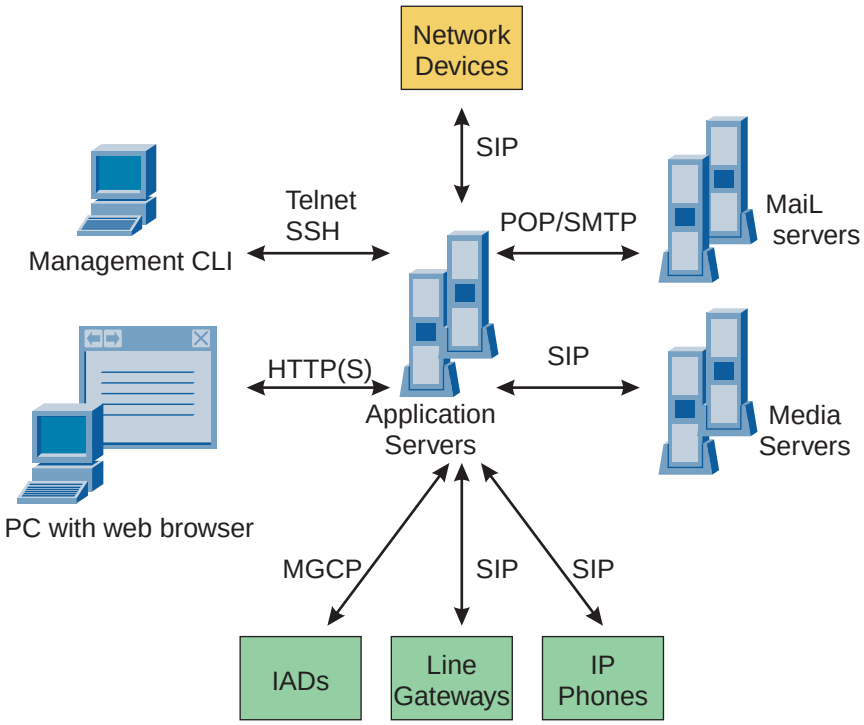
Application server

Overview

The application server's primary role is a line-side softswitch. It hosts all the endpoints, providing a full IP Centrex feature set.

Graphical overview

Application server overview:



Functions

The function of the application server is to:

- Provide features
- Administer users
- Interface with:
  - SIP and MGCP devices
  - The media server for announcements and Interactive Voice Response
  - The network server for call routing and dial plans
  - Mail servers using POP3 or IMAP4 for the delivery of voice mail messages.

Application server redundancy

The application server is deployed in a primary/secondary redundancy architecture. It contains a subscriber database that is replicated in real-time between the primary and secondary servers. In the event of failure of an application server, the end user will not experience loss of dial tone and loss of calls.

Redundancy architecture

In order to understand the documentation the reader should be familiar with the following definitions:

- *Primary application server* – One node in an application server pair is identified as the primary node. All end users have the same primary application server.
- *Active application server* – The application server currently active for a given end user (the active server is on a per user basis).
- *Rollover or Failover* – Reversion of an end user's endpoint to the alternate application server in the event of a failure condition being detected on that server.
- *Rollback* – The process of bringing back an endpoint to its primary application server.

Redundancy premises

The redundancy solution relies on three basic premises:

- Application server data replication
- End user's active node tracking
- Per endpoint rollover and rollback capability.

Data replication

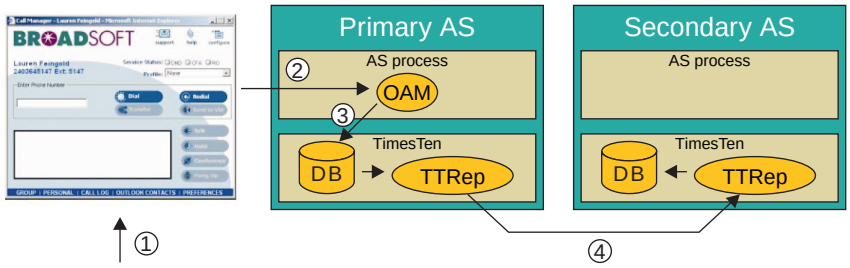
Data replication ensures that end users receive a consistent service, that is, the features available to the end user and the current calls are all maintained, no matter what server is hosting the endpoint.

Data replication is achieved in two ways:

- *TimesTen® replication* – TimesTen is a memory-based relational database. All end user data, and data that defines the nodes that are active, is stored in this database. Each server has its own TimesTen database with near real-time replication between them.
- *File-based replication* – Using RSYNC, this replication uses differential synchronization and runs about every 30 seconds. Data such as announcements, voice mail greetings, web branding and other file-based configuration is replicated using this mechanism.

Example of data replication

The figure show an example of data replication:



1. End user enabled Dialed Number Display (DND) at the call manager. The call manager is the interface program used to make phone calls by users.
2. Call manager event sent to the primary Application Server (AS).
3. The primary application server stores the DND configuration in its database.
4. The DND information is pushed to the secondary server database by TimesTen replication.

□

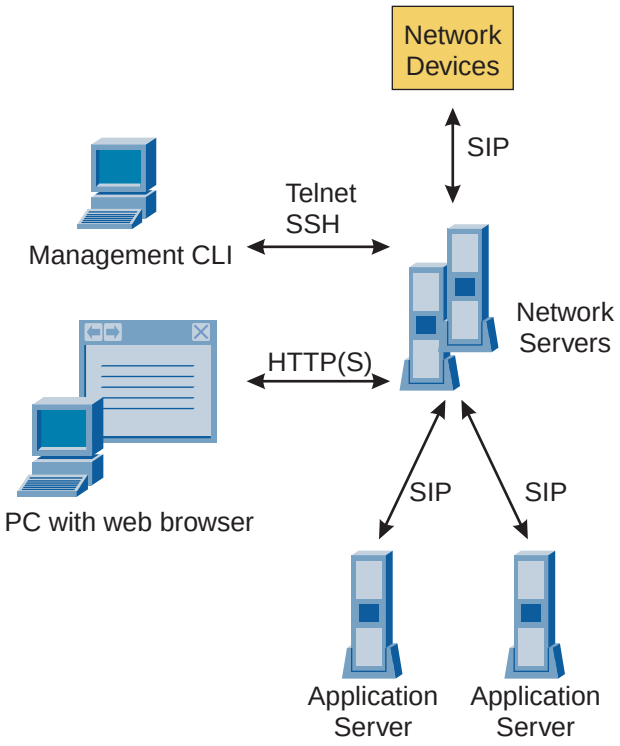
Network server

Overview

The network server provides routing functions and translations for SIP traffic.

Graphical overview

Network server overview:



Functions

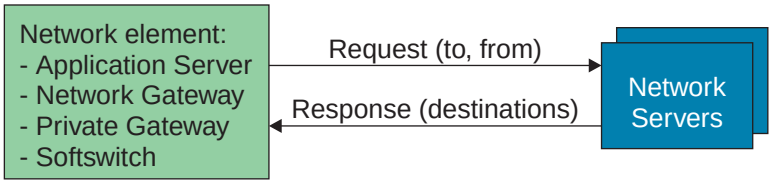
The network server functions are:

- *Translations:* network server maps the incoming INVITE's dialed digits to a call type (for example, an emergency call) and optionally performs calling area screening
- *Routing:* network server identifies a destination based on the INVITE's originator or dialed digits and call type.

SIP redirect server

The network server performs the role of the SIP redirect server (for more information on SIP refer to RFC 3261). As such, all SIP INVITE messages that are not for a user hosted on the same application server, are routed to the network server, and the

network server locates where that INVITE message should be sent. This may be an application server if the user is using an IP phone located on an application server, or a gateway if the user is located in the PSTN.



Redundancy

The network server is deployed in an N+1 configuration to achieve redundancy.

□

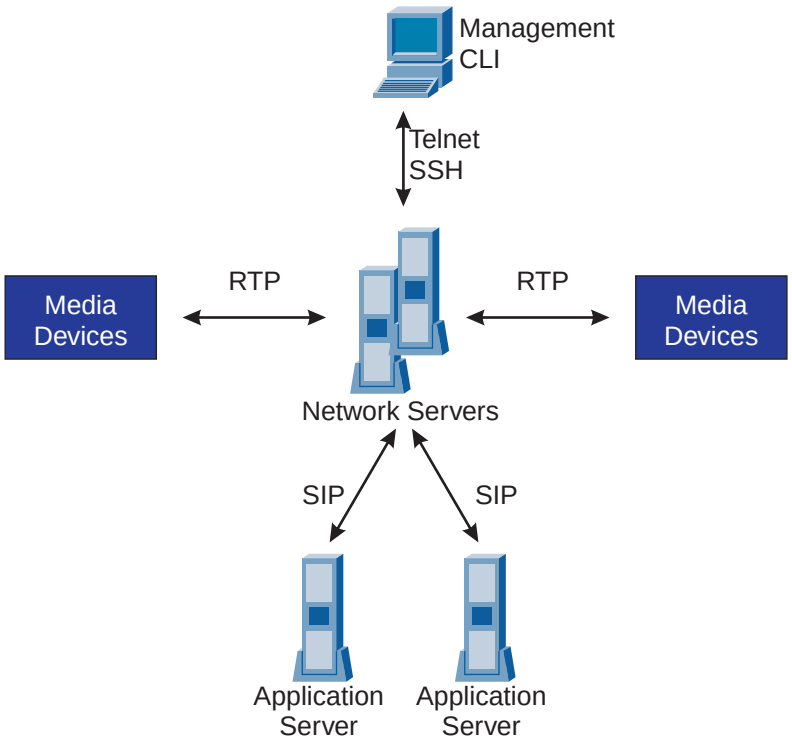
Media server

Overview

The media server is a software-based solution providing specialized media resources for media mixing and conferencing, announcement and recording playback, DTMF digit collection, and Interactive Voice Response (IVR).

Graphical overview

Media server overview:



Media server functions

The media server performs a role with the following functions:

- *Voice messaging:* Voice messages are encoded with DVI ADPCM encoding at 32 kbps and are attached to e-mails in MIME format
- *Dial-up voice message retrieval:* Playback of voice messages
- *Auto attendant:* Pre-recorded messages
- *Three-way conferencing:* Performs any transcoding required for G.711, G.726, and G.729 as well as mixing of RTP audio streams

- *Account codes and authorization codes (digit detection):* collects digits if required for use of certain features or dialing patterns (for example, international calls)
- *System announcements and tones:* plays any announcements or call progress tones.
- *Video support*: Playback and record video in .MOV file format for:
  - Video mail
  - Video on hold
  - Video queueing.

The media server supports the video codec H.263 for video-enabled phones.

Redundancy

The media server is deployed in an N+1 configuration to achieve redundancy.

□

External web server

Overview

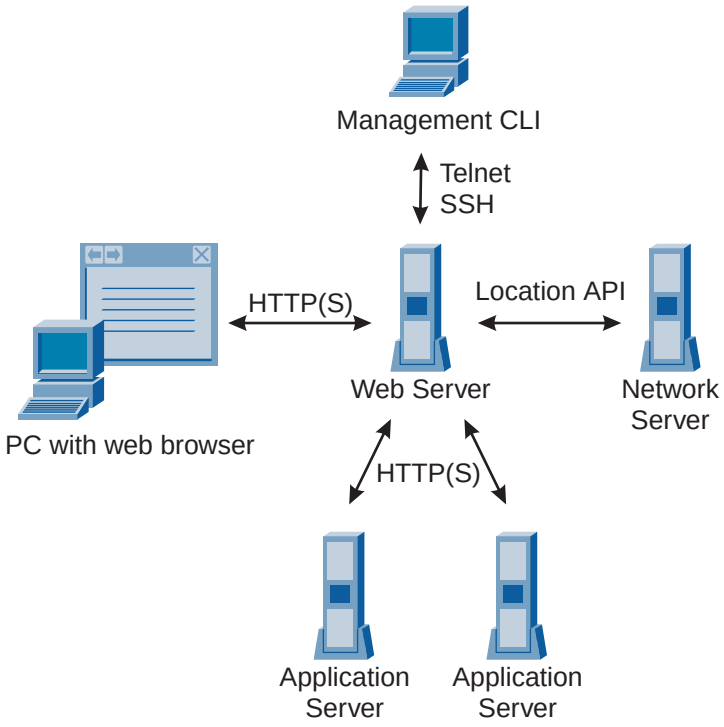
The Lucent Feature Server 3000 deploys an external web server. Using an external web server improves security and scalability, since end users and administrators are not accessing the application server directly to manage their services. The administrators access the web server, which communicates with the application server on their behalf.

The web server supports two separate interfaces:

- The CommPilot interface
- The Open Client interface

Graphical overview

Web server overview:



The web server is deployed as a farm of web servers to front multiple Application Server (AS) clusters and is usually deployed in a DMZ, whereby traffic between the web server and application server or network server goes through a firewall.

Functions

The web server:

- Manages connections to multiple ASs at the same time. The location of a given user is obtained from the network server through the NS Location API
- Offers additional security by not allowing direct access to the application servers
- Provides transparant redundancy by moving user session to the secondary AS when the first AS goes down. The user does not have to login again.
- Offloads AS web server processing providing more CPU for call processing-related operations.

CommPilot interface

The CommPilot interface supports use of the various CommPilot web portals, CommPilot call manager, and the attendant console.

Open Client interface

The Open Client Server (OCS) resides on the web server and enables a more simplified and scalable approach to support service creation by eliminating the need for third-party call clients to have their own proxy servers.

The Open Client Interface (OCI) consists of:

- A call control interface (CAP) to enable third-party applications to leverage call control functions (for example, call transfer, call hold).
- A provisioning interface (OSS) to receive allocated phone numbers, allocated access resources, and authorized services from an external provisioning system.

OCS supports multiple application servers simultaneously and a HTTP/SOAP interface.

For more information about the OSS provisioning interface, refer to:

- *Broadworks OSS Developer's Guide*
- *Broadworks Application Server Provisioning Interface Specification*
- *Network Server Provisioning Interface Specification*

□

Element Management System

Overview

The Element Management System (EMS) is an optional server that provides a single point of entry into the Feature Server 3000 for the system provider's OAM systems. System providers still have the option of using the Feature Server 3000 existing OAM interfaces directly. The EMS provides visibility to all servers for provisioning, network management, and maintenance.

Support functions

The following functionality is supported:

- Auto discovery
- Administrator and password management
- Web cut-through to network elements
- Performance management reporting
- Alarm consolidation and reporting
- Command line interface (CLI) cut-through to network elements.

□

Call Detail Server

Overview

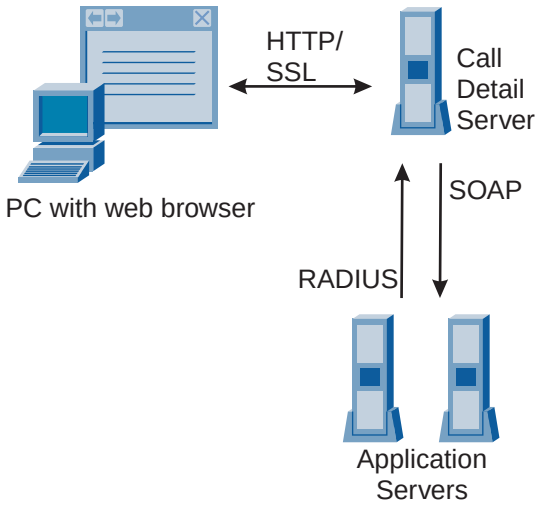
The Call Detail Server (CDS) is an optional server that is used for storing and retrieving call log information that is forwarded from Application Servers. The use of a CDS increases the amount of call log information that can be stored.

With the CDS, service providers can store more call log information per phone line than is allowed by the Application Server, and for extended periods of time.

Important! The CDS is not designed to store Call Detail Records for accounting (billing) purposes.

Call Detail Server graphical overview

CDS overview:



CDS interfaces

The Call Detail Server receives call log information from one or more Application Servers, in real time over the RADIUS Accounting Protocol. The call logs are stored in an SQL database.

SOAP requests are used to return all call logs for a given user.

Configuration data

Besides the call logs themselves, the Call Detail Server also stores configuration data. Each service provider or enterprise has a maximum count of logs per user, and a maximum number of storage days for each log. Such information is also provided over SOAP from the Application Server.

The Call Detail Server then runs a task once a day to clean up logs that are too old or exceed the maximum count.

CDS and CommPilot Personal portal

The CDS adds a webpage to the CommPilot Personal portal. The CDS webpage provides access for enterprise and residential users to the call logs of all received, missed and placed calls.

