



Avaya Agile Communication Environment Overview

Course number: 8672W

Student Guide

Part Number: 298-8672-031.06.01

Copyright © 2010 Avaya Inc. All Rights Reserved.

This document contains Avaya Inc. confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of Avaya Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing AVAYA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Contents

Welcome.....	5
Purpose.....	5
Resources.....	9
Navigation guidelines.....	11
Overview.....	13
Introduction.....	13
What is Avaya ACE?.....	15
Services and features summary.....	18
Benefits and differentiators.....	19
Module summary.....	21
Service-Oriented Architecture and web services.....	23
Introduction.....	23
Service-Oriented Architecture (SOA).....	24
Checkpoint.....	29
Web services.....	30
WSDLs.....	33
Supported web services.....	36
Parlay and Parlay X fundamentals.....	38
Checkpoint.....	39
Module summary.....	40
Architecture.....	41
Introduction.....	41
Design architecture.....	42
Basic deployment architecture.....	44
Federated (multi-regional) deployment architecture.....	46
Checkpoint.....	47
Module summary.....	49
Deployment guidelines.....	51
Introduction.....	51
Supported configurations.....	52
High availability network: Windows.....	54
High availability network: Linux.....	55
Security guidelines.....	56
Checkpoint.....	60
Module summary.....	61
Service provider integration.....	63
Introduction.....	63
Service provider fundamentals.....	65
Translation rules fundamentals.....	68
Media terminals.....	75
CS 1000 service provider fundamentals.....	77
Supported CS 1000 network configurations.....	78

CS 2000 service provider fundamentals.....	79
Supported CS 2000 network configurations.....	81
CS 2100 service provider fundamentals.....	82
Supported CS 2100 network configurations.....	83
MCS service provider fundamentals.....	84
Supported MCS 5100 and AS 5200 network configurations.....	86
Multimedia Conferencing service provider fundamentals.....	87
Supported Multimedia Conferencing network configurations.....	89
Contact Center/MLS service provider fundamentals.....	90
Supported Contact Center/MLS network configurations.....	92
Cisco Unified CM service provider fundamentals.....	93
Supported Cisco Unified CM network configurations.....	95
Tandberg VCS service provider fundamentals.....	96
Supported Tandberg VCS network configurations.....	98
Avaya service provider fundamentals.....	99
Supported Avaya network configurations.....	102
Checkpoint.....	104
Module summary.....	105
Operations, administration, and management.....	107
Introduction.....	107
OAM framework.....	108
Avaya ACE GUI overview.....	112
Configuration management.....	115
Fault management.....	119
Performance management.....	122
SNMP monitoring.....	123
Security and user management.....	126
Checkpoint.....	132
Module summary.....	134
Avaya ACE web services.....	135
Introduction.....	135
Supported web services.....	137
Application development.....	139
WSDL download.....	141
Checkpoint.....	142
Module summary.....	143
Avaya ACE applications.....	145
Introduction.....	145
Applications overview.....	147
Personal Assistant solution overview.....	149
Browser and Microsoft Office Add-ins solution overview.....	150
Message Drop and Blast solution overview.....	152
CEBP solution overview.....	153
AIE solution overview.....	155
AIE architecture.....	156

Hot Desking solution overview.....	157
Hot Desking and Sametime integration solution overview.....	159
Mobility application solution overview.....	160
Event Response Manager solution overview.....	162
Module summary.....	163
IBM Lotus Sametime integration.....	165
Introduction.....	165
IBM Lotus Sametime fundamentals.....	166
Supported network elements and telephony features.....	167
IBM Lotus Sametime integration guidelines.....	168
Telephony services for IBM Lotus Sametime.....	171
User profiles for IBM Sametime integration.....	178
Plug-in installation, configuration, and update.....	182
Hot Desking and Sametime integration solution overview.....	183
Checkpoint.....	184
Module summary.....	186
Microsoft Office Communications Server integration.....	187
Introduction.....	187
Microsoft OCS fundamentals.....	188
Avaya ACE and Microsoft OCS interworking.....	189
Microsoft OCS integration guidelines.....	192
Microsoft OCS telephony services.....	195
User profiles for Microsoft OCS integration.....	197
Microsoft OCS application integration.....	198
Checkpoint.....	199
Module summary.....	200
Hardware.....	201
Introduction.....	201
Avaya ACE on Linux platform hardware.....	202
Avaya ACE on Windows platform hardware.....	204
Module summary.....	205
Software and ordering.....	207
Introduction.....	207
Avaya ACE platform software.....	208
Software ordering and keycode management.....	210
Module summary.....	211
Customer support.....	213
Introduction.....	213
Documentation and online help.....	214
Global Services.....	216
Module summary.....	217
Case study.....	219
Introduction.....	219
Big Bank case study.....	220
Checkpoint.....	226

Module summary..... 228

Conclusion..... 229

Course summary..... 229

Welcome

Purpose

Purpose

Avaya Agile Communication EnvironmentTM (Avaya ACETM) is an open software platform for building multi-vendor Unified Communications (UC) and Communications Enabled Business Process (CEBP) applications. ACE provides both a developer-friendly tool kit for custom applications and a set of packaged applications that are easy to install and offer customers a hard dollar return on investment – often with an in-year payback.

Avaya ACE offers integration into common business applications such as Microsoft® Outlook, Internet Explorer, IBM Lotus Notes, Sametime and Microsoft® Office Communications Server 2007. It is targeted at the medium-to-large enterprise market with applications that deliver hard return on investment (ROI) savings across almost every vertical market.

Avaya Agile Communication Environment OverviewTM (8672W) provides a high-level description of the ACE solution, including its architecture, services and features, hardware, and software.

Prerequisites

There are no prerequisites for this product; however, a basic knowledge of voice and data communications is recommended.

Intended audience

This product is intended for anyone who requires basic knowledge of the Avaya ACE solution. This is an introductory-level product.

Avaya ACE 2.2

Features

The following features are new for this release. For more information, see the Avaya ACE™ documentation listed in the Resources section of the Welcome.

- **Planning and installation**
 - Procedure for defining MaxUserPorts registry key for Avaya ACE on Windows deployment
 - Ability to download software, such as Sametime Server plug-in (Telephony Provider), Sametime client plug-ins, Hot Desking, Message Drop and Blast, OCS ASA 32 bit, and OCS ASA 64 bit, from the Avaya ACE GUI (Help menu - Software Downloads)
 - **Important:** Single subnet configuration without segregation of high availability management traffic only supported for demos or trials with less than 250 users
- **Network elements**
 - Avaya service provider:
 - Support for Third Party Call Control (v2) (Avaya TR/87 or SIP service provider)
 - Call Notification (v3.2 and v3.8) for H.323 clients (Avaya TR/87 service provider)
 - Presence (Avaya TR/87 service provider)
 - Integration with Microsoft OCS - Beta
 - Avaya CS 2100 integration with IBM Lotus Sametime 8.0.2
 - Avaya Contact Center/MLS integration with Microsoft OCS - Beta
- **User administration**
 - Support for Calling Line ID in Avaya ACE user profile
- **Web services**
 - Text-to-Speech (TTS) service: Supports voice synthesis capabilities through AudioCall playTextMessage
- **Applications**
 - Application Integration Engine™ (AIE); Support for Secure Socket Layer (SSL)
 - Event Response Manager: Installed on AIE; supports automatic and manual team trigger of events
 - Hot Desking: AIE license required
- **Other enhancements**
 - Hot Desking (default CLI): Callers see user's normal desk phone when user is hot desked to a different device
 - Application Integration Engine™ (AIE); Support for Secure Socket Layer (SSL)
 - Mobility: Support for Avaya Aura™ and Cisco Unified Communication Manager
 - Browser and Office Add-ins:
 - Support for smart tags
 - Browser add-in support for Ajax extensions (for example, Google Map or Bing search)
 - Support for Avaya Aura™ and Cisco Unified Communications Manager



Tip

Beta-designated and controlled release software is currently under evaluation by select customers and implementation is subject to change, based on input from customer trials.

Objectives

After completing this course, you will be able to:

- Describe the Avaya ACE solution, including purpose, design, basic features and services, and benefits.
- Communicate about SOA and web services fundamentals.
- Describe the basic components that comprise the Avaya ACE architecture.
- Identify basic deployment guidelines for Avaya ACE, such as communications and network infrastructure requirements, supported configurations, and security.
- Identify integration guidelines for Avaya ACE network elements (service providers), including supported services, network configurations, configuration guidelines, and how the service provider interacts with Avaya ACE.
- Describe the operations administration and management (OAM) capabilities that Avaya ACE offers, including security, users and groups, fault management, and performance management.
- Identify the web services that the Avaya ACE supports, describe the basic steps for developing web-enabled application, and provide examples of commonly used application development tools and technologies.
- Describe the applications, add-ins, service extenders and communications-enabled applications and business processes (CEBP) that Avaya ACE supports, including their purpose and functionality.
- Describe the Unified Communications - IBM Sametime desktop integration capabilities that Avaya ACE supports.
- Describe the Microsoft OCS desktop integration capabilities that Avaya ACE supports.
- Identify and distinguish between supported configurations and baseline hardware for an Avaya ACE solution.
- Describe the Avaya ACE software ordering and license management process.
- Identify the types of help and support that Avaya ACE offers.
- Given customer requirements, identify deployment recommendations for an Avaya ACE solution.

Description

The systems and clients applicable for this course are listed below. For more information about other supported network elements, see *Agile Communications Environment - Administration* (NN10850-005).

- Avaya AuraTM
- Avaya Communication Server 1000 (Avaya CS 1000)
- Avaya Communication Server 2000 (Avaya CS 2000)
- Avaya Communication Server 2100 (Avaya CS 2100)
- Avaya Multimedia Communication Server 5100 (Avaya MCS 5100)
- Nortel Application Server 5200 (AS 5200)
- Avaya Interactive Communications Portal (Avaya ICP)
- Avaya Media Conferencing
- Avaya Media Application Server (Avaya MAS)
- Avaya Contact Center/Meridian Link Services (MLS)
- Cisco Unified Communications Manager - sometimes referred to as Cisco Call Manager (CCM)
- Tandberg Video Communication Server (VCS) and Tandberg clients
- IBM Lotus Sametime, IBM Lotus Notes, and IBM Sametime Connect client
- Microsoft Office Communications Server (OCS) and Microsoft Office Communicator

Resources

Resources

Avaya ACE core documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Fault and Performance Management* (NN10850-009)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)
- *Administration - Microsoft Office Communications Server Integration* (NN10850-012)
- *Alarms Reference* (NN10850-015)
- *Audit Log Reference* (NN10850-016)
- *Performance Measurement Reference* (NN10850-017)
- *Error Messages Reference* (NN10850-018)

Resources

Avaya ACE applications documentation:

- *Personal Assistant Application* (NN10850-032)
- *Message Drop and Message Blast Administration* (NN10850-025)
- *Hot Desking User Guide* (NN10850-030)
- *Hot Desking Application Installation Guide* (NN10850-035)
- *Hot Desking Mobile Interface Guide* (NN10850-036)
- *Hot Desking Administration Guide* (NN10850-037)
- *Hot Desking Application Web Portal Integrator Guide* (NN10850-038)
- *Hot Desking Application for Sametime Connect User Guide* (NN10850-046)
- *Avaya Application Integration EngineTM Fundamentals* (NN10850-021)
- *Mobility Application Administration* (NN10850-027)
- *Mobility Application for BlackBerry* (NN10850-028)
- *Event Response Manager Installation* (NN10850-048)

Avaya ACE on Linux:

- MySQL database, www.mysql.com
- Red Hat Linux, www.redhat.com
- Red Hat Cluster Suite, <http://www.redhat.com/docs/manuals/csgfs>

Avaya ACE on Windows:

- MySQL database, www.mysql.com
- Microsoft operating system, www.microsoft.com
- JBoss Enterprise Application Platform, www.jboss.com
- rsync features or functionality, www.samba.org/rsync

Unified Communications desktop integration:

- IBM Lotus Sametime, www.ibm.com
- Microsoft Office Communications Server, www.microsoft.com
- Firefox add-in Regular expressions tester 3.0

Navigation guidelines

Web navigation

Web navigation guidelines are listed below.

- Content is divided into the modules, which display in the contents tree on the left side of the page.
- Navigation controls appear on the menu bar at the top of the page.
- To launch a module, click its title in the tree.
- To access a topic, click its title.
- Use the controls at the topic of the page to move navigate through the product (forward, back, etc.).



Tip

This product includes links to external content, such as demos and web sites. Click the link to access a selected item. After completing your review, close the window to return to the information product.

Overview

Introduction

Purpose

This module provides an overview of the Avaya Agile Communication Environment™ (Avaya ACE™) solution, including its design, benefits, services, and features.

Objectives

After completing this module, you will be able to:

- Describe the Avaya ACE solution.
- Describe Avaya ACE services and features.
- Identify benefits and differentiators of ACE.

Resources

Avaya ACE core documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Fault and Performance Management* (NN10850-009)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)
- *Administration - Microsoft Office Communications Server Integration* (NN10850-012)
- *Alarms Reference* (NN10850-015)
- *Audit Log Reference* (NN10850-016)
- *Performance Measurement Reference* (NN10850-017)
- *Error Messages Reference* (NN10850-018)

Resources

Avaya ACE applications documentation:

- *Personal Assistant Application* (NN10850-032)
- *Message Drop and Message Blast Administration* (NN10850-025)
- *Hot Desking User Guide* (NN10850-030)
- *Hot Desking Application Installation Guide* (NN10850-035)
- *Hot Desking Mobile Interface Guide* (NN10850-036)
- *Hot Desking Administration Guide* (NN10850-037)
- *Hot Desking Application Web Portal Integrator Guide* (NN10850-038)
- *Hot Desking Application for Sametime Connect User Guide* (NN10850-046)
- *Avaya Application Integration EngineTM Fundamentals* (NN10850-021)
- *Mobility Application Administration* (NN10850-027)
- *Mobility Application for BlackBerry* (NN10850-028)
- *Event Response Manager Installation* (NN10850-048)

What is Avaya ACE?

Description

Avaya ACE is an open software platform for building multi-vendor Unified Communications (UC) and Communications Enabled Business Process (CEBP) applications.

Avaya ACE leverages a Service-Oriented Architecture (SOA) programming philosophy to offer services as modular, non-proprietary building blocks. This simplified service-based architecture facilitates clients access into more complex networks and systems. This provides the capability to combine and link services, without worrying about the underlying architecture or technology; for example:

- Connection types
- Protocols
- Operating systems



Key areas

Two key areas that Avaya ACE addresses are described below.

Unified Communications (UC) desktop integration

Avaya ACE supports tight integration with popular third party communications systems, such as IBM Lotus Sametime and Microsoft Office Communications Server (OCS).

UC desktop integration offers enhanced user communications and business effectiveness; for example, a single communications interface and aggregated (consolidated) presence for multiple network devices, including voice, video, chat, and other applications.

Communications-Enabled Applications and Business Processes (CEA/CEBP)

Avaya ACE offers communications capabilities, such as Click-to-Call, Audio Call, Video Call, Location and Presence, as open and vendor-neutral building blocks. This design enables simple and rapid integration in the customer's existing network infrastructure to create Communications-Enabled Applications and Business Processes (CEA/CEBP).

Avaya ACE also offers the ability to combine/link services with logic to meet specific business needs; for example, supply management, corporate directory and web portals, and alerts/event notifications.

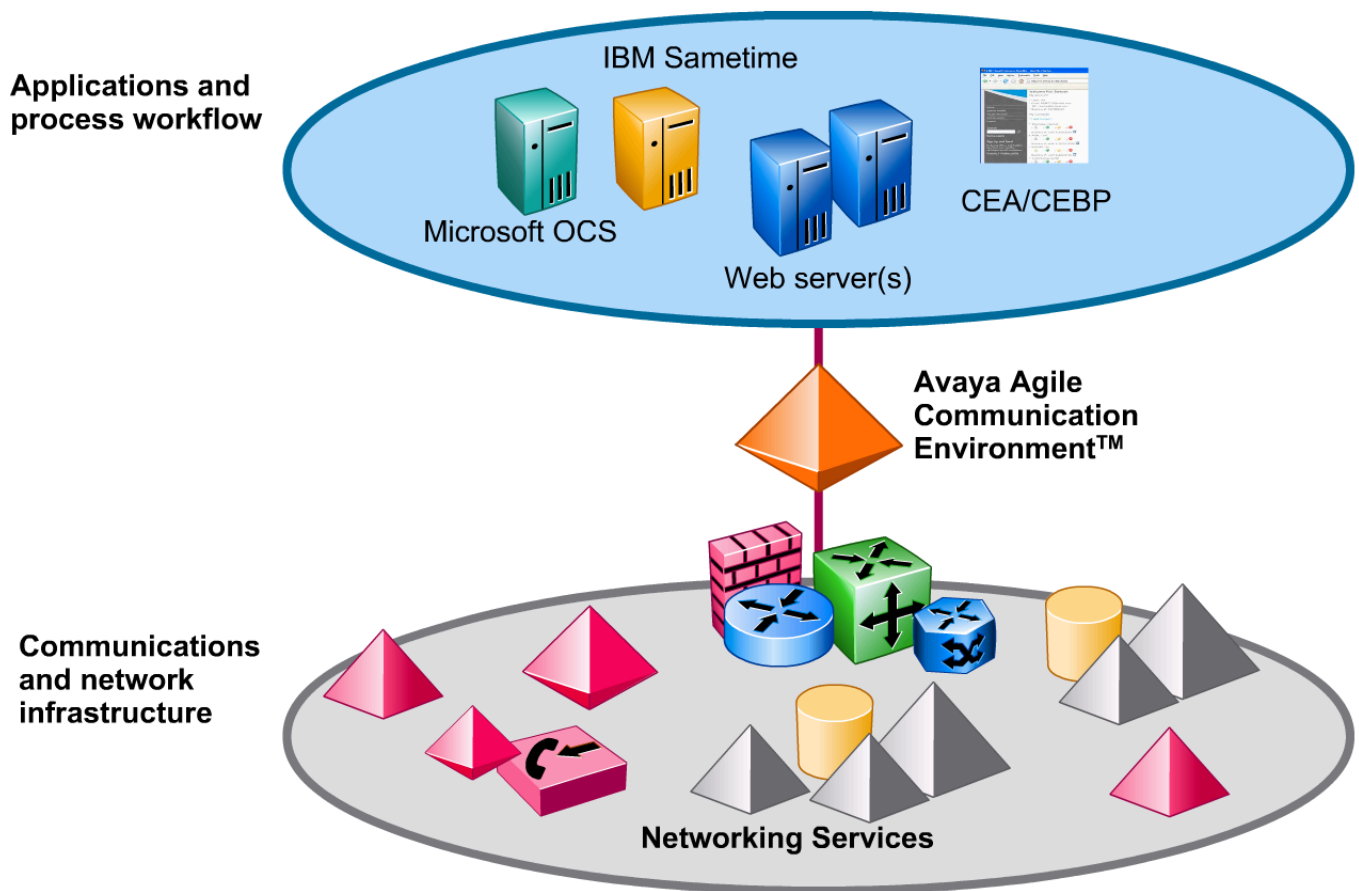
Where Avaya ACE Lives

Avaya ACE sits between an application layer and communications and network service infrastructure, providing a bridge between the two.

The application layer includes SOA-based web services available to clients that are hosted in either a private or a public network. The clients invoke web services through web-based applications and processes.

The communications and network services infrastructure includes call servers and systems, including Private Branch Exchange (PBX) and Internet Protocol/SIP-based systems, that deliver communication services. Within Avaya ACE, these are also known as network elements.

Bridging the application layer and communications and network service infrastructure



Tip

Requests from the Application layer are referred to as coming from the **Web Services** interface. This is sometimes known as **Northbound**.

Requests from the Communications and network services infrastructure are referred to as coming from the **Service Provider** interface. This is sometimes known as **Southbound**.

Services and features summary

Description

Architecture

Avaya ACE is hosted on a non-proprietary, commercially available hardware platform. It offers flexible and scalable deployment options, including standalone and redundant (standby) configurations. Linux and Windows operating systems are supported.

OAM

The Avaya ACE operations administration and management (OAM) framework includes a web-based interface for system administration, configuration, fault management, performance management, and user management. Avaya ACE also integrates with popular third-party management systems, such as HP OpenView.

Unified Communications (UC) integration

Avaya ACE supports integration and application customization for popular communications systems, such as IBM Lotus Sametime and Microsoft Office Communications Server, for consistent user experience and group collaboration.

Web services

Avaya ACE provides modular, non-proprietary web service application programming interfaces (APIs) that simplify development, customization, and integration into existing network infrastructure. Example services include: Third Party Call Control, Audio Call, Video Call, Call Notification, Multimedia Conference, Presence, Subscriber Management, Third Party Call Extensions, Remote Call Control, and more.

Value add applications, add-ins, and service extenders

Avaya ACE interworks with a wide range of value add applications, add-ins, and service extenders to offer enhanced communications offerings, such as Browser and Microsoft Add-ins, Hot Desking, Mobile Cost Optimizer, and Event Response Manager.

Communications-enablement solutions

By leveraging Avaya ACE services, customers can communications-enable applications and business processes (CEBP); for example, offer click-to-call and presence from a corporate directory and sales portal.

Customer support

Avaya ACE includes a suite of technical documentation, references, and guides, as well as a comprehensive online help system. A partnership and alliance with industry leaders, such as IBM and Microsoft allow customers to accelerate the evolution of next-generation technologies. Global professional services offer a suite of services, including enablement, deployment, application development, and consultancy.

Benefits and differentiators

Benefits

Avaya ACE enables customers to improve business agility by removing delay from people-dependant business processes and by reducing the time associated with repetitive tasks. For example, typical workflows require review, validation and approval as they proceed and in many cases these steps are disjointed and introduce latency. ACE can communications-enable these processes in a way that drives out latency, resulting in reduced business costs and improved customer responsiveness.

Key benefits are:

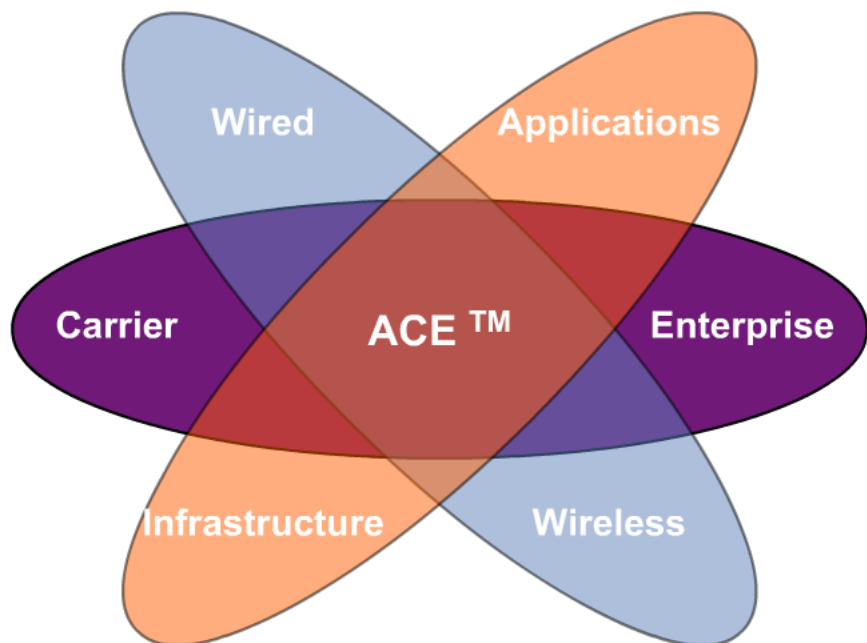
- Improved business agility, with ability to react to changes and implement them quickly
- Improved customer/supplier relationships (CRM/SCM) and faster time to market and to revenues
- Reduced operating and capital expenditures
- Richer communication and collaboration experience and employee and group effectiveness
- More engaging customer service (often integrated into a business process)
- Reduced human delays

Differentiators

Key differentiators are:

- Cross-domain alignment: Allows enterprises and carriers to not only address their domain opportunities but also create new cross-domain opportunities.
- Vendor neutral: Supports multi-vendor interoperability and improves business agility, accuracy, and speed and maximizes return on investment.
- Real-time orchestration: Facilitates events-driven communications where the event can be triggered by a business process.
- Toolkit solution: Allows businesses to purchase selected service capabilities and modify the services to meet their own needs, using standard application development tools.

Cross-domain alignment simplifies the path to communications-enabled applications and business processes.



Module summary

Objectives

In this module you have learned how to:

- Describe the Avaya ACE solution.
- Describe Avaya ACE services and features.
- Identify benefits and differentiators of ACE.

Service-Oriented Architecture and web services

Introduction

Purpose

Avaya Agile Communication Environment™ (Avaya ACE™) supports a Web Service approach in compliance with open Service-Oriented Architecture (SOA) frameworks and development environments to facilitate the development of communications enabled applications. This module reviews basic SOA and web services concepts and terminology.

Objectives

After completing this module, you will be able to:

- Describe the Service-Oriented Architecture (SOA) programming philosophy, as well as how Avaya ACE fits into a SOA.
- Describe basic web services concepts, including definition and standards.
- Define Web Service Description Language (WSDL), and identify important WSDL attributes.
- Describe the web services that Avaya ACE supports.
- Communicate about Parlay and Parlay X, including purpose and related standards organizations.

Resources

Avaya ACE documentation:

- *Web Services* (NN10850-007)

Service-Oriented Architecture (SOA)

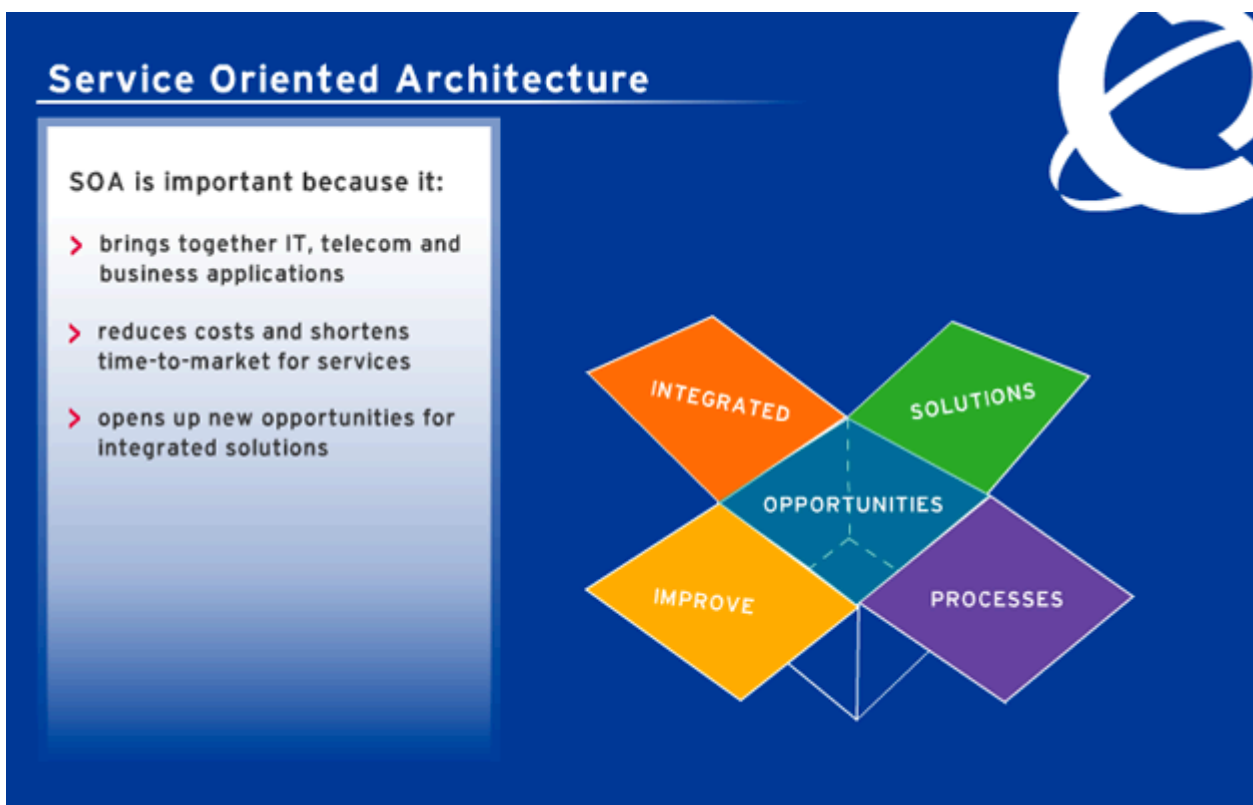
Overview

Service-Oriented Architecture (SOA) is a programming philosophy that uses loosely coupled services and components. It is evolutionary in terms of its distributed computing approach (software running on multiple platforms) and modular programming style (building blocks of functions or services).

Traditionally, vendors develop products by combining multiple capabilities into a single system. A private branch exchange (PBX), for example, often includes voice services, voice mail, audio conferencing, and contact center functionality, which are often based on proprietary hardware or software. These telephony services are not easily integrated with external business applications and processes.

In an SOA environment, services are modular and can be combined, assembled, and sequenced in different ways. This design reduces time-to-market and opens new opportunities for integrated solutions. Interactions are self-contained and independent. This friction-free relationship is referred to as **loose coupling**, a trademark of a SOA.

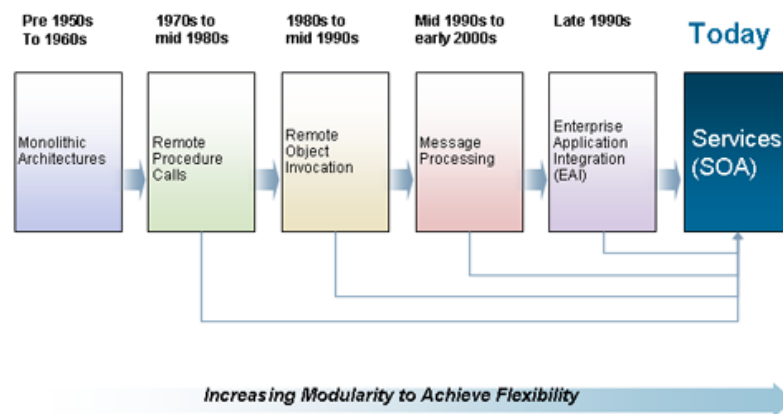
Benefits of a SOA



Software architectural evolution

To understand the SOA programming philosophy, it is helpful to understand how the software programming architecture has evolved to what we have today.

- Monolithic architecture: Software originally was built with monolithic architectures that were all encompassing and proprietary.
- Breaking up of software into components: Moving forward, we saw the breaking up of software into components; for example, Remote Procedure Calls, Remote Object Invocation, Message Processing, and Enterprise Application Integration (EAI).
-



OASIS SOA reference model

has adopted the terminology in the SOA reference model issued by the Organization for the Advancement of Structured Information Standards (OASIS). OASIS is a not-for-profit consortium whose focus is on advancing open, global information standards. For more information, go to www.oasis-open.org.

OASIS states: "Service Oriented Architecture (SOA) represents a collection of best practices principles and patterns related to service-aware, enterprise-level, distributed computing. SOA standardization efforts at OASIS focus on workflows, translation coordination, orchestration, collaboration, loose coupling, business process modeling, and other concepts that support agile computing."

Key OASIS terms

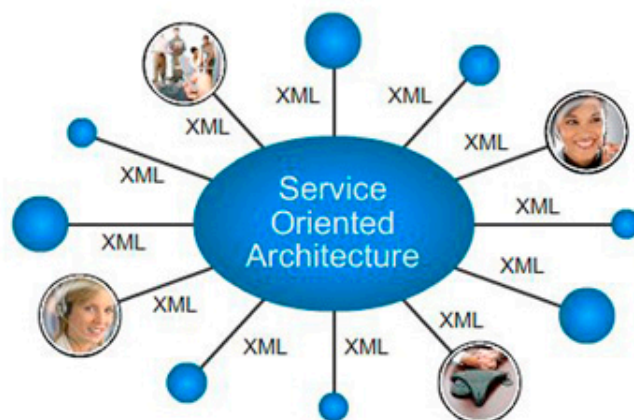
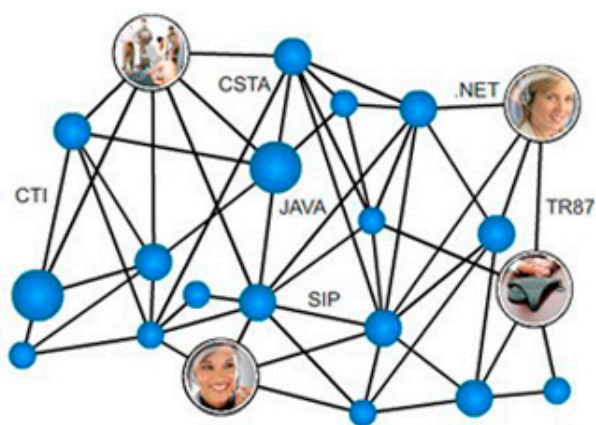
- **Service:** A capability together with its specification, contract, and real-world effect is known as a service. Typically, services are implemented separately from a wrapper, which adds the necessary security to them.
- **Providers and consumers:** In the OASIS terminology, SOAs are centered on providers that offer capabilities (sometimes called enablers). When a service consumer invokes one of these capabilities through an interaction with the provider, a real-world effect occurs. A real-world effect is the actual result of using a service, not just the capability that the service provider offers.
- **Service participants:** Service providers and service consumers are together known as service participants.
- **Exposed service:** The term exposed service is sometimes used to represent an implemented service and wrapper. Service providers must make their services visible to allow potential consumers to discover them. They do this by publishing (exposing) a service description containing information about three aspects of the service:
 - Its behavior
 - Its interface
 - Its policies and contracts
- **Orchestrated service:** Once a service has been made visible, it can be combined with other visible services to create a higher-level service. Orchestration is the process of organizing a sequence of web services into a business flow to implement a higher-level functionality.
- **Choreography:** In addition to orchestration, new higher-level services can be created from simpler ones through choreography. Although there are several differences between orchestration and choreography, the primary outward difference lies in where the state of the flow is held: in the case of orchestration, it is held in a central controller. In the case of choreography, it is held in each invoked service.

How ACE fits into a SOA

A SOA is just a programming style or architecture. You cannot buy a SOA.

ACE is designed to fit seamlessly into a SOA. The SOA provides the framework for services. It also provides the mechanisms for services to discover and communicate securely with each other. Through this model, ACE enables business applications to integrate with communications capabilities.

