Nortel Communication Server 1000

Nortel Converged Office Fundamentals — Microsoft Office Communications Server 2007

Release: 6.0
Document Revision: 03.09

www.nortel.com

NN43001-121

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-121
Document release date: 1 February 2010

Contents

New in this release

The following sections detail what is new in *Nortel Converged Office Fundamentals — Microsoft Office Communications Server 2007* (NN43001-121) for Nortel Communication Server 1000 Release 6.0.

Navigation

Features

See the following sections for information about feature changes:

TLS and sRTP

Enhancements to TLS and sRTP are implemented in Release 6.0 to provide enhanced interoperability with third-party products such as Microsoft products.

The following subsystems on the Communication Server 1000 are affected by the sRTP enhancements:

- Call Server
- Signaling Server
- Digital Signal Processors (DSP)
- Phase 2 UNIStim clients
- SIGMA Release 3.0 telephones
- SDesc

The following three areas of sRTP implementation changed:

- Best effort method for sRTP negotiation. The three additional attributes are tcap, pcfg, and acfg.
- Crypto keying materials used in SIP REINIVITES for call holding and resuming. SIP, SDP, and SDESC crypto attribute lines are updated to remove trailing zeroes as specified in RFC4568
- Master Key Index (MKI) can be configured for no support

The following are the TLS enhancements:

- increased chance of being authenticated by other users by sending the full certificate chain
- improved process to validate certificates by verifying that any certificate in the certificate chain was not revoked and that the FQDN and IP of the connection are consistent

AML Front End and IP Call Recording

The IP Call Recording feature complements the Nortel Converged Office solution by providing the ability to record calls simultaneously. The AML link is used to converge the Microsoft Office Communicator (OC) client and the Nortel IP phone for Remote Call Control (RCC) to monitor an IP phone for IP Call Recording. The AML front end is introduced in Release 6.0 and enables both co-resident and non-co-resident applications to simultaneously acquire and control the same or different phone DNs. The AML front end splits a single stream of AML messages from the call server into two or more outgoing streams of AML messages and multiplexes two or more streams of incoming AML messages into a single stream of AML messages to the call server. The components affected by the IP Call Recording feature are as follows:

- a new AML Front End on the Signaling Server
- modifications to AML message processing on the Call Server for desktop telephones converged by an Office Communicator (OC) client and additional related procedures
- modifications to the CSTA Front End for TR/87 on the Signaling Server to use the AML Front End
- a modified AML library module on the Signaling Server that is a component of the AML Front End

The AML Multiplex feature provides the ability to establish call recording on Converged Office with Microsoft Live Communications Server or Office Communications Server.

For more information about IP Call Recording, see *Automatic Call Distribution* (NN43001-551).

Zone Based Dialing (ZBD)

The Zone Based Dialing (ZBD) feature enables the removal of small, traditional PBX systems in multiple enterprise locations and replaces these with a single high-capacity Call Server model. New customers who plan to setup a private network in multiple locations can deploy the ZBD.

The migration to a single high-capacity Call Server is transparent to the end user. For example, the private and public (E.164) dialing plans and features are retained. OCS with E.164 dialing is not supported within the core system. Numbering zones are introduced to represent one location. All dialing and numbering parameters are configured for each numbering zone. Each telephone must be configured with a numbering zone.

For more information, see *Dialing Plans Reference* (NN43001-283).

Calling Party Privacy Enhancement

The Calling Party Privacy Enhancement (CPPE) feature provides a route option to ignore the Calling Party Privacy Indicator on incoming calls received from the North American public Integrated Services Digital Network (ISDN). When the Privacy Indicator Ignore (PII) prompt is configured to Yes in LD 16, the Calling Line Identification (CLID) Presentation Indicator and the Calling Party Name Display (CPND) Indicator (if it exists) are changed from Restricted/Denied to Allowed. This results in the number and the name (if available) to appear on the user's telephone display.

In Release 6.0, this new feature extends the CPPE feature to all ISDN interfaces including signaling applications that use ISDN formatted signaling such as VoIP. A new prompt is available to selectively allow or reject sending the calling party number to Auxiliary (Aux) applications when the calling party number is received with Presentation Indicator configured to Restricted/Denied. Consequently, applications can use the number to route without making the number or name available to all users.

Other changes

See the following sections for information about changes that are not feature-related:

Revision History

February 2010 Standard 03.09. This document is up-issued to update Telephony Gateway and Services planning section.

December 2009 Standard 03.08. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

August 2009 Standard 03.07. This document is up-issued to update Planning and Engineering section.

July 2009 Standard 03.06. This document is up-issued to update the UDP Location Code in the table Table 19 "Feature Interactions of RCC" (page 96).

June 2009 Standard 03.05. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

June 2009 Standard 03.04. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

June 2009 Standard 03.03. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

May 2009 Standard 03.02. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

May 2009 Standard 03.01. This document is up-issued for Nortel Communication Server 1000 Release 6.0.

How to get help

This chapter explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:
www.nortel.com/support
This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the telephone number for your region:
www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:
www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introduction

This document describes the elements and processes necessary to integrate Nortel Communication Server 1000 (CS 1000) with the Office Communications Server 2007 (OCS 2007) in the Nortel Converged Office.

Prerequisites

- Ensure Communication Server 1000 Release 6.0 is installed.
- Microsoft supports the coexistence of LCS 2005 SP1 Standard Edition or Enterprise Edition with OCS 2007 Standard Edition or Enterprise pools. For more information, see “LCS 2005 and OCS 2007 coexistence” (page 99).

Navigation

Converged Office component overview

This chapter provides a brief technical description of all the components associated with Nortel Converged Office.

Navigation

Converged Office

Many Nortel Communication Server 1000 customers base their multimedia strategy on deploying Office Communications Server (OCS) 2007 and the Office Communicator (OC) 2007 soft clients.

The Nortel Converged Office feature combines the business-grade telephony of the Communication Server 1000 with the OCS 2007 Enterprise Voice solution to offer a powerful converged office solution set that improves worker productivity. Telepresence and Multimodal (business set Voice over Internet Protocol (VoIP), Instant Messaging (IM), and e-mail) communications bundles, with applications such as Click-to-call and Access mobility, allow workers to stay connected when not at their desks.

Nortel Converged Office comprises the following components:

- Remote Call Control (RCC) with Session Initiation Protocol Computer Telephony Integration (SIP CTI) (TR/87) provides full Microsoft Office telephony integration to control business-grade telephony phones from within Microsoft Office applications, as well as support for a standards-based CTI interface defined by the TR/87 protocol.
- Telephony Gateway and Services provides a basic SIP Telephony Gateway to connect between Private and Public Telephony networks and OC 2007 clients.

  Nortel offers unique value with the two components that provide its telephony services to OC 2007 clients and connectivity between the Office Communications Server 2007 and the Nortel telephony network.

Nortel Converged Office provides the following benefits:

- federated IM with industry name instant messaging
- Microsoft application integration
- click-to-call commands and missed call log
- easy-to-use single soft client for IM, telepresence, and VoIP telephony presence integration with Microsoft desktop and applications
- a powerful suite of Nortel applications
  - — Nortel Unified Messaging
  - — Contact Center
  - — Interactive Voice Response (IVR)
  - — conferencing
  - — click-to-call

The Communication Server 1000 and Microsoft desktop software allows end users to access business-grade telephony services on the Nortel Communication Server 1000 from the Microsoft Office Communicator desktop client. End users can

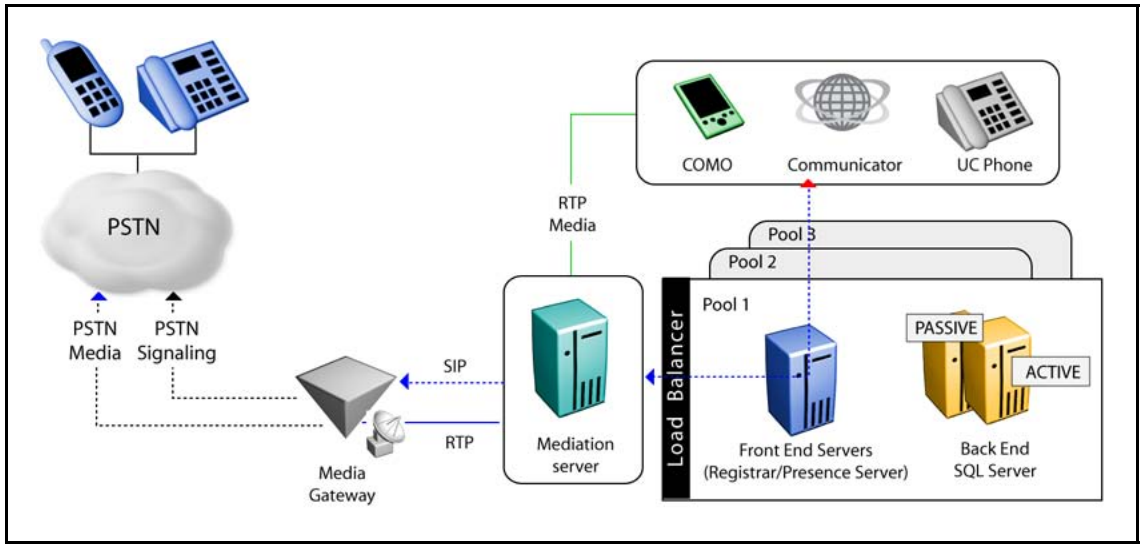
- originate and receive telephone calls over existing Communication Server 1000 phones from an Office Communicator (OC) 2007 desktop client.
- originate and receive Public Switched Telephone Network (PSTN) calls from the Office Communicator (OC) 2007 soft client when away from the office.
- take advantage of existing business telephony features on the Communication Server 1000.

Enterprise Voice

This section describes the Office Communications Server (OCS) 2007 Enterprise Voice solution. The Nortel Converged Office feature integrates the OCS 2007 with the Communication Server 1000. For a description of the integrated network from the Communication Server 1000 perspective, see “Network configuration” (page 50). Enterprise Voice is Microsoft’s software-powered VoIP solution, a SIP-based implementation of IP telephony for the enterprise that does not rely on proprietary hardware investments. Enterprise Voice is a full-featured VoIP solution that includes connectivity to the PSTN gateways and interoperation with the Communication Server 1000. Enterprise Voice, IM, group IM, enhanced presence, and audio-video conferencing together constitute the Microsoft Unified Communications solution.

The following figure shows the OCS 2007 Enterprise Voice components extracted from the overall OCS 2007 architecture. COMO refers to Communicator Mobile.

Figure 1
Enterprise Voice components—OCS 2007



When a user calls from an Enterprise Voice client by dialing or clicking on a contact name or number in OC 2007 or Outlook, the following occurs.

- the OCS Front End server normalizes the number to the E.164 format, and invokes routing rules based on the location profile and user policy, and directs the call to the appropriate Mediation Server
- the Mediation Server performs all necessary media transcoding and routes the call to the IP-PSTN gateway.
- the IP-PSTN gateway, based on topology, applies local or PBX dialing rules and passes the call to the PSTN or PBX

Enterprise Voice uses Real-Time Transport Protocol (RTP) for media. Like SIP, RTP is an Internet Engineering Task Force (IETF) standard. The standard defines a packet format to carry audio and video over IP networks.

Enterprise Voice uses SIP for signaling and RTP for media. In the OCS, SIP is used for IM, conferencing, presence subscriptions, video, and voice enabling Enterprise Voice clients to provide a common user experience across the communication modes.

Enterprise Voice is the Microsoft SIP–based implementation of IP telephony for the Enterprise.

SIP sessions can include the sharing of real-time media. However, SIP itself does not handle the actual media data, such as audio, video, and application sharing. This separation means that SIP and various media protocols can evolve independently.

OCS 2007 Voice components

The core routing components for Enterprise Voice reside on the following:

- Standard Edition Server (in the role of Front End Server or Director)
- Enterprise Edition Front End Server

Other core routing server components include

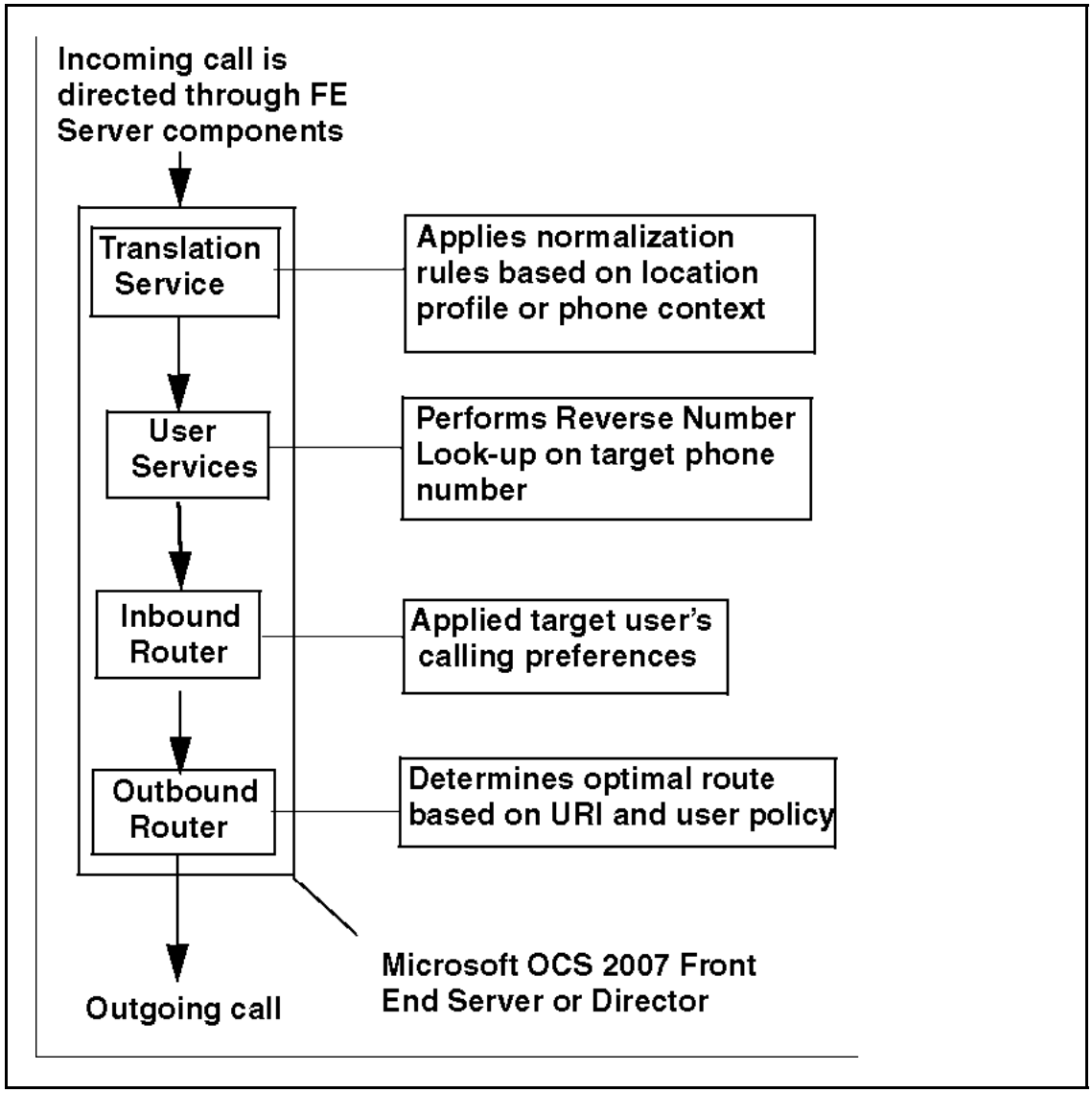
- Translation Service: translates a dialed number into E.164 format based on the normalization rules defined by the administrator.
- Inbound Router: handles incoming calls according to user-specified preferences.
- Outbound Router: routes calls to Communication Server 1000 or PSTN destinations after it applies authorization rules to callers and determines the optimal media gateway to route each call.

OCS 2007 Front End or Director components essential for voice support, but are not voice components, include

- User Services: performs Reverse Number Look-up on the target phone number for incoming phone calls.
- User Replicator: extracts user phone numbers from the Active Directory for use by User Services and the Address Book Service.
- Address Book Service: normalizes enterprise user phone numbers to E.164 format to provision user Contacts in Office Communicator.

The following figure shows the components essential for voice support.

Figure 2
Core routing server components



Media Gateways

Media gateways are third-party hardware components that provide a common interface between the Enterprise Voice infrastructure and the PSTN. Media gateways translate signaling and media between the PSTN and Enterprise Voice infrastructure.

Media gateways translate the following protocols between the circuit-switched PSTN network and the packet-switched Enterprise Voice infrastructure:

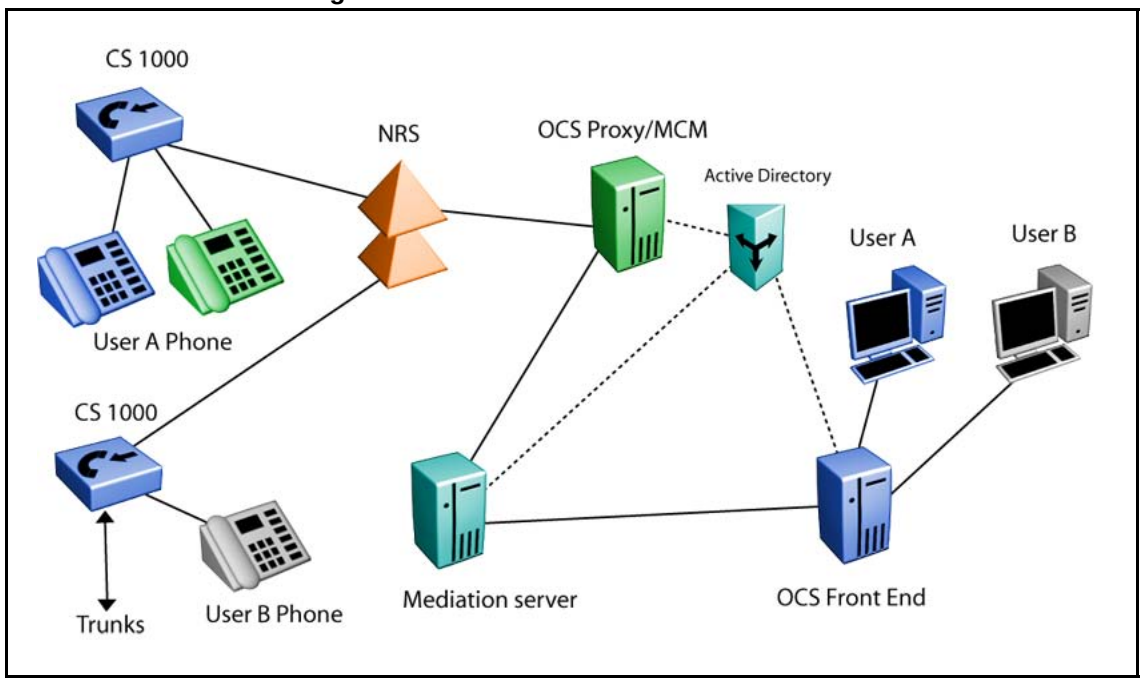
- Signaling protocol—SS7 and other protocols on the PSTN translate to SIP for Enterprise Voice
- Transport protocol—T-Carrier or E-Carrier on the PSTN converts to RTP or Secure Real-Time Transport Protocol (sRTP) for Enterprise Voice

From the Nortel perspective, the Communication Server 1000 functions as a media gateway for the clients of the OCS 2007 server.

Mediation Server

The Mediation Server provides signaling and media translation between the Enterprise Voice infrastructure and a Communication Server 1000 gateway.

Figure 3
CS 1000 and OCS 2007 logical network elements



The Mediation Server provides the following functions:

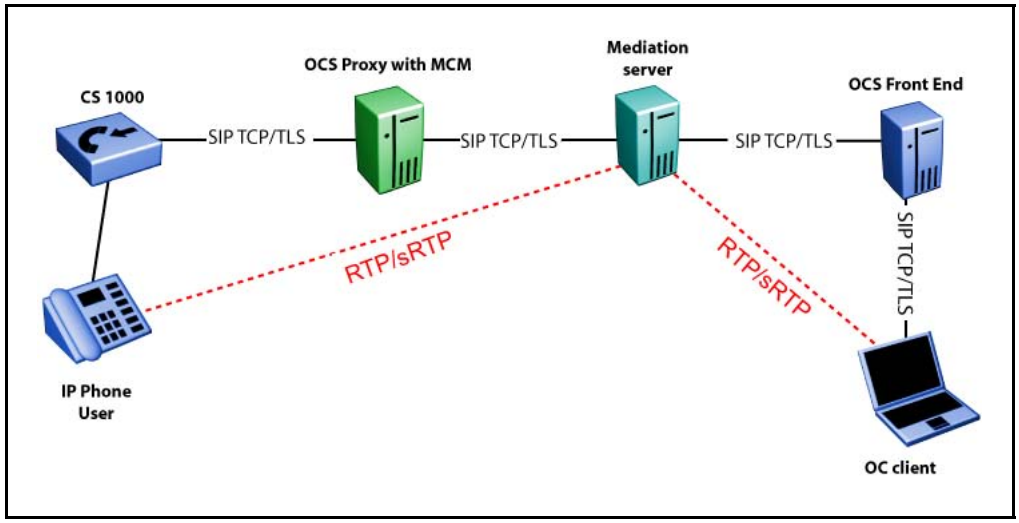
- translates SIP over Transport Control Protocol (TCP) and Transport Layer Security (TLS) on the Communication Server 1000 gateway side to SIP over mutual TLS on the Office Communications Server side
- encrypts and decrypts sRTP on the Office Communications Server side

- translates media streams (G.711) on the Communication Server 1000 gateway side and RT Audio on the Office Communication Server side
- connects clients outside the network to internal Interactive Connectivity Establishment (ICE) components, to enable media traversal of NAT and firewalls
- is an intermediary for call flows that a gateway does not support (such as calls from remote workers on an Enterprise Voice client)

The Mediation Server uses the following types of signaling:

- For an inbound call from the Communication Server 1000, the ms-call-source:non-ms-rtc SIP header is inserted by the Mediation Server.
- For an inbound call from the Communication Server 1000, the Mediation Server Back 2 Back User Agent (B2BUA) generates a Session Description Protocol (SDP) offer based on its capabilities in the OCS 2007.
- For an inbound call from the Communication Server 1000, the Mediation Server adds a phone-context attribute to a number that is not in E.164 format.
- For an outbound call from an OC 2007 client, the Mediation Server Back 2 Back (B2B) terminates the dialog and originates a new dialog with the Communication Server 1000. The From header is replaced with a phone number derived from the p-asserted-identity header.
- OC 2007 single step transfer. The Mediation Server terminates the REFER message and returns the response code 202. The Mediation server sends an INVITE message. The Mediation Server does not forward the REFER message to the Communication Server 1000.

Figure 4
Signaling and media path between OC client and CS 1000



Remote Call Control with SIP CTI (TR/87)

The Communication Server 1000 and OCS 2007 integration feature allows clients of the two systems (Microsoft OCS 2007 and Nortel Communication Server 1000) to communicate with each other. You can associate an OC Client, which connects to the OCS, with a Communication Server 1000 line. You can perform operations on the Communication Server 1000 line through the OC Client using Remote Call Control (RCC) often referred to as Phone-Mode. This feature provides consistent access to RCC, service control and configuration, and telepresence functions across various endpoints supported by the Communication Server 1000.

The Nortel Converged Office Solution is implemented through an open interface to ensure that any Communication Server 1000 feature supported through OC 2007 is also accessible to applications from other vendors and application developers who support these interfaces.

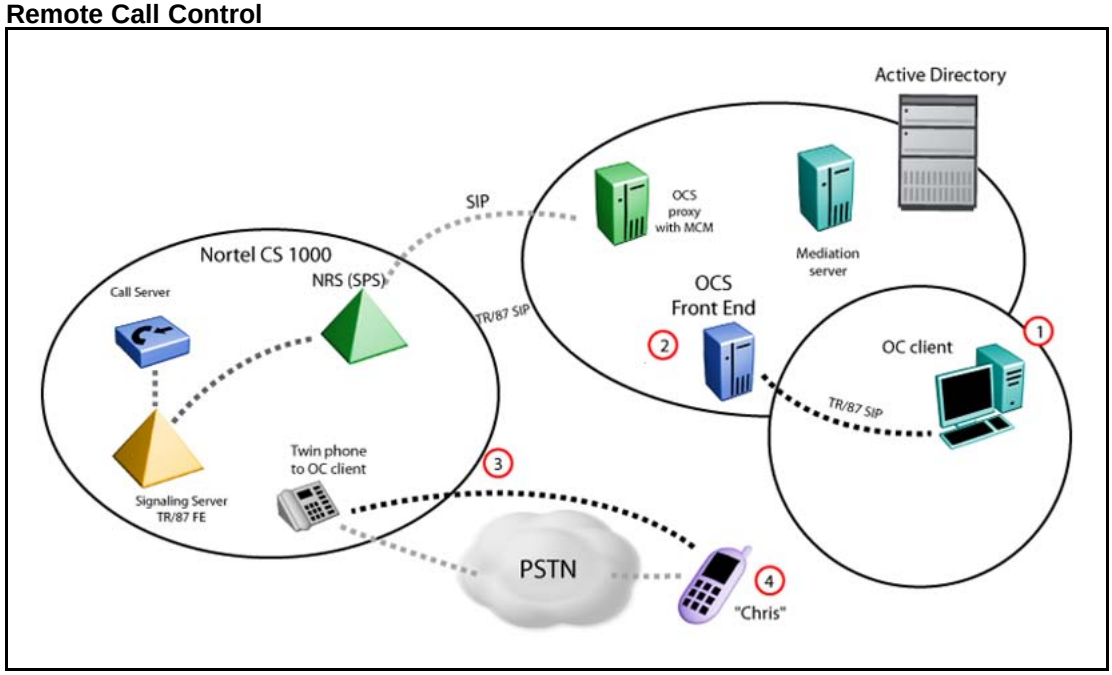
The SIP CTI (TR/87) protocol is on the Communication Server 1000 Signaling Server. OC 2007 uses the TR/87 specification to implement phone integration throughout the suite of Microsoft Office applications. You cannot use Office Communicator to invoke a feature that the phone does not support.

Example of RCC with SIP CTI (TR/87)

Figure 5 "Remote Call Control" (page 28) shows an example of a Communication Server 1000 call to a mobile client. The following steps correspond to the numbers in the figure:

1. A user selects Call to Chris' mobile phone number from the Communication Server 1000 telephone.
2. The Office Communications Server 2007 sends a call request to the Communication Server 1000.
3. The Communication Server 1000 sets up a call from the user's phone to Chris' mobile phone number.
4. Chris answers his mobile phone and a media path is established between the two phones.

Figure 5
Remote Call Control



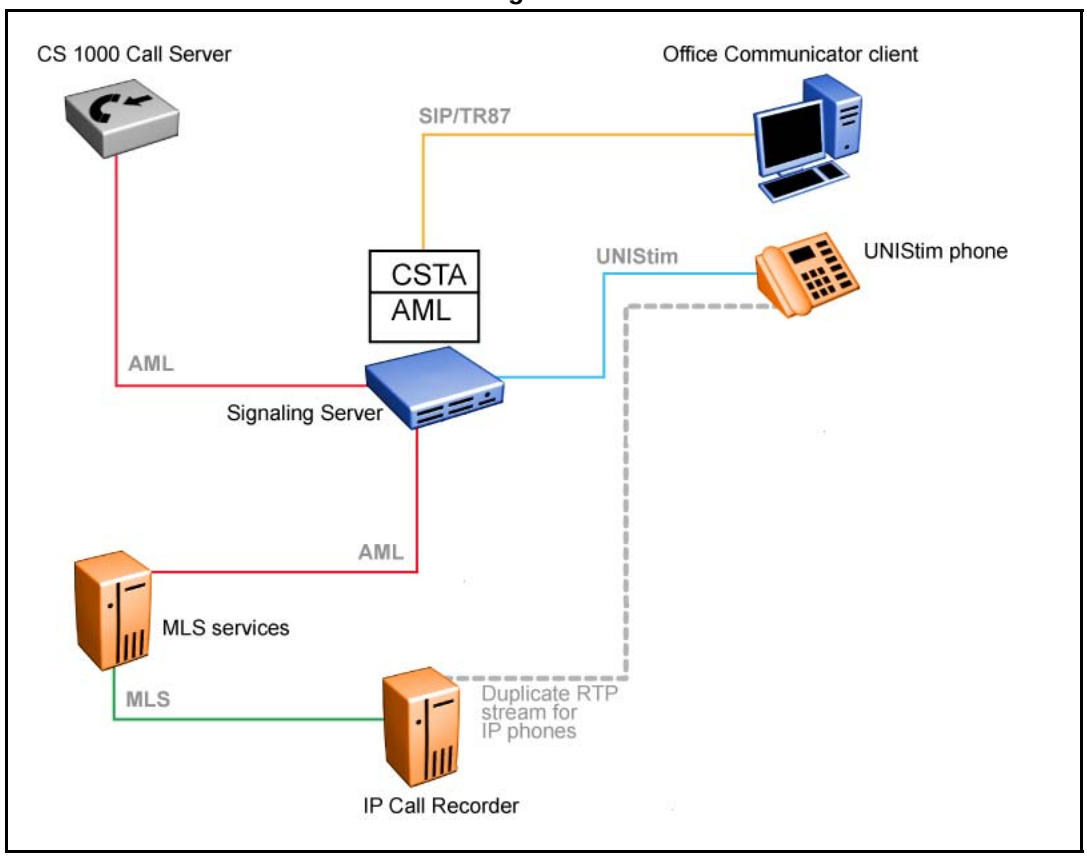
The full set of business-grade telephony features available with Communication Server 1000 telephones is integrated with the OC 2007 client and can be operated from a Communication Server 1000 IP Phone, even when the client is unavailable. This integration ensures that telephony service reliability is preserved during interruptions in soft client operation.

With the convergence of the Communication Server 1000 with the OCS 2007, the OC 2007 client complements the voice communications between two users by allowing other media types, such as IM, file, and application sharing to an existing voice call without the need to establish an independent session between the users.

AML Front End and Library module

When SIP CTI services is enabled in the node configuration for IP Telephony in Element Manager, the AML Front End starts up when the master Signaling Server initializes. The AML Library module on the Signaling Server is started by an application that needs the AML IP link. When two or more Signaling Servers are configured in a node with SIP CTI services enabled, the leader-follower scheme takes effect and the AML Front End co-resides with the SIP Gateway. The AML link is used to converge the Microsoft Office Communicator (OC) client and the Nortel IP phone for Remote Call Control (RCC), to monitor an IP phone for IP call recording functionality. The following diagram shows the general architecture for IP call recording.

Figure 6
General architecture for IP call recording



Node master Signaling Server is down

If a Signaling Server loses node mastership, the AML Front End and all related data structures stop. The Signaling Server that becomes the new node master takes over the node IP address and launches the AML Front End. The AML Front End contacts the Call Server to ask for an AML link, the Call Server sends an AML INIT message to the AML Front End and the co-resident applications are notified by a related ITG event. The same AML IP link number as the previous node master is used.

For example, an OC client attempts to acquire the DN of a desktop phone by using the AML FE on the new node master. A positive response to the OC client is received from the Call Server through the AML Front End. The AML Front End has the same AML link number and Application ID as the AML Front End running on the previous node master. The OC client and IP Call Recorder must recreate DN registration through Meridian Link Services (MLS), and the AML FE on the new node master. An active conversation using an IP phone converged by an OC client remains operational when the node master Signaling Server loses mastership; however, the Remote Call Control functionality on the OC client does not work. To reestablish the OC client connection after a Signaling Server becomes the new node master, the OC client user can either manually log on to the OC client or wait up to 25 minutes for the OC client to acquire the IP phone automatically through the new master Signaling Server.

The master Signaling Server loses mastership when the following network failures occur:

- Lost ELAN connection with Call Server, detected by keepalive messages through the pbxLink
- Lost TLAN carrier connection, detected by a network interface signal

After one of the preceding failures is detected, the current node master Signaling Server calls an election whereby a follower Signaling Server in the node becomes the new node master. The master Signaling Server does not vote for itself. If the current node master Signaling Server is isolated from the remainder of the network, the follower Signaling Servers do not receive the broadcast of I am the master from the current node master. In this case, a follower Signaling Server calls the election and becomes the new node master.

Call Server warm or cold start

During a warm or cold bootup of the Call Server, the active AML Front End is notified by related ITG events Master Off and Master On. After receiving the Master On notification, the AML Front End sends an ITG message to the Call Server for an AML link and the Call Server sends an AML INIT message to the AML Front End. After receiving the AML INIT message,

the AML Front End clears all old data in the related tables and lists and then raises a relevant ITG event to notify co-resident applications. When a connection between the AML Front End and a non-co-resident application is established, an AML INIT message is sent to this newly connected application. After receiving the AML INIT message, the newly connected application can acquire related resources on the Call Server through the AML Front End.

Telephony Gateway and Services

With the Telephony Gateway and Services component, users can choose how to make and receive calls. For outgoing calls, users can make a call from their Office Communicator (OC) 2007 soft client instead of their phone. You can handle incoming calls in one of two ways: through the computer with OC 2007 or through a phone. This feature provides users with computer-to-phone and phone-to-computer connectivity, leveraging the Nortel provided dial plan, telephony infrastructure, and telephony features to make and receive calls using OC 2007 as a soft client.

With this solution, you can configure Telephony Services (TLSV) on the Communication Server 1000 for each user with this functionality. The Communication Server 1000 configured with the TLSV provides number plan translations, Call Detail Recording (CDR) for outgoing calls, and enables telephony features, such as Call forward No Answer to Voice Mail, Attendant Recall, and participation as a client in a Group Call for incoming calls.

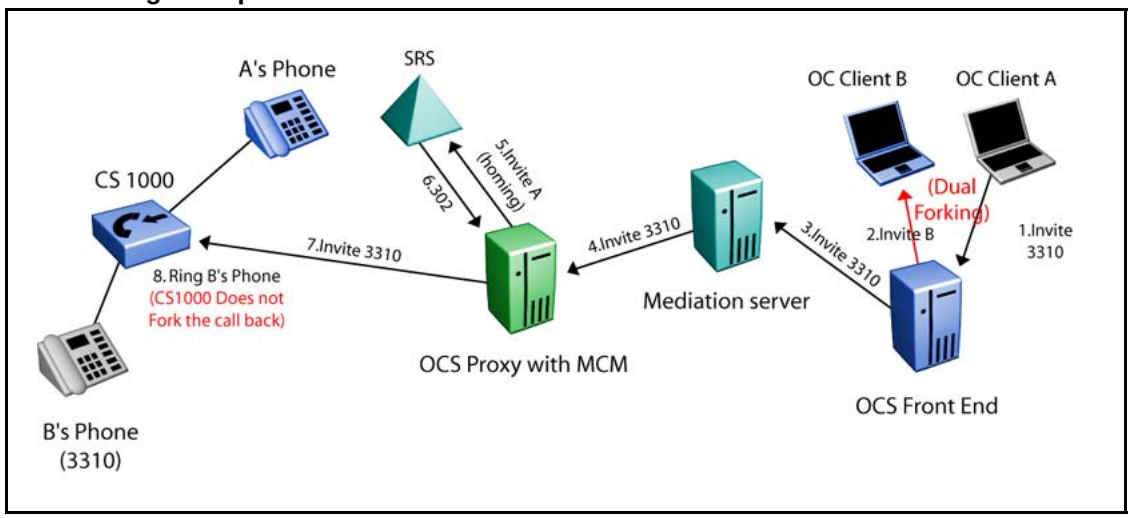
With the Telephony Gateway and Services component, you can configure the OC 2007 client as a Multiple Appearance Directory Number (MADN) member for users with TLSV on the Communication Server 1000. With TLSV, calls to a user's phone number can be presented to both the desktop phone and to the OC 2007 client simultaneously. The user can then choose to answer on the most convenient device.

The ability to connect between computers and phones is not natively provided by Office Communications Server 2007; however, the Telephony Gateway and Services component enables this functionality using the SIP Gateway and Multimedia Convergence Manager (MCM) application. MCM directs calls from an Office Communicator user to the Communication Server 1000 connected to their twinned telephone. With Telephony Gateway and Services, you can originate and receive SIP calls (for example, VoIP and Computer calls) from Office Communicator.

In Figure 7 "Dual forking example" (page 32), OCS Front End (FE) forks the call to the Communication Server 1000 . The twin phone rings once and does not send another invite. The same scenario applies to calls originating from the Communication Server 1000 , the OCS is not informed

to perform another fork. A setting on OCS 2007 server is available to enable or disable dual forking for each user. Remote Call Control (SIP CTI) is available when dual forking is enabled.

Figure 7
Dual forking example



Telephony Services (TLSV)

Many of the features provided by CS 1000 to traditional telephones extend to Office Communicator clients configured with Telephony Services (TLSV). For example, calls that remain unanswered can be forwarded using the Call Forward No Answer feature.

To use the Office Communicator soft client for voice calls using the Telephony Gateway and Services, a TLSV must be configured with the same DN as the user in a MADN arrangement. This offers incoming voice calls to the user's DN on their Office Communicator, as well as any phones that they are configured with the same DN.

For incoming calls to be extended to the "twinned" Office Communicator client, a UEXT Terminal Number (TN) must be defined for that DN. The TLSV subtype has been introduced so a distinction exists between UEXT associated with the OCS 2007 client and UEXT associated with other types of clients. During call processing, the subtype is checked to determine whether an incoming call should be extended to the UEXT target DN or not. For more information about configuring TLSV, see "Configuring Telephony Services" (page 187).

For outgoing calls from the Office Communicator, the user must have at least one TN configured on the Communication Server 1000 Call Server. The MCM locates the Call Server associated with a user by the Mediation Server used to place the call. This generates calls from Office

Communicator clients on Telephony Gateway and Services to always tandem through the user's active Call Server. Note that with Geographic Redundancy features, a user's active Call Server may change during failure scenarios. Multiple Call Servers can be associated with the Mediation Server.

The Network Class of Service (NCOS) setting for outgoing calls from Office Communicator clients is determined by the configuration of the MARP TN when in a MADN group, or by the configuration of the UEXT when it is the only TN for the user.

With TLSV and Remote Call Control configured, users receive one pop-up window for the incoming call to the phone or computer. Users can choose the most convenient way to answer an incoming call.