□

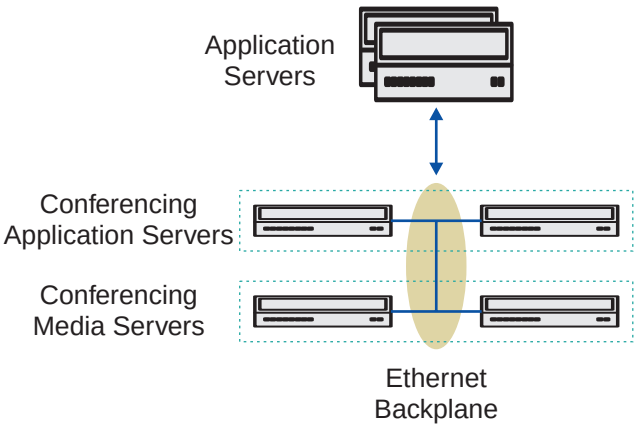
Conferencing server

Overview

The conferencing server enables the set-up, use, and monitoring of *n*-way conferences via a web interface. Both internal and external participants can use a conference bridge once it has been set-up.

Architecture

Conferencing server architecture.



Note: For small conference configuration the conference application server and conference media server may be combined onto one redundant server pair.

Redundancy

To achieve redundancy:

- The conference application servers are deployed in pairs.
- The conference media servers are deployed in an N+1 configuration (2 to 10 conference media servers are allowed).

Main features

The conferencing service includes the following features:

Feature	Examples
Audio and web conferencing	• Scheduled, recurring, reservation-less, and ad-hoc • Meet-me dial-in numbers.

Feature	Examples
Web collaboration	• Share *Microsoft® PowerPoint®*, Excel, and Word files • Secure SSL and password protection • Web browser viewable, no client required.
Moderator control	• Dial-out capability • Mute, hold, drop and add participants • DTMF and web portal interfaces.
In-call functions	• Roll call, hand raising, optional leader.
PIM integration	• Automated e-mail invitations & *Outlook®* calendar entries.
Reporting	• Web-based reporting • Department and project codes.
Recording	• Recording and playback of individual conferences.
Access code generation	• Automatic, pre-assigned, or user-defined.

Messaging services

Overview

The Lucent FS 3000 supports different configurations to support e-mail messaging. This allows the FS 3000 to operate with existing external mail applications or use the FS 3000 itself to handle messaging.

Lucent Technologies offers a basic messaging store architecture to support messaging.

FS 3000 voice mail configurations

The Lucent FS 3000 supports the following (concurrently supported) configurations:

Configuration	Description
Stand-alone	The FS 3000 provides all voice messaging services and the basic phone services. The voice mail messages are stored on a POP3 or IMAP mail server.
Network voice mail	The FS 3000 provides voice mail messaging. The useŕs phone is hosted externally. For example in the PSTN. The FS 3000 performs: • Voice mail recording • Voice mail playback • Message Waiting Indicators
External voice mail	The FS 3000 hosts the useŕs phone. An external voice mail system provides voice mail messaging. The FS 3000: • Transfers incoming calls to the users to the voice mail system • Sets and clears Message Waiting Indicators The external voice mail system performs: • Voice mail recording • Voice mail playback • Message Waiting Indicators

Reference

For more information on the FS 3000 mail configurations, refer to *Voice Messaging Solutions Guide*

Basic messaging architecture

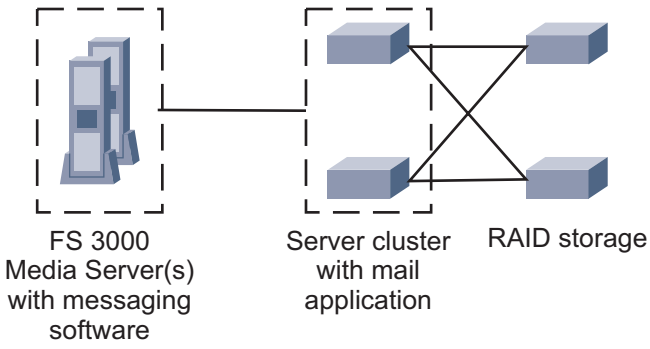
The solution offers a messaging architecture to support e-mail messaging. The messaging architecture is available in different configurations, using different types of Sun servers depending on the customer requirements and capacities.

The messaging architecture uses Sun servers and is available in the following configurations:

- Duplex messaging server configuration
- Duplex messaging server configuration with RAID external storage
- Server cluster configuration with RAID external storage

Messaging architecture example

Basic messaging architecture using server cluster configuration with RAID external storage:



Supported messaging architecture hardware

Component	Supported HW
Server in duplex configuration	Sun Fire V240
RAID storage	Sun StorEdge 3320
Server cluster	Sun Fire V210 Sun Fire V440

Messaging applications

The following messaging applications are supported and can be installed on the messaging architecture platform:

- Sun Java messaging
- Eudora Qpopper
- BayPackets Unified Communications package

Message Waiting Indication

The Lucent Feature Server 3000 can control the Message Waiting Indication (MWI) status of users with Voice Messaging who have their access lines on a PBX, a Class 5 switch, or another IP-based application server.

Terminal server

The Lucent Feature Server 3000 supports this service through an outgoing SIP NOTIFY MWI.

For legacy-based users on a PBX or Class 5 switch, a terminal server is required to convert the SIP NOTIFY MWI message to SMDI TCP MWI and SMDI RS-232 MWI messages, respectively.

□

4 *APX*® 1000 Universal Gateway

Overview

Purpose

This chapter provides an overview of the *APX*® 1000 Universal Gateway.

Contents

APX® 1000 overview

Introduction

The APX 1000 Universal Gateway is a carrier-class access gateway optimized for seamless integration of dial, Voice-over-IP, fax-over-IP, virtual private network, and other IP services. The size and density of the APX 1000 makes it ideal for both small and large Points of Presence (POPs).

Features

The APX 1000 provides the following features:

- Highest throughput and most universal ports in its class
- Universal port technology for “any service, any port, any time” versatility
- Uniform capacity for consistent application performance and density.
- SS7-based Internet Call Diversion (ICD) for dial-up IP port wholesaling
- Feature-rich True Access Operating System (TAOS)
- Lucent Voice Natural technology from Bell Labs for enhanced VoIP call quality
- Multiple IP protocol support including SIP.
- DTMF support: in-band, RFC 2833, via H.245 (H.323)
- G.168 echo cancellation
- Voice Activity Detection
- Comfort noise generation and silence suppression
- Dynamic jitter buffer

Supported codecs

The APX 1000 supports the following codecs:

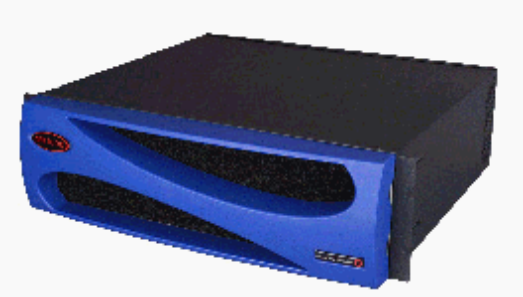
- G.711
- G.729a
- G.729a/b
- G.723.1

□

APX 1000 hardware layout

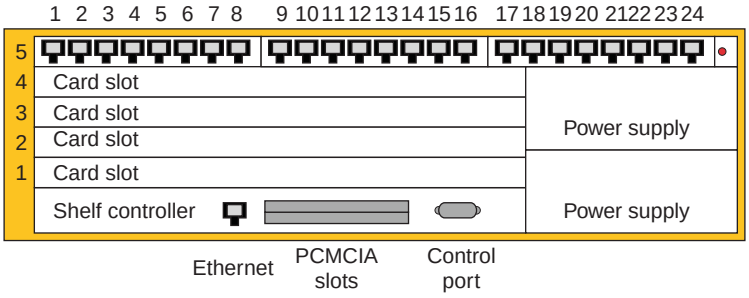
Front view

The diagram shows the front view of the APX 1000:



Rear view

The diagram shows the shelf layout of the APX 1000:



Hardware units

The shelf holds the following units:

Part	Function
Shelf controller	The shelf controller controls the operations of the entire APX 1000 unit. The controller is placed in the bottom slot in a single configuration. Functions of the shelf controller: • Out-of-band management via serial access on the RS-323 control port • System management via the UTP port. The UTP port is an auto-sensing, 10/100 BASE-T Ethernet port. • Dual Flash memory slots provide additional memory for storing code for the slot card, the shelf controller, and configuration backup.
Card slots	The card slots can be equipped as follows: • Slots 1 to 4 can be equipped with Ethernet or different types of MultiDSP cards • Slot 5 contains a 24 E1/T1 port card.
Power supply	Two hot-swappable AC or DC power supplies in redundant, load balancing configuration.

References

For more information, refer to:

- *APX1000 getting started guide 7820-0834-xxx.*

□

APX® 1000 configurations

Primary configurations

The table shows the combinations of ingress, egress, and DSP slot cards that make up the five primary configurations of the APX 1000.

Configuration	Ingress slot card(s)	Egress slot card	DSP slot cards
T3	Channelized T3 card	Ethernet-3ND card	Two 288-port MultiDSP cards One 96-port MultiDSP card Total DSPs: 672
Multi-T1 (24 ports)	24-port T1 card	Ethernet-3ND card	Two 288-port MultiDSP cards Total DSPs: 576
Multi-E1 (24 ports)	24-port E1 card	Ethernet-3ND card	Three 240-port MultiDSP cards Total DSPs: 720
Multi-E1 (16 ports)	Two 8-port E1 cards	Ethernet-3ND card	Two 240-port MultiDSP cards Total DSPs: 480
Multi-T1 (8 ports)	8-port T1 card	Ethernet-3ND card	One 240-port MultiDSP card, or one 288-port MultiDSP card Total DSPs: dependent on card selection. *Note:* 96-port MultiDSP cards are not supported with the 8-port T1 configuration.

Slot cards for primary configurations

The table shows the slot cards supporting the primary configurations of an APX 1000 unit and identifies the port speed and port capacity for each card type.

Slot card	Port speed	Port capacity	Installation location
24-port T1	1.544 Mbps	24 channelized T1 ports (576 DS0 channels).	Slot 5
24-port E1	2.048 Mbps	24 channelized E1 ports (720 DS0 channels).	Slot 5

Slot card	Port speed	Port capacity	Installation location
8-port E1 (wide)	2.048 Mbps	8 channelized E1 ports (240 DS0 channels).	Slot 5
8-port E1 (narrow)	2.048 Mbps	8 channelized E1 ports (240 DS0 channels).	Slots 1 to 4
8-port T1 (wide)	1.544 Mbps	8 channelized T1 ports (192 DS0 channels).	Slot 5
Channelized T3	44.736 Mbps	One active port (672 DS0 channels) and one bypass port.	Slot 5
Ethernet-3ND	10/100 Mbps	Four autosensing 10/100 Mbps ports (RJ-45 connectors).	Slots 1 to 4
MultiDSP (96 ports)	N/A	96 ports that can be used as voice ports, data ports, or some combination of voice and data ports	Slots 1 to 4
MultiDSP (240 ports)	N/A	240 ports that can be used as voice ports, data ports, or some combination of voice and data ports	Slots 1 to 4
MultiDSP (288 ports)	N/A	288 ports that can be used as voice ports, data ports, or some combination of voice and data ports	Slots 1 to 4

Slot cards for other configurations

The table shows the other slot cards that may be use in an APX 1000 unit for additional configurations to meet local needs:

Card	Port speed	Port capacity	Installation location
DS3-ATM2	44.736 Mbps	One active and one bypass trunk connection.	Slots 1 to 4
OC3-ATM2	155.52 Mbps	One unchannelized OC-3 port.	Slots 1 to 4

Card	Port speed	Port capacity	Installation location
SWAN2	V.35 (V.36) • 2.048 Mbps in the U.S. • 64 kbps in Europe X.21 • 2.048 Mbps	One of the following, depending on cable and configuration: • Four V.35 DTE ports • Four V.35 DCE ports • Four X.21 DTE ports.	Slots 1 to 4
HDLC2	N/A	186 HDLC channels.	Slots 1 to 4
APX Ethernet	10/100 Mbps	Two auto-sensing 10/100 Mbps ports (RJ-45 connectors).	Slots 1 to 4

References

For detailed slot card descriptions, see Appendix B of the *APX 1000 Getting Started Guide*, "Slot Card Specifications."

□

5 AudioCodes Mediant VoIP Media Gateway

Overview

Purpose

This chapter describes the AudioCodes Mediant VoIP Media Gateway products.

Contents

AudioCodes Mediant VoIP Media Gateway overview

Introduction

The Mediant VoIP gateways enables voice, fax, and data traffic to be sent over the same IP network. The Mediant VoIP gateways provides excellent voice quality and optimized packet voice streaming over IP networks.

The gateways can also route calls over the network using SIP signaling protocol, enabling the deployment of ″Voice over Packet″ solutions in environments where access is enabled to PSTN subscribers by using a trunking media gateway. This provides the ability to transmit voice and telephony signals between a packet network and a TDM network. Routing of the calls from the PSTN to a SIP service node (e.g., Call Center) is performed by the internal routing feature or by a SIP Proxy.

Mediant VoIP gateway product family

There is a family of Mediant VoIP gateway products to supports different deployments. Models include:

- Mediant 1000, for enterprises or small scale carrier locations. Combines:
  - Digital modules to connect to PSTN or PBX
  - Analog FXS
  - Analog FXO
- Mediant 2000, to connect to PSTN for large and medium-sized VoIP applications.

Mediant 2000 physical description

The Mediant 2000 VoIP gateway comprises the following hardware components:

- A 19-inch 1U high rack mount chassis
- A single compactPCI™ TP-1610 board
- A single TP-1610 Rear Transition Module (RTM)
- A single available cPCI slot for an optional third-party CPU board.
- Dual redundant 10/100 Base-TX Ethernet ports via RJ-45 connectors
- Power supply options:
  - Single universal 90-260 V AC
  - Dual redundant AC
  - Single -48 V DC

Mediant 1000 physical description

The Mediant 1000 VoIP gateway comprises the following hardware components:

- A 19-inch 1U high rack mount chassis
- Up to 4 digital modules for E1/T1 or J1 spans
- Up to 6 analog modules for FXo or FXS
- Dual redundant 10/100 Base-TX Ethernet ports via RJ-45 connectors
- RS-232 port for debugging
- Single universal 90-260 V AC power supply

□

6 Edgewater EdgeMarc converged network appliance

Overview

Purpose

This chapter provides an overview of the Edgewater EdgeMarc converged network appliance.

Contents

Edgewater EdgeMarc overview

Introduction

The Edgewater EdgeMarc Series reduce the cost and complexity of securing and maintaining mission-critical voice and video services for enterprise customers.

Features

Summary of the Edgewater EdgeMarc features:

VoIP	• SIP • MGCP • H.323 • SCCP • Survivability - Softswitch redundancy and local station-to-station call switching in the event of WAN link or softswitch failure (SIP).
Security	• VoIP Application Layer Gateway • Stateful Packet Inspection Firewall • NAT/PAT for topology hiding • Hardened OS.
Traffic Management	• Prioritizaton of VoIP traffic • Traffic shaping • Diffserv marking • Policing • Call Admission Control.
Monitoring	• Passive call quality monitoring • Mean Opinion Score prediction • Raw statistics - jitter, latency, packet loss, etc.
Management	• Web-based GUI • SNMP, SSH, Telnet • Local and external syslog reporting • Ping, traceroute, TCPdump utilities • Automated phone provisioning (MGCP for Polycom IP phones).

E911 support

The Edgewater devices support emergency calls in cooperation with the Lucent Feature Server 3000 and Intrado.

Supported hardware

The table shows the supported EdgeMarc CNAs:

Model	WAN	LAN	Ports	Features
EdgeMarc 4200 Series	1 × 10/100 Ethernet	4 × 10/100 Ethernet	1 × RS-232	• Small to medium enterprise • Supports 10 to 50 WAN calls • Standalone chassis.
EdgeMarc 4300 Series	1 × 10/100 Ethernet T1 CSU/DSU	4 × 10/100 Ethernet	1 × RS-232	• Small to medium enterprise • Supports 15 to 30 WAN calls
EdgeMarc 5300T & 5300T2	T1 CSU/DSU	1 × 10/100/1000 Ethernet	Aux Port: 1 × 10/100/1000 Ethernet Serial Port: 1 × RS-232	• Small to medium enterprise • Supports 10 to 50 WAN calls • Standalone chassis • FXO, FXS, LAN switch.
EdgeMarc 5300 Series	1 × 10/100/1000 Ethernet	1 × 10/100/1000 Ethernet	Aux Port: 1 × 10/100/1000 Ethernet Serial Port: 1 × RS-232	• Medium to large Enterprise • Up to 500 WAN calls • 1U rackmount • Slot options: T1/Dual T1.
EdgeMarc 6400 Series	1 × 10/100/1000 Ethernet	1 × 10/100/1000 Ethernet	Aux Port: 1 × 10/100/1000 Ethernet Serial Port: 1 × RS-232	• Large Enterprise • Up to 1000 WAN calls • 1U rackmount • Slot options: T1/Dual T1.