ACE operates seamlessly with most Enterprise Service Bus (ESB) types but, as it already provides a web services interface, it does not require an ESB to operate.



Enterprise Service Bus

When the SOA standards were developed, it was anticipated that Information Technology (IT) departments deploying the SOA components would have legacy services that did not meet the SOA interface standards. An Enterprise Service Bus (ESB) technology was necessary for interoperability.

An ESB provides two functions:

- It accepts legacy interfaces and normalizes them, typically to web services, the most commonly used interface within a SOA.
- It provides simple orchestration; for example: Invoke Service A. If the result is acceptable, then pass its output to Service B. If the results are not acceptable, invoke Service C.

Business coordination languages, such as Business Process Execution Language (BPEL), are used for more sophisticated orchestrations, although the expressive power of some of the more complex ESBs is encroaching on some of the least able coordination engines. If all the deployed services offer interfaces compatible with the SOA (typically web service interfaces) and orchestration is handled either in a coordination engine or an ad hoc manner, then there is no requirement to deploy an ESB.

Checkpoint



SOAs are centered on service providers that offer capabilities (sometimes called enablers). When a service consumer invokes one of these capabilities through an interaction with the provider, a real-world effect occurs.

_____ True

_____ False

Answer : True



Service orchestration is the same as service choreography. The terms are synonymous.

_____ True

_____ False

Answer : False



Providers make their services visible to potential consumers by:

_____ Wrapping the service

_____ Binding the service

_____ Exposing the service

Answer : Exposing the service

Web services

Overview

Web services are application programming interfaces (APIs) that enable interoperability between applications on different hardware and software platforms. Web services are invoked over a data network connection by another application, (even a loopback/local connection within a machine) where the services requested are hosted on a remote system.

Web standards

Web services are governed by web standards (rules) for information exchange. Some examples are listed below.

- **Extensible Markup Language (XML):** General-purpose specification for creating custom markup languages
- **Hypertext Transfer Protocol (HTTP):** Client/server protocol for linking text files to one another to share information on the Internet and the World Wide Web (WWW)
- **Web Service Description Language (WSDL):** XML format for describing Web services; provides common language for entities to interact
- **SOAP** (originally defined as Simple Object Access Protocol): Protocol specification for exchanging structured information in the implementation of Web Services in computer networks that relies on eXtensible Markup Language (XML) as its message format and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission
- **Representational State Transfer (REST):** Specification for exchanging self-describing resource representations over HTTP without an additional messaging layer

Web service attributes

Some key attributes associated with a web service are:

- **Platform/language-independent:** Has well defined platform-independent and language-independent interfaces used to accept requests and to deliver service responses
- **Loosely coupled:** Operates in a loosely coupled unit that operates independently of other services
- **Business functionality:** Represents a high level business functionality; for example, getAccountBalance

Description

Web services technologies are standardized by organizations. Some key organizations are listed below.

- Distributed Management Task Force, Inc. (DMTF): The DTMF focuses on common management infrastructure components for enterprise and Internet environments. For more information, go to www.dmtf.org
- European Telecommunications Standards Institute (ETSI): The ETSI publishes global information and communications standards for fixed, mobile, radio, converged, broadcast and internet technologies. For more information, go to www.etsi.org .
- Organization for the Advancement of Structured Information Standards (OASIS): OASIS focuses on the development and standardization of open standards for Web services, security, and e-business. For more information, go to www.oasis-open.org.
- The Parlay Group: Focuses on the development open application programming interfaces (APIs) to simplify the creation of web services. For more information, go to www.parlayx.com.
- Third Generation Partnership Project (3GPP): Consists of standards organizations who have partnered to develop specifications for evolved third generation and beyond mobile system. For more information, go to www.3gpp.org.
- World Wide Web Consortium (W3C): Focuses on technologies that support interoperability across the web. For more information go to www.w3.org.

SOAP and REST services

Avaya ACE leverages two types of application programming interfaces (APIs) to deliver web services: SOAP and REST.

- SOAP: The description of a service is written in a Web Services Description Language (WSDL), and the XML messages are wrapped by XML-envelopes conforming with the SOAP specification.
- REST: Each system resource is identified by an Universal Resource Identifier (URI), upon which a handful of basic, standard operations can be performed using the GET, POST, PUT, and DELETE operations of the HTTP protocol.

Major Differences between SOAP and REST

Major Differences between SOAP and REST are discussed below.

- SOAP exchanges XML documents. Things that can't be expressed in XML (for example, recorded speech) travel as document attachments. REST exchanges self-describing resource representations, such as MIME (Multipurpose Internet Mail Extensions) types.
- SOAP uses WSDL to define the data structures to be exchanged. If the data structure changes, then both the consumer and provider must be changed. This means some measure of coupling. REST can make use of the HTTP header to indicate the formats it can accept.
- SOAP supports an unlimited number of verbs that are defined as part of the WSDL; for example: "Here is a document. Count the words in it. Here is a document. Translate it into French." In contrast, REST simply exchanges representations of the data and the endpoint to which requests are sent defines the action to be taken.

WSDLs

WSDLs defined

Each web service has a corresponding Web Service Description Language (WSDL). The WSDL contains the message definitions and syntax necessary for dissimilar entities to communicate.

As defined by the World Wide Web Consortium (W3C), a WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services).

The WSDL does not include any of the semantics of the web service; for example, what the service actually does. While users can read a WSDL, the WSDL format is really designed for simple parsing by a computer program. Application developers typically use a tool within their development environments to analyze the WSDL.

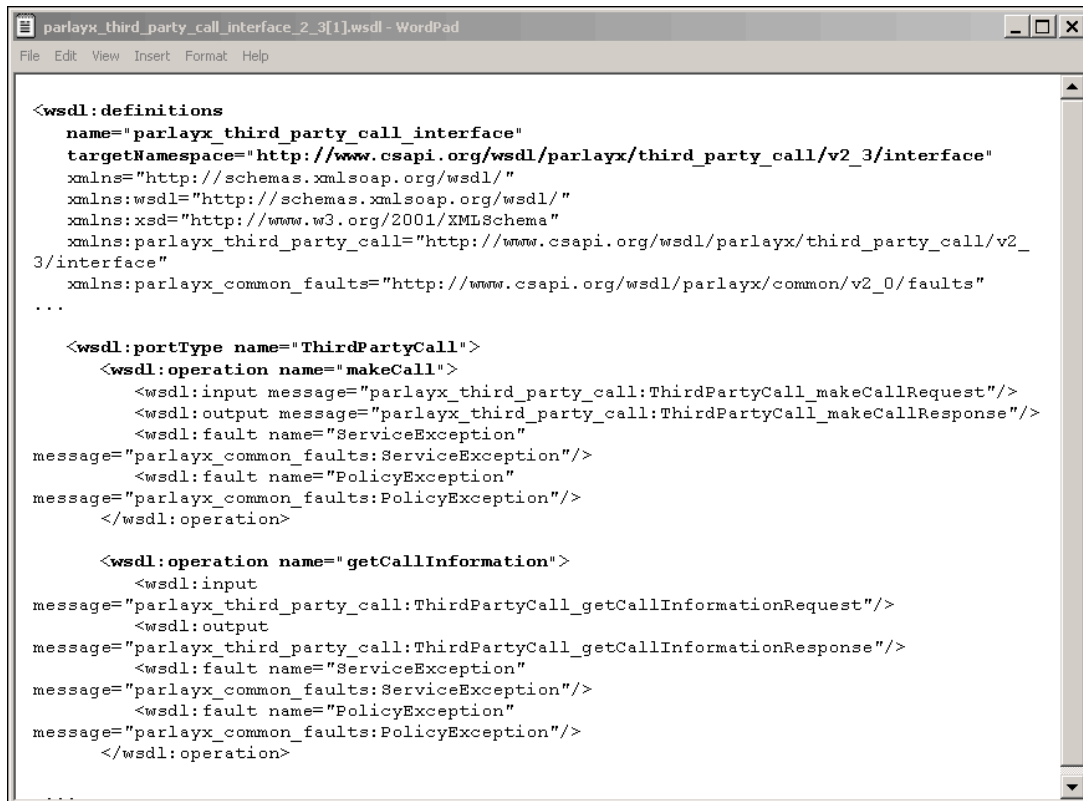
Important WSDL attributes

Some important WSDL attributes are:

- **Target namespace:**
 - Is similar to an XML schema target namespace.
 - Requires absolute URI; for example, a web site that is within the service provider's control.
- **Operations:**
 - Describes a web service's functionality as a set of abstract operations.
 - Each operation specifies the types of messages that the service perform as part of that operation.
- **Message:**
 - Includes the information needed to perform the operation; typically, corresponds to an operation.
- **Service definition:**
 - Specifies the supported interface attribute. (A service is only allowed one interface.)
- **Binding:**
 - Defines Fully Qualified Domain name of the server, as well as where the service is found on the server.
 - Specifies concrete message format; for example, SOAP. Defines underlying transmission protocol; for example, HTTP.
- **Port Type:**
 - Specifies what services the web service can provide; for example, a web service might provide various services on documents containing English-language text, translating the text into another language, counting the words in the text, checking the spelling of the text, etc. Each of these services would be defined as a separate **port** on the web service.
- **Operation Type:**
 - Specifies how the service operates.
 - **Request-response:** The is the most common operation type. The web service accepts a request and returns a response; for example, accepts text in English and returns a list of spelling mistakes.
 - **One-way:** Accept a request and return nothing; for example, a logging service.
 - **Notification:** Supports unsolicited messages from a web service. The web service spontaneously generates and delivers a message to a client but does not expect a response; for example, alerts a consumer if some event occurred.
 - **Solicit-response:** Service spontaneously sends a message to its consumer, as with the notification operation type, but also expects a response.
- **Messages:**
 - Are transmitted during the invocation of a web service. Depending on the operation type of the port, one or more messages are transmitted during the invocation of a web service; for example, if this is a request-response type, the consumer sends a message to the port and the web service responds with a message.

Inside a WSDL

Following is an excerpt from a Third Party Call (v2) WSDL interface file, which is available for download from the Avaya ACE GUI. It is important to note that while users can **read** a WSDL, the WSDL format is really designed for simple parsing by a computer program.



```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions
  name="parlayx_third_party_call_interface"
  targetNamespace="http://www.csapi.org/wsdl/parlayx/third_party_call/v2_3/interface"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:parlayx_third_party_call="http://www.csapi.org/wsdl/parlayx/third_party_call/v2_3/interface"
  xmlns:parlayx_common_faults="http://www.csapi.org/wsdl/parlayx/common/v2_0/faults"
  ...

  <wsdl:portType name="ThirdPartyCall">
    <wsdl:operation name="makeCall">
      <wsdl:input message="parlayx_third_party_call:ThirdPartyCall_makeCallRequest"/>
      <wsdl:output message="parlayx_third_party_call:ThirdPartyCall_makeCallResponse"/>
      <wsdl:fault name="ServiceException"
        message="parlayx_common_faults:ServiceException"/>
      <wsdl:fault name="PolicyException"
        message="parlayx_common_faults:PolicyException"/>
    </wsdl:operation>

    <wsdl:operation name="getCallInformation">
      <wsdl:input
        message="parlayx_third_party_call:ThirdPartyCall_getCallInformationRequest"/>
      <wsdl:output
        message="parlayx_third_party_call:ThirdPartyCall_getCallInformationResponse"/>
      <wsdl:fault name="ServiceException"
        message="parlayx_common_faults:ServiceException"/>
      <wsdl:fault name="PolicyException"
        message="parlayx_common_faults:PolicyException"/>
    </wsdl:operation>
  </wsdl:portType>
  ...
</wsdl:definitions>
```

Supported web services

Supported web services

Avaya ACE supports selected Parlay X Version 2 and Version 3 web services and custom services. Parlay X Version 3 consists of functional updates to existing Parlay X Version 2 web services, and the addition of new web services. Supported services are:

- **Third Party Call Control (v2):** Provides click-to-call functionality between two endpoints.
- **Third Party Call Control (v3):** Initiates and manages a single- call or multiple-party calls through a call server.
- **Call Notification (v3):** Allows an application to manages call notification functionality, such as called party address and number for Third Party Call Control (v2/v3) sessions.
- **Call notification (v3.8):** Allows an application to receive an event each time a user's terminal device is called, containing the number of the party attempting to place the call.
- **Call Forwarding:** Allows a device to redirect an incoming call to another device when specific conditions are met.
- **Call History:** Allows an application to instruct the Avaya ACE host to create and store records for incoming calls for retrieval by address or user name (user ID).
- **Terminal Location (v3):** Retrieves location information about a mobile terminal and supports queries from applications to trigger other events.
- **Location Supplier:** Allows a device to publish location information to a terminal device.
- **Audio Call (v3):** Allows an application to add or drop audio content in an existing call, and monitor message delivery.
- **Multimedia Conference web service (v.3):** Allows an application to create multimedia conferences and dynamically manage the participants involved.
- **Presence:** Collects presence information for users registered with one or more network elements.
- **User profile:** Supports user management operations, including operations related to the management of global security policies and individual user group policies. It is included automatically and enabled by default.
- **System monitoring:** Allows a service client to monitor the health of applications.
- **Subscriber Management:** Allows client applications to query subscriber information either locally or globally for federated deployments.
- **Third Party Call Extensions:** Allows an application to support Third Party Call Control (v2) call sessions and call sessions placed through the CS 1000 TR/87 network element.
- **Message Drop and Message Blast:** Automates voice recording and broadcasting of audio messages to specified recipients.

Authentication and authorization

Access to Avaya ACE is controlled using HTTP 1.1 basic authentication. Requests must contain a valid user name and password that correspond to a user profile configured in Avaya ACE.

Authorization for individual web services is configured on a service-by-service basis. The user account configured for the web service client (application) must have the appropriate access control rules set to invoke a particular web service.

Secure web service communication

By default, web service communication is supported on the secure (HTTPS) and non secure (HTTP) ports. A consumer of a web services can choose to completely secure all web service communication (including notifications).

Important: For secure communication, ensure that the Avaya ACE version and the ports on the host server match. To establish secure-only communication with the Avaya ACE host, you must explicitly disable the nonsecure ports. For high availability (HA) deployments, perform this procedure on both hosts.

Parlay and Parlay X fundamentals

Parlay and Parlay X

The Parlay Group was founded in 1998 and is a multi-vendor consortium formed to develop open, technology-independent application programming interfaces (APIs) that enable the development of applications that operate across multiple, networking-platform environments.

Parlay/Open Services Architecture (OSA) APIs were designed to be independent of the underlying networking technology. The goal of this design was to enable service creation by application developers, rather than programming experts.

The first Parlay/OSA APIs were feature rich but complex. To make functionality more accessible to application developers, Parlay X Web Services APIs were released in 2003. Parlay X Web Services specify a suite of API specifications for telecom services, such as: call control, conferencing, and user interaction (audio and text messaging).

The Parlay X Web Services APIs are defined jointly by:

- European Telecommunications Standards Institute, ETSI
- Parlay Group
- Third Generation Partnership Program, 3GPP

Source: Wikipedia, the free encyclopedia

Checkpoint



A WSDL provides the common language necessary for dissimilar entities to interact.

_____ True

_____ False

Answer : True



The most common WSDL operation type is Request-Response.

_____ True

_____ False

Answer : True

Module summary

Objectives

In this module you learned how to:

- Describe the Service-Oriented Architecture (SOA) programming philosophy, as well as how Avaya ACE fits into a SOA.
- Describe basic web services concepts, including definition and standards.
- Define Web Service Description Language (WSDL), and identify important WSDL attributes.
- Describe the web services that Avaya ACE supports.
- Communicate about Parlay and Parlay X, including purpose and related standards organizations.

Architecture

Introduction

Purpose

Avaya Agile Communication Environment™ (Avaya ACE™) is a software solution that is deployed in the customer's existing network infrastructure. Avaya ACE operates on a non-proprietary server platform, which offers flexible configurations and deployment scenarios.

This module provides an overview of the components that comprise the Avaya ACE architecture.

Objectives

After completing this module, you will be able to:

- Identify the main design components of the Avaya ACE design architecture: adapters, Service-Oriented Architecture (SOA) services and composites, and application programming interfaces (APIs).
- Identify the key components in a basic Avaya ACE deployment architecture.
- Identify the basic components in an Avaya ACE multi-regional (federated) architecture.

Resources

Avaya ACE documentation:

- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *ACE Integration Engine Fundamentals* (NN10850-021)

Design architecture

Abstraction layer

Avaya ACE is designed to act as an abstraction layer between business applications and the customer network to deliver simple communications-enablement. Avaya ACE does this through three main design components.

- Adapters (special interfaces)
- SOA services and composite services
- Web service application programming interfaces (APIs)



Examples of adapters

Adapters (special interfaces) enable communications between the customer's existing network elements (call servers, communications systems, video servers, etc.) and Avaya ACE.

Avaya ACE provides adapters for many system types, such as the ones listed below. See *Agile Communication Environment Administration* (NN10850-005) for a complete list of supported adapters.

- Avaya Aura™
- Communication Server 1000 (CS 1000)
- Communication Server 2000 (CS 2000)
- Communication Server 2100 (CS 2100)
- Multimedia Communication Server 5100 (MCS 5100)
- Application Server 5200 (AS 5200)
- Contact Center/Meridian Link Services (MLS)
- Cisco Unified Communications Manager (Cisco Unified CM)
- Tandberg Video Communication Server (VCS)
- IBM Lotus Sametime

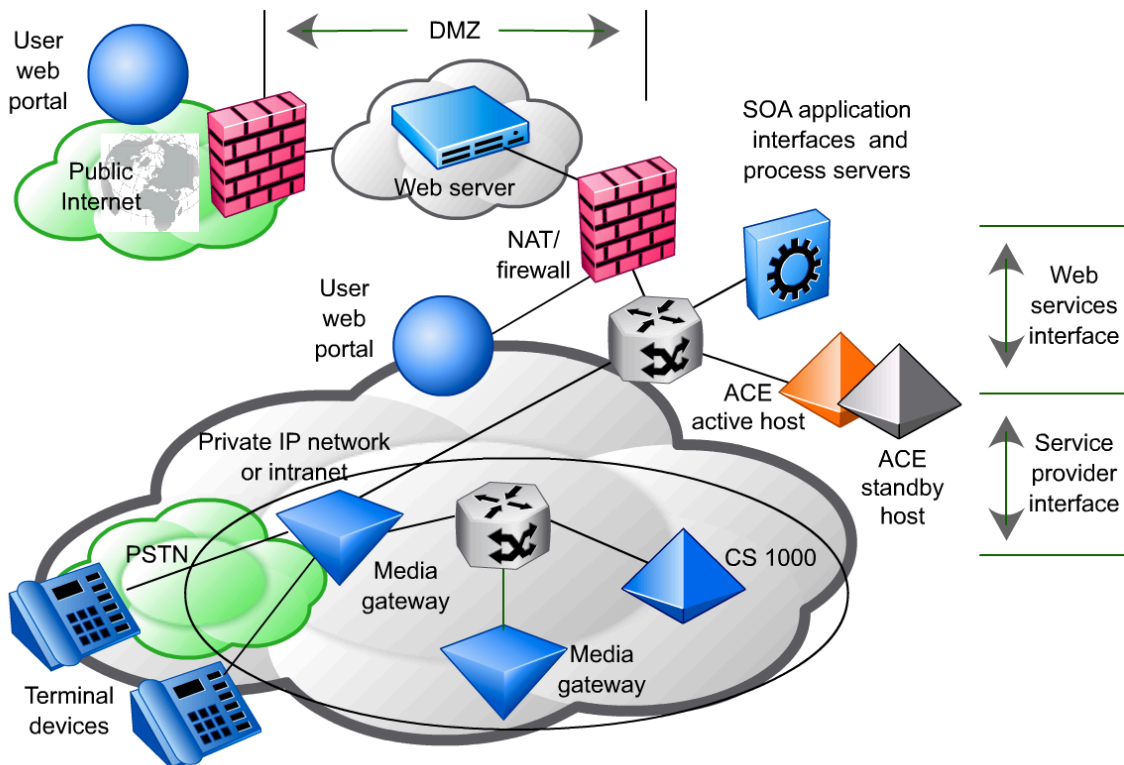
Basic deployment architecture

Description

Avaya ACE is integrated in the customer's existing network infrastructure. The components in a basic Avaya ACE deployment architecture are:

- Avaya ACE Linux or Windows host, which is standalone or optionally available in a high availability (HA) configuration (active and standby host)
- Interfaces and call control protocols, which enable network elements to communicate
- Network elements that provide the telephony services invoked through the Avaya ACE adapters
- Customer-supplied web servers, typically installed within a demilitarized zone (DMZ) to protect customer resources from unauthorized access

Example deployment architecture



Interfaces and call control protocols

Avaya ACE interfaces and call control protocols enable network elements to communicate.

- **Web services interface:** Connects the web clients to Avaya ACE and carries traffic containing SOA service requests. Requests are not constrained to those initiated by clients. Network servers can also initiate requests; for example, when the Presence service is available from Avaya ACE and a monitored client changes its state, a network server notifies Avaya ACE of the change.
- **Service provider interface:** Connects with supported network elements that provide the enhanced IP telephony services.
- **Call control protocols:** Some services require a specific call control protocol. ACE supports combinations of web service operations, network elements, and call control protocols, such as:
 - Session Initiation Protocol (SIP)
 - Computer Telephony Integration (CTI) TR/87
 - Java Telephony Application Programming Interface (JTAPI)
 - Virtual Places (VP)



Tip

Requests from the web clients (SOA service requests) are referred to as coming from the **Web Services interface**.

Requests from the supported network elements are referred to as coming from the **Service Provider interface**.

Federated (multi-regional) deployment architecture

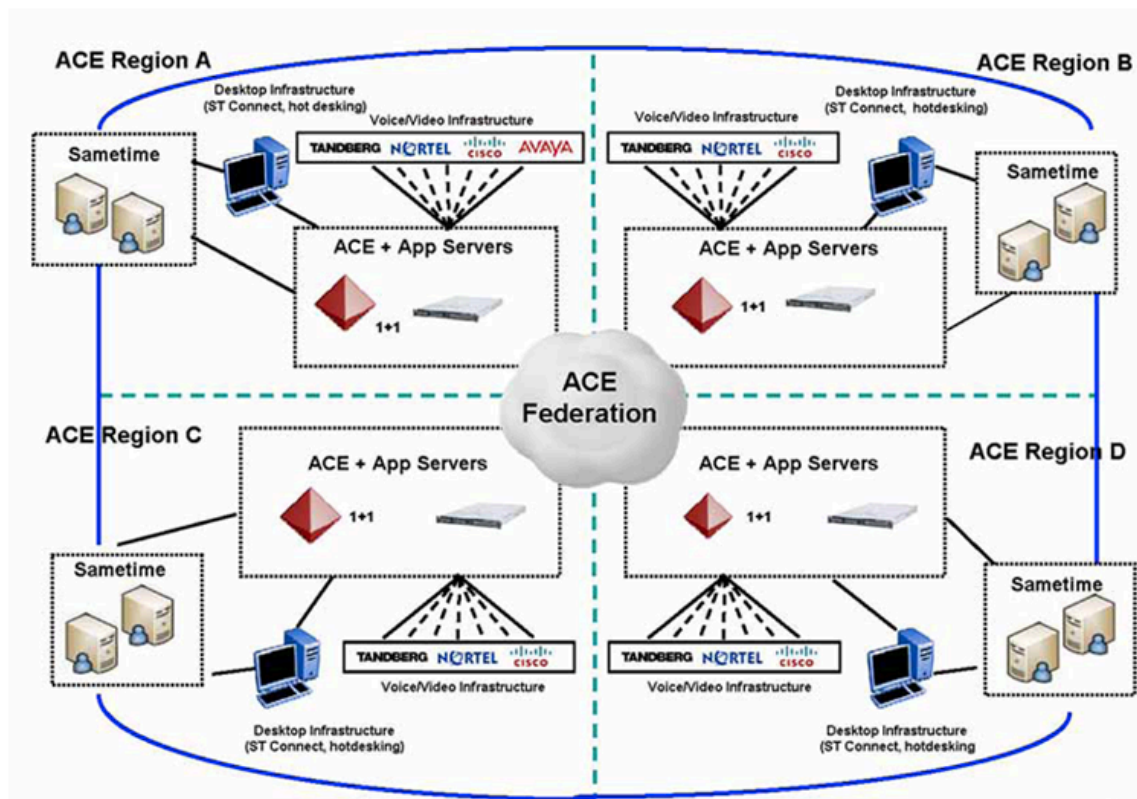
Description

Avaya ACE supports a multi-regional deployment architecture. With this architecture, multiple servers are synchronized to form a logical group, or federation. This provides distributed client applications with seamless global web service access across geographical locations.

Servers that are part of the same federation are able to share service provider rules. This enables a server in one region to discover and provide call treatment for a user whose home server is in a different region.

Example federated deployment architecture

A federated architecture provides seamless global web service access across geographical locations.



Checkpoint



The web services interface connects the web clients to Avaya ACE and carries traffic containing SOA service requests.

_____ True

_____ False

Answer : True



The Service Provider interface is used for network server traffic; for example, call servers and communications systems.

_____ True

_____ False

Answer : True



The Avaya ACE architecture requires the deployment of a standby server.

_____ True

_____ False

Answer : False



Which Avaya ACE deployment architecture enables multiple servers to be synchronized to form a logical group, providing seamless global web service access across geographical locations.

- ☐ Basic deployment architecture
- ☐ Basic deployment architecture
- ☐ Federated deployment architecture
- ☐ None of the above (not supported)

Answer: , Federated deployment architecture

Module summary

Objectives

In this module you learned how to:

- Identify the main design components of the Avaya ACE design architecture: adapters, Service-Oriented Architecture (SOA) services and composites, and application programming interfaces (APIs).
- Identify the key components in a basic Avaya ACE deployment architecture.
- Identify the basic components in an Avaya ACE multi-regional (federated) architecture.

Deployment guidelines

Introduction

Purpose

This module provides a high level overview of key Avaya Agile Communication Environment™ (Avaya ACE™) deployment considerations, supported configurations, network configuration, capacity, performance, and security.

Topics

After completing this module, you will be able to:

- Identify and distinguish between the supported Avaya Avaya ACE configurations.
- Identify high availability deployment fundamentals for an Avaya ACE on Windows deployment.
- Identify configuration guidelines for an Avaya ACE on Linux high availability configuration.
- Identify general security guidelines for the Avaya ACE solution, such as physical security, network security, and user access controls.

Resources

Avaya ACE documentation:

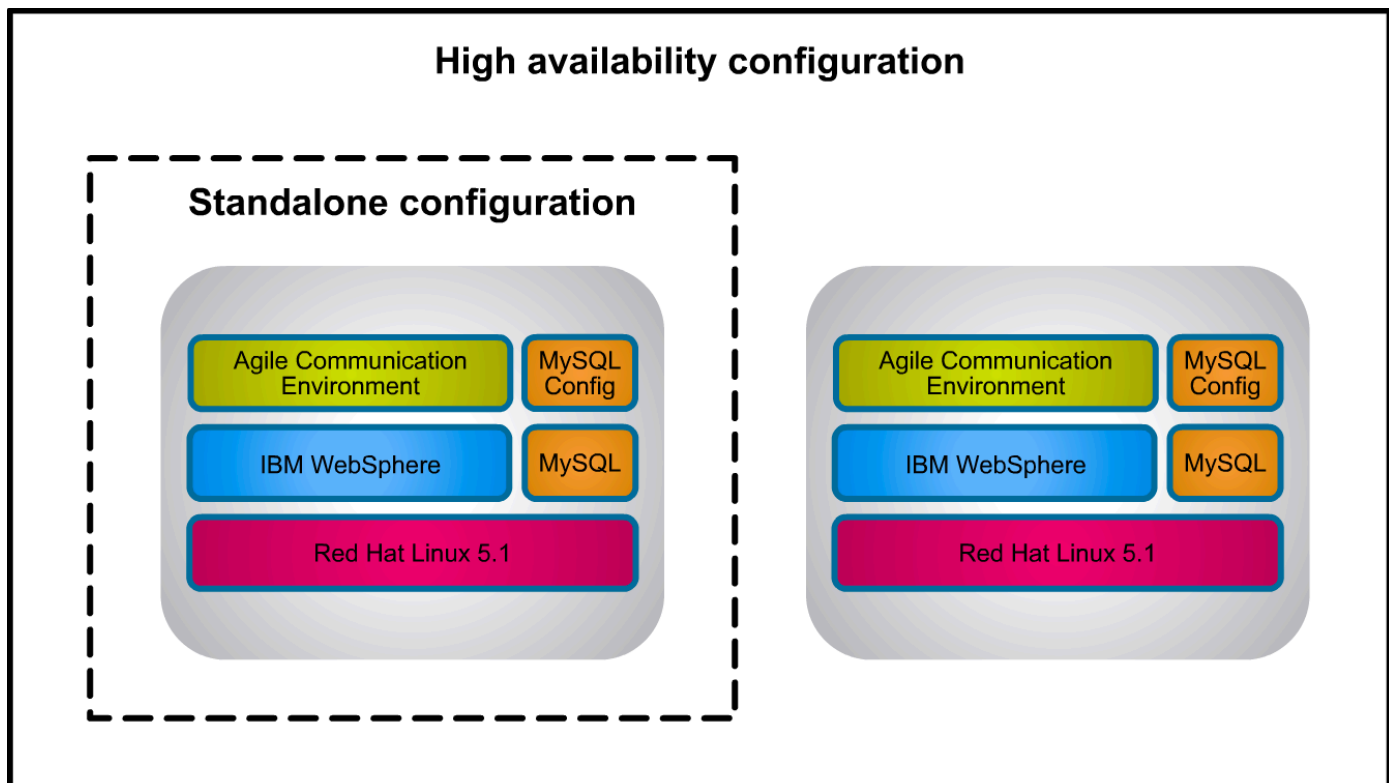
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)

Supported configurations

Supported configurations - Linux

Standalone and high availability (HA) Linux configurations are supported. In a standalone configuration, Avaya ACE is installed on a single host. In a high availability configuration, Avaya ACE is installed on both hosts (active and standby). In the event of a failure condition on the active server, a failover (switchover) to the standby server occurs.

Avaya ACE stores user profile data and call session information in a MySQL database, an open source software product that is owned, developed and supported by Sun Microsystems.

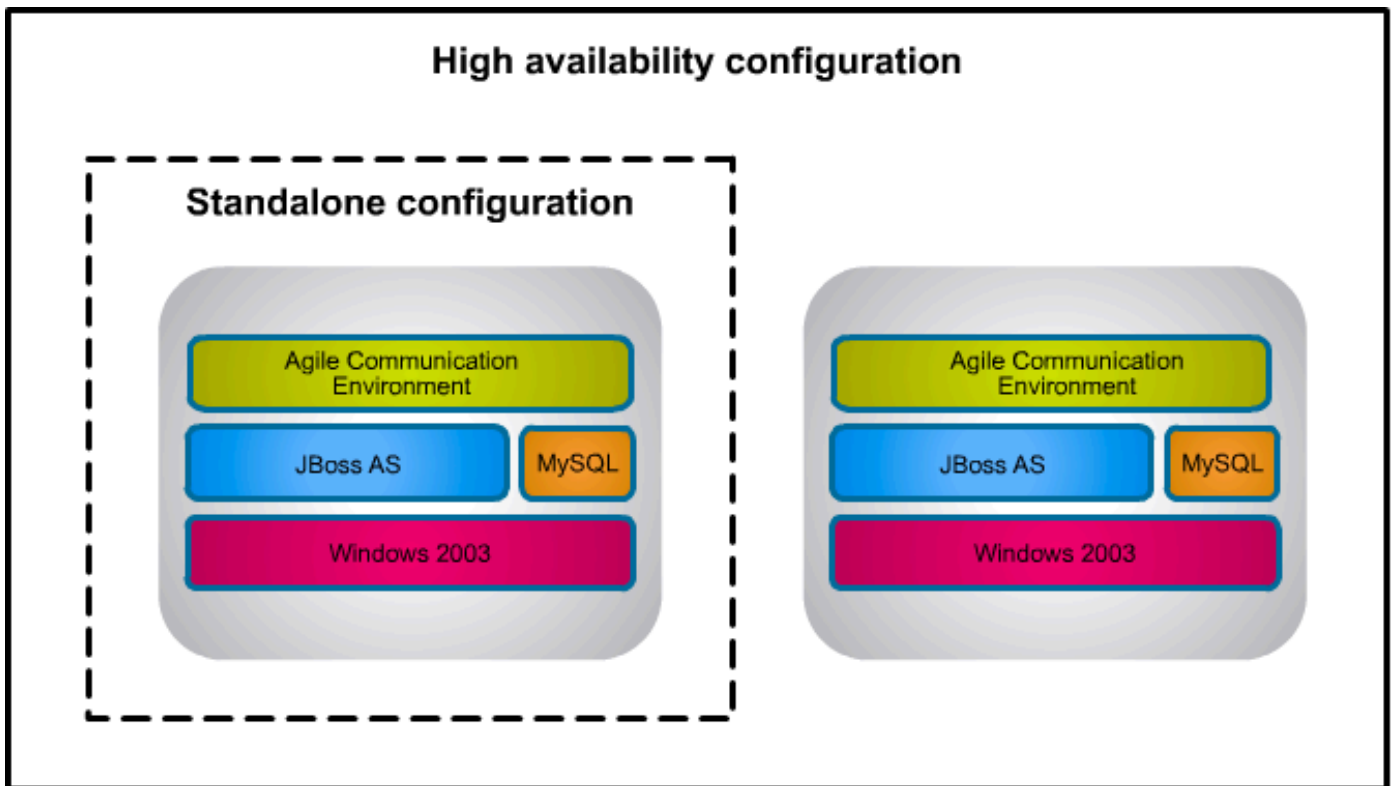


Supported configurations - Windows

Standalone and high availability (HA) Windows configurations are supported. In a standalone configuration, Avaya ACE is installed on a single host. In a high availability configuration, Avaya ACE is installed on both hosts (active and standby). In the event of a failure condition on the active server, a failover (switchover) to the standby server occurs.

The supported Windows operating system is Windows 2003 with service pack 2 or higher. The 64 bit version is not supported. Windows 2008 is not supported.

Avaya ACE stores user profile data and call session information in a MySQL database, an open source software product that is owned, developed and supported by Sun Microsystems.



High availability network: Windows

Description

Availability refers to the ability of the user community to access the system. High availability refers to the implementation of system features that ensure operational continuity during a given measurement period.