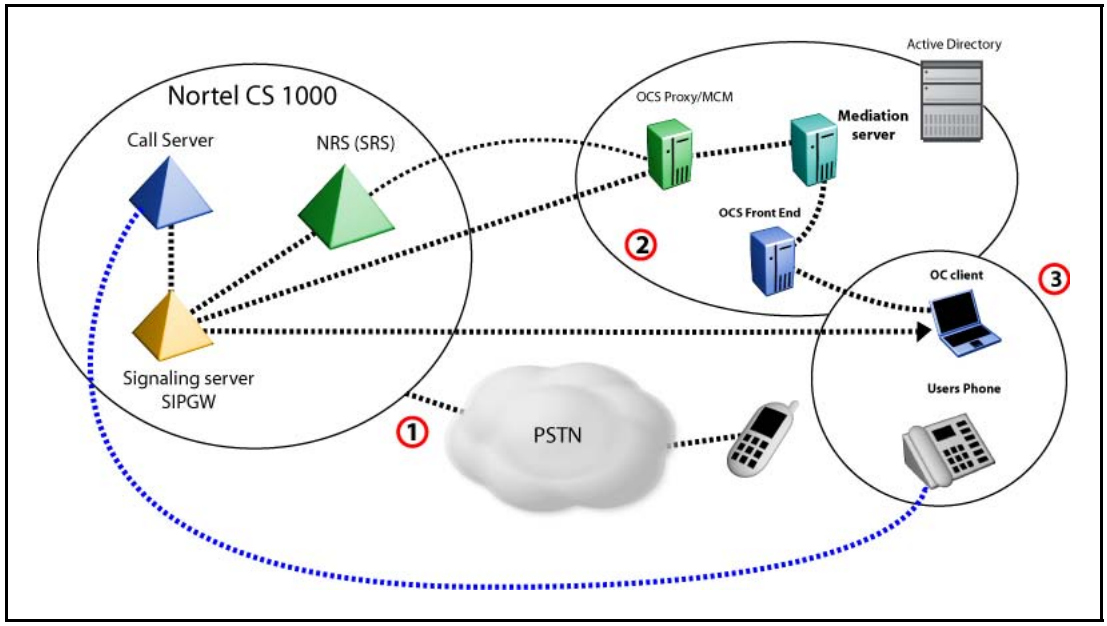
Telephony Services (TLSV) example

While at the office, a user may decide to use a desktop phone to answer calls. However, the user can still accept calls through the OC 2007 while they travel to locations that have network connectivity (for example, at hotels).

The following steps correspond to the numbers in the figure:

1. The Communication Server 1000 system receives a PSTN call to the user's phone number.
2. The Communication Server 1000 rings the user's phone and uses the TLSV subtype to provide simultaneous ringing to both the user's phone and the Office Communicator voice client.
3. The user can answer the call through the Communication Server 1000 phone or the Office Communicator voice client.

Figure 8
Example call scenario



Users can be reached anywhere on the network and significant cost savings are incurred by using IP telephony through Virtual Private Network (VPN) access to their private network.

As part of the telephony services, many incoming call features are available even when using the OC 2007 as a telephony device or more specifically in Computer mode. Features such as Call Forward No Answer, Unified Messaging, Call Detail Recording, and Attendant Recall are maintained within the Communication Server 1000 system for calls presented to the OC 2007.

Telephony Gateway and Services can access all of the telephony network resources using the OC 2007 client. Calls can originate from the OC 2007 client to the PSTN, phones, or services within the telephony network. Users can access all of their telephony network resources as long as they have the soft client and a high-quality connection to their private network. Telephony Gateway and Services is enabled by the interworking of the Communication Server 1000 SIP Gateway with the OCS 2007 SIP gateway software.

Access Edge Server

Access Edge Servers allow internal and external users to communicate across corporate firewalls. Access Edge Servers enable IM and presence, as well as Web conferencing and audio/video (A/V) collaboration between internal and external users.

Access Edge Servers include the following server roles deployed on one or more computers in the perimeter network:

- The Access Edge Server handles the SIP traffic necessary to establish and validate connections between internal and external users.
- The Web Conferencing Edge Server enables external users to participate in internal conference meetings. The Web Conferencing Edge Server handles the exchange of meeting content between internal and external users.
- The Audio/Video (A/V) Edge Server enables A/V conferencing between internal and external users to allow for the sharing of audio and video with external users.

  Microsoft recommends that you use the OCS 2007 Director, although it is not required.

ATTENTION
Office Communicator video is supported only for Remote Call Control between two Office Communicator clients. Office Communicator video is not supported if one of the clients goes through the SIP Gateway.

OCS 2007 snap-in

The Office Communications Server 2007 snap-in for MMC is redesigned. The Status pane of the Office Communications Server 2007 snap-in provides configuration settings at-a-glance for your forest, domains, pools, servers, and users. The Status pane also features a new Database tab, which can be used to query a pool back-end database. Each query is displayed as an expandable item in a list.

Microsoft Management Console (MMC) is automatically installed on each server in the domain that runs Office Communications Server 2007 or any computer on which Office Communications Server 2007 administrative tools are installed. It is not used to administer Edge Servers or Proxy Servers.

ATTENTION
Enhanced presence must be enabled prior to Converged Office telephony integration. You can enable enhanced presence from the Office Communications Server Users Wizard in the Configure Users Settings window.

Multimedia Convergence Manager

Multimedia Communications Manager (MCM) 4.x is a software component that ensures interoperability between the Communication Server 1000 and the Microsoft Office Communications Server (OCS) 2007. MCM 4.x is compatible with Communication Server 1000 Release 5.0 and 5.5 with PEP, and Communication Server 1000 Release 6.0. MCM 4.x can be used

in a mixed environment. For example, you can configure MCM with SIP TLS to SPS and communicate with nodes from earlier releases. MCM 4.0 is not compatible with the SPS releases 5.0 and 5.5 (lower than SU 5.50.12.006).

The MCM ensures Communication Server 1000 and OCS interoperability of protocols, users, and phone numbers are managed within the Microsoft Active Directory. The MCM also allows the system to block calls where the client is not in the Active Directory (AD). The MCM performs a number of functions.

- translation between telephony phone numbers and user IDs within the Active Directory
- authentication of user phone numbers for RCC
- Numbering Plan normalization
- protocol interworking
- redundant connections to the Communication Server 1000 network components (SIP Redirect Service (SRS), Sip Proxy Server (SPS), and redundant Signaling Servers)

CDR data collection

OCS 2007 supports CDR capability. OCS 2007 CDRs collect different kinds of data that include user logon and logoff, IM and audio call details, Conferencing start and join. You must install the Archiving and CDR Server to support these features. The outgoing calls from the OC 2007 to Communication Server 1000 telephone are captured by this server, as well as OC to OC calls. Thus a call accountant can retrieve CDRs from both the Communication Server 1000 and Archiving server to obtain a consolidated report. In RCC mode, CDRs are captured only on the Communication Server 1000 side. For more information, see *Microsoft Office Communications Server 2007 Archiving and CDR Server Deployment Guide* . Download Microsoft technical documentation from the Download Center at www.microsoft.com.

SIP CTI (TR/87) Protocol

The SIP CTI (TR/87) FE application introduced with this package is not limited to Microsoft applications. Through support of the ECMA TR/87 standard, Nortel partners can use this interface to develop SIP CTI capabilities for use with any specification-compliant application.

If Preferred Calling Device is configured as Phone, a user receives one pop-up notification with an incoming call, as depicted in Figure 9 "Call Appearance pop-up window" (page 37). The OC user can click Redirect to choose the client as the answering device.

Certain portions of the protocol are not supported. Additional information about the SIP CTI (TR/87) protocol is available to Nortel partners upon request.

Figure 9 "Call Appearance pop-up window" (page 37) shows an example of an incoming call pop-up window.

Figure 9
Call Appearance pop-up window

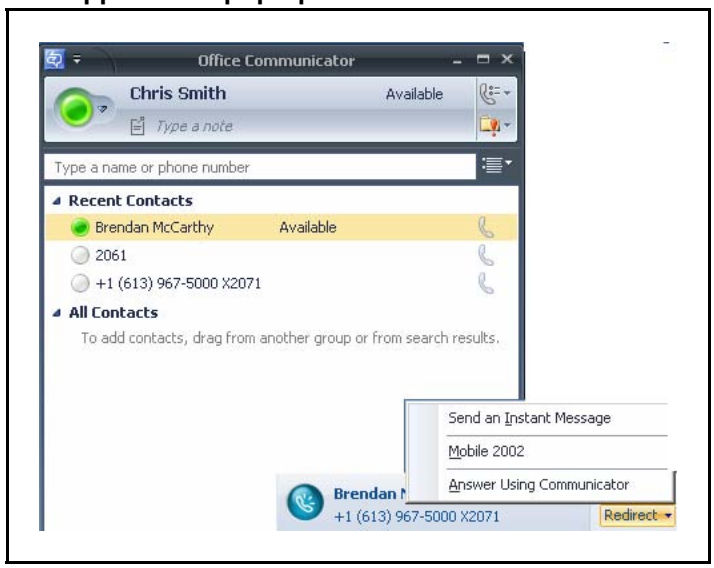


Figure 10 "SIP diagram" (page 38) depicts the SIP protocol information.

Figure 10
SIP diagram

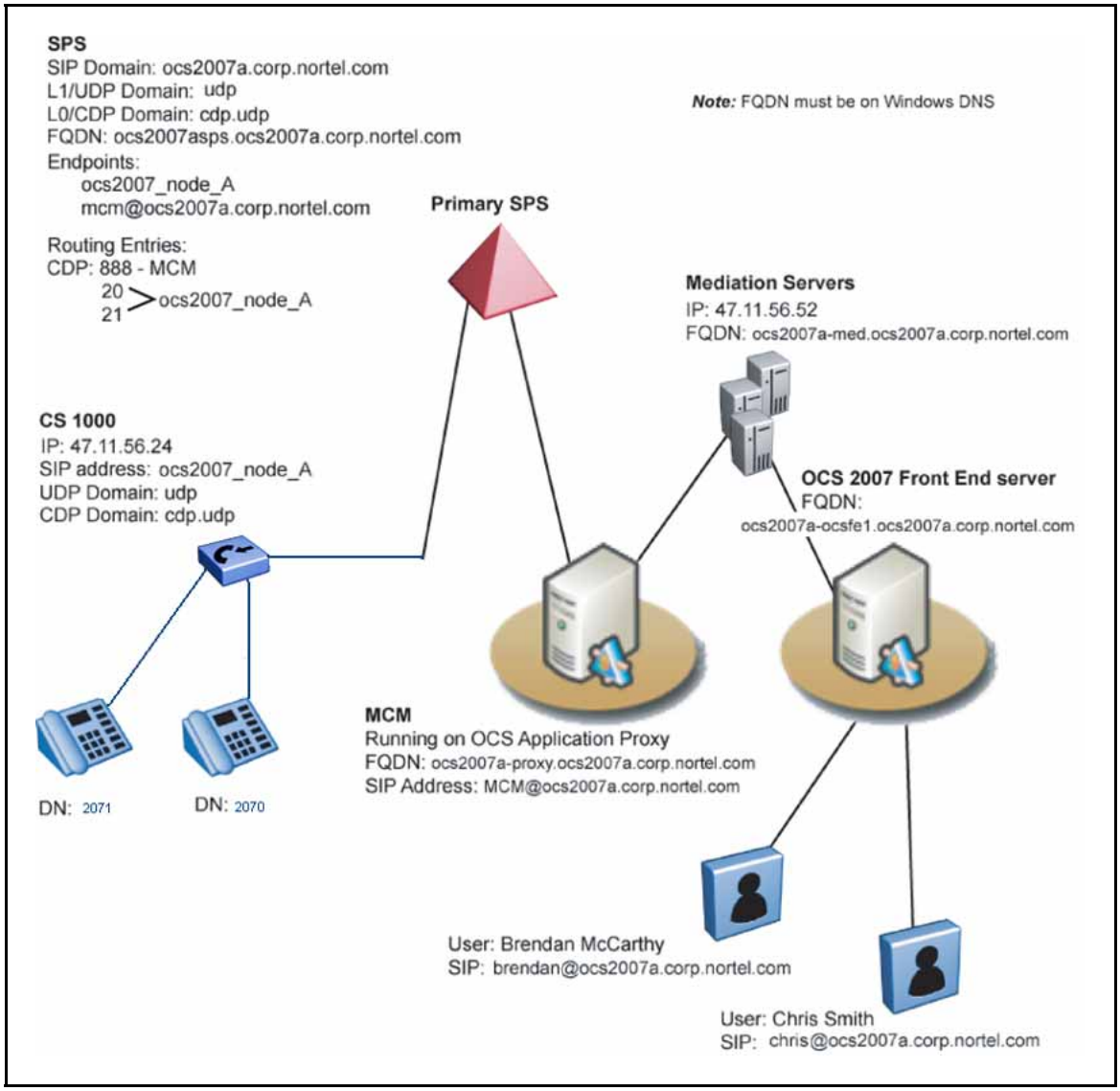
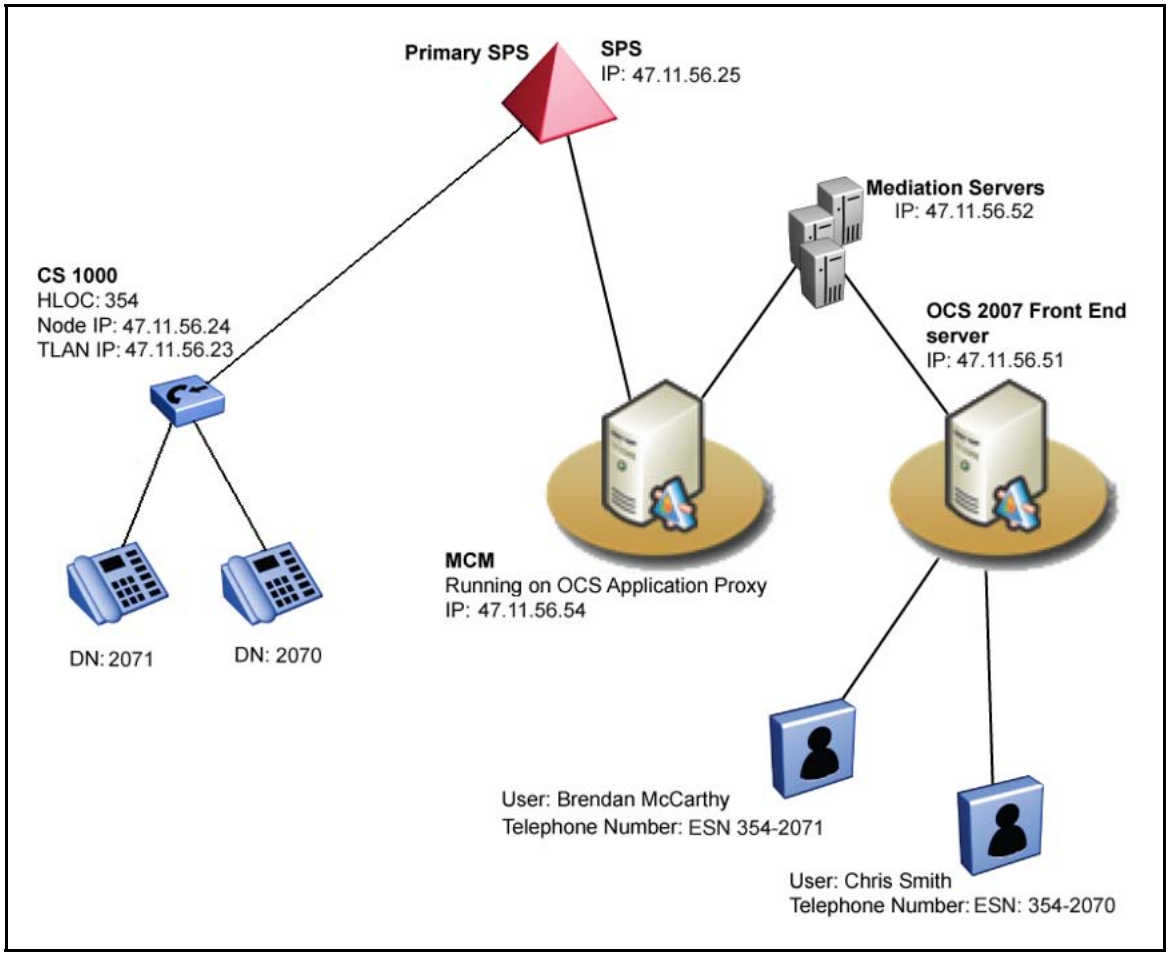


Figure 11 "IP diagram" (page 39) depicts the IP protocol information.

Figure 11
IP diagram



ATTENTION
Customers must not use their Office Communicator client to call Emergency numbers (for example, 911). To ensure that emergency service organizations can accurately trace the source of the call, always use a desktop phone to place an emergency call.

Hardware Load Balancer

Hardware IP Load Balancers (for example, Nortel Application Switches) are required for multiple Office Communications Server 2007 Enterprise Edition deployment. The Load Balancer presents a single virtual IP (VIP) address to clients to prevent direct access to individual OCS 2007 Enterprise Edition servers. The Load Balancer uses an algorithm (for example, round-robin, or fewest connections) to route new client requests to the Office Communications Servers.

Hardware Load Balancers deliver load distribution to avoid a single point of failure. Other benefits include increased performance and added redundancy. The Communication Server 1000 uses Load Balancers for the signaling path of VoIP calls and Remote Call Control.

A Load Balancer is not required if you deploy:

- a Standard Edition server
- a single Enterprise Edition Front End server

A load balancer is required if you deploy:

- multiple OCS 2007 Enterprise Edition Front End servers
- an Array of Edge Servers
- an Array of Directors in OCS 2007
- an Array of OCS Proxy/MCM servers (for redundancy)

Microsoft recommends that you deploy a hardware load balancer for arrays of Office Communications Server 2007, Edge Servers, and Directors but it is not a requirement. Office Communications Server 2007 does not support the use of Windows Server 2003 Network Load Balancer in production or lab deployments. The Communication Server 1000 handles only the load balancers for the signaling path for VoIP and Remote Call Control (RCC).

Dialing plan considerations

For a successful Zone Based Dialing (ZBD) configuration, it is critical to develop the dialing plan. The dialing plan is centralized to control call routing for many sites with various dialing plans. The following is a list of the dialing plan considerations for migrating to the ZBD:

- independent dialing patterns for each location
- local dialing—dialing local extensions with three to five digits.
- Non-DID/DID phones, for example, a conference room, and lobby
- Special Numbers, for example, emergency, voice mail, and help
- numbering plan to accommodate a large number of locations

OCS 2007 R2 feature interactions

The following table describes the feature interactions associated with OCS 2007 R2. For interoperability with OCS 2007, all endpoints must support RFC2833. The MC32 card is not supported for interoperablity with OCS as

the MC32 media card does not support RTCP reports that are required by OCS. In a scenario where the Music on Hold feature is provided by OCS, the call is dropped.

Table 1
R2 feature interactions

Component	Description
Call forward on OC client	When the call forward feature on the OC client is used, in some instances a delay occurs before media is established. This scenario can occur when using a direct SIP configuration with OCS.
Microsoft Exchange UM: Call Forward No Answer	If a call receives Call Forward No Answer (CFNA) after being transferred twice, a delay occurs before a media path is established to Microsoft Exchange UM Scenario.
OC client	Logging off the OC client when on a call causes OC to hang.

Office Communicator 2007

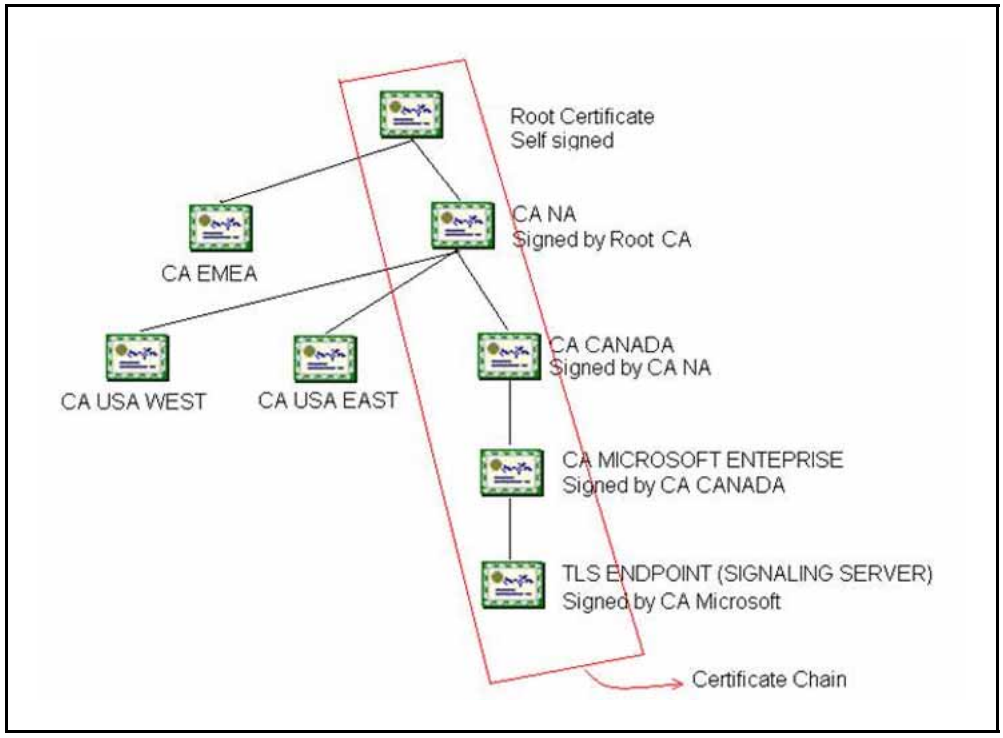
For detailed information about using Office Communicator 2007 and components, see *Converged Office User Guide — Microsoft Office Communications Server 2007* (NN43001-123).

Certificate chain

The supported application is the SIP Gateway. A certificate chain is a series of certificates issued by successive CAs. The certificate chain starts with the peer certificate and finishes with the root of the hierarchy. Each certificate is signed with the private key of the issuer and can be verified with the public key of the issuer certificate that is next in the chain.

The following figure depicts a certificate chain with a length of five.

Figure 12
Certificate chain example



The CA that issues the certificate to the peer (or endpoint) provides the certificate chain. To import all certificates into the Signaling Server from Unified Communications Management (UCM), all certificates must be packed into a single file that is formatted as Privacy Enhanced Mail (PEM).

The certificate chain is pushed down to OpenSSL during configuration of the SIP stack as part of the Signaling Server bootup sequence. The certificate is then sent to the far end where an SSL/TLS session is negotiated.

The following figure is an example of a PEM formatted certificate chain. It starts from the TLS endpoint certificate and finishes with the root certificate.

Figure 13
Certificate chain example

```
-----BEGIN CERTIFICATE-----
MIIE2jCCA8KgAwIBAgIQT2vtM5bxD7ZGDavj2B+fEDANBgkqhkiG9w0BAQUFADBu
MRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGbm9ydGVsMRQw      - TLS Endpoint certificate
EgYKCZImiZPyLGQBGRYEY29ycDEXMBUGCgmSJomT8ixkARkWB3VtMjAwN3IxEDAO
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
BgNVBAMTB2txdnpwNDYwHhcNMDcwNTE0MTkxNDQ4WhcNMTIwNTE0MTkyMTM3WjBu
MRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGbm9ydGVsMRQw    -  CA Microsoft Enterprise Certificate
EgYKCZImiZPyLGQBGRYEY29ycDEXMBUGCgmSJomT8ixkARkWB3VtMjAwN3IxEDAO
...
BgNVBAMTB2txdnpwNDYwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCq
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
TzONdBtRaI6F4tQRezrnB9m3nWbgkELt/XT6OBB6f2F2WD4rPAmJF5LFdwJGH9QK
ljFgYwTlkqdhuITQTBVHtVGNscTY8Cys40gpXxtWipqOOENARDuPR9K8hLLfIY9C    -  CA CANADA Certificate
...
/5UzLvB8g0qE+AODywGyDuyBAkuaaOc3hi23EU6VSe+Gf+BgS5/7rH4wnb/XYJbT
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
YAjRGbnR+/3XYK1ftTEpHpHdFpfj3n+YydLzZn0xLa4iuovKf4rQmh1FBEOlO8LF
WtEuqqVjLeWdo0Phux9sDsEHEv3n8m1v03y4oMvirRWpmxL9E5veyq6etkYKzX0J     - CA NA Certificate
...
C1RsQOJIZZFLOI6MnwTVAgMBAAGjggFyMIIBbjALBgNVHQ8EBAMCAYYwDwYDVR0T
AQH/BAUwAwEB/zAdBgNVHQ4EFgQUTlrwrYzeLXl/U7IuMPEtijdk9eUwggEbBgNV
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
HR8EggESMIIBDjCCAQqgggEGoIIBAoaBwGxkYXA6Ly8vQ049a3F2enA0NixDTj1r     - Root CA certificate (Self signed)
cXZ6cDQ2LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2
...
aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXVtMjAwN3IsREM9Y29ycCxEQz1ub3J0
ZWwsREM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
-----END CERTIFICATE-----
```

Certificate validation

The supported applications are SIP Gateway and SIP Proxy server.

When a private key of a certificate is compromised, some CAs issue a Certificate Revocation List (CRL), which can be checked to determine if a particular certificate is revoked. CRL files are signed with the private key of the CA issuing it. UCM provides a mechanism to transfer CRL files into each element in the UCM Security Domain. A periodic update must occur on all CRL files as CA regularly publishes new versions of the CRL files.

During the TLS session negotiation, the far endpoint sends a certificate chain to be verified. To verify if each certificate in the chain is revoked you must enable CRL checking in OpenSSL. This prompts an application call back function to pass back to the CRL for the requested CA.

OpenSSL checks the integrity of the CRL file with the public key of the CA issuing the CRL. The correctness and expiry date of the CRL is verified, and then OpenSSL determines if the certificate is revoked. If the certificate is revoked, OpenSSL notifies the application through a call back function that a particular certificate in the chain is revoked so that the application can take proper action.

The FQDN or IP address in the certificate is verified to ensure that it is consistent with the IP address of the underlying TCP connection for TLS. A certificate can include an FQDN or IP address in the Common Name field or in the SubjectAltName extension. This enhancement calls for an FQDN or IP address to always be included in the Common Name field. In addition, external DNS or local static DNS table must be available; you can configure these values in Element Manager for SIP Gateway and UCM for SIP Proxy Server. The *Linux Platform Base and Applications Installation and Commissioning* (NN43001-564) explains configuring DNS in the Linux Base. After the certificates are verified, a post connection check verifies the client/server certificate FQDN or IP address against the IP address connection.

SIP Gateway

The call back function receives the connection ID and the host name as parameters. If the host name contains a FQDN, the application function performs a DNS lookup and compares the IP address with the one derived from the connection ID. If the DNS lookup fails, the connection cannot be guaranteed to be from the intended endpoint and the TLS channel is not established.

If the host name contains an IP address, the application call back compares it with the IP derived from the connection ID. If a match occurs the connection is established; otherwise, it is closed.

SIP Proxy server

Verification of the FQDN occurs after connection where the Subject Alternative Field for DNS name is verified first. If the SAN and CN field do not exist or if the DNS name does not match the FQDN derived from the IP address then the Common name field is used. The connection terminates if the client/server certificate fails these tests.

Table 2
TLS connection FQDN comparison against certificate SAN and CN fields

Certificate Subject Alternative Name: DNS name	Certificate Common Name	Result
Does not match with FQDN of connection	Does not match with FQDN of connection	Fail
Matches with FQDN of connection	Does not match with FQDN of connection	Succeed
Does not Match with FQDN of connection	Matches with FQDN of connection	Succeed

Documentation References

A list of Nortel and Microsoft documentation is available for reference from the following Web sites.

- You can download Nortel documentation from the Nortel technical documentation Web site at www.nortel.com.
- Download Microsoft technical documentation for R1 and R2 content from the Download Center at www.microsoft.com.

The following Nortel technical documents are relevant to Nortel Converged Office.

Table 3
Nortel technical documentation

Technical document	Content	Primary audience
Converged Office User Guide — Microsoft Office Communications Server 2007 (NN43001-123)	Information about using the OC client	General users
Communication Server 1000E Planning and Engineering (NN43041-220)	Instructions about calculating the anticipated call traffic for the CS 1000	Administrators
Features and Services (NN43001-106)	Information about the Multiple Customer environment, Multiple Appearance DN , Call Forward On feature, and defining and configuring a UEXT TN	Administrators
CallPilot Network Planning Guide (NN44200-201)	Information about configuring CallPilot for Telephony Gateway (Computer mode) calls	Administrators
Communication Server 1000M and Meridian 1 Large System Installation and Commissioning (NN43021-310)	Information about CS 1000 Installation and Commissioning	Administrators
Communication Server 1000E Installation and Commissioning (NN43041-310)	Information about CS 1000 Installation and Commissioning	Administrators
Signaling Server IP Line Applications Fundamentals (NN43001-125)	Information about Signaling Server installation	Administrators

Technical document	Content	Primary audience
IP Peer Networking Installation and Commissioning (NN43001-313)	Information about creating the required components on a Call Server, dialing plans, configuring codecs, configuring HLOC and HNPA, configuring SIP trunks, configuring NRS, and alternate routing logic (for Geographic Redundancy)	Administrators
Transmission Parameters Reference (NN43001-282)	Iinformation about configuring the loss plan and DTI Data Bock	Administrators
Element Manager System Reference — Administration (NN43001-632)	Information about how to access Operational Measurements through Element Manager	Administrators
NRS Fundamentals (NN43001-130)	Procedural information	Administrators
Communication Server 1000 with Microsoft Exchange Server 2007 Unified Messaging Fundamentals (NN43001-122)	Information about how to setup Unified Messaging on Microsoft Exchange.	Administrators
Dialing Plans Reference (NN43001-283)	Dialing plan information	Administrators

Table 4
Microsoft OCS 2007 and OC 2007R1 documentation

Guide	Contents	Primary audience
Microsoft Office Communications Server 2007 Documentation Roadmap	Guide to the contents and uses of the documentation	Administrators
Office Communications Server 2007 Technical Overview	Contains a high-level survey and summary of the features, architecture, and protocols of Office Communications Server 2007	Administrators
Microsoft Office Communications Server 2007 Planning Guide	Contains step-by-step information about planning your deployment	Senior Administrators responsible for planning deployment
Microsoft Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide	Contains information about how to plan, deploy, and manage the new Enterprise Voice capabilities in Office Communications Server 2007	Administrators and Telephony Engineers responsible for planning an IP telephony infrastructure and deploying Enterprise Voice

Guide	Contents	Primary audience
Microsoft Office Communicator 2007 Getting Started Guide	Contains information about how to get started with Office Communicator 2007	End-users and Administrators
Office Communicator 2007 Quick Reference Cards	Contains a summary of information for Office Communicator 2007	End-users and Administrators
Migrating to Microsoft Office Communications Server 2007	Contains information about migrating from LCS 2005 to OCS 2007	Administrators

Planning and engineering

This chapter contains information to consider before you implement Converged Office.

Navigation

Planning process

Before you install and configure Nortel Converged Office, you must consider the network size and the impact on the type of software and hardware required.

Nortel recommends that you implement the Telephony Gateway and Services component to provide basic connectivity (which you can more readily debug), followed by the Remote Call Control (RCC) for more complex feature operation. Configure both Telephony Gateway and Services and RCC only in situations where both components are required.

Consider the following during the planning process.

- Consider the size of your network. See “Network configuration” (page 50) for detailed information about determining your network architecture.
- Determine the type of users (internal and external users) and anticipated call traffic. For more information about type of users, see Table 7 "Maximum supported users for each topology" (page 66). For information about calculating the anticipated call traffic for the Communication Server 1000, see *Communication Server 1000E Planning and Engineering* (NN43041-220) .
- Determine that the software and hardware components required for the Communication Server 1000 are installed and have the most recent software versions. For more information, see “CS 1000 and Signaling Server installation” (page 124).
- Determine that the software and hardware components required for Office Communications Server (OCS) 2007 have the latest software versions. For more information, see “OCS 2007 component installation” (page 124).
- Determine the system requirements for the OC 2007 client. For more information, see “OC 2007 client requirements” (page 61).
- Determine capacity requirements for all components. For more information, see “Capacity planning” (page 60).
- Prepare your infrastructure.
- Plan for external user setup. For more information, see “Access Edge Server” (page 34).
- Plan your implementation strategy.

Microsoft Office Communications Server 2007 Planning Guide explains how to deploy OCS 2007. Download Microsoft documentation from the Download Center at www.microsoft.com.

Network configuration

The main consideration when you plan and engineer the Converged Office desktop is the size of the network. Networks are divided into three main categories: small, medium, and large. Each type requires specific configuration.

The following sections describe typical network topologies to assist in determining capacity and robustness requirements.

ATTENTION
The descriptions and graphical representations of the following three network types are for illustration only and are not actual configurations. The number of Communication Server 1000 systems and Office Communications Server 2007 servers required are based on the engineering guidelines in this document and those provided by Microsoft.

Small network

If you have a small, easily managed network, you can choose a basic configuration. Microsoft recommends the following configuration for small organizations that do not require high availability for OCS 2007.

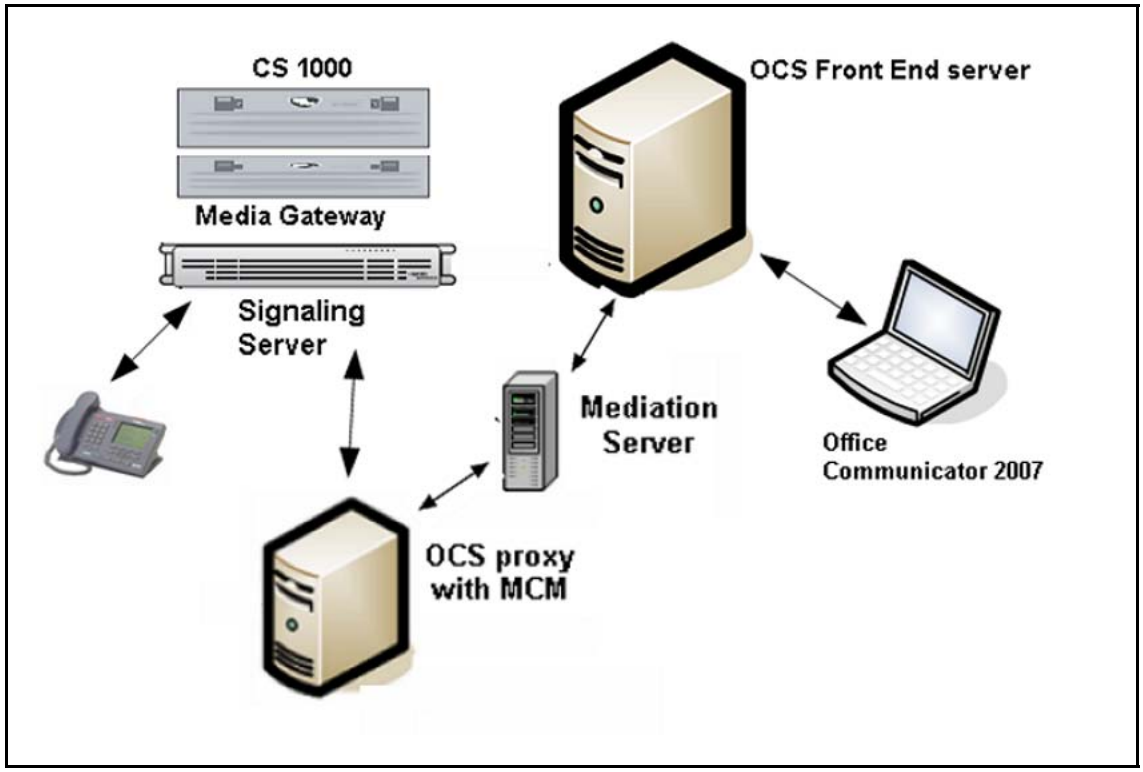
A small network can include the following components.

- a CS 1000 system with Media Gateway and Signaling Server
- support for IM and conferencing for internal users and can include external users
- up to 5 000 users

You need the following components.

- an Office Communications Server 2007 Standard Edition server
- a single Edge Server deployed in the perimeter network for external user access
- an OCS Proxy server that runs MCM 4.x
- a Mediation server

Figure 14
Small network configuration



Medium network

A medium network can include the following components.

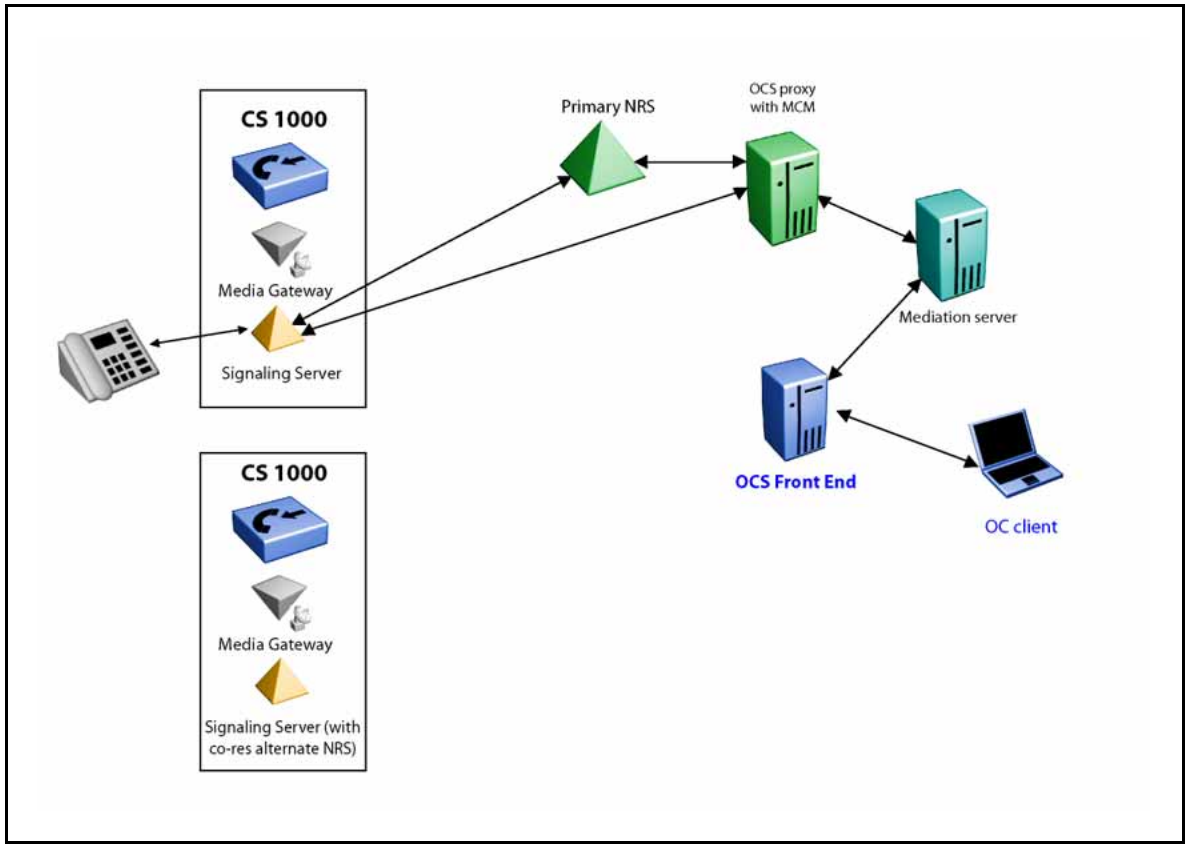
- one or multiple CS 1000 systems with Media Gateway and Signaling Server
- a Primary NRS with an Alternate Network Routing Service (NRS) that co-reside on one of the Signaling Servers
- up to 5 000 users
- high availability with system redundancy for OCS 2007

You need the following components.