Remote survivability

Overview

In the solution, multiple remote locations are supported. In order to provide survivability at the remote location, an integrated solution with the Converged Network Appliance (CNA) from Edgewater Networks is supported

The Converged Network Appliance supports:

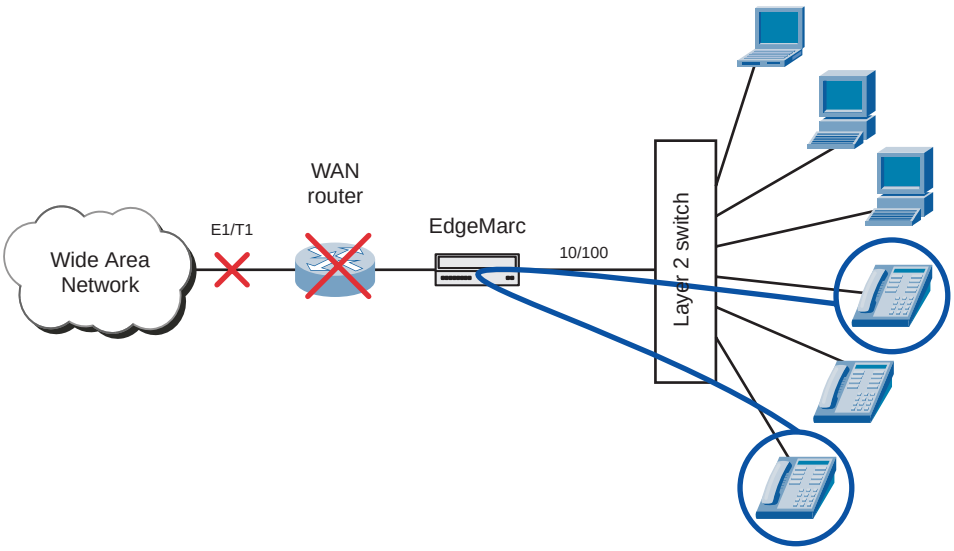
- Remote survivability
- Emergency call handling

Edgewater EdgeMarc

The Edgewater EdgeMarc series of products, installed at the edge of the remote locations LAN, monitors connectivity of the location over the WAN to the Lucent Feature Server 3000 application servers. If at any time the CNA detects failure of the WAN, it takes over as a SIP proxy for all new call originations. The CNA knows which devices are registered as it monitors the registration messages being sent between endpoint devices and the application servers.

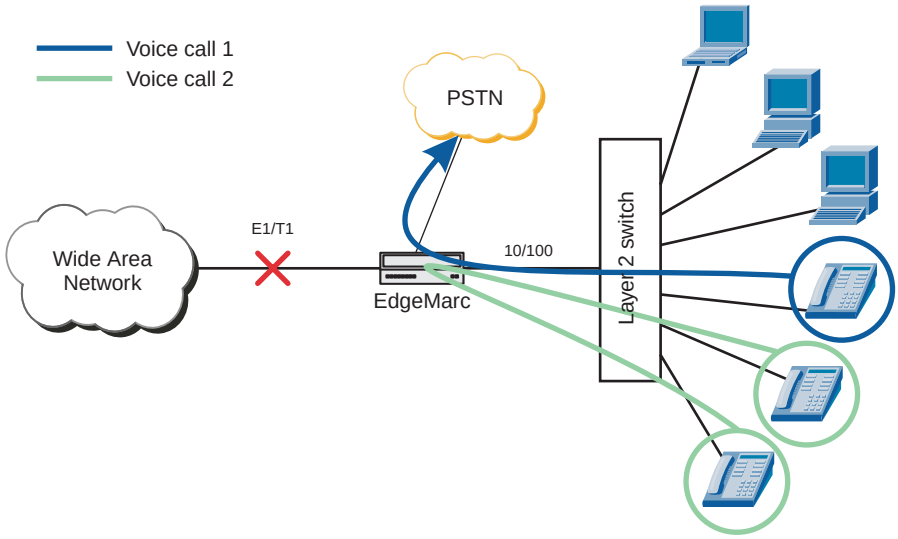
Remote survivability

The EdgeMarc series of products provide service in the event of failure of any WAN component.



Remote survivability with PSTN routing

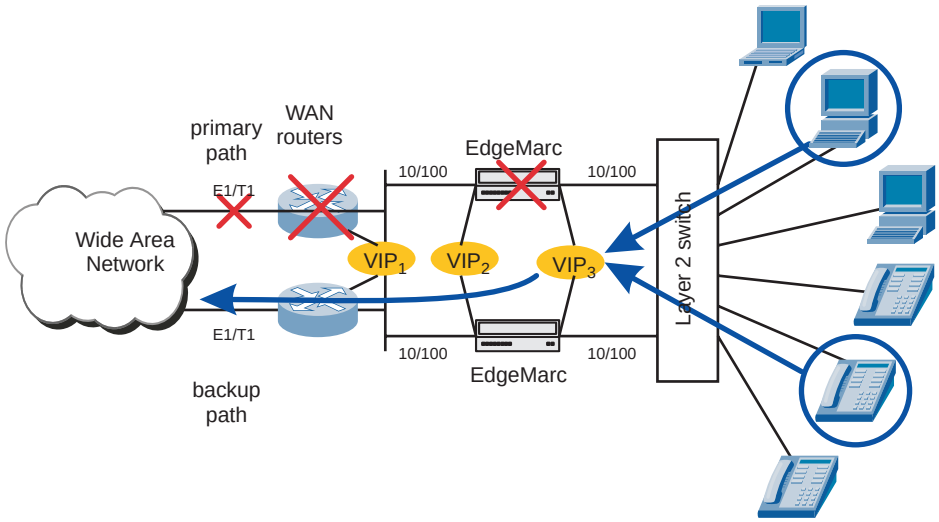
The EdgeMarc will also allow routing of calls to the PSTN in the event of WAN failure (only valid for EdgeMarc products with PSTN interface, see product table).



Session border controller redundancy

The EdgeMarc series may also be deployed in a redundant configuration using Virtual Router Redundancy Protocol (VRRP) for added reliability in the event of an EdgeMarc failure. Two EdgeMarcs are placed in parallel between the LAN and the WAN, using Ethernet networking on each side. One device is designated the master, the other is the backup. Attached LAN devices, as well as the far-end WAN devices, are unaware that

two EdgeMarcs are installed, the two appliances appear as a single device, using a single, constant IP address called a Virtual IP Address (VIP).



Emergency calls

Purpose

This topic describes how emergency calls are handled in the solution.

Emergency calls handling involves the following network elements:

- Edgewater CNA
- Lucent Feature Server 3000
- Intrado Positioning Server
- E911 tandem switch and Public Safety Answering Point (PSAP)

Intrado, the E911 switch, and PSAP are not part of the solution.

Emergency call handling problems in a VoIP network

Emergency call handling is an important issue in VoIP network. VoIP networks can potentially create problems for emergency call handling. Traditionally, emergency call handling relies on the Calling Line Identifier (CLID) of a subscriber. In traditional wireline networks, this is a reliable method to locate a subscriber.

VoIP subscribers are often mobile and their CLID is not coupled to their physical location. So in VoIP networks, relying on the CLID can resulted in emergency calls being sent to PSAPs in other cities.

Emergency call handling in Lucent VoIP for Enterprise

In Lucent VoIP for Enterprise, the EdgeWater CNA device and the Lucent Feature Server 3000 handle emergency calls.

The EdgeWater CNA device ensures the proper location of a subscriber becomes available and once that is available the FS 3000 can use that information to properly handle an emergency call.

Registration requirements for emergency call handling

In the solution the following stages are performed to ensure emergency calls can be properly handled:

1 The EdgeWater CNA device challenges mobile VoIP users to enter their location information.

Users are required to provide this information to get access to VoIP services.

The location information includes ANI information

2 Once the information is provided by the end user, the registration is permitted with Lucent FS 3000.

3 The Lucent FS 3000 passes the ANI information to the Intrado Positioning Server.

4 The ALI database updates the selective router database on the 911 tandem switch (typically daily).

Emergency call handling

The following stages are performed when a subscriber makes an emergency call:

1 The Lucent FS 3000 passes the emergency call to the Positioning Server.

2 The Positioning Server analyzes the originator directory number and provides the Lucent FS 3000 with the Emergency Services Routing Number (ESRN) and Emergency Services Query Key (ESQK)

The Positioning Server also passes on the location information from the last registration to the ALI.

3 The Lucent FS 3000 translates the ESRN and routes to a softswitch or a gateway that interconnects the call with a PSTN Tandem switch.

4 Based on the ESQK, the tandem switch routes the call to the PSAP.

5 The PSAP receives the emergency call with the ESQK as CLID.

The PSAP uses the ESQK as index in the ALI database. The ALI database returns the real ANI and location information for the user and the PSAP dispatches emergency services.

□

EdgeView element management system

EdgeView EMS overview

The Edgewater's EdgeMarc and EdgeProtect Series products are managed through the EdgeView element management system. Edgeview enables service providers and enterprise customers to easily monitor and scale their VoIP service offerings from a central management location.

Edgeview EMS

The Edgeview EMS is delivered in an appliance form factor on a 1U chassis, like the EdgeMarc 5300. The EdgeView appliance can be mounted in a 19 inch rack.

EdgeView EMS features

The EdgeView element management system features include:

- Authenticated access to browser-based GUI launched from any workstation, PC or management console.
- Image management and group upgrades for multiple Edgewater nodes
- Backup and restore the configuration for multiple Edgewater nodes
- Active call count on a node by node basis
- Launch a console management session with individual Edgewater nodes
- Extensive trend analysis and statistics reporting for items such as uptime, utilization
- Monitoring of 3rd party devices using SNMP
- Node inventory and tracking information
- Multiple user accounts with different access level privileges.

□

7 Juniper VoiceFlow session border controller

Overview

Purpose

This chapter provides an overview of the Juniper VoiceFlow session border controller product. A hardware layout of the Juniper VoiceFlow 3000 is shown. The hardware of the other Juniper VoiceFlow series is similar.

Contents

Juniper VoiceFlow session border controller

Introduction

The Juniper VoiceFlow is a session border controller that addresses multiple border issues that can occur in VoIP networks. All the issues are addresses using one platform.

Product range

The Juniper VoiceFlow series consists of:

- Juniper VoiceFlow 1000
- Juniper VoiceFlow 3000
- Juniper VoiceFlow 4000

Features

Summary of the Juniper VoiceFlow features

Security	• VoIP NAT and firewall traversal • VoIP firewall (DoS, intrusion prevention, Call admission control) • Topology hiding.
Service Assurance	• QoS packet marking • SLA and QoS reporting • Bandwidth policing and admission control • CDR collection • Remote VoIP endpoint management.
Regulatory Compliance	• Lawful Interception / CALEA • E-911.
Interworking	• H.323 – SIP Protocol Translation • H.323 and SIP versions

Juniper VF 3000

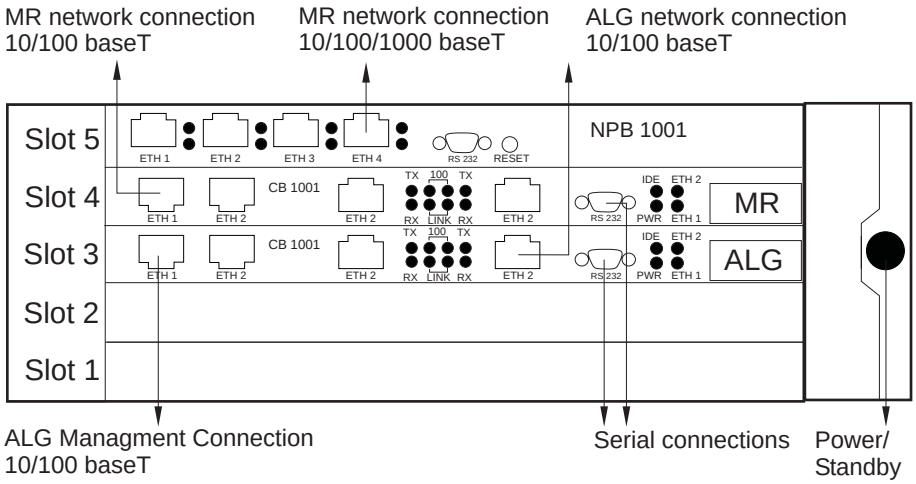
Overview

The Juniper VF 3000 is available as:

- VF 3031 option with two CB 1001 controller boards and one NPB 1001 processing board (10/100/1000 base T copper interfaces (RJ-45)
- VF 3032 option with two CB 1001 controller boards and one NPB 1002 processing board (GigE optical interfaces (LC multi mode)

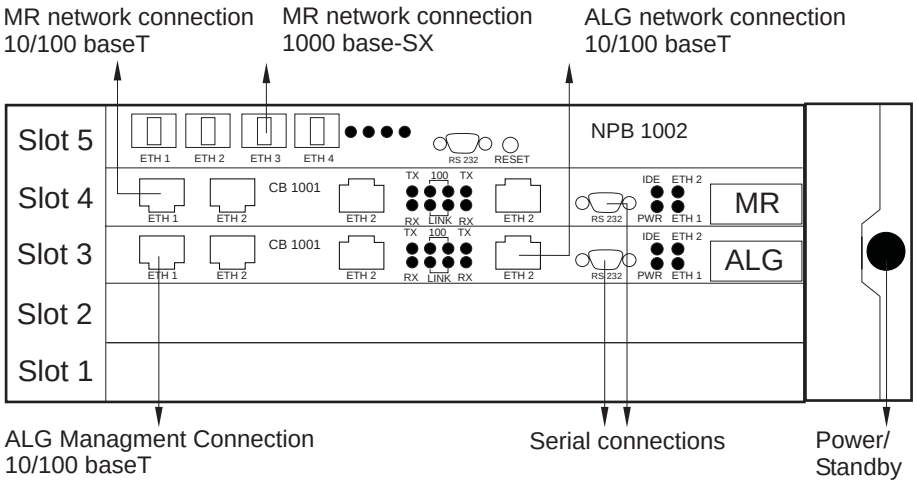
Front view VF 3031

Front view with MR network connection 10/100/1000 baseT (copper).



Front view VF 3032

Front view with MR network connection 1000 base SX (optical).

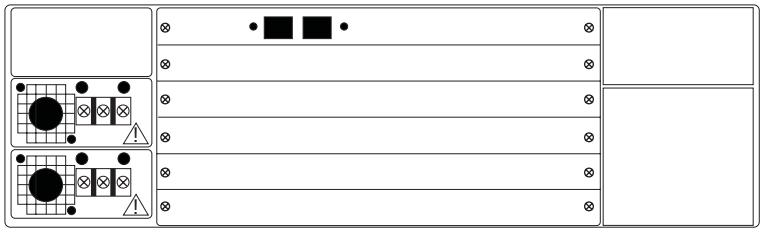


Hardware items VF 3000

The unit holds the following items:

VF 3031	VF 3032	Function
2x Controller board (CB-1001)	2x Controller board (CB-1001)	This board can be configured to work as the Application Level Gateway (ALG) or as Media Relay (MR).
1x Network Processing Board NPB-1001 (Copper)	1x Network Processing Board NPB-1002 (Optical)	This board is specially designed to accommodate high throughput of media. It is controlled by a controller board configured as an MR.

Rear view



References

For more information, refer to:

- *VoiceFlow series v/OS Release 5.3.1. Network NAT Traversal Installation & User manual*

□

8 End user equipment and features

Overview

Purpose

This chapter provides an overview of the endpoints supported by Lucent VoIP for Enterprise.

Contents

End user equipment

Overview

Lucent VoIP for Enterprise works with any commercially available Customer Premise Equipment (CPE) that supports the SIP protocol. However, with the SIP protocol being relatively new, certain features require messages within the SIP protocol that may not be supported by all CPE.

IP phone capabilities

All certified SIP IP phones should support at least the following capabilities:

- Speaker phone
- Call waiting
- Visual message waiting indicator
- Caller ID
- Mute

Analog telephones

To support “standard” analog telephones a line gateway or IAD is needed.