With a high availability (HA) deployment, Avaya ACE supports the deployment of two Avaya ACE hosts in a Windows Network Load Balancing (NLB) cluster. Because the Avaya ACE application is not running on the redundant Avaya ACE host, the redundant Avaya ACE host is in a cold standby state. During a failover (switchover), Avaya ACE is started and becomes in an active state.



Alert

Avaya ACE must never be running on both hosts at the same time.

Failure detection and failover scenarios

A failover (switchover) to the standby server occurs during the following conditions:

- The active node system is shut down.
- The active server is restarted.
- The Avaya ACE application on the active server fails to start in a given period of time.
- The Avaya ACE ClusterManager service stops running on the active node.
- The Avaya ACE ClusterManager service fails to recover the Avaya ACE JBossService.
- The NLB Cluster detects that the active node is not a valid node in the cluster.

Node synchronization

In a high availability deployment, the two Avaya ACE nodes communicate using rsync to maintain configuration file and database synchronization. The following rsync applications are installed during the initial installation.

- cwRsync
- cwRsyncServer
- ICW Base
- ICW RsyncServer

After the Avaya ACE installation, the applications are listed in the Windows Add or Remove Programs tool. **Do not remove the applications.**

The rsync applications are open source utilities that speed file transfer and synchronization. For more information about rsync features or functionality, go to www.samba.org/rsync.

High availability network: Linux

Description

The high availability configuration (HA) consists of two physical hosts in a 1+1 warm standby, non-revertive configuration, using Red Hat Cluster Suite software, integrated with the Linux operating system, to detect failures and trigger failovers.

Software components are installed on the active and standby (redundant) host. In the event of a failure condition on the active server, a failover (switchover) to the standby server occurs. Fencing isolates the standby node, preventing it from accessing shared resources such as the database or network call servers.

For more information about Red Hat Linux or the Red Hat Cluster Suite software, go to www.redhat.com.



Alert

Avaya ACE must never be running on both hosts at the same time.

Failure detection and failover scenarios

Failure scenarios can be categorized in three areas.

- **Cluster membership:** If the active host unexpectedly leaves the cluster, then the mate node power fences the active host and Cluster Suite relocates the cluster service to the mate node. If the standby host unexpectedly leaves the cluster, the active host power fences the standby host, but no cluster service relocation is initiated.
- **OAM status file failover:** The HA cluster service monitors the health of the active node. As long as the system checks are successful, the `/var/adm/status` file is time-stamped. If the time-stamp is older than 30 seconds, or the file is not present, a failover without power cycling is initiated. The standby node starts, registers the floating IP addresses and becomes the active node. No power fence occurs.
- **Floating IP address failover:** The cluster service monitors the floating IP address. If the floating IP address becomes unresponsive or is unbound from the interface, a failover is initiated. No power fence occurs.

Security guidelines

General security guidelines

It is important to protect the ACE solution resources from unauthorized use, as well as protect data integrity and confidentiality. Some general security considerations are listed below.

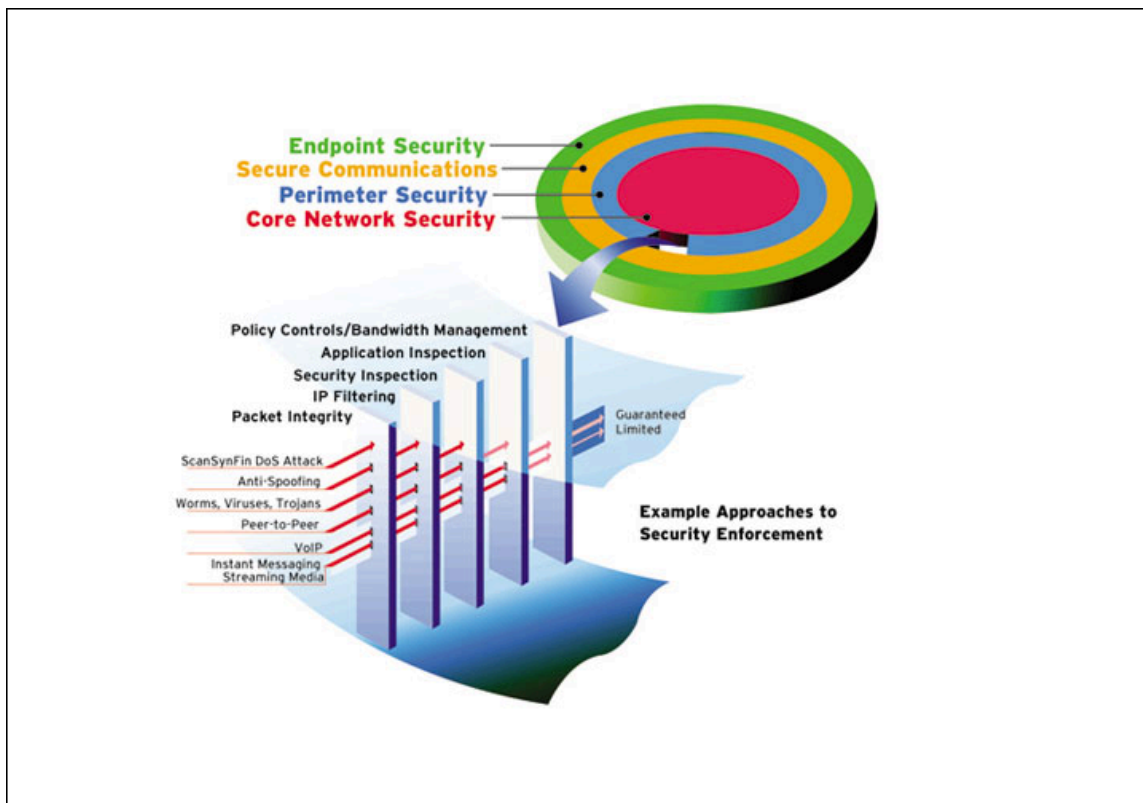
- **Physical security:** Deploy any ACE host in secure facility that only permits access by authorized personnel.
- **Network security:** Deploy the ACE host in a trusted environment, with secure networking technologies, such as firewalls, to protect direct network access to the ACE resources, and a layered defense for protection against a broad range of security threats.
- **Secured server-side communications:** Ensure either a self-signed certificate or a certificate signed by a Certificate Authority (CA-signed certificate) is implemented and that the certificate is current.
- **User access controls:** Control user access to solution resources through global and group policies and a password management strategy; for example, compliance with recommended password conventions and required password change at defined intervals.

Benefits of a layered defense

A layered defense allows the network to:

- Quickly disable ports that are implicated in an attack.
- Segregate network servers and domains to limit the impact of an attack.
- Quickly recover from a successful system breach through backup/restore.
- Provide redundancy so backup resources are available if necessary.
- Protect and prioritize critical traffic and applications.

Example approaches to security enforcement



Server-side security

ACE supports the Secure Socket Layer (SSL) protocol to perform server-side authentication using X.509 certificates. The SSL protocol encrypts data sent over connections to ensure secured communications; for example, prevent eavesdropping, replaying attacks, and message tampering and forgery.

ACE supports X.509 certificates that are self-signed or signed by a Certificate Authority (CA). By default, a self-signed certificate is enabled upon an initial installation.

Self-signed certificates are issued by the user themselves. This type of certificate does not provide any authentication, and are vulnerable to man-in-the-middle attack.

Based on your security requirements, you can configure, you can implement a certificate that is signed by a public Certificate Authority (CA). A public CA can be an existing internal CA of the customer organization; for example, the CA from the customer's IT department or an outside commercial CA; for example, Verisign or Thawte.

SSL client authentication

The SSL client authenticates the server X.509 certificate by performing a series of validations, including:

- Validating the CA digital signature on the certificate
- Verifying that the signing CA public key certificate is on the client's trusted certificate list
- Verifying that the server certificate is not expired



Authentication and authorization

Access to Avaya ACE is controlled using HTTP 1.1 basic authentication. Requests must contain a valid user name and password that correspond to a user profile configured in Avaya ACE.

Authorization for individual web services is configured on a service-by-service basis. The user account configured for the web service client (application) must have the appropriate access control rules set to invoke a particular web service.

Secure web service communication

By default, web service communication is supported on the secure (HTTPS) and non secure (HTTP) ports. A consumer of a web services can choose to completely secure all web service communication (including notifications).

Important: For secure communication, ensure that the Avaya ACE version and the ports on the host server match. To establish secure-only communication with the Avaya ACE host, you must explicitly disable the nonsecure ports. For high availability (HA) deployments, perform this procedure on both hosts.



Tip

Communication port management is supported on Linux and Windows hosts. For more information about port usage, see *Avaya Agile Communication EnvironmentTM Planning and Installation* (NN10850-004).

Checkpoint



In a high availability Linux deployment, the ACE application must never be running on both ACE hosts at the same time.

- ☐ True
- ☐ False

Answer : True



ACE supports Secure Socket Layer (SSL) to perform server-side authentication using X.509 certificates. By default, a self-signed certificate is enabled upon an initial ACE installation.

- ☐ True
- ☐ False

Answer : True



It is recommended that you deploy the ACE host in an open environment that supports direct access to external network devices.

- ☐ True
- ☐ False

Answer : False

Module summary

Objectives

In this module you learned how to:

- Identify and distinguish between the supported Avaya Avaya ACE configurations.
- Identify high availability deployment fundamentals for an Avaya ACE on Windows deployment.
- Identify configuration guidelines for an Avaya ACE on Linux high availability configuration.
- Identify general security guidelines for the Avaya ACE solution, such as physical security, network security, and user access controls.

Service provider integration

Introduction

Purpose

Avaya Agile Communication Environment™ (Avaya ACE™) works with multi-vendor network infrastructures (such as private branch exchange (PBX) systems and video systems) through software adapters that interface to and control these environments. This module provides a high level overview of integration considerations for the Avaya ACE service providers.

Important: IBM Lotus Sametime and Microsoft Office Communications Server (OCS) are beyond the scope of this module.

Objectives

After completing this module, you will be able to:

- Identify supported network elements and general service provider configuration guidelines.
- Identify the types and purpose of translation rules.
- Identify when it is necessary to deploy a media terminal, as well as general media terminal configuration parameters.
- Identify CS 1000 service provider fundamentals, including supported ACE web services and how Avaya ACE interacts with CS 1000 service provider network elements.
- Identify minimum CS 1000 configuration prerequisites to support communications with Avaya ACE.
- Identify CS 2000 service provider fundamentals, including supported Avaya ACE web services and how Avaya ACE interacts with CS 2000 network elements.
- Identify minimum CS 2000 configuration prerequisites to support communications with Avaya ACE.
- Identify CS 2100 service provider fundamentals, including supported web services and how Avaya ACE interacts with CS 2100 network elements.
- Identify minimum CS 2100 configuration prerequisites to support communications with ACE.
- Identify MCS 5100 service provider fundamentals, including supported services and how Avaya ACE interacts with MCS 5100 and AS 5200 network elements.
- Identify minimum MCS 5100 and AS 5200 configuration prerequisites to support communications with Avaya ACE.

- Identify NMC service provider fundamentals, including supported Avaya ACE web services and how Avaya ACE interacts with NMC network elements.
- Identify minimum NMC configuration prerequisites to support communications with ACE.
- Identify Avaya Contact Center/MLS service provider fundamentals, including supported web services and how Avaya ACE interacts with Contact Center/MLS network elements.
- Identify minimum Contact Center/MLS configuration prerequisites to support communications with Avaya ACE.
- Identify CCM service provider fundamentals, including supported web services and how Avaya ACE interacts with Cisco Unified CM network elements.
- Identify minimum Cisco Unified CM configuration requirements to support communications with Avaya ACE.
- Identify Tandberg VCS service provider fundamentals, including supported web services and how Avaya ACE interacts with Tandberg VCS network elements.
- Identify minimum Tandberg VCS configuration requirements to support communications with Avaya ACE.
- Identify Avaya service provider fundamentals, including supported web services and how Avaya ACE interacts with Avaya network elements.
- Identify minimum Avaya configuration requirements to support communications with Avaya ACE.

Resources

Avaya ACE documentation:

- *Administration* (NN10850-005)

Service provider fundamentals

Commonly used network elements

Within the customer network, network elements (communication systems, call servers) interact with Avaya ACE to deliver communications solutions. Some commonly used network elements that Avaya ACE supports are listed below.

- Avaya Communication Server 1000 (Avaya CS 1000)^{1,2}
- Avaya Communication Server 2000 (Avaya CS 2000)²
- Avaya Communication Server 2100 (Avaya CS 2100)¹
- Avaya Multimedia Communication Server 5100 (Avaya MCS 5100)¹
- Nortel Application Server 5200 (Nortel AS 5200)¹
- Avaya Contact Center, through Meridian Link Services (MLS)²
- Avaya Interactive Communications Portal (Avaya ICP)³
- Avaya Multimedia Conferencing/Avaya Media Application Server (Avaya MAS)¹
- Cisco Unified Communications Manager (Cisco Unified CM)¹
- Tandberg Video Communication Server (VCS)¹
- Avaya Aura[™] ²
- IBM Lotus Sametime⁴
- Microsoft Office Communications Server (OCS)⁵

1 - Integrates with IBM Lotus Sametime.

2 - Integrates with Microsoft OCS.

3 - Is not configured as a service provider. Is assigned to a service provider.

4 - Configured as a service provider and interworks with other service providers.

5 - Is not configured as a service provider but interworks with other service providers.

Service Providers window

The Configuration menu provides access to the Service Providers window. From this window the Avaya ACE administrator can:

- Add, view, edit, and remove service providers.
- Change the order of service providers.

The Service Providers window is organized by the following tabs:

- Local Service Provider(s) tab: Displays service providers configured on an Avaya ACE host for a local region.
- Remote Region(s) tab: Displays service providers configured on an Avaya ACE host that belongs to an Avaya ACE federation.
- Rule Validation tab: Used to view and validate rules configured for service providers.

Service Providers window

In the figure, there are three local service providers. The Avaya ACE host is not federated; therefore, there are no remote service providers.

The screenshot displays the 'Service Provider(s)' window. At the top, there are three tabs: 'Local Service provider(s)', 'Remote Region(s)', and 'Rule Validation'. The 'Local Service provider(s)' tab is selected. Below the tabs, a table lists three service providers. The table has columns for No, Name, Type, Signaling, IP Address, Port, Terminals Addresses, and Rules. To the right of the table are 'Up' and 'Down' buttons. Below the table are 'Add', 'Edit', and 'Remove' buttons.

No	Name	Type	Signaling	IP Address	Port	Terminals Addresses	Rules
1	as5200	MCS	sip	47.140.88.205	5060		
2	cs1000	CS 1000	sip	47.160.131.11	5060	N/A	
3	sametime	SAMETIME	sametime	47.140.111.231	1516	N/A	N/A

Common configuration tasks

In addition to basic service provider configuration, it is necessary to perform one or more of the tasks below.

- Configure a route address to indicate call origination (third party call scenarios). You can keep the default or configure a different one, as necessary, as appropriate.
- Configure translation and transformation rules to ensure proper routing calls to the appropriate service provider. Each service provider requires one rule, at a minimum.
- Change the order of service providers (when there are multiple providers) so that the providers that experience the most activity are placed at the top of the provider list.
- Add and define a media terminal (such as the Interactive Communications Portal - ICP) and associated addresses for services that require media treatment. A media terminal anchors call sessions and hosts media services added to a call; for example, announcements, conference media path for Third Party Call (v3) and audio call scenarios, and Text-to-Speech services.

Translation rules fundamentals

Description

Each service provider requires at least one translation rule. Translation rules manipulate web service Uniform Resource Identifiers (URIs) to ensure routing to the appropriate service providers.

Avaya ACE supports simple, advanced, remote, and reverse transformation rules. The type of rule used depends upon the service provider, customer dial plan, and services used in the network.

- Simple translation rules route a web service request to a particular service provider and if necessary, transform the parameters in the request before presenting them to the service provider.
- Reverse transformation rules transform the URI back to the required format before it is presented to a web service interface.
- Remote translation rules are configured on remote Avaya ACE servers (remote regions) when Avaya ACE is deployed in a federation.
- Advanced translation rules support URI manipulation when simple rule is not sufficient to meet routing/transformation needs.



Tip

It is recommended to first validate all rules before you activate them. Deactivate rules that no longer needed. You cannot activate or deactivate remote rules.

Simple translation rules

Define simple translation rules to route a web service request to a particular service provider and, if necessary, transform the parameters in the request before being presented to the service provider. See the table for guidelines.

Tip: Avaya ACE supports a URI format that is in accordance with RFC2396: Uniform Resource Identifier (URI) Generic Syntax.

If	Then
the service provider supports both SIP and tel URIs	select the URI scheme against which the incoming URI should be matched .
the service provider supports only one URI scheme	no action is required as the field is populated with the default value.
Range From and Range To ARE configured	the other fields are optional and can be left blank (empty)
Range From and Range To are NOT configured	configure the Domain , and leave the other fields blank (empty).
URI transformation is required	configure Digits to Insert , Number of Digits to Delete , and Digits or string to append .

Example simple rule: Calling Party Translation

The figure shows a simple Calling Party Routing Rule for a CS 1000 TR/87 service provider (DN range 1000-5999).

- There is one URI scheme: tel.
- The Range To and Range From fields are completed.
- The other fields are left blank (empty).

Translation Rule for Service Provider -- CS 1000 : cs1000

Calling Party Translation Rule

Type	Rules	Reverse Transformation
Simple	URIScheme=tel,RangeFrom=1000,RangeTo=5999,	No

Up
Down
Remove

Switch to Advanced Configuration

Simple Configuration

Routing Rules

URI Scheme: tel
Range From: 1000
Range To: 5999
Domain:

Transformation Rules

Number of Digits to Delete:
Digits to Insert:
Digits or string to append:

Example Called Party Translation Rule

The figure shows the companion simple Called Party Routing Rule for the Calling Party Routing Rule.

- There is one URI scheme: tel.
- The Range To and Range From fields are completed.
- The other fields are left blank (empty).

Translation Rule for Service Provider -- CS 1000 : cs1000

Called Party Translation Rule

Type	Rules	Reverse Transformation
Simple	URIScheme=tel,RangeFrom=1000,RangeTo=5999,	No

Up
Down
Remove

Switch to Advanced Configuration

Simple Configuration

Routing Rules

URI Scheme:

Range From:

Range To:

Domain:

Transformation Rules

Number of Digits to Delete:

Digits to Insert:

Digits or string to append:

Reverse translation rules

Reverse translation rules apply in the opposite direction of translation rules. Reverse translation rules are used to reformat URIs for outgoing web services such as Call Notification to eliminate the need for additional intelligence in the application; for example, translate Call Notification callingParticipant values to E.164 format before being used by the called party for makeCall operations.

Important: Reverse translation rules are not used for routing. They are only used to transform a DN to its original format before passing it to a service interface.

Example reverse translation rule

The example shows a reverse translation rule configuration where Call Notification callingParticipant values must be translated to E.164 format before being used by the called party for makeCall operations. This manipulation could be required for an application to support make call functionality directly from a call log or call history client interface.

- An application starts callNotification on **DN 4914** (calledParticipant).
- Based on information provided by the serving CS 1000, the callingParticipant is **555 8424**.
- A calling party reverse translation rule is applied to provide the callingParticipant URI to the application in E.164 format.
- Using the calling party rule configuration, ACE transforms **tel: 555 8424** to **tel:16135558424**. The callingParticipant parameter value included in call notification service request is **tel: 16135558424**.



Tip

From Wikipedia, the free encyclopedia:

E.164 is an International Telecommunication Union (ITU) recommendation that defines the international public telecommunication numbering plan used in the public switched telephony network (PSTN) and some other data networks. It also defines the format of telephone numbers. E.164 numbers can have a maximum of fifteen digits and are usually written with a + prefix. To actually dial such numbers from a normal fixed line phone, the appropriate international call prefix must be used.

Advanced translation rules

Use advanced translation rules when simple rule is not sufficient to meet routing/transformation needs; for example:

- Keep the Uniform Resource Identifier (URI) as is.
- Append a prefix to a 4 digit DN.
- Add a prefix to a Directory Number (DN) based on a matching pattern.

You can configure the advanced translation rules to route calls for a service provider, apply URI transformation, or both. See the table below for guidelines.

When you configure advanced translation rules using regular expressions, ensure that you use the Java variant of the regular expression syntax that Avaya ACE supports. For more information, see the examples and job aids in *Avaya Agile Communication Environment AdministrationTM* (NN10850-005).

Alert: Use this option only if you are familiar with regular expressions and need more flexibility to configure routing rules that are not otherwise configurable using simple translation.

Variable	Type	Description
Matching Pattern	String	This is a regular expression for matching incoming URIs to service providers. This field is mandatory when defining rules through the advanced translation rules.
Transform URI Rule	String	This is regular expression resulting from the matching pattern that indicates how the digits must be formatted in the signaling message sent to the service provider. This field is optional . If a transform URI rule is not defined, the original URI is passed to the service provider in the signaling messages.

Example advanced incoming translation rule: Append prefix

The example shows an advanced translation rule for appending a prefix to a 4-digit DN.

Calling Party Translation Rule

Type Rules Reverse Transformation Rule Active Up Down Remove

Switch to Simple Configuration

Advanced Configuration

Matching Pattern:

Transform URI Rule:

Reverse Transformation ☐ Activate Rule ☐

Add Update

Example advanced translation rule: Keep URI as is

The example shows an advanced translation rule configured to keep the URI as is.

Calling Party Translation Rule

Type Rules Reverse Transformation Rule Active Up Down Remove

Switch to Simple Configuration

Advanced Configuration

Matching Pattern:

Transform URI Rule:

Reverse Transformation ☐ Activate Rule ☐

Add Update

Media terminals

Media terminal fundamentals

A supported media terminal is required to provide media treatment for Third Party Call Control (v3) multi-party calls, Audio services (audio files and announcements), and Text-to-Speech voice synthesis for communications-enabled applications, such as Event Response Manager.

To provide these services, the Avaya Interactive Communications Portal (Avaya ICP) is required. The ICP is a software solution that provides intelligent, personalized, unassisted self-service to customers, as well as conversational dialog processing using natural language understanding.

ICP interworking

The ICP platform itself must be installed and operational. Within the Avaya ACE GUI, the ICP is defined as a media terminal, during the service provider configuration.

Note that the ICP is not required for ring back tones for Third Party Call Control (v2) with SIP. A SIP refer message provides the ring back tone.

Important: If the prerequisite software is not installed on the ICP (for example, RFC 4240 SIP media services or TTS software), download the files from the Avaya ACE GUI and install them on the ICP.

Avaya ACE and ICP interworking

The figure shows how the media terminal configured in the Avaya ACE GUI corresponds to the ICP configuration.

The screenshot displays the Avaya ACE GUI configuration for a media terminal. The top section, titled "CS 1000 : Milan 3 Address(es)", contains a table with the following data:

No	Name	Type	URI	Terminals
1	thirdPartyCallController	Route	sip:AppCore@ace.com	N/A
2	annc	Media	sip:annc@ace.com	Milan
3	conf	Media	sip:conf@ace.com	Milan

An orange box highlights the "annc" and "conf" entries. An orange arrow points from the "annc" entry to the "Address Details" section below, which shows "Type" set to "Media". Another orange arrow points from the "conf" entry to the "Application Translations" table in the bottom right window.

The "Application Translations" table in the bottom right window has the following data:

Application Name	Pattern	Rank	Mode	Alarm When
Corporate Directory Dialer	cdd	1	SIP Request URI User	Case Insensitive
RFC4240	annc	10	SIP Request URI User	Exact Match
RFC4240	conf	10	SIP Request URI User	Exact Match
RFC4240	*conf*	10	SIP Request URI User	Regular Expression

CS 1000 service provider fundamentals

Overview

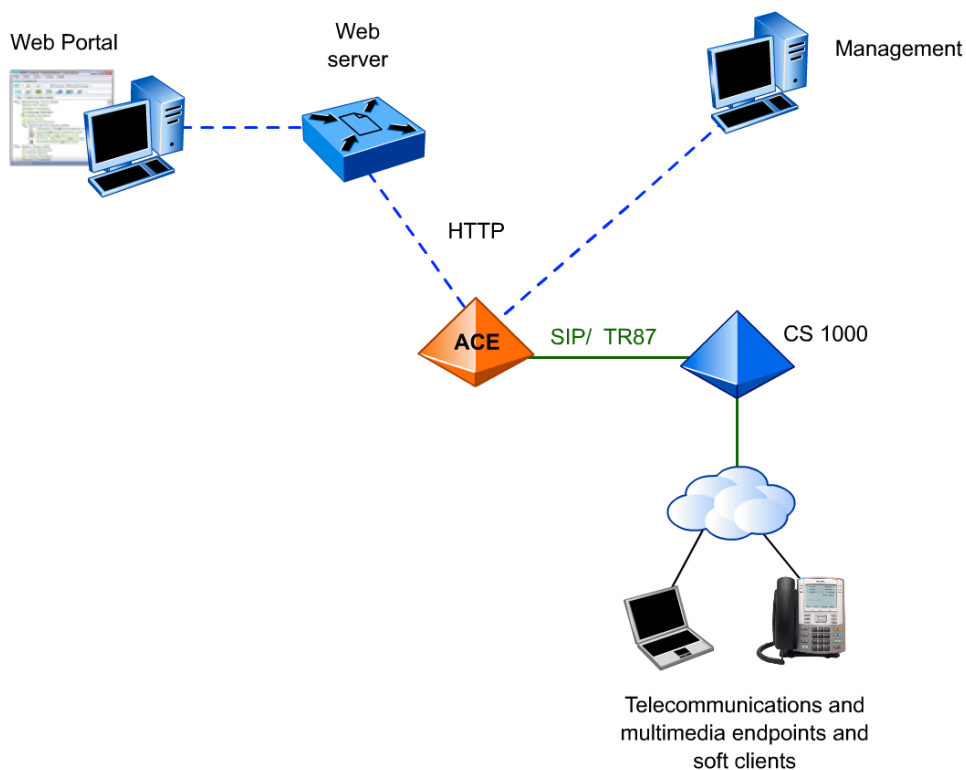
The Avaya Communication Server 1000 (Avaya CS 1000) is a server-based, full-featured IP PBX. The CS 1000 system supports traditional public switched telephony network (PSTN) as well as Session Initiation Protocol (SIP) and H.323 communications.

Avaya ACE and CS 1000 interworking

Avaya ACE provides CS 1000 TR/87, SIP, TR/87-SIP hybrid service provider interfaces to provide web services and enable communications between ACE client applications and CS 1000 network elements. The Avaya Interactive Communications Portal (Avaya ICP) is used for services that require media treatment.

Example CS 1000 service provider deployment

The figure provides a simplified view of an ACE deployment that includes a CS 1000 service provider.



Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Supported CS 1000 network configurations

CS 1000 service provider configuration requirements

CS 1000 SIP service provider

To support communications with Avaya ACE using standard SIP, the CS 1000 network element must meet the following minimum configuration requirements:

- The CS 1000 system is running Release 4.5 or higher software. If the CS 1000 system is using a SIP Proxy Server (SPS), then SPS Release 6.0 or higher is required for proper SIP routing.
- The CS 1000 is SIP-enabled and supports SIP signaling over UDP.
- SIP virtual trunking is configured to receive traffic (SIP control messages) from ACE.
- The Avaya ACE server (IP address) is configured as a gateway endpoint (trusted node) on the primary network routing service (NRS).

CS 1000 TR/87 and CS 1000 TR/87-SIP hybrid service providers

To support communications with Avaya ACE using TR/87 and TR/87-SIP, the CS 1000 network element must meet the following minimum configuration requirements:

- The CS 1000 system is running Release 4.5 or higher software. If the CS 1000 system is using a SIP Proxy Server (SPS), then SPS Release 6.0 or higher is required for proper SIP routing.
- The CS 1000 is SIP-enabled and supports SIP signaling over UDP.
- SIP virtual trunking is configured to receive traffic (SIP control messages) from ACE.
- SIP Computer Telephony Integration (CTI) operations are configured on the CS 1000 system to allow third-party applications to control phone operations.
- The following packages are equipped:
 - SIP 406 (SIP Package)
 - MS_CONV 408 (Multimedia Systems Convergence)
- A virtual Application Module Link (AML) and Value Added Server (VAS) are configured on the system.
- SIP CTI is configured and enabled on the CS 1000 IP Telephony Node.
- Phones are configured to support CTI operations (receive remote control messages).
- Each phone configured for CTI operations requires an Associated Set (AST) license.
- The Avaya ACE host name and IP address are defined on the CS 1000 IP Telephony node.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).



Tip

Technical Report ECMA TR/87, published by Ecma International, describes the use of Computer Supported Telecommunications Applications (CSTA) to invoke features not possible with standard SIP; for example, enable an application to send control messages to a Computer Telephony Integration (CTI)-capable terminal to perform various functions, such as establish calls and obtain presence information.

CS 2000 service provider fundamentals

Overview

The Communication Server 2000 (CS 2000) is a Carrier Voice over IP (VoIP) superclass softswitch. It supports a wide range of signaling, transport and control protocols for line gateways. The CS 2000 functions as the centerpiece of an open, standards-based, scalable packet trunking solution or packet access solution enabled by the Carrier VoIP portfolio.

Avaya ACE and CS 2000 interworking

Avaya ACE provides the following service provider interfaces to provide web services and enable communications between Avaya ACE client applications and CS 2000 network elements.

- CS 2000 SIP service provider
- CS 2000 SIP SIP_IN service provider
- CS 2000 SIP SIP_SSL (Session Server Lines) service provider

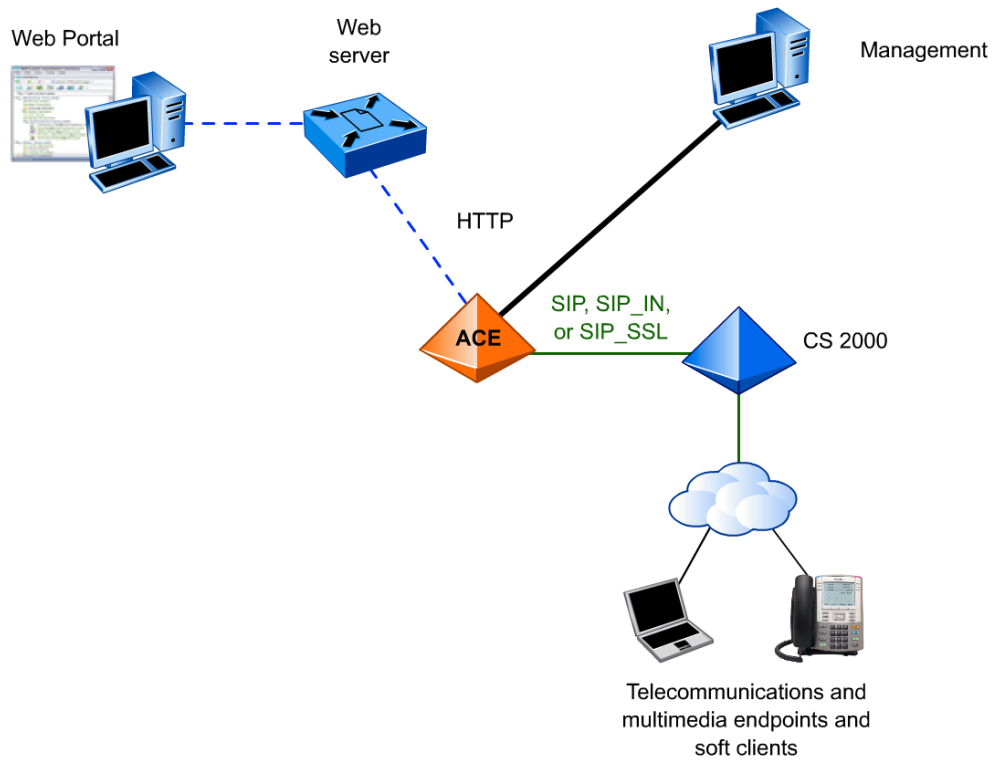


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example CS 2000 deployment

The figure provides a simplified view of an Avaya ACE deployment that includes a CS 2000 service provider.



Supported CS 2000 network configurations

CS 2000 service provider requirements

Basic configuration

To support communications with Avaya ACE, the CS 2000 network element must meet the following minimum configuration requirements:

- Signalling System 7 (SS7) links between the CS 2000 and IN-SIP Gateway (ISSG)
- Advanced Intelligent Networks (AIN) Software Optionality Control (SOC) Options
- AIN Subsystem and Triggers associated with the Avaya ACE server
- CS 2000 lines with TERMATT and OFFHKDEL AIN Triggers
- Session Server Trunks (SST) support of Avaya ACE over SIP for Third Party Call Control (v2)

ISSG configuration requirements

- Avaya ACE System ID and Application Server
- SS7 Links between the ISSG and CS 2000
- Signaling Connection Control Part (SCCP)

SST configuration requirements

- Avaya ACE Remote SIP Server
- Avaya ACE Access Link Map

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

CS 2100 service provider fundamentals

Overview

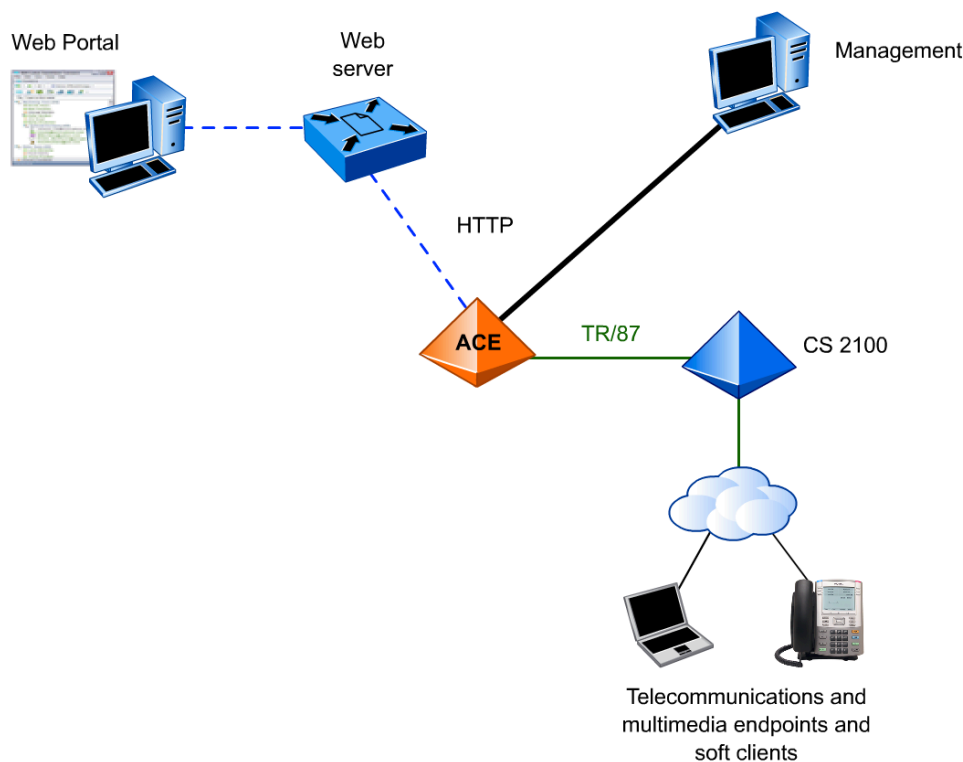
The Communication Server 2100 (CS 2100) is a large-scale converged solution that is based on its carrier derivative, the Communication Server 2000. The CS 2100 addresses the needs of demanding large enterprises through combined carrier and enterprise attributes.