- an Office Communications Server 2007 Enterprise Edition
- an OCS Proxy server that runs MCM 4.x
- one or multiple Mediation Servers (at least one Mediation Server for each CS 1000 SIP Gateway)

If you install only one OCS 2007 Enterprise Edition server, a Load Balancer is not required. SPS (Linux-based NRS) does not support co-residency.

Figure 15
Medium network configuration



Large network

A large network can include the following components.

- multiple CS 1000 systems with Media Gateway and Signaling Server
- configured collaborative NRS
- redundant Primary and Alternate NRS
- more than 5000 users
- high availability with system redundancy for OCS 2007

You need the following components.

- an OCS 2007 Enterprise Edition server with Load Balancers to Front End the pool of Enterprise Edition servers
- a redundant OCS Proxy servers that run MCM 4.x (the recommended deployment requires that MCM reside on a separate OCS Proxy server)

- Mediation servers (at least one Mediation Server for each CS 1000 SIP Gateway
- Load Balancers

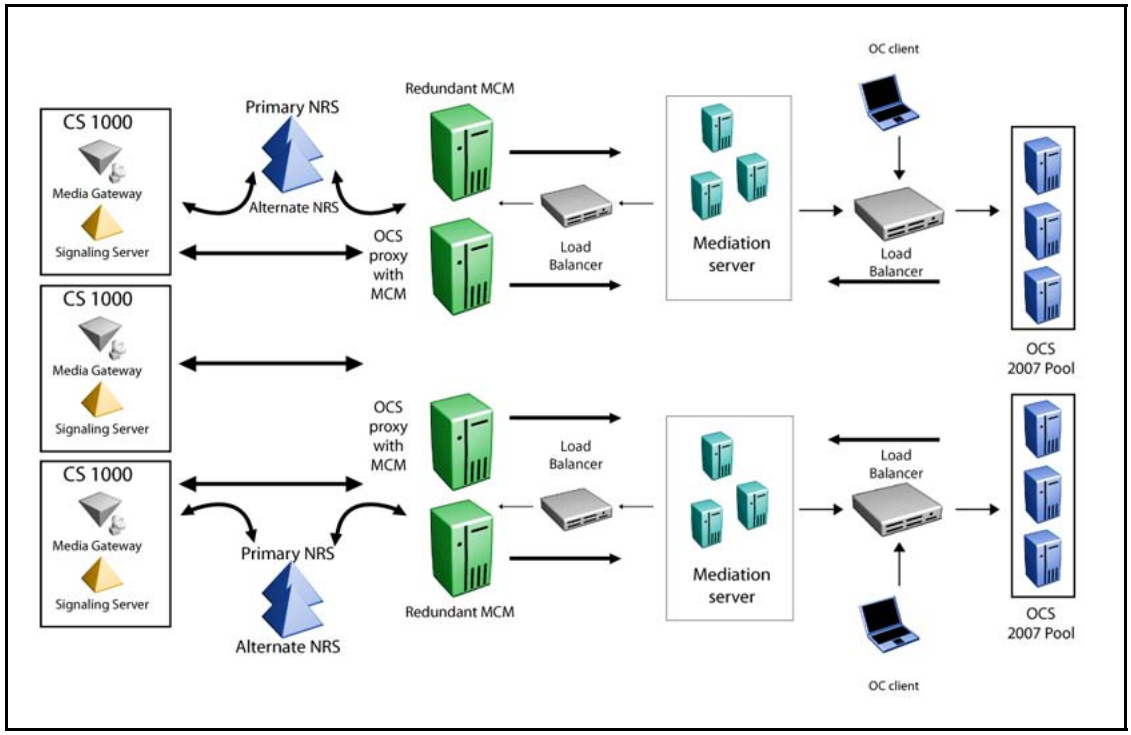
The redundant, primary, and alternate NRS can be either the VxWorks NRS or the Linux-based NRS (SPS/SRS). For the OCS 2007 Enterprise Edition server, a SQL back end database server is a requirement.

ATTENTION
If you set up more than one server that runs the Enterprise Edition of Microsoft Office Communications Server 2007, you must use a Load Balancer in accordance with the Unified Communications Engineering Rules and Guidelines.

The Load Balancer ensures that the Fully Qualified Domain Name (FQDN) of the pool is not equal to the FQDN of any Front End server in the pool.

The following figures shows a large network configuration.

Figure 16
Large network configuration



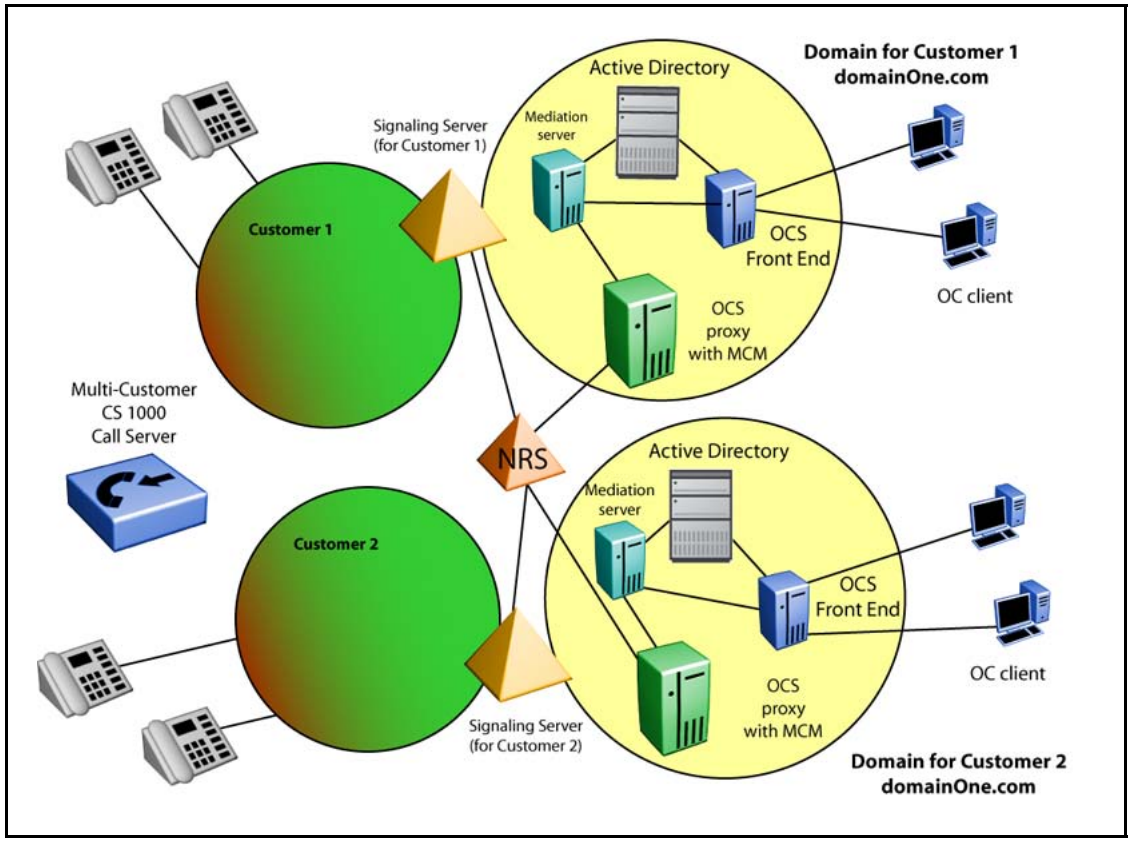
Multiple customer network

You can configure the Communication Server 1000 with a number of customers that have their own set of telephones, trunks, features, restrictions, and numbering plans. In the Converged Office environment, each customer is treated as a separate machine. Each customer shares one OCS deployment, but has their own Node Number, MCM,

Signaling Server, and SIP domain in the forest. For more information about the Multiple Customer environment, see *Features and Services* (NN43001-106).

Figure 17 "Multiple customer network" (page 55) provides an example of a multiple customer network. The figure shows two customers: Customer 1 (Ottawa) and Customer 2 (Belleville), each with their own set of associated phones and Signaling Servers. This type of configuration is required for any deployment that uses the Telephony Gateway and Services functionality, or in scenarios where both Telephony Gateway and Services and Remote Call Control functionality is deployed.

Figure 17
Multiple customer network



The Signaling Server for Customer 1 is in the domainOne.com domain. For each customer, you must configure a separate Office Communications Server domain. The Office Communications Server domain used by Customer 1 is in the same domain as the Signaling Server domainOne.com. Each OCS domain requires a separate Active Directory.

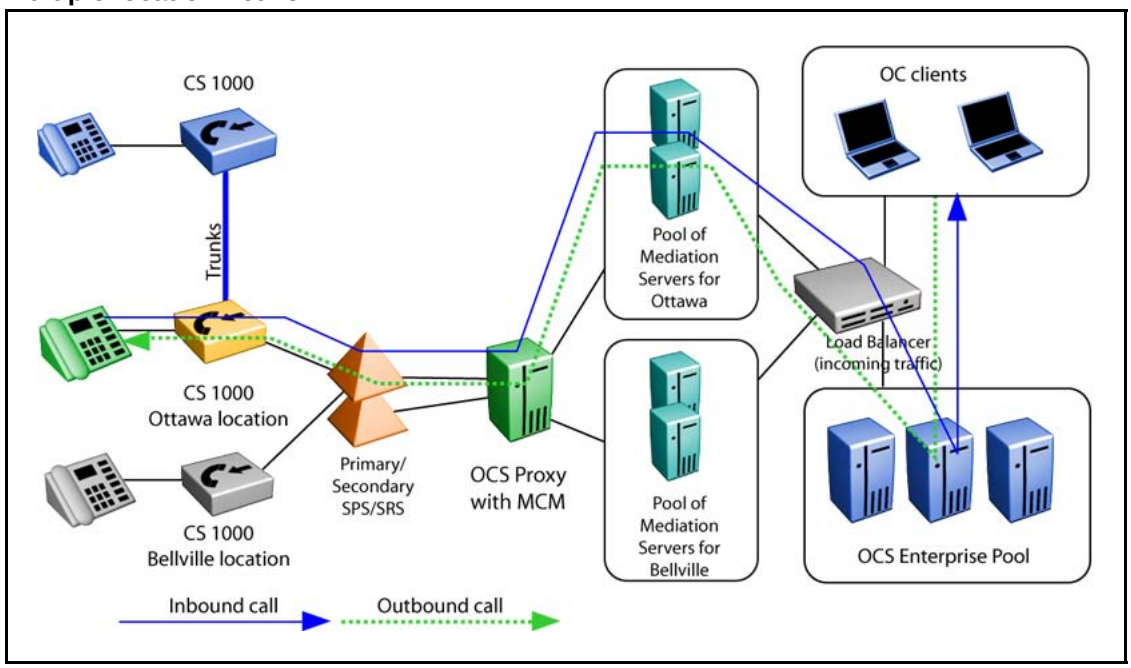
The only equipment that Customer 1 and Customer 2 share is the Communication Server 1000 and the NRS. The NRS can only be shared by the two customers if it is configured with both domainOne.com and domainTwo.com.

The Signaling Server, OCS Proxy server (which runs MCM), OCS 2007 Front End server, and Active Directory are separate. The number of Signaling Server(s), OCS 2007 Proxies, and OCS 2007 Front End servers required for each customer are the same as if each customer were part of a single system. However, the number of users allowed for the Communication Server 1000 is the number of users for all customers.

Multiple location network

The following diagram shows the path of an inbound and outbound call in a multiple location network configuration in a single forest deployment. The MCM routes inbound calls from the Signaling Server to the appropriate Mediation Server within the Mediation Server pool. When the current Mediation Server does not answer, MCM jumps to the next Mediation Server.

Figure 18
Multiple location network



For regional or multiple location deployments, you must install SPS/SRS. Two Primary/Secondary SPS/SRS may co-exist within one configuration to improve system robustness. In the previous versions of the program, the MCM performs polling by sending SIP OPTION request to determine which SPS/SRS is active. The active SPS/SRS becomes the last one to send an OK response. The SIP Proxy Server (SPS) sits between MCM and the

TR/87 FE application that reside on Communication Server 1000. This SIP proxy allows communication between the Communication Server 1000 and OCS when different transport protocols (TLS and TCP) are used.

Load Balancer planning

This section provides information about the Load Balancer requirements.

Navigation

- "Load Balancer prerequisites" (page 57)
- "Load Balancer requirements" (page 58)
- "Redundancy with Load Balancers" (page 59)
- "High-scale and high availability configuration" (page 59)
- "Nortel Application Switch" (page 60)

Load Balancer prerequisites

- Before you configure a Load Balancer to connect to the Office Communications Server Enterprise pool, ensure you configure the following:
  - The Load Balancer must meet the Microsoft criteria for a Load Balancer. See "Load Balancer requirements" (page 58)
  - Configure a static IP address for servers within your pool.
  - For each server within the pool a certificate, include for both user and server authentication issued by a certification authority in the pool's local domain.
  - Configure a VIP address and a DNS record for the load balancer.
  - Test users created and SIP-enabled in the pool.
  - Install root certificate from CA in the domain (or trusted CA) on client computers.
  - Log on to all servers in the pool using TLS to ensure server and client certificates work.
  - Configure Port 135 on Load Balancers to enable server-side block and give functionality for users and move user scenarios to pools through DCOM. For example, perform remote DCOM-based database operations. Nortel recommends the minimum configuration, as shown in the following table.
  - Optionally, configure the TCP pool on port 5060 for clients to connect to the Load balancer through TCP.

Table 5
Load balancer minimum configuration

Service	Protocol	Port (range)	Description
TLS pool	TCP	5061	The client listens over the same connection that is open to the server. By default, the server listens on port 5061 (TCP). The server sends packets to the client only over the client TLS session.
DCOM	TCP	135	Installation and management.

Load Balancer requirements

A Load Balancer for the Office Communications Server (OCS) Enterprise pool must meet the following requirements:

- The Load Balancer must expose a VIP Address through Address Resolution Protocol (ARP).
- The VIP must have a single DNS entry, called the pool FQDN.
- The VIP must be a static IP address.
- The Load Balancer must allow multiple open ports on the same VIP. Specifically, it must expose the ports 5060, 5061, 135, 80, 443, and 444.
- The Load Balancer must provide TCP-level affinity. This means that the Load Balancer must ensure that it can establish TCP connections with one Office Communications Server in the pool and all traffic on that connection is destined for that same Office Communications Server.
- The Load Balancer must provide a configurable TCP idle-timeout interval with a maximum value greater than or equal to the minimum of the REGISTER refresh or SIP Keep-Alive interval.
- The Load Balancer must support a rich set of metrics (round-robin, least connections, and weighted). Nortel recommends a weighted least connections-based load balancing mechanism for the Load Balancer. This means that the load balancer ranks all Office Communications Servers based on the weight assigned to them and the number of outstanding connections. The Load Balancer use the rank to pick the Office Communications Server to use for the next connection request.
- The Load Balancer must detect Office Communications Server availability by establishing TCP connections to ports 5060, 5061, or both (often called a heartbeat or monitor). The polling interval must be a configurable value with a minimum value of at least 5 seconds. The load balancer must not select an Office Communications Server

that shuts down until it can establish a successful TCP connection (heartbeat) again.

- Every Office Communications Server must have exactly one network adapter. Multihoming an Office Communications Server is not supported. If a 10/100 network adapter does not meet the required bandwidth constraints, a gigabit network adapter must be used.
- The network adapter must have at least one static IP address. This IP address will be used for the incoming load-balanced traffic.
- The computer must have a registered FQDN. The IP address registered for this FQDN must be publicly accessible from within the enterprise.
- The Load Balancer must include less than one gigabit capacity for up to 50 000 concurrent client connections. One gigabit of capacity is required to support more than 50 000 concurrent client connections.

For more information about Load Balancer requirements, see *Microsoft Office Communications Server 2007 Document: Planning Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Redundancy with Load Balancers

You can add redundancy to your network by placing Load Balancers, such as a Nortel Application Switch, for the OCS 2007 Front End servers, and for the OCS 2007 Proxy servers (MCM pool).

The Load Balancer of the MCM pool balances SIP invites from the Mediation Server to the OCS Proxy server (for VoIP mode). The Mediation Server sends all SIP invites to the Virtual IP of this Load Balancer. The Load Balancer then sends the SIP Invite to the least busy Office Communications Server 2007 OCS Proxy. Redundancy is also ensured for calls to an Office Communicator user from the Communication Server 1000 by having a Load Balancer for multiple OCS Proxy servers (MCM pool).

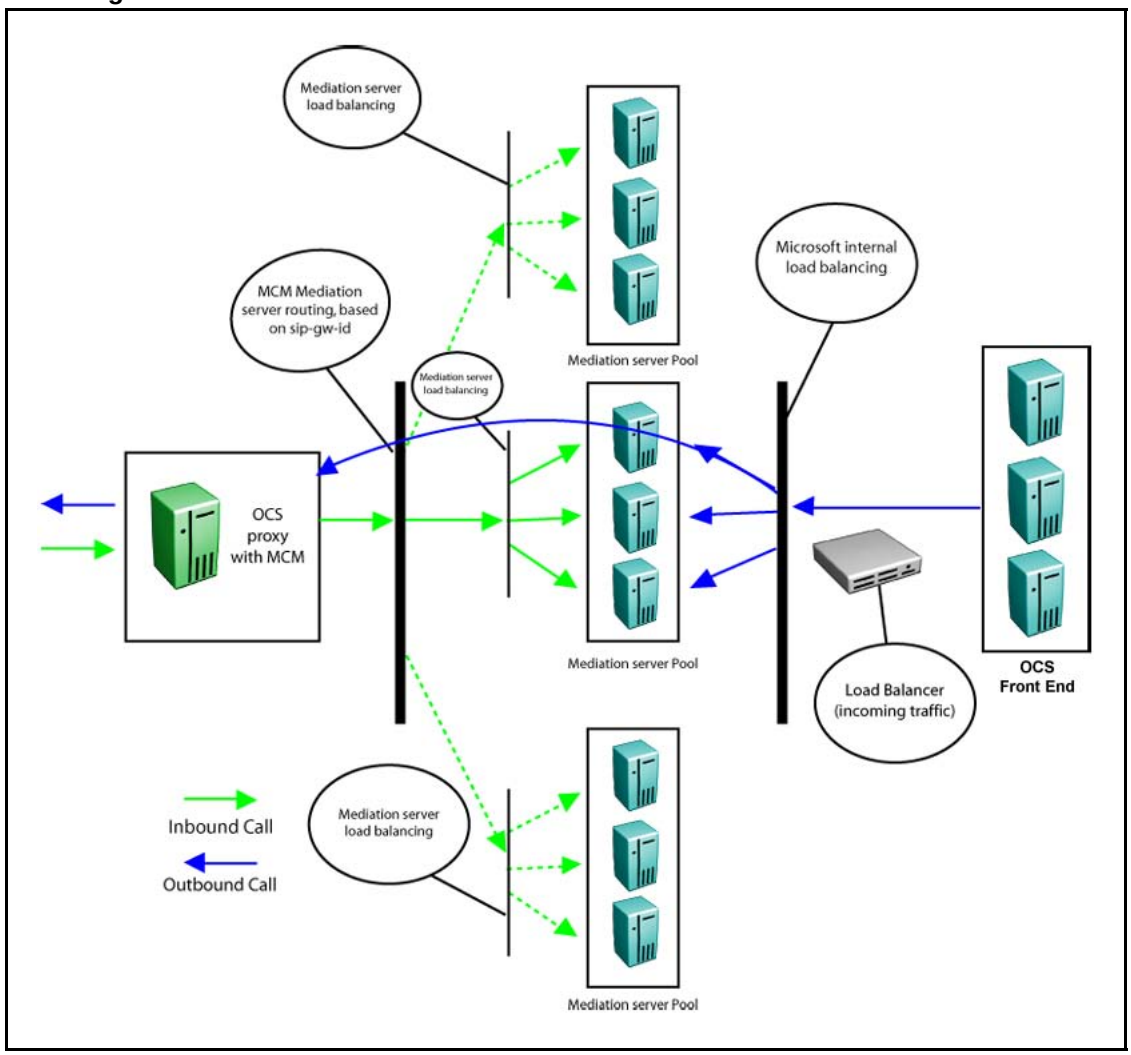
The Load Balancer of the OCS 2007 Front End servers balances SIP invites from the Mediation Server (for VoIP mode) to the least busy Front End server. This is the same load balancer that is used when the Office Communicator addresses the pool for registration. The incoming load balancer balances the incoming traffic to the Front End servers. See Figure 19 "Incoming Load Balancer" (page 60) for an example.

High-scale and high availability configuration

The pool of Front End servers processes inbound and outbound traffic. In this example, the Load Balancer routes incoming SIP messages to the less busy server based on a configured algorithm. The Load Balancer VIP

address is used by clients as a single point of connection to the pool. This address is listed in DNS and has an FQDN. Internal OCS clients require the DNS server to establish a connection with the Enterprise Edition Pool.

Figure 19
Incoming Load Balancer



Nortel Application Switch

Nortel recommends that you use the Nortel Application Switch (NAS) for Load Balancing. For more information, see *Load Balancing Microsoft Office Communication Server 2007 in an Expanded Topology for Application Switch Technical Configuration Guide* (NN48500-561). This document is available on the Nortel Web site at www.nortel.com.

Capacity planning

This section provides information about the capacity requirements.

Navigation

OC 2007 client requirements

The PC that runs the OC 2007 must be registered to the domain in which the OCS 2007 server runs. The OC 2007 client can be installed on a PC that runs most versions of Microsoft Windows with the hardware device driver API DirectX 9 or later. For more information about the OC client requirements, see Table 13 "Office Communicator client requirements" (page 68).

For more information about deploying the OC client, see *Microsoft Office Communicator 2007 Deployment Guide* . Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Load Balancer capacity requirements

Capacity planning for OCS 2007 is measured in terms of the number of clients. However, this becomes difficult to measure because of the enhanced capabilities and services for a pool and the variety of components that can be enabled in OCS 2007. Components can reside on separate servers, which adds to the complexity of capacity planning. A single client user can have multiple connection instances that depend on the features enabled. Each feature has different bandwidth requirements that can differ from one enterprise to another.

For more information about capacity guidelines, see Table 7 "Maximum supported users for each topology" (page 66).

For more information about capacity planning, see the *Microsoft Office Communications Server 2007 Planning Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

SIP CTI (TR/87) services requirements

When you plan for capacity with Session Initiation Protocol Computer Telephony Integration (SIP CTI) services, observe the following restriction: For a single Communication Server 1000 that supports multiple nodes,

(each with SIP CTI services enabled), you can establish multiple SIP CTI (TR/87) sessions for a DN through the same node—but not through different nodes.

To illustrate this, consider the following high-level example:

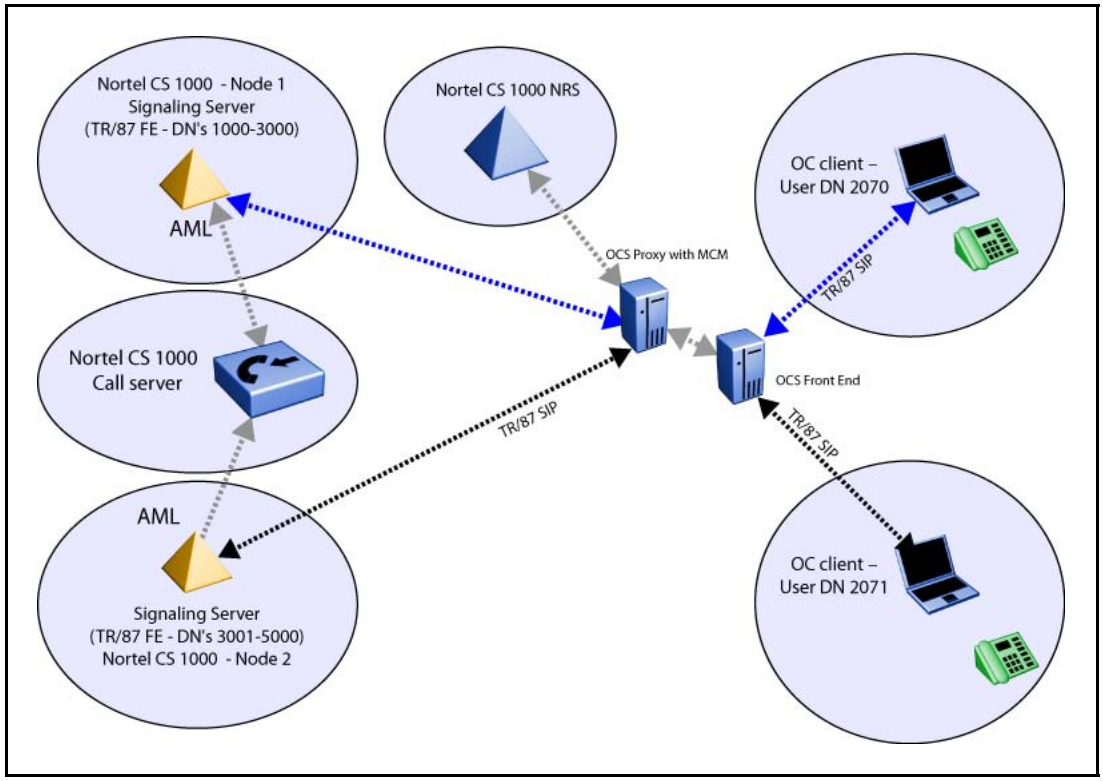
Client A sends a TR/87 SIP INVITE to Node 1 to monitor DN 1000. The TR/87 association is established. Client B then sends a TR/87 SIP INVITE to Node 1 (the same node) to monitor DN 1000. Both sessions are established successfully. As a result of this sequence, two TR/87 sessions exist for DN 1000 through Node 1.

However, if Client B attempts to send a TR/87 SIP INVITE to Node 2 (which has an AML link to the same call server as Node 1), the attempt to establish the TR/87 session fails because the DN is already in use by Client A session through Node 1.

To solve this issue when you plan for capacity, SIP routing must ensure that all TR/87 sessions for a DN always terminate on the same node when there are multiple nodes for a single Communication Server 1000 call server, as depicted in Figure 20 "SIP CTI (TR/87) example" (page 63).

This issue can arise in cases where a single user has multiple clients logged on simultaneously (for example, a client at home, a client in the office, and a mobile client; each with TR/87 capability).

Figure 20
SIP CTI (TR/87) example



Mediation server requirements

The Communication Server 1000 can process up to 13 000 simultaneous calls. Therefore, you may require several Mediation servers for one Communication Server 1000. To correctly deploy OCS 2007 to interwork with the Communication Server 1000, you must correctly engineer the network to handle the anticipated call traffic. Calculate the anticipated call traffic for the Communication Server 1000 using the instructions in *Communication Server 1000E Planning and Engineering* (NN43041-220). For more information about hardware requirements, see Table 9 "Mediation Server hardware requirements" (page 67).

Signaling Server requirements

The maximum number of SIP CTI (TR/87) users on a single Signaling Server is 5000. One Signaling server can support up to 1800 SIP trunks; therefore, you require up to two Mediation servers for a single Signaling Server. To increase the system capacity, associate a pool of Mediation Servers with each Call Server. MCM routes inbound calls from the Signaling Server to the appropriate Mediation Server within the Mediation Server pool.

For example, MCM works as a software load balancer in addition to a router. MCM uses a round-robin algorithm for load balancing. When the current Mediation Server does not answer, MCM jumps to the next Mediation Server. You can use load balancing for direct mode and with SPS or SRS.

For Release 5.0 or later, 1 GB of memory is required for a standard Signaling Server. All signaling servers must run the most recent software version. For information about geographic redundancy, see "Geographic redundancy" (page 95).

Call Server requirements

The Communication Server 1000 must run Release 6.0.

For various CPUs, the number of supported users are as follows.

- CP PII: 7 000 users
- CP PIV: 13 000 users
- CP PM: 13 000 users

OCS Proxy and MCM capacity requirements

The MCM must reside on a separate OCS Proxy server and the capacity of the OCS Proxy server with MCM depends on the hardware platform and the usage. For example, VoIP calls only, SIP CTI calls only or a combination of both. Because capacity characterization cannot be conducted on all server platforms, Nortel recommends that you use standardized sets of relevant benchmarks available from the Standard Performance Evaluation Corporation (SPEC). SPEC is a nonprofit corporation formed to establish, maintain, and endorse benchmarks that can be applied to the newest generation of high-performance computers. A compressive list of benchmarks is available at www.spec.org.

The server used for capacity characterization had a SPECint_rate2000 value of 18.6. See Table 6 "Maximum call rate" (page 64) for the maximum call rate of this server for the three configurations.

Table 6
Maximum call rate

Usage	Maximum call rate
VoIP calls	15 000
SIP CTI (TR/87) calls	10 000
Combined	12 500*
* Depends on the ratio of either call scenarios assumed 50% of each. For example: Worst case–all SIP CTI calls, Best case–all VoIP calls.	

The number of users the OCS Proxy server with MCM can handle depends on the usage and the number of calls per hour per user. For example, assuming 5 cph/user for VoIP calls would give 3000 users (15 000 cph/5 cph/user = 3000 users).

The following are the formulas (based on SPECint_rate2000) to calculate the maximum call rate for different platforms:

- VoIP calls only. Number of calls per hour supported = (15 000 x SPECint of HW) / 29.8.
- SIP CTI (TR/87) RCC calls only. Number of calls per hour supported = (10000 x SPECint of HW) / 29.8.
- Both VoIP and SIP CTI (TR/87) RCC calls combined. Number of calls per hour supported = [(15 000 x SPECint of HW) x (VoIP_call%) + (10 000 x SPECint of HW) x (SIPCTI_call%)]/ 29.8.

ATTENTION
VoIP_call% or SIPCTI_call% must be less then 100%.

ATTENTION
An OCS Proxy is not an Access Proxy. For more information about OCS proxy hardware requirements, see Table 10 "OCS Proxy server hardware requirements" (page 67).

General requirements

This section provides general guidelines and requirements to follow when you deploy the Office Communications Server 2007.

Navigation

- “Authorization of TR/87 (Remote Call Control) service requests” (page 73)
- “Signaling and media encryption” (page 73)
- “Dialing plan considerations” (page 75)
- “Computer (SIP) Calls” (page 75)
- “Phone (RCC or TR/87) Calls” (page 76)
- “Number formats supported by Office Communicator” (page 77)
- “E.164 international format numbers for SIP Gateway and SIP CTI” (page 80)

Server topology

Use the following table to determine the maximum supported users for your topology.

Table 7
Maximum supported users for each topology

Topology	Servers required	Maximum clients
Standard Edition Server	1 Standard Edition server, (Optional) Archiving Server collocated	5000
Enterprise pool: Consolidated Configuration	4 Enterprise Edition Front End servers running all server roles, 1 back end SQL server (Optional), 1 Archiving server	4 servers X 5000 users per server = 25 000 maximum clients
Enterprise pool: Expanded configuration with Mid-Range Performance SQL back end	4 Front End servers, 2 Web Conferencing servers, 2 A/V Conferencing servers, 2 IIS servers, 1 back end SQL server (Optional), 1 Archiving server	10 000 users per access edge server and 50 000 maximum clients
Enterprise pool: Expanded configuration With High Performance SQL back end	8 Front End servers, 4 Web Conferencing servers, 4 A/V Conferencing servers, 2 IIS servers, 1 back end SQL server (Optional), 2 Archiving servers	125 000

Operating System Requirements

The operating system platform requirements for all Office Communications Server 2007 server roles are as follows.

- Minimum: Microsoft Windows Server 2003 SP1.
- Recommended: Windows Server 2003 R2 with SP2.

Hardware Requirements

Use the following table to determine hardware requirements for the OCS 2007 Standard and Enterprise Edition server.

Table 8
Office Communications Server 2007 Standard and Enterprise Edition hardware requirements

Hardware	Requirements
CPU	Dual processor, dual core 2.6 GHz +
Disk	2 x 18 GB For collocated Standard Edition Server, add: 2 x 36 GB, 15K RPM, RAID 0, for database log files 2 x 36 GB, 15K RPM, RAID 0, for database data
Cache	1 MB L2 per core
Memory	2 GB (4 GB for Standard Edition server or Consolidated Enterprise Edition server)
Network	Gbit NIC

Table 9
Mediation Server hardware requirements

Hardware
Single processor, dual core, 2 GHz, Memory: 2 GB RAM 2 x 1 Gbit NIC
Single processor, dual core, 3 GHz Memory: 2 GB RAM 2 x 1 Gbit NIC
Dual processor, dual core, 3 GHz Memory: 2 GB RAM 2 x 1 Gbit NIC
Dual processor, quad core, 2.66 GHz, Memory: 2 GB RAM 2 x 1 Gbit NIC

Table 10
OCS Proxy server hardware requirements

CPU	Dual processor, dual core 2.6 GHz +
Disk	2 x 18 GB
Cache	1 MB L2 per core
Memory	2 GB
Network	Gbit NIC

Table 11
Back end database for a small to medium Enterprise pool

CPU	Dual processor, dual-core 2.6 GHz +
Disk	Drive 1 (2 × 18 GB) for OS and Page File Drive 2 (36 GB, 15K RPM) for database log file Drive 3 (36 GB, 15K RPM) for database log file Drive 4 (8 x 36 GB, 15K RPM, RAID 0+1) for database files
Cache	2 MB L2 for each core
Memory	8 GB
Network	Gbit NIC

Table 12
Back end database for a large Enterprise pool

CPU	Quad processor, dual-core 2.6 GHz +
Disk	Drive 1 (2 × 18 GB) for OS and Page File Drive 2 (4 x 36 GB, 15 000 RPM, RAID 0+1) for database log file Drive 3 (4 x 36 GB, 15 000 RPM, RAID 0+1) for database log file Drive 4 (8 x 36 GB, 15 000 RPM, RAID 0+1) for database files
Cache	2 MB L2 for each core
Memory	16 GB
Network	Gbit NIC

Table 13
Office Communicator client requirements

Operating System	• Windows Vista 32-bit (RTM) operating system • Microsoft Windows XP Professional with Service Pack 2 • Windows 2000 Professional with Service Pack 4 (requires Microsoft Windows Media technologies player, version 9, and Microsoft Windows Installer, version 3.0 or most recent) Hardware device driver must be API DirectX 9 or most recent.
Computer/Processor	• Data and Voice: 500-megahertz (MHz) or most recent processor. Intel Pentium-compatible • For video: 1 GHz or most recent
Memory	512 megabytes (MB) of RAM
Install Space	1.5 MB

Virtual Server 2005

Microsoft Virtual Server 2005 is not supported as part of the Nortel Converged Office feature. The Nortel software component Multimedia Convergence Manager (MCM) must not be installed on Office Commu

nications Server that runs Microsoft Virtual Server 2005. For additional information about Virtual Server 2005, see the Virtual Server Web site at www.microsoft.com/windowsserversystem/virtualserver/default.mspx.

Storage

Store internal hard disks used for operating system and executable software, data, and transaction files separately. The following lists shows storage options:

- Direct access storage device (DASD)
- Storage Area Network (SAN)
- Redundant Array of Independent Disks (RAID)

Onboard storage:

- 2 SCSI Channels (split backplane)
- Five 18 GB hard disks, 15 000 RPM SCSI disk drives

Optional SAN:

- One Fibre Channel Host Bus Adapter (HBA)
- SAN unit

Trunks

To handle the traffic between the Communication Server 1000 and the Office Communications Server 2007, you must configure sufficient SIP trunks and UEXTs. The number of additional SIP trunks needed is determined by:

Determine the number of SIP trunks required by multiplying the number of OC 2007 clients that use the SIP Gateway feature by the percentage of users you expect to be on the phone at any time.

For example, 100 Office Communicator SIP Gateway users x 10% on the phone at a time = 10 additional SIP trunks.

The percentage of users on the phone is decided by standard practice and the environment involved (For example, Call Center or Normal Office).

TLSV has replaced Personal Call Assistant (PCA). TLSV is used to extend the call over a SIP trunk to the OCS client from the Communication Server 1000 system.

SIP access port

Table 14 "Inputs" (page 70) defines the inputs used to calculate SIP access ports and TLSV requirements.

Table 14
Inputs

Input	Description
TN_MO_Users	Total number of Office Communicator users that use the SIP Access Ports for voice services.
UEXT_MO_Users	Number of Office Communicator users that use Universal Extension (UEXT) with Telephony Services (TLSV) subtype. The UEXTs required here are additional to the number of UEXTs provided in the Enterprise Configurator (EC) tool Software screen.
P_UEXT_SIP	Percentage of UEXT calls that use the soft client to answer a call.

Calculations

Use the following formulas to calculate traffic requirements (MO indicates Microsoft Office Communicator):

- Traffic for UEXTs = (UEXT_MO_Users) x (CCS per user) x (1 – P_UEXT_SIP) x 10%
- Traffic for SIP ports = (TN_MO_Users – UEXT_MO_Users) x (CCS per user) + (UEXT_MO_Users x P_UEXT_SIP) x (CCS per user)
- Total SIP Traffic = (Traffic for UEXTs) + (Traffic for SIP ports)
- Number of MO SIP ports = Poisson (Total SIP Traffic) at P.01 Grade of Service

Table 15 "Traffic figures" (page 70) shows traffic in CCS and number of ports calculated based on the Poisson formula at P.01 Grade of Service.