Wireless IP phones

The solution supports WIFI IP phones in combination with any WIFI access point.

Video phones

The solution supports video hard phone, or video softclient.

Reference

See Appendix A, “Supported hardware” for supported SIP endpoints, line gateways, and IADs.

□

CommPilot™ personal portal

Purpose

The *CommPilot*™ personal web portal provides individual users with the ability to configure and manage a host of traditional and advanced telephony services. Each user is empowered with the control and flexibility to easily configure these services to meet their unique needs.

Customized web portal

Users can customize their services to follow them anywhere, whether at work, at home or on the road.

After logging into the personal web portal through the user id and password, users can activate, deactivate, and modify the parameters of his/her own services, provisioned by the system administrator.

Example

The Call Notify service enables users to indicate which incoming calls they want to be notified of, as well as during which hours of the week. They can also choose to have their notifications sent to their mobile phone and/or email address.

CommPilot Call Manager

The CommPilot call manager provides users with a web-based alternative for managing their incoming and outgoing calling and offers a variety of common functions (e.g. Click-to-dial, hold, transfer, three-way calling, etc.)

A visual display shows the status and details of each active call, so users no longer have to wonder which line is on hold, or whether a party was dropped. One-click dialing is performed using a variety of handy phone lists: Personal, Group, Missed, Received, and Dialed.

In addition, a tool is provided for users to search their personal Microsoft Outlook contacts by name or company for quick retrieval of phone numbers and v-cards.

The complete set of system features and how to configure them is described in the *BroadWorks Service Guide*

Web branding

Each Service Provider can design its own unique web branding to create a custom look (or “skin”) for its respective CommPilot pages (e.g. Personal, Group, etc). Five different skins, or “themes”, are provided to alter the appearance of the web portals. Each Service Provider can also customize headers, screen titles, and the left navigation menu.

For details on branding, refer to the *BroadWorks Web Branding Guide.*

□

CommPilot™ group portal

Purpose

The CommPilot Group web portal empowers companies to self-configure and manage their telephony services with instant results. Each group service is set up and configured by the group administrator through intuitive web screens. The group web portal also enables companies to perform administrative functions, such as setting up users and provisioning their personal telephony services and devices.

Example

Calling plans can be set up and modified for each member of the business group without having to call the service provider or wait for the requested changes to take effect. The group administrator simply checks and unchecks the various call types to activate and deactivate them for a particular user.

Reference

For more details on the group web portal refer to the *Application Server Group Web Interface Guide.*

Conference services

The group administrator can create and manage conference bridges through the CommPilot group web portal. When creating a bridge, the group administrator assigns it a name, a phone number, a maximum number of ports, and one or more moderators (users). Each moderator has access to the Bridge page to start new conferences.

Moderators have access to a bridge management portal that is integrated into the CommPilot Personal web portal. The portal allows for creating and managing bridges before the conference as well as moderating a live conference by adding, removing, muting, holding, and retrieving participants.

The moderator has access to enhanced functions during the conference:

- Hand raising
- Drop, mute and put individual call legs on hold
- Record conference calls to play back later
- Document sharing (Excel, Word, and PowerPoint documents).

□

CommPilot™ Enterprise portal

Purpose

The CommPilot Enterprise web portal provides an optional layer of administration above the group layer to facilitate the management of large enterprises spanning multiple groups and sites. This enterprise layer is parallel to the service provider layer. Thus, system administrators have the option to create service providers and/or enterprises, each of which is administered separately.

Example

Enterprise administrators can use this administrative layer to manage selected services across their business groups and sites. For example, a Voice VPN private dialing plan can be configured to enable users to call one another using location codes and extensions instead of full phone numbers.

□

BroadWorks Communicator

Introduction

The BroadWorks Communicator is an audio and video SIP softphone for Windows 2000 and XP that is tightly integrated with the Lucent Feature Server 3000 platform. The Communicator has access to BroadWorks' many advanced VoIP features such as video services, complete call control, and messaging/voicemail integration.

Characteristics

The BroadWorks Communicator is a feature-rich desktop application that allows residential users and businesses utilize the client as a primary or secondary phone device their IP communications services. As an integrated device with the BroadWorks platform, service providers are able to auto provision the client, provide automatic updates, and version management seamlessly through the BroadWorks application server.

Key benefit of integration for users is the central storage contacts, eliminating the need to duplicate contact lists. The BroadWorks Communicator allows for the separation the audio and video stream for redirection of audio to a headset and video to the desktop. This separation provides maximum flexibility and options for end-users.

The BroadWorks Communicator is available in English, Spanish, and Simplified Chinese, in addition to having multilanguage support through the BroadWorks platform.

BroadWorks Communicator options

The following BroadWorks Communicator options are available:

- BroadWorks Communicator
  Offering audio only calling, notification, messaging, and contact features.
- BroadWorks Communicator Multimedia.
  Offering audio and video calling features, allowing point-to-point video calling, audio conferencing for up to 6 lines, and ability to utilize the BroadWorks portfolio of video services.

Video services

The BroadWorks Communicator – Multimedia offers the following group and individual services using the video services that are offered by the Lucent Feature Server 3000 application platform:

- Individual Services:
  - Video Messaging
  - Video Add On
  - Video Custom Ringback

  Group Services:
  - Video Auto Attendant
  - Video On Hold
  - Video Call Center
  - Group Video Custom Ringback

Features

Features include:

- Fully SIP compliant Audio Video Soft Phone (New RFC 3261 compliant stack)
- Co-branded SoftClient for Enterprise
- QoS Support including TSL for SIP Messaging
- Supports SIP Auto Provisioning
- Audio and Video Stream Separation Support
- Redirection of Audio Call to Handset and Video to Desktop
- Centralized contacts management and Microsoft Outlook contact integration
- Full automatic update and version management
- Skinning and co-branding
- Standard PC hardware support (soundcards, USB headset)
- Message waiting indicator

Telephony features

Telephony features include:

- Audio Codec Selection (G.711, a law & u law, G.726, G.729a)
  Video Codec Selection (H.263, H.264)
- Call Forwarding
- Dial, redial and hang up
- Caller ID [SIP ID]
- Line Hold

- Line Transfer
- Multi Party Conferencing

Reference

For full feature lists and other additional information, refer to *BroadWorks Communicator Datasheet*

□

BroadWorks Assistant - Enterprise

Overview

BroadWorks Assistant - Enterprise is a telephony toolbar and call management tool that provides an easy to use tool for your daily telecommunication needs. BroadWorks Assistant - Enterprise allows a user make and receive calls, use directories and to use and configure services.

BroadWorks Assistant - Enterprise is formerly known as Carbon Twelve miPA Corporate. You may find documentation or references still referring to the old name.

BroadWorks Assistant - Enterprise functionality

Functionality offered by BroadWorks Assistant - Enterprise includes:

- Initiate calls from web pages, directories, vCards or Outlook contact lists.
- Receive calls
- Configure and use services such as:
  - Call forwarding (always, busy and no answer)
  - Do not disturb (call forward to voicemail)
  - Simultaneous ringing
  - Use of an alternative phone number to receive calls
- Manages Group and personal directories
- View call history.

Customization

The interface of the BroadWorks Assistant - Enterprise toolbar can easily be changed in size, color, and layout. This allows enterprises and service providers to give BroadWorks Assistant - Enterprise a look and feel that is consistent with their brand and allows for marketing.

Localization

For users in non-English speaking markets, the BroadWorks Assistant - Enterprise can easily be localized to support other languages.

□

BroadWorks Receptionist

Description

BroadWorks Receptionist is an IP Telephony attendant console for use by front-of-house receptionists, or telephone attendants, who screen inbound calls for enterprises. It realizes the promise of next-generation networks by enhancing business processes and delivering rich services in a personalized way.

BroadWorks Receptionist is formerly known as Carbon Twelve miRECEPTION. You may find documentation or references still referring to the old name.

Supported functions

Functions that are supported by the attendant console include:

- Call control functions (for example dial, accept, end calls, call hold)
- Call Park (park a call at an extension for manual and timer based retrieval)
- Transfer Control (distribute call to contacts using blind and/or announced transfer methods)
- Call history and statistics
- Customization and skinning of the interface
- 3-way call conferencing
- Multiple Messaging Techniques (SMS, E-mail and Instant Messaging).

For a full list of functions, refer to the *miRECEPTION Administrator Guide.*

User interface

The BroadWorks Receptionist attendant console is accessed by the attendant via a web interface.

Lucent Feature Server 3000 interoperation

The BroadWorks Receptionist attendant console interoperates with the Feature Server 3000 to make full use of the services provided by the Feature Server 3000.

The BroadWorks Receptionist client communicates with the Open Client Server of the Feature Server 3000.

□

Features and feature packages

Overview

Different feature packages are available for enterprises. Packages contains services that are available for individual end users or groups.

Reference

For information about available features:

- Refer to *Broadworks Service Guide*
- Contact your local Lucent Technologies sales representative.

Personal services

Personal services are available to individual end users. It allows end users to provision assigned features for themselves, eliminating the need to contact administrators for provisioning and reducing the time for implementation.

Group services

Group services are services on group level administrator. It allows the group administrator to manage users of the group and to provision group level capabilities.

□

Emergency zones

Overview

The Emergency Zone feature allows a service provider to configure a home zone or location for a group, and deny SIP registrations or call originations or emergency call originations based on the home zone. The home zone is a list that contains IP addresses or IP address ranges.

Reject SIP Registrations and Outgoing Calls Outside Home Zone

The feature can be configured to deny SIP registrations and call originations from outside of the home zone. For example, if this configuration was set for a group, and a user in the group tries to use their SIP phone or device from outside of the home zone, the device would not be able to register or originate calls. On a registration attempt by the SIP phone or device, the system responds with a 403 Forbidden, and triggers a system alarm. On a call origination attempt, the user receives a treatment.

Permit or Deny SIP Emergency Calls from Outside Home Zone

A more granular control is also provided by this feature. It is used to deny emergency calls from outside the home zone. Hence, this configuration allows SIP users to make calls from outside of the home zone, but it denies emergency calls, hence preventing invalid locations being provided to emergency response teams based on the user's calling line ID. If an emergency call is denied, then the user receives a treatment.

Determine In-Zone or Out-of-Zone Requests

The via header(s) in the SIP request messages for registrations and invites is used to build a list of IP addresses. If any of these IP addresses are contained in the home zone list, then the request is considered to be from within the home zone.

Reference

For more information on the emergency zone feature refer to the *Broadworks Service Guide*.

□

Lucent Communication Manager user client introduction

Effective communication

Lucent Communication Manager provides a single ″screen″ or ″portal″ for subscribers to access their communications applications whether using a wireline or wireless device.

The purpose of the Lucent CM is to integrate, simplify, and unify the presentation of features and session control to the end user, regardless of the underlying infrastructure of application servers and regardless of the endpoint in use.

Lucent Communication Manager client on a desktop

Example of the Lucent Communication Manager client main interface on a desktop computer:

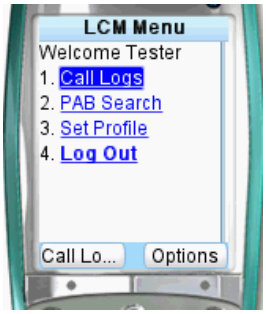
Desktop main functions

Through the Lucent Communication Manager client you can:

- Manage voice, data, or video communication sessions
- Manage and invoke services:
  - Instant Messaging
  - E-mail
  - Video mail.
- Manage user profiles
- Manage contacts in a personal address book
- View presence and availability of contacts
- View call history.

Lucent Communication Manager client on a mobile device

Example of the Lucent Communication Manager client main interface on a mobile device:



Mobile client functions

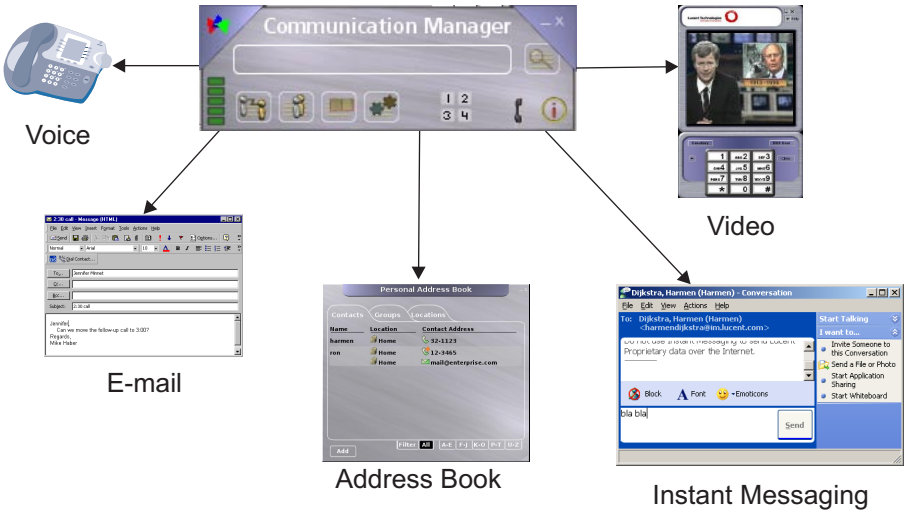
Through the Lucent Communication Manager mobile client you can:

- Search your personal address book
- Establish a voice call from PAB search results or call log
- View call logs
- Set a user profile and forward incoming calls
- Log out.

Access services

The Lucent Communication Manager user client provides you with a single interface that gives easy access to a wide range of services. Services are accessed directly from the Lucent CM user client or by launching external applications from the Lucent CM user client.

Access to a wide range of services:



Skinning

To suit your exact needs and preferences, nearly every aspect of the Lucent Communication Manager user client is “skinnable”. You can change the appearance of the user client, such as buttons or colors, until it matches your wishes.

9 Lucent VPN firewall

Overview

Purpose

This chapter provides an overview of the Lucent VPN firewall.

Contents

Lucent VPN firewall

Overview

The Lucent VPN Firewall portfolio delivers service level-assured security, VPN, and QoS services in environments ranging from the largest data center to the smallest office, providing ample flexibility, availability, and scalability to meet exacting needs across diverse applications:

- Advanced security services
- Site-to-site and remote access VPN services
- Bandwidth management services
- Secure data center web/application hosting
- Mobile data services.

Components

The Lucent VPN Firewall includes:

- VPN Firewall*Bricks*®. These are integrated firewall/VPN/QoS/VLAN/virtual firewall platforms
- Lucent IPSec Client. This is secure remote access software for mobile workers
- Lucent Security Management Server. This is carrier-grade software to streamline security and VPN management as well as QoS provisioning.

More information

For more information on this product, see http://www.lucent.com.

□

10 *Polycom® MGC™* video conferencing server

Overview

Purpose

This chapter provides an overview of the *Polycom® MGC™* video conferencing server.

Contents

Polycom MGC video conferencing server

Overview

The Polycom MGC video conferencing server provides full featured audio and video conferencing capabilities on a single platform. The key features are:

- Same conferencing features for audio and video
- Frame rates up to 60 fps, delivers highest quality video
- Wideband audio 14khz delivers high quality sound
- PSTN and VoIP audio conferences simultaneously on one platform
- Supports ad hoc and scheduled conference modes

Supported video algorithms

The Polycom MGC supports the following video algorithms:

- H.261
- H.263
- H.264

Dedicated platform

The MGC is a dedicated hardware platform with a purpose built architecture which efficiently shares both hardware and software resources across audio and video applications.

□

11 Covergence Eclipse

Overview

Purpose

This chapter describes the Covergence Eclipse.

Contents

Covergence Eclipse

Purpose

This topic describes the Covergence Eclipse family of products. The main function of the Covergence Eclipse is to offer interoperatibility with the MicroSoft Live Communication Server

Eclipe models

The Covergence Eclipse family consist of the following models:

- Eclipse 50
- Eclipse 350
- Eclipse 550

Main functions

The Covergence Eclipse performs the following roles:

- Gateway to third party applications such as Microsoft Live Communication Server (LCS).
  For example allowing third party call control and phone presence on LCS clients.
- Secure connectivity.
  To provide secure SIP connectivity between enterprise locations or between an enterprise location and users.

Gateway to 3rd party applications

Eclipse provides a gateway to 3rd party applications such as Microsoft Live Communication Server (LCS).

The Covergence comprehensive access edge in a dual voice and LCS deployment provides:

- Remote traversal and security for both LCS and voice endpoints in a single platform
- LCS client telephony feature support (uaCSTA) to application server inter-working
- TLS and SRTP termination and conversion
- Network based LCS virus scanning for file transfers
- LCS IM content control and modification
- URL filtering and virus checking
- IM logging
- Voice recording, video recording, and file logging
- Integration with Active Directory for user provisioning and control

- User portal support for retrieving and playing back IM logs, voice calls, video sessions, etc
- Complete policy based control including location based enforcement
- Identity management and enforcement
- Advanced call completion features including ‘find-me, follow-me’ based on presence and location

Third party telephony

Eclipse supports Microsoft Third Party Call Control features.