Avaya ACE and CS 2100 interworking

ACE provides a CS 2100 TR/87 service provider interface to provide web services and enable communications between ACE client applications and CS 2100 network elements.

Example CS 2100 deployment

The figure provides a simplified view of an Avaya ACE deployment that includes a CS 2100 service provider.



Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Supported CS 2100 network configurations

CS 2100 service provider configuration requirements

To support communications with ACE, the CS 2100 network element must meet the following minimum configuration requirements:

- The CS 2100 system is running Release SE 10 or higher software.
- The CS 2100 is SIP-enabled and supports SIP signaling over UDP.
- SIP virtual trunking is configured to receive traffic (SIP control messages) from Avaya ACE.
- Support for Remote Call Control (RCC) is enabled.
- The Session Server Trunks (SST) meet the following configuration requirements:
 - Avaya ACE is defined as a Remote Call Control Server.
 - RCC customer groups are created.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

MCS service provider fundamentals

Overview

The Avaya Multimedia Communication Server 5100 (Avaya MCS 5100) is a unified communications solution that integrates IP telephony, multimedia conferencing, instant messaging (IM), presence, and other collaboration tools for the enterprise market.

The Application Server 5200 (AS 5200) delivers voice and multimedia services to carrier (residential) and enterprise uses.

Avaya ACE and MCS 5100 or AS 5200 interworking

Avaya ACE provides an MCS service provider interfaces to provide web services and enable communications between Avaya ACE client applications and MCS 5100 or AS 5200 network elements. The Avaya Interactive Communications Portal (Avaya ICP) is used for services that require media treatment.

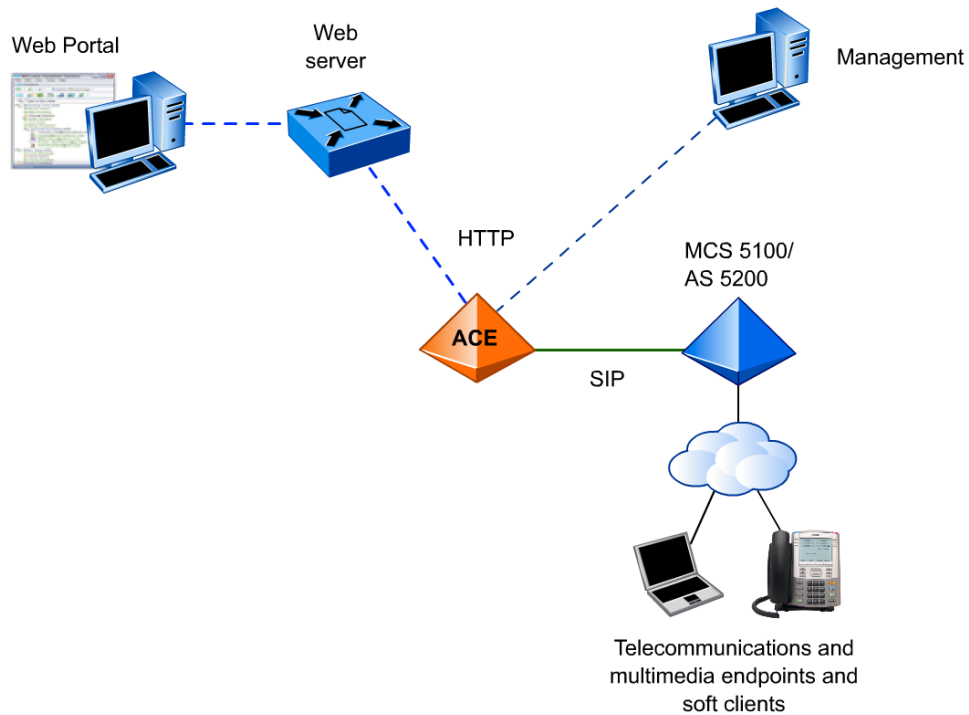


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example MCS service provider deployment

The figure provides a simplified view of an Avaya ACE deployment that includes an MCS service provider.



Supported MCS 5100 and AS 5200 network configurations

MCS service provider configuration requirements

MCS 5100

To support communications with Avaya ACE, the MCS 5100 network element must meet the following minimum configuration requirements: </p>

- The system is running MCS 5100 Release 4.0 or higher software.
- User accounts, profiles, and endpoints are created and properly provisioned
- SIP signaling over UDP is configured to receive ACE traffic (SIP control messages).
- The Avaya ACE host is defined as an informational element (trusted node).
- The appropriate network data configuration and management parameters are defined.

AS 5200

To support communications with Avaya ACE, the AS 5200 network element must meet the following minimum configuration requirements:

- The system is running AS 5200 Release 10.2 or higher software.
- User accounts, profiles, and endpoints are created and properly provisioned
- SIP signaling over UDP is configured to receive Avaya ACE traffic (SIP control messages).
- The Avaya ACE host is defined as an informational element (trusted node).
- The appropriate network data configuration and management parameters are defined.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Multimedia Conferencing service provider fundamentals

Overview

Avaya Multimedia Conferencing (also known as NMC) is a reservationless audio and video conferencing solution hosted on the Avaya Media Application Server (MAS) platform. Multimedia Conferencing provides subscribers with access to an always on multimedia conferencing resource that is highly scalable, highly available, and fully redundant.

A Multimedia Conferencing user assumes one of two roles:

- **Chairperson:** The chairperson is the owner of the conference resource and is provisioned as an NMC subscriber.
- **Participant:** Participants are invited to join a conference and may or may not be provisioned as NMC subscribers.

Avaya ACE and Multimedia Conferencing interworking

Avaya ACE provides an NMC service provider interface to support Multimedia Conference service operations for Avaya ACE client applications.

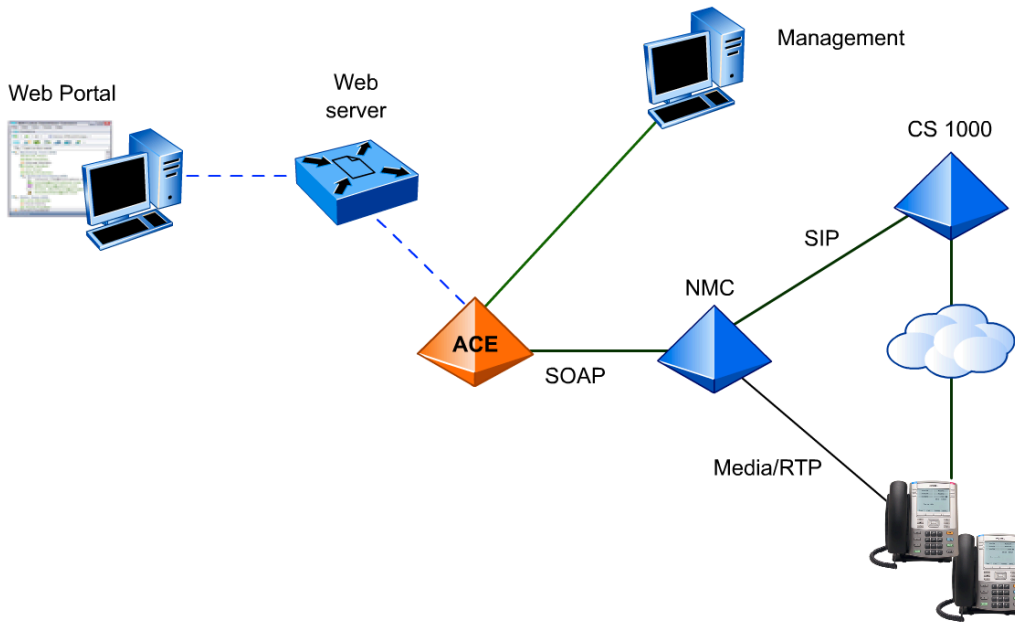


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example Multimedia Conferencing deployment

The figure provides a simplified view of an example Multimedia Conferencing deployment. The NMC is installed in a network that includes a SIP-enabled CS 1000 system. The Multimedia Conferencing servers are configured as a gateway endpoints on the Network Routing Service (NRS). The NRS can be either a SIP Proxy Server (SPS) or SIP Redirect Server (SRS).



Supported Multimedia Conferencing network configurations

Multimedia Conferencing (NMC) service provider configuration requirements

To support communications with Avaya ACE, the Multimedia Conferencing network element (also known as NMC) must meet the following minimum configuration requirements:

- **Multimedia Conferencing (NMC)**
 - Multimedia Conferencing (NMC) is running a supported software release.
 - Subscribers are configured on the Multimedia Conferencing server.
 - Because Multimedia Conferencing requires the presence of a conference chair person, it is recommended to set the Chair Ends Conference option to enabled in the subscriber configuration.
- **Avaya Media Access Server (Avaya MAS)**
 - MAS is running MAS Release 6.1 or higher software.
 - SIP signaling parameters are defined on the MAS. The Avaya ACE host (IP address or host name) must be defined on the MAS as a SOAP trusted node.
- **CS 1000**
 - The CS 1000 is running CS 1000 Release 6.0 or higher software.
 - SIP signaling over UDP and SIP virtual trunking is configured.
 - Multimedia Conferencing (NMC) and CS 1000 integration requirements are met.
 - The Multimedia Conferencing (NMC) network element is configured as a gateway endpoint on the CS 1000 Network Routing Service (NRS).

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Contact Center/MLS service provider fundamentals

Overview

The Avaya Contact Center includes a suite of applications to meet varied business requirements, call processing, agent handling, management and reporting, and networking third-party application interfaces.

The following subsystems work together in the Contact Center environment to provide processing for a call:

- Telephony system
- Meridian Link Services (MLS) interface
- Contact Center Manager server
- Voice-processing system

Avaya ACE and Contact Center/MLS interworking

Avaya ACE provides a Contact System/MLS service provider interface to provide web services and enable communications between Avaya ACE client applications and Contact Center network elements.

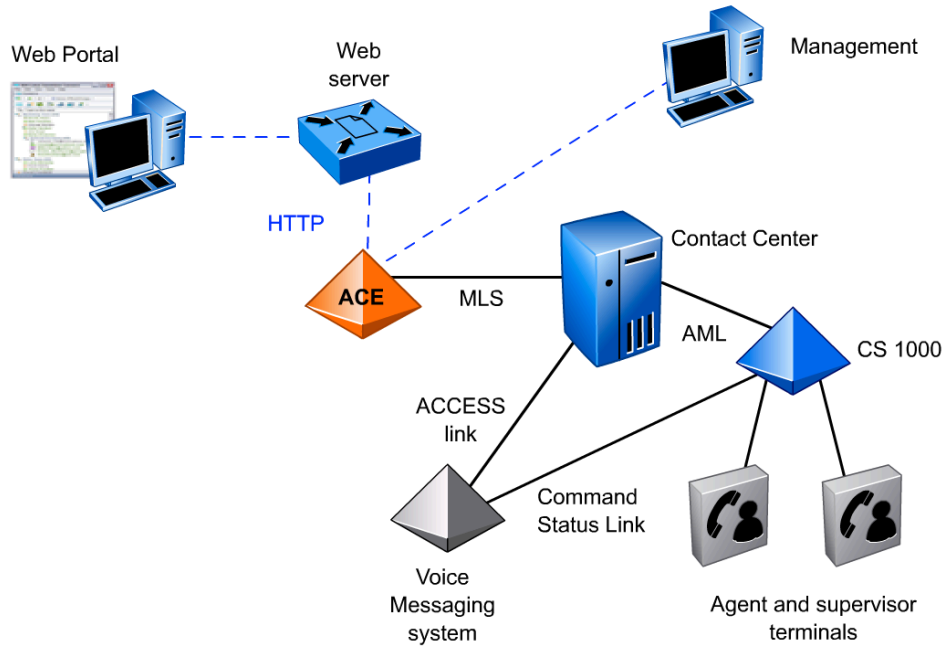


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example Contact Center/MLS deployment

The figure provides a simplified view of a Contact Center/MLS deployment.



Supported Contact Center/MLS network configurations

Contact Center/MLS service provider configuration requirements

To support communications with Avaya ACE, the Avaya Contact Center/MLS network element must meet the following minimum configuration requirements:

- The CS 1000 system is running software compatible with Contact Center Release 5.0 or higher.
- The CS 1000 is configured to enable the full functionality of the Meridian Link Services (MLS).
- An Application Module Link (AML) is configured on the CS 1000.
 - AML is the proprietary messaging protocol used between Contact Center and the CS 1000 system to support Contact Center functionality.
- A Value Added Server (VAS), Associated Set (AST), and other settings must be enabled on the CS 1000, as well as the appropriate software packages to permit full Ethernet signaling for communications to occur
 - Phones are defined as an associated set (AST) so that they can receive messages.
- The Avaya ACE host is configured to access the Contact Center server's subnet IP address.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Cisco Unified CM service provider fundamentals

Overview

Cisco Unified Communications Manager (Cisco Unified CM), formerly Cisco Call Manager (CCM), is the software call processing component of a Cisco Unified Communications solution. Cisco Unified CM software is installed on a supported Cisco server or a customer-supplied server that meets the Cisco Unified CM operating specifications.

Avaya ACE and Cisco Unified CM interworking

Avaya ACE provides CCM SIP and JTAPI service provider interfaces to provide web services and enable communications between ACE client applications and Cisco Unified CM network elements. The Avaya Interactive Communications Portal (Avaya ICP) is used for services that require media treatment.

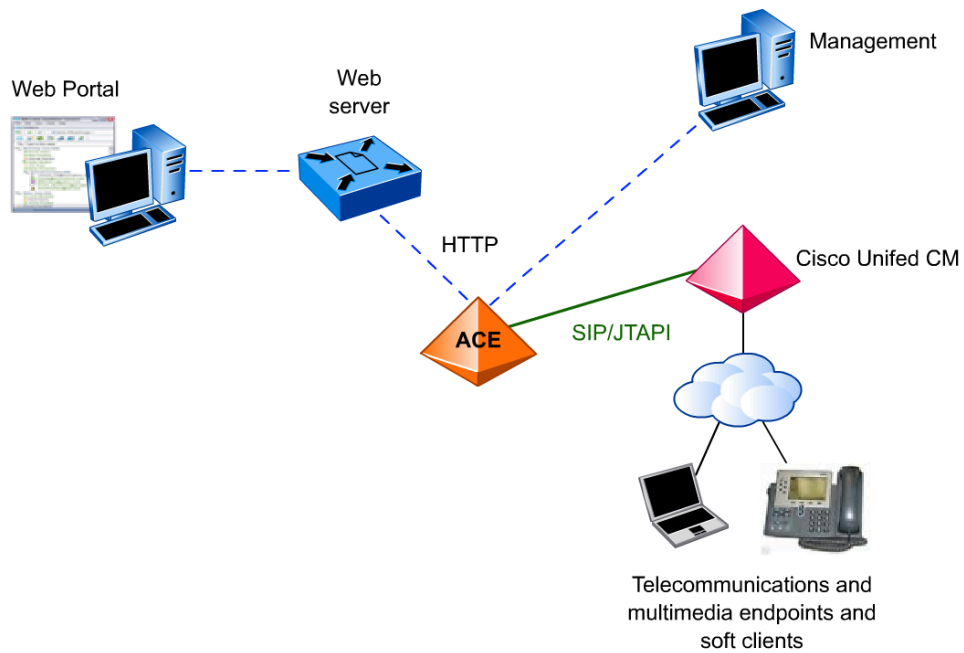


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example Cisco Unified CM deployment

The figure provides a simplified view of a Cisco Unified CM deployment.



Supported Cisco Unified CM network configurations

Cisco Unified CM service provider configuration requirements

CCM SIP service provider requirements

To support communications with the Avaya ACE, the Cisco Unified CM* network element must meet the following minimum configuration requirements:

- Cisco Unified CM is running Release 6.0 or higher software.
- SIP signaling over UDP is configured to receive traffic (SIP control messages) from ACE.
- SIP trunk is created.
- SIP Route Pattern is created.

CCM JTAPI service provider requirements

In addition, to support JTAPI, the CCM JTAPI service provider must meet these additional requirements.

- Cisco Unified CM is configured to support SIP Computer Telephony Integration (CTI).
- Avaya ACE is defined as an application user that can control CTI devices.
- The devices that Avaya ACE can control are assigned to the Avaya ACE application user.

* Also sometimes referred to as Cisco Call Manager (CCM)



Tip

JTAPI is a Java-based programming interface for computer telephony applications.

As defined by SearchNetworking.com: "JTAPI consists of a set of language packages. The core package provides the basic framework for simple Telephony processes such as placing a call, answering a call, and dropping a call. Several extension packages provide additional telephony features. JTAPI is interoperable across various computer platforms. JTAPI is similar to Microsoft and Intel's Telephony Application Programming Interface (JTAPI). JTAPI was developed in 1996 by a working group of computer and telecommunications companies including Intel, Lucent, Nortel Networks, Novell, and Sun Microsystems."

JTAPI is leveraged for selected web service because it is a more robust technology than SIP alone.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Tandberg VCS service provider fundamentals

Overview

The Tandberg video communication server (VCS) is a client-server solution that is deployed in the customer network to facilitate video networking and communications between H.323 and Session Initiation Protocol (SIP) video devices such as:

- video conferencing
- desktop video
- video
- voice over IP (VoIP)
- PC video

Avaya ACE and Tandberg VCS interworking

Avaya ACE provides a Tandberg service provider interfaces to provide web services and enable communications between Avaya ACE client applications and Tandberg VCS network elements.

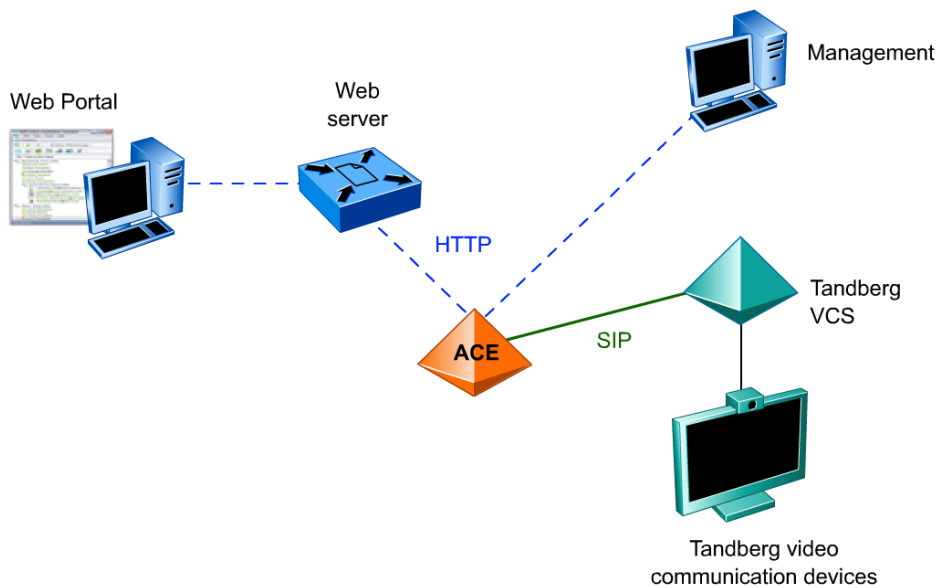


Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Example Tandberg VCS deployment

The figure provides a simplified view of a Tandberg VCS deployment.



Supported Tandberg VCS network configurations

Tandberg VCS service provider configuration requirements

Basic configuration requirements

To support communications with Avaya ACE, the Tandberg VCS network element must meet the following configuration requirements:

- The Tandberg VCS is running Release 2.0 or higher software.
- SIP mode is enabled on the VCS so that the VCS may act as a SIP Proxy Server.
- The UDP transport protocol is active.
- A SIP domain has been added and configured, and the Avaya ACE host has been added to the domain as a trusted endpoint.
- Authentication credentials (username and password) for the Avaya ACE host are defined in the VCS database.
- Tandberg video communication devices are provisioned and have successfully registered as SIP endpoint to the Tandberg VCS.
- SIP trunking over UDP between the Tandberg VCS and the ACE host is configured to support Avaya ACE traffic.

Click-to-video call support

For Click-to-video call support, the Tandberg video communication devices (for example, hard clients) have successfully registered as SIP endpoint to the Tandberg VCS.

Video soft client support

For Video soft client support, the Tandberg Movi server is installed, configured properly, and connected to the Tandberg VCS as a SIP registrar. (Movi is a server-based PC video conferencing solution.)

Tandberg VCS cluster support

For Tandberg VCS cluster, ensure that the call route mode is set to **Always** and that SIP interworking mode is set to **On**.

Caution: If the call routed mode is set to **Optimal**, the Tandberg VCS connected with the Avaya ACE may be dropped from the call.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Avaya service provider fundamentals

Overview

Avaya Aura™ is Avaya's flagship enterprise communications platform, supporting unified communications and contact center solutions. It enables SIP-based session management with innovative and powerful capabilities and provides a rich upgrade path for legacy DEFINITY systems. Key system components include:

- Communication Manager
- SIP Enablement Services
- Application Enablement Services (AES)
- Business phones, terminals, and other endpoint devices

The Communication Manager software is hosted on a supported server and controls call processing, call routing, and management for an Avaya communications solution.

In addition to traditional telephony services, the Communication Manager supports IP telephony and unified communications by leveraging open signaling standards, such as H.323 and Session Initiation Protocol (SIP). These services are offered through the SIP Enablement Services (SES) software platform. The Communication Manager also integrates with the Application Enablement Services (AES) software platforms to support applications development, and third-party client integration.

Avaya ACE and Avaya interworking

Avaya ACE provides TR/87 and SIP service provider interfaces to provide web services and enable communications between ACE client applications and Avaya Aura network elements. The Avaya Interactive Communications Portal (Avaya ICP) is used for services that require media treatment.



Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

SIP Enablement Services

A SIP trunk is configured on the SIP Enablement Services (SES) server to route the call back to the Avaya ACE server, so that Avaya ACE can choose an appropriate SIP endpoint to answer the call (for example, a supported media terminal). ACE can then add media services to an Avaya call either at call setup or as a new participant to an existing call.

The SES and Communication Manager are also linked by a SIP trunk. Dial plan changes and routing are set up on the Communication Manager and the proxy configuration is done on the SES.

Secure communications

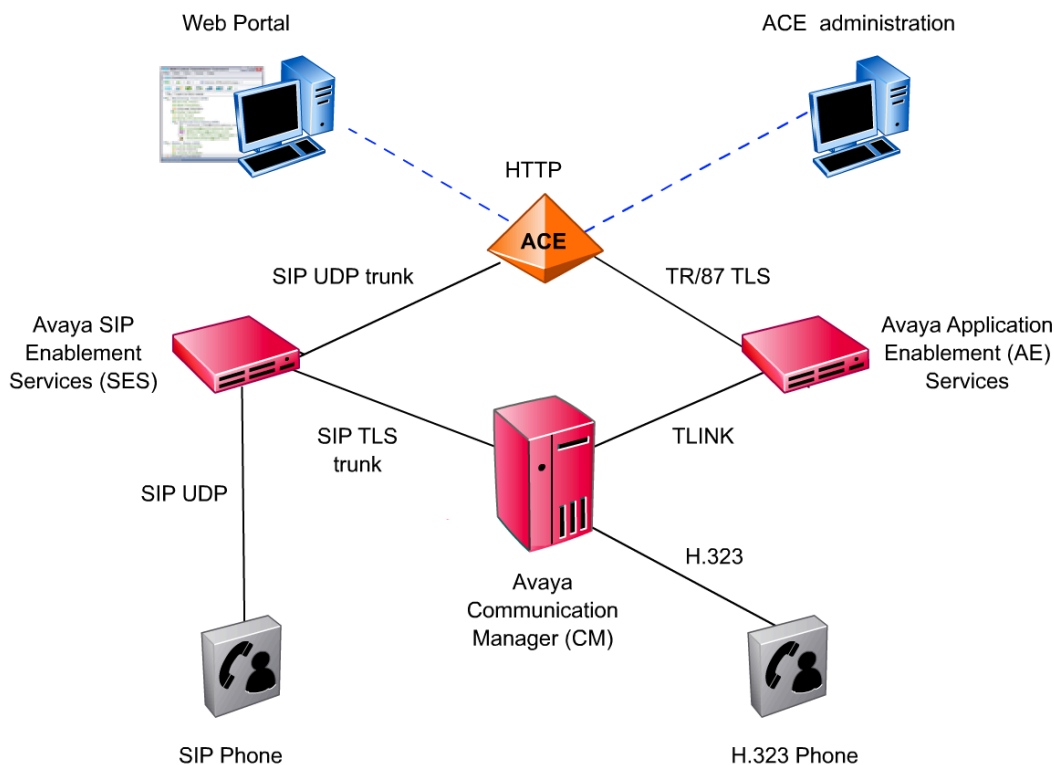
Avaya ACE supports secure connections to the Avaya AE Services using the Transport Layer Security (TLS) protocol. TLS encrypts data sent over connections between the servers. To secure communications from Avaya ACE to the AE Services server, you must have the required certificates on Avaya ACE and the AE Services server.

Example Avaya deployment

Within the Avaya ACE GUI, the Avaya network element is configured as an Avaya SIP or TR/87 service provider to support the Third Party Call Control (v2) or Third Party Call Control (v3). The Interactive Communications Portal (ICP) is required to support media services.

Avaya ACE connects to Avaya system via a standard SIP trunk, which is preconfigured on the Avaya SIP Enablement (SE) Services server. The SE Services server routes the Third Party Call Control (v3) calls back to Avaya ACE, so that ACE can choose an appropriate endpoint to answer the call; for example, the ICP. Avaya ACE can then add media services to a call either at call setup or as a new participant joins an existing call.

The SE Services and Communication Manager are also linked by a SIP trunk. Dial plan changes and routing are set up on the Communication Manager, and the proxy configuration is done on the SE Services trunk.



Supported Avaya network configurations

Avaya service provider configuration requirements

Avaya TR/87 service provider

To support communications with Avaya ACE using TR/87, the Avaya network element must meet the following minimum configuration requirements:

- The AE Services is running Release 4.1 or higher software.
- The AE Services is communicating with the Avaya Communication Manager.
- The AE Services has a dial plan for converting from Avaya ACE E.164 numbers to extensions on the Communication Manager.
- Each remote call controlled phone has an AE Services license for Unified CC API Desktop Edition.
- To support media services, the Avaya communications network must also meet the following configuration requirements:
 - The SES is running Release 5.0 or higher software.
 - The Communication Manager has the necessary dial plan changes configured to route to a trunk.
 - The SES is configured to proxy the trunk on to Avaya ACE.

Avaya SIP service provider requirements

To support communications with Avaya ACE using standard SIP, the Avaya network element must meet the following minimum configuration requirements:

- The SES is running Release 5.0 or higher software.
- The SES is communicating with the Avaya Communication Manager.
- The Communication Manager has the necessary dial plan changes configured to route to a trunk.
- The SES is configured to proxy the trunk on to Avaya ACE.
 - For standalone configurations, use the static IP address.
 - For high availability configurations, use the service provider interface floating IP address.
- Avaya ACE is added as a trusted host on the SES.
 - For standalone configurations, use the static IP address.
 - For high availability configurations, use the floating IP address for the service provider interface.

For more information, see *Avaya Agile Communication Environment Administration*TM (NN10850-005).

Secure communications requirements

Avaya ACE supports secure connections to the Avaya AE Services using the Transport Layer Security (TLS) protocol. TLS encrypts data sent over connections between the servers. To secure communications from Avaya ACE to the AE Services server, you must have the following:

- a trusted root certificate representing the Certificate Authority (CA) that signed the AE Services server certificate
- a CA-signed ACE certificate presented by the Avaya ACE server to the AE Services server
 - You must include the common name (CN) of the ACE certificate in the authorized hosts list on the Avaya AE Services.
 - This certificate must be signed by a trusted CA whose root certificate is imported into the Avaya AE Services trusted certificate list.
- the unencrypted private key associated with the Avaya ACE certificate

For high availability configurations, make sure that Avaya ACE certificates are created based on the service provider interface floating IP address and the DNS record for this IP address.

Checkpoint



When configuring a service provider, you must define at least one translation rule.

- ☐ True
- ☐ False

Answer : True



A supported media terminal is required to provide conferencing services and define the supported media treatment for selected web services; for example Third Party Call Control (v3) and Audio Call.

- ☐ True
- ☐ False

Answer : True

Module summary

Objectives

In this module you learned how to:

- Identify supported network elements and general service provider configuration guidelines.
- Identify the types and purpose of translation rules.
- Identify when it is necessary to deploy a media terminal, as well as general media terminal configuration parameters.
- Identify CS 1000 service provider fundamentals, including supported ACE web services and how Avaya ACE interacts with CS 1000 service provider network elements.
- Identify minimum CS 1000 configuration prerequisites to support communications with Avaya ACE.
- Identify CS 2000 service provider fundamentals, including supported Avaya ACE web services and how Avaya ACE interacts with CS 2000 network elements.
- Identify minimum CS 2000 configuration prerequisites to support communications with Avaya ACE.
- Identify CS 2100 service provider fundamentals, including supported web services and how Avaya ACE interacts with CS 2100 network elements.
- Identify minimum CS 2100 configuration prerequisites to support communications with ACE.
- Identify MCS 5100 service provider fundamentals, including supported services and how Avaya ACE interacts with MCS 5100 and AS 5200 network elements.
- Identify minimum MCS 5100 and AS 5200 configuration prerequisites to support communications with Avaya ACE.
- Identify NMC service provider fundamentals, including supported Avaya ACE web services and how Avaya ACE interacts with NMC network elements.
- Identify minimum NMC configuration prerequisites to support communications with ACE.
- Identify Avaya Contact Center/MLS service provider fundamentals, including supported web services and how Avaya ACE interacts with Contact Center/MLS network elements.
- Identify minimum Contact Center/MLS configuration prerequisites to support communications with Avaya ACE.
- Identify CCM service provider fundamentals, including supported web services and how Avaya ACE interacts with Cisco Unified CM network elements.
- Identify minimum Cisco Unified CM configuration requirements to support communications with Avaya ACE.
- Identify Tandberg VCS service provider fundamentals, including supported web services and how Avaya ACE interacts with Tandberg VCS network elements.
- Identify minimum Tandberg VCS configuration requirements to support communications with Avaya ACE.

- Identify Avaya service provider fundamentals, including supported web services and how Avaya ACE interacts with Avaya network elements.
- Identify minimum Avaya configuration requirements to support communications with Avaya ACE.

Operations, administration, and management

Introduction

Purpose

This module provides an overview of the operations administration and management (OAM) capabilities that the Avaya Agile Communication Environment™ (Avaya ACE™) offers, including interfaces, security, users and groups, fault management, and performance management.

Information about the configuration or management of IBM hardware and software is beyond the scope of this module.

Objectives

After completing this module, you will be able to:

- Identify the Avaya ACE OAM framework.
- Identify how to launch, log in to, navigate, and log out of the Avaya ACE GUI.
- Identify the configuration capabilities of Avaya ACE.
- Identify the fault management capabilities of Avaya ACE.
- Identify the performance management capabilities of the Avaya ACE.
- Identify the SNMP capabilities that Avaya ACE supports.
- Identify the security and user management capabilities of Avaya ACE.

Resources

Avaya ACE documentation:

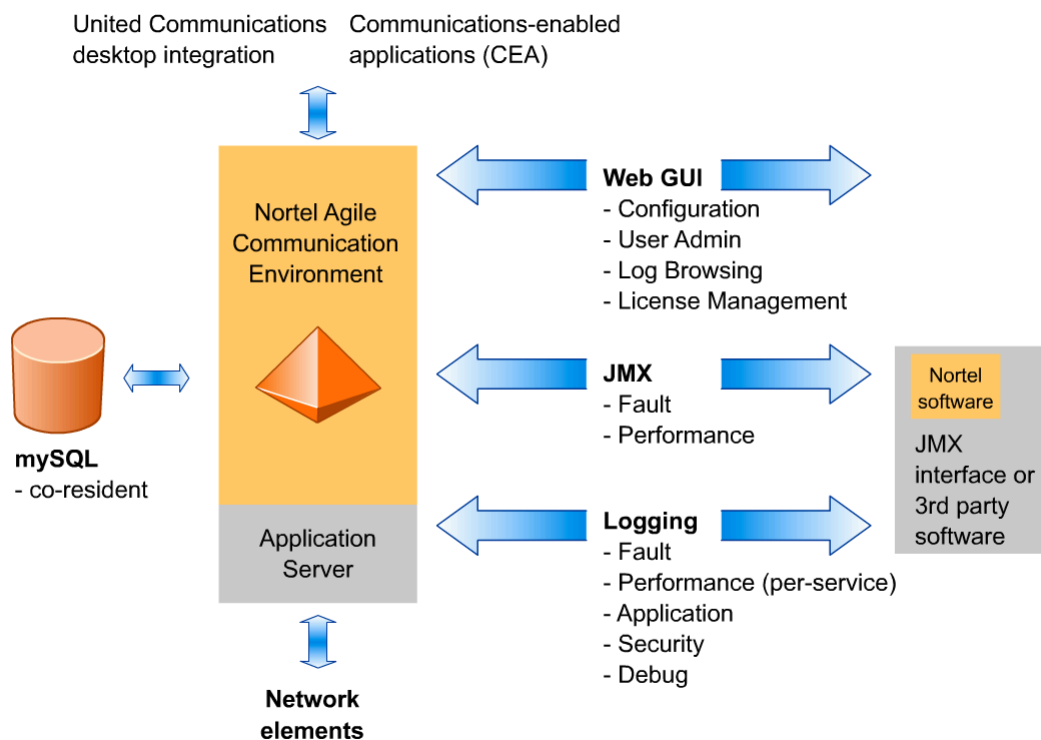
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Fault and Performance Management* (NN10850-009)

OAM framework

Description

From an OAM perspective, a system consists of a collection of managed components. A managed component is anything that needs to be monitored, configured, or controlled by user; for example, a hardware device or a collection of software objects. Each managed component is visible as a distinct entity at the management interface.