Table 15
Traffic figures

Traffic (CCS)	Traffic (Erlang)	Number of ports
5	0.14	2
10	0.28	3
15	0.42	3
20	0.56	4
25	0.69	4
30	0.83	4
35	0.97	5
40	1.11	5
45	1.25	5
50	1.39	6
55	1.53	6

Table 15
Traffic figures (cont'd.)

Traffic (CCS)	Traffic (Erlang)	Number of ports
60	1.67	6
65	1.81	6
70	1.94	7
75	2.08	7
80	2.22	7
85	2.36	7
90	2.5	8
95	2.64	8
100	2.78	8
125	3.47	9
150	4.17	10
175	4.86	12
200	5.56	13
225	6.25	14
250	6.94	15
275	7.64	16
300	8.33	17
325	9.03	18
350	9.72	19
375	10.42	19
400	11.11	20
425	11.81	21
450	12.5	22
475	13.19	23
500	13.89	24
550	15.28	26
600	16.67	28
650	18.06	29
700	19.44	31
750	20.83	33
800	22.22	35
850	23.61	36
900	25	38

Table 15
Traffic figures (cont'd.)

Traffic (CCS)	Traffic (Erlang)	Number of ports
950	26.39	40
1000	27.78	42
1500	41.67	58
2000	55.56	74
2500	69.44	90
3000	83.33	106
3500	97.22	121
4000	111.11	137
4500	125	152
5000	138.89	168
6000	166.67	198
7000	194.44	228
8000	222.22	258
9000	250	288
10 000	277.78	318
20 000	555.56	611
30 000	833.33	908
40 000	1111.11	1205
50 000	1388.89	1502
60 000	1666.67	1799
70 000	1944.44	2096

Basic Client Configuration

Basic Client Configuration (BCC) can program the new TLSV subtype for UEXT TNs. The TLSV subtype is the required value for all UEXTs associated with OCS 2007.

LD 11 supports the administration of telephones. BCC uses REQ commands, such as NEW, CHG, and OUT. In LD 20, BCC uses the PRT command to retrieve phones from the Call Server.

Port use

The Communication Server 1000 uses the following ports related to TCP and TLS.

- 5060: TCP
- 5061: TLS

The dynamic port range used by Office Communicator for SIP/RTP is 1024 – 65535.

The port range can be controlled (restricted) to a smaller range using the group policy settings. For more information, see the Help and Support home page on the Microsoft Web site at www.microsoft.com.

Port ranges must not overlap.

Security

When you consider a Converged Office deployment, ensure you understand the following security concepts and integrate them into your deployment planning.

OC client authentication

Authentication of Office Communicator clients is provided by the Office Communications Server. For more information about authentication, see *Microsoft Office Communications Server 2007 Planning Guide* . Download Microsoft documentation from the Download Center at www.microsoft.com.

Authorization of TR/87 (Remote Call Control) service requests

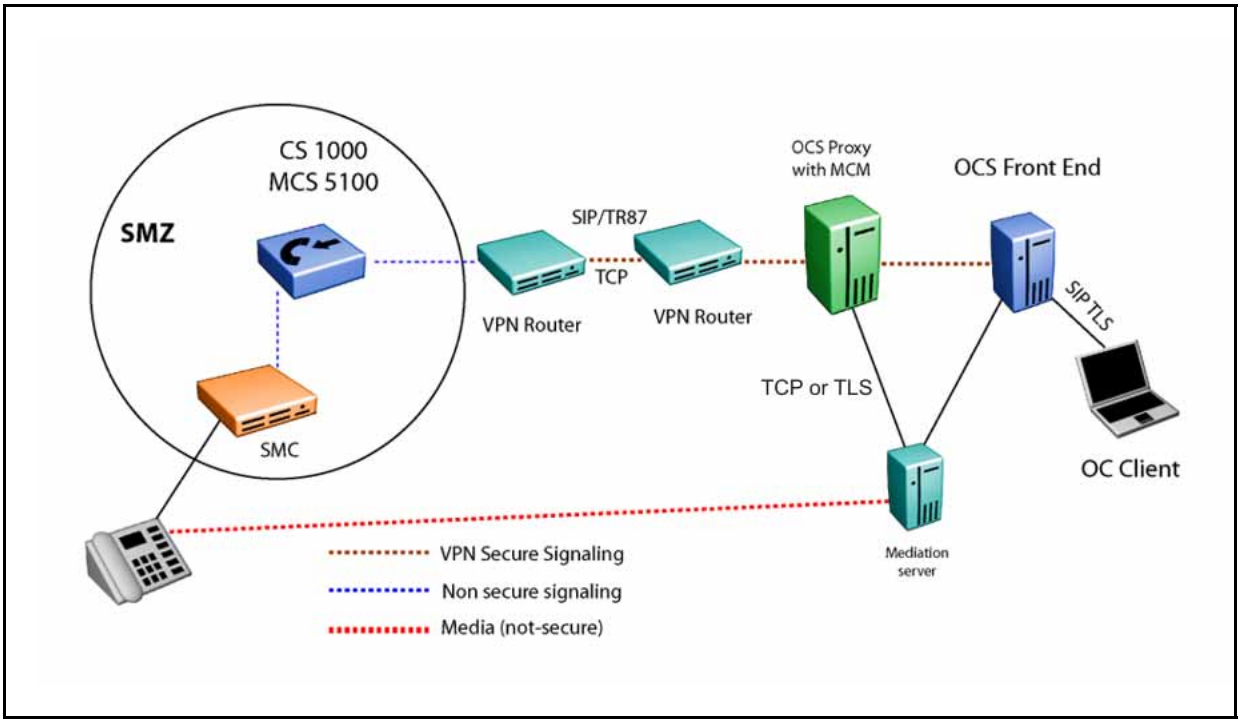
Authorization of TR/87 (Remote Call Control) service requests within a Converged Office deployment is handled by the Nortel MCM. The main requirement for authorization of service requests arises from Office Communicator users who can manually override the Phone Integration settings in Active Directory provisioned by an administrator. To ensure that each Office Communications Server user is restricted to the Active Directory configuration provisioned by an administrator for Remote Call Control, MCM provides an option to enable or disable authorization of TR/87 service requests. For details about the authorization process and MCM configuration requirements, see “MCM for Remote Call Control” (page 182) .

Signaling and media encryption

IP connectivity between the Office Communications Server and the Communication Server 1000 is provided by TCP and TLS. Similarly, Office Communications Server server-to-server traffic can also be TCP or TLS.

To provide signaling security between the Office Communications Server and the Communication Server 1000 (see Figure 21 "Signaling security" (page 74)), Nortel Contivity VPN routers can be used to tunnel SIP signaling between the Office Communications Server and the Communication Server 1000. A single VPN router that supports the Office Communications Server can service multiple individual VPN routers from multiple Communication Server 1000 deployments.

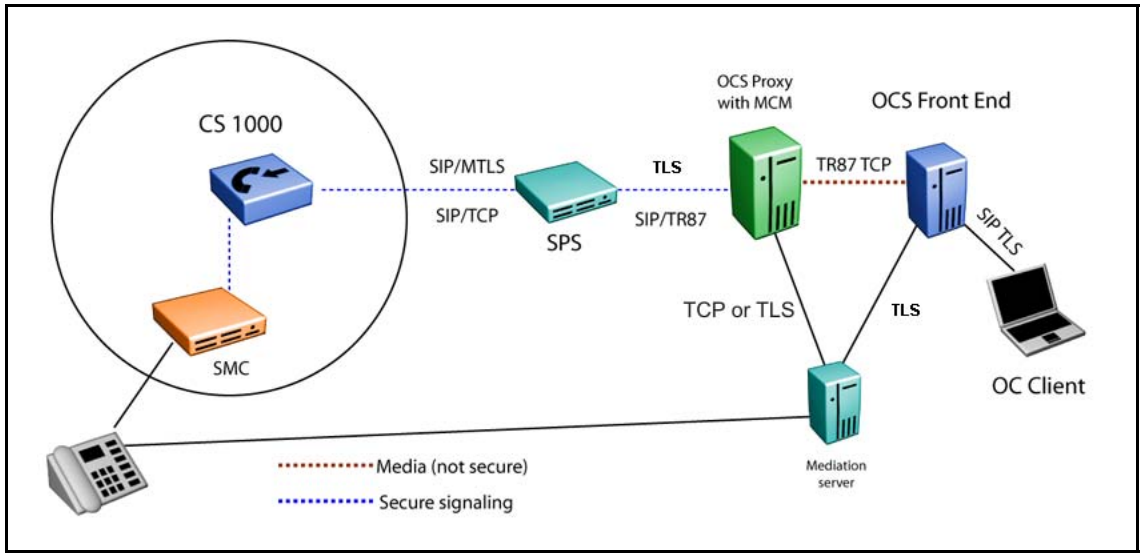
Figure 21
Signaling security



- Secure Management Zone (SMZ) provides management access to local and remote devices over a secure connection. SMZ documents the LAN and WAN configurations required for secure management.
- Virtual Private Network (VPN) enables secure communications through Secure Internet Protocol (IPSec) encryption.
- Transport Layer Security (TLS) ensures that third parties cannot eavesdrop or tamper with messages when a server and client communicate. On the SIP Gateway, TLS supports a certificate chain with a maximum length of five. A configured DNS server is required to support FQDN verification on the SIP Gateway and SIP Proxy Server (SPS).

Secure end-to-end policy is not supported with this application.

Figure 22
Signaling security with TLS



Dialing plan considerations

Nortel Converged Office is comprised of the following two components:

- SIP CTI Services provides CS 1000 native TR/87 support to enable the Remote Call Control functionality available with Office Communicator.
- Telephony Gateway and Services provides the ability to originate and receive SIP calls (for example, VoIP and Computer calls) from Office Communicator.

Whether you choose one or both components for deployment, an Office Communicator is essential. This allows the existing dial plan (that users have become accustomed to with their existing telephony interfaces) to extend seamlessly to the Office Communicator client for either call type. This includes all existing CS 1000 dialing plan features such as Coordinated Dial Plan (CDP) and Uniform Dial Plan (UDP), and Group Dial Plan.

The following lists summarize the features that contribute to the dialing plan configuration for the Converged Office feature from the perspective of calls originated and received from Office Communicator.

Computer (SIP) Calls

- Number format entered in Active Directory or Office Communicator
- Office Communications Server Address Book Service Normalization rules
- Network Redirect Service (NRS)

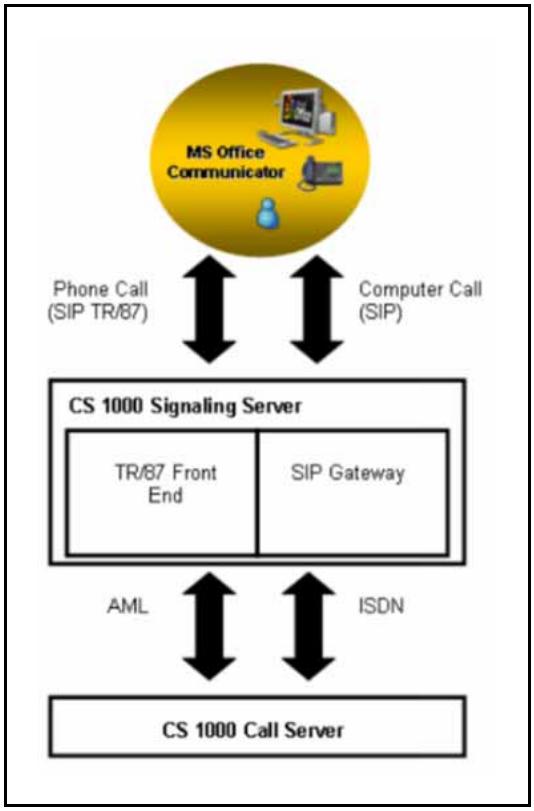
- CS 1000 SIP Gateway configuration
- CS 1000 Call Server configuration relating to the SIP Gateway
- OCS Location Profile, Policy, Phone Usage, and Route configuration.
- OC client configuration in the Active Directory

Phone (RCC or TR/87) Calls

- The format of the number itself entered in Active Directory or entered in Office Communicator
- Office Communications Server Address Book Service Normalization rules
- CS 1000 SIP CTI Services Configuration
- CS 1000 Call Server Configuration relating to PBX telephones
- OC Client configuration in the Active Directory

The number format and normalization support provided by Office Communications Server is used to format numbers for both Remote Call Control and computer calls. However, the interface from which they originate and receive calls from the Communication Server 1000 is the TR/87 Front End and SIP Gateway respectively (as illustrated in Figure 23 "Signaling and media paths" (page 77)).

Figure 23
Signaling and media paths



Number formats supported by Office Communicator

Dialstrings and E.164 International number format are the two types of numbers used by Office Communicator. Both number formats apply to computer and phone calls with Office Communicator.

Dialstrings

By default, digits dialed from Office Communicator that are not fully qualified are sent as dialstrings. The sequence of digits entered in Office Communicator are sent directly to the Call Server to be dialed. This allows a user to dial all numbers that you typically expect to dial from a phone local to the Communication Server 1000. Normalization rules should be defined in the Location Profile to convert the dialstrings to the E.164 International format for all types of PSTN calls. For example, NXX, NPA and International.

E.164 International Format Numbers

The recommended format of numbers stored in Microsoft applications is the E.164 International number format. This is a variable length number that consists of a plus sign (+) followed by a 1 to 3 digit country code and a national number 15 to n digits in length—where n is the length of the country code.

All E.164 numbers presented to the CS 1000, computer, or phone are expected in the following format:

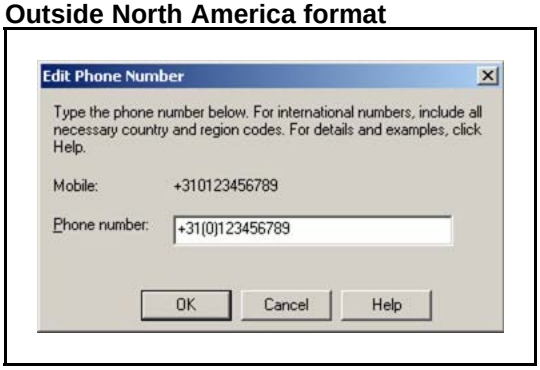
+<country code><national number>

For example, in North America, the Office Communicator Phone Number configuration input dialog box has an entry similar to Figure 24 "North American format" (page 78).

Figure 24
North American format

Outside North America, the Office Communicator Phone Number configuration input dialog box has an entry similar to Figure 25 "Outside North America format" (page 78).

Figure 25
Outside North America format



You can use the Normalization feature, provided by the Office Communications Server Address Book Service, to ensure that formats used within a local deployment that do not conform to the convention can be converted without changing the original numbers.

For example, in the Netherlands, numbers in Active Directory can be entered in the following format: +31(0)123456789

You can use a normalization rule to strip the digit in brackets to conform to the expected format for E.164 numbers when using the Converged Office feature: +31123456789

For more information about Normalization rules, see “Creating Normalization rules” (page 246).

Handling numbers called from Office Communicator in E.164 format requires that you configure the Call Server to ensure that the number requested is within the defined dialing plans:

For calls from the Call Server to the Office Communicator (OC) client, the usual mechanism is used; the ZBD requires no specific configuration.

x-nt-ocn-id identifies the user in OCS. Each user with a private unique CDP/UDP number maps to an E.164 number on the Active Directory. For every incoming call, the MCM maps the private numbering plan to an E.164 number in the SIP message sent to the OC client. The Communication Server 1000 modifies the calling, called, or redirected numbers to CDP/UDP format for MCM to perform the E.164 lookup. All users on OCS 2007 are identified with a unique E.164 number. This applies for SIP Gateway services and Remote Call Control (RCC).

For calls to the OC client, the Network Routing Service (NRS) routes a call from the Call Server to the appropriate OCS Proxy server with MCM, which defines the called OC user. The seven-digit DN is converted to E.164 format before sending a call to the OC client.

For an incoming call to the OC client in Computer Mode, the Calling Line ID (CLID) appears in E.164 international format. When the OC receives a call from a phone from the PSTN, the CLID appears in E.164 international format, even if the caller is in the same country or same area.

For calls from the OC client to the Call Server, changes are made in the SIP message to define the destination telephone. The INVITE URI contains an E.164 number to use common SPN blocks in the Call Server.

Within North America

Various types of numbers can be recognized, including international, national, local (for example, NPA, NXX, and Free Calling Area Screening), or private, that use one or two access codes and number translators (AC1 and AC2). The E.164 number that enters the Call Server for Converged Office calls must be recognizable by the Call Server so that the call can be routed appropriately. The number is interpreted based upon the access code used within the called number as it enters the Call Server (AC1 or AC2).

If calls that enter the Call Server are identified as international and outside of North America (for example, the country code is not 1), the translator must contain entries that recognize the international numbers and route

the call to the appropriate route list. These entries are generally within the existing AC1/AC2 translator, as they are used to route international calls that are dialed directly from telephones.

If calls that enter the Call Server are national or local, the translation used must recognize numbers with the national dialing prefix (for example, Converged Office calls) and numbers without the national prefix (for example, local calls dialed by users). To enable this recognition without duplication of number plan entries, a Home NPA (HNPA) entry can be added to the AC1 translator to recognize calls within the local NPA that include the North American national dialing prefix (for example, 1613 within NPA 613). After matching the HNPA entry within AC1, the translation software automatically uses the AC2 translator to recognize the rest of the digits received.

Outside North America

Various types of numbers are recognized, including international, national, local, or private that use one of two access codes and number translators (For example, AC1 and AC2) and SPN entries. The E.164 number that enters the Call Server for Converged Office calls must be recognizable so that the call can be routed appropriately. The number is interpreted based upon the access code used within the called number as it enters the Call Server (AC1 or AC2).

If calls that enter the Call Server are international and outside of the country of the caller, the translator must contain entries that recognize the international numbers and route the call to the appropriate route list. These entries are generally within the existing AC1/AC2 translator, as they are used to route international calls that are dialed directly from telephones.

E.164 international format numbers for SIP Gateway and SIP CTI

For information about E.164 international format numbers for SIP Gateway (Computer) calls, see “E.164 International Format Numbers from Office Communicator - Computer Calls (SIP Gateway)” (page 203).

For information about E.164 international format numbers for SIP CTI (Phone) calls, see “Dialing E.164 International Format Numbers from Office Communicator - Phone Calls (SIP CTI)” (page 223).

Telephony Gateway and Services planning

This section describes the planning and engineering issues associated with the Telephony Gateway and Services component.

Table 16 "Systems, platforms, and applications" (page 81) identifies the systems, platforms, and applications supported by the Telephony Gateway and Services component.

Navigation

Systems, platforms, and applications

Table 16
Systems, platforms, and applications

System, platform, or application	Supported
M1/CS 1000 Systems	
CS 1000M Cabinet	Yes
CS 1000M Chassis	Yes
CS 1000M HG	Yes
CS 1000M SG (CP3/4)	Yes
CS 1000M SG (CP PIV)	Yes
CS 1000M MG (CP3/4)	Yes
CS 1000M MG (CP PIV)	Yes
CS 1000E	Yes
MG 1000B	Yes

Capacity

For more information relating to the Telephony Gateway and Services and Remote Call Control components, see "Capacity planning" (page 60).

Redundancy

Office Communications Server 2007 redundancy model is supported, with limitations, using Load Balancers.

NRS redundancy

NRS redundancy is similar to Converged Office redundancy; a heartbeat mechanism between MCM 4.x and NRS servers is implemented. When a heartbeat failure from the primary NRS server is detected, all messages are redirected to the secondary NRS server.

SIP routing

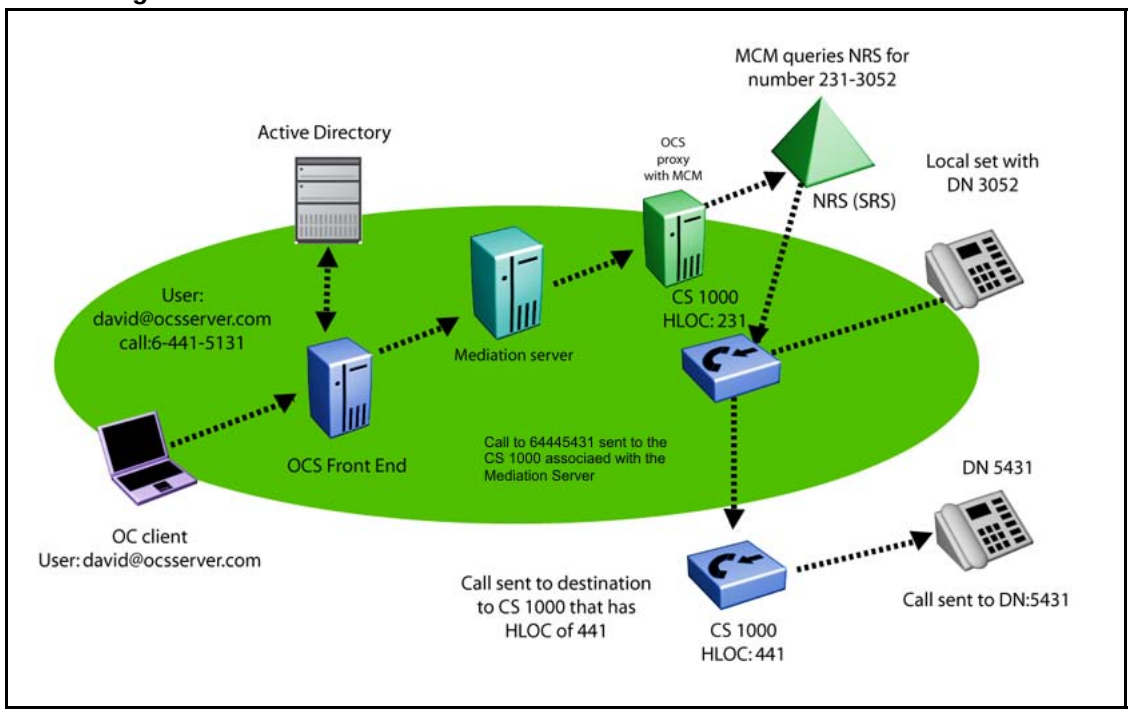
MCM directs calls from an Office Communicator user to the CS 1000 connected to the twinned telephone. A user can have a telephone number in Active Directory associated with their account as depicted in Figure 26 "SIP routing" (page 82), the number is 231-3052. Calls made from a user to any endpoint (Public or Private) are directed to the CS 1000. The CS 1000 tandems the call to the other CS 1000 (if necessary).

SIP routing ensures the following:

- Outgoing Office Communicator calls made by a twinned client can be tracked by Call Detail Recordings (CDR).
- Calls from an Office Communicator to incompatible systems can be made.

In Figure 26 "SIP routing" (page 82) the user david@ocsserver.com calls 6-441-5431 (AC1-LOC-DN). The From header in the INVITE has David's Line URI in the format of E.164;ext=2313051. The MCM picks up the IP address of the Mediation Server from where the call originated, looks up the SIP Gateway endpoint name associated with the Mediation Server in the Routing table and uses the NRS to get the call routed to the CS 1000 SIP Gateway. This CS 1000 directs the call to the CS 1000 that has the destination number of 441-5431, which then directs the call to the appropriate end user device.

Figure 26
SIP routing



Calls made to a CS 1000 that is different from the twinned telephone base uses two SIP trunks: one incoming and one outgoing.

Additional SIP trunks are needed, if users commonly call between CS 1000 systems.

For more information about the number of required SIP trunks, see the calculations described in "Trunks" (page 69) and the platform-specific Planning and Engineering document.

Feature interactions

This section describes the interactions of the Telephony Gateway (VoIP) component.

SIP and H.323 protocol interaction

VoIP tandem calls to OCS over H.323 trunks are not supported, as the H.323 protocol does not maintain RFC 2833 that is required for the Mediation Server.

Call transfers for Office Communicator direct PC-to-PC call

If an Office Communicator user sets up a call in Computer mode to another Office Communicator user directly, the call is sent to a Computer instead of a telephone number. As a result, the CS 1000 is not involved in the call and cannot transfer it to a telephone number.

LG-Nortel IP Phone 8540 OCS desk phone

An Enterprise Voice only client (no PBX integration enabled) that is configured for an OC 2007 client or 8540 OCS desk phone, is able to make PSTN calls using the CS 1000 as the gateway. You are required to configure a TN and twinned UEXT on the CS 1000 even if no actual phone is present for this client. This is because the MCM will perform homing on each OC client that makes an outgoing call before allowing it to proceed with the call.

Mixed network with SPS and SRS servers

On a mixed network where both SPS and SRS servers are present, MCM must be configured in SRS mode for collaboration server routing to work properly.

RCC only mode

Nortel recommends you do not define users with RCC-only mode because certain restrictions apply.

Bandwidth usage direct OC-to-OC audio call

The bandwidth usage of a Mediation Server direct OC-to-OC audio call is not calculated on the CS 1000. This portion of the required bandwidth should be calculated with Microsoft consultation and added to the Nortel bandwidth recommendations for Converged Office users. Failure to do so can affect the quality of the Converged Office calls in case bandwidth usage exceeds the planned limits.

Microsoft CFAC

Microsoft does not support Call Forward All Calls (CFAC) to voice mail on the OC client when users have Call Forward No Answer (CFNA) configured to voice mail and not Office Communicator. To have this functionality for an Enterprise Voice user with PBX integration, voice mail should be configured on the user's phone. If the user is in VoIP only mode (no phone) then the only option is for the administrator to configure the TLSV with Call Forward No Answer (CFNA). In this case, the calls will ring 4 times before being redirected to voice mail.

Office Communicator-initiated Call Transfer in Computer and PBX Integration Enabled

If the Office Communicator transfers a call, the SIP stack of the CS 1000 must handle the request to transfer the call. As such, the number a user is transferred to is not subject to the Class of Service associated with either user (the transferred party or the party performing the transfer). The Class of Service and Call Restriction that control the transfer is that of the SIP trunk itself.

Multiple customer operation

Multiple customer operation is not supported within a single Signaling Server; a separate Signaling Server is required for each customer. Each customer configured on the Call Server requires a separate node number and domain. For more information about how to configure a multiple customer environment, see "Multiple customer network" (page 54).

Deployment

You can find all of the information required to support Office Communications Server 2007 and Microsoft Office Communicator deployment on the Microsoft Web site. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

MCM uses LDAP queries to the Active Directory server for some OC user's attributes. You must engineer the Active Directory server properly to provide the expected performance for the LDAP queries (less than 25 milliseconds). Office Communications Server and Active Directory APIs are used for queries and mapping.

Office Communications Server 2007 availability

The Office Communications Server 2007 delivers an availability of up to 99.99% as described on the Microsoft Web site at www.microsoft.com. This is a Microsoft limitation.

Office Communications Server 2007 redundancy

The Office Communications Server 2007 redundancy model is supported, with limitations, using Load Balancers.

Office Communicator Web Access

Converged Office requires the client support SIP Gateway functionality. The Web version of Office Communicator, called Office Communicator Web Access, does not support SIP Gateway. Therefore, Office Communicator Web Access does not work with Converged Office.

Office Communicator Mobile

Converged Office requires the client to support Telephony Gateway. The Mobile version of Office Communicator, called Office Communicator Mobile (COMO), has limited support for Telephony Gateway. Telephony Gateway is supported only when the device runs Windows Mobile 5.0. VoIP calls work for incoming calls, but outgoing VoIP calls can only be placed to other Office Communicator users (computer to computer calls). Outgoing VoIP calls to telephone numbers for Microsoft Office Communicator Mobile are not supported.

OC client presence with Mobile Extension

Users of the Mobile Extension (Mobile X) feature, who are licensed to use Office Communication Server (OCS) 2007, automatically have mobile phone presence extended to OCS for SCR but not for MCR. However, OCS users must configure additional licenses (AST and TR/87) for each Mobile X user that is not associated with OCS, if presence indication is required.

One of the following scenarios can apply when using OC client with Mobile X.

- The OC client works in Computer mode, like a SIP software phone. There is no convergence on either the UEXT for a Mobile X or a desktop telephone associated with Mobile X. The OC client status does not affect the status of Mobile X.
- A desktop telephone is configured with a UEXT for a Mobile X. Nortel recommends that an OC client must converge on the desktop telephone. All OC client call control features such as Call Making, Call Transferring, Call Forwarding, and others continue to function on the OC client. The converged OC client works in Phone mode.

The displayed status must reflect the status of the converged desktop telephone, instead of the UEXT for a Mobile X.

- No desktop telephone and UEXT is configured for a Mobile X, therefore an OC client can converge on the UEXT. The OC client does not support call control features. When a mobile phone is idle and the UEXT is in idle status, the converged OC client displays Online. When a mobile phone user is on a call and the UEXT is busy, the converged OC client displays In a call.

The interoperability issues between the OC client and Mobile X are as follows.

- no MADN/MCR interworking for OCS with desktop telephone or multiline.
- no handoff from the OCS client to a desktop telephone through the handoff key (no busy detection).
- no presence indication when talking on a Mobile telephone for watchers on the OCS client when OCS client is logged off.
- no support for ACD with Mobile X in combination with desktop telephone using ACD.
- no RCC control of MOBX when there is only one telephone on the CS 1000 with presence.

Microsoft Virtual Server 2005

Microsoft Virtual Server 2005 is not supported as part of Nortel Converged Office.

DTMF

CS 1000 supports in-band DTMF digits and out-of-band DTMF digits for SIP calls through RFC2833. RFC2833 is an out-of-band mechanism for DTMF signaling. DTMF digit handling using RFC2833 enables Nortel CS 1000 products to work with other SIP products that support out-of-band DTMF signaling.

With RFC2833, a key press on a telephone translates to a signaling packet (or packets) that flow with the VoIP stream to the far end. These signaling packets are RFC packets which contain the DTMF key that was pressed. The same principle applies to TDM devices that are involved in a VoIP call. The Voice Gateway (VGW) TN that converts the TDM stream to VoIP also detects a tone on the TDM side and translates it to RFC2833 packets on the VoIP side. The VGW TN can receive an RFC2833 packet on the VoIP side and generates a tone on the TDM side.

Configure the correct Loss Values for in-band DTMF. For more information about configuring the CS 1000 to support in-band DTMF tones, see “Call Server configuration” (page 184).

ITG-Pentium cards

ITG-Pentium cards are not supported (regardless of load) due to RFC2833 not being supported.

Multimedia Communicator Server MeetMe Conference support

In Release 6.0, no limitations for Office Communicator calls to the Multimedia Communicator Server (MCS) MeetMe bridge exist, provided that all tandem nodes run Release 6.0 software.

Codecs

G.711 A/MU law is supported for the Mediation Server. The G.711 codec must use a 20 millisecond (ms) payload at this time, due to the Microsoft Office limitation. The Mediation Server does not support G.723 and G.729.

Video support

Office Communicator video is supported for Remote Call Control between two Office Communicator clients and VoIP calls directly between two OC clients without going through the Mediation Server. Office Communicator video is not supported if one of the clients goes through the Mediation Server.

Video Call Transfer

Office Communicator calls made in Computer mode that have established video can transfer to another Office Communicator user in Computer mode—although the new call is audio only. The transferred Office Communicator user experiences the call becoming audio only. After the transferred call is answered by the new endpoint, video can be established. As with all Call Transfers in Computer mode, it is a Blind Call Transfer, where the call is immediately transferred to the new party.

Local Tones

Office Communicator supports the generation of local tones (for example, Ringback), but the tones that the Office Communicator generates are unique tones that are not specific to any country. Ringback is generated only for a configured number of cycles; after which the other end continues to ring, but no audible ringback is heard.

Quality of Service

Office Communicator 2007 supports Quality of Service (QoS) 802.1 p and 801.2.

Voice mail

Voice mail is not supported for direct Office Communicator calls. Voice mail is supported only with TLSV, SimRing, and CD1 Call Forward No Answer and MCS 5100 Advanced Screening calls.

Long distance/overseas control

Long distance or overseas calls from Office Communicator are allowed based on the Network Class of Service (NCOS) for the MARP TN of the number and extension associated with the Office Communicator user. For example, if user david@ocsuser.com has a number and extension of 3052, david@ocsuser.com can call the same long distance and overseas numbers that the number and extension 3052 can on the CS 1000. For more information, see "Call Server configuration" (page 184).

MCS 5100

MCS 5100 interoperability and federation with Office Communications Server requires that a CS 1000 reside between the two servers, and is limited to voice.

SIP Trunks

TCP or TLS-based SIP trunks are supported. SIP trunks and gateways must be enabled with enough trunks to handle the traffic between the CS 1000 and Office Communications Server. For more information, see "Trunks" (page 69).

Phone mode

Office Communicator supports phone mode where it controls the desktop telephone to originate or answer calls and the VoIP mode where voice calls can originate or be answered from the client.

Hold and Transfer

Office Communicator supports Hold and Transfer in stand-alone or VoIP mode.

ipDialog Ethernet Phone

Office Communicator clients can work with the ipDialog Ethernet Phone only if it goes through a CS 1000.

Country or region tone configuration

Country or region tone configuration is not supported by Office Communications Server or Office Communicator.

Conference

Incorrect participants appear on the conference conversation window in the following scenario. For example, User A makes a call by SIP alias in Office Communicator–Computer mode to User B in Office Communicator–VoIP mode. User B answers the call and conferences

in User C in Office Communicator–VoIP mode. User C is invited to the conference by phone number. User C joins the conference. This results in four participants being displayed in the conversation window instead of three. This is a Microsoft limitation and can be reproduced when the CS 1000 system, Mediation Server outbound routing, and static Front End routes are disabled.

Active Directory configuration

A record in the Active Directory must be created for all Communication Se rver 1000 phones whether an Office Communicator client is associated with it or not. If a Communication Server 1000 phone is not in the Active Directory, an OC client user notices the following:

- Cannot add the telephone number to the Office Communicator Contact List.
- Receives two toasts when calls are made from these telephones.

UEXT (TLSV) Busy status feature

UEXT Busy status feature is not applicable for TLSV subtype. TLSV acts in the same way as PCA based on SCR or MCR treatment.

The busy status of Office Communicator (OC) cannot be tracked because calls made to or from Office Communicator (OC) that are not routed through the CS 1000 Call Server are not known to the CS 1000 Call Server.

DTMF detection

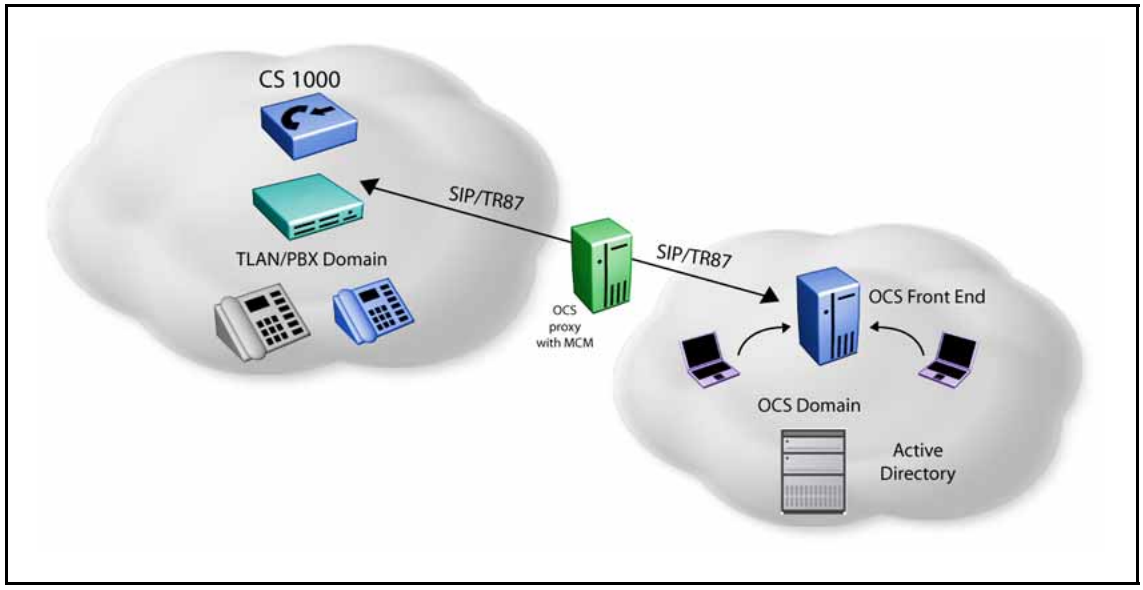
To handle DTMF detection properly with OCS 2007, all network components must support RFC283. A minimum software release of Release 5.0 is required for all branch or main offices; otherwise, problems occur when interacting with Interactive Voice Response (IVR) systems, collect calls, and using meet-me conference bridges.

Remote Call Control with SIP CTI

The Remote Call Control component works in all configurations that include a Signaling Server and is supported for IP, digital, and analog telephone types.

Office Communicator client uses the ECMA TR/87 specification. Figure 27 "Simple network diagram" (page 90) shows a sample customer network that deploys Active Directory, the OCS 2007 Front End, OCS proxy server with MCM, and Communication Server 1000.

Figure 27
Simple network diagram



The TR/87 FE is the application that resides on the CS 1000 Signaling Server to support the telephony control requests and responses received from the Office Communicator 2007 client within an Office Communications Server 2007 deployment.

CS 1000 is supported in both the Office Communications Server 2007 Standard Edition and Enterprise Edition network configurations. For more information about restrictions, see “Capacity planning” (page 60).

Table 17 "Supported systems, platforms, and applications" (page 90) identifies the systems, platforms, or applications that are interoperable or supported by the Remote Call Control component. Interoperable means that this feature does not negatively impact existing functionality (regardless of whether this feature actually interacts with the system, platform, or application).

Table 17
Supported systems, platforms, and applications

Systems, platforms, and applications	Interoperable	Supported
M1/CS 1000 systems		
Option 11C Cabinet	Y	N
Option 11C Chassis	Y	N
Option 61C (CP-PII and -PIV)	Y	N
Option 81C (CP-PII and -PIV)	Y	N
CS 1000M SG (CP-PII and -PIV)	Y	Y

Table 17
Supported systems, platforms, and applications (cont'd.)