This enables Live Communication Server clients to:

- Set up calls between registered SIP telephony endpoints, using the Lucent Feature Server 3000.
- Set up calls between PSTN enabled phones via standard SIP gateways.
- Transfer call control and conference in third parties.
- Monitor call status, and perform telephony services such as call hold.

Secure connectivity

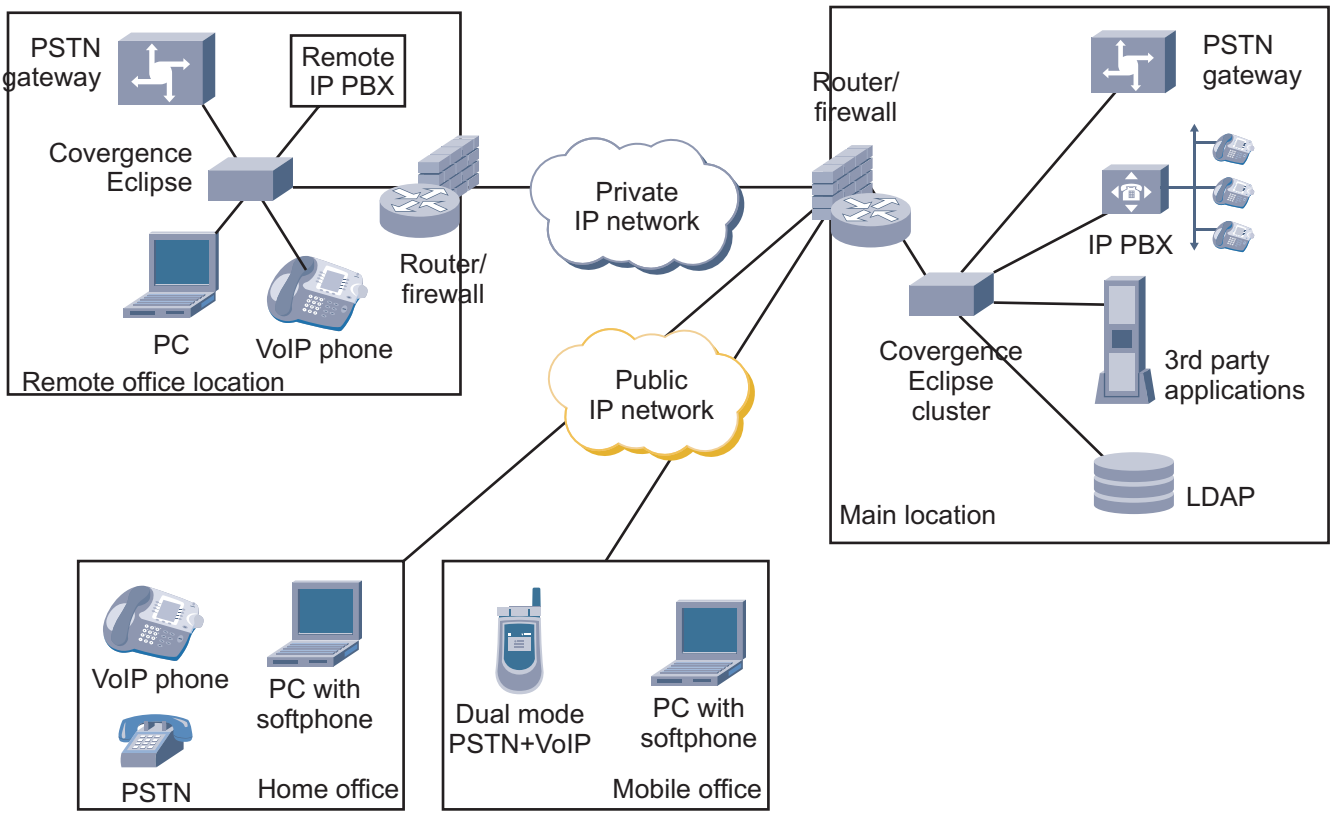
Covergence Eclipse acts a a security device to securely interconnect SIP applications from enterprise main locations to remote locations and home offices.

Covergence Eclipse provides:

- Signaling and media encryption
- Local call completion, fail-over IP routing, and PSTN gateway routing when hosted VOIP service is unavailable or unreachable
- Policy based security, control and monitoring of any or all SIP traffic in enterprise
- Auto-phone provisioning, remote phone upgrade, QOS marking and monitoring, SLA verification, local debug and demarcation features

The following figure shows enterprise connectivity using Covergence Eclipse. Please PSTN gateway and remote IP PBX may not be present at smaller enterprise locations.

Small enterprise locations may also connect through a public IP network. The Eclipe model that is used depend on capacity requirements:



Live Communications Server 2005 overview

Introduction

Microsoft® Office Live Communications Server 2005 provides a stable, extensible, enterprise-ready Instant Messaging and presence awareness platform based on the SIP (Session Initiation Protocol) and SIMPLE (SIP IM and Presence Leveraging Extensions) standards.

Live Communications Server 2005 supports audio and video exchange, application sharing, and data collaboration on a peer-to-peer basis.

Editions

Live Communications Server 2005 offers the following editions:

- Live Communications Server 2005 Standard Edition for use in small- or medium-size organizations.
- Live Communications Server 2005 Enterprise Edition for use in larger organizations.

Live Communications Server 2005 Standard Edition

The Live Communications Server 2005 Standard Edition consists of a single, stand-alone IM and presence server along with a local MSDE (Microsoft Data Engine) database for storing user data.

The Standard Edition supports up to 15,000 concurrent connections. The Standard Edition assigns users to a single home server. Although a domain might contain two or more home servers, each user is assigned to only one home server. User data, such as contact lists and registration status, are stored in a SQL MSDE database on the same server.

Live Communications Server 2005 Enterprise Edition

The Live Communications Server 2005 Enterprise Edition uses a server pool.

A server pool consists of a group of Enterprise Edition front-end servers connected to a separate, shared SQL Server database. This two-tier architecture enables Enterprise Edition to deliver substantial improvements in availability, scalability, performance and data recovery.

The Enterprise Edition supports up to 125,000 users per pool. In an Enterprise pool, one or more Live Communications Servers share a central SQL database that stores user data.

Live Communications Server components

Live Communications Server 2005 runs on Microsoft *Windows Server*™ 2003 and takes advantage of Windows tools and technologies, including:

- *Active Directory*® directory service for authentication and group policy
- *Microsoft SQL Server*™ for maintaining user data, logging, and archiving.
- Microsoft Office Communicator 2005 for the default client.
- WMI (Windows Management Instrumentation), MOM (Microsoft Operations Manager), and MMC (Microsoft Management Console) for management.

Live Communications Server 2005 is also integrated with Microsoft Office, allowing users of applications such as *Microsoft Outlook*® to take advantage of IM and presence awareness from within those applications.

Clients

Live Communications Server 2005 supports:

- Microsoft Windows Messenger 5.1 for basic presence and IM scenarios
- Microsoft Office Communicator 2005 client for enhanced capabilities

Microsoft Office Communicator 2005 features supported by Live Communications Server 2005 include:

- Contact search capabilities, using Live Communications Server Address Book Service.
  This allows users to search for others from their corporate global address list and from local address information on their computer.
- Integration with Microsoft Office® Outlook® and Microsoft Exchange Server™
  This allows users to view other contacts' presence information from their schedule.
- Integration with enterprise telephony systems.
  This allows the user to control their enterprise phone directly from their computer to initiate calls and divert calls to a remote location.
- Conference calls with partner service providers

□

12 Lucent Communication Manager

Overview

Purpose

This chapter describes the Lucent Communication Manager product.

Contents

Lucent Communication Manager

Overview

The Lucent Communication Manager (Lucent CM) provides easy to use interfaces for administrators and end users.

Administrators use Lucent CM Explorer clients to define and manage:

- Applications and hardware
- Services
- Partitions
- End users.

End users use a web launchable client as a single, integrated interface to access a wide range of services and applications that enable them to communicate efficiently.

The interface is easy to use and can be customized to the individual needs and wishes of an end user.

An end user can:

- Establish calls (or sessions)
- Search and define contacts
- Invoke services
- Define preferences
- Manage services.

Type of users

The Lucent CM system is accessed by:

- System administrators
- Partition administrators
- End users.

Components of the Lucent CM

The Lucent CM includes:

- Lucent CM servers that run the Lucent CM applications
- Lucent CM Explorer client used by administrators to manage the Lucent CM system
- Databases to store information
- Load balancers to balance traffic
- Lucent CM web launchable user client software to access services.

Solution components

Other components that are used in Lucent solutions that use the Lucent CM include:

- Call servers to provide call features
- (External) LDAP servers to store information
- Lucent Active PhoneBook to store address book information
- Presence servers to store and retreive presence information
- Applications to provide services to end users.
  - Voice mail
  - E-mail
  - Video
  - Instant Messaging

Lucent CM web launchable user client

Users access and manage services through a web launchable client. The Lucent CM user client is downloaded on the user's PC for easy use by the end user. The Lucent CM user client can be customized and skinned according to the needs and wishes of an end user or groups of users. Lucent CM can also be accessed using a mobile device.

Call servers

Calling features for the Lucent CM users are provided by call servers.

The call servers supported by Lucent CM are:

- Lucent Feature Server 3000
- Lucent Feature Server 5000

End users can access calling features through a managed IP connection to the call server.

Administrators can administer the call servers via the Lucent CM Explorer.

□

Lucent CM system main components

Introduction

The Lucent CM system consists of the following main components:

- Servers running the Lucent CM applications
- Databases to store information
- Load balancers to distribute traffic.

Lucent CM servers

The Lucent CM system consists of multiple application servers running on multiple Linux hosts. The servers are responsible for processing the requests from the Lucent CM user clients. The servers forward information to external services (for example call servers). Information that is received from external services is processed by the Lucent CM servers and forwarded to the Lucent CM user clients.

An application monitoring program, Lucent High Availability (LU-HA) monitors the activity and status of the applications, detects faults and initiates recoveries. The program is also used to provide Lucent CM Explorer access and to control software upgrades.

Databases

The databases in the Lucent CM system are used to store information about the partitions and users. They also store information about the services, such as authentication services.

The servers redirect information and requests to the databases for data storage or data retrieval.

A database monitoring program monitors the activity and status of the databases, detects faults and initiates recoveries.

Load balancer

Depending on the configuration that is deployed, the Lucent CM system may consist of multiple application servers running on multiple Linux hosts. Lucent CM user clients, however, use only a single host name or IP address for initial access to the system.

The host name or IP address is known as a Virtual IP (VIP).

Load balancing is performed for logon requests. The load balancer forwards a logon request that comes into the single (virtual) IP address to one of the available application servers. Load balancing is performed on a round-robin base. Once connected to the assigned application server, all subsequent requests are handled by the server that is assigned to the session.

One load balancer acts as active load balancer. Additional optional load balancers act as standby. Heartbeat daemons run on the active and the standby load balancers. When the heartbeat daemon of the standby cannot hear the heartbeat message from the active in the specified time, it will take over the virtual IP address to provide the load-balancing service.

When the failing load balancer recovers, it becomes the standby load balancer.

Load balancing is based on Linux Virtual Server technology. Refer to http://www.linuxvirtualserver.org/ (http://www.linuxvirtualserver.org/)

□

Requirements and specifications - Lucent CM system server

Purpose

This topic lists the system requirements and specifications for the Lucent CM system servers.

Certified Lucent CM servers

CAUTION

Voiding of product warranty

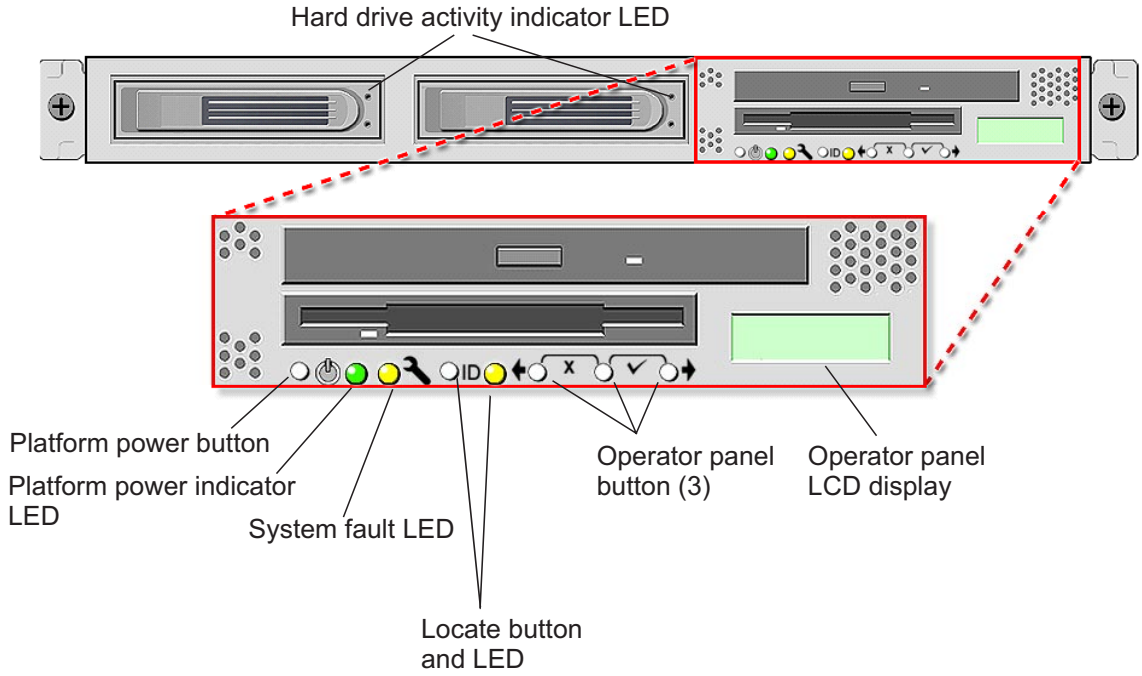
Non-certified servers are not supported and void product warranties.

Only use Lucent certified servers.

Certified server	Vendor
Sun Fire™ V20z	*Sun Microsystems™*

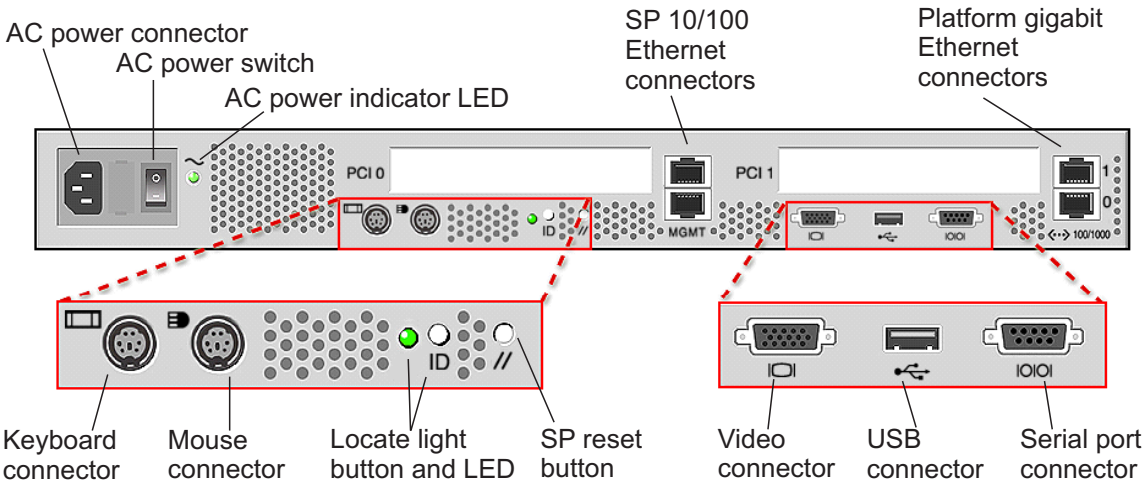
Front layout

The diagram shows the front layout of the unit:



Rear layout

The diagram shows the rear layout of the unit:



Lucent CM server hardware specifications

Specifications for the Sun *Fire*™ V20z are:

- AMD Opteron 244 processor
- 1 GB RAM
- 73 GB 1000 RPM Ultra320 SCSI disk
- Two 10/100/1000 Ethernet ports
- One RS–232 console port
- CD drive
- AC power supply, variable speed fans
- Keyboard, video and mouse connections (for initial installation only).