Avaya ACE utilizes a Java Management Extensions (JMX) bus with Web-Based Enterprise Management (WBEM) as the preferred external management interface. This open standard allows management through the Avaya ACE or by a third-party administrative terminal that is JMX-compliant, such as HP OpenView or IBM Tivoli.



JMX API

Java Management Extensions (JMX) is a Java application programming interface (API), developed and distributed by Sun Microsystems, Inc. As explained on the Sun Developers Network (SDN) web site:

"The Java Management Extensions (JMX) API is a standard API for management and monitoring of resources such as applications, devices, services, and the Java virtual machine. The JMX technology was developed through the Java Community Process (JCP) as Java Specification Request (JSR) 3, Java Management Extensions, and JSR 160, JMX Remote API."

Typical uses of the JMX technology include:

- Consulting and changing application configuration
- Accumulating statistics about application behavior and making them available
- Providing notifications of state changes and erroneous conditions

The JMX API includes remote access, so that a remote management program can interact with a running application for these purposes.

Within Avaya ACE, fault events are sent as JMX notifications to the Audit Logger and Alarm Manager, which are JMX agent services. User can retrieve fault logs and alarms via the management interface. In addition, users can acknowledge, unacknowledge, clear, and view alarms via the Avaya ACE GUI.

WBEM specification

The Web-Based Enterprise Management (WBEM) specification is published on the Distributed Management Task Force (DMTF) web site. The DMTF defines the WBEM specification as “set of management and Internet standard technologies developed to unify the management of distributed computing environments. WBEM provides the ability for the industry to deliver a well-integrated set of standard-based management tools, facilitating the exchange of data across otherwise disparate technologies and platforms.”

The DMTF describes key WBEM protocols as:

- **Common Information Model (CIM):** Conceptual framework for describing management data in an object-oriented environment.
- **Web Services for Management specification (WS-Management):** General web services management protocol based on SOAP that exposes services in the WS-Management interface.

JSR-262 specification

The Avaya ACE OAM uses the JSR-262 specification, Web Services Connector for Java Management Extensions (JMX) Agents, to define the mapping between Java applications and web management resources.

JSR-262 is published on the Community Development of Java™ Technology Specifications (JCP) web site. The JCP defines JSR-262 as, “a connector for the JMX Remote API that uses web services to make JMX instrumentation available remotely. Clients do not have to be Java applications, but can be.”

Avaya ACE GUI overview

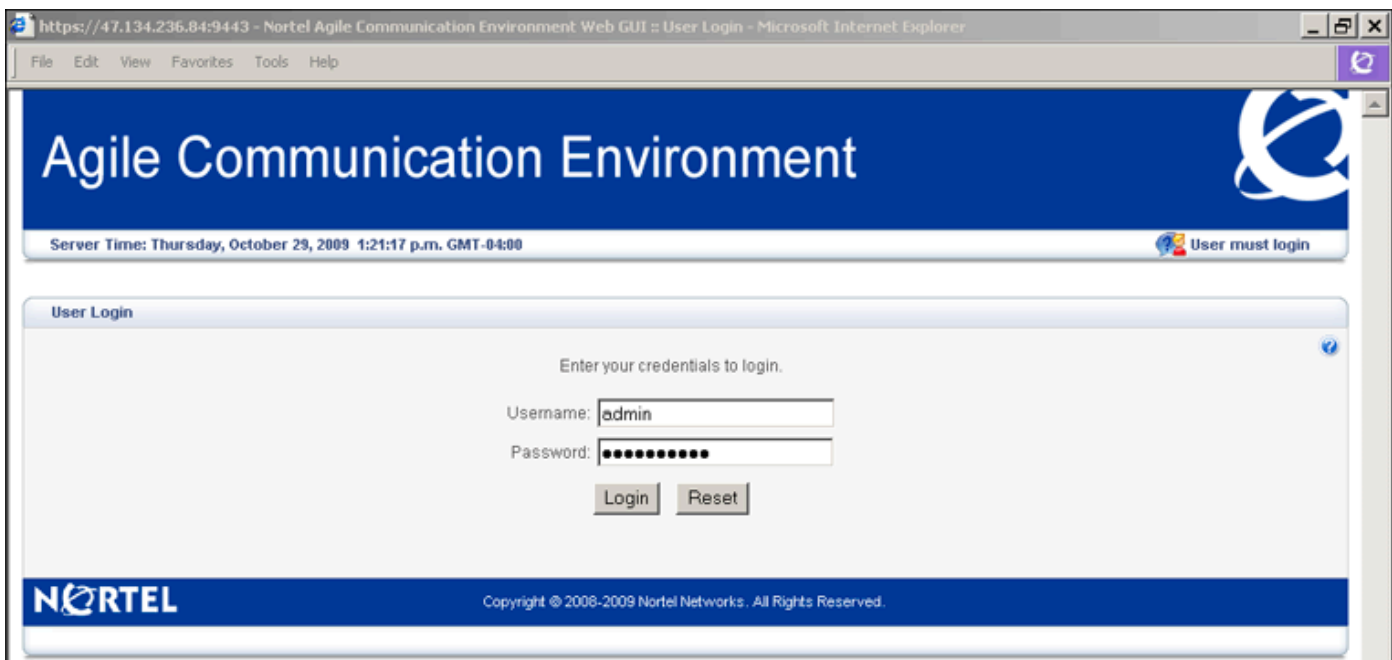
Description

Avaya ACE hosts a web-based graphical user interface (GUI). The Avaya ACE GUI allows administrators to perform all tasks related to system administration, configuration, fault management, performance management, and user management.

The Avaya ACE GUI is available following installation of Avaya ACE and is accessible via a supported browser as soon as the host is started. To access the Avaya ACE GUI, you must enter a valid username and password, previously defined in the Avaya ACE user profile database. Avaya ACE validates the user's credentials to determine access permissions. If a match is found, the user is successfully authenticated and granted access to the system.

For security reasons, change your password when you log onto the system for the first time. If you are the administrator, upon initial login using the root admin user account, Avaya ACE enforces a password change. This password change is only enforced on the root.

User Login

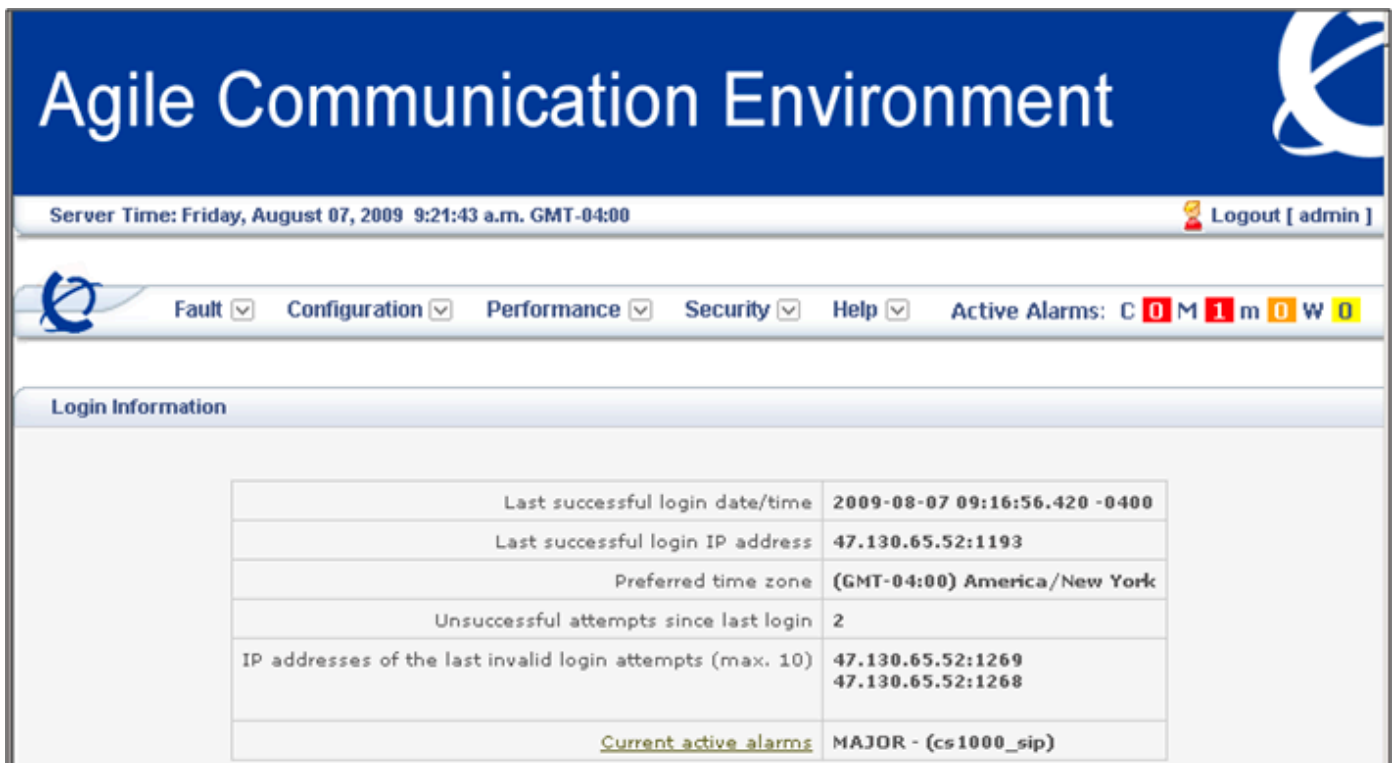


The screenshot shows a web browser window titled "https://47.134.236.84:9443 - Nortel Agile Communication Environment Web GUI : User Login - Microsoft Internet Explorer". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The main content area has a blue header with the text "Agile Communication Environment" and a logo on the right. Below the header, a status bar shows "Server Time: Thursday, October 29, 2009 1:21:17 p.m. GMT-04:00" and a "User must login" message. The central part of the page is a "User Login" form with the instruction "Enter your credentials to login." It contains two input fields: "Username:" with the value "admin" and "Password:" with masked characters. Below these fields are "Login" and "Reset" buttons. At the bottom of the page, there is a blue footer bar with the "NORTEL" logo and the text "Copyright © 2008-2009 Nortel Networks. All Rights Reserved."

Login information window

The Login Information window is the first window displayed upon successful authentication when you log on the ACE GUI. In addition, to user login information, the window includes an alarm banner that provides a real-time count of active alarms (**C**ritical, **M**ajor, **m**inor, and **w**arning).

The menu bar at the top of the window provides access to additional menus used for administration and management of the Avaya ACE system and services, service providers, and users.



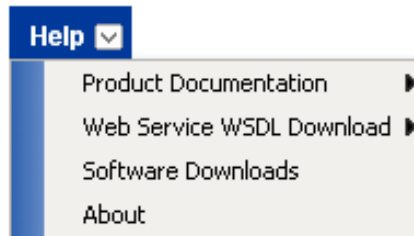
Last successful login date/time	2009-08-07 09:16:56.420 -0400
Last successful login IP address	47.130.65.52:1193
Preferred time zone	(GMT-04:00) America/New York
Unsuccessful attempts since last login	2
IP addresses of the last invalid login attempts (max. 10)	47.130.65.52:1269 47.130.65.52:1268
<u>Current active alarms</u>	MAJOR - (cs1000_sip)

Help menu

Avaya ACE provides a comprehensive help system to configure, operate and administer Avaya ACE. From the Help menu, you have quick access to:

- Product documentation
- Parlay X and custom WSDL APIs that ACE supports
- Software downloads
- Release information and end user license agreement

In addition to the Help menu, you can access contextual, web-based online help from the Avaya ACE GUI by clicking on the help icon (question mark) present on that window.



Configuration management

Description

The Configuration menu is used by the system administrator to perform configuration and management tasks related to the Avaya ACE server, services, and supported network elements (service providers).

Server

The Server window is used to view and configure information about the server that hosts Avaya ACE; for example:

- Name and fixed (static) IP address of the host
- Time when the system was initiated
- Version of operating system
- Debug log levels and log file rotation size
- Schedules
 - Removal of historical alarms in the database
 - Clearing of event data in the database
 - Performance logs

Services

The Services window is used to configure the format of logs that contain performance data for a web service.

The configurable parameters are:

- **Level:** Turns the recording of performance on or off.
- **Number of Backup Files:** Indicates the number of backup files allowed to reach before it is rolled over to backup files. Decreasing the Number of Backup Files is possible and the files collected during this period will be rolled over to the remaining backup files.
- **Maximum File Size:** Indicates the maximum size of the output file allowed to reach before it is rolled over to backup files. Changing the Maximum File Size is allowed during the collection period, but the change will only take effect on the next cycle. File size may be in the format of Kilobyte (KB), Megabyte (MB), and Gigabyte (GB). When the file reaches the maximum file size, the system closes the log file and rotates it to a backup log file. The system then opens a new current log file.

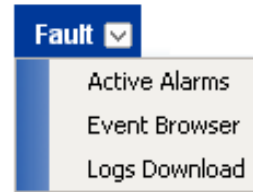
Service Providers

Within the Avaya ACE GUI, the Service Providers window is used to add, modify, and remove service providers to enable communications with Avaya ACE.

Fault management

Fault menu

The Avaya ACE fault management system allows you to monitor and manage the performance of the Avaya ACE system. In addition to a real-time count of active alarms on the Login window, the Fault menu provides access to access to the following windows:



- Active alarms: View and manage active alarms.
- Event browser: View event details.
- Logs download: Download logs for further analysis.

Active Alarms window

The Active Alarms window is used to view, analyze, and manage the active alarms. The Search Criteria dialog box enables you to filter your view.

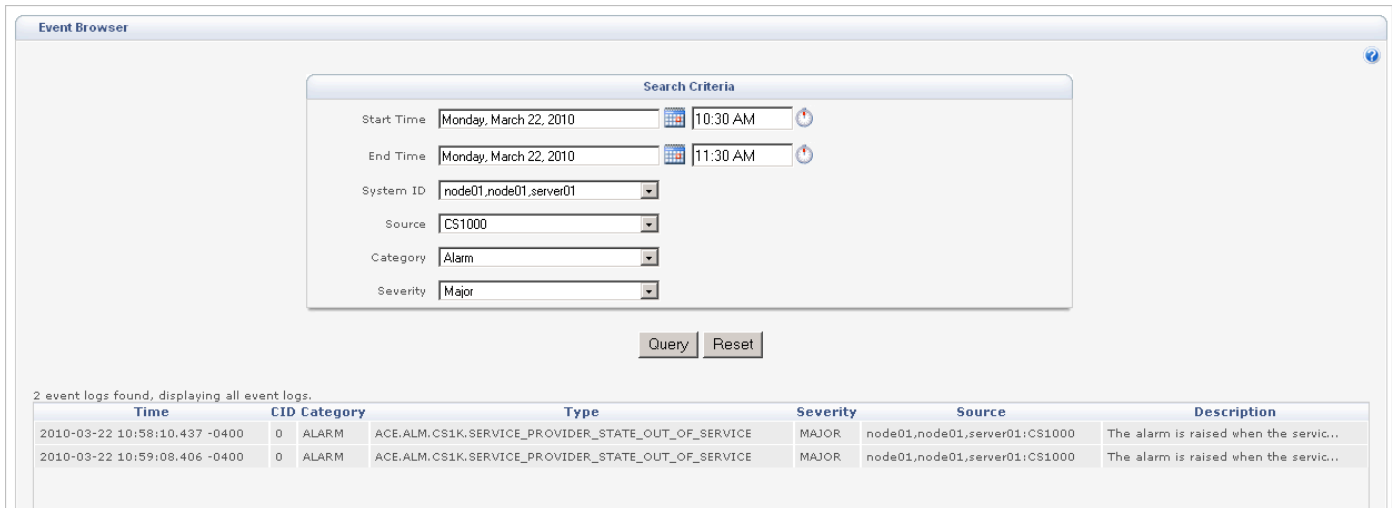
Attention: Clearing an alarm from the active alarm list does not fix the problem that caused the alarm. If the alarm condition continues, the system raises the alarm again until the problem causing the alarm is resolved.

Ack UnAck Clear Refresh							
Select: All None Unacknowledged Acknowledged							
Index	Severity	Category	System ID	Component ID	Type	Time Raised	
1	<input type="checkbox"/>	MAJOR	COMMUNICATIONS	node01,node01,server01	CS1000	ACE.ALM.CS1K.SERVICE_PROVIDER_STATE_OUT_OF_SERVICE	2010-03-22 10:59:08.406 - 0400
2	<input type="checkbox"/>	MINOR	ENVIRONMENTAL	node01,node01,server01	ADDRESS_MANAGER	ACE.ALM.ADDRESS_MANAGER.REQUIRE_SERVICE_AUDIT_FOR_PROVIDER_RULE_CHANGES	2010-03-22 11:00:16.093 - 0400

Event Browser window

During operation, all activities which take place within Avaya ACE are tracked and recorded. These are called events, which are either software or hardware related.

You can view them from the Event Browser, which is accessed from the Fault menu. You can view all events or search by specific criteria.



The screenshot shows the 'Event Browser' window. At the top, there is a 'Search Criteria' dialog box with the following fields:

- Start Time: Monday, March 22, 2010 10:30 AM
- End Time: Monday, March 22, 2010 11:30 AM
- System ID: node01,node01,server01
- Source: CS1000
- Category: Alarm
- Severity: Major


Below the search criteria, there are 'Query' and 'Reset' buttons. Below the buttons, a message states: '2 event logs found, displaying all event logs.'

The event logs are displayed in a table with the following columns: Time, CID, Category, Type, Severity, Source, and Description.

Time	CID	Category	Type	Severity	Source	Description
2010-03-22 10:58:10.437 -0400	0	ALARM	ACE.ALM.CS1K.SERVICE_PROVIDER_STATE_OUT_OF_SERVICE	MAJOR	node01,node01,server01:CS1000	The alarm is raised when the servic...
2010-03-22 10:59:08.406 -0400	0	ALARM	ACE.ALM.CS1K.SERVICE_PROVIDER_STATE_OUT_OF_SERVICE	MAJOR	node01,node01,server01:CS1000	The alarm is raised when the servic...

Logs Download window

Log files contain a historical record of system activities. The Log Downloads window is used to view information from the Avaya ACE GUI or download logs for future analysis using a third party network management tool.



The screenshot shows the 'Logs Download' window. At the top, there is a 'Filter Criteria' section with 'Start Date' and 'End Date' fields, each with a calendar icon, and 'Filter' and 'Reset' buttons. Below this, a status bar indicates '21 items found, displaying 1 to 20. [First/Prev] 1, 2 [Next/Last]'. The main area is a table with four columns: 'File Name', 'Time', 'Size', and 'Download'. Each row represents a log file, and the 'Download' column contains a blue download icon.

File Name	Time	Size	Download
adaptor_health_check.log	2009-11-05 09:54:35.562 -0500	0k	
alarmlog.xml	2009-11-05 13:01:06.250 -0500	2k	
appcore_event.log	2009-11-09 17:36:07.640 -0500	9k	
appcoredebuglog.log	2009-11-09 17:37:38.640 -0500	35k	
AUDIO_CALL_V3pmlog.xml	2009-11-09 17:35:02.421 -0500	2384k	
CALL_FORWARDING_V1pmlog.xml	2009-11-09 17:35:02.421 -0500	3710k	
CALL_HISTORY_V1pmlog.xml	2009-11-09 17:35:02.421 -0500	2387k	
CALL_NOTIFICATION_V38pmlog.xml	2009-11-09 17:35:02.421 -0500	3711k	
CALL_NOTIFICATION_V3pmlog.xml	2009-11-09 17:35:02.421 -0500	3710k	
CcmJtapiProviderpmlog.xml	2009-11-05 09:54:44.312 -0500	1k	
LOCATION_SUPPLIERpmlog.xml	2009-11-09 17:35:02.421 -0500	2389k	
MULTIMEDIA_CONFERENCE_V3pmlog.xml	2009-11-09 17:35:02.421 -0500	2398k	
PRESENCE_V3pmlog.xml	2009-11-09 17:35:02.421 -0500	8462k	
SametimeProviderpmlog.xml	2009-11-05 09:54:44.312 -0500	1k	
SUBSCRIBERpmlog.xml	2009-11-09 17:35:02.421 -0500	2381k	
SYSTEM_MONITORINGpmlog.xml	2009-11-09 17:35:02.421 -0500	2389k	
TERMINAL_LOCATION_V3pmlog.xml	2009-11-09 17:35:02.421 -0500	2393k	
THIRD_PARTY_CALL_V2pmlog.xml	2009-11-09 17:35:02.421 -0500	7739k	

Performance management

Performance menu

The Performance menu provides is used to view and analyze the performance of supported web services and service providers.



Example performance metrics

The figure shows performance metrics for the Audio Call service. Note that not all performance metrics are applicable to a specific web service; for example, Number of Notifications applies only to Presence (v3), Call Notification (v3.2), and Call Notification (v3.8) web services.

Search Criteria		
Service	Audio Call (v3)	

Performance Metrics for Audio Call (v3)		
Name	Value	Unit
Start Time	2010-03-22 11:55:00.000 EDT	
End Time	2010-03-22 12:00:00.000 EDT	
Number of Service Requests	0	
Number of Successful Responses	0	
Number of Failed Responses	0	
Request Completion Rate	0.0	
Average Response Time	0.0	Milliseconds
Maximum Response Time	0	Milliseconds
Minimum Response Time	0	Milliseconds
Total Response Time	0	Milliseconds

SNMP monitoring

Description

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-connected devices for conditions that require administrative attention. The capability is supported for ACE Linux and Windows deployments. Supported versions are SNMPv1 and SNMPv2c.

SNMP for Linux

SNMP for Linux monitors cluster status, storage, processes, memory, and system load. To enable SNMP for Linux, configure the ACE cluster SNMP while logged in as the root user. The appropriate parameters are defined in the `snmpd.conf` file.

SNMP for Windows

SNMP for Windows enables you to capture information about a device and report the information back to the central authority. SNMP for Windows is enabled through the Windows Control Panel.

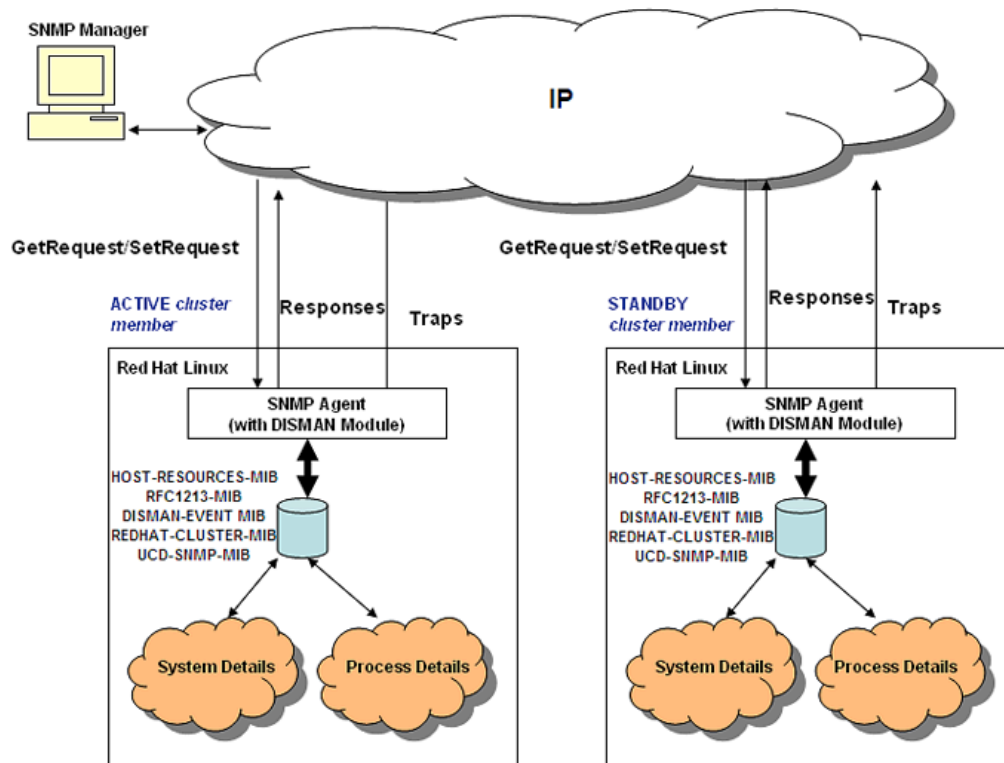


Tip

For general information about SNMP frameworks, see RFC 2571 at www.ietf.com.

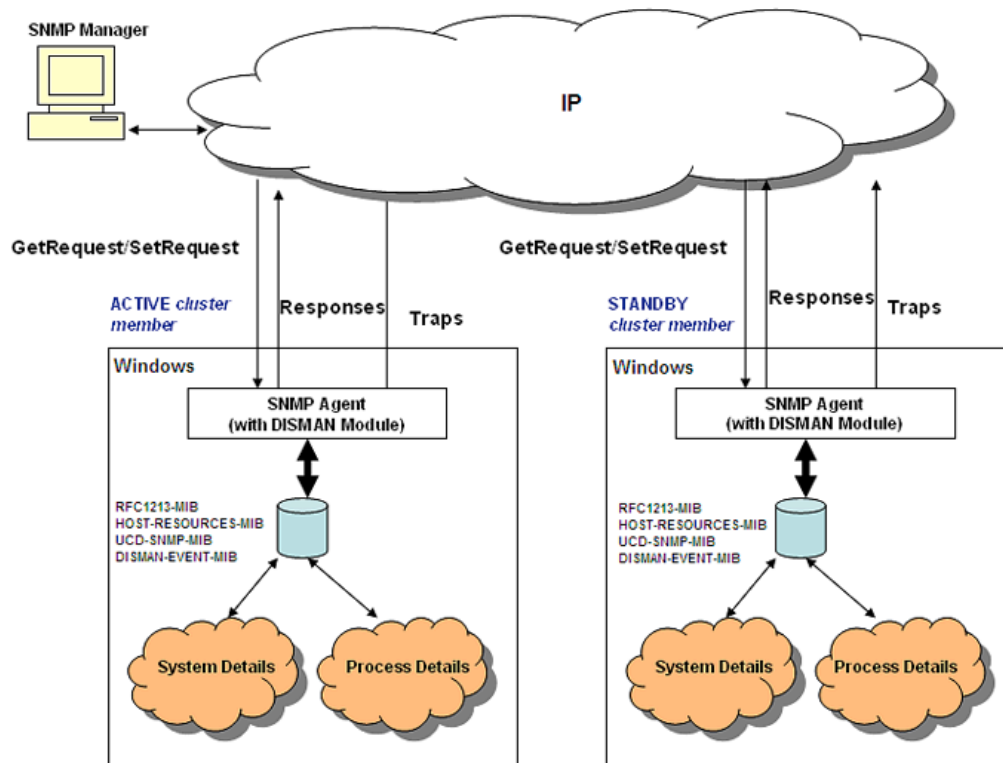
SNMP for Linux

The figure illustrates the relationship between Avaya ACE, Red Hat Linux, and SNMP.



SNMP for Windows

The figure illustrates the relationship between Avaya ACE, Microsoft Windows, and SNMP.



Security and user management

Security menu

The Security menu is accessed from the Avaya ACE GUI menu bar. From this menu the administrator can:

- List, edit, and create users
- List, edit, and create user groups
- View and change global security policies
- Change passwords
- View login information



User management

Users are anyone who uses Avaya ACE or consumes a service, including applications and clients. User information is stored in the Avaya ACE database in a user profile. At a minimum, each user profile requires a user ID and a password for user authentication. This password is subject to a set of rules specified in Global Security Settings, which are predefined by default but can be modified by the administrator, as necessary.

The screenshot shows a web-based form titled "User Information". It has a tabbed interface with the following tabs: "User", "Personal Data", "Organization Data", "Preferences", "User Group Membership", and "Account Policy". The "User" tab is currently selected. The form contains the following fields and controls:

- User ID:** A text input field containing the value "user".
- Account State:** A dropdown menu currently set to "Enabled".
- User Password:** A text input field filled with 12 dots, indicating a masked password.
- Confirm User Password:** A text input field filled with 12 dots, indicating a masked confirmation password.
- User must change password at next logon:** A checkbox that is currently unchecked.

User IDs guidelines

- Use only alphanumeric characters (a–z, A–Z, 0–9), hyphen (-), underscore (_), period (.), the symbol @ and the tilde (~).
- Ensure the user ID must be unique locally and across the federation (if ACE is part of a federated deployment). The system then uses these credentials to authenticate a user (or application) requesting access.
- Assign user IDs that already exist in the customer network.
- For integration with selected Windows-based applications, such as Hot Desking, make sure that user ID matches the user's desktop domain name; otherwise, users are prompted for their domain credentials when accessing the application.

Password guidelines

- The passwords must contain between 6 to 20 characters, with at least 1 alpha, 1 numeric, and 1 special character.
- The passwords must not contain the user ID, the reverse of the user ID, or more than 3 consecutive characters from the old password.
- The new password must differ from the old password by at least 2 characters

Contact information

The user profile often contains contact information for the user's registered communication devices (desktop, clients, mobile, video, etc.).

Guidelines for defining contact information are:

- **Contact Type:** Select the appropriate media type for the device; for example, telephone, video, chat, etc.
- **Contact Name:** Enter a meaningful name for the user's communication device that will help the user (or Avaya ACE client applications) identify it easily; for example, assign all mobile devices the contact name **mobile** and all office desk phones the contact name **deskphone**.

Important: Contact names are sometimes used by Avaya ACE client applications such as Hot Desking or Mobility to distinguish a user's mobile phone from a regular desk phone. For more information on the contact name requirements for Avaya ACE client applications, see the respective application documentation.

- **Contact Identifier:** Enter the number or address (in URI format) associated with the contact type.

Important: The expected syntax of the contact identifier value depends on the contact type and the format expected by the web service who makes use of this information.

- **Priority:** Enter a unique routing priority between 0.0 and 1.0, where 0.0 is the lowest and 1.0 is the highest.
- **Default CLI:** If enabled, specifies that this telephone contact is the default calling line identifier (CLI) for this user. When the user makes a call, regardless of the device or the priority of the device used to make the call, the contact information associated with the default CLI is presented to the called party.

User groups

Users are optionally assigned to a one or more user groups. User groups are logical groupings of users that share common characteristics and privileges. The group to which a user is assigned governs the access privileges. There are three types of user groups, from highest to lowest in privileges.

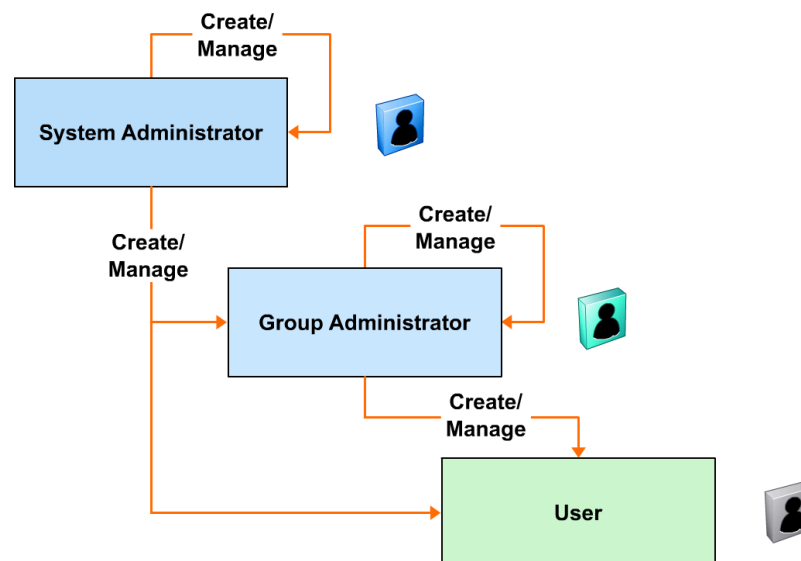
- **System Admin:** Can perform all tasks related to Avaya ACE system configuration, user management, and user authorization management.
- **Group Admin:** Can view, create, modify and delete user profiles under their own administrative domain.
- **User:** Can query their own user profile, change their own user password, and edit personal data and organizational data in their own user profile.

Access control rules

For each configured user group, the administrator selectively defines the required access level for the appropriate services. The options are Off (default), Read only, Read-Write, and Admin. When assigning access controls, remember the following.

- Access controls are inherited from parent to child. When an administrator creates a user group, the group automatically inherits access control rules settings of its parent. If required, the administrator can make the user group policy more restrictive, but a child can never have more permissions than its parent.
- Some client application users, such as IBM Sametime, Microsoft OCS, and Hot Desking, must be members of a group with Write privileges to invoke the specific web services they support.
- Some client applications, such as Event Response Manager, require their users be members a group with Write privileges to specific web services.

User group hierarchy



Predefined users

The following users are include with Avaya ACE, by default.

- **Admin:** Predefined system administrator profile, which cannot be deleted. Users with system administrator privileges can perform all tasks related to Avaya ACE system configuration, user management, and user authorization management. Change the default password upon initial login.
- **Federation:** Predefined profile used by internal system processes to allow inter-regional communications in a federated deployment. Change the default password upon initial login to the Avaya ACE GUI or disable the account if it is not required.
- **Sysmonitor:** Predefined profile used by internal system processes. No action is required upon initial login to the Avaya ACE GUI.

Predefined user groups

The following user groups are include with Avaya ACE, by default.

- **SystemAdminGroup:** Includes the predefined admin user as a member; however, other users or user groups can be added as members, as appropriate (for example, users, clients, or applications that require system administrator privileges). Service access controls are set to Off, by default.
- **FederationGroup:** Includes the predefined federation user as a member. Service access controls are set to Off, by default.
- **SystemMonitorGroup:** Includes the predefined sysmonitor user as a member. Service access controls are set to Off, by default.

Global security settings

Avaya ACE provides predefined global security settings that control user access to the Avaya ACE GUI and supported services; for example:

- General account policies, such as dormant and inactivity periods, maximum login attempts, and lockout periods
- Password rules, such as minimum and maximum length, character minimums, and invalid characters
- Access levels for configured services, such as Third Party Call Control, Audio call, Multimedia Conferencing, etc.