Systems, platforms, and applications	Interoperable	Supported
CS 1000M SG (CP PIV)	Y	Y
CS 1000M MG (CP-PII and -PIV)	Y	Y
CS 1000E SA/HA (CP-PII, -PIV, and -PM)	Y	Y
MG 1000T (SSC)	Y	N
MG 1000B (MGC and CP-PM)	Y	Y*
MG 1000E (MGC)	Y	Y*
* Digital and analog telephones in Branch Offices are supported when access to the proxy/redirect server and OCS 2007 is available.		
Other systems, call servers and gateways		
CS 2000	Y	N
CS 2100	Y	N
MCS 5100/CD	N	N
SRG 1.0	Y	Partial*
SRG 50	Y	Partial*
BCM 50 version 2.0	Y	Partial**
BCM 50 version 3.0	Y	Partial*
BCM 200/400	Y	Partial**
Norstar VoIP Gateway (NT9B10AA)	Y	N
NetRIO Service Management Center (SMC)	Y	N
* Telephones in normal mode (network connection to the main office up) are supported. No RFC 2833 support. Tandem calls out of a BCM/SRG from OCS with DTMF do not work. ** Telephones in normal mode are supported. No RFC2833 support. Tandem calls out a BCM/SRG from OCS with DTMF would not work.		
Nortel applications		
IP Phone 2001	Y	Y
IP Phone 2002 Phase I	Y	Y
IP Phone 2002 Phase II	Y	Y
IP Phone 2004 Phase 0/I	Y	Y
IP Audio Conference Phone 2033	Y	Y
IP Softphone 2050 release 3.0	Y	Y
Mobile Voice Client 2050	Y	Y

Table 17
Supported systems, platforms, and applications (cont'd.)

Systems, platforms, and applications	Interoperable	Supported
WLAN Handset 2210	Y	Y
WLAN Handset 2211	Y	Y
WLAN Handset 2212	Y	Y
IP Phone 1110	Y	Y
IP Phone 2007	Y	Y
IP Phone 1120E	Y	Y
IP Phone 1140E	Y	Y
IP Phone 1150E	Y	Y
IP Phone 1200 series	Y	Y
TDM Phones M3900 series	Y	Y
M3000	Y	Y
M2317	Y	Y
M2006	Y	Y
M2008	Y	Y
M2316	Y	Y
M2016S	Y	Y
PC Console Interface Unit	Y	Y
CDR	Y	N
Telephony Manager (TM)	Y	Y
Element Manager (EM)	Y	Y
Element Subscriber Manager (ESM)	Y	N
CallPilot	Y	N
CallPilot Mini	Y	N
Meridian Mail	Y	N
Meridian Mail Card Option	Y	N
Meridian/Succession Companion DECT (DMC8 version)	Y	N
VoIP-802.11 Wireless IP Gateway	Y	N
Remote Gateway 9150	Y	N
Meridian Home Office MHO-II – MD'ed	Y	N
Remote Office 9115/ IP Adaptor	Y	N
Carrier Remote	Y	N
Fiber I and Fiber II	Y	N

Table 17
Supported systems, platforms, and applications (cont'd.)

Systems, platforms, and applications	Interoperable	Supported
Symposium Desktop TAPI Service Provider for MCA	Y	N
Meridian Link Services [MLS]	Y	N
Symposium TAPI Service Provider	Y	N
Symposium Agent	Y	N
Symposium Agent Greeting	Y	N
Symposium Express Call Center (SECC)	Y	N
Symposium Call Center Server [SCCS]	Y	N
Symposium Web Centre Portal (SWCP)	Y	N
Periphonics Open IVR (VPS/is)	Y	N
Periphonics Integrated Package for Meridian Link (IPML) – VPS	Y	N
Periphonics Multimedia Processing Server (MPS) 100	Y	N
Periphonics Multimedia Processing Server (MPS) 500	Y	N
Integrated Call Assistant	Y	N
Integrated Conference Bridge	Y	N
Integrated Recorded Announcer	Y	N
Integrated Call Director	Y	N
Hospitality Integrated Voice Services (HIVS)	Y	N
Enterprise Data Networking	Y	N
UM2000	Y	N
Multimedia Application Server MAS	N	N
Nortel Multimedia Conference	Y	N
Third party applications		
Application gateway 1000	Y	N
Microsoft Office Communication Server	Y	N
MS Exchange Server	Y	N
MS Virtual Server 2005	Y	N
Audio Code Mediant 2000 SIP-PRI Gateway	Y	N
Competitors		

Table 17
Supported systems, platforms, and applications (cont'd.)

Systems, platforms, and applications	Interoperable	Supported
Cisco H.323 GW	Y	N
Avaya H.323 GW	Y	N
Cisco SIP GW	Y	N
Avaya SIP GW	Y	N
Verizon SIP Trunk	Y	N
AT&T SIP trunk	Y	N
Broadsoft	Y	N
ACME SBC	Y	N
3100 Mobile Communication Gateway	Y	N

Analog devices are supported by Converged Office. However, you must have a handsfree device to take on- and off-hook when using the OC client.

Redundancy

Remote Call Control (RCC) services are supported (with limitations) in the following scenarios:

- Single node redundancy
- Campus redundancy
- Geographic redundancy

Single node Redundancy

The same master and follower mechanism used for Virtual Trunk (VTRK) and TPS applications is used to support redundancy within a node for RCC. After the master of the node fails, one of the followers takes over the node IP and continues to deliver service. VoIP mode session state is preserved when a new master is elected.

Redundancy across multiple nodes is possible using the Least Cost Routing feature of NRS. When considering a multinode redundant configuration, see the restrictions for establishing TR/87 sessions from multiple nodes that have AML links to a single Call Server. For more information, see "Capacity planning" (page 60) .

Campus redundancy

Campus Redundancy increases the distance between the two CPU cores of CS 1000E.

The CS 1000E is the only large system that supports this feature.

Geographic redundancy

Geographic Redundancy can be supported with the limitations that currently exist for SIP gateway SIP traffic. The main impacts are.

- During transition periods, situations can arise where IP phones are registered to a Call Server that is different from the call server that provides support for the TR/87 FE. In this situation, TR/87 support is undefined. TR/87 clients can register successfully; however, the status of the IP Phone is impacted by any actions performed on the telephone or the TR/87 client, as the FE and IP Phone interface different Call Servers. NRS is required to support redundancy.
- After an event occurs that causes the IP Phones to register to a server other than the Front End server (and then to return to the Front End server), the Office Communicator 2007 client does not automatically follow the IP Phone registration. To direct the TR/87 sessions back to the TR/87 FE that corresponds to the home TPS, take one of the following actions:
  - Users must log off and log back on the TR/87 client (for example, Office Communicator 2007) to force the previous SIP dialog to terminate so that a new dialog can be established, which NRS redirects to the correct TR/87 FE.
  - An administrator issues the SIPCTIStop all command on the Signaling Server on which the TR/87 sessions currently reside to terminate the SIP dialogs. This forces the clients to send another association request (for example, SIP INVITE), which the NRS redirects to the correct TR/87 FE, as depicted in Table 18 "SIPCTIStop all command" (page 95).

Table 18
SIPCTIStop all command

Command	Description
SIPCTIStop all	De-acquire all AST DNs and terminate all TR/87 SIP sessions.

Branch Office redundancy (MG 1000B/SRG)

Branch Office scenarios can be supported; however, SIP CTI support and Telephony Gateway and Services are available for Branch user IP telephones in Local mode (registered in the Branch Office) only when the following conditions are met:

- The Branch Office has SIP CTI and Telephony Gateway and Services enabled and has a Signaling Server dedicated to each branch.
- The network dialing plan is a Coordinated Dialing Plan (CDP).
- The IP Phone (Branch User) has the same domain name configured in both the Main Office and Branch Office.

- The Branch Office has access to the NRS and Office Communications Server (OCS). If access is disrupted, failure cases may not be supported if the NRS and OCS are located in close proximity to the Main Office, which is no longer available. For example, when the WAN link to the Main Office is down, the NRS and OCS are out-of-service.
- The SIP Gateway in the Main Office is out -of-service (in which case the SIP Gateway in the Branch Office is used).

The Microsoft Office Communicator client has no automated mechanism to register to the branch. Users must wait for the existing dialog to time out (30 minutes) or manually log off and log on again after the IP phones change to local mode.

When the Main office link is up, the IP phone registered to the Branch office will be redirected back to the Main Office. The corresponding OC client need not logout and login to acquire that IP phone. The OC client will automatically acquire it. This depends on the LTPS-NCS polling, which at most will take 10 minutes. This will not cover Geographic Redundancy.

Digital and analog telephones in the Branch Office can have Remote Call Control (RCC) and PBX Integration Enabled support when the Branch Office has access to the NRS and OCS.

Feature Interactions

This section describes the interactions of the Remote Call Control with the SIP CTI component.

Table 19
Feature Interactions of RCC

Feature Operation	Description
Call Forwarding	Office Communicator does not reflect call forward state changes made to the CS 1000 telephone itself.  **WARNING** **Call Forward state changes** Office Communicator does not reflect Call Forward state changes made to the CS 1000 telephone. When Office Communicator is active and controls a DN, make Call Forward changes through Office Communicator to ensure that it is in the correct state. When a user logs on to the OCS 2007 from their Office Communicator client, the forwarding status saved within Office Communicator overrides the forwarding status configured from the telephone. For example, if forwarding is off within Office Communicator, it is turned off following logon,

Feature Operation	Description
	regardless of the phone forwarding status at the time.
Analog telephone usage	As a general rule, Office Communicator in phone mode can control and invoke only telephony features supported by the telephone. If a feature is not supported or configured on a particular telephone (either Analog, IP, or Digital), it is not supported by Office Communicator. An Office Communicator in phone mode that supervises an analog phone (2500) has the following limitations: • Make Call: cannot be made by using Office Communicator if the analog phone (2500) phone does not go off-hook prior to placing the call. • Answer Call: cannot be answered by using Office Communicator. Answer Call must be answered by using the analog phone (2500). • Conference Call: cannot occur by using Office Communicator. • Call Hold: can occur by using Office Communicator. • Call Transfer: analog telephones do not support the Conference and Transfer key features. As a result, Call Conference and Call Transfer (Announced and Blind) cannot occur by using Office Communicator. Flexible Feature Code (FFC) is not supported by AML and RCC. • Send DTMF digits: DTMF digits work with both Voice Mail and Conferencing.
Multiple Customer operation	Multiple Customer operation is not supported within a single Signaling Server; a separate Signaling Server is required for each customer. Multi-customer support is a consideration for future releases. For more information about how to configure a Multi-Customer environment, see "Multiple customer network" (page 54).
TR/87 Front End application	The TR/87 FE application on a Signaling Server can support only a single Call Server.
UDP Location Code	Only one UDP Location Code can be associated with each Signaling Server TR/87 interface. For example, a different HLOC cannot be used inside the same customer for SIP CTI feature. When using UDP, local calls are represented as CDP so you cannot define which HLOC to insert into calling DN.
Office Communicator Web Access	Converged Office requires that the client support RCC. The Web version of Office Communicator, called Office Communicator Web Access, does not support RCC.

Feature Operation	Description
Office Communicator Mobile (COMO)	Converged Office requires the client to support Remote Call Control, but the Mobile version of Office Communicator, called Office Communicator Mobile, has limited support for Remote Call Control. Outgoing VoIP calls to telephone numbers for Office Communicator Mobile are not supported. Remote Call Control permits only telephone status updates (for example, on a call or not) when you use Office Communicator Mobile. Remote Call Control supports Call Forward with COMO.
Virtual Server 2005	Virtual Server 2005 is not supported as part of Nortel Converged Office.
Office Communicator 2007 Call Forward All Calls	When the CS 1000 Call Forward All Calls feature is enabled, only calls to the Prime DN or any single-appearance DN on the telephone are forwarded. Therefore, if an Office Communicator 2007 acquires a MADN, and it is not the Multiple Appearance Redirection Prime (MARP), the call is not forwarded even if the Call Forward feature is enabled. For more information, see *Features and Services* (NN43001-106.).
Office Communications Server and MCS coexistence	**ATTENTION** All Converged Office users must have their extension configured as CLS CDMR. A user cannot have both Office Communications Server and MCS enabled for their extension (all TNs that have a particular number and extension). If any TN has CLS CDMV or CLS CDMO configured, the extension is treated as having MCS enabled. When MCS (SIP CD) is enabled on an extension, Office Communications Server Converged Office is not supported for that extension.
CallPilot configuration	For PBX Integration Enabled (Computer Mode) calls to access the CallPilot mailbox, the Pound key (#) is pressed. Every mailbox must have the optional messaging network configured. In a normal CS 1000 - CallPilot scenario, this configuration is optional. For PBX Integration Enabled (Computer Mode) calls to CallPilot to work properly, this extra configuration is required. For more information about the configuration of CallPilot, see *CallPilot Network Planning Guide* (NN44200-201.)
Conference Call and Do Not Disturb (DND) features	Conference Call and DND features in RCC mode are not supported by Microsoft.
Flexible Feature Code (FFC)	All Flexible Feature Codes (FFC) are not supported by RCC. FFC codes can be used from a converged phone but cannot be performed through Office Communicator in RCC mode.

OCS 2007 interactions

For information about OCS 2007 limitations, go to www.microsoft.com.

LCS 2005 and OCS 2007 coexistence

This section describes the coexistence limitations of LCS 2005 and OCS 2007.

Client considerations

Features hosted on Office Communications Server 2007 are not supported by the OC 2005 client. After a user is configured for enhanced presence, the account can no longer use previous versions of OC 2005, Communicator Web Access 2005, or Communicator Mobile 2005. Microsoft recommends that you upgrade all client computers for a particular user at the same time. Communicator 2007 clients cannot log on to Live Communications Server 2005. Verify that any user whose client is upgraded to Communicator 2007 is already provisioned on an Office Communications Server.

Converged Office functionality

An upgrade from the LCS Application Proxy to the OCS Proxy Server and MCS 2.0 to MCM 4.x is required to manage CS 1000 telephones by the OC 2007 client in either VOIP or RCC mode. Inter-working of MCM 2.0 with OCS Proxy Server or MCM 4.x with LCS Application Proxy is not a supported configuration because of incompatible underlying libraries. The same CS 1000 can be connected to two or more communication servers (LCS 2005 or OCS 2007).

The following must be considered for coexistence of LCS 2005 and OCS 2007:

- The CS 1000 must be upgraded to Release 6.0.
- OCS 2007 patches from Microsoft must be in service. For more information, see the Attention box under “OCS 2007 component installation” (page 124).
- NRS is required to appropriately route a call to the Communication Server.
- Different server DNs (Hot Ps) are assigned for each Communications Server (LCS or OCS). The TLSV for each user is configured with the corresponding server DN as a target DN
- LCS 2005 and OCS 2007 can share the same Active Directory but you can only have one OC client user account on either LCS 2005 or OCS 2007.
- For Remote Call Control (RCC) support , a single Signaling Server cannot be used for both LCS 2005 and OCS 2007 as the configuration of the SIP CTI FE is different for both. In this case, the following options can be considered:
  - RCC supported for both LCS 2005 and OCS 2007. Upgrade the existing Communication Server 1000 to support OCS 2007 RCC

users. Configure an additional SIP CTI FE Signaling Server for LCS 2005 RCC users. An additional AML ELANs is defined on the Call Server. Change the static routing rule on the LCS 2005 Home server to route RCC traffic directly to the SIP CTI FE for LCS 2005. Geographic Redundancy is not supported for LCS 2005 RCC users in this case.

— RCC supported for only LCS 2005 users. Enable RCC only for LCS users in the Active Directory, on the OC clients, or both. Configure the SIP CTI FE according to the document *Nortel Converged Office Fundamentals* (NN43001-525) for LCS 2005. For example, the Phone context=dialstring configuration on the Signaling Server is used.

— RCC supported only for OCS 2007 users. Enable RCC only for OCS users in the Active Directory, on the OC clients, or both. Configure the SIP CTI FE according to this document. For example, the Phone-context=<SIP URI Map Entries> configuration on the Signaling Server is used.

MCM 2.0 to MCM 4.x

No direct upgrade path from MCM 2.0 to MCM 4.x exists. MCM 4.x must be installed on the OCS Proxy server. The OCS Proxy install is done from the command line and not from the install wizard. It is still possible to preserve the configuration data from a previous installation by first performing a backup operation on MCM 2.0 and restore the data to MCM 4.x on the OCS Proxy server. However, this causes the new configuration parameters to be reset to default values as follows:

Table 20
Default configuration parameters

Parameter	Default value
Call Server	CS1000
MediationServer	enabled
RoutingTable	empty
DialPlan	CDP
AccessCode	empty

For more information about MCM 4.x configuration, see “MCM configuration” (page 154).

Load balancer considerations

You cannot use a single logical load balancer for LCS 2005 and OCS 2007. For example, if you have an LCS 2005 application proxy with MCM 2.0 attached to a logical load balancer, you cannot simultaneously attach an OCS Proxy server with MCM 4.x to the same one. This same restriction applies to all other server roles.

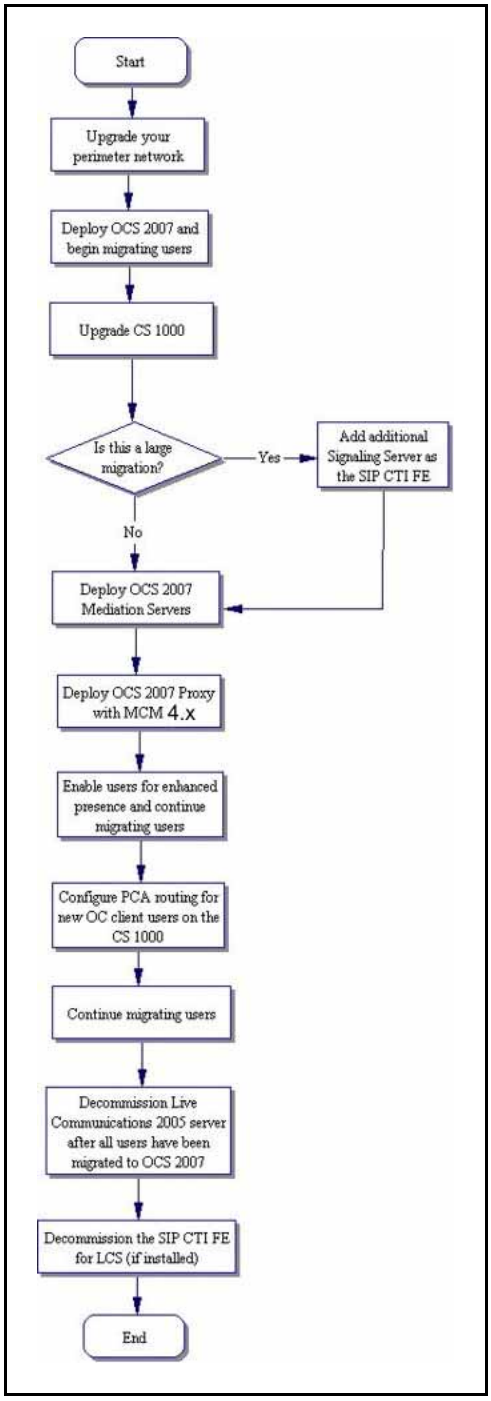
Migration planning from LCS 2005 to OCS 2007

Yuo can upgrade Live Communications Server 2005 SP1 only to Office Communications Server 2007 by using a side-by-side migration. This involves deploying an Office Communications Server 2007 Standard Edition or Enterprise pool alongside existing Live Communications Server 2005 with SP1 Standard Edition or Enterprise pool thus allowing the two environments to coexist with minimal service disruption.

When migrating servers, Office Communications Server 2007 servers can be deployed using a phased, outside-in approach. This involves replacing the Access Proxies with Office Communications Server 2007 Access Edge Servers before you migrate to Office Communications Server 2007 in your internal environment. Upgrading all the servers of a particular type at one time helps to minimize service disruptions.

The following flow chart depicts the migration phases:

Figure 28
LCS to OCS migration task flow



Prerequisites

Upgrading to Office Communications Server 2007 is based on the following assumptions:

- You understand the basic migration process.
- You understand the coexistence interactions. For more information, see “LCS 2005 and OCS 2007 coexistence” (page 99).
- You understand CS 1000, Signaling Server, and networks.
- You understand the user migration process.

Determine your deployment options

Two deployment options exist depending on whether you are migrating a small or large client base.

For a small client base, Office Communicator client users can be migrated from LCS to OCS inside a set maintenance window. No extra servers are required.

For a large client base, Office Communicator client users need to be migrated over multiple maintenance windows using a phased approach. The following choices must be made:

1. If using one SIP CTI FE Signaling Server
   — Only LCS users have RCC

   OR

   — OCS users have RCC
2. If deploying an additional SIP CTI FE Signaling Server
   — RCC is supported for both LCS and OCS. One Signaling Server for LCS RCC and the other for OCS RCC

ATTENTION
Before migrating to Office Communications Server 2007, existing Live Communications Servers must have Live Communications Server 2005 SP1 installed.

Migration process

The following table breaks down the migration process using a phased, outside-in approach and defines the impact for the user at each phase.

Table 21
User experience

Phase	Description	User experience
1. Upgrade your perimeter network.	Introduce a new Office Communications Server (OCS) 2007 Access Edge Servers and Directors into your Live Communications Server (LCS) 2005 SP1 environment.	No changes. Users continue to use the Microsoft Office Communicator (OC) 2005 client and have the same IM and presence functionality.
2. Deploy OCS 2007 and begin moving users to the new server or pool.	Deploy a new Office Communications Server 2007 Enterprise pool or Standard Edition server. If required, deploy an Archiving and CDR Server. Users are moved to the new server or pool but will continue to use OC 2005 .	No changes. OC 2007 client is not rolled out at this phase so users continue to use OC 2005 and have the same IM and presence functionality.
3. Upgrade CS 1000 and if determined for your migration, add an additional Signaling Server as the SIP CTI FE.	Upgrade Call Sever and Signaling Server. If you have a large client base, add an additional Signaling Server as the SIP CTI FE so both LCS 2005 and OCS 2007 can have RCC.	No changes. Users continue to use OC 2005 and have the same IM and presence functionality.
4. Deploy OCS 2007 Mediation Server.	Deploy OCS 2007 Mediation Servers.	No changes. Users continue to use OC 2005 and have the same IM and presence functionality
5. Deploy OCS Proxy server with MCM 4.x.	Deploy OCS Proxy Server with MCM 4.x.	No changes. Users continue to use OC 2005 and have the same IM and presence functionality
6. Enable enhanced presence, roll out OC 2007 client, and continue migrating users	Enable users for enhanced presence, roll out the OC 2007 client, and the Live Meeting 2007 client to the users.	• The migrated users can use the full functionality of OC 2007 when communicating with other migrated users. • Once enabled for enhanced presence, these users can no longer sign in to a OC 2005 client or previous Communicator Web Access or Communicator Mobile Access clients.

Phase	Description	User experience
7. Configure TLSV routing for new OC 2007 client users on the CS 1000.	Configure TLSV on the CS 1000. Change NRS and SPS routing.	Migrated users are able to use Telephony Gateway and Services functionality (VoIP) and RCC.
8. Continue migrating users.	Migrate remaining users. Enable users for enhanced presence. Roll out the OC 2007 client and the Live Meeting 2007 client to the users.	• OC 2007 users can use the full functionality of OC 2007 when communicating with other OC 2007 users. • When OC 2007 client users are communicating with OC 2005 users, they cannot use the new features in OC 2007. • After Live Meeting 2007 is rolled out to your users, they can participate in on-premise conferences internally and connect to these conferences remotely by using the Web Conferencing Edge Server. • RCC is only available to either OCS 2007 or LCS 2005 users when one SIP CTI FE Signaling Server is deployed. For more information, see “Converged Office functionality” (page 99).
9. Decommission all Live Communications 2005 servers and MCM 2.0 after all users have been migrated to OCS 2007	Remove Live Communications Server 2005 and MCM 2.0 from your environment.	All users are on OC 2007, enabled for enhanced presence and have full functionality of OC 2007. If Live Meeting is deployed, users can participate in on-premise conferences internally and connect to these conferences remotely by using the Web Conferencing Edge Server.
10. Decommission the SIP CTI FE for LCS (if installed)	Remove the SIP CTI FE for LCS (if an additional Signaling Server was deployed).	None.

Description of Migration Phases

To deploy OCS 2007 in an existing Live Communications Server 2005 topology, Nortel recommends that you perform the following steps:

Migrating users from LCS to OCS

Step	Action
1	Upgrade your perimeter network by deploying an Access Edge Server that communicates with Live Communications Server 2005 Director. When Director is not deployed, the edge server communicates directly with your internal Live Communications Server 2005 Standard Edition servers or Enterprise pool and the new Access Edge Server is configured as the next hop server to which existing pools and Standard Edition Servers will route external traffic. Next, an Office Communications Server 2007 Director is deployed to replace Live Communications Server 2005 Director. Incoming and outgoing traffic is configured to go through the new Director (if a Director was previously not used and you do not want to use one now, skip this step). For more information, download Microsoft technical documentation from the Download Center at www.microsoft.com.
2	In this phase, an internal Office Communications Server 2007 Standard Edition Server or Enterprise pool is deployed. Move an initial group of users to the new server or pool but they continue to use OC 2005 as their client. If required, deploy an Archiving and CDR Server. DNS update is required next. For more details, see “LCS 2005 and OCS 2007 coexistence” (page 99).
3	Upgrade CS 1000 and if determined for your migration, add an additional Signaling Server as the SIP CTI FE. Upgrading Call Sever and Signaling Server according to standard procedures. For more information, see “LCS 2005 and OCS 2007 coexistence” (page 99).
4	Deploy OCS 2007 Mediation Server. For more information about deploying Mediation Server, download Microsoft technical documentation from the Download Center at www.microsoft.com.
5	Deploy OCS Proxy server with MCM 4.x . For more information, see “Installing the OCS Proxy server (R1)” (page 126) and “Installing MCM” (page 129).
6	Enable enhanced presence and continue migrating users. Start to move users from Live Communications Server 2005 to Office Communications Server 2007. By enabling enhanced presence, users are allowed to use Office Communicator 2007 and the new functionality that it provides. After enabling the users for enhanced presence, roll out OC 2007 client to each computer for these users. Once a user is enabled for enhanced presence, they can no longer use any previous client versions. For more information about enhanced presence, download

Microsoft technical documentation from the Download Center at www.microsoft.com.

7 Configure TLSV routing for new OC client users on the CS 1000. After configuration of TLSV routing, users will be allowed to use Telephony Gateway and Services (VoIP) and RCC functionality. A Server URI field should be changed for migrated users to enable SIP CTI functionality. Change NRS and SPS routing.

8 Continue migrating users. Enable users for enhanced presence. Roll out the OC 2007 client and the Live Meeting 2007 client to the users. For more information about enhanced presence, download Microsoft technical documentation from the Download Center at www.microsoft.com.

9 Decommission all Live Communications 2005 servers and MCM 2.0 after all users have been migrated to OCS 2007.

10 Decommission the SIP CTI FE for LCS (if installed).

--End--

Unified Messaging

This section describes the interactions and inter-workings of Unified Messaging (UM) with Converged Office. Office Communications Server (OCS) 2007 users can access Unified Messaging capabilities by using CallPilot or Exchange Server 2007. Features that are accessible to the OCS 2007 users from CallPilot or Exchange are determined by the deployment. The following sections describe the user experience based on deployments when using CallPilot, Exchange integrated with OCS, and Exchange non integrated with OCS. For more information about the signaling that occurs in an integrated or non integrated configuration, see “Signaling with integrated Voice Mail” (page 118) and “Signaling with nonintegrated Voice Mail” (page 119).

Navigation

Feature interactions

This section describes the sRTP interactions of the Exchange 2007 Unified Messaging component.

Secured dialing plan

If Microsoft Exchange 2007 has VoIP security configured as secured, the following interactions are present:

- All mailboxes associated with the secured dialing plan are treated with a media security Class of Service of Always Secured.
- TLS is required for SIP signaling between Exchange 2007 and the Communication Server 1000.
- IP or digital telephones that do not support sRTP are not compatible with Exchange 2007.

Exchange 2007 Unified Messaging Service Pack 1

Exchange 2007 SP 1 with sRTP does not support rekeying. In usual RTP/RTCP voice usage, supporting key update is not a security concern because the rekeying threshold is not normally reached.

Exchange 2007 SP 1 with sRTP does not renegotiate a new security context. During a SIP REINVITE, the current security context is used for both send and receive streams.

Table 22
Features not supported with Exchange 2007 SP 1 and TLS enabled

Action	Support
Call on Hold	Not supported
Call Transfer (Blind)	Not supported

Action	Support
Call Transfer (Consultative)	Not supported
Call Conference	Not supported

The Product Enhancement Patch (PEP) to negotiate best effort sRTP does not affect previous interactions between Communication Server 1000 5.x and Exchange 2007 Unified Messaging SP 1.

Configuration requirements

For the Communication Server 1000 to use sRTP and TLS with Exchange 2007 Unified Messaging, you must ensure the following requirements:

- System-wide Media Security must be on.
- Telephones on the CS 1000 must support sRTP.
- TN for the telephone must have a Class of Service (CoS) of MSBT (Best Effort security) or MSAW (Always Security).
- Exchange Server 2007 must be configured. For more information, see *CS 1000 with Microsoft Exchange Server 2007 UM* (NN43001-122).

General user description

The following list describes the various possible user configurations. All Enterprise voice users require Telephony Services (TLSV).

- Enterprise Voice Converged Office (CO) user—has a CS 1000 phone, an OC client, and RCC enabled. In addition, the OC client is configured with the Enterprise Voice and PBX integration options selected and the Server URI field contains valid information.
- Enterprise Voice Non-Converged Office (NCO) user—has a CS 1000 phone, an OC client, and RCC disabled. In addition, the OC client is configured with the Enterprise Voice and PBX integration options selected and the Server URI field is empty.
- Enterprise Voice Office Communicator (OC) user—does not have a CS 100 phone but has an OC client and/or an LG 8540 phone. In addition, the OC client is configured with only the Enterprise Voice option selected, the PBX integration option is not selected, and the Server URI field is empty.
- Remote Call Control (RCC) only user—has a CS 1000 phone, an OC client, and RCC enabled. In addition, the OC client is configured with only the Remote Call Control option selected, the Enterprise Voice and PBX integration options are not selected, and the Server URI field contains valid information.

The following table shows the various possible user configurations.

Table 23
CS 1000 user configurations

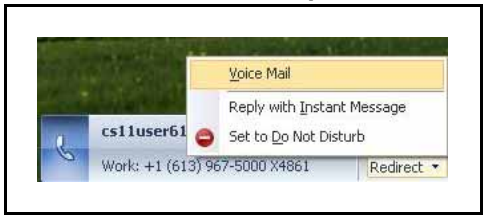
	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC-only user
Enterprise Voice	Yes	Yes	Yes	No
PBX Integration (Dual Forking enabled)	Yes	Yes	No	No
Server URI field (RCC enabled)	Yes	No	No	Yes
CS 1000 phone	Yes	Yes	No	Yes
Enable RCC-onl y option	No	No	No	Yes

Additional OC client features and capabilities using Exchange integrated with OCS

You can integrate OCS and Exchange 2007. This capability provides additional OC client features depending on your individual deployment configuration. The features are as follows:

- You can use the Voice Mail option to redirect calls from the OC client to Exchange UM instead of redirecting them to the system access DN, as shown in the following figure.

Figure 29
Redirect to Voice Mail option



- With the OC client, you can call Voice Mail instead of dialing the system access DN, as shown in the following figure.

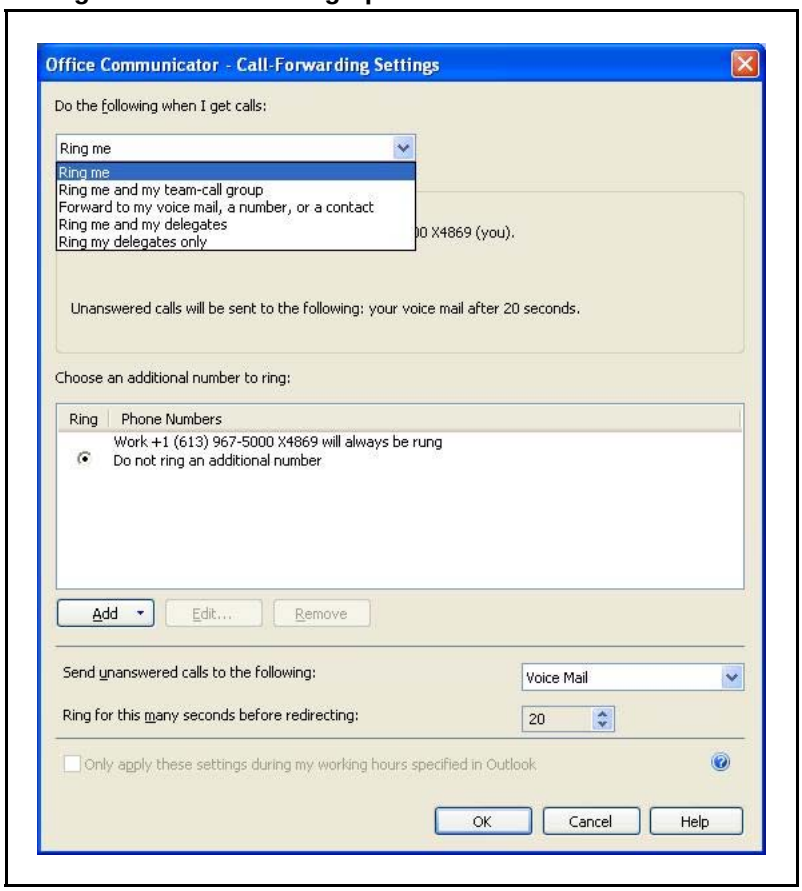
Figure 30
Call voice mail

- With the OC client, you can change your Voice Mail greeting, as shown in the following figure.

Figure 31
Change voice mail greetings

- With the OC client, you can configure Call Forwarding using the Voice Mail option, as shown in the following figure.

Figure 32
Configure Call Forwarding option



Communication Server 1000 configuration

The following sections describe the two types of configurations on the CS 1000—user configuration and phone configuration.

User configuration

The following table depicts the user configurations as determined by the Voice Mail application used.

- Enterprise Voice Converged Office (CO) user—when configuring Enterprise Voice Converged Office CO users, you must enable Telephony Services (TLSV) and SIP/CTI services on the CS 1000.
- Enterprise Voice Non-Converged Office (NCO) and Enterprise Voice Office Communicator (OC) users—when configuring Enterprise Voice NCO users and Enterprise Voice OC users, you must enable Telephony Services (TLSV) on the CS 1000.
- Remote Call Control (RCC) only user—when configuring RCC only users, you must enable SIP/CTI services on the CS 1000 for each user.

Table 24
CS 1000 user configuration

	Enterprise Voice CO user	Enterprise Voice NCO user	Enterprise Voice OC user	RCC only user
CS 1000	TLSV and SIP/CTI	TLSV	TLSV	SIP/CTI

Phone configuration

The following table depicts the phone configurations as determined by the Voice Mail application used for Call Forward No Answer (CFNA), Call Forward Busy (CFB), and Call Forward All Calls (CFAC). The Enterprise Voice OC user does not have a CS 1000 phone so the phone configuration is not applicable. When configuring the CS 1000 phones for Enterprise Voice CO users, Enterprise Voice NCO users, and RCC only users, you must configure the options CFNA, CFB, and CFAC to use the CallPilot DN or the Exchange Subscriber Access (SA) DN.

Table 25
CS 1000 phone configuration

	Enterprise Voice CO user	Enterprise Voice NCO user	Enterprise Voice OC user	RCC only user
Phone Call Forward No Answer	configure using CallPilot or Exchange SA DN	configure using CallPilot or Exchange SA DN	not applicable	configure using CallPilot or Exchange SA DN

	Enterprise Voice CO user	Enterprise Voice NCO user	Enterprise Voice OC user	RCC only user
Phone Call Forward Busy	configure using CallPilot or Exchange SA DN	configure using CallPilot or Exchange SA DN	not applicable	configure using CallPilot or Exchange SA DN
Phone Call Forward All Calls	configure using CallPilot or Exchange SA DN	configure using CallPilot or Exchange SA DN	not applicable	configure using CallPilot or Exchange SA DN

OC client configuration

The following section describes the OC client configuration, as determined by the Voice Mail application used for forwarding calls.

Forward calls

The following table depicts the configuration of OC client Forward Calls, as determined by the Voice Mail application used.

- Enterprise Voice Converged Office (CO) user and RCC only users:
  - — You can configure the OC client Call Forwarding ON option for each user.
  - — You can configure the Forward Call option to the CallPilot DN or the Exchange Subscriber Access (SA) DN for each user.
- Enterprise Voice Non-Converged Office (NCO) and Enterprise Voice Office Communicator (OC) users:
  - — You cannot configure the OC client Call Forwarding On option or the Forward Call option to the CallPilot DN or the Exchange Subscriber Access (SA) for Enterprise Voice NCO and Enterprise Voice OC users when using the Exchange nonintegrated with OCS or the Exchange integrated Option 1 with OCS.
  - — You can configure the OC client Call Forwarding ON option and Forward Call option to voice mail when using Exchange integrated Option 2 with OCS.

Table 26
OC client Forward Calls configuration

	Enterprise Voice CO user	Enterprise Voice NCO user	Enterprise Voice OC user	RCC only user
OC client Forward Calls—CallPilot, Exchange nonintegrated or Exchange integrated with OCS Option 1	configure using CallPilot or Exchange SA DN	not available	not available	configure using CallPilot or Exchange SA DN
OC client Forward Calls—Exchange integrated with OCS Option 2	configure using Exchange SA DN	Voice Mail option	Voice Mail option	configure using Exchange SA DN

Voice mail access

The following section describes voice mail access using a CS 1000 phone or OC client configuration.

Voice mail access using a CS 1000 phone

Enterprise Voice CO user, Enterprise Voice NCO user, and RCC only user— to access voice mail using a CS 1000 phone, you are required to dial the CallPilot or Exchange SA DNs and enter your password when prompted. The following table depicts voice mail access using a CS 1000 phone. Voice mail access is independent of the Voice Mail application used. The Enterprise Voice OC user does not have a CS 1000 phone so this capability is not applicable.

Table 27
Voice mail access with a CS 1000 phone

	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC only user
Voice mail access from phone	dial CallPilot or Exchange SA DN	dial CallPilot or Exchange SA DN	not applicable	dial CallPilot or Exchange SA DN
Log on from phone	password only	password only	not applicable	password only

Voice mail access using an OC client

The following table depicts voice mail access using an OC client, as determined by the voice mail application used.