Additional components

Additional components for deployment:

Component	Component
Cabinet	Sun Rack 900: • 38RU AC • Dual Power Distribution System with power jumper cables • Power cable kit • Side Panels • Lockable doors • Filter panel kit.
Slide rail	Slide rail kit for Sun Fire V20z for use in Sun Rack 900
L2 Ethernet switch	24-port Cajun 100BaseT L2 Ethernet switch
Terminal server	Sun 8-port Cluster Terminal Concentrator
Cables	• Ethernet (CAT5): straight, crossover and RJ45 to RJ45 • Serial: null modem and RJ45 to RJ45 • RJ45 to DB9 adapter for Sun Fire V20z COM0 port

Lucent CM server software specifications

The software that is used on the Lucent CM nodes:

Component	Minimum requirement
Operating System	RedHat Linux R3.0 WS standard edition update 6
Load balancer	Lucent customized based on Linux Virtual Framework
SQL database	MySQL 4.0.20, using MySQL database replication for high availability
J2EE Application server	JBoss AS 3.2.5

13 BayPackets messaging

Overview

Purpose

This chapter describes the BayPackets Unified Communications product.

Contents

BayPackets' Agility Unified Communications

Overview

Agility Unified Communications from BayPackets Inc. integrates voicemail, email and fax into a single mailbox accessible by multiple devices incuding IP and POTS telephones, cell phones, and web browsers. Unified Communications offers multiple options for message notification, including E-mail, SMS, and IM.

Hardware platform

The Agility Unified Communications software package is deployed on the messaging architecture that supports messaging services with the Lucent Feature Server 3000.

Refer to the Lucent Feater Service 3000 product description.

Features

The BayPackets Unified Communications package supports the following features:

- Basic voice mail services, including:
  - Secured access to the message box
  - Greetings for busy, no-answer, standard, custom and Extended-absence
  - Options for playing header information, with date, time and caller information
  - Voice Message Play/Replay, Skip, Save/Delete, Forward/Reply and recording
  - Mark message urgent and/or private
  - Message waiting indications - SIP-MWI, SMDI
- Visual voice mail capabilities:
  - Web-based subscriber self-administration
  - Web-based Voice mailbox Access
  - Notification via Email (with or w/o attachment)
- Unified messaging capabilities, including:
  - Fax (G.711 pass-through and T.38)
  - Store incoming faxes in tiff format
  - Forward faxes as email messages
  - Unified Message box (voicemail, fax, email with separate icons on web-mail)
  - Single Message Store (voicemail, fax, email)
  - Support for Notifications via pager/cell via SMTP, SMS/SMPP

□

14 Antepo IM and Presence

Overview

Purpose

This chapter describes the Antepo IM and Presence product.

Contents

Antepo™ Open Presence Network™ (OPN) System™ 4.5 overview

Purpose

This topic describes the Antepo™ Open Presence Network™ (OPN) System™ 4.5. The OPN System™ 4.5 is a standards based, interoperable system for building real-time Instant Messaging and Presence networks. The OPN System™ 4.5 consists of servers and a client.

OPN System™ 4.5 Server

The OPN System™ 4.5 Server is a software application that runs on Windows, Linux and Solaris platforms. The servers provide a flexible and scalable way to create Instant Messaging and Presence networks and provide text and multimedia communication to users.

The OPN System™ 4.5 Server offers carrier-class reliability and scalability.

OPN System™ 4.5 Client

The OPN System™ 4.5 Client is a desktop application for Instant Messaging and Presence based on the XMPP protocol. It is designed to facilitate real-time conversations from Microsoft™ Windows workstations in 1-to-1, 1-to-many, and many-to-many modes.

The client offers you a fast and efficient means of communicating messages and presence. You can search directories, manage list of contacts and synchronize your availability with them.

□

Antepo OPN System™ 4.5 Server

Configuration

The OPN System™ 4.5 supports the following types of deployment:

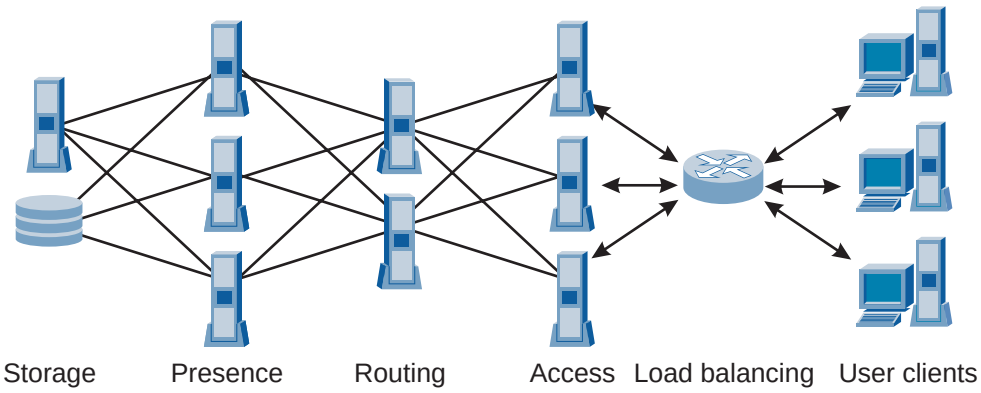
- Single server deployment with database, LDAP and external store on the same server
- Single server deployment with databases, LDAP and external storages on remote systems
- Multiple server deployment with databases, LDAP and external storages on remote systems.

The configuration that is deployed depends on the needs and requirements of the providers.

By using multiple servers the system can be deployed in parallel and load-balanced to ensure redundancy or hot-standby.

Architecture

The OPN System™ 4.5 architecture:



The OPN System™ 4.5 uses a three layer architecture that provides carrier-class reliability and allows scalability for Instant Messaging systems.

The OPN System™ 4.5 layers are:

Layer	Description
Access	To terminate and manage all client connections from the OPN user clients to the servers. Incoming TCP sockets are multiplexed and forwarded to the routing layer.

Layer	Description
Routing	To dynamically route traffic between Access and Management layers and to external systems. The routing layer provides load-balancing, redundancy and resiliency functions.
Management	To manage all user sessions, maintain presence information and handle subscription, notifications and all message traffic.

Information is stored externally from the OPN System™ 4.5. This allows the OPN System™ 4.5 to use existing, highly reliable, carrier grade, external storage systems. In particular, the state that is associated with each user session is stored

Supported server platforms

The Antepo OPN System™ 4.5 server is based on fully compliant Java™ 2 SE.

OPN System™ 4.5 server supports

- Windows 2000 Server, Advanced Server, and Datacenter
- Windows Server 2003, Standard Edition, Enterprise Edition, and Datacenter Edition
- Windows Small Business Server 2003
- Sun SPARC with Solaris 8 and 9
- Red Hat Linux Kernel 2.4.9.

Supported databases and directory systems

OPN System™ 4.5 is easily integrated with widely used corporate authentication and directory systems based on LDAP. This allows companies to use LDAP systems to control access to Instant Messaging networks and to control the use of IM, using policies.

Supported directory systems are:

- Embedded directory system
- Sun™ Identity Server
- Microsoft™ Active Directory™
- Microsoft™ Exchange
- Lotus™ Domino LDAP
- Computer Associates™ eTrust™ Directory

Supported databases are:

- McKoi (embedded database)
- MySQL™ (version 3.23.xx and higher)
- Microsoft™ SQL Server (version 7.x and higher)
- Oracle™ (version 8.x and 9.x)

Interface

The OPN System™ 4.5 Server provides an administrator web interface for tasks such as:

- Configuration
- Controlling IM client features
- Managing messaging traffic.

□

15 Network monitoring systems

Overview

Purpose

This chapter provides an overview of the network performance management systems that are available in Lucent VoIP for Enterprise.

This chapter describes the functions and the collected key performance indicators from the Lucent Feature Server 3000.

Contents

VitalNet™ network performance management software

Overview

VitalNet network performance management software is a comprehensive, automated tool that provides network performance information needed to pre-empt problems, optimize resources and plan operations. VitalNet enables enterprises to monitor, analyze, manage and predict network performance from a single, centralized location.

The VitalNet system collects performance data from elements and resources network-wide and delivers this data via graphical heat charts that provide top-level views of network operations. Enterprises can expand or narrow the view to observe overall performance or drill down for more detail in specific areas.

Features

Global VitalNet features:

- Fully automated performance monitoring
- Flexible executive reporting
- Streamlined capacity planning
- Efficient service-level management
- Simplified network operations

Supported hardware

VitalNet can be installed on a PC platform running *Windows NT*® or *Windows 2000*®

System requirements

The hardware platform must have:

- A minimum of 2 GB RAM
- 85 GB available hard disk space

□

Application Server key performance indicators

Collected KPI

The table shows the key performance indicators (KPIs) of the application server (part of the Lucent Feature Server 3000) collected by VitalNet.

KPI Name	VitalNet calculation	Description
Total Attempts	bwCallpNetworkOriginationAttempts + bwCallpNetworkTerminationAttempts + bwCallpUserOriginationAttempts + bwCallpUserTerminationAttempts	Total Attempts (#)
Ntwk Orig Attempts	bwCallpNetworkOriginationAttempts	Network Origination Attempts (#)
Ntwk Term Attempts	bwCallpNetworkTerminationAttempts	Network Termination Attempts (#)
Ntwk Term Answered %	100 * bwCallpNetworkTerminationsAnswered / bwCallpNetworkTerminationAttempts	Network Termination Answered (%)
User Orig Attempts	bwCallpUserOriginationAttempts	User Origination Attempts (#)
User Term Attempts	bwCallpUserTerminationAttempts	User Termination Attempts (#)
User Term Answered %	100 * bwCallpUserTerminationsAnswered / bwCallpUserTerminationAttempts	User Termination Answered (%)
Avg Active Calls	Avg(bwCallpActiveCalls)	Avg Active Calls (#)
Peak Active Calls	Max(bwCallpActiveCalls)	Peak Active Calls (#)
MCP Res Alloc Failures #	bwMCPResourceAllocFailures	MCP Resource Allocation Failures (#)
MCP Res Alloc Failures %	100 * bwMCPResourceAllocFailures / bwMCPResourceAllocAttempts	MCP Resource Allocation Failures (%)
SIP Total Transactions	bwSipSummaryTotalTransactions	Total SIP Transactions (#)

Network server key performance indicators

Collected KPIs

The table shows the key performance indicators (KPIs) of the network server (part of the Lucent Feature Server 3000) collect by VitalNet.

KPI Name	VitalNet calculation	Description
Policy Requests	bwNbPolicyRequests	Policy Requests (#)
Policy Req Failures #	bwNbPolicyRequestFailures	Policy Request Failures (#)
Policy Req Failures %	100 * bwNbPolicyRequestFailures / bwNbPolicyRequests	Policy Request Failures (%)
Sip Stats Failures	bwNbSipStatsFailures	SIP response Failures (#)
Avg Ports Used	Avg(msPortsInUse)	Avg Ports Used (#)
Peak Ports Used	Max(msPortsInUse)	Peak Ports Used (#)
No Port Avail Errors	msNoPortAvailableErrors	No Port Available Errors (#)
Peak Conf Ports Used	Max(msConfCurrentPortsInUse)	Peak Conference Ports Used (#)
RTP Sessions	msRtpSessionsCount	RTP Sessions (#)

Quality Index

Overview

The quality index specifies how measurement data is calculated and defines the parameters for the Vital charts and graphs.

Application server QIs

QI Name	Measured resource
qiCongestion	MCP Res Alloc Failures (%)
qiOverall	qiCongestion

Network server QIs

QI Name	Measured resource
qiCongestion	Policy Req Failures (%)
qiOverall	qiCongestion

Media Server QIs

QI Name	Measured resource
qiCongestion	msNoPortAvailableErrors * 3600 / seconds
qiOverall	qiCongestion

Part III: Operations, Administration, Maintenance and Provisioning aspects

Overview

Purpose

This part provides an overview of Operations, Administration, Maintenance and Provisioning aspects of Lucent VoIP for Enterprise.

The part describes OAM and P roles that can be distinguished and provides information about the OAM&P capabilities for the Lucent Feature Server 3000.

An overview of the OAM&P capabilities for the Lucent FS 3000 is provided because the FS 3000 is the main network element in the solution.

For information on OAM&P capabilities of other network elements, refer to the documentation set of the network element. describers

Contents

16 Operations, Administration, Maintenance and Provisioning

Overview

Purpose

This part provides an overview of Operations, Administration, Maintenance and Provisioning aspects of Lucent VoIP for Enterprise.

Contents

Roles in Lucent VoIP for Enterprise

Use of the roadmap

The documentation roadmap shows the roles of personnel involved in the solution and the tasks they perform.

Roles

The following roles can be distinguished:

Role	Task description
Installer[1]	• Hardware installation and basic configuration • Software installation and basic configuration • Install CPE • Configure CPE.
System administrator[2]	• Server management • Security management • Using administration tools for management • Managing log files.
OAM&P	• Troubleshooting solution components.
Enterprise system provider[2]	• System configuration • Create service providers • Allocating resources to a group.
Enterprise service provider	• Add and provision groups • Add and delete domains • Assign and authorize resources for existing groups • Change service provider definitions.
Enterprise group administrator[3] Enterprise department administrator[3]	• Add groups • Add departments • Add users • Configure groups services.

Role	Task description
End user	• Add and drop services • Configure services • Customize services.

Notes:

1. Typically Lucent personnel or enterprise IT personnel.
2. Typically enterprise IT personnel.
3. Typically selected enterprise personnel such as department heads or teamleaders.

□

Lucent Feature Server 3000 OAM&P capabilities

Overview

The Lucent Feature Server 3000 provides a range of interfaces to performs OAMP tasks. This topic provides an overview of the interfaces and provides a brief descriptions of each interface and OAMP area.

Web interfaces

The web interfaces (portals) and service management permissions provide secure access to the necessary information for each user type. A hierarchy of password-protected administrative control is supported, allowing for delegation of administrative responsibilities, as required.

The FS 3000 offers web interfaces for the following administrative levels:

Portal	Description
System Provider	Allows access to all web screens in the system, for the Application Server, Media Server, and Network Server. The screens permit offsetting responsibilities to service providers with Service Provider access, and to customer service representatives with Provisioning Administrator access.
Service Provider	Allows service providers access to system-level setup and monitoring functions, as well as group and personal management. Service Provider differs from the system provider access in that only tasks related to a service provider or reseller are accessible, rather than functions for monitoring and maintaining the solution. The Service Provider level administration supports customizing and branding of solution interfaces.
Enterprise	Facilitates the administration of large enterprises spanning multiple groups and sites. This level is parallel to the Service Provider layer, but with enterprise-specific attributes.
Group	Distributes some of the service provider responsibilities and management to the group administrator, empowering the business customer to provision services to users and manage group-related activities. The group administrator is a company employee such as an office manager or technology representative. On the Network Server, an enterprise administrator controls the functions, such as dialing plans, for one or more groups.

Portal	Description
Department	Allows department administrators to provision services to users and manage department related activities.
Personal	Grants individual users easy access to service configuration and management. Activating and customizing services such as call forwarding and call notification is simple and intuitive. Other Personal administrative and control functions are provided via the Personal interface, which allows users to control calls (using functions such as hold, transfer, and conference), via a familiar web screen.

Command line interfaces

The Lucent Feature Server 3000 provides a Command Line Interface (CLI) for configuration and maintenance of the system. The CLI is a text-based, password-protected application that allows system administrators to manage the FS 3000 servers.

The CLI provides management functions for:

- System Management, including:
  - Device management
  - Interface management
  - Conferencing ports
  - System timers
- Subscriber Management:
  - Creation and management of Service Providers, Groups, and Users
  - Password management
- Service Management, including:
  - Management of system-wide service data
  - Management of system-wide dial plans
  - Emergency numbers
  - Translations and routing data
  - Country codes
- System Monitoring, including:
  - Monitoring of system alarms
  - Performance statistics
  - Customizable reports

- Audit trails
- Protocol monitors

CORBA and XML

The Lucent Feature Server 3000 provides an external provisioning interface that can be used to configure subscriber and service data on both the Application Server and Network Server.

This interface can be used for:

- OSS and back-office integration
- Service creation

OSS and back-office integration

This interface allows for easy integration with a legacy back-office Operation Support Systems (OSS). The provisioning interface allows external OSS systems to configure and provision subscribers, enterprises, services and service providers.

Service creation

Third–party applications can use the provisioning interface as part of creating enhanced services.