The default global security settings apply to all users who are not assigned to a configured user group. The ACE administrator can modify the default values, as appropriate.

The screenshot displays the 'Global Security Settings' window. It features a 'Policy Information' section with two tabs: 'Internal Account Policy' (selected) and 'User Group Policy'. Under the 'Internal Account Policy' tab, there are two sub-tabs: 'Account Policy' and 'Password Policy'. The 'Password Policy' sub-tab is active, showing the following settings:

- Password Expiry Period:** 0 day(s)
- Password Expiration Notification:** 5 day(s)
- Password History Size:** 12
- Password Rules:**
 - Minimum Password Length:** 6
 - Maximum Password Length:** 20 characters
 - Minimum Alpha Characters:** 1
 - Minimum Numeric Characters:** 1
 - Minimum Different Characters:** 2
 - Minimum Special Characters:** 1
 - Mixed Case Characters:** ☒ Yes, ☐ No
 - Permitted Special Characters:** |!#\$%&'()*+,-./=<>@{}^_~
- Invalid Passwords:**
 - Invalidate this Password:** [Text Field] **Add**
 - Invalid Passwords:** [List Box] **Remove**

Checkpoint



Global security settings apply to all users requesting access to the ACE GUI or a supported web services and cannot be changed, even by the system administrator.

- _____ True
_____ False

Answer : False



After you or the system correct a fault, ACE automatically clears the alarm condition.

- _____ True
_____ False

Answer : True



To prevent against the loss of administration control, the predefined admin user account cannot be deleted.

- _____ True
_____ False

Answer : True



SNMP monitoring is supported only in ACE Linux deployments.

_____ True

_____ False

Answer : False

Module summary

Objectives

In this module you learned how to:

- Identify the Avaya ACE OAM framework.
- Identify how to launch, log in to, navigate, and log out of the Avaya ACE GUI.
- Identify the configuration capabilities of Avaya ACE.
- Identify the fault management capabilities of Avaya ACE.
- Identify the performance management capabilities of the Avaya ACE.
- Identify the SNMP capabilities that Avaya ACE supports.
- Identify the security and user management capabilities of Avaya ACE.

Avaya ACE web services

Introduction

Purpose

The Avaya Agile Communication Environment™ (Avaya ACE™) enables application developers to communications-enable applications and business process, without needing to know detailed knowledge of the underlying network implementation and protocols. Because web services are exposed as individual components through their application programming interfaces (APIs), developers can combine, link, and customize services more rapidly and efficiently.

This module provides an overview of web service technologies, including how to build a web service. It also describes the web service APIs Avaya ACE supports.

Topics

After completing this module, you will be able to:

- Describe the web services that Avaya ACE supports.
- Describe the basic steps of web-enabled application development and common application development tools and technologies.
- Identify how to download supported WSDLs from the Avaya ACE GUI.

Resources

Avaya ACE documentation:

- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)

Supported web services

Supported web services

Avaya ACE supports selected Parlay X Version 2 and Version 3 web services and custom services. Parlay X Version 3 consists of functional updates to existing Parlay X Version 2 web services, and the addition of new web services. Supported services are:

- **Third Party Call Control (v2):** Provides click-to-call functionality between two endpoints.
- **Third Party Call Control (v3):** Initiates and manages a single- call or multiple-party calls through a call server.
- **Call Notification (v3):** Allows an application to manages call notification functionality, such as called party address and number for Third Party Call Control (v2/v3) sessions.
- **Call notification (v3.8):** Allows an application to receive an event each time a user's terminal device is called, containing the number of the party attempting to place the call.
- **Call Forwarding:** Allows a device to redirect an incoming call to another device when specific conditions are met.
- **Call History:** Allows an application to instruct the Avaya ACE host to create and store records for incoming calls for retrieval by address or user name (user ID).
- **Terminal Location (v3):** Retrieves location information about a mobile terminal and supports queries from applications to trigger other events.
- **Location Supplier:** Allows a device to publish location information to a terminal device.
- **Audio Call (v3):** Allows an application to add or drop audio content in an existing call, and monitor message delivery.
- **Multimedia Conference web service (v.3):** Allows an application to create multimedia conferences and dynamically manage the participants involved.
- **Presence:** Collects presence information for users registered with one or more network elements.
- **User profile:** Supports user management operations, including operations related to the management of global security policies and individual user group policies. It is included automatically and enabled by default.
- **System monitoring:** Allows a service client to monitor the health of applications.
- **Subscriber Management:** Allows client applications to query subscriber information either locally or globally for federated deployments.
- **Third Party Call Extensions:** Allows an application to support Third Party Call Control (v2) call sessions and call sessions placed through the CS 1000 TR/87 network element.
- **Message Drop and Message Blast:** Automates voice recording and broadcasting of audio messages to specified recipients.

Authentication and authorization

Access to Avaya ACE is controlled using HTTP 1.1 basic authentication. Requests must contain a valid user name and password that correspond to a user profile configured in Avaya ACE.

Authorization for individual web services is configured on a service-by-service basis. The user account configured for the web service client (application) must have the appropriate access control rules set to invoke a particular web service.

Secure web service communication

By default, web service communication is supported on the secure (HTTPS) and non secure (HTTP) ports. A consumer of a web services can choose to completely secure all web service communication (including notifications).

Important: For secure communication, ensure that the Avaya ACE version and the ports on the host server match. To establish secure-only communication with the Avaya ACE host, you must explicitly disable the nonsecure ports. For high availability (HA) deployments, perform this procedure on both hosts.

Application development

Commonly used tools and technologies

Some commonly used development tools and technologies are listed below.

- **Apache AXIS:** Java platform for creating and deploying web services applications
- **Apache Web Services Invocation Framework (WSIF):** Java API for invoking Web services
- **.NET:** Microsoft Web browser-oriented platform that includes servers, building-block services (such as Web-based data storage), and device software
- **Perl:** High-level, general-purpose, interpreted, dynamic programming language
- **Ruby on Rails:** Open source development toolkit for creating web services
- **SOAP4R:** Implementation of Ruby SOAP 1.1 specification that provides support for developing clients/servers and generating client interfaces from WSDL files
- **soapUI:** Software used to test SOA applications

Example tools and technologies

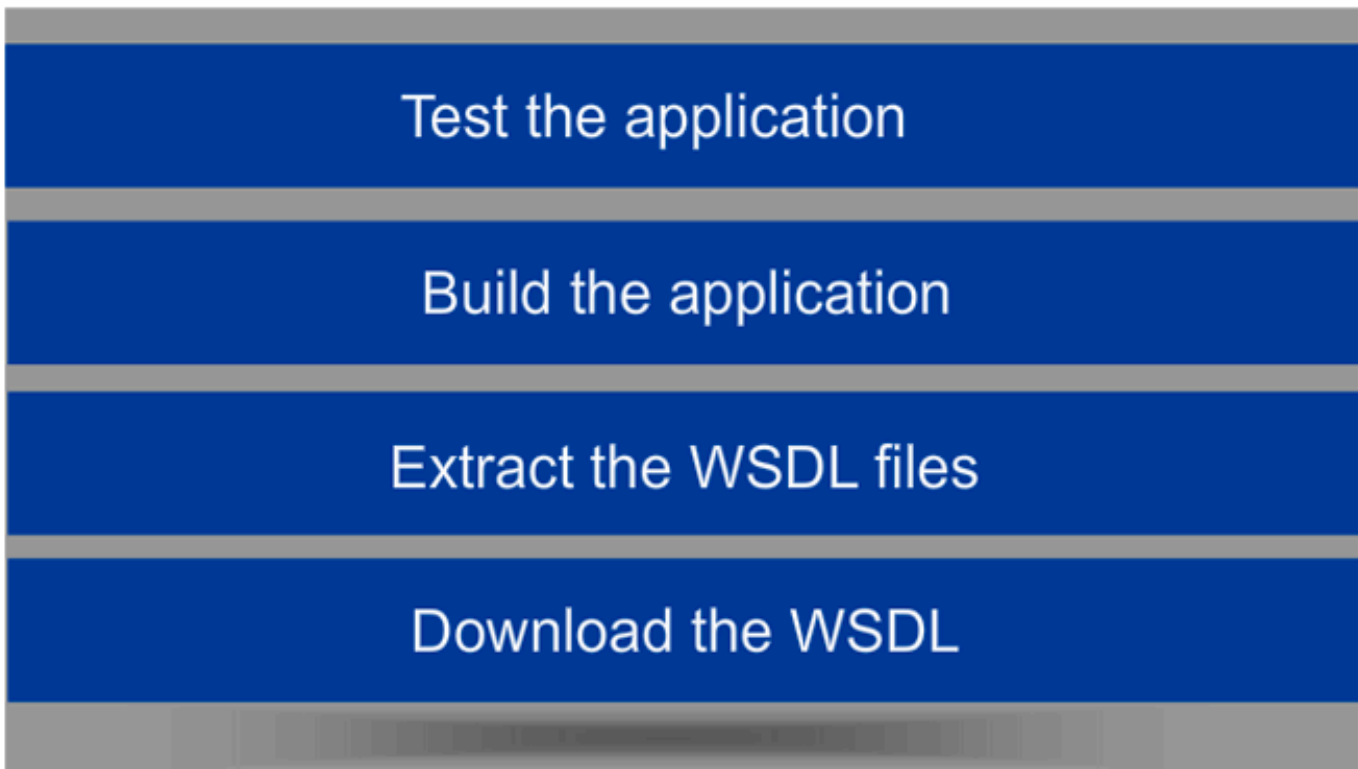


Basic steps for developing a web-enabled applications

The basic steps for developing a web-enabled application are:

- Download the WSDL.
- Extract, if necessary. (May not be required, if downloading from the ACE GUI.)
- Build the application.
- Test the application.

Basic steps for developing a web-enabled applications

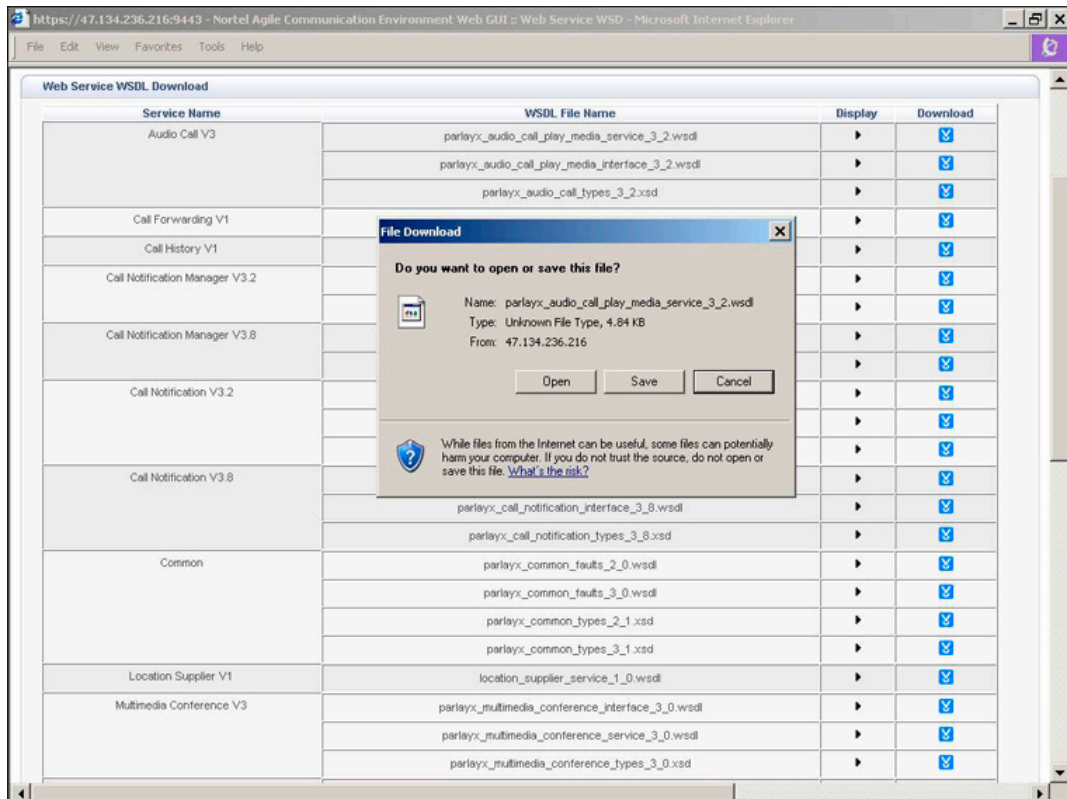


WSDL download

Description

Supported Avaya ACE WSDL APIs are available for download from the Help menu of the Avaya ACE GUI.

Web Service WSDL download



Checkpoint



Match the web service to the best definition or example. The correct answers display when you check your work.

1. Prompts a call to be redirected to another device in an incoming call situation.
2. Includes mandatory user data such as a user name, password, and optionally personal data and contact information such as email, address, telephone number(s), and other information that may be required in support of other web services.
3. Can provide click-to-call functionality on a web portal.
4. Sends a prerecorded, automated meeting reminder.

Third party call control (v2)

___ 1 ___ 2 ___ 3 ___ 4

Audio call (v2)

___ 1 ___ 2 ___ 3 ___ 4

User profile

___ 1 ___ 2 ___ 3 ___ 4

Call forwarding

___ 1 ___ 2 ___ 3 ___ 4

Answer: Third party call control (v2): 3. Can provide click-to-call functionality on a web portal. Audio call (v2): 4. Sends a prerecorded, automated meeting reminder. User profile: 2. Includes mandatory user data such as a user name, password, and optionally personal data and contact information such as email, address, telephone number(s), and other information that may be required in support of other web services. Call forwarding: 1. Prompts a call to be redirected to another device in an incoming call situation.

Module summary

Objectives

In this module you learned how to:

- Describe the web services that Avaya ACE supports.
- Describe the basic steps of web-enabled application development and common application development tools and technologies.
- Identify how to download supported WSDLs from the Avaya ACE GUI.

Avaya ACE applications

Introduction

Purpose

Avaya Agile Communication Environment™ (Avaya ACE™) provides both a developer-friendly tool kit for custom applications and a set of packaged applications that are easy to install and offer customers a hard dollar return on investment – often with an in-year payback.

This module provides an overview of the applications and add-ins that Avaya ACE supports. It reviews some common types of Communications-Enabled Applications and Business Process (CEBP) solutions that Avaya ACE supports.

Topics

After completing this module, you will be able to:

- Identify the applications, add-ins, extenders and communications-enabled applications and business processes (CEBP) that Avaya ACE supports.
- Describe the Personal Assistant solution, including its purpose and key features.
- Describe the Unified Communications add-ins solution, including its purpose and key features.
- Describe the Message Drop and Blast solution, including its purpose and key features.
- Identify the Communications-Enabled Applications and Business Processes (CEBP) that Avaya ACE supports, and describe their purpose and key capabilities. Describe ACE Communications-Enabled Applications and Business Processes (CEBP) solutions, including its purpose and key features.
- Describe the AIE.
- Describe key features and capabilities of the AIE.
- Describe the Hot Desking solution, including its purpose and key features.
- Describe the Hot Desking and IBM Sametime integration solution, including its purpose and key features.
- Describe the Mobility application solution, including its purpose and key features.
- Describe the Event Response Manager solution, including its purpose and key features.

Resources

Avaya ACE core documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Fault and Performance Management* (NN10850-009)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)
- *Administration - Microsoft Office Communications Server Integration* (NN10850-012)
- *Alarms Reference* (NN10850-015)
- *Audit Log Reference* (NN10850-016)
- *Performance Measurement Reference* (NN10850-017)
- *Error Messages Reference* (NN10850-018)

Resources

Avaya ACE applications documentation:

- *Personal Assistant Application* (NN10850-032)
- *Message Drop and Message Blast Administration* (NN10850-025)
- *Hot Desking User Guide* (NN10850-030)
- *Hot Desking Application Installation Guide* (NN10850-035)
- *Hot Desking Mobile Interface Guide* (NN10850-036)
- *Hot Desking Administration Guide* (NN10850-037)
- *Hot Desking Application Web Portal Integrator Guide* (NN10850-038)
- *Hot Desking Application for Sametime Connect User Guide* (NN10850-046)
- *Avaya Application Integration EngineTM Fundamentals* (NN10850-021)
- *Mobility Application Administration* (NN10850-027)
- *Mobility Application for BlackBerry* (NN10850-028)
- *Event Response Manager Installation* (NN10850-048)

Applications overview

Description

This section provides an overview of the following applications and solutions that Avaya ACE supports.

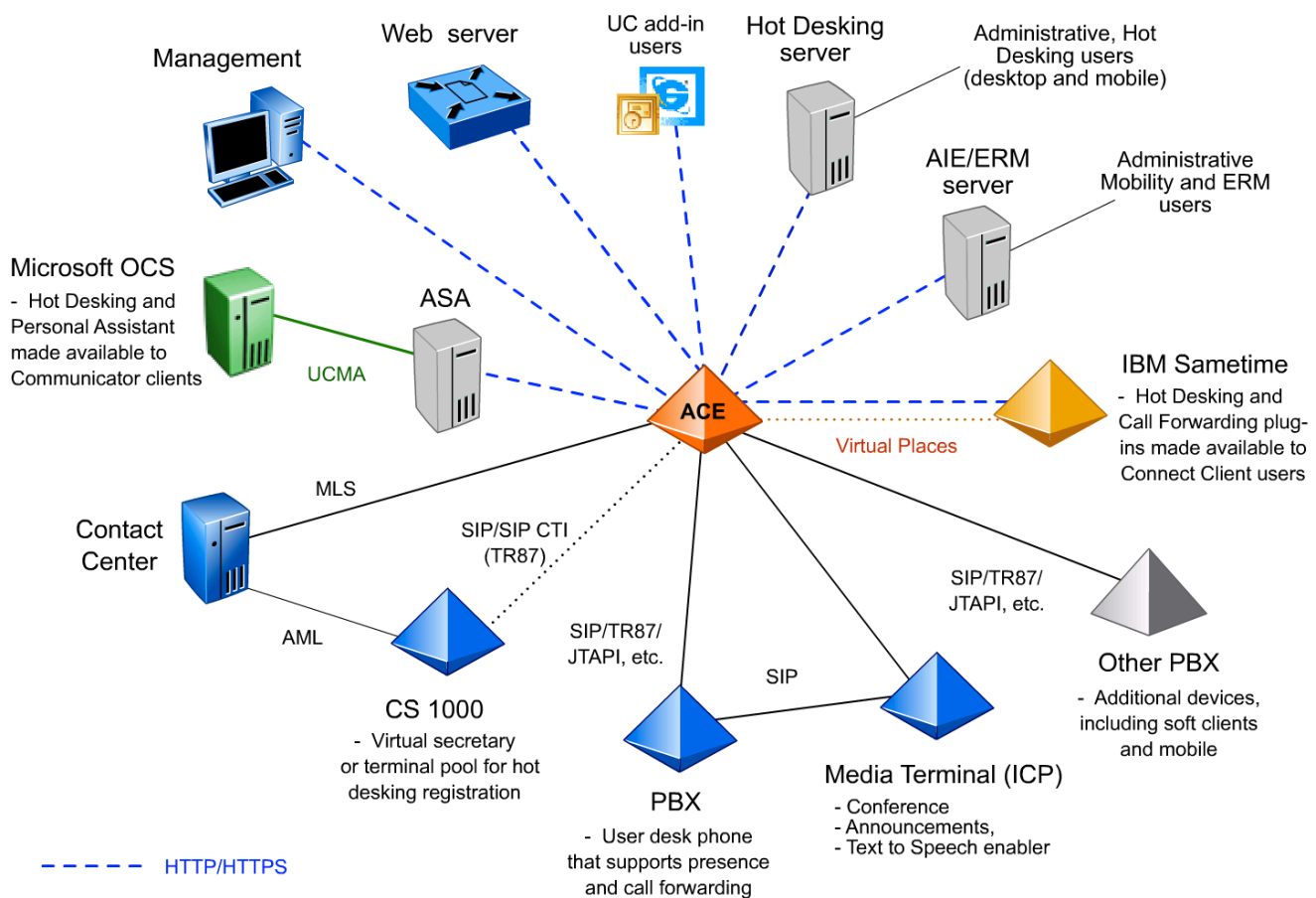
- Personal Assistant
- Mobile Blast and Drop
- Communications-enabled solutions
- Browser and Microsoft Outlook Add-ins
- Avaya Application Integration Engine™ (AIE)
- Hot Desking
- Hot Desking and Call Forwarding plug-ins for IBM Sametime
- Mobility application
- Event Response Manager

Example applications deployment architecture

The figure shows a simplified view of a network that includes Avaya ACE and selected applications.

Access to web services is controlled using HTTP 1.1 basic authentication, where all SOAP messages to the web service interface must contain a valid user name and password that correspond to a user profile configured in the Avaya ACE user profile database.

Avaya ACE, by default, supports web service communication on both the secure (HTTPS) and non secure (HTTP) ports. As a consumer of the web services, you can choose to completely secure all web service communication (including notifications) with Avaya ACE.



Personal Assistant solution overview

Description

The Personal Assistant (PA) is an application that gives Avaya ACE users basic user privileges to manage personal preferences and settings, previously defined in Avaya ACE; for example, contact device settings and passwords. The PA application is included with Avaya ACE and is installed automatically when Avaya ACE is initially deployed. It is accessible via a desktop or mobile browser.

The PA application is also accessed from the Microsoft Office Communicator client tab (Communication Server 2000 deployments only). For use with Microsoft OCS, the PA plug-in must first be installed and configured.

PA user login from desktop browser

Agile Communication Environment

Call History Devices Settings Logout ?

Profile Settings

🔒 Change Password

Old Password

New Password

Confirm New Password

✓ Change Password ✗ Cancel

- Min Password Length: 6
- Min Alpha Characters: 1
- Min Numeric Characters: 1
- Min Different Characters From Old Password: 2
- Min Special Characters: 1
- Mixed Case: true
- Permitted Special Characters: !#\$%()*+,-./=<>@[]{}~_-

Browser and Microsoft Office Add-ins solution overview

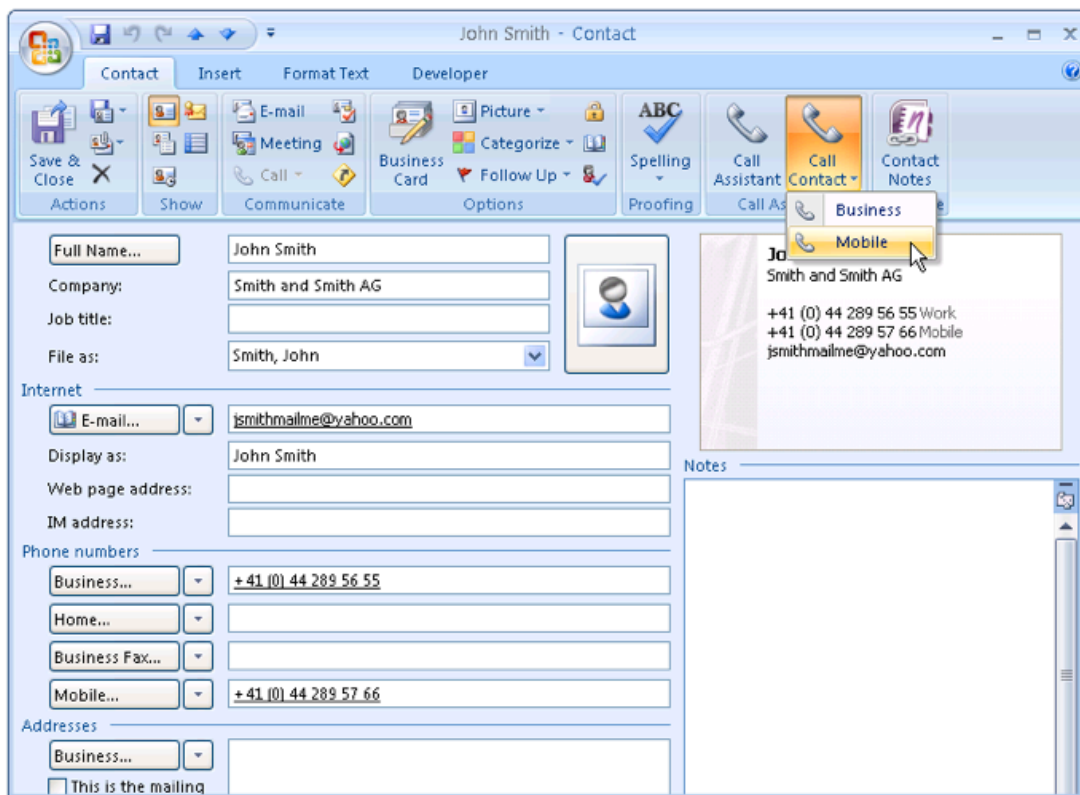
Description

Avaya ACE provide add-ins that integrate with Microsoft Outlook and Internet Explorer to offer new communications capabilities.

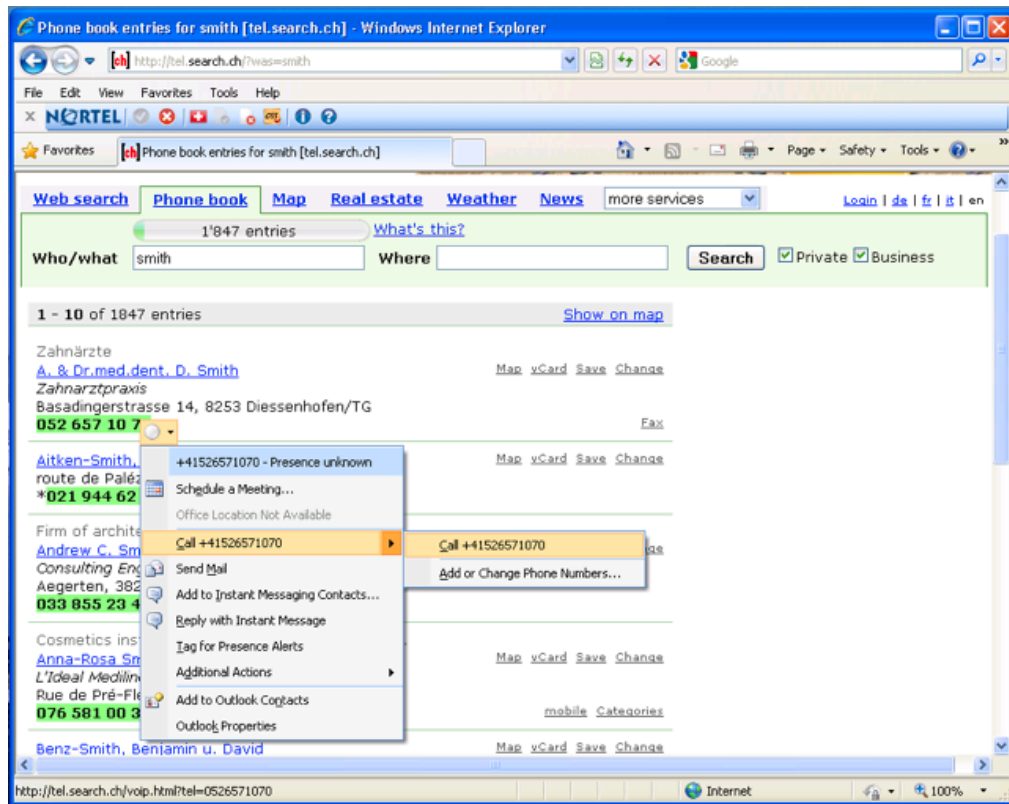
- The **Office add-in** gives Outlook 2007 users the ability to select mail, contact, calendar, task, or journal items and initiate a call, to the originator of the item, with a simple click.
- The **Browser add-in** for Internet Explorer embeds additional functionality, such as click-to-call, click-to-IM, import contacts, and email, into external and internal web pages.

The add-ins are installed on the user's PC and communicate directly to Avaya ACE using SOAP over HTTP/HTTPS.

UC Office add-on



Browser add-on



Message Drop and Blast solution overview

Message Drop and Blast

The Message Drop and Blast web service communications-enables customer relationship management (CRM) tools.

Key features include:

- **Click to Dial:** Allows users to initiate a call with a soft client or a desktop.
- **Voice Drop:** Allows users to insert audio messages into an ongoing call.
- **Voice Blast:** Allows users to deliver the same pre-recorded message to a selected group of individuals at a specified time.
- **Telset Recording:** Allows users to record announcements from their desktop phone or system and store the announcements on the network for retrieval in a Voice Drop or Voice Blast action.
- **Scheduled Distribution and Logs:** Allows users to predefine the time for the blast
Maintains a record of what the user does and what are the results of the actions

Benefits include:

- One click to provide thousands with same message at same time
- Inform employees or user groups of critical events
- Can be driven by external events automatically (CEA)
- Time Savings, Ease of Use and Mass Coverage

The Message Drop and Blast service resides on the ACE Windows-based server. An Avaya Interactive Communications Portal (Avaya ICP) is required to supply media treatment.

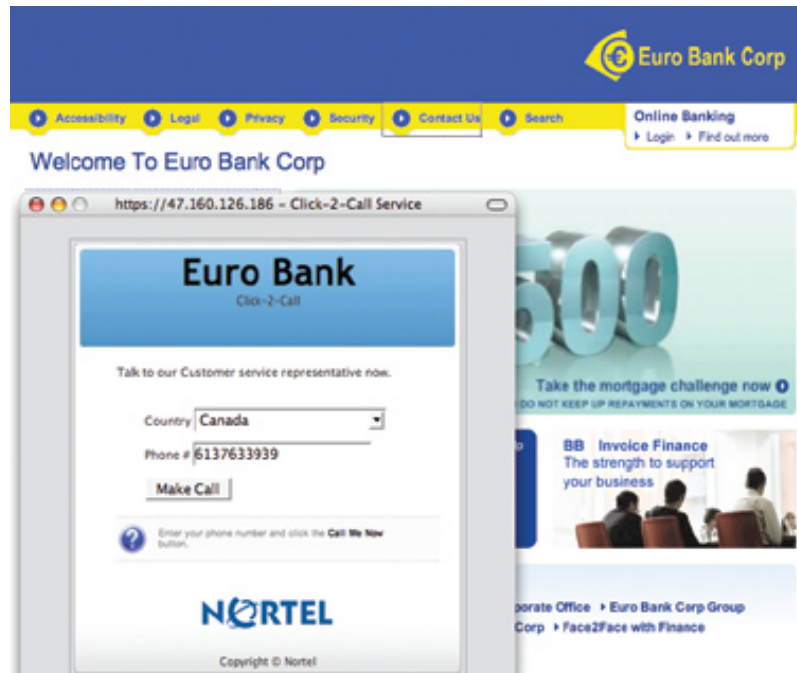
CEBP solution overview

Sales Portal

The Sales Portal communications-enables your external customer portal with Click-to-Call.
Key capabilities are:

- Click-to-call anyone who is in the directory or contact list (internal or external).
- Optional: Allow customers to see the presence of employee, whether telephony, IBM Sametime, or Microsoft OCS

Example Sales Portal



Corporate Directory

Avaya ACE enables you to communications-enable your corporate directory, with Click-to-Call and Presence. Key capabilities are:

- Call a co-worker from the web directory.
- Check to see if a co-worker is on the phone before calling.
- Click-to-call anyone who is in the directory or contact list (internal or external).
- Easily add video or other communication devices
- Optional: See a co-worker's IBM Sametime or Microsoft OCS presence.

Example Corporate Directory

Top Links

- Knowledge Base
- Human Resources
- Blogs & Forums
- Travel Resources
- IT Help
- Job Shop

Top Stories

Nortel Reveals Managed Services
Lancor Corp has announced an extension of its global capabilities in the IT domain. The company has presence in managed services and systems integration, and now further capabilities are established – enabling increased focus on managed services and hosting in the IT domain. [Full Story]

Business Monitors

Condor Trade Policy
Date: 05/05/2009 - 10:27:02
Status: In Progress
Info Edit Remove

SAP Orders
Date: 02/05/2009 - 10:32:02
Status: In Progress
Info Edit Remove

E-Store System Health
Date: 05/05/2009 - 10:32:02
Status: In Progress
Info Edit Remove

Competitor Edge

IT in the News	Stocks
Infrastructure big winner in NT budget (Bl...	CONDOR 38.9 ▼ -1.35
Modest Budget boost for NT regions (Austra...	RINM 74.92 ▲ 0.429
NT budget focusses on Infrastructure (SKY...	HP 32.5 ▼ -0.71
Internet glitch hits NT again (Australian...	CSC 37.66 ▼ -0.21
	MSFT 19.85 ▼ -0.33
	IBM 106.0 ▼ -0.15
	AAPL 131.8 ▼ -0.17

Corporate Wiki

Popular Items	Recent Wiki News
Knowledge Base Training 2009-05-04 John McKinnon	Wiki Security Updates 2009-05-05 Jane Altmann
Intelligent Routing 2009-05-03 Jane Altmann	Attaching Documents 2009-05-04 Albert Bekker

Contacts

Department Location

SE Stuttgart

Sunrise
John McKinnon
Jane Altmann

Personal Banking
Sunrise

Finance
Macquarie
Albert Bekker
Sunrise
Evan Pearson

Marketing
Falls Church
Ed Purdy

Technical Sales
Falls Church
Lamont
McGlynn
Melany Schimmel

IT Support
Anderi
Laurianne D'Amore

Jane Altmann
1500 Concord Terrace
Sunrise, FL
US
Away (Chat) and Available (Phone). Updated 17 minutes ago.
View Service Deliveries
Send SMS
Call Business - 61919-271-5801
Call Mobile - 954-899-1621

AIE solution overview

Description

The Avaya Application Integration Engine™ (AIE) is hosted on a supported Windows server and provides a software engine to deliver selected Avaya ACE applications, such as Mobility and Event Response Manager. The AIE is configured to interwork with the Avaya ACE host and acts as a bridge between Avaya ACE and client application service requests.

After installation and configuration, the AIE provides a web-based graphical user interface (GUI) for AIE administration and maintenance of applications. For more information about the Avaya ACE core solution, see *Avaya Agile Communication Environment™ Planning and Installation™ Fundamentals* (NN10850-004).