- Enterprise Voice CO user or an RCC only user—you can access voice mail using an OC client by dialing the CallPilot or Exchange SA DNs and entering the extension and password when prompted.
- Enterprise Voice OC user and Enterprise Voice NCO user—access to voice mail using an OC client varies according to the voice mail application used.
  - — CallPilot, Exchange nonintegrated, and Exchange integrated with OCS using option 1: you can access voice mail by dialing the CallPilot DN and entering the password when prompted.
  - — Exchange is integrated with OCS using Option 2: you can access voice mail by using the Voice Mail option or by dialing the Exchange SA DN and entering the extension and password when prompted.

Table 28
Voice mail access with an OC client

	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC only user
Voice mail access—CallPilot, Exchange nonintegrated, and Exchange integrated with OCS Option 1	dial CallPilot or Exchange SA DN	dial CallPilot or Exchange SA DN	dial CallPilot or Exchange SA DN	dial CallPilot or Exchange SA DN
Log on from OC—CallPilot, Exchange nonintegrated, and Exchange integrated with OCS Option 1	password only	password only	password only	password only
Voice mail Access from OC—Exchange integrated with OCS Option 2	dial Exchange SA DN	use the Voice mail option or Dial Exchange SA DN	use the Voice mail option or Dial Exchange SA DN	dial Exchange SA DN
Logon from OC—Exchange integrated with OCS Option 2	password only	direct access or enter extension and password	direct access or enter extension and password	password only

OCS 2007 user experience

The following sections describe the user experience for OCS 2007 users when using CallPilot, Exchange nonintegrated, and Exchange integration with OCS Option 1 and Exchange integrated with OCS Option 2 as the Voice Mail application.

CallPilot, Exchange nonintegrated, and Exchange integrated with OCS Option 1

The following table depicts the user experience for OCS 2007 users. The Message Waiting Indicator (MWI) on Office Communicator (OC) is provided to the user by the OC client indicator, as shown in Figure 33 "MWI on OC client indicator" (page 116) and as a flashing envelope with a telephone in the system tray, as shown in Figure 34 "MWI on OC in system tray" (page 116).

Figure 33
MWI on OC client indicator

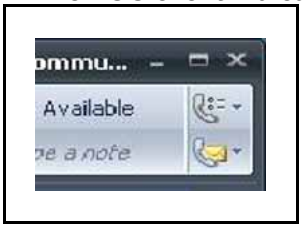


Figure 34
MWI on OC in system tray

Table 29
User experience for CallPilot, Exchange nonintegrated, and Exchange integrated with OCS Option 1

	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC only user
MWI on phone	yes	yes	not applicable	yes
MWI on OC	No for CallPilot Yes for Exchange	No for CallPilot Yes for Exchange	No for CallPilot Yes for Exchange	No for CallPilot Yes for Exchange
Outlook voice mail notification	new message in CallPilot mailbox or Outlook inbox	new message in CallPilot mailbox or Outlook inbox	new message in CallPilot mailbox or Outlook inbox	new message in CallPilot mailbox or Outlook inbox
OC client redirect	Use CallPilot or Exchange SA DN	not available	not available	Use CallPilot or Exchange SA DN
OC forward to Exchange (using voice mail option)	not available	not available	not available	not available

ATTENTION

- Calls redirected to the CallPilot DN by the Office Communicator 2007 client while in computer mode for the Enterprise Voice CO user and RCC only user are answered by the CallPilot logon prompt instead of the user mailbox greeting. For example, calls are answered with the prompt, “CallPilot from Nortel Networks. Mailbox?”.
- Calls redirected to the Exchange SA DN by the Office Communicator 2007 client while in computer mode for the Enterprise Voice CO user and RCC only user are answered by the Exchange logon prompt instead of the mailbox greeting of the user. For example, calls are answered with the prompt, “Welcome, you are connected to Microsoft Exchange”.
- The Voice Mail option is not available to the Enterprise NCO user and Enterprise Voice OC user when using Exchange Integrated with OCS Option 1.
- When using Exchange integrated with OCS, the added features as described in “Additional OC client features and capabilities using Exchange integrated with OCS” (page 110) are not available to any of the users if Option 1 is used for the integration of Exchange and OCS.
- You can experience various call-answering behaviors depending on the TLSV state. For example:
  - If the TLSV is in a ringing state, for example, a caller is waiting for you to answer, a second caller is then forwarded immediately to your voice mail.
  - If you have already answered a call, a second caller is forwarded to your voice mail after the number of rings specified by the TLSV Call Forward No Answer setting.

Exchange integrated with OCS Option 2

The following table depicts the user experience for OCS 2007 users. The Message Waiting Indicator (MWI) on Office Communicator (OC) is provided to the user by the OC client indicator, as shown in Figure 33 "MWI on OC client indicator" (page 116) and as a flashing envelope with a telephone in the system tray, as shown in Figure 34 "MWI on OC in system tray" (page 116).

Table 30
User experience for Exchange integrated with OCS Option 2

	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC only user
MWI on phone	yes	yes	not applicable	yes
MWI on OC	yes	yes	yes	yes
Outlook voice mail notification	new message in inbox	new message in inbox	new message in inbox	new message in inbox

	Enterprise Voice CO user	Enterprise Voice NCO User	Enterprise Voice OC user	RCC only user
OC client redirect	use Exchange SA DN	Voice Mail option	Voice Mail option	use Exchange SA DN
OC forward to Exchange (using voice mail)	not available	yes	yes	not available

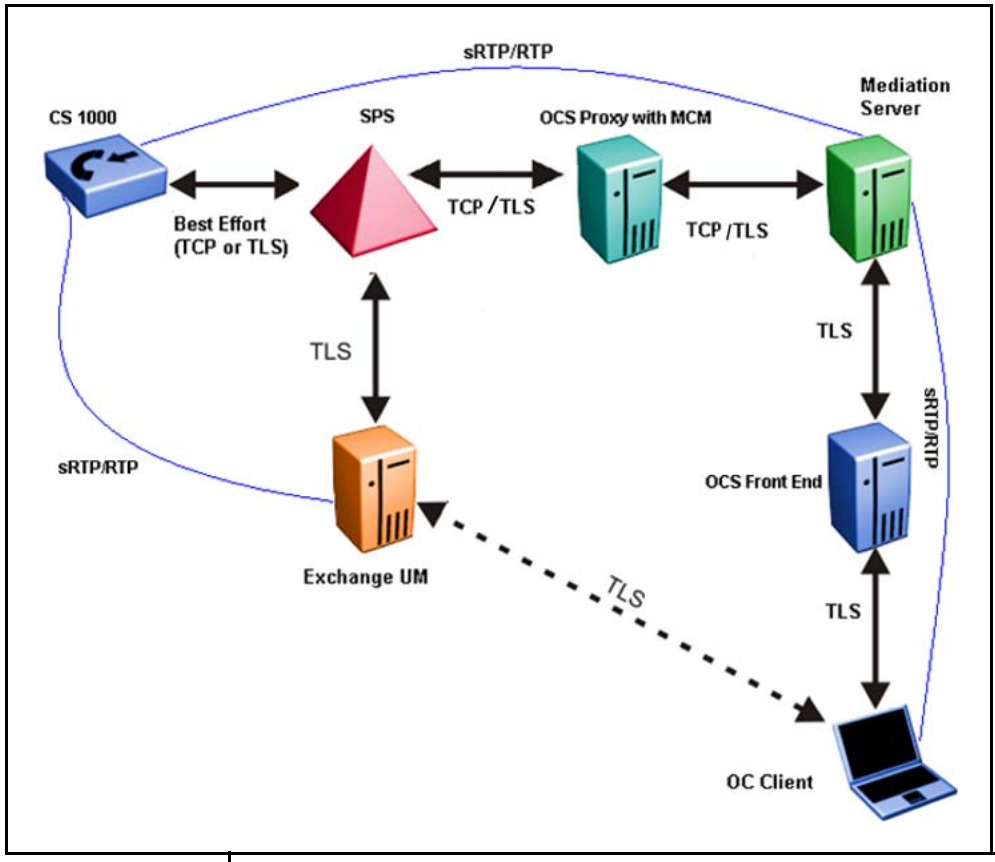
ATTENTION

- Enterprise Voice NCO user and Enterprise Voice OC user—when using the OC to redirect calls to voice mail, you must use the Voice Mail option and not the Exchange SA DN. If calls are redirected using the Exchange SA DN, calls are answered by the Exchange logon prompt instead of the mailbox greeting. For example, calls are answered with the prompt, “Welcome, you are connected to Microsoft Exchange”.
- Enterprise Voice NCO user and Enterprise Voice OC user—when the Play-on-Phone feature of Exchange 2007 is used, you must update the Play-on-Phone destination with the proper telephone number when the option is used for the first time. The default SIP URI does not work.

Signaling with integrated Voice Mail

In an integrated configuration, the Office Communicator (OC) client can select a Voice Mail option and the dialing plan is TLS secure. Element Manager has an option to allow sRTP negotiation between the CS 1000 and Exchange 2007. The following diagram depicts the signaling between OCS 2007 release 2.0, Exchange, and the CS 1000 components in an integrated configuration.

Figure 35
Signaling integrated

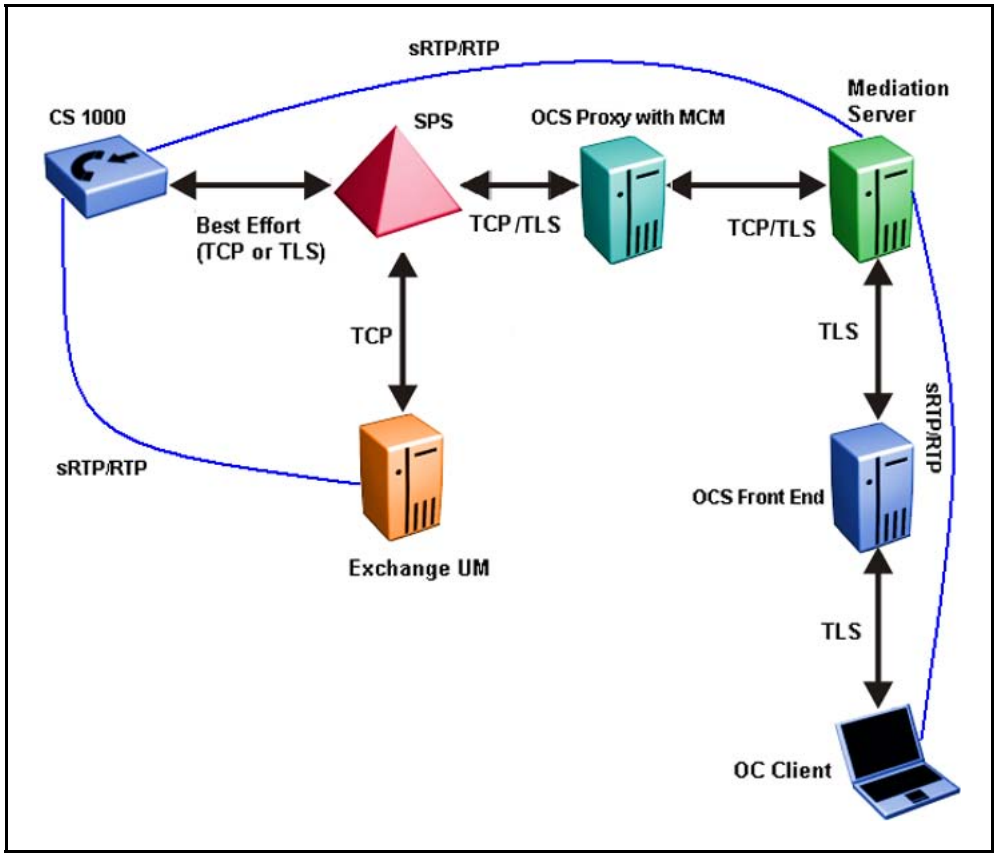


ATTENTION
After you configure a UM dialing plan with VoIP Security configured as Secured, the associated CS 1000 IP Gateway must have the Element Manager variable enabled. Failure to do so will result in calls not going through.

Signaling with nonintegrated Voice Mail

In a nonintegrated configuration, the Office Communicator (OC) client cannot select a Voice Mail option; the signaling between Exchange and the OC client is not defined. The following diagram depicts the signaling between OCS 2007 release 2.0, Exchange, and the CS 1000 components in a nonintegrated configuration.

Figure 36
Signaling nonintegrated



Installation

This chapter contains the procedures necessary to install CS 1000 components and Office Communications Server (OCS) 2007 on a CS 1000 system.

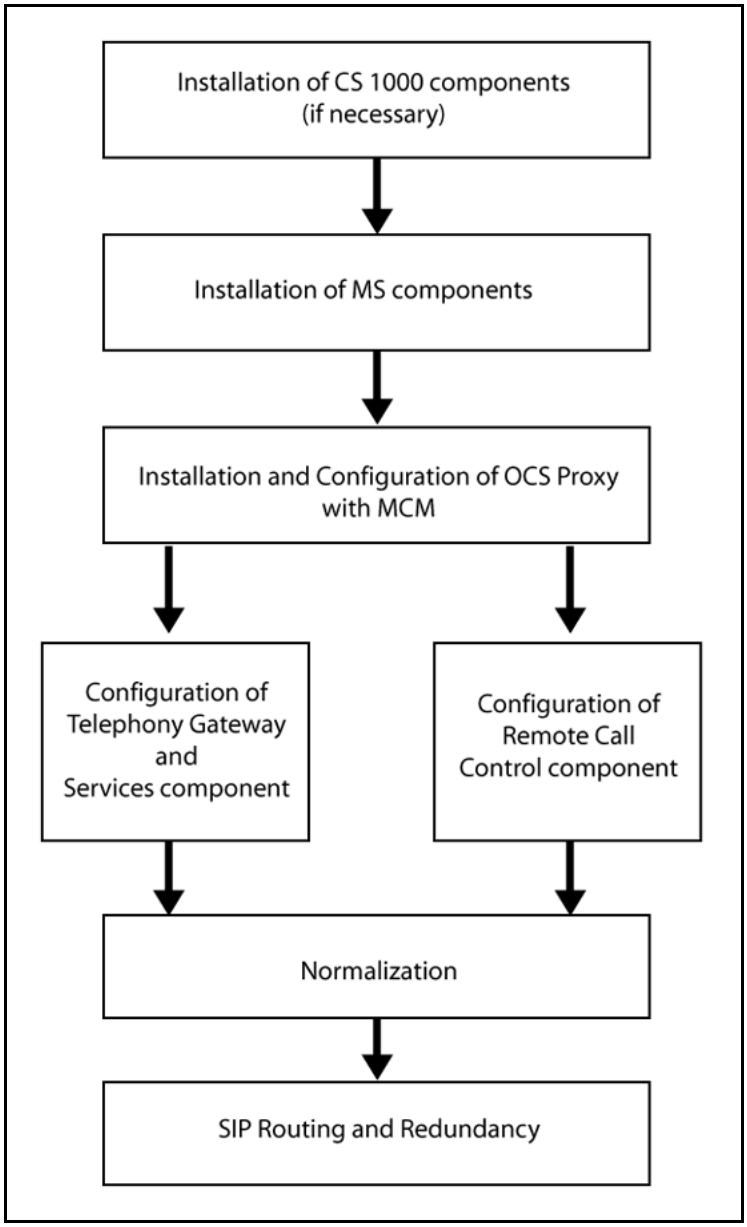
Navigation

Installation and configuration task flow

The first step is to install the necessary CS 1000 components (if you do not already have a working CS 1000 system in place), and then install the Microsoft server components. After all hardware and software is installed, you can then configure the Telephony Gateway and Services or Remote Call Control components.

After configuration is complete, normalization of telephone numbers, SIP routing, and redundancy help you integrate the Nortel and Office Communications Server 2007 domains. The following task flow illustrates this process.

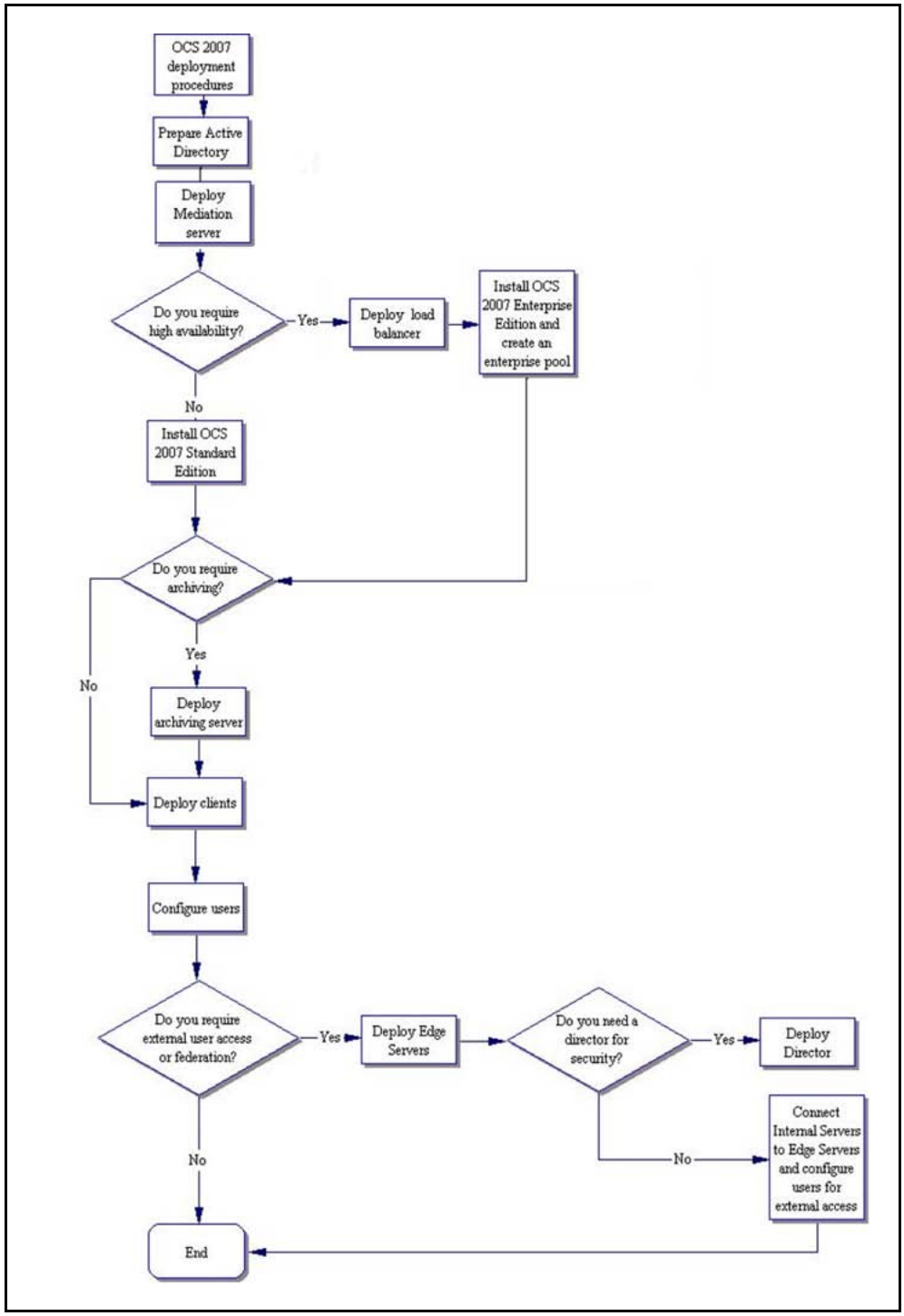
Figure 37
Installation and configuration flow



OCS 2007 installation preparation and deployment

The following task flow depicts the high-level topics required to deploy OCS 2007. After your internal deployment is complete, you can then deploy Edge Servers for external user access.

Figure 38
OCS 2007 installation preparation and deployment task flow



CS 1000 and Signaling Server installation

The first step in the installation and configuration process is to install the CS 1000 and Signaling Server.

Installing the CS 1000 system

To install and configure a CS 1000 system, see the following documents:

- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *CS 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)

ATTENTION
Converged Office requires the Call Server and Signaling Server to have Release 6.0 installed.

See the Nortel Converged Office Product Bulletin to ensure that you are using the most current versions of the Call Server and Signaling Server PEPs.

Installing the Signaling Server

The Signaling Server must be installed. If it is not installed, see *Signaling Server Installation and Commissioning* (NN43001-312).

For information about configuring the Signaling Server, see "Signaling Server checklist" (page 324).

OCS 2007 component installation

After all CS 1000 components are installed, go to the Microsoft Web site www.microsoft.com for information about installing the OCS components, beginning with the Active Directory.

ATTENTION
The following is a list of the required patches for the Microsoft OCS 2007 installation:

- OCS 2007 – Standard Edition RTM KB 942872Version 6362.0 plus hotfix
- Description of the Office Communicator 2007 hotfix package: December 17, 2007 KB 943083Version 2.0.6362.36
- Description of Office Communications Server 2007, Unified Communications Managed API v1.0 Redist: December 17, 2007KB 944285Version 3.0.6362.36
- Description of the Update for Office Communication Server 2007, Mediation Server: December 17, 2007KB 943086 Version 3.0.6362.36

- OCS Application Proxy Server: OCS 2007 – Standard Edition RTMKB 942872Version 6362.0 plus hotfix

Microsoft SR1 RTM documentation can be obtained from the Microsoft Web site. Go to www.microsoft.com.

Prerequisite OCS 2007 information

The following section describes the prerequisite information.

Active Directory

The Office Communications Server 2007 and Office Communicator 2007 environment have a strong dependency on Active Directory to authenticate, authorize, provision, and configure Office Communications Server 2007.

With the OC 2007 client, Active Directory supplies the enterprise address list to facilitate search-based lookups.

Ensure that you install Active Directory in accordance with Microsoft documentation. For more information about Active Directory planning, see *Office Communications Server 2007 Document: Active Directory Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Office Communications Server (OCS) 2007 Enterprise Pool

OCS 2007 Enterprise Edition is designed for large-scale deployment where multiple Office Communications Server Enterprise Edition servers are deployed as a pool, typically behind a load balancer. Servers in the pool share a central SQL back end database server that stores user data.

If your pool consists of more than one server, a Load Balancer is required. If your pool consists of only one server, which is connected to a separate SQL back end database server, a Load Balancer is not required.

OC clients register on an Enterprise pool. The client user is directed to a specific server within the pool by a hardware load balancer that distributes the load to these servers. Static data, such as contact lists and access control lists (ACLs), are stored as persistent data on the back end database server.

A client can have multiple concurrent connection instances and can register on multiple servers at the same time. Each device to which the client is logged on (called an endpoint) can be connected through a different server at the same time.

The load balancer exposes a single Virtual Internet Protocol (VIP) address that is used by the clients to access the pool. Each Enterprise Edition server within the pool is responsible for connection processing, security and authentication, protocol processing, and server applications. The user data resides in the back end database server. The database contains records that hold static data and dynamic user data (such as endpoints and active descriptions for a user). The database runs a set of stored procedure calls that form the core of the operational software. Office Communications Servers within the pool are networked to the back end database server using a high-speed network. These Office Communications Servers also run User Replicator (UR) software to provide a connection to the Microsoft Active Directory service so that user account information can be synchronized between the back end database server and the Active Directory.

For more information about Office Communications Server 2007 Enterprise Edition, see the *Office Communications Server 2007 Document: Enterprise Edition Deployment Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Installing the OCS Proxy server (R1)

The following section describes the OCS Proxy server installation procedures.

Step	Action
1	On the Windows **Start** menu, choose **Run**.
2	Navigate to the C:\Office Communications Server_Eval\se_eval\setup\i386\ folder.
3	For OCS Standard Edition: server.msi SERVER=PROXY SKU=SE **OR** For OCS Enterprise Edition: server.msi SERVER=PROXY SKU=EE A new Windows wizard opens prompting you to install the Forwarding Proxy. You must complete all the steps in the wizard before continuing.
4	Activate the proxy server using the command line (from Office Communications Server_Eval\StandardEdition\setup\i386 folder): Activate on domain: **`lcscmd /server /password:`** <password> **`/action: activate /role:proxy`** Activate on workgroup: **`LcsCmd.exe /server /action:activate /role:workgroupProxy /password`** <password> **OR** For Office Communications Server Enterprise Edition: Activate on domain: **`lcscmd /server /user:`** <user>

/password:<password> /action: activate /role:proxy
Activate on workgroup: **lcsCmd.exe /server /user: <user> /password:<password> /action:activate /role:workgroupProxy**

The user is the service user on the domain that is used by the OCS Proxy service. You can enter any user and password.

> ***Note:*** For the TLS connection between the OCS Front End and the OCS Proxy with MCM, the Activate on workgroup option must be used.

5 Type **Exit** on the command line.

6 Run the Installation wizard and select the defaults.

7 To get Proxy to appear in OCS, navigate to Admin tools/Computer Management and select **Services and applications**.

8 Select Microsoft Office Communications 2007 and then Proxy (for example, ocs2007a-proxy.ocs2007a.corp.nortel.com.

--End--

Installing the OCS Proxy server (R2)

The following procedure describes the OCS Proxy server installation for OCS R2.

Step	Action
1	On the Windows **Start** menu, choose **Run**.
2	Navigate to the installation OCS R2 installation source directory on the hard drive or CD/DVD drive.
3	Log on as Administrator.
4	On the network drive, the installation procedure starts from the installation directory.
5	Change the directory by typing **cd:\setup\amd64**.
6	To install the VC++ Redistributable package, type the command **vcredist_x64.exe** and follow the prompts on the screen to complete the installation.
7	Return to the amd64 directory, install NET Framework 3.5 by typing the command **dotnetfx35.exe** and following the prompts on the screen to complete the installation.

8 Restart the computer if prompted to do so to complete the .NET framework installation.

9 Return to the amd64 directory after restarting the computer and install the native SQL client by typing **`sqlncli_x64.msi`** and following the prompts on the screen to complete the installation.

10 Change to the subdirectory by typing cd:\Setup.

11 To install the UCMA redistributable package, type **`run ucmaredist.msi`**. If the Run program security warning pop-up appears, click **Run**.

> **ATTENTION**
> You are not informed when the installation is complete; however, the screen disappears when installation is finished.

12 To install the OCS R2 core components, type ocscore.msi. If the Run program security warning pop-up appears, click **Run**. Follow the prompts on the screen to complete the setup.

13 To install the OCS R2 proxy role, type server.msi SERVER=PROXY SKU=SE and press enter. The OCS proxy installation screen appears. Click **Next**.

The OCS Proxy installation screen appears.

14 Click **Next**.

15 Enter Product key and click **Next**.

16 Specify the location where the Proxy is to be installed and click **Next**.

17 Follow the steps for activating the OCS Proxy, as shown in Step 4.

18 Type **`exit`** and install the MCM.

--End--

Installing the Load Balancer

The following section describes the Load Balancer installation procedures. For more information, see *Load Balancing Microsoft Office Communication Server 2007 in an Expanded Topology for Application Switch Technical Configuration Guide* (NN48500-561).

Step	Action
1	Go to the **Start** menu and select **Settings**.
2	Select **Network Connections**.

3 Select **TCP/IP properties** and add DNS server IP. For example, 47.11.108.50.

4 Go to **My Computer**, right-click and select **System Properties**.

5 Enter the Computer Name of each FE server. For example, ocs-fe-1.

6 Click domain. For example, ocs2007a.corp.nortel.com.

7 Restart server.

--End--

Installing MCM

The following section describes the MCM installation procedures.

Prerequisite MCM information

- Ensure MS Windows Server 2003 operating system is installed with SP1 or R2.
- Ensure the OCS Proxy server is installed.
- Uninstall previous versions of MCM (if any previous versions exist).
  - — Stop MCM service. On the MCM management console window and from the **Actions** menu, select **Stop**.
  - — Use the Windows **Add/Remove Programs** utility to uninstall MCM.
- To use the Use an existing account option, you require a domain user account and password to install the MCM. The domain user account is a member of the local groups RTC Server Applications and Group. The user account must also have full control permissions on the MCM folder. For example, c:\program files\Nortel\MCM.
- To use the Create a new account option, you can log on to the server with a user ID and permissions to create users in the Active Directory
- To create a new account during the MCM installation, the new user is added to all the necessary groups automatically by the MCM.

Step	Action
1	To install the MCM software, run the MCM Installation wizard.
2	Select **Use an existing account** and enter your user ID and password **OR** select **Create a new account**.
3	Open the MCM Console window and select the **Actions** menu.

4 On the **Actions** menu, choose **Start** to start the MCM service.

--End--

MCM must be installed on the OCS Proxy Server. See “MCM menu options” (page 158) for more information about using the MCM menu options.

MCM has two main components: **MCM Service**, which handles call processing, and **MCM Management Console**, which interfaces with the MCM Service component for configuration, administration, and maintenance.

Configuration

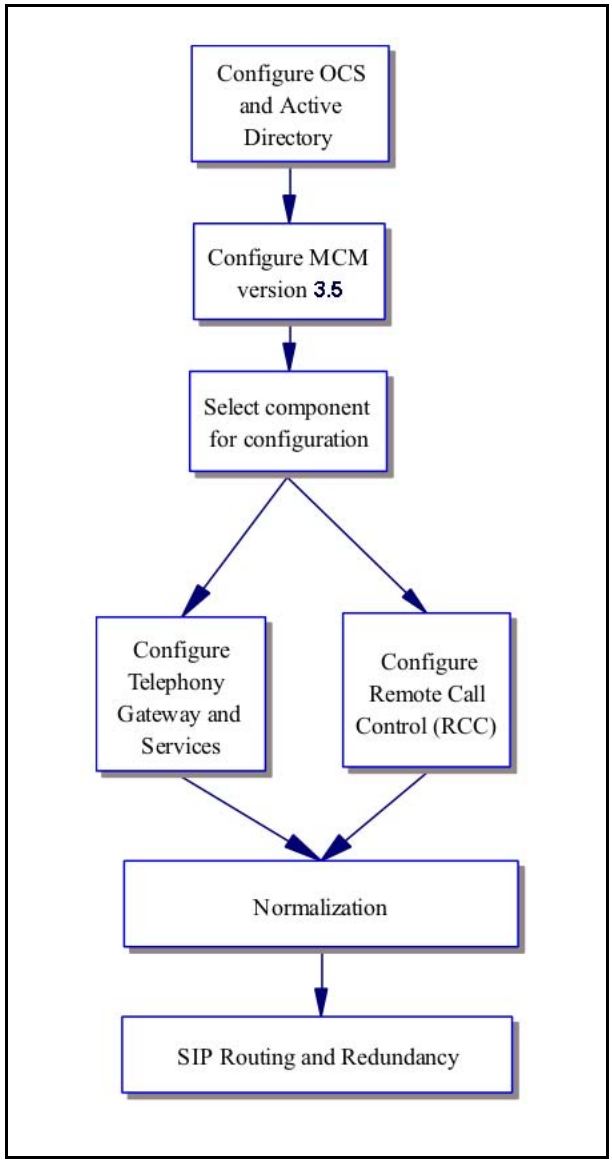
This chapter contains the procedures necessary to configure the CS 1000 components and Office Communications Server (OCS) 2007 on a CS 1000 system.

Navigation

Configuration task flow

The following task flow illustrates the configuration order of the components.

Figure 39
Configuration task flow



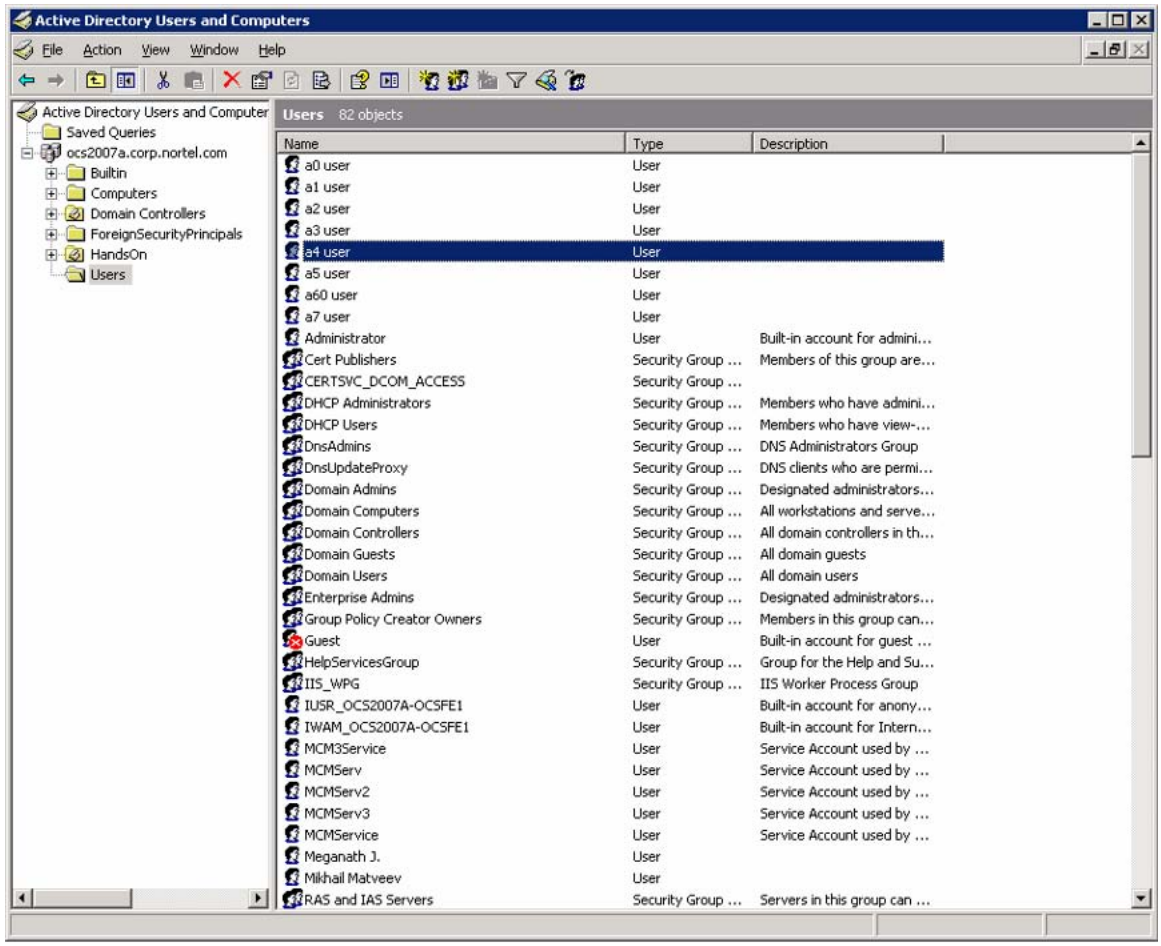
Active Directory configuration

Active Directory configuration takes place in the Active Directory Users and the Computers (ADUC) window. Selecting the Users folder reveals the list of users as depicted in Figure 40 "Active Directory (Microsoft LDAP server)" (page 133). All users are defined in this folder.

By default, MCM uses GC LDAP server which contains partial information about all objects in the Active Directory domain forest. It requires replication from all Domain controllers to the GC domain controller to be performed after changes are made in the Active Directory User configuration **Active Directory Sites and Services** snap-in.

ATTENTION
All CS 1000 phones must be added in the Active Directory even when there is no Office Communicator user associated with the CS 1000 phone. The administrator can create a user account with the Enterprise Voice and PBX Integration enabled in the Active Directory for every CS 1000 phone. For example, a lab phone or a lobby phone. Some feature interactions will apply. See "Active Directory configuration" (page 89) in the Feature Interactions section.

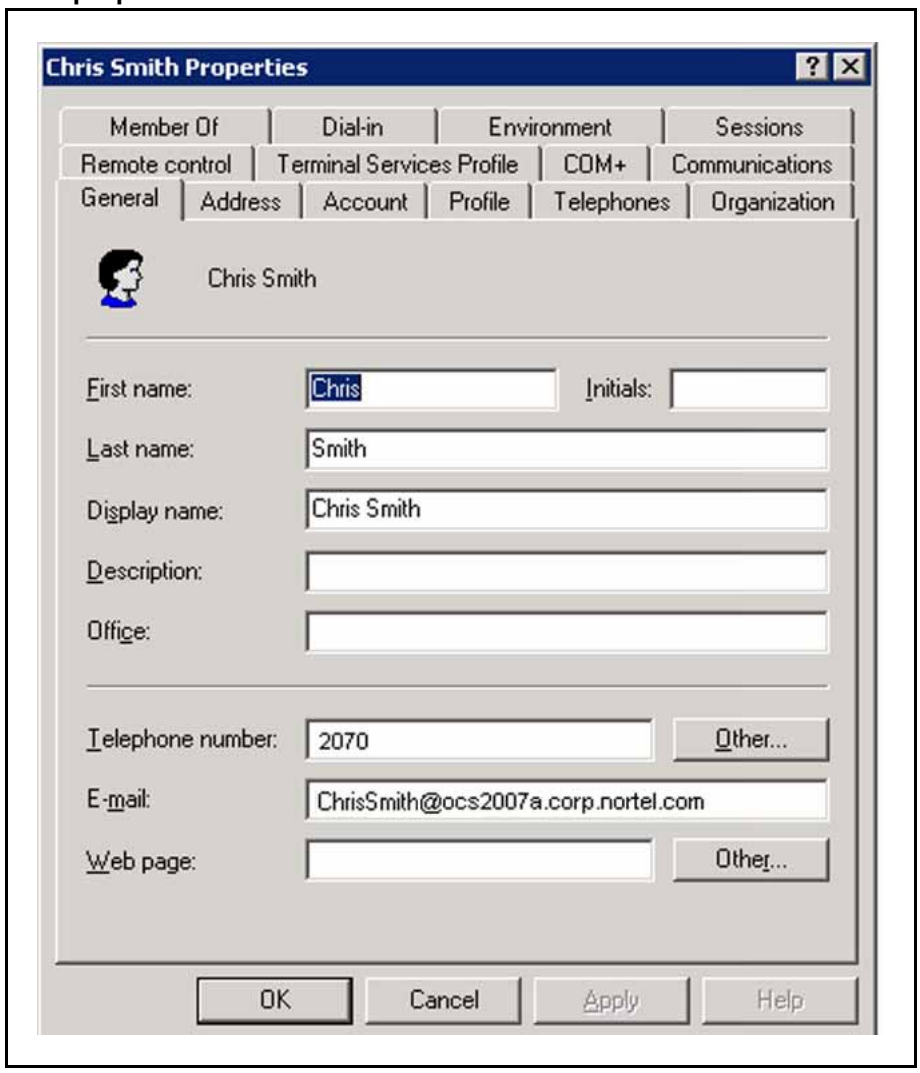
Figure 40
Active Directory (Microsoft LDAP server)



Defining users

Step	Action
1	Select a user from the list in the Users folder.
2	Right-click the user, and select **Properties**.
3	The Properties window opens, as shown in the following figure.