For example, an external pre-paid application could be designed with the Network Communications Platform. The application would monitor subscriber usage. When the user's minutes are used up, the application would send a message over the provisioning interface to activate the "Intercept User" service. This would bar any calls to or from the user and play an appropriate announcement. The provisioning interface uses CORBA for transport, and carries XML data payload. The interface is secured. The interface is easily extendable, in new releases, the XML DTD may change, but the CORBA IDL remains constant.

Accounting management

For accounting management, the Lucent Feature Server 3000 supports:

- Call Detail Records (CDRs)
- Event Messages

Call Detail Records

Call Detail Records (CDRs) are captured by the Lucent FS 3000 for all calls that are made by users. The CDRs:

- Calling party
- Called party
- Redirecting party
- Call start timestamp

- Call stop timestamp
- Answer timestamp
- Long distance carrier ID

The CDR interface supports a seamless mediation to a legacy accounting format like AMA/BAF, and provides all the required information to perform toll communication billing (for example, duration-based billing) and carrier access charge settlements. The CDR interface is well suited (but not limited) to a centralized billing model where the Lucent FS 3000 acts as the single source of billing information in the network.

The Lucent FS 3000 CDR format is based upon PacketCable and ISDN billing standards.

Event messages

The FS 3000 also generates accounting event messages whenever a call event occurs which may impact billing (origination, answer, feature invocation, etc.) These event messages allow a specialized accounting node to collect accounting events from various points within a distributed network (such as an application server, a softswitch, or a media gateway). The accounting node correlates these events and generates billable records.

Event messages include:

- Signaling Start – call start, inbound or outbound
- Call Answer – call is answered
- Call Disconnect – call is released
- Signaling Stop – call ends
- Service Instance – a service is used on the call
- System Restart – the Application Server is restarted
- Long Duration Call Event – heartbeat for long calls

Event messages are stored in XML format and follow the PacketCable event message specification. This CDR interface can output accounting records in either XML format or comma-separated values (CSV).

Fault and performance management

The Lucent FS 3000 servers generate events and alarms that can be managed and monitored via SNMP traps. The events and alarms can be monitored and managed from a network management systems using standard network management tools.

The servers also distinguish fault and performance management alarms and counters. All servers generate operational measurements that are accessible via SNMP GET commands. The operational measurements can be retrieved using standard performance management systems.

The servers can also send periodic performance reports formatted in XML to one or more external network management systems via FTP. Thresholds on external systems can also be set so that the servers are polled and these systems generate alarms based on targeted operational devices and variables for capacity status and other critical performance measurements.

□

Security

Introduction

Security for all enterprises is of utmost concern in order that corporate resources are properly protected. The solution architecture provides security via a combination of mechanisms.

Security mechanismes include:

- Server hardening
- Secure access
- Endpoint registration
- Solution design

Server hardening

Each Lucent FS 3000 server (Application Server, Network Server, Media Server, Conferencing Server) is hardened through the use of Suns' Solaris Security toolkit, tailored specifically for the FS 3000 servers. This JumpStart Architecture and Security Scripts (JASS) toolkit, application hardens the Sun servers by disabling all unnecessary services and ports. After the application of JASS, no vulnerabilities are detectable by standard security probes.

Secure access

All access to the system by users and administrators is secure. Users and administrators must be authenticated and authorized to access the system.

All authentication and authorization requests are either encrypted via SSL or are allowed only through SSH interfaces.

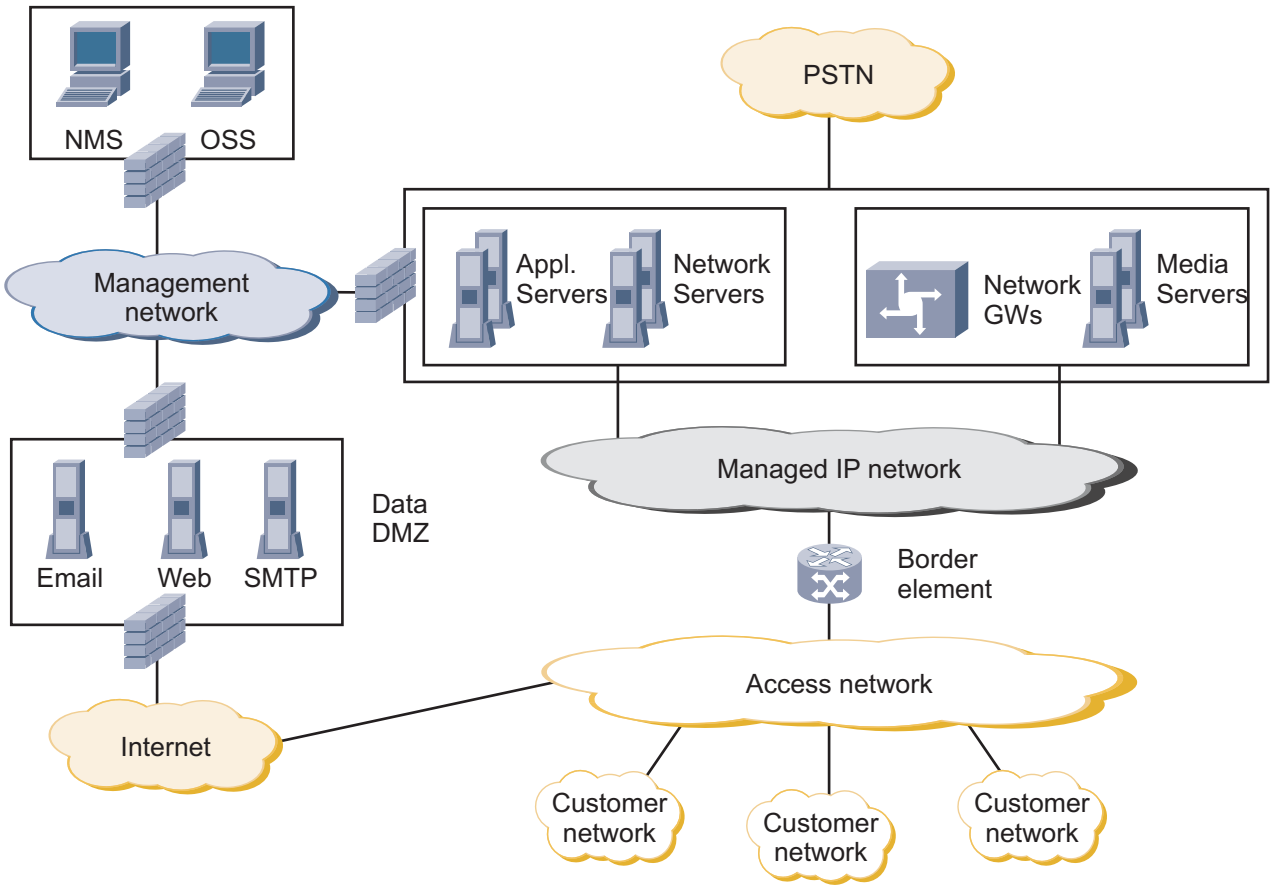
Endpoint registration

The solution supports SIP registration for endpoints. This ensures access is only allowed to devices that have properly registered with the Lucent FS 3000 servers.

Solution network design

The network of the solution is designed with security in mind. This includes the use of subnets and ensures protocols to support VoIP are isolated.

For a complete description of all the protocols and ports utilized, allowing for complete specification of necessary firewall policies, refer to Lucent FS 3000 documentation set.



The customer enterprise network represents a network of a subscribing enterprise, each operated under their own unique enterprise security policies and enforcement mechanisms. From a solution perspective, the VoIP protocols that are typically to be supported include SIP, MGCP, and RTP. Other protocols in use include HTTP (for web access).

The access network interconnects the customer enterprise network with a managed IP network of a service provider. Flowing through this network is all the customer data traffic (including possibly Internet traffic), and all the customer VoIP traffic. Typically, the access network is largely an “unmanaged” IP network, using security features built into the routing equipment. The managed IP network represents the core transport network.

A security layer between this subnet and the net that actually hosts the FS 3000 servers can be provided. Customer VoIP traffic is admitted from the access network, as are the RTP media traffic and the SIP and MGCP signaling traffic. Session Border Controllers can be deployed to admit packets from the access network.

In the management network, the Network Management Systems (NMS) and the Operations Support Systems (OSSes) reside. Through this subnet runs the service management traffic, including the XML/CORBA, SNMP, HTTP, HTTPS, CLI traffic.

In the Data DMZ, the servers for e-mail and the Lucent FS 3000 external web server reside. Here flow the SMTP and POP3/IMAP4 and HTTP/HTTPS protocols. Firewalls or Session Border Controllers are typically configured to provide the inter-subnet traffic screening.

RTP media streams are not encrypted.

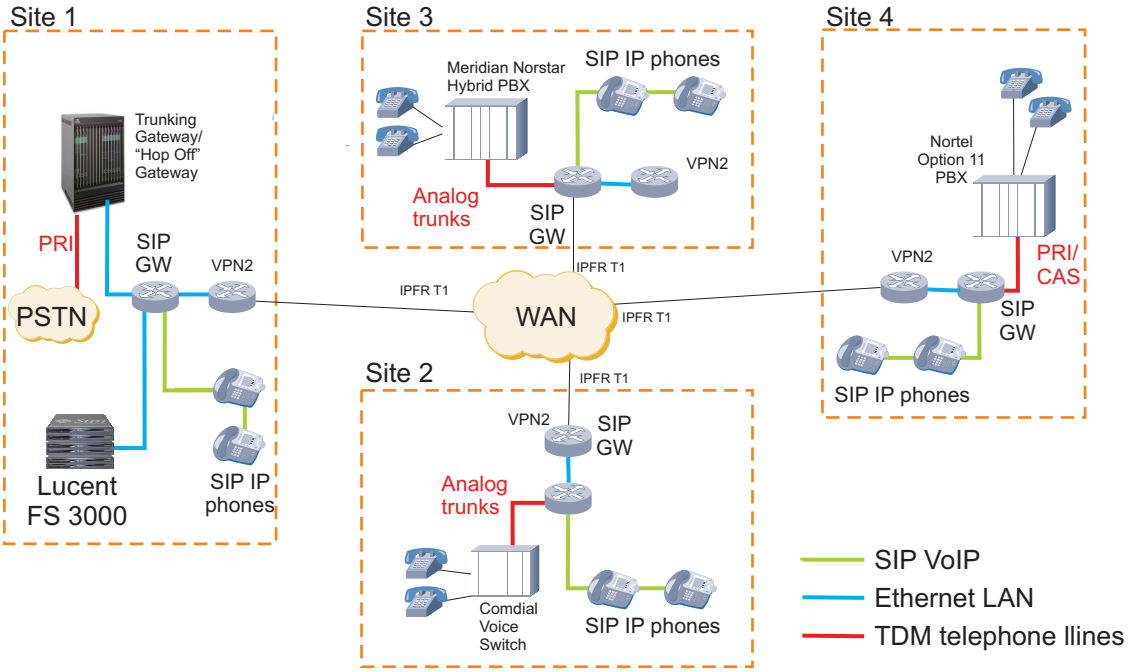
□

Migration

Introduction

The solution is designed to interoperate with TDM systems that are already deployed by an enterprise and accommodates smooth transitions of end users from TDM technology. Already deployed systems can migrate to the solution depending on the needs of the enterprise.

Example of network with deployed systems that require migration:



The example shows several sites of an enterprise, each hosting its own legacy PBX.

The solution can interconnect with an existing PBX via either PRI or T1 interface connections to some kind of SIP gateway. TDM-originated calls can be routed to either the PSTN or to the solution and other internal (to the enterprise) users through the services of the APX 1000 or other vendors' network gateways or FXOs. The same accommodations can be made for VoIP-initiated calls.

For external calls, the PSTN can route calls to either the existing PBX or to the network gateway associated with the solution. This approach allows an enterprise to retain some legacy capability while migrating over time to the solution.

Abbreviated dial plans already in place at an enterprise can be preserved and accommodated via translation services at either the network gateway or the FS 3000 Network Server. At the same time, SIP phones can be introduced into the enterprise at

any of the enterprise locations. Enterprises may choose to migrate users because of organization affiliations or site residency. Enterprises may choose to deploy solutions' native Voicemail System (VMS) or they may choose to continue with a VMS already deployed for the enterprise. In the latter case, Voicemail interoperability can be achieved by utilizing SMDI interfaces between them.

Lucent can readily support a site-by-site migration or full or transitional migration of large sites.

□

Appendix A: Supported hardware

Overview

Purpose

This appendix describes the hardware that is supported by the solution.

The hardware that is listed has undergone interoperability testing for the solution.

Contents

Supported IP phones

IP phones

IP phones (hard phones):

Vendor	Model	SIP / MGCP	Lines	Codecs	Features
SwissVoice	IP 10S 	SIP MGCP	1	G.711 G.723.1 G.729a	• PC LAN port • Power over LAN • Headset jack • Built-in speakerphone • 802.1q (VLAN).
Innomedia	MTA 3308 	SIP	2	G.711 G.726 G.728 G.729E G.723.1	• PC LAN port • Speakerphone • Message Waiting Indicator • 802.1p (QoS), 802.1q (VLAN) • TOS tagging • Priority SwitchPoE • Supports TCP/IP, UDP, DHCP, ARP, RTP, ICMP, HTTP, SNMP, TFTP, CCD
	MTA 5531 Video Phone (not CE marked) MTA 5410 Video Phone (CE marked) 	SIP	2	H.263(+) H.261 GCIF G.711 G.726 G.728 G.729 G.723.1	• Auxiliary Audio In/Out • Video Input/Output • Remote/PIP • QoS • NAT router • Messaging • Voice/video answering machine • 3G and mobile interoperability • Supports TCP/IP, UDP, DHCP, ARP, RTP, ICMP, HTTP, SNMP, TFTP, STUN, CCD,

Vendor	Model	SIP / MGCP	Lines	Codecs	Features
Polycom	SoundPoint IP300/IP301[1] 	SIP	2	G.711 G.723.1 G.729a RFC2833	• PC LAN port • 802.3af • Cisco Inline Power • Auto-line support • Headset jack • 802.1p (CoS) • 802.1q (VLAN). • HTTPS secure provisioning (Soundpoint IPx01 models) • SoundPoint IP601 supports up to 3 Expansion Modules (EM) for attendants
	SoundPoint IP500/IP501[1]	SIP MGCP	3		
	SoundPoint IP600	SIP	6		
	SoundPoint IP601 Supports Expansion Modules	SIP	6 12, with EM		
Unidata	WIFI 5000 	SIP	2	G.711 G.729a G.729b	WIFI IP phone: • Security (IEEE 802.1x MD5/TLS/TTLS 64/128/256 bits WEP • Multilingual • Management (SNMP, Sys log, HTTP)

Notes:

1. IP301 and IP501 are currently undergoing interoperability testing. Testing is scheduled to be completed at March 6, 2006.

Supported Conference phones

Interoperability tested conference IP phones (hardphones):

Vendor	Model	SIP / MGCP	Lines	Codecs	Features
Polycom	Soundstation IP4000 	SIP	1	G.711 G.729a G.723.1 RFC2833	• PC LAN port • IEEE 802.3af • Cisco Inline Power • Auto-line support • Headset jack • IEEE 802.1p (CoS) • IEEE 802.1q (VLAN).