AIE Server Status	
Host name	47.134.235.32
IP Address	47.134.235.32
Operating System Time	Mon Mar 01 16:04:47 EST 2010
AIE Version	2.2.0-SNAPSHOT revision 12072
Operating System	Windows 2003 5.2
Application Container Version	Apache Tomcat/6.0.18
Application Container Status	RUNNING (5 days, 4 hours, 46 minutes and 24 seconds)
Application Status	hotdesk RUNNING (sessions:0) devices RUNNING (sessions:0) mobility RUNNING (sessions:0) thirdpartycall RUNNING (sessions:0) oamp RUNNING (sessions:2)
Memory (free/total)	1313 MB / 1799 MB
JVM Version	1.6.0_16-b01
JVM Memory (free/total/max)	27656 KB / 129792 KB / 259264 KB
ACE Connectivity	UP
Database Connectivity	UP

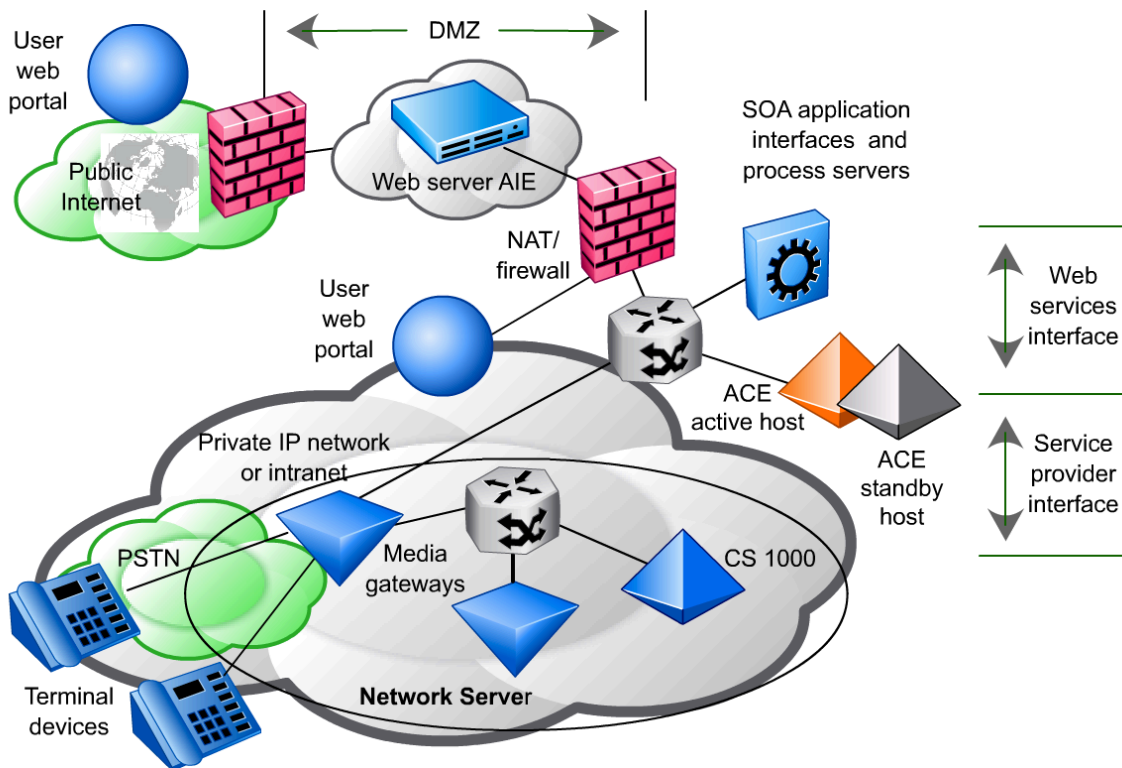
NORTEL Copyright © 2008-2009 Nortel Networks. All Rights Reserved. 2.2.0-SNAPSHOT revision 12072

AIE architecture

AIE interface

Administration for selected applications is available through the Application Integration Engine™ (AIE) web-based graphical user interface (GUI).

Example AIE deployment architecture



Hot Desking solution overview

Description

Hot Desking allows users to bring their office wherever they go. Hot Desking improves productivity for mobile workers and reduces real estate and telephony costs, while improving customer satisfaction through increased employee availability.

Hot Desking is deployed on a Windows server in an existing customer network that includes a SIP-enabled communication system. It interworks with Avaya ACE to provide a signalling-based solution that requires no reserved circuits.

Key features

Key Hot Desking features are:

- Profile management: Ability to modify personal settings, such as primary device and call forwarding parameters
- Hot Desking registration wizard: Automatic assignment of a temporary phone
- Context-aware routing: Ability for desk phone to forward altered settings automatically, depending on the user's IBM Sametime presence state
- Corporate directory phone integration: Click-to-call and Presence services through integration with a corporate directory
- Speech Dial integration (if supported in the network): Quick call icon that allows callers to simply speak the name of the person or department to be connected

Hot Desking web interface

ACE Hot Desking Application - Microsoft Internet Explorer

File Edit View Favorites Tools Help

AVAYA
INTELLIGENT COMMUNICATIONS

ACE Hot Desking Application

Jane SMITH

Communication

Phone Call Video Call

My Devices No Outgoing Calls My Settings

Status	Type	Device	Address	
Primary Device	Phone	Office Desk Phone	64442126	Unknown
Make Primary	Phone	MCS	63004442126	
Make Primary	Phone	Hotdesk		

Hotdesk Registration

Hotdesk Setup Hotdesk Release Hotdesk Settings

If you are away from your desk, you can use this feature to register a temporary/hotdesk phone. This phone will then become your primary phone for both presence and calls until you cancel it.

Set Up Your Hotdesk

At the end of the process, your desk phone will be call forwarded to the hotdesk.

v2.2.0.12323 - Logged in as ACE UserID LISASTEP Administration Console © 2010 Avaya Inc. All rights reserved.

Hot Desking and Sametime integration solution overview

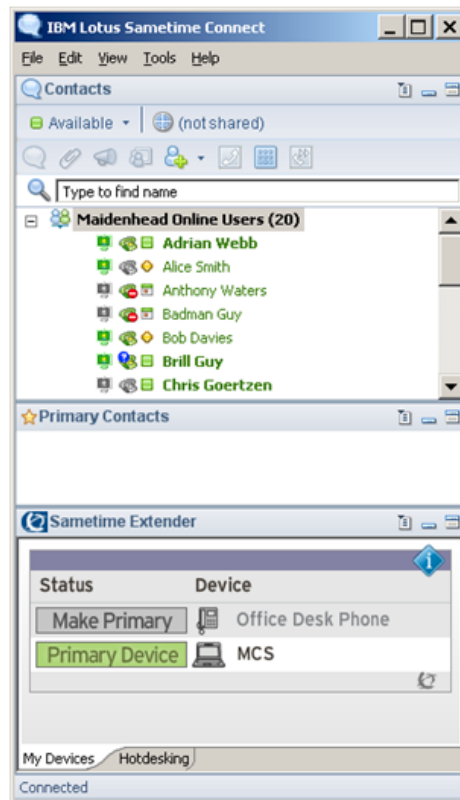
Description

The Hot Desking and Call Forwarding plug-ins for Sametime extend device management capabilities to Sametime Connect client users. Once the plug-ins are installed and made available by the administrator, a Sametime Extender panel appears automatically when users launch their Sametime Connect client. From this panel, users can:

- View devices associated with the user's personal Hot Desking Application account. Note that the user devices are provisioned by an administrator. The list of devices cannot be modified from the Hot Desking interface. Users can, however, select a different primary device.
- Register a phone as the user's Hot Desk phone. This is useful when a roaming-enabled phone profile is not available.
- Automatically reroute calls to alternative devices by setting Context Aware Routing when the user's presence is set to something other than available.

Sametime Extender interface

The figure shows how key Hot Desking and Call Forwarding capabilities integrate with IBM Sametime.



Mobility application solution overview

Mobility

The Mobility application is delivered through the Application Integration Engine™ (AIE) and provides the following features from a supported mobile device.

- **Cost optimizer:**
 - Reduces corporate long distance and international mobile phone costs significantly by integrating supported smartphones with a company's communications environment.
 - Leverages the mobile network data channel to instruct a company's private branch exchange (PBX) or non-PBX to set-up the call. MCO.
 - In effect, turns an outbound call from the mobile into an inbound call from the PBX, and instructs the PBX to route the called party leg of the call over the enterprise voice.
- **Conference call dialing:**
 - Allows users to join or chair a conference call from an appointment in calendar without having to switch between the calendar and phone applications on the mobile device.
- **Hot Desking:**
 - Provides selected Hot Desking functionality that enables users to manage the various communication devices associated with their user account through their mobile device.

Administration of Mobility application is through the AIE GUI.

Key capabilities

Key capabilities are:

- Provides access to private (corporate) dial plans.
- Re-uses existing corporate voice infrastructure.
- Provides user authentication beyond based Personal Identification Number (PIN) number.
- Does not require local or toll-free access numbers in every region.
- Eliminates pre-authorization with Mobile Operator for outgoing calls when roaming.
- Provides a simplified web-based interface for configuration and administration

- Includes web-based online help.



Event Response Manager solution overview

Event Response Manager

The Event Response Manager (ERM) is a web-based application that is hosted on the Application Integration Engine™ (AIE) server and supports automatic and manual team conferencing triggered by events.


The ERM:


- Determines the right team members (call participants) to respond to a defined event.
- Plays a text-to-speech or pre-recorded audio message to notify team members of a specific event.
- Joins all team members into a conference call without delay, enabling them to communicate and respond to the event in a timely and effective manner.
- Provides audible updates, announcing them directly into a conference in progress. (A beep tone alerts conference participants to an imminent update.)


The ERM synchronizes with Avaya ACE to ensure that all users (potential call participants) are available to the application for automatic or manual event conferencing and that the ERM uses to the appropriate contact preferences.


Event Response Manager GUI


Event Response Manager

 Overview

 Contacts

 Teams

 Audio Files





 Events

Respond to emerging events. Faster and more effectively.

With the Event Response Manager from Nortel, you can:

- ✓ Determine the right team members to respond to an event, by name or dynamically by role, skill, and location
- ✓ Notify team members that an event has occurred, using either pre-recorded audio messages or text-to-speech
- ✓ Invite team members to join a conference call, enabling quick communication and response to events
- ✓ View event history, including which team members joined the conference call

How it works:

-  First, tell the system a bit about your contacts: who they are, their roles, skills, and locations
-  Then, set up event response teams: the people who will be called when events happen
-  Upload your own pre-recorded messages, or use text-to-speech for detailed notifications
-  Last, define and trigger events. Event Response Manager will notify the team and start a conference call

Module summary

Objectives

In this module you learned how to:

- Identify the applications, add-ins, extenders and communications-enabled applications and business processes (CEBP) that Avaya ACE supports.
- Describe the Personal Assistant solution, including its purpose and key features.
- Describe the Unified Communications add-ins solution, including its purpose and key features.
- Describe the Message Drop and Blast solution, including its purpose and key features.
- Identify the Communications-Enabled Applications and Business Processes (CEBP) that Avaya ACE supports, and describe their purpose and key capabilities. Describe ACE Communications-Enabled Applications and Business Processes (CEBP) solutions, including its purpose and key features.
- Describe the AIE.
- Describe key features and capabilities of the AIE.
- Describe the Hot Desking solution, including its purpose and key features.
- Describe the Hot Desking and IBM Sametime integration solution, including its purpose and key features.
- Describe the Mobility application solution, including its purpose and key features.
- Describe the Event Response Manager solution, including its purpose and key features.

IBM Lotus Sametime integration

Introduction

Purpose

This module provides an overview of the integration of the Agile Communication Environment™ (Avaya ACE™) and IBM Sametime integration fundamentals, including prerequisite programming, integration procedures, and supported services.

Topics

After completing this module, you will be able to:

- Identify key solution components of IBM Lotus Sametime.
- Identify supported network elements and telephony features for an Avaya ACE and IBM Lotus Sametime solution.
- Identify integration guidelines for an Avaya ACE and IBM Lotus Sametime solution.
- Identify and describe the purpose and functionality of Avaya ACE telephony services for IBM Lotus Sametime.
- Identify the types of user profiles configured to support an IBM Lotus Sametime solution, and configure user profiles with the Avaya ACE GUI.
- Identify and describe the purpose and functionality of Avaya ACE plug-ins, as well as how to install and update plug-ins to support an IBM Lotus Sametime solution.
- Describe the Hot Desking and IBM Sametime integration solution, including its purpose and key features.

Resources

Avaya ACE documentation:

- *Release Notes* (NN10850-019)
- *Planning and installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)

IBM Lotus Sametime fundamentals

Description

IBM Lotus Sametime is a popular communications software solution that combines presence awareness, instant messaging, and web conferencing into a single integrated business application. Sametime also supports advanced features, such as security and integrated Voice over IP (VoIP).

Key solution components include:

- IBM Sametime server
- Domino server
- Sametime Connect client

IBM Sametime server and Domino server

IBM Sametime server and Domino server software are installed on a supported server hardware platform. The term **Sametime server** is a generic term that refers to the server that hosts the IBM Sametime server and Domino server software.

The Sametime server can be installed in standalone or multiple server environments. Sametime also supports a Community Clustering environment, where dedicated servers are grouped together to provide fail-over and load balancing capabilities. For more information about supported hardware and configurations, see the IBM website.

Sametime Connect client

The Sametime Connect client refers to IBM software, which is downloaded from an authorized Sametime site and installed on a user desktop PC. Once installed and configured, the Sametime Connect Client provides the user interface for Sametime services via a supported Java-based browser.

Supported network elements and telephony features

Supported network elements and telephony features

Network element	Support Sametime 7.5.1 features	Support Sametime 8.0.2 features
Communication Server 1000 (CS 1000)	<ul style="list-style-type: none"> - Quick Call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward 	<ul style="list-style-type: none"> - IBM click-to-call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward
Communication Server 2100 (CS 2100)	Not applicable	<ul style="list-style-type: none"> - IBM click-to-call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward
Multimedia Communications (NMC)	Not applicable	<ul style="list-style-type: none"> - Click-to-conference - Hot Desking - Hot Desking - Call Forward
Cisco Unified Communications Manager (Cisco Unified CM)	<ul style="list-style-type: none"> - Quick Call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward 	<ul style="list-style-type: none"> - IBM click-to-call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward
Multimedia Communications Server 5100 (MCS 5100) or Application Server 5200 (AS 5200)	<ul style="list-style-type: none"> - Quick Call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward 	<ul style="list-style-type: none"> - IBM click-to-call - Dialpad - Presence - Hot Desking - Hot Desking - Call Forward
Tandberg Video Communication Server (VCS)	<ul style="list-style-type: none"> - Quick Video - Call Presence - Hot Desking - Hot Desking - Call Forward 	Not applicable



Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

IBM Lotus Sametime integration guidelines

Supported IBM Lotus Sametime versions

Avaya ACE supports integration with the IBM Lotus Sametime 7.5.1 or 8.0.2 as follows.

- IBM Lotus Sametime 7.5.1:
 - Sametime server 7.5.1 CF1 on a Windows Server 2003
 - Domino server 7.0.2
 - Sametime Connect Client 7.5.1
- IBM Lotus Sametime 8.0.2:
 - Sametime server 8.0.2 CF1 on a Windows Server 2003
 - Domino server 7.0.2
 - Sametime Connect Client 8.0.2

Task summary

Sametime server

Complete the following tasks on the Sametime server.

- Add the Avaya ACE host (static IP address) as a trusted node on the Sametime server.
 - A Sametime server only accepts connections from an Avaya ACE server that is configured as a trusted node on the Sametime server.
 - Note that if necessary, you can remove the Avaya ACE server as a trusted node on the Sametime server.
- Install the telephony provider module on the Sametime server.
- Configure telephony services on the Sametime server.
 - Sametime 7.5.1: Disable IBM native click-to-call feature on Sametime server 7.5.1.
 - Sametime 8.0.2: Enable Sametime Connect client users to use Avaya ACE-hosted features through the Sametime server.
- Configure update site for plug-ins.

Sametime Connect client

Complete the following tasks for each user.

- Install the Sametime Connect client and all appropriate patches or hot fixes. See the Release Notes for more information.
- Install the appropriate plug-ins, either manually or automatically from previously defined update site.
- Define user preferences, as appropriate.

Avaya ACE server

Complete the following tasks on the Avaya ACE server.

- Configure a user profile for the Sametime application.
 - Create user (user ID and password).
 - Assign the user to a user group that is configured with the appropriate privileges necessary to invoke web services.
- Create a user profile for each Sametime Connect client user.
 - Create user if one does not already exist (user ID and password).
 - Define registered network devices; for example: desktop phone, clients, chat.
- Verify that the Sametime service provider is configured.



Tip

The Software Downloads window, accessed from the Avaya ACE GUI Help menu, provides you with a convenient location on the ACE GUI to download software needed for integration with Avaya ACE.

Troubleshooting

Refer to the IBM Lotus Sametime integration documentation for common troubleshooting scenarios; for example:

- Presence status is inaccurate or not displayed.
- Selected error messages generate on the Sametime Connect client.
- Call and Presence services are currently under fault condition.
- IBM click-to-conference fails.
- Plug-ins do not automatically download.

Telephony services for IBM Lotus Sametime

Overview

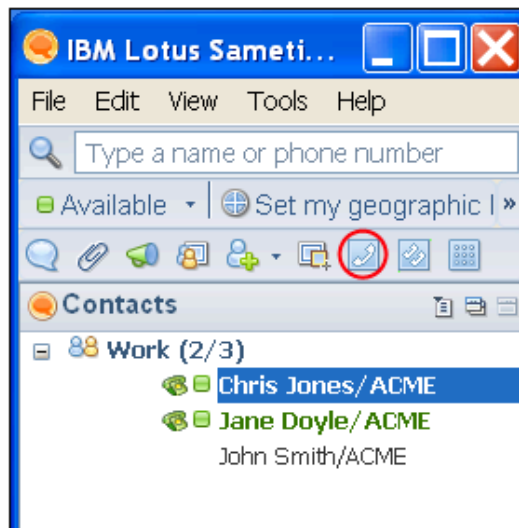
Supported telephony services are an IBM Sametime integration are:

- Quick call (Sametime 7.5.1 client)
- IBM Click-to-call (Sametime 8.0.2 client)
- Quick Video Call
- Dialpad
- IBM Click-to-conference
- Prioritized call routing
- Telephony and video client presence

Following is a brief description of the supported telephony services.

Quick Call (Sametime 7.5.1)

With the Quick Call plug-in installed on the Sametime Connect 7.5.1 client, Avaya ACE-enabled Sametime users can initiate voice calls to other Avaya ACE-enabled or non-enabled Sametime Connect 7.5.1 users. Quick Call is supported on Sametime 7.5.1 only.

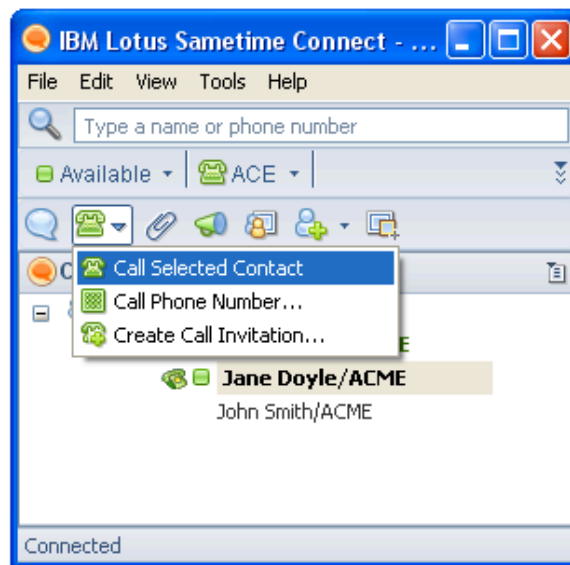


Click-to-call (Sametime 8.0.2)

With the Auto-provisioning plug-in installed on the Sametime Connect 8.0.2 client, Avaya ACE-enabled Sametime users can initiate voice calls to other Avaya ACE-enabled or non-enabled Sametime users from the native IBM interface.

Sametime users can initiate quick calls from the main Sametime Connect window or a chat window by:

- Clicking on the Quick Call icon in the toolbar
- Selecting the Quick Call option from the Tools pull-down menu
- Right-clicking on a contact and selecting Quick Call from the drop-down menu

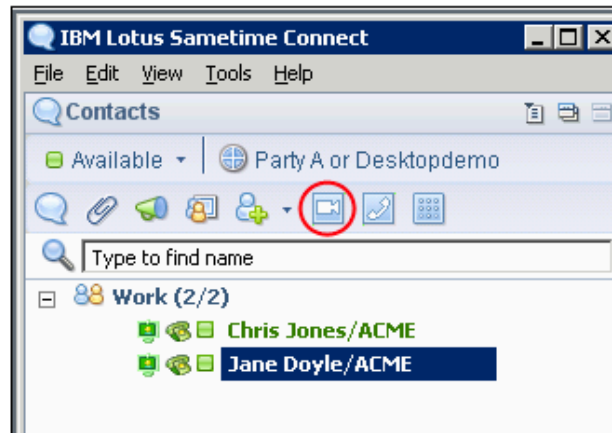


Quick Video Call (Sametime 7.5.1)

With the Quick Video Call plug-in installed on the Sametime Connect client, Sametime 7.5.1 users with a video client configured in their ACE user profile can initiate video calls to other Sametime users who have a video client configured in their Avaya ACE user profiles.

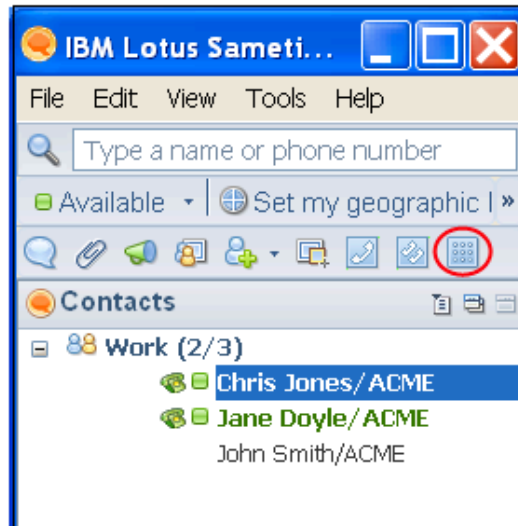
Sametime users can initiate video calls from the main Sametime Connect window or a chat window by:

- Clicking on the Quick Video Call icon in the toolbar
- Selecting the Quick Video Call option from the Tools pull-down menu
- Right-clicking on a contact and selecting Quick Video Call from the drop-down menu (main window only)



Dialpad (Sametime 7.5.1)

The Dialpad plug-in for the Sametime 7.5.1 client allows the user to launch a Dialpad and enter a phone number manually.

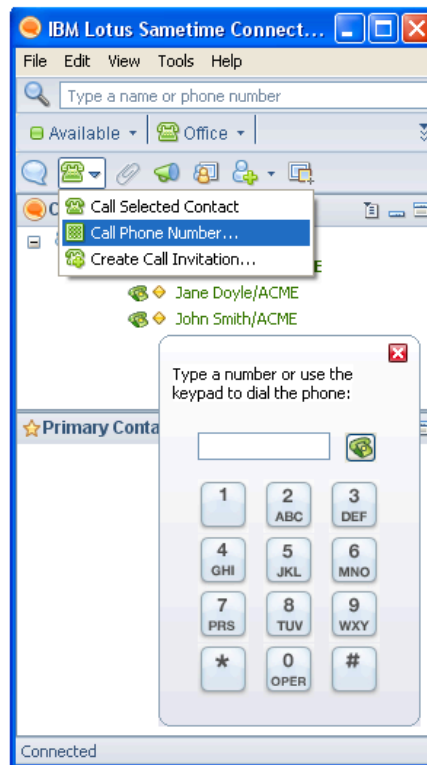


Dialpad (Sametime 8.0.2)

Users launch the IBM Dialpad from the native IBM interface.

In the text field of the IBM Dialpad, you can enter any valid URI prefixed with **tel:**, **sip:** or **sips:**. However, for URIs prefixed with **tel:**, the Dialpad truncates tel: before displaying on the title bar. For example, the URI **tel:user1234@domain.com** appears as **user1234@domain.com**.

Alert: It is recommended that non ACE-enabled users have their business card number configured in their Sametime user accounts in order to be reachable using the IBM click-to-call, when off-line.



IBM Click-to-conference

The IBM Click-to-Conference feature allows Avaya ACE-enabled Sametime Connect client users can initiate and manage conference calls with other Sametime users (online or offline) on their contacts list. The maximum number of participants in a conference call is 100.

IBM Click-to-conference is supported through the Multimedia Conferencing (NMC) network element.



Prioritized call routing

Avaya ACE-enabled Sametime users have a user profile configured on Avaya ACE. This user profile contains contact information about user's accounts on different communication devices. Each device configured as a contact in the Avaya ACE user profile has an assigned priority, indicating a relative preference.

When a Sametime user initiates click-to-call from the Sametime Connect interface, the Sametime server uses a special URI format (ace:[USER]) for the calling party in the call setup request that triggers a look-up in the Avaya ACE user profile database for the specified user. Avaya ACE uses the priority value associated with any contact address of type Telephone to determine the preferred (highest priority) telephone contact number and routes the call accordingly.

Prioritized call routing (Sametime 8.0.2)

To support prioritized call routing on the Sametime 8.0.2 client side Avaya ACE provides a Sametime Connect client plug-in that automatically provisions the specialized Avaya ACE URI in the client's telephony preferences. With the Auto-provisioning plug-in installed on the Sametime Connect client, Avaya ACE automatically populates the Preferred numbers field with the Sametime user's ACE URI (ACE user name). As a result, the user's Avaya ACE URI is available in the Preferred Device for Making and Receiving Calls field located in the client's tool bar, along with the Computer option for making computer-to-computer calls if Allow client-to-client video call is enabled in the Sametime telephony provider module.

Alert: If there is a primary phone number configured in the Preferences - Geographic Location page, or in the Sametime user's business card, those numbers are ignored by the call setup process. The Sametime server uses the ace: URI for the calling party in the call setup request.

Telephony presence

The Sametime telephony provider module provides telephony presence service to Sametime Connect clients through the Sametime server. With the Aggregated Presence plug-in installed on the Sametime Connect client, Sametime users can view aggregated presence information for their contacts who are registered with different network devices.

Video presence

Sametime users can also see which of their contacts have a video client configured in their Avaya ACE user profile. The video presence status depends on which version of Tandberg VCS is used. Tandberg VCS X4 supports real-time presence updates.

Alert: When deploying the Telephony and video client presence features, read the attentions and alerts in *Agile Communication Environment Administration - IBM Lotus Sametime IntegrationTM* (NN10850-011), which describe differences in feature operation for various service providers.

User profiles for IBM Sametime integration

Sametime Server user profile

You must configure a user profile for the Sametime Server. Because only Avaya ACE users with administrator privileges can query other user profile accounts, the Sametime server must be assigned to a user group with administrator privileges and access privileges to the appropriate services. For successful web service enablement, the same user credentials must be set in the Sametime telephony provider module on the Sametime server.

Ensure the user name and user group name for the Sametime server are meaningful and unique.

Sametime Server user profile (screen excerpt)

The screenshot displays the configuration interface for a Sametime Server user profile, organized into three main sections:

- User Group:** This section contains the following details:
 - Name: `sametime_user_group`
 - Parent User Group: [SystemAdminGroup](#)
 - User Group Type: `System Administrator`
 - Last Modified User ID: `admin`
 - Creation Date: `2009-10-09 17:14:24.270 -0400`
 - Last Modified Date: `2009-10-09 17:14:24.270 -0400`
- Membership Information:** This section shows the process of adding users to the group:
 - Available Users (User ID):** A list box containing `admin`, `asa`, `federation`, `ocs`, and `sysmonitor`. Navigation arrows (up, down, left, right) are present.
 - User Group Members:** A list box currently containing `sametime`.
 - Buttons: `>>` (to add) and `<<` (to remove).
 - Links: [View User](#) (below the available users list) and [View User](#) (below the members list).
- User Group Policy:** This section defines access control rules for various services:

Service Name	Access Level	Commands
AudioCallService	Off	
CallForwardingService	Off	
CallHistoryService	Off	
CallNotificationService	Write	startCallNotification (WRITE) stopCallNotification (WRITE)
LocationSupplierService	Off	
MultimediaConferenceService	Write	getParticipants (READ) createConference (WRITE) disconnectParticipant (WRITE) inviteParticipant (WRITE) endConference (WRITE)

Sametime Connect client users

Configure an Avaya ACE user profile for each Sametime Connect client user. In addition to user name and password, define contact information for the user's registered network devices. This allows Avaya ACE to query each device for the user's presence status and aggregates the results before making the presence status available to the Sametime server. This also to determine the preferred contact number for a Sametime user who is initiating a call from the Sametime client.

User contact information

The figure shows contact information for a user with multiple devices.

Contact Information

Contact TypeChat

Contact Name

Contact Identifier







Priority

PIN

Confirm PIN

Save Contact Information

Cancel

Delete	Contact Type	Contact Name	Contact Identifier	PIN	Priority	Edit
	Telephone	cs1000	tel:1701		0.09	
	Telephone	mcs	sip:user1@ace.com		0.08	
	Chat	sametime	st:CN=user1/O=nortel		0.07	

IBM Sametime click-to-conference users

If using the Avaya ACE-enabled IBM Sametime click-to-conference, configure these types in the user profile:

- Chat: Defines the ID (contact identifier) for user on Sametime server.
- Telephone: Defines the user's telephony Uniform Resource Identifier (URI); for example, SIP or tel format.
- Conference: Defines Multimedia Conferencing (NMC) subscriber's access code, subscriber's chairperson PIN, and contact name.

Contact information for IBM click-to-conference

Delete	Contact Type	Contact Name	Contact Identifier	PIN	Priority	Edit
	Telephone	cs1000	tel:1701		0.09	
	Chat	sametime	st:CN=userx/O=nortel		0.07	
	Conference	nmc	1701	*****	0.05	

International characters for chat

For Sametime desktop integration, Avaya ACE supports the use of international characters for Chat contact type provisioning. International characters support is limited to configuring or querying an ACE user's contact identifier when the contact type is set to chat. Other GUI fields do not support international characters.

Ensure that your computer environment - such as the Web browser you use to login to the Avaya ACE GUI for user profile provisioning - is configured for UTF-8 variable length encoding, if required. For general information about UTF-8, go to Unicode Consortium website. For more information about ACE character support, see *Avaya Agile Communication Environment - AdministrationTM* (NN10850-005).

Plug-in installation, configuration, and update

Description

Avaya ACE plug-ins are distributed via an update site on the Sametime server. The update site can only be used for Avaya ACE plug-ins.

Once the update site is set up, Sametime administrators can allow users to manually poll for updates through the Plug-in Manager on the Sametime Connect client or configure an automatic push of updated plug-ins to Sametime users. To allow users to poll for updates through the Plug-in Manager, make sure that users have access to the URL where the update site is located.



Tip

It is not recommended to use the Avaya ACE embedded web server as the update site for Avaya ACE plug-ins as this might impact operating performance.

Hot Desking and Sametime integration solution overview

Description

The Hot Desking and Call Forwarding plug-ins for Sametime extend device management capabilities to Sametime Connect client users. Once the plug-ins are installed and made available by the administrator, a Sametime Extender panel appears automatically when users launch their Sametime Connect client. From this panel, users can:

- View devices associated with the user's personal Hot Desking Application account. Note that the user devices are provisioned by an administrator. The list of devices cannot be modified from the Hot Desking interface. Users can, however, select a different primary device.
- Register a phone as the user's Hot Desk phone. This is useful when a roaming-enabled phone profile is not available.
- Automatically reroute calls to alternative devices by setting Context Aware Routing when the user's presence is set to something other than available.

Sametime Extender interface

The figure shows how key Hot Desking and Call Forwarding capabilities integrate with IBM Sametime.



Checkpoint



Sametime overrides any option that a user enters in the Sametime Connect client.
The Avaya ACE URI is always used.

- _____ True
_____ False

Answer : True



Configure the Sametime service provider on the Avaya ACE host to enable
communication between the Avaya ACE host and the Sametime server.

- _____ True
_____ False

Answer : True



Avaya ACE plug-ins are configured on the Sametime Connect client.

- _____ True
_____ False

Answer : True



The Avaya ACE telephony provider module is installed on the Sametime Connect client.

_____ True

_____ False

Answer : False

Module summary

Objectives

In this module you learned how to:

- Identify key solution components of IBM Lotus Sametime.
- Identify supported network elements and telephony features for an Avaya ACE and IBM Lotus Sametime solution.
- Identify integration guidelines for an Avaya ACE and IBM Lotus Sametime solution.
- Identify and describe the purpose and functionality of Avaya ACE telephony services for IBM Lotus Sametime.
- Identify the types of user profiles configured to support an IBM Lotus Sametime solution, and configure user profiles with the Avaya ACE GUI.
- Identify and describe the purpose and functionality of Avaya ACE plug-ins, as well as how to install and update plug-ins to support an IBM Lotus Sametime solution.
- Describe the Hot Desking and IBM Sametime integration solution, including its purpose and key features.

Microsoft Office Communications Server integration

Introduction

Purpose

Avaya Agile Communication Environment™ (Avaya ACE™) supports Unified Communication (UC) desktop integration with Microsoft OCS 2007. By leveraging web services and user profile management, administrators can communications-enable existing Microsoft OCS services.

This module provides an overview of Microsoft OCS integration.

Objectives

After completing this module, you will be able to:

- Identify key characteristics of Microsoft OCS.
- Identify how the Avaya ACE and Microsoft OCS interact.
- Identify integration guidelines for a Microsoft OCS and Avaya ACE solution.
- Identify and describe the purpose and functionality of Avaya ACE telephony Services for Microsoft OCS.
- Ensure that the required Avaya ACE user profiles are configured to support a Microsoft OCS integration solution.
- Identify the Avaya ACE applications that integrate with Microsoft OCS.

Resources

Avaya ACE documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Administration - Microsoft Office Communications Server Integration* (NN10850-012)

Microsoft OCS fundamentals

Overview

Microsoft Office Communications Server (OCS) 2007 is a popular unified communications solution that provides real-time functionality, such as instant messaging, presence, and conferencing for Microsoft OCS users. Key solution components include:

- **Microsoft OCS server:** Microsoft Office Communications Server (OCS) 2007 software is installed on a supported server host. The host runs a supported operating system. Standalone and multiple server configurations are supported.
- **Microsoft Office Communicator client:** Microsoft Office Communicator 2007 software is installed on each client (user) PC. The Office Communicator client provides a unified interface for communications services, such as instant messaging, presence, and conferencing.