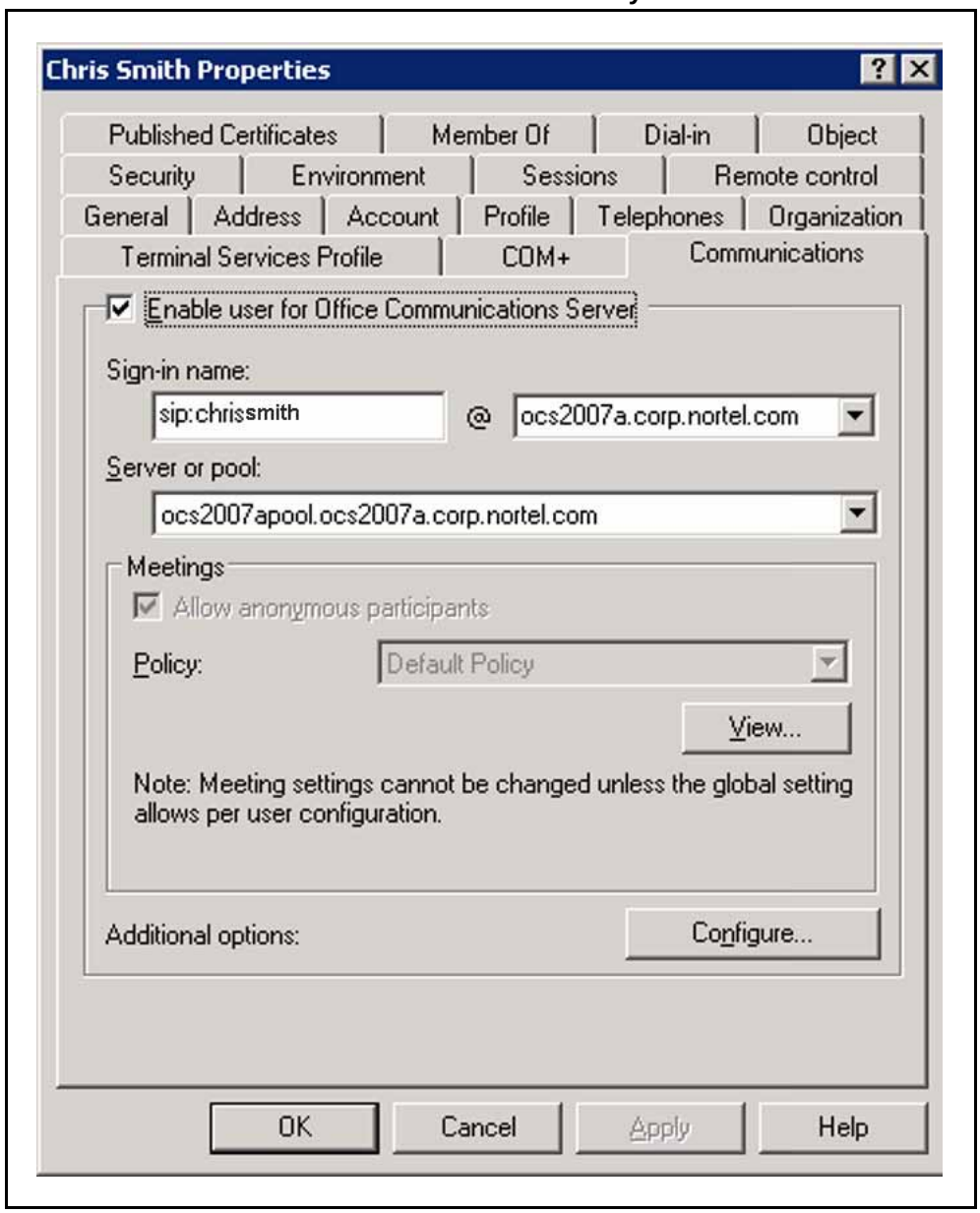
Figure 41
User properties



4	Enter the user information (first name, last name, telephone number, and so on) in the appropriate fields in the **General** tab.
5	Select the **Communications** tab.
6	Click the check box next to **Enable user for Office Communications Server**.

7 In the fields provided, define the user **Sign-in name** and the **Server or pool**). Office Communicator 2007 uses these addresses to place calls.

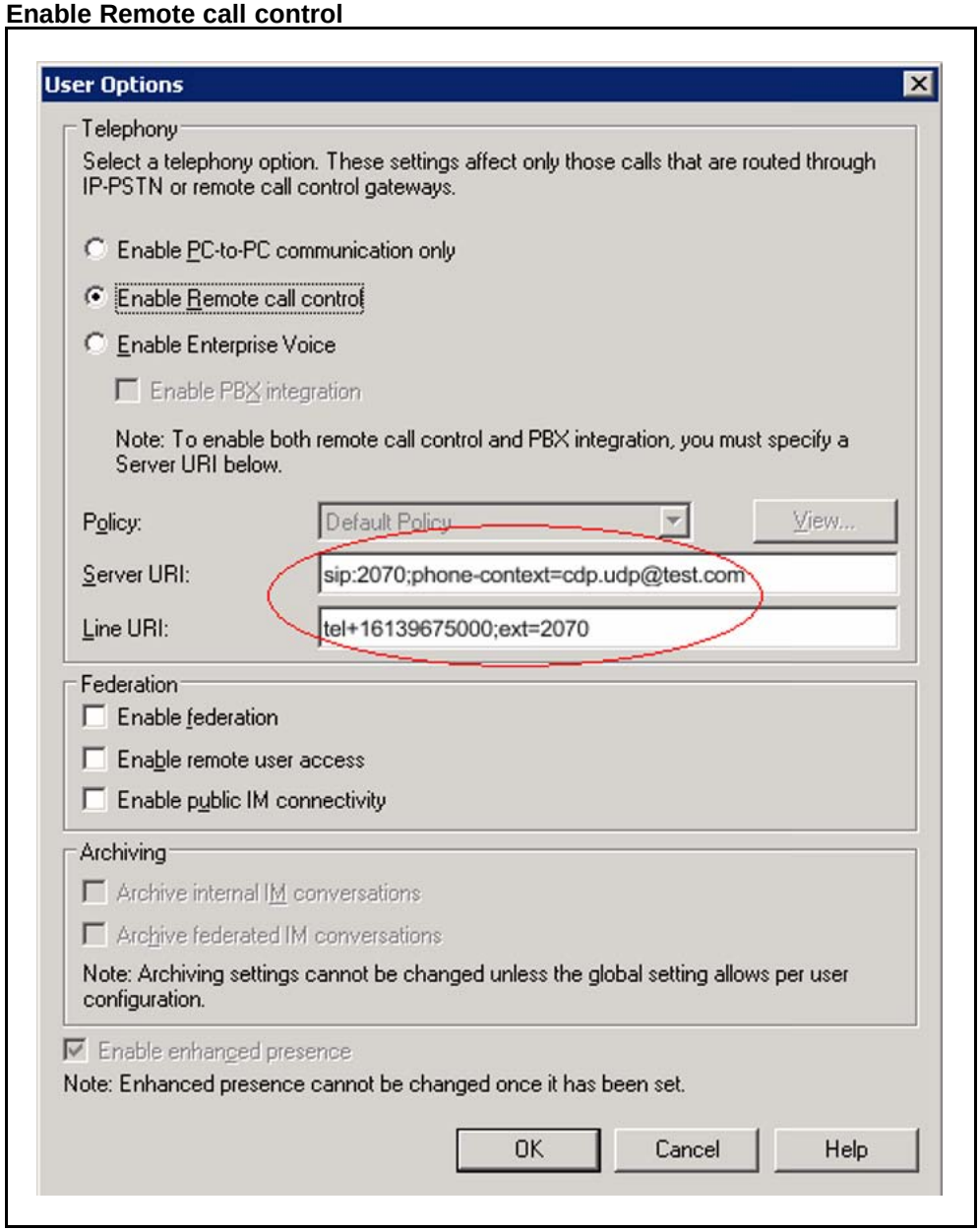
Figure 42
Enable Office Communications Server connectivity for a user in Active Directory



8 Click the **Configure** button.

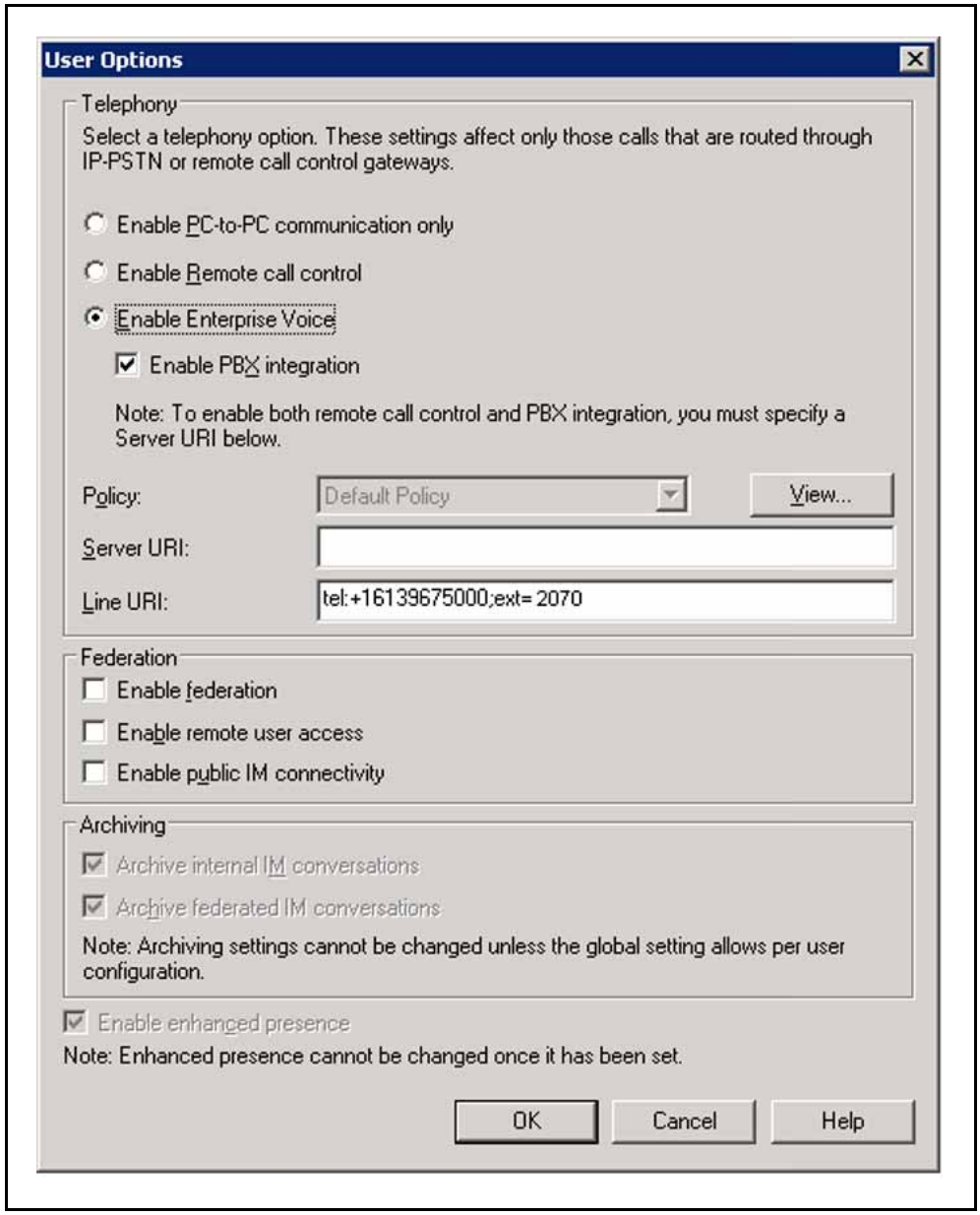
9 For enabling Remote Call Control only, select **Enable Remote Call Control** and configure the Server URI and Line URI, as shown in the following figure

Figure 43
Enable Remote call control



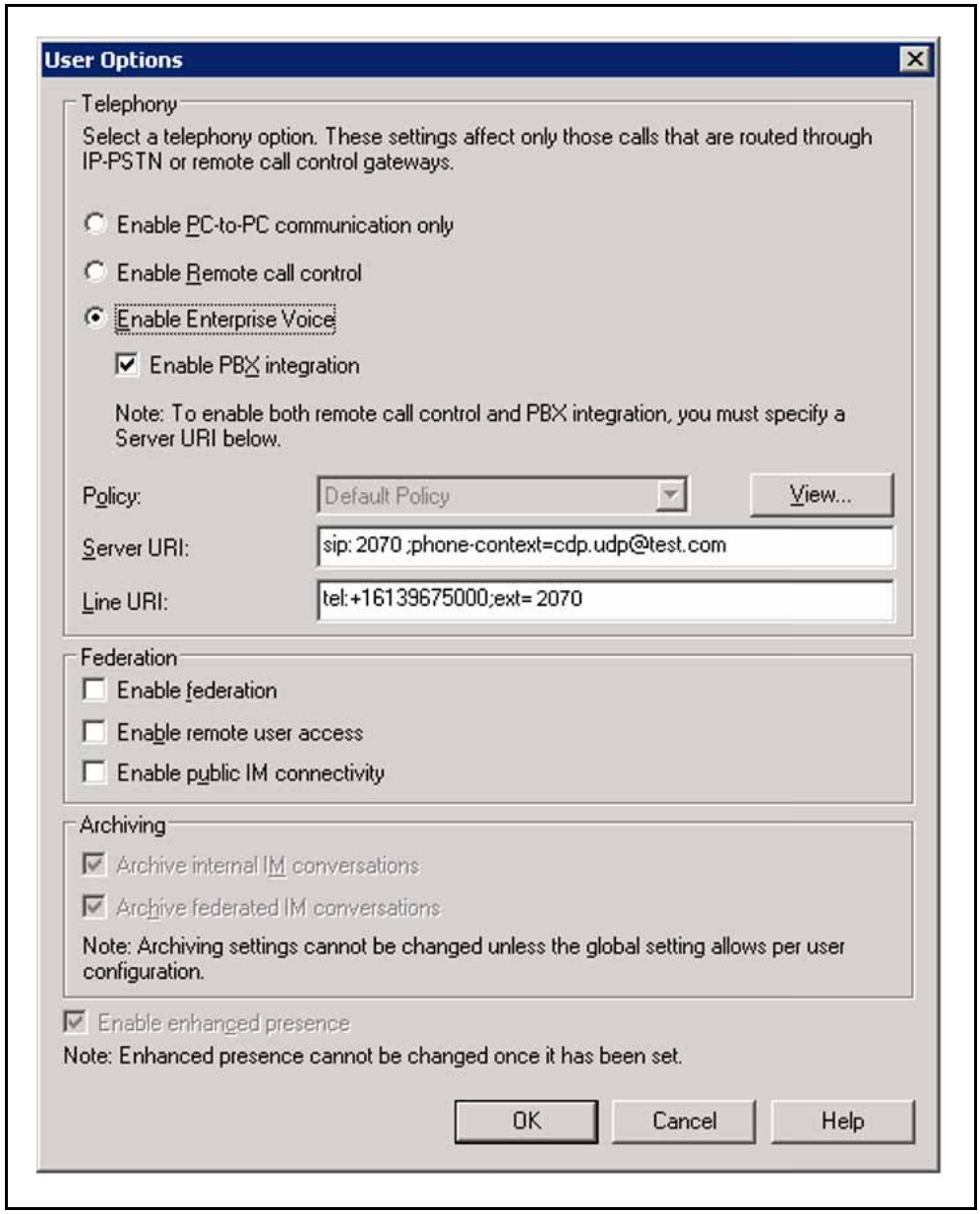
10 For enabling Enterprise Voice and PBX integration only (without RCC), select **Enable Enterprise Voice** and the **Enable PBX integration** check box, as shown in the following figure.

Figure 44
Enable Enterprise Voice and PBX integration



11 For enabling both Remote call control and Enterprise Voice, you must select **Enable Enterprise Voice** and the **Enable PBX integration** check box and specify the Server URI, as shown in the following figure.

Figure 45
Enable both RCC and Enterprise Voice



12 Specify the MCM/App Proxy FQDN in the Server URI field. This must be in the format of sip:CDP or UDP;phone-context=CDP domain or UDP domain@MCM/APP Proxy FQDN. For example:

- Sip:2070;phone-context=cdp.udp@test.com – CDP format
- Sip:3432070;phone-context=udp@test.com – UDP format

Specify the URI of the user's telephone in the Line URI field. The Line URI must be in the format tel:E164;ext=CDP or UDP. For example:

- tel:+16139675000;ext=2070 – CDP format
- tel:+16139672070;ext=3432070– UDP format.

ATTENTION
It is important to note that the chosen numbering plan must be applied to the TLSV and MCM configurations.

--End--

Office Communications Server configuration

The starting point for Telephony Gateway and Services configuration is the Office Communications Server 2007 component.

Load Balancer configuration

The pool of Front End servers is organized to process inbound and outbound traffic. The role of the Load Balancer in this architecture is to route incoming SIP-messages to the less busy server on the base of configured algorithm. Load Balancer's VIP-address is used by clients as a single point of connection to the pool. This address is listed in DNS and has a FQDN. Internal OCS clients require a DNS server to establish connection with an Enterprise Edition Pool.

Configuring Voice Properties

When introducing telephony support to an OCS 2007 the following OCS FE entities must be configured:

Step	Action
1	Location profiles. A location profile defines all phone numbers that can be dialed from a named location. A location contains one or, typically, more normalization rules. Normalization rules should be defined in the Location Profile to convert the dialstrings to the E.164 International format for all types of PSTN calls. For example, NXX, NPA and International. For all calls using private dialing plan (CDP or UDP), normalization rules must be defined in the Location Profile to convert the dialstrings to the Line URI format. For example, E.164;ext=xxxxxxx format.
2	Normalization rules. Normalization rules are .NET regular expressions that define a phone number pattern. A set of normalization rules associated with a particular location constitute a location profile.
3	Phone usage records. A phone usage record specifies a class of call (internal, local, long distance, or whatever) that can be made by various users, or groups of users, in an organization.

4 Voice policy. A voice policy associates one or more phone-usage records with one or a group of users.

5 Route. A voice route associates target phone numbers with particular IP-PSTN gateways and phone usage records. Source-based routing must be used for CS 1000 and OCS 2007 integration.

6 Define users and enable their Voice and RCC capabilities.

--End--

Voice mail must always be configured on the CS 1000 and not Office Communicator. Configuring communication to the CS 1000 gateway is performed at the Mediation Server.

Dual forking is configured based on OCS Voice Policies, which in turn may be applied globally or on a per user basis. For more information about configuring Voice Policies, see *Microsoft Office Communications Server 2007 Enterprise Voice Planning and Deployment Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Enabling dual forking–globally

Step	Action
1	Click **Forest** and then **Properties**.
2	Select **Voice Properties** in the OCS management console.
3	Under **Global Policy**, select the desired policy and click **Edit**. This policy will be applied for all users.
4	In the **Edit Policy** window, click the **Allow simultaneous ringing of phones** box.

--End--

Enabling dual forking–by user

When applying voice policies on a per user basis, dual forking can be enabled for the user by selecting an appropriate policy.

Step	Action
1	Click **Forest** and then **Properties**.
2	Select **Voice Properties** in the OCS management console.

3 Under **Use per user policy**, select the desired policy and click **Edit**. This policy will be applied on a user basis.

4 In the **Edit Policy** window, click the **Allow simultaneous ringing of phones** box.

5 Go to Users in the OCS configuration console.

6 Select a user and click **Properties**.

7 In the properties window, click **Additional Options configure**.

8 Select the desired policy.

--End--

Applying policy

Step	Action
1	In the **User Options** window, click **Enable Enterprise Voice**.
2	Select **Another Policy**. The policy can be assigned simultaneously to several users using the Configure Users wizard.

--End--

OCS configuration procedures

Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Configuration of Static Routes

Configuration of the Office Communications Server involves the configuration of static routes and host authorization.

You must configure static routes between the client and server. For information about configuring static routes (Enterprise Edition pool behind a Load Balancer), see *Office Communications Server 2007 Administration Guide* and the *Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

Host Authorization and Routing configuration

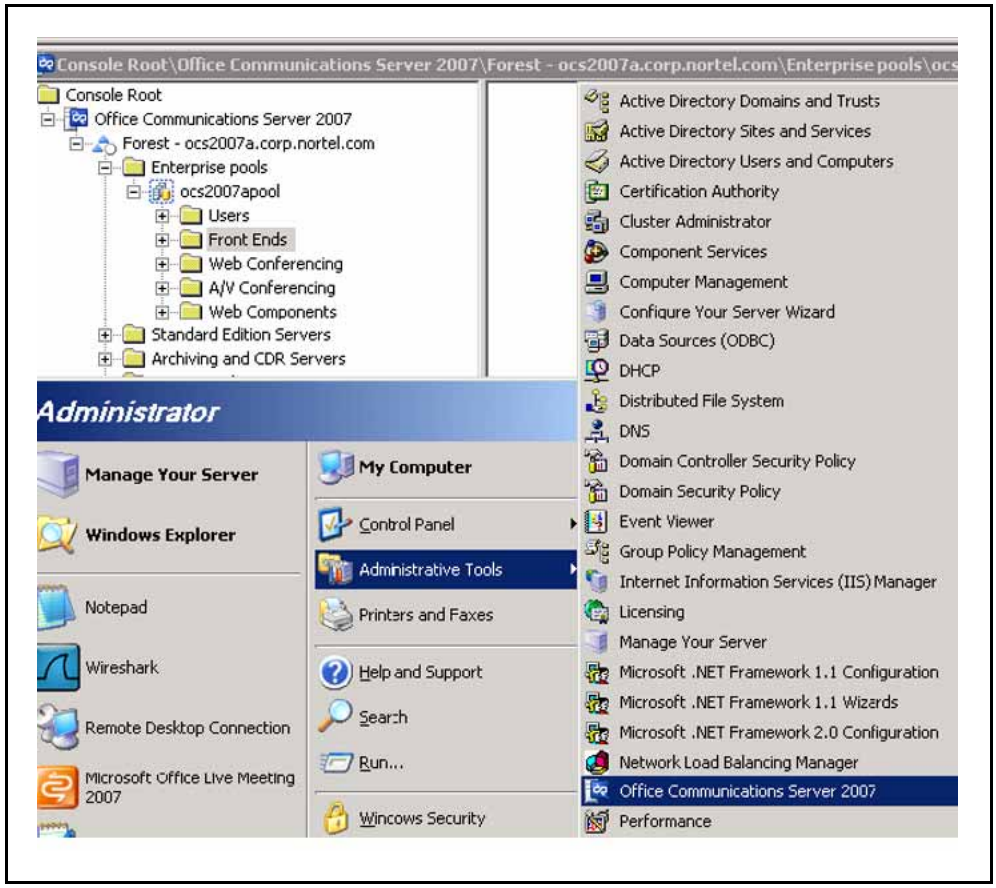
For one Office Communications Server to communicate with another Office Communications Server, each server must have authorization to speak to the other. The Host Authorization tab, as depicted in Figure 47 "Office Communications Server Front Ends" (page 143) is where you establish this authorization.

The Host Authorization tab, located in the OCS Proxy with MCM is where all the CS 1000 endpoints are configured. These endpoints must be configured as authorized endpoints in the OCS Proxy with MCM. Configure the CS 1000 IP addresses which, in turn, talk to the Office Communications Server. The same authorization must take place for both OCS to OCS authorization and OCS to CS 1000 authorization.

Configuring the Host Authorization and Routing for the OCS Front End server

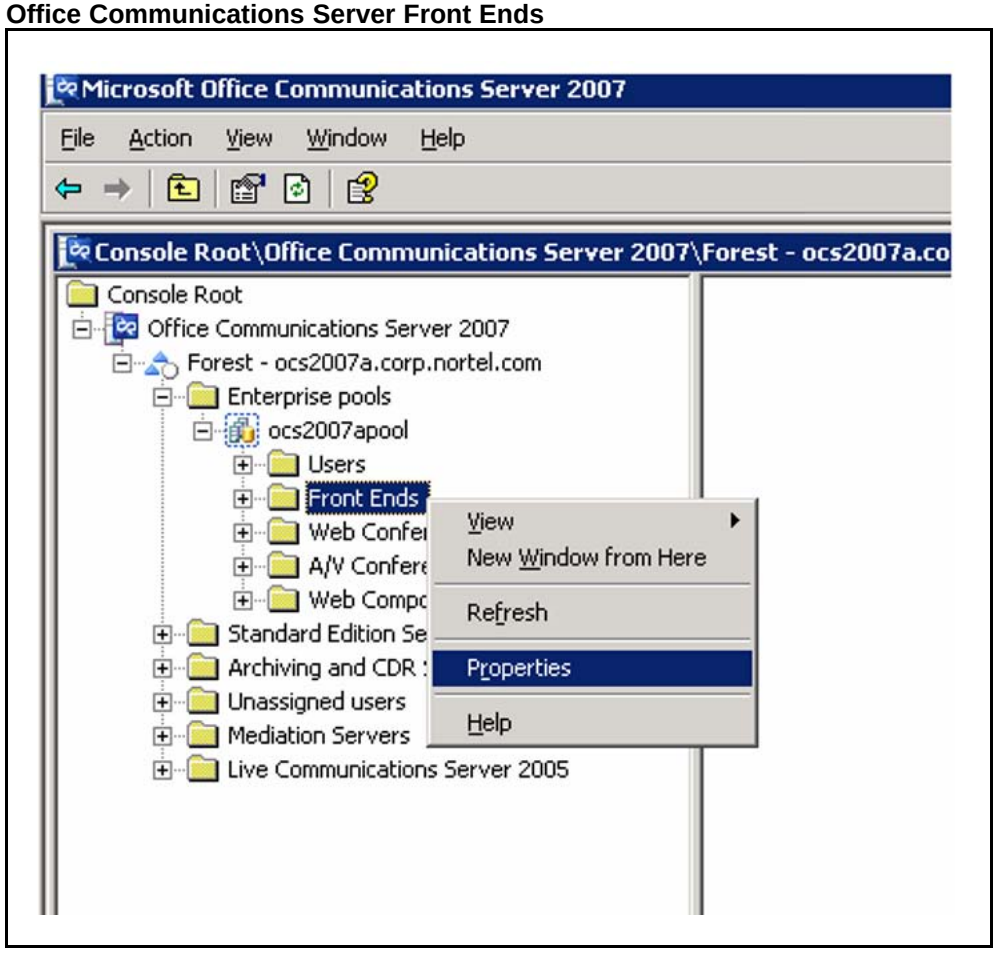
Step	Action
1	Open Office Communications Server (accessed from the Windows server that runs the OCS server), as shown in the following figure. Click the **Start** menu and then select **Administrative Tools, Office Communications Server 2007**.

Figure 46
Opening Office Communications Server



2	Click the Office Communications Server (the server to which you want to add Host Authorization and change the Routing), right-click **Front Ends** and choose **Properties**. See Figure 47 "Office Communications Server Front Ends" (page 143).

Figure 47
Office Communications Server Front Ends



3 Click the **Host Authorization** tab and click **Edit** .

4 In the Server section, click the **IP Address** button and enter the IP address of the OCS Proxy server. For details, see Table 32 "Routing rules" (page 149).

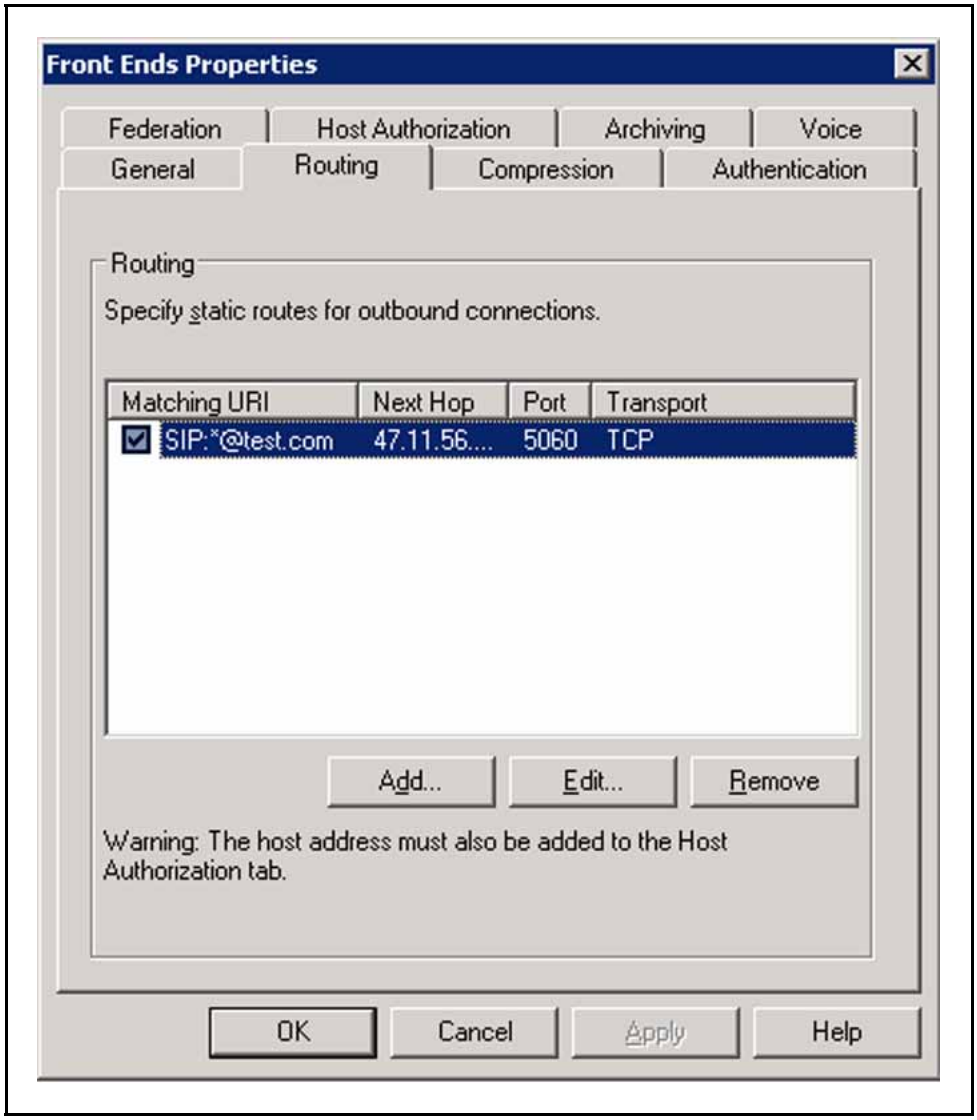
5 In the Settings section, select **Throttle As Server** and the **Treat as Authenticated** check boxes.

6 Click **OK**.

7 On the Routing tab of the Front End server, a Routing rule is defined to route the SIP message in which the Request URI matches the Server URI as defined in the Active Directory for each user to the OCS Proxy server where MCM runs.

For an example, see Figure 48 "Routing tab" (page 144).

Figure 48
Routing tab



8 In the Add Static Route window, For Domain: enter the domain defined in the Server URI. For Next Hop: enter the IP address of the OCS Proxy.

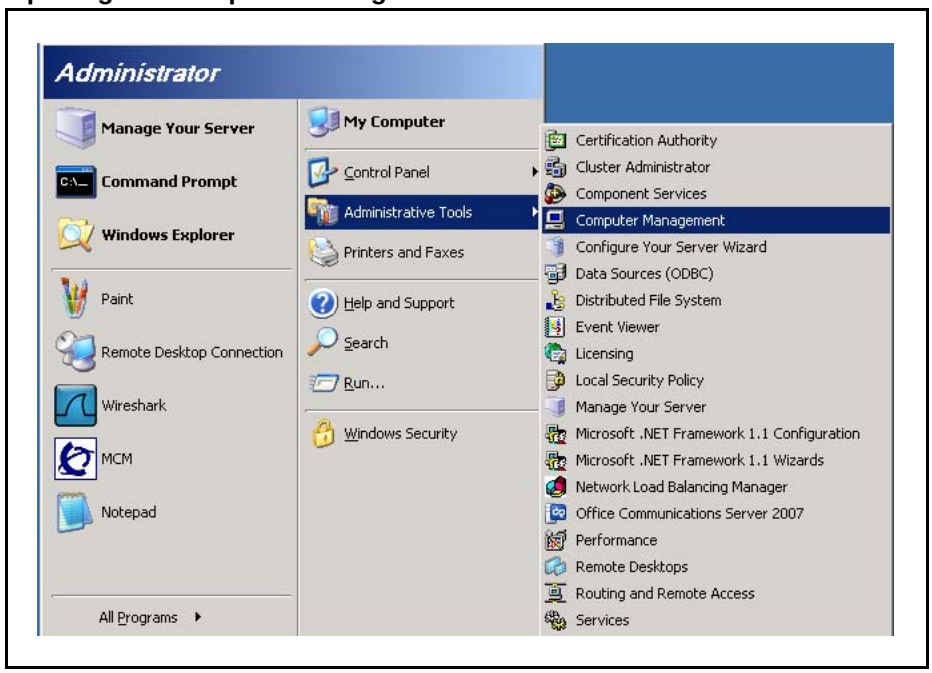
--End--

Configuring host authorization for the OCS Proxy

For each OCS Proxy with MCM, Host Authorization is required for the Node IP address of all CS 1000 servers that the Office Communications Server interacts with, as well as the TLAN IP address of the Primary, Secondary, and all possible collaborative NRS.

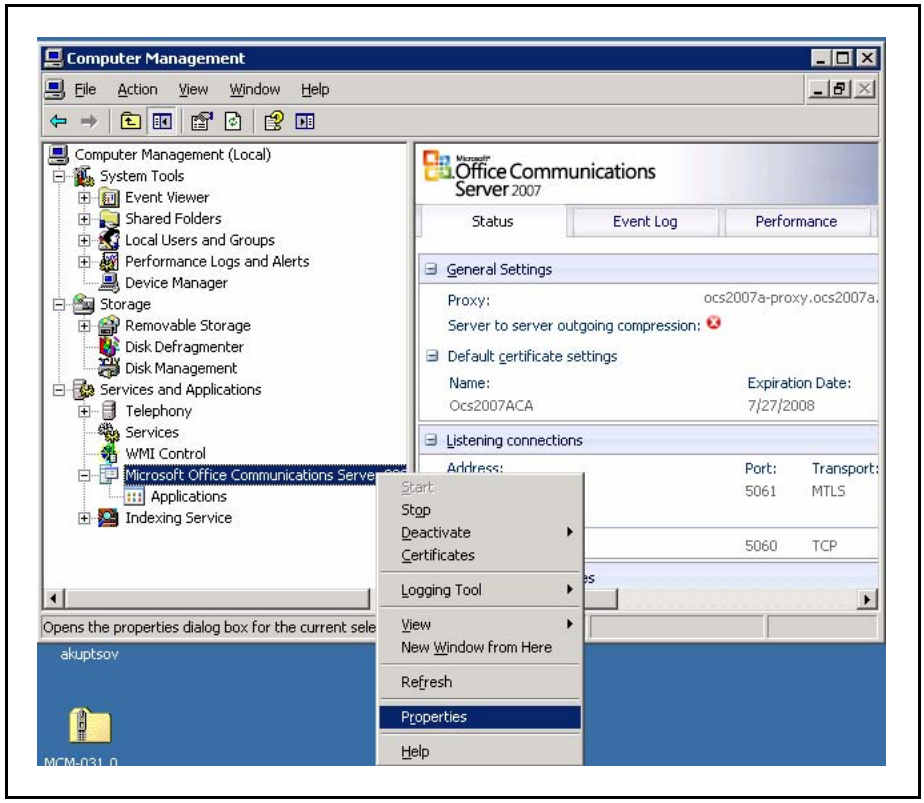
Step	Action
1	Open the OCS Proxy server, click the Windows **Start** button, point to **Administrative Tools**, and then click **Computer Management**.

Figure 49
Opening the Computer Management console



2	Choose Microsoft Office Communications Server and right-click to select **Properties**.

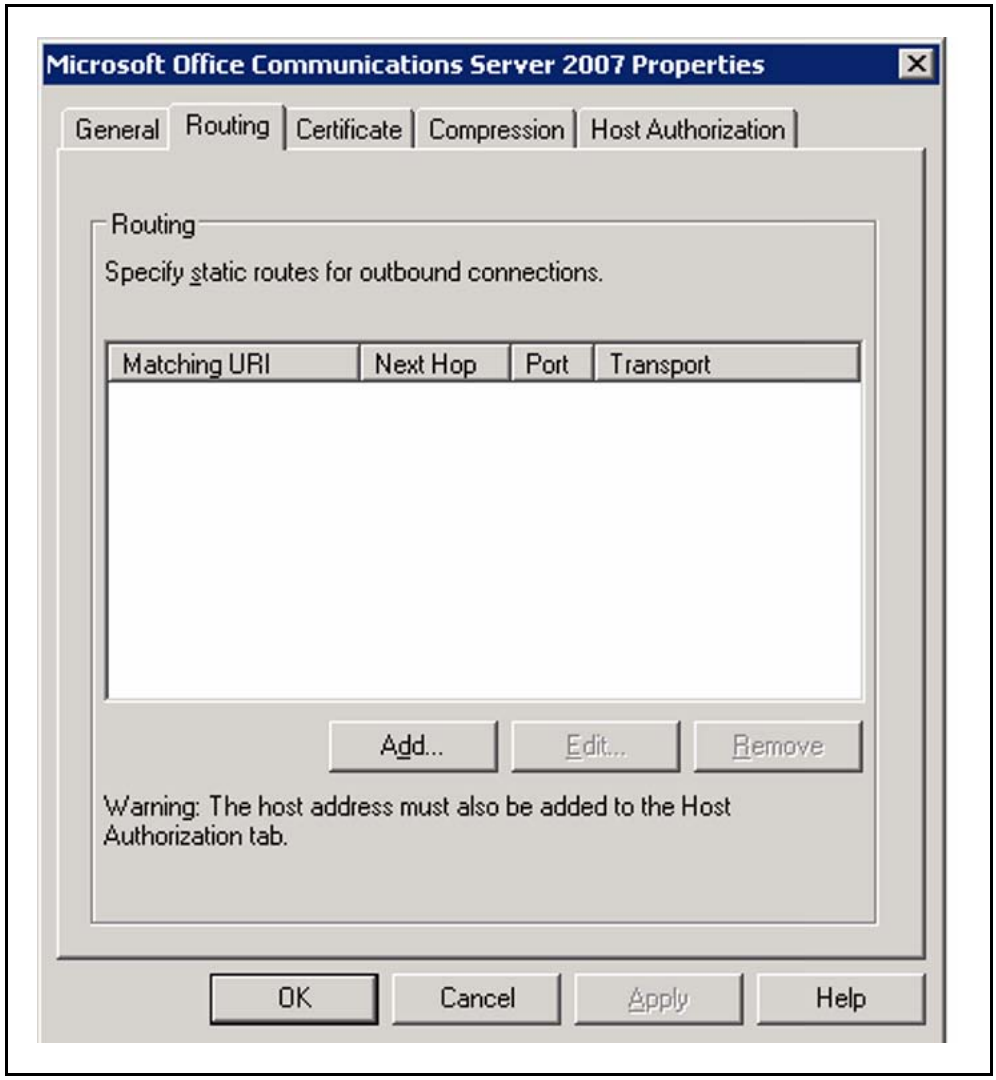
Figure 50
Office Communications Server Management Console



3 For the OCS Proxy, no static route is required. MCM routes inbound calls to the proper Mediation Server based on the Routing Table settings on the MCM.

4 Click the **Routing** tab to confirm no route is configured.

Figure 51
Routing tab

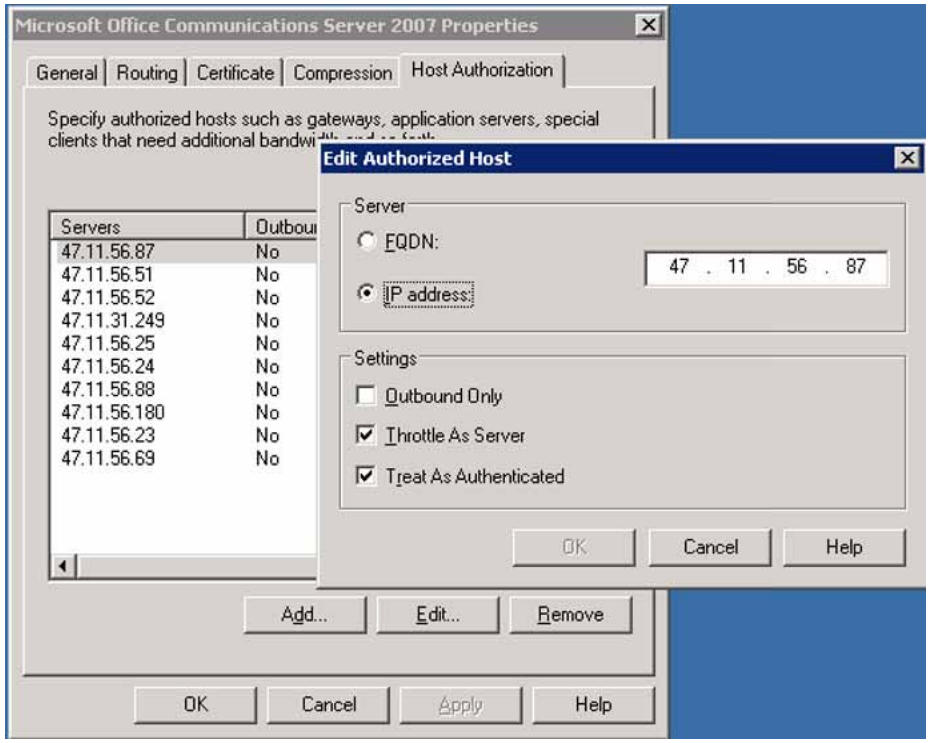


5 Click the **Host Authorization** tab.

6 Click **Edit** to open the Edit Authorized Host window.

7 In the Edit Authorized Host window, enter the **IP address**, select both the **Throttle As Server** and **Treat As Authenticated** check boxes, and then click **OK**. The IP addresses that require authorization on the OCS Proxy are the Node IP addresses of all the CS 1000 systems in the network, IP address of the NRS (SRS or SPS), all the IP addresses of the OCS Front End servers, IP addresses of the Mediation Servers, and the IP addresses of all Front End Servers. For more details, see Table 32 "Routing rules" (page 149).

Figure 52
Edit Authorized Host



--End--

The following table shows a number of possible configurations of OCS 2007 and the required entries for each. The transport to CS 1000 is TCP for all configuration types.

Table 31
OCS Servers Routing and Host Authorization Summary

	OCS Front End Servers Pool	OCS Mediation Server	OCS Proxy Server
Routing	Domain: OCS Proxy Server FQDN Next hop IP: IP Address of the OCS Proxy Server Transport: TCP Port: 5060 Phone URI: No	None	None

	OCS Front End Servers Pool	OCS Mediation Server	OCS Proxy Server
	Replace host in request URI: No		
Host Authorization	• IP Address of the OCS Application Proxy Server Outbound Only: No Throttle as Server: Yes Treat as Authenticated: Yes	None	• NRS/SPS IP Address • Signaling Server Node IP Address • All IP Addresses of Mediation Servers • IP Address of all Front End Servers

Table 32
Routing rules

Config. type	Component	Host Auth.	Destination	User/ Domain	Phone URI	Transport	Port
1. Single Front End server and single OCS Proxy. All TCP	Front End server	OCS Proxy IP	OCS Proxy IP	<domain name>	No	TCP	5060
	OCS Proxy	Front End server IP					
		SPS/SRS IP					
		Node IP					
		Mediation Servers IP					
2. Single Front End server and single OCS Proxy. SIP CTI TLS	Front End server	OCS Proxy FQDN	OCS Proxy FQDN	<domain name>	No	TLS	5061
	OCS Proxy	Front End server FQDN					
		SPS/SRS FQDN					

Table 32
Routing rules (cont'd.)

Config. type	Component	Host Auth.	Destination	User/ Domain	Phone URI	Transport	Port
		Node FQDN					
		Mediation Servers IP					
3. Pool of Front End servers and Single OCS Proxy. All TCP	Front End servers Pool	OCS Proxy IP	OCS Proxy IP	<domain name>	No	TLS	5061
		Load Balancer IP					
	OCS Proxy	Front End servers IP					
		Load Balancer IP					
		SPS/SRS IP					
		Node IP					
		Mediation Servers IP					
4. Pool of Front End servers and Single OCS Proxy. SIP CTI TLS	Front End server Pool	OCS Proxy FQDN	OCS Proxy FQDN	<domain name>	No	TLS	5061
	OCS Proxy	Pool FQDN					
		SPS/SRS FQDN					
		Node FQDN					
		Mediation Servers IP					

Table 32
Routing rules (cont'd.)

Config. type	Component	Host Auth.	Destination	User/ Domain	Phone URI	Transport	Port
5. Single Front End server and Pool of OCS Proxies, All TCP	Front End server	Proxy Load Balancer IP	Proxy Load Balancer IP	<domain name>	No	TCP	5060
		OCS Proxies IP	Load Balancer IP	CS 1000 SIP address	NO	TCP	5060
	OCS Proxies	Front End server IP					
		Proxy Load Balancer IP					
		SPS/ SRS IP					
		Node IP					
		Mediation Servers IP					
6. Single Front End server and Pool of OCS Proxies, SIP CTI TLS	Front End server	Proxy Load Balancer FQDN	Proxy Load Balancer FQDN	<domain name>	No	TLS	5061
	OCS Proxies	Front End server FQDN					
		Proxy Load Balancer FQDN					
		SPS/SRS FQDN					
		Node FQDN					
		Mediation Servers IP					

Table 32
Routing rules (cont'd.)

Config. type	Component	Host Auth.	Destination	User/ Domain	Phone URI	Transport	Port
7. Pool of Front End servers and Pool of OCS Proxies. All TCP	Front End server Pool	Proxy Load Balancer IP	Proxy Load Balancer IP	<domain name>	No	TCP	5060
		Front End Load Balancer IP					
		OCS Proxies IP					
	OCS Proxies IP	Front End servers IP					
		Proxy Load Balancer IP					
		Front End Load Balancer IP					
		SPS/SRS IP					
		Node IP					
		Mediation Servers IP					
8. Pool of Front End servers and Pool of OCS Proxies. SIP CTI TLS	Front End servers Pool	Proxy Load Balancer FQDN	Proxy Load Balancer FQDN	<domain name>	No	TLS	5061
	OCS Proxies	Proxy Load Balancer FQDN					

Table 32
Routing rules (cont'd.)

Config. type	Component	Host Auth.	Destination	User/ Domain	Phone URI	Transport	Port
		Front End Load Balancer FQDN (Pool FQDN)					
		SPS/SRS FQDN					
		Node FQDN					
		Mediation Servers IP					

Configuring a Mediation Server

Use the following procedures for configuring a Mediation Server.

WARNING
The Microsoft configuration procedures in this document are provided for your convenience and are based on Microsoft OCS technical documentation. For more information about configuring OCS and the most recent configuration instructions, go to www.microsoft.com.

Step	Action
1	Log on to a Communications Server 2007 Mediation Server.
2	Click **Start**, point to Administrative Tools, and then click **Office Communications Server 2007**.
3	Expand the appropriate forest node.
4	Expand the Mediation Servers node, right-click the Mediation Server to be configured, click **Properties**, and then click the **General** tab.
5	In the FQDN box, make sure the FQDN listed matches that of the Mediation Server you have selected.
6	Open a command prompt, change to the root directory, and type **`nslookup`** and (FQDN of the server) using the FQDN displayed on the Mediation Server General tab, and then press Enter.
7	From the list of IP addresses displayed in the Communications Server listening IP address list, select the IP address returned in Step 6. If the IP address selected, does not match the IP address in Step 6, Communications Server traffic will be directed

toward an interface that is not listening for such traffic and away from the one that is.

8 From the list of two IP addresses displayed in the Gateway listening IP address list, select the other IP address (can be a media gateway or the Communication Server 1000).

9 From the A/V Edge Server list, select the A/V Edge Server that hosts the A/V Authentication Service for this Mediation Server.

10 In the Default location profile list, select the default location profile for this Mediation Server

11 In Media port range accept the default range of 60,000 to 64,000.

12 Click the **Next Hop Connections** tab.

13 On the Next Hop Connections tab under Office Communications Server next hop. In the FQDN list, select the FQDN of the next-hop internal server. This server could be a Director or pool. In the Port box, accept the default of 5061 for TLS.

14 On the Next Hop Connections tab under PSTN Gateway next hop. In the IP address box, specify the IP address of the OCS Proxy where the MCM runs. In the Port box, accept the default of 5060 for TCP.

15 Click OK.

--End--

MCM configuration

The Multimedia Convergence Manager (MCM) is a software component provided by Nortel to enable voice connectivity between CS 1000 clients and the Office Communications Server (OCS) 2007 clients. MCM consists of the following modules:

- Call Processing Service
- Management Console

The MCM Call Processing Service handles the Session Initiation Protocol (SIP) telephony traffic between the CS 1000and the Office Communications Server. The Management Console provides real-time status of the MCM, Office Communications Server, Primary Network Routing Service (NRS), and Secondary NRS. It also provides Administrative, Maintenance, and Configuration tools.

Office Communications Server 2007 provides multimedia and collaboration features such as Video, Internet Messaging (IM), Presence, White Board, Application Sharing, and Voice over Internet Protocol (VoIP) capability. MCM enables SIP VoIP connectivity between the CS 1000and the Office

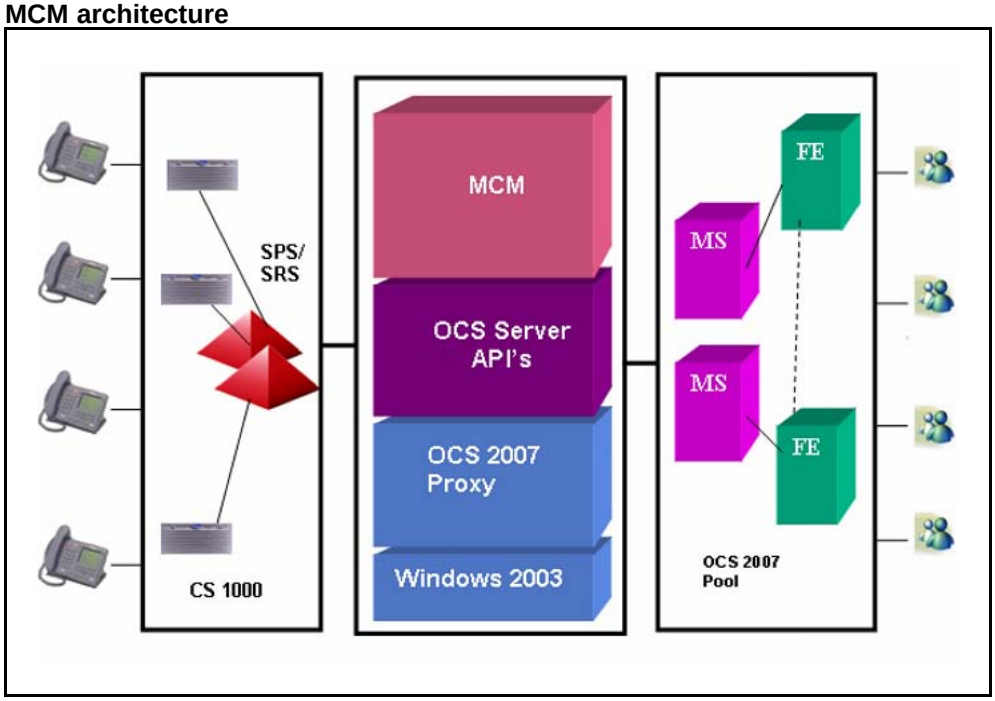
Communications Server 2007 and TR/87 authorization functionality required for the Office Communicator (OC) 2007 Remote Call Control capability.

Telephones in a CS 1000 system can make direct SIP calls to OCS clients when the dialed number maps to a corresponding user's Line URI using LDAP queries to the corporate Active Directory. MCM also allows Office Communications Server clients to originate ESN and trunk calls to corporate and external users.

MCM architecture

The MCM is situated between the Mediation Server and the CS 1000. The MCM must run on top of the OCS Proxy server with Windows 2003 as depicted in the following figure.

Figure 53
MCM architecture



The following examples illustrate how MCM handles call information. Understanding the role of MCM in the Telephony Gateway and Services component helps you to determine the configuration.

Example 1: Outgoing calls from Office Communicator

In this example, an invite travels from the client to the OCS Front End server, and then to the Office Communications Server MCM Proxy through the Mediation Server. MCM checks which NRS is active, and then sends an invite to that SIP Redirect Service (SRS). In this case, the invite is

qualified. To return from the SRS, 302 is used. The invite is then sent unqualified to the CS 1000associated with the originator's location code and DN.

Example 2: Incoming calls to Office Communicator

In this example, the user has a desktop telephone and a Telephony Services (TLSV) that points to an Office Communications Server 2007 server. The TLSV sends a DN or Routing DN. The call was originally made to 6 231 3052, but the TLSV hot key is configured with 6 344 5000. This is a dummy routing DN; it can be configured with all hot keys in the network.

In a CDP network, the dummy routing DN (for example, 6 231 3052) must also be configured by a DSC (for example, 8200). The DSC is configured on the NRS as a routing entry for the MCM Gateway endpoint.

The call is routed to the NRS. The invite is sent to the NRS, which returns a 302, and the CS 1000 sends an invite to the MCM Proxy. At this stage, the invite includes a special header called x-nt-ocn that contains the actual number called. Use this header to compare against the Active Directory map for the user's Line URI. This method is used to prevent you from having to program the for each user to determine the correct DN upon which to terminate the call. The MCM then routes this call to the proper Mediation Server based on the SIP GW ID provided in the INVITE and the Routing Table configured on the MCM.

You need not configure each user. Configure only the routing DN, and the header is automatically injected to identify the called party.

MCM Direct configuration

For small CS 1000 deployments (without NRS), MCM supports Direct configuration. In this mode, MCM sends an invite from the client directly to the CS 1000 node IP address specified in the MCM configuration. MCM does not check CS 1000 availability in Direct mode configuration.

For more information about the various MCM configuration fields, see Figure 55 "MCM configuration window" (page 160).

MCM management console

The following list contains possible statuses for the various MCM components:

- MCM

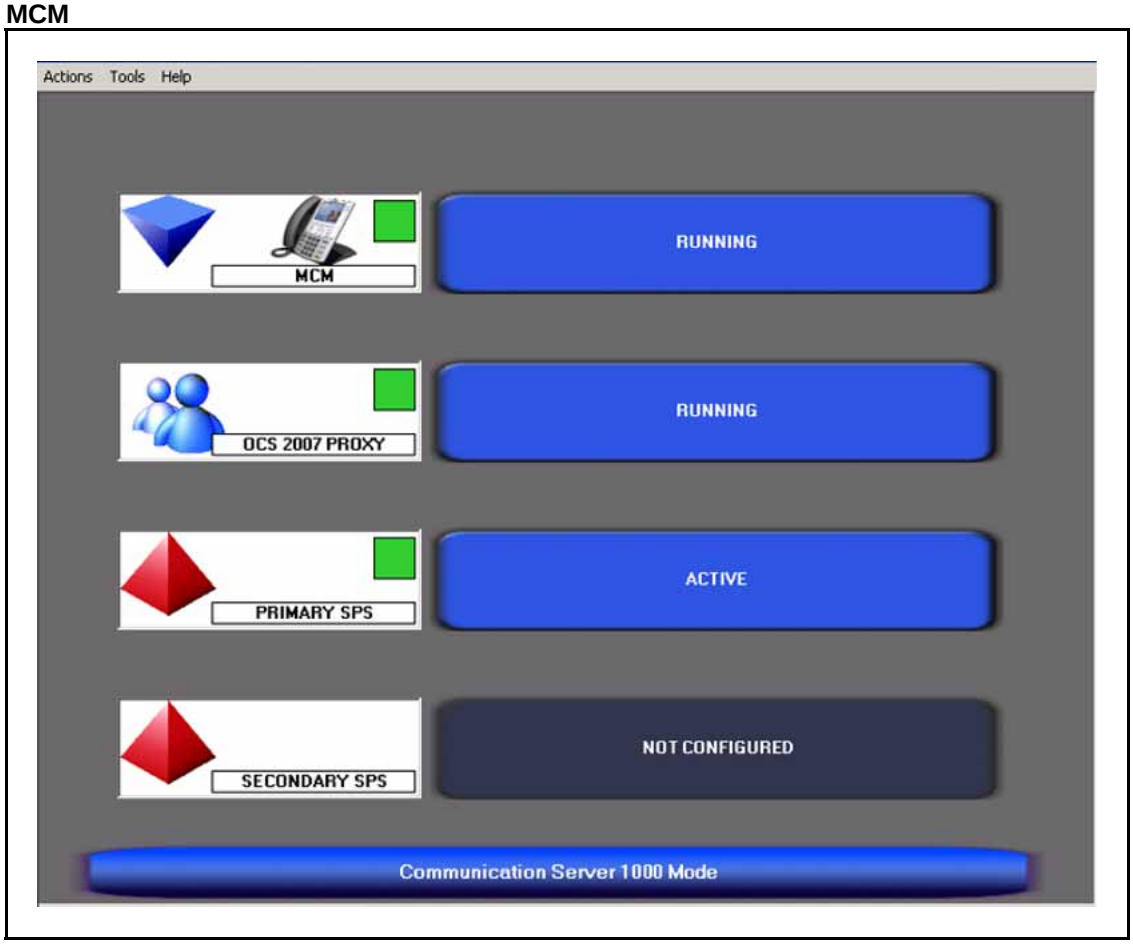
- Running
- Pending
- Stopped

- OCS
  - Running
  - Pending
  - Stopped

- Primary SRS/SPS (the IP address of the Primary SRS/SPS server)
  - Active - Primary SRS/SPS is active. All messages are sent through the Primary NRS.
  - Standby - Primary SRS/SPS is alive. The Secondary SRS/SPS is active.
  - Not responding - Primary SRS/SPS is not responding. For normal processing, the Secondary SRS/SPS must be switched to an Active state.
  - Unknown - An unknown response is received by the SRS or SPS.

- Secondary SRS/SPS (the IP address of the Secondary SRS/SPS server)
  - Active - Secondary SRS/SPS is active, which is possible only if the Primary SRS/SPS is down.
  - Standby - Secondary SRS/SPS is alive, which is the normal state if the Primary SRS/SPS is active.
  - Not responding - Secondary SRS/SPS is not responding. You cannot switch to it.
  - Unknown - An unknown response is received by the Secondary SRS or SPS.

Figure 54
MCM



MCM menu options

The following describes the function of each MCM menu command:

- Actions
  - Start - start MCM service
  - Stop - stop MCM service
  - Restart - stop and start MCM service
  - Exit - close current GUI for MCM service

- Tools
  - Configuration
  - Active Calls Count
  - Active Directory Query
  - Backup

- Restore
- Set Log Level

- Help
  - Get help and general information about MCM

MCM command line parameters

The MCM console application can be run with command line parameters to configure some advanced settings. The following parameters are available.

Parameter	Description and example
/h	show help about using command line parameters For example: MCMConsole.exe /h
/MedSrvHealthCheck	enable/disable Mediation server health checking process For example: MCMConsole.exe /MedSrvHealthCheck:true
/Remove100rel	indicate whether the 100rel from Supported header needs to be deleted For example: MCMConsole.exe /Remove100rel:true
/VoIPChange	allow a change of the anonymous FROM header value to another specified number. For example: MCMConsole.exe "/VoIPChange:<sip:anonymous@anonymous.invalid><sip:+1234567777@domain.com;user=phone>
/RCCChange	allow a change of the RCC anonymous calling number to another specified number. For example: MCMConsole.exe "/RCCChange:<tel:anonymous><tel:+1234567777>

ATTENTION
/VoIPChange and /RCCChange parameters can be used repeatedly to create mapping table. Use these two parameters to resolve most scenarios that involve double pop-ups when there is a call from an unknown user. See example, as shown below.

Unknown calling number example

If the calling number is unknown, Office Communicator cannot merge VoIP and RCC pop-ups into one pop-up.

In the following scenario, if you have:

- VoIP address: sip:anonymous@anonymous.invalid
- RCC number: <tel:anonymous>

The mapping must be defined on the MCM as:

- MCMConsole "/VoIPChange:<sip:anonymous@anonymous.invalid><sip:+1234567777@domain.com;user=phone>
- MCMConsole "/RCCChange:<tel:anonymous><tel:+1234567777>

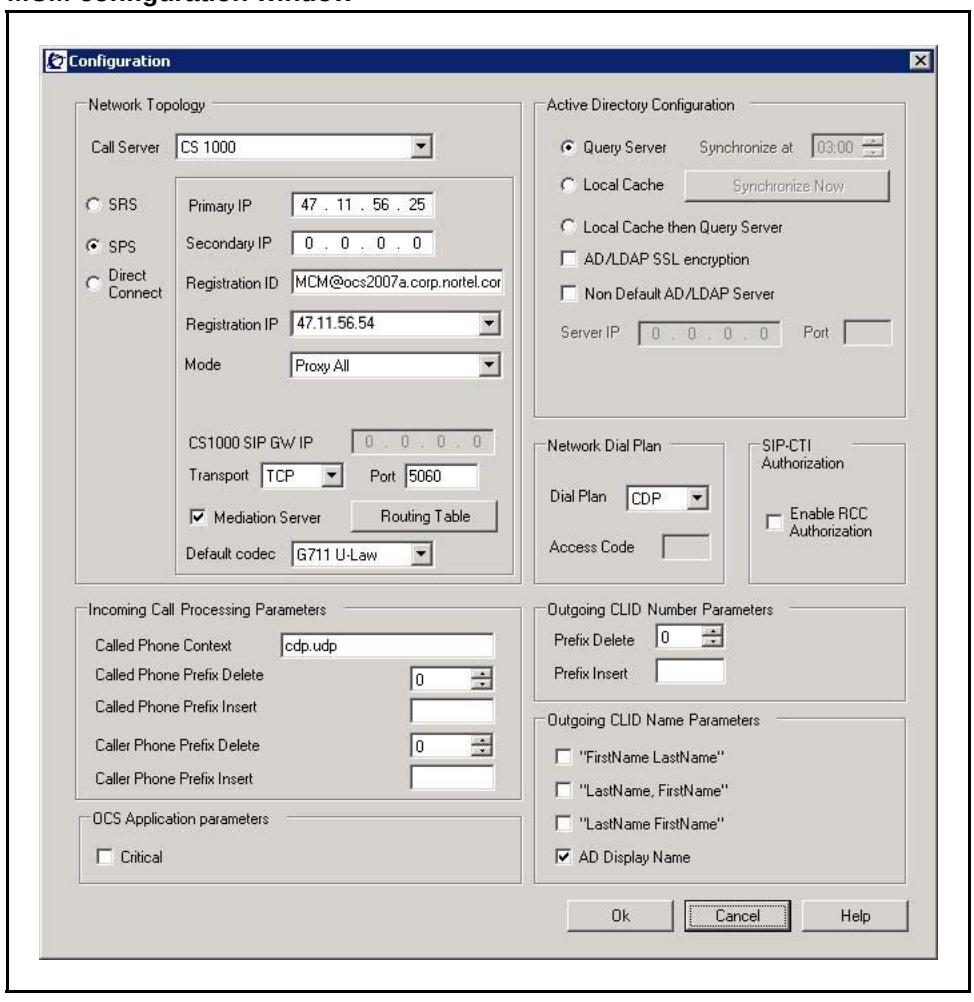
The expected result is:

Communicator has one merged pop-up with CLID "+71237777"

MCM Configuration window

To access the MCM configuration window, go to the MCM console window, select the **Tools** menu and then select **Configuration**.

Figure 55
MCM configuration window



Network Topology section

The following is a description of some of the configuration fields in the Network Topology section of the MCM configuration window.

Table 33
Network topology fields

Configuration field	Description
Call Server	Type of call server CS 1000, CS 2000, CS 2100
SRS	Outgoing SIP messages from the MCM will use the SIP Redirect Server for routing.
SPS	Outgoing SIP messages from the MCM will go through the SIP Proxy Server.
Direct	Outgoing SIP messages from the MCM will terminate directory to a CS 1000 SIP GW.
Primary IP	IP address of primary SRS/SPS. Not used in the case of Direct SIP Routing.
Secondary IP	IP address of secondary SRS/SPS. Not used in the case of Direct SIP Routing.
Registration ID	MCM endpoint ID. This ID is in the format of host@domain. The host must match the endpoint name as defined in the NRS/SPS for MCM.
Registration IP	Select the MCM proxy IP to register with the SRS/SPS.
Mode	Proxy mode for SPS. The SIP Proxy Server (SPS) acts as a redirect server as well as a proxy server: • Proxy All—SPS will proxy/route all messages from the MCM. • Proxy SIP and Re-direct SIP-CTI—SPS will proxy/route SIP calls and redirect SIP-CTI calls. In this mode, traffic going through the SPS is reduced. This can also be useful for administration purposes. • Redirect All—SPS will redirect all messages. In this mode, SPS will work in the same way as SRS. If this mode is selected, ensure that DNS server IP addresses have been configured on the SIP Proxy Server.
CS 1000 SIP GW IP	IP address of the CS 1000 Node. Used only for Direct SIP routing with the CS 1000.
Transport	Only TCP is supported. The Transport and Port parameters are the SIP transport and TCP port that is configured on the Mediation Server for the PSTN Gateway Listening Connection. The default value for transport is TCP. For more information about TLS transport configuration, see “Configuring TLS between OCS Proxy with MCM and Mediation Server (OCS R1 only)” (page 240) .
Port	SIP Port on SRS, SPS, and CS 1000. Default values are 5060 for TCP and 5061 for TLS connections.
Mediation Server	Select the check box to use Mediation Server. For more information about configuring the Mediation Server routing table, see “Configuring the Mediation Server routing table” (page 162) and for two configuration examples, see “Configuring MCM homing logic—CS 1000 main office and MG 1000B Branch Office ” (page 164) and “MCM homing logic—Geographic Redundancy (N-way) ” (page 167).

Configuration field	Description
Routing table	Click the Routing Table button when using Mediation Server.
Default codec	The default companding law configured on the corresponding CS 1000 system. If the CS 1000 deployment consists of CS 1000 systems configured with different companding laws, a separate server with MCM is required for each law. For more information about mulaw and alaw companding preference settings, see “Mulaw and alaw companding preference setting” (page 174).

Mediation Server routing table configuration

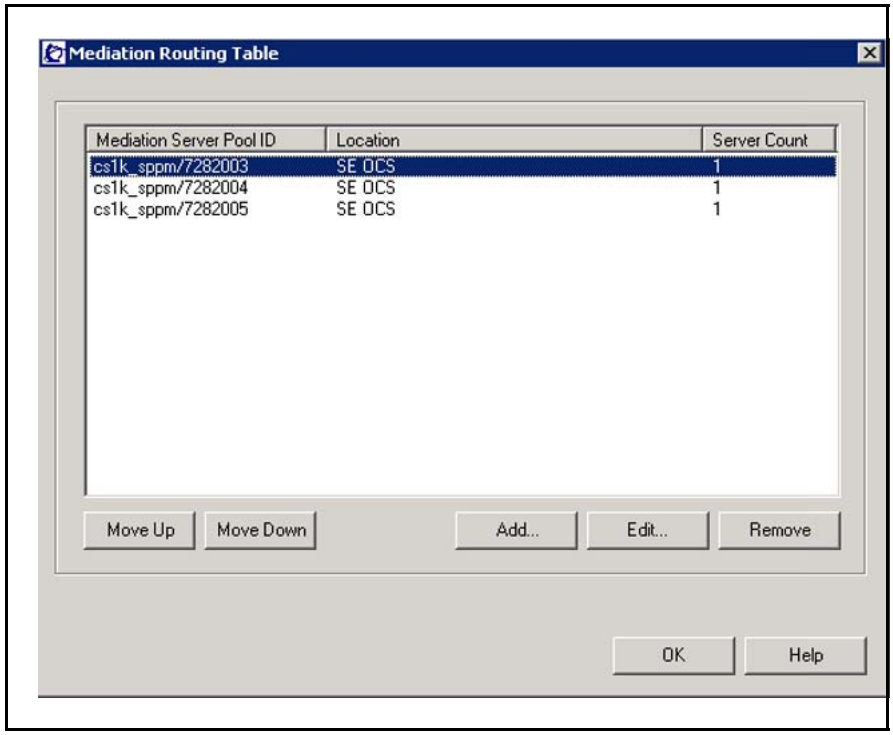
Several Call Servers from different geographic locations may be connected to one MCM with one SIP Gateway. For each geographic location, one or several Mediation Servers forming a pool of Mediation Servers can be used. The sip-gw-id parameter is passed as an INVITE request providing information about which dedicated Mediation Server or Mediation Server pool to process this message. The parameter value for SIP Gateway Endpoint Name is configured in Element Manager under **System, IP Network, Nodes: Servers, Media Cards, Signaling Server Properties**.

For configuration examples, see sections “Configuring MCM homing logic—CS 1000 main office and MG 1000B Branch Office ” (page 164) and “MCM homing logic—Geographic Redundancy (N-way) ” (page 167).

Configuring the Mediation Server routing table

Step	Action
1	From the **MCM configuration** window, click **Routing Table**. The Mediation Routing Table appears, as shown in the following figure.

Figure 56
Mediation routing table



The routing table is used by MCM 4.x to get Home CS 1000 sip-gw-id for the Mediation Server for calls from the OC to the CS 1000. This only applies for Geographic Redundancy and main and branch office deployments when multiple CS 1000 SIP Gateways can share one Mediation Server.

The Mediation Routing Table must be configured with the Mediation Pool ID as Gateway ID/Service DN. For example, if Gateway ID is cs1k_sppm and the Service DN is 7294000, then the Mediation Pool ID has to be cs1k_sppm/7294000. The MCM is then able to determine what pool is used. The server count is the number of the Mediation Servers in the pool. The server count increments automatically by the MCM.

Click **Move Up** and **Move Down** to sort the list of SIP Gateway IDs. The main office sip-gw-id should go before the Branch Office sip-gw-id.

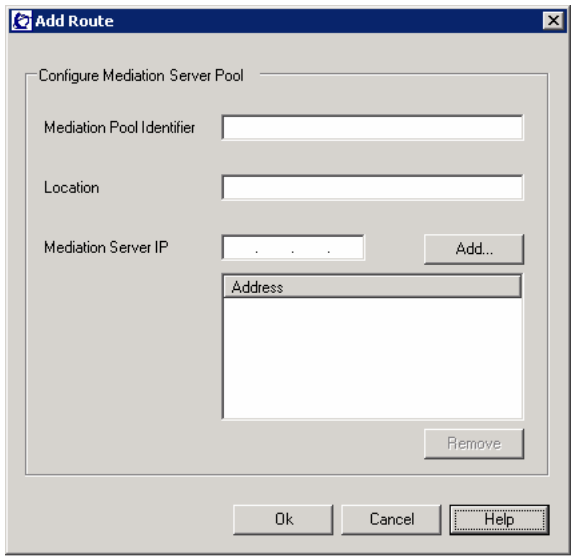
2 Click **Add**.

The Add Route page appears.

3 Configure the Mediation Server pool information, as shown in the following figure.

- Mediation Pool Identifier: Ensure this is the same as the sip-gw-id header.
- Location: Description of the pool.
- Mediation Server IP: Add the IP address of the Mediation Server and click **Add**.

Figure 57
Add Route



ATTENTION
When a new Mediation Server is added into the Mediation Server pool, the MCM configuration must be manually updated with the Mediation Server IP address because Mediation Servers do not support an auto discovery mechanism.

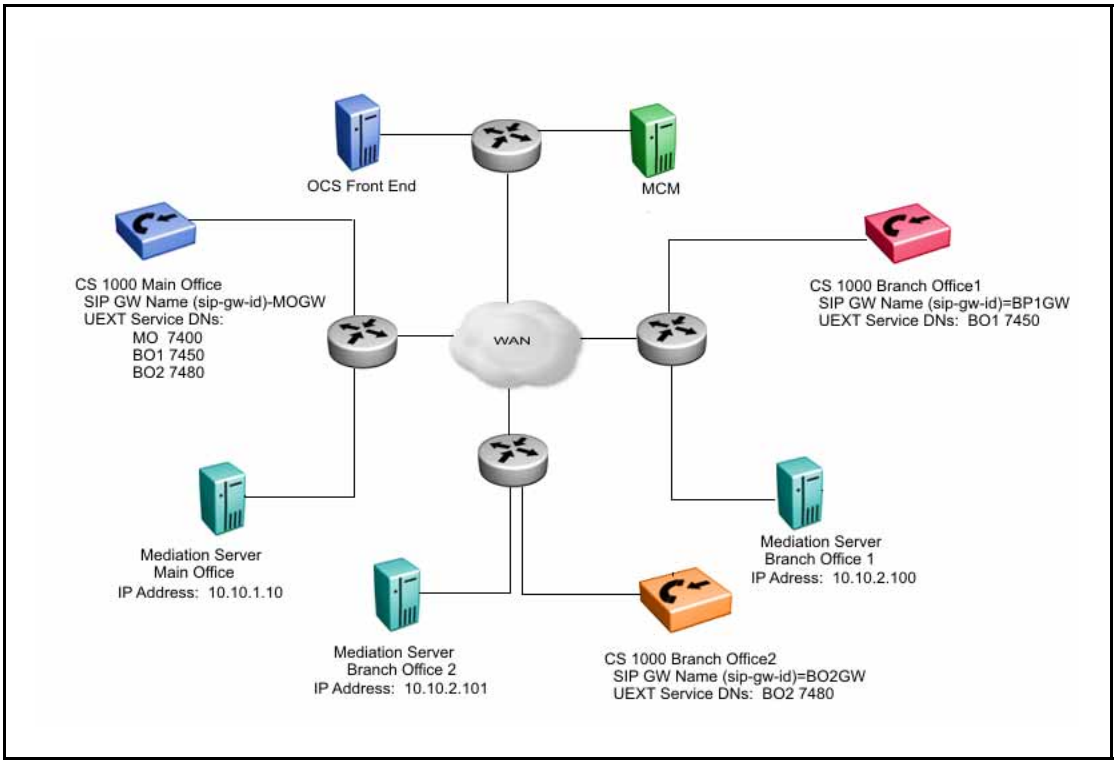
4 Click **Ok**.

--End--

Configuring MCM homing logic—CS 1000 main office and MG 1000B Branch Office

The following topology depicts an example configuration of the CS 1000 main office and MG 1000B Branch Office where OC VoIP call redundancy and media stream localization is required. You are required to have at least one Mediation Server at each main office and branch office location.

Figure 58
Topology of a main office and two branch offices



Prerequisites

The following UEXT TLSV service DNs must be planned for the main and branch offices.

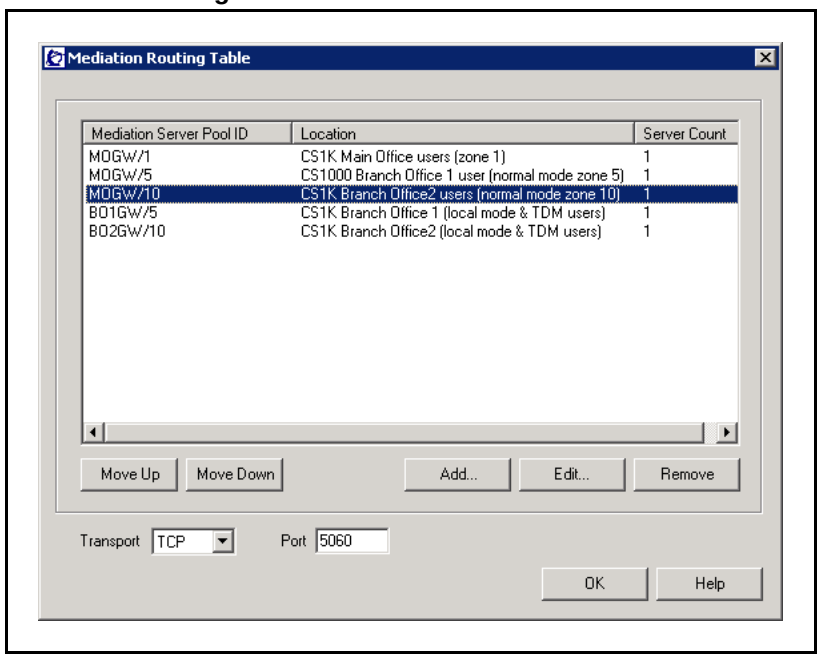
- Main Office:
  - — The UEXT TLSV service DNs for the main office IP phone and branch office IP phone users must be planned.
- Branch Office:
  - — THE UEXT TLSV service DNs must