Supported SIP IP softphones

Interoperability tested SIP IP softphones:

Vendor	Model	SIP / MGCP	Lines	Codecs	Features
CounterPath™ Solutions, Inc.	*eyeBeam*™ Video Softphone[1] 	SIP	6	Basic H.263 H.263+ H.263++CIF G.711 a+u SPX iLBC GSM	• Supports Windows (98SE, NT4, ME, 2000, XP), Mac OSX, Lindows OS • Video Quality Settings • Supports Multple SIP Proxy Registration • NAT traversal • Auto-detect IP address and manual IP address • Acoustic Echo Cancelation • Message Waiting Indicator

Notes:

1. The eyeBeam is not sold through and not supported by Lucent Technologies.

□

Supported integrated access devices and line gateways

Supported IADs

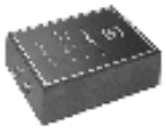
Integrated Access Devices (IADs):

Vendor	Model	SIP / MGCP	WAN	Ports	LAN	Features
Verilink	NE 6104i 	SIP MGCP	ADSL	4	10/100 BaseT	G.711 G.723.1 G.726-le G.729a Fax & Modem Pass-through
	NE 6108		ADSL	8		
	NE 6200		T1/E1	8		
	NE 6300		SDSL	8		
	NE 6500 Series		G.SHDSL	8 - 16		
	NE 6504i		G.SHDSL	4		
	NE 7200 Series		T1	16 or 24		
	NE 7300 Series		SDSL	16 or 24		
	NE 7500 Series					
	NE 8100 Series		ADSL	4 or 8		
	NE 8200 Series		T1/E1	8, 16 or 24		
	NE 8300 Series		SDSL	4, 8, 16 or 24		
	NE 8500 Series		SHDSL	4, 8, 16 or 24		

Supported desktop line gateways

Desktop line gateways:

Vendor	Model	SIP / MGCP	Ports	LAN	Codecs	Features
AudioCodes	MP102 MP104 MP108 MP114 	SIP MGCP	2 4 8 4	10/100 BaseT	G.711 G.723.1 G.726 G.727 G.729a NetCoder T.38 RFC2833	• G.168 echo cancellation • Voice Activity Detection • Comfort Noise Generation • Dynamic Jitter Buffer • Long Haul up to 10000 feet • T.38 and G.711 fax support.
Mediatrix	1402 	SIP	2 (BRI)	10/100 BaseT	G.711 G.723.1 G.729 G.729ab T. 38 RFC2833	• Euro ISDN EDSS-1 • ETS 300 011 (ISDN PRI UNI) • ETS 300 012-1 (ITU-T I.430) • ETS 300 402-2 (ITU-T Q.921) • ETS 300 403-1/2 (ITU-T Q.931) • ETS 300 102-2 (ITU-T Q.931)
	1404	SIP	4 (BRI)			

Vendor	Model	SIP / MGCP	Ports	LAN	Codecs	Features
Sipura	SPA-2000 	SIP	2		G.711u,a G.723.1 G.726 G.729a	• Music on hold client
Neogadgets	MC-9700 	SIP				

Supported rack mountable line gateways

Rack mountable line gateways:

Vendor	Model	SIP / MGCP	Ports	LAN	Codecs	Features
AudioCodes	MP-124 	SIP MGCP	24 FXS ports Telco 50 pin	10/100 BaseT	G.711 G.723.1 G.726 G.727 G.729a NetCoder T.38 RFC2833	• G.168 echo cancellation • Voice Activity Detection • Comfort Noise Generation • Dynamic Jitter Buffer • Long Haul up to 10000 feet • T.38 and G.711 fax support.

Vendor	Model	SIP / MGCP	Ports	LAN	Codecs	Features
Citel	*CITELink*™ 	SIP	24 ports		G.711 G.723.1a G.729a	Supported handsets: • Avaya Model DEFINITY • Nortel Norstar • Nortel Meridian • Nortel Model P Sets • NEC Model DTERM

Supported rack mountable trunk gateways

Supported rack mountable trunk gateways

Rack mountable trunk gateways:

Vendor	Model	SIP / MGCP	Ports	LAN	Codecs	Features
AudioCodes	Mediant 2000 	SIP MGCP	1 - 16 T1/E1 (PRI, CAS)	10/100 BaseT	G.711 G.729a G.723.1 G.726 G.727 NetCoder T.38 RFC2833	• G.168 echo cancellation • Voice Activity Detection • Comfort Noise Generation • Dynamic Jitter Buffer • Long Haul up to 10000 feet • T.38 and G.711 fax support.
	Mediant 1000	SIP MGCP	1 - 4 T1/E1/J1 (PRI, CAS) Up to 24 analog ports (FXS)			
Lucent Technologies	APX 1000 Universal Gateway 	SIP MGCP	1-16 (T1/E1, PRI, CAS)	10/100 BaseT	G.711 G.729a G.729a/b G.723.1	• DTM in-band • RFC2833 • H.245 (H.323) • Expandable modules • G.168 • Voice Activity Detection • Comfort Noise Generation. • Silence suppression • Dynamic Jitter Buffer

Supported optional equipment

Supported session border controller

Session border controllers:

Vendor	Model	SIP / MGCP	Ports	LAN	Features
Juniper	VoiceFlow series	SIP MGCP H.323		10/100/1000 BaseT	• Call routing • Call admission control • Topology hiding • Data − Header NAT, HTTP, HTTPS and TFTP support • E911/local address, CDRs, SNMP,

Supported video conferencing server

Video conferencing servers:

Vendor	Model	SIP / MGCP	Ports	Codecs	Features
Polycom	MGC-25 	SIP	24 vidoe conferencing 2 PRI T1/E1	G.711 G.722 G.722.1 G.723 G.728 G.729a Siren 7/14 RFC2833	• H.323, SIP, ISDN, V.35 • Video in H.261, H.263, H.264 • QCIF, CIF • Rack mountable

Notes:

1. Not orderable through Lucent

Supported remote survivability equipment

Remote survivability:

Vendor	Model	SIP / MGCP	Ports	LAN	Features
Edgewater	4200 Series 	SIP MGCP		10/100/1000 BaseT	• Management (Web GUI, CLI, SNMP, Syslog, SSH, Telnet) • H.323, RTP
	4300 Series	SIP MGCP			
	5300 Series	SIP MGCP			
	6400 Series	SIP MGCP	500-10,000		

Supported interoperability equipment

Interoperability:

Vendor	Model	SIP / MGCP	Ports	LAN	Features
Covergence	Eclipse 50 Eclipse 350 Eclipse 550	SIP MGCP		10/100 BaseT	• Management (Web GUI) •

Supported firewall equipment

Firewalls:

Vendor	Model	SIP / MGCP	Ports	LAN	Features
Lucent Technologies	Brick Firewall 350  Also available 20, 80, 150, 500, 1000, 1100 models	N/A	N/A	10/100 BaseT 10/100/1000 BaseT	• High throughput • Virtual firewalls • 3DES • VPN tunnel support

Supported terminal server equipment

Terminal servers:

Vendor	Model	SIP / MGCP	Ports	Features
MRV Communi-cations	IR-8020–101 	SIP	N/A	• Terminates legacy voicemail systems • RS-232 • 20 console ports • AC power

Supported backup power equipment

Backup power:

Vendor	Model	Ports	Features
APC	SmartUPS 	N/A	• Backup power with batteries for extended runtime • APC configuration based on power requirements and battery runtime

□

Supported FXOs

Supported FXOs

FXOs:

Vendor	Model	Ports	LAN	Codecs	Other features
AudioCodes	MP-104	4 FXO	10/100 BaseT	G.711 G.723.1 G.726 G.727 G.729a NetCoder T.38 RFC2833	• G.168 echo cancellation • Voice Activity Detection • Comfort Noise Generation • Dynamic Jitter Buffer • Long Haul up to 10000 feet • T.38 and G.711 fax support
	MP-108	8 FXO	10/100 BaseT		
Multitech	*MultiVOIP*™ MVP 210-SS	2 FXS/FXO	10/100 BaseT	G.711 G.723 G.726 G.727 G.729	• Voice Activity Detection • Comfort Noise Generation • QoS support (DiffServ, 802.1p, G.165, G.168) • Adaptive echo cancellation • Dynamic jitter buffers
	MultiVOIP™ MVP410-SS	4 FXS/FXO	10/100 BaseT		
	MultiVOIP™ MVP810-SS	8 FXS/FXO	10/100 BaseT		

Vendor	Model	Ports	LAN	Codecs	Other features
Quintum	Tenor AS series: ASM series	2 or 4 FXO/FXS	10/100 BaseT	G.711 G.723.1a G.729ab T.38 RFC2833	• G.168 echo cancellation • Voice Activity Detection • Comfort Noise Generation • Adaptive Jitter Buffer • T.38 and G.711 fax support • QoS support (IP TOS, DiffServ) • DHCP client
	Tenor AS series: ASG series	2 or 4 FXS, no FXO	10/100 BaseT		
	Tenor AX series: AXM series	8, 16, or 24 FXS/FXO	10/100 BaseT		
	Tenor AX series: AXG series	8, 16, or 24 FXS, no FXO	10/100 BaseT		
	Tenor AX series: AXT series	8, 16, or 24 FXO, no FXS	10/100 BaseT		
	Tenor AX series: AXE series	8 FXS/2FXO 16 FXS/2FXO 24 FXS/2FXO	10/100 BaseT		
	MVP410-SS	4 FXS/FXO	10/100 BaseT		
	MVP810-SS	8 FXS/FXO	10/100 BaseT		

Appendix B: Lucent VoIP for Enterprise offer matrix

Offer matrix

Offer matrix

The offer matrix lists the options that are available with the solution offer. Some of the functionality of the system relies upon the enterprise having certain facilities available already, and these are not provided as part of the solution offer.

Capability	Customer provided offer component	Customer supplied component
IP-enabled feature server providing personal and group services and a web server.	Application servers in redundant pairs, including hardware. Refer to *BroadWorks Recommended Hardware Guide* for hardware.	
Centralized network translations and routing; also delivers Voice VPN applications and private network gateway routing.	Network servers in an N+1 configuration, including hardware. Refer to *BroadWorks Recommended Hardware Guide* for hardware.	
Unified messaging, three-way conferencing, IVR, auto attendant, video services and network service announcements.	Media servers in an N+1 configuration (normally located close to the APX 1000 to prevent media traffic from traveling too far), including hardware. Refer to *BroadWorks Recommended Hardware Guide* for hardware.	

Capability	Customer provided offer component	Customer supplied component
Audio and web conferencing - Scheduled, recurring, reservation-less, and ad-hoc. Meet-me dial-in numbers. *Web collaboration* - Share *Microsoft® PowerPoint®*, Excel, and Word files, Secure SSL and password protection, Web browser viewable, no client required.	Conferencing application server, including hardware. Refer to *BroadWorks Recommended Hardware Guide* for hardware.	
Media resource for conferencing.	Conferencing media server, including hardware (This may be co-located on the conferencing application server hardware for smaller configurations). Refer to *BroadWorks Recommended Hardware Guide* for hardware.	
Enhanced call logging. To move storage of large volumes of call related information from the application servers to seperate servers.	Call detail server, including hardware. Refer to *BroadWorks Recommended Hardware Guide* for hardware.	
Control of the Message Waiting Indication (MWI) status of users with BroadWorks voice messaging who have their access lines on a PBX, a class 5 switch, or another IP-based application server.	MWI converter and terminal server.	
Carrier-class access gateway optimized for seamless integration of dial, Voice-over-IP, fax-over-IP, virtual private network, and other IP services.	APX 1000. At least one required for each location.	

Capability	Customer provided offer component	Customer supplied component
Alternate line access to PSTN can be used in the event of APX 1000 failure for the routing of emergency calls.	FXO At least one required for each location.	
If the enterprise uses private IP addresses by deploying a NAT/PAT solution at the entry point to the enterprise, this causes a problem to SIP communication and to RTP. If the enterprise is using NAT/PAT but no edge router that supports SIP/RTP, then an Application Layer Gateway (ALG) should be deployed. The solution interoperates with Kagoor and AcmePacket.		Application Layer Gateway interoperability with Kagoor and AcmePacket.
If the enterprise consists of a number of satellite locations interconnected by a wide-area network. Continued telephone service can be assured at each remote location in the event of WAN failure by deploying a Converged Network Appliance (CNA) at each location. This device can also work as a router, ALG, firewall, DHCP server, and PSTN gateway.	Edgewater CNA. The model depends upon traffic requirements at the remote location and the functionality required.	

Capability	Customer provided offer component	Customer supplied component
Enhanced IP phone configuration. This feature makes it easier to manage a subscriber's IP phone. It allows an administrator to use default configuration data applied to every IP phone in a system or group and then automatically use specific parameters from a user's profile to create a unique configuration file for that user's IP phone. The devices MAC address is used to create a unique configuration file name that is downloaded from the (T)FTP server by the phone.		An (T)FTP server is required to use this feature depending on the phones deployed. The Linux, *Solaris*™ and *UNIX*® operating systems come with a built in (T)FTP server. (T)FTP servers for *Windows*® are available from a large number of vendors.
The solutions redundancy capabilities requires DNS. The solution should be configured so that there is a single FQDN that represents the application server primary/secondary pair (both A and SRV records) and another FQDN representing the network server cluster (both A and SRV records). The application server FQDN A/SRV records must be returned in fixed order. The network server FQDN A/SRV records can be load balanced or fixed order.		DNS server.

Capability	Customer provided offer component	Customer supplied component
BroadWorks supports the SMTP standard for email dispatch. SMTP is used for both messaging and notification services. The unified messaging service makes use of this protocol to dispatch messages to a user's mailboxes. The notification service makes use of this protocol to dispatch notifications to a user's email account or short message service. BroadWorks is fully compliant to the IETF standard: • RFC 821 http://www.ietf.org/rfc/rfc821.txt.		SMTP Server compliant with RFC 821.
BroadWorks supports the POP3 and IMAP4 standards for email reception. These interfaces are used for messaging services, such as unified messaging applications. All voice/fax messages for a user are stored in a standard POP3 or IMAP4 server. The user can access these messages via a standard email client or via the BroadWorks voice portal (for example, standard voice mail access). BroadWorks is fully compliant to the IETF standards: • RFC 1939 (POP3) http://www.ietf.org/rfc/rfc1939.txt • RFC 2060 (IMAP4) http://www.isi.edu/innotes/rfc2060.txt.		POP3 or IMAP4 Server compliant with RFC1939 or RFC2060 respectively.

Capability	Customer provided offer component	Customer supplied component
If the enterprise's current email server does not have enough spare capacity for storage of voicemail messages Lucent can supply an additional message store server.	(Optional) Refer to *BroadWorks Recommended Hardware Guide* for suitable server.	
BroadWorks incorporates a translation service, which determines the type of a call between two directory numbers (DNs). The translation service makes use of a translation table for call typing built from the NPA-NXX Active Code List (NNACL), available from Telcordia Technologies, Inc. In case location based routing is to be used on the network server, an operator shall subscribe derive the NNACL file from the LERG files (also available from Telcordia). This is required to include the vertical and horizontal codes in the NNACL file.		It is the customer's responsibility to subscribe and receive updates to the NNACL file and LERG files. The customer must also ensure that the updated information is added to the network server. These are available from Telcordia Technologies Inc.

Capability	Customer provided offer component	Customer supplied component
SSL uses encryption technology so that the data between the server and the browser is not human readable. The web server creates an encrypted session to the web browser using a server key. As part of this session, a digital certificate is sent to the web browser by the web server, which identifies the web server as holding an SSL encryption key, and allows the web browser to decrypt the data coming from the server. If you are using the web server for public access (you have customers that connect over the Internet), you should get a signed certificate from a Certificate Authority. If you are only using BroadWorks internally on an Intranet or similar private network, you have to use self-signed certificates.		If you are using the web server for public access (you have customers that connect over the Internet), the customer is responsible for getting a signed certificate from a Certificate Authority.
If using private addressing, provision of analog line with modem for remote support via dial-up.		Analog line with modem.
If an external management system is required for maintaining the Feature Server 3000.	EMS Server including hardware	
For enhanced auto attendent, or if more than 500 CommPilot users are configured.	External Web Server	

Glossary

A

AC
Alternating Current

ALG
Application Layer Gateway

ALI
Automatic Location Identification

ANI
Automatic Number Identification

AS
Application Server

C

CDR
Call Detail Record

CDS
Call Detail Server

CPE
Customer Premises Equipment

D

DC
Direct Current

DND
Dialled Number Display

DNS
Domain Name System

DTMF
Dual Tone Multi Frequency

E

ESQK
Emergency Services Query Key

ESRN
Emergency Services Routing Number

EWS
External Web Server

F

FQDN
Fully Qualified Domain Name

FXO
Foreign Exchange Office

G

GUI
Graphical User Interface

I

IAD
Integrated Access Device

ICD
Internet Call Diversion

IMAP4
Internet Mail Access Protocol version 4

IVR
Interactive Voice Response

K

KPI
Key Performance Indicator

L

LAN
Local Area Network

M

MAC
Media Access Controller

MGCP
Media Gateway Control Protocol

MWI
Message Waiting Indicator

N

NAT
Network Address Translation

P

PAT
Port Address Translation

PBX
Private Branch Exchange

POP
Point of Presence

POP3
Post Office Protocol version 3

PSAP
Public Safety Answering Point

PSTN
Public Switched Telephone Network

Q

QoS
Quality of Service

R

RSYNC
Remote file Synchronization

RTP
Real Time Protocol

RTP
Real-time Transport Protocol

S

SBC
Session Border Controller

SCCP
Signaling Connection Control Part

SIP
Session Initiation Protocol

SNMP
Simple Network Management Protocol

SSL
Supplementary Service Layer

T

TAOS
True Access Operating System

V

VIP
Virtual IP Address

VoIP
Voice over IP

VPN
Vitual Private Network

VRRP
Virtual Router Redundancy Protocol

W

WAN
Wide Area Network

Index