Supported configurations

Standalone and multiple server configurations are supported.

- **Standalone configuration:** Microsoft Standard Edition software and all server components are installed on a single server.
- **Multiple server configuration:** Multiple Enterprise Edition servers are deployed as a pool behind a load balancer and share a centralized SQL Server database.



Tip

The software installed on the host depends upon the number of servers deployed, desired functionality, customer infrastructure requirements, and other parameters. For more information, including infrastructure and operations requirements, see the Microsoft website.

Avaya ACE and Microsoft OCS interworking

Description

The Avaya ACE Service Agent (ASA) acts as a protocol converter between ACE and the Microsoft OCS server. The ASA provides light-weight integration and adaptation services between Microsoft OCS and Avaya ACE, for example: Remote Call Control (RCC), Extended Presence Bootstrapping, and Proxy Services.

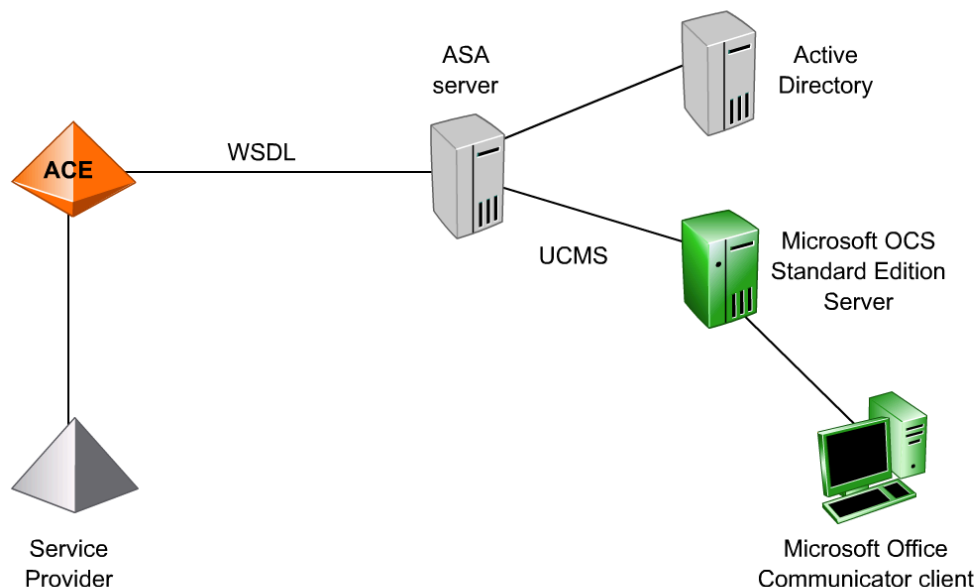
To Microsoft OCS, ASA appears as a Unified Communications Management API (UCMA) application server. To Avaya ACE, the ASA appears as a Parlay X web services application. ASA adapts (interprets) UCMA messages into Parlay X web services, and vice-versa.

The service provider configured depends upon the existing customer network infrastructure and the type of service deployed.

Note: Avaya ACE does not alter the functional operation of Microsoft Office Communicator. No Avaya ACE-specific configuration of Microsoft Office Communicator is required.

Example Microsoft OCS deployment

The figure shows an example Microsoft OCS integration. The network includes a Microsoft Standard Edition server (which hosts the Certificate Authority), the Active Directory, and a stand-alone ASA server.





Tip

Avaya ACE does not require a mediation server. A mediation server is only required when the Microsoft OCS server needs to communicate through a gateway to other network elements.

Supported network elements and telephony features

Network element	Feature
Communication Server 1000 (CS 1000) service provider	Remote Call Control (RCC) capabilities: <ul style="list-style-type: none">- Make call- Release call- Answer call- Call deflect- Caller ID- Forward to another telephone number- Call hold and retrieve Extended presence
Communication Server 2000 (CS 2000)	Remote Call Control (RCC) capabilities: <ul style="list-style-type: none">- Make Call- Release Call- Conversation history Extended Presence
Contact Center/MLS	Remote Call Control (RCC) capabilities: <ul style="list-style-type: none">- Make call- Answer call- Release call- Caller ID- Forward to another telephone number- Single-step transfer- Consultative call- Consultative transfer- Call Hold and Retrieve- Call Deflect (Redirect) Extended presence
Cisco Unified Communications Manager (Cisco Unified CM)	Remote Call Control (RCC) capabilities: <ul style="list-style-type: none">- Make Call- Release Call Extended presence
Avaya Aura TM	Remote Call Control (RCC) capabilities: <ul style="list-style-type: none">- Make call- Release call Extended presence



Tip

The type of service provider that you configure varies, depending upon which services you plan to deploy. For more information about supported network elements and services, see Tables of supported Avaya ACE services and applications in *Avaya Agile Communication Environment Administration* (NN10850-005).

Microsoft OCS integration guidelines

ASA deployment requirements

The recommended deployment of the ASA is on a standalone Windows 2003 or 2008 64 bit server. The minimum hardware requirements are 2 x 2.5 Ghz processor and 2 GB memory. The ASA can interact with Microsoft OCS Office Communications Server 2007 (32 or 64 bit) or Office Communication Server 2007 R2 (64 bit).

Microsoft OCS can be deployed in a Standard Edition configuration or an Enterprise Edition server pool configuration. When deploying an Enterprise Edition server pool, a loadbalancer is configured.

Other ASA deployment requirements are:

- The ASA server must be part of the Microsoft OCS domain.
- The ASA application must be able to use web server certificate issued by the domain certificate authority (CA).
- The ASA application must be enabled as a trusted application with Microsoft OCS.

Task summary

ASA installation and setup

- Configure the Avaya ACE server as authorized host on the Microsoft OCS server.
- On the Microsoft OCS Front End server, add the user to the OCS RTC groups.
- On the ASA host, install the ASA prerequisite software and the ASA software.
- If the ASA is installed on a Windows 2008 server and the CA is on a Windows 2003 server, install the appropriate Microsoft patch.
- Perform certificate management for secure communications.
- On the ASA host, configure a web server certificate friendly name. This name must match the one defined during the ASA software installation.
- On the Microsoft OCS Front End server, configure the active directory users.
- On the ASA host, start the ASA.

Avaya ACE GUI

- Add an ASA user profile.
- Configure a user profile for each Microsoft OCS user.
- Ensure a supported service provider is configured.
- Add the appropriate translation and transformation rules



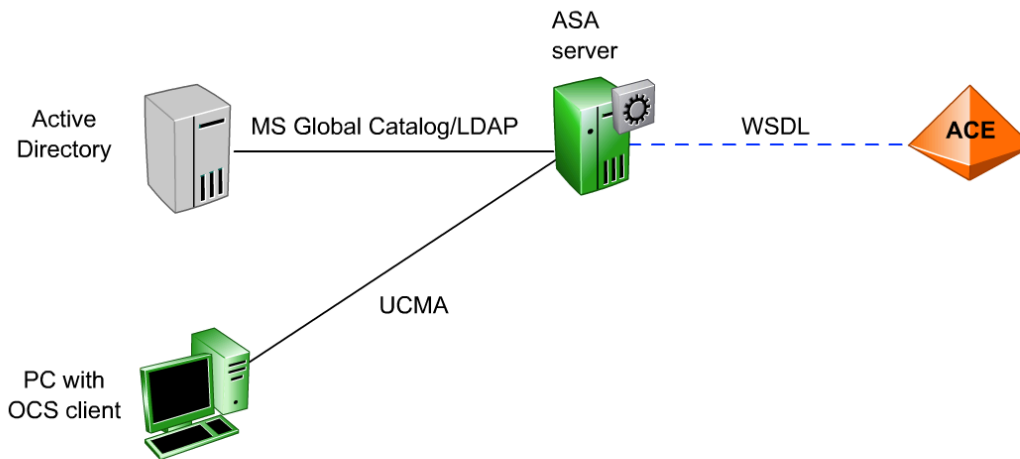
Tip

The Software Downloads window, accessed from the Avaya ACE GUI Help menu, provides you with a convenient location on the ACE GUI to download software needed for integration with Avaya ACE.

ASA integration with Active Directory

The Microsoft Active Directory Global Catalog serves as the central information store of Active Directory objects. At startup, Active Directory is queried for Microsoft OCS users. Each Microsoft OCS user is then queried against Avaya ACE. Users verified to exist in the Active Directory and Avaya ACE become ASA users (Microsoft OCS user + Avaya ACE user = ASA user). ASA then initiates services on behalf of its users.

Existing ASA users are re-validated at each login (maximum login session is 8 hours). To remain synchronized with the Active Directory for new users, ASA queries Active Directory every 60 minutes (configurable). If a new user is detected within Active Directory, an Avaya ACE profile query is invoked. If the Avaya ACE profile query is successful, ASA begins providing services for that user.



Microsoft OCS telephony services

Overview

Microsoft OCS integrates with Avaya ACE and supported service providers to deliver selected Remote Call Control (RCC) and Presence operations. Following is a brief description of supported telephony services.

Remote Call Control (RCC)

RCC capabilities are seamlessly integrated into the Microsoft Office Communicator by virtue of the ASA and Avaya ACE. The ASA and Avaya ACE act as the Computer Supported Telecommunications Applications (CSTA) gateway on behalf of the Microsoft OCS Front End server.

Note that Avaya ACE sends control messages in the form of a pop-up on the Microsoft Office Communicator interface. Computer-to-computer calls are not actually initiated.

Supported RCC capabilities are listed below.

- **Make Call:** User can make a call from phone by clicking on a contact in the Contact list or entering a number on Office Communicator client.
- **Release Call:** User can Release a phone call by clicking on the Phone X icon in the Office Communicator client.
- **Answer Call:** User can accept an incoming call that is presented to them via a pop-up window. **Call Deflect (Redirect):** On a incoming call user can divert this call to another device.
- **Caller ID:** User receives Calling Party Name in pop-up window.
- **Forward to another telephone number:** Through Office Communicator client, user can activate Call Forward on telephony system for incoming calls.
- **Single-step Transfer:** User can forward an existing call unannounced to another phone number.
- **Consultative Transfer:** User can place an existing call on hold, establish another call, and later connect the former call with the later.
- **Consultative Call:** User can place an existing call on hold and initiate another call.
- **Call Waiting:** While in call, user sees a pop-up window indicating a second call when a second call is received.
- **Call Hold and Retrieve:** User can place call on hold and retrieve it.
- **Conversation History:** While Office Communicator client is logged in, user can see incoming and outgoing calls in the Outlook Conversation History folder.
- **Missed Call:** While Office Communicator client is logged in, user receives Missed Call Notifications in Outlook.

Extended presence

Extended presence enhances telephony presence by allowing a watcher to see the telephony presence of a contact even when that contact is logged out of their Microsoft Office Communicator. If a user is logged off of the Microsoft Office Communicator and another device listed in the Avaya ACE user profile goes off-hook, Avaya ACE sends the presence status change through the ASA to the Microsoft OCS server. The Microsoft OCS server then broadcasts the presence change to all interested clients.

If your deployment is providing extended presence, you can enable custom offline presence display during installation. When this feature is enabled, if a user is logged off of the Office Communicator, contacts watching this user see the offline presence status for the user, but also see an additional message. For example, if your OCS network environment includes a short message service (SMS), you could configure the presence status to display IM available, indicating that the user can still receive an instant message (IM) on a mobile device.

User profiles for Microsoft OCS integration

Description

A Microsoft OCS integration solution requires two types of user profiles.

- **User profile for ASA:** Because only users with administrator privileges can query other user profile accounts, the ASA user must be assigned administrator privileges.
- **User profile for each Microsoft OCS user:** In addition to user name and password, define contact information for each network device (telephone, Microsoft Office Communicator, etc.) to which the Microsoft OCS user subscribes and device priority (if the user has multiple devices).

For integration in a network with multiple provider types, it is recommended to use the same Uniform Resource Identifier (URI) type be used for all telephone devices.

Microsoft OCS application integration

Hot Desking

Hot Desking is a standalone application that allows users to bring their office wherever they go. Through a simple, web-based interface, users can make any phone their primary office phone, whether corporate, personal or mobile. Users can choose between devices defined in the ACE user profiles or assign a temporary number for a device not currently defined in their profile through a special registration process.

Hot Desking software is installed on a Windows 2003 server and is configured to communicate with ACE. Desktop and mobile interfaces are supported. In addition, Hot Desking integrates with IBM Lotus Sametime to provide key functionality from within the user's Sametime Connect client.

Upon initializing the Hot Desking application, the Microsoft OCS user is directed to log out and re-log in to Office Communicator. At this time, Avaya ACE begins providing Remote Call Control services for the user's new hotdesked number.

Example scenarios are:

- The user is hotdesked to another phone with greater Remote Call Control capabilities. This could happen when a user travels from one location to another, or when a worker who is usually remote works on-site. In this case, the user would typically have similar or greater call control capabilities.
- The user is hotdesked to another phone with lesser Remote Call Control capabilities. This could happen when an on-site worker works temporarily at a remote location. In this case, the user would have lesser call control capabilities.

Personal Assistant

The Personal Assistant (PA) is an application that gives ACE users basic user privileges to manage personal preferences and settings, previously defined in ACE; for example, contact device settings and passwords. The PA application is included with ACE and is installed automatically when ACE is initially deployed. It is accessible via a desktop or mobile browser.

The PA application is also accessed from the Microsoft Office Communicator client tab (Communication Server 2000 deployments only). For use with Microsoft OCS, the PA plug-in must first be installed and configured.

Checkpoint



The user profile for the ASA must be assigned system administrator privileges.

_____ True

_____ False

Answer : True



The Microsoft OCS server is configured as a service provider on the Avaya ACE host.

_____ True

_____ False

Answer : False



It is recommended to install the ASA co-resident with Microsoft OCS on a Standard Edition Front End 32-bit server.

_____ True

_____ False

Answer : False

Module summary

Objectives

In this module you learned how to:

- Identify key characteristics of Microsoft OCS.
- Identify how the Avaya ACE and Microsoft OCS interact.
- Identify integration guidelines for a Microsoft OCS and Avaya ACE solution.
- Identify and describe the purpose and functionality of Avaya ACE telephony Services for Microsoft OCS.
- Ensure that the required Avaya ACE user profiles are configured to support a Microsoft OCS integration solution.
- Identify the Avaya ACE applications that integrate with Microsoft OCS.

Hardware

Introduction

Purpose

The Avaya Agile Communication Environment™ (Avaya ACE™) software is hosted on a supported hardware platform.

This module reviews the supported baseline hardware.

Objectives

After completing this module, you will be able to:

- Identify Avaya ACE on Linux platform hardware.
- Identify Avaya ACE on Windows platform hardware.

Resources

Avaya ACE documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)

Avaya ACE on Linux platform hardware

Avaya ACE on Linux hardware

Capacity and performance data is measured on a specific hardware platform. The recommended hardware platform for Avaya ACE on Linux is the IBM BladeCenter HT or IBM System x3550 server.

The IBM 3550 server is typically housed in a rack that requires 4-post mounting. A supported power fence device is required for high availability (HA) configurations.

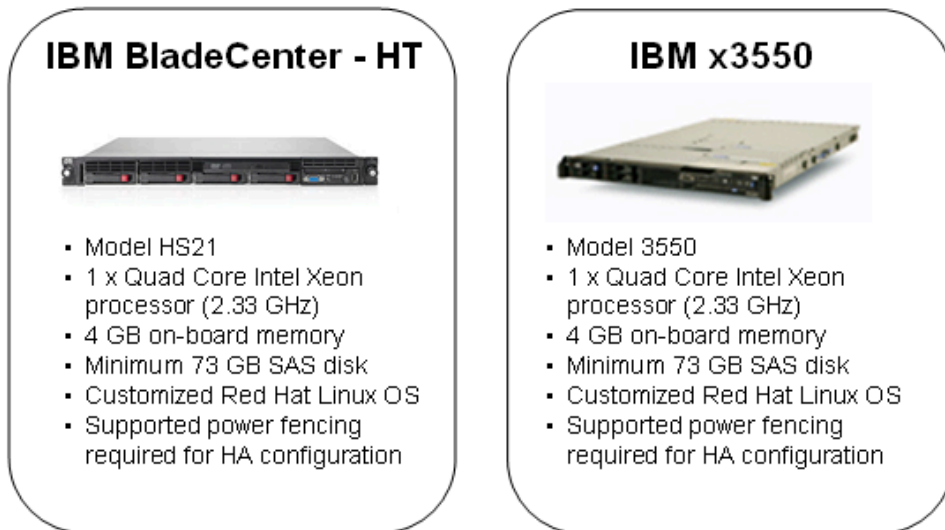


Warning

Running other applications on the Avaya ACE server that compete for system resources such as CPU and memory may result in performance degradation or Avaya ACE failure.

Key hardware specifications

The figure summarizes key hardware specifications.



Power fence devices

Fencing isolates the standby node, preventing it from accessing shared resources such as the database or network call servers. Supported power fence devices are listed below.

- BladeCenter chassis:
 - The supported power fence for the BladeCenter chassis is the BladeCenter management module. This module is integrated into the chassis and is assigned a unique IP address.
- IBM x3550:
 - The recommended (preferred) power fence device is the Remote Supervisor Adapter II (RSA II) Slimline card. The RSA II is an out-of-band management interface card that plugs into a dedicated slot on the system board).
 - The APC power module is supported. The APC power module is an external device used to power cycle nodes that need to be fenced.

Mirrored RAID array

Avaya ACE requires a RAID 1 (mirrored disks) configuration. RAID 1 uses two or more disks, each of which store the same data. This ensures that data is not lost provided one disk survives. The total capacity of the array is just the capacity of a single disk.



Tip

Different arrangements are possible, which have their own trade-offs on protection against data loss, capacity, and speed. RAID levels 0, 1, and 5 are most commonly used.

Avaya ACE on Windows platform hardware



Avaya ACE on Windows hardware

Capacity and performance data is measured on a specific hardware platform. The recommended hardware platform for Avaya ACE on Windows is the IBM System x3550 server (orderable item with Avaya ACE) or the HP Proliant server (not orderable with Avaya ACE).

Note that Avaya ACE requires a RAID 1 (mirrored disks) configuration. RAID 1 uses two or more disks, each of which store the same data. This ensures that data is not lost provided one disk survives. The total capacity of the array is just the capacity of a single disk.

Key hardware specifications

The figure summarizes key hardware specifications. For more information, see *Agile Communication Environment Planning and Installation* (NN10850-004).

HP Proliant	IBM x3550
	
<ul style="list-style-type: none">▪ Model DL360 G6▪ Intel Xeon processor E5540 (2.53 GHz)▪ 4 GB on-board memory▪ Minimum 73 GB disk▪ Microsoft 2003 operating system with service pack 2 or higher▪ DVD drive	<ul style="list-style-type: none">▪ Model 3550▪ 1 x Quad Core Intel Xeon processor (2.33 GHz)▪ 4 GB on-board memory▪ Minimum 73 GB SAS disk▪ Microsoft 2003 operating system with service pack 2 or higher▪ DVD drive



Warning

Running other applications on the Avaya ACE server that compete for system resources such as CPU and memory may result in performance degradation or Avaya ACE failure.

Module summary

Objectives

In this module you learned how to:

- Identify Avaya ACE on Linux platform hardware.
- Identify Avaya ACE on Windows platform hardware.

Software and ordering

Introduction

Purpose

This module provides a high-level overview of the Avaya Agile Communication Environment™ (Avaya ACE™) software ordering, license management, and packaging.

Objectives

After completing this module, you will be able to:

- Identify Avaya ACE platform software.
- Describe the Avaya ACE software ordering and keycode management process.

Resources

Avaya ACE documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)

Avaya ACE platform software

Avaya ACE on Linux software

Avaya ACE software is delivered via DVD. Software upgrades are available for download from the technical support website.

The packaged software is described below.

- Red Hat Enterprise Linux 5.1
- Avaya ACE software
- IBM WebSphere 6.1.0.17

Alert: The Red Hat Enterprise Linux 5.1 image is customized for Avaya ACE. It includes content and configuration that is not included in the generic Red Hat Enterprise Linux 5.1 image commercially available from Red Hat.

Avaya ACE on Windows software

The supported Windows operating system for Avaya ACE is Windows 2003 with service pack 2 or higher. The 64 bit version is not supported. Windows 2008 is not supported.

The Windows operating system is customer supplied (not provided with the Avaya ACE software). For information, go see the Microsoft website.

Avaya ACE on Windows platform software is delivered via DVD. Software upgrades are available for download from the technical support website.

JBoss by open source middleware is installed with the Avaya ACE software on the Avaya ACE Windows host. JBoss provides the environment to run Web-enabled e-business applications. Avaya ACE runs on JBoss Enterprise Application Platform 4.3. For information about JBoss go to www.jboss.com.

Software ordering and keycode management

Description

Software options are defined with a Product Engineering Code (PEC). Once you have created a purchase order that includes the required PECs, you must use the Keycode Retrieval System (KRS) to generate a keycode. The keycode is installed on the Avaya ACE host to enable the options you have purchased.

The base software PECs pertain to the operating system running on the Avaya ACE host: Linux or Windows. You must purchase one instance of the appropriate base software PEC for each Avaya ACE host.

You must purchase one instance of a PEC for each user provisioned to use a service; for example, if you plan to provision 300 users for the Presence service, you must purchase 300 Presence service user PECs. Note that there are three options for the Click to Connect service. You can purchase a PEC for the service or enable the service per user. For a communication enabled web site where the users are anonymous, you can enable the service using a PEC for 100 clicks per month.

You can deploy Avaya ACE in a high availability (HA) configuration with a redundant Avaya ACE host. In this scenario, you must purchase a base software PEC for each Avaya ACE host. Each user PEC or service license PEC is valid on both Avaya ACE hosts. You do not need duplicate user or service PECs for the redundant Avaya ACE host.

For information, including supported PEC types and their corresponding PECs (part numbers), see *Avaya Agile Communication Environment™ Planning and Installation* (NN10850-004).



Module summary

Objectives

In this module you learned how to:

- Identify Avaya ACE platform software.
- Describe the Avaya ACE software ordering and keycode management process.

Customer support

Introduction

Purpose

This module reviews key resources and services available that Avaya offers.

Objectives

After completing this module, you will be able to:

- Identify the documentation and online help that the Avaya ACE offers.
- Identify the Global Services that Avaya offers.

Resources

Avaya ACE documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)

Documentation and online help

Documentation and online help

Documentation and online help is integrated with the Avaya ACE software, providing your first level of support. Standard documentation, updates, and other important resources are available from the technical support web site.

Resources

Avaya ACE core documentation:

- *Release Notes* (NN10850-019)
- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Fault and Performance Management* (NN10850-009)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)
- *Administration - Microsoft Office Communications Server Integration* (NN10850-012)
- *Alarms Reference* (NN10850-015)
- *Audit Log Reference* (NN10850-016)
- *Performance Measurement Reference* (NN10850-017)
- *Error Messages Reference* (NN10850-018)

Resources

Avaya ACE applications documentation:

- *Personal Assistant Application* (NN10850-032)
- *Message Drop and Message Blast Administration* (NN10850-025)
- *Hot Desking User Guide* (NN10850-030)
- *Hot Desking Application Installation Guide* (NN10850-035)
- *Hot Desking Mobile Interface Guide* (NN10850-036)
- *Hot Desking Administration Guide* (NN10850-037)
- *Hot Desking Application Web Portal Integrator Guide* (NN10850-038)
- *Hot Desking Application for Sametime Connect User Guide* (NN10850-046)
- *Avaya Application Integration EngineTM Fundamentals* (NN10850-021)
- *Mobility Application Administration* (NN10850-027)
- *Mobility Application for BlackBerry* (NN10850-028)
- *Event Response Manager Installation* (NN10850-048)



Tip

The Software Downloads window, accessed from the Avaya ACE GUI Help menu, provides you with a convenient location on the ACE GUI to download software needed for integration with Avaya ACE.

Global Services

Service areas

As a unified organization, Avaya can help businesses make the most of the new roadmap, whether they want to protect existing investments and lengthen investment useful life, extend gradually into new capabilities, or prepare for transformative growth by adopting the Avaya vision of plug-and-play communications.

Avaya Global Services delivers world-class support in three areas:

- **Avaya Professional Services:** Avaya Professional Services consultants are technically proficient, possess strong business acumen and have developed vertical industry specialization to help you address the challenges of today's converged voice, video and data communications environments. At the same time, we actively help you look for ways to optimize your communications environment to better enable your people, increase your business agility, and drive costs out of your operations.
- **Global Support Services:** Avaya support services are backed by global resources, including more than 5,800 industry-certified service desk and backbone engineers and 34 regional network operations centers delivering 24x7 monitoring, diagnostics and problem resolution, as well as support in 14 languages.
- **Avaya Operations Services.** Avaya Operations Services are available for customers that want to out-task the proactive management and monitoring of their communications infrastructure. These services can be delivered by Avaya directly or may be private-labeled and co-delivered by Avaya authorized partners.

For more information, talk to your Avaya Account Manager or Authorized partner. Also, visit us at www.avaya.com.

Module summary

Objectives

In this module you learned how to:

- Identify the documentation and online help that the Avaya ACE offers.
- Identify the Global Services that Avaya offers.

Case study

Introduction

Purpose

The Avaya Agile Communication Environment™ (Avaya ACE™) enables Unified Communications (UC) into a multi-vendor, multi-site network. This includes click-to-connect service, exposing user presence data and integrating with the customer's existing corporate directory.

This module illustrates how Big Bank leverages Avaya ACE and IBM Lotus Sametime for UC desktop integration and to provide enhanced communications-enabled applications to a geographically dispersed user base.

Objectives

After completing this module, you will be able to:

- Given an example customer scenario, identify deployment recommendations for an Avaya ACE solution.

Resources

Avaya ACE documentation:

- *Planning and Installation* (NN10850-004)
- *Administration* (NN10850-005)
- *Web Services* (NN10850-007)
- *Administration - IBM Lotus Sametime Integration* (NN10850-011)



Tip

Avaya simplifies the path to communications enablement, with a unique, four-part approach.

- Multi-vendor interoperability through an open, non-proprietary framework that improves business agility, accuracy and speed and maximizes return on investment
- A cross-domain strategy that allows customers to integrate solutions into their existing infrastructures and create new service opportunities
- Real-time orchestration of services to deliver dynamic work flows and user-/event-initiated processes.
- Toolkit/solution approach that provides the flexibility to integrate a standard service set of build custom solutions to meet their own needs

Big Bank case study

Scenario



Big Bank is a large international financial institution, with a geographically distributed, converged network infrastructure. It currently has two sites, with over 5,000 users worldwide and anticipated expansion to 10,000 users within the next five years.

Site A

- 2,500 users
- Located in the United States
- Has Communication Server 1000E High Availability (CS 1000E HA) system located onsite
- Has a combination of terminal devices, including digital and IP phones

Site B

- 2,500 users
- Located in the United States
- Has CS 1000E HA system located onsite
- Has a combination of terminal devices, including digital and IP phones

Both sites utilize an external LDAP-compliant server to maintain corporate information.

Customer need

Big Bank wants a solution that includes:

- Integration with IBM Lotus Sametime
- Subsequent integration with their corporate directory portal

The telecom managers for both sites require the ability to leverage existing telecom equipment.

The information technology (IT) managers for both sites require a security strategy that includes secure communications and the protection of network resources from unauthorized or malicious access to the customer network from external clients.

The IT department wants to use existing web servers.

Configuration

The customer chose a hardware platform that supported the Red Hat Linux operating system customized for Avaya ACE.

To achieve resiliency, a High Availability (HA) configuration was recommended, which included two nodes in a 1+1 active/standby configuration at each site. The customer chose a Linux deployment. The customer will supply the hardware (servers) to host the Avaya ACE solution.



Tip

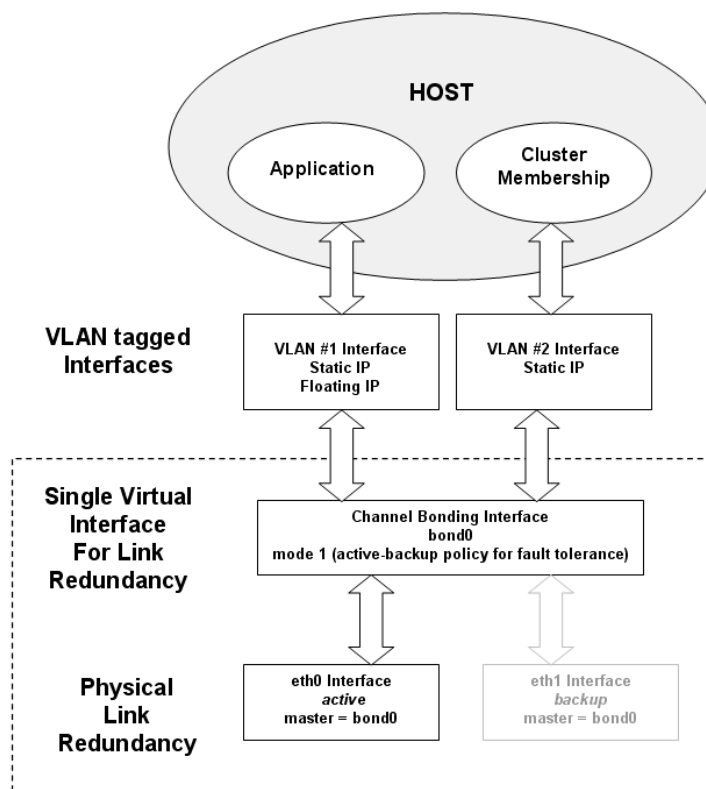
If VLANs are not supported in the customer network, a default network configuration can be established that contains a single floating IP address shared by the nodes in the cluster and a fixed address assigned to each physical node.

It is strongly recommended that HA cluster traffic be configured on its own VLAN to prevent interference of the heartbeat signal as a result of congestion that may occur during high traffic periods on the other interfaces. At a minimum, there should be two VLANs.

Alternatively, it is possible to configure the internal, external and Operations, Administration, and Management (OAM) addresses on separate networks, such as the web services interface network, service provider interface network and the management network. These networks can be realized through VLANs or Layer 3 networking, depending on customer network strategy and server capabilities and configuration. It is customer's responsibility, however, to configure Avaya ACE hardware and network elements to support this networking arrangement.

Example VLAN configuration

The figure shows a two VLAN configuration where channel bonding is used for network interface redundancy.



Security

A security audit was conducted prior to deployment. Big Bank was advised about of two aspects to security:

- Physical
- User access

Physical security

Big Bank ensured that Avaya ACE was deployed in a private internal enterprise network that was protected from direct access through the web server in the DMZ. Access between Avaya ACE and the web servers were secured through an HTTPS interface.

Big Bank IT confirmed port assignments, as noted in the *Agile Communication Environment Communication Environment Installation and Planning* (NN10850-004).

The network servers on the service provider interface were already located in the internal network and isolated through firewalls/NATs. Big Bank IT ensured that their protection strategy was in accordance with established corporate security practices. The web service interfaces did not have to be secured because the enterprise internal network was considered a trusted network.

Big Bank IT ensured that the network infrastructure included a layered defense with multiple layers of network security for protection against a broad range of security threats.

User access

Big Bank ensured that system administrator privileges to Avaya ACE and IBM WebSphere Application Server configuration and management resources were limited to designated personnel. They ensured that all default passwords were changed after deployment to protect against unauthorized access. In addition, the Avaya ACE administrator created specific user groups for general users to ensure their permissions were limited to individual user password changes and update of personal contact information.

Ordering

To support the Big Bank deployment the following software and licenses were merchandise ordered. The customer chose to supply the hardware (servers) to host the Avaya ACE Linux-based solution.

Component	Quantity
Base software	2 (one per server - redundant 1+1 configuration)
Click-to-connect service	2 (One per server - redundant 1+1 configuration)
Sametime license	5000 (one per user)
Presence license	5000 (one per user)

Corporate Directory

After a successful deployment of Avaya ACE with Sametime, Big Bank procured Avaya ACE Global Services to integrate a simple click-to-call solution into their existing Corporate Directory application.

Once originated, these calls do not need to be managed by Avaya ACE. In addition, Presence integration is not required.

It is expected that the increase in traffic will be about 1,000 users making a call through the portal at Busy Day Call Hour in addition to the existing traffic generated through Sametime.

Checkpoint

Big Bank case study

Use the customer meeting notes to answer the questions.

The customer has two sites:

- Site A has 2,500 users
- Site B has 2,500 users
- Both sites have a CS 1000E HA system.
- Both sites have a combination of terminal devices, including digital and IP phones.

How many Presence licenses are required to support Site A users?



_____ 0 (none required)

_____ 1 per node

_____ 2,500

_____ 5,000

Answer: 2,500



How many Sametime licenses are required to support Site A and Site B users combined?

_____ 0 (none required)

_____ 2,500

_____ 5,000

_____ 10,000

Answer: 5,000



How many Avaya ACE base software licenses does the customer require to support both Sites? Enter a numeric value (1, 2, 3, 4, etc.).

Answer: 2

Module summary

Objectives

In this module you learned how to:

- Given an example customer scenario, identify deployment recommendations for an Avaya ACE solution.

Conclusion

Course summary

Course objectives

In this course you learned how to:

- Describe the Avaya ACE solution, including purpose, design, basic features and services, and benefits.
- Communicate about SOA and web services fundamentals.
- Describe the basic components that comprise the Avaya ACE architecture.
- Identify basic deployment guidelines for Avaya ACE, such as communications and network infrastructure requirements, supported configurations, and security.
- Identify integration guidelines for Avaya ACE network elements (service providers), including supported services, network configurations, configuration guidelines, and how the service provider interacts with Avaya ACE.
- Describe the operations administration and management (OAM) capabilities that Avaya ACE offers, including security, users and groups, fault management, and performance management.
- Identify the web services that the Avaya ACE supports, describe the basic steps for developing web-enabled application, and provide examples of commonly used application development tools and technologies.
- Describe the applications, add-ins, service extenders and communications-enabled applications and business processes (CEBP) that Avaya ACE supports, including their purpose and functionality.
- Describe the Unified Communications - IBM Sametime desktop integration capabilities that Avaya ACE supports.
- Describe the Microsoft OCS desktop integration capabilities that Avaya ACE supports.
- Identify and distinguish between supported configurations and baseline hardware for an Avaya ACE solution.
- Describe the Avaya ACE software ordering and license management process.
- Identify the types of help and support that Avaya ACE offers.
- Given customer requirements, identify deployment recommendations for an Avaya ACE solution.

Copyright © 2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ®, TM or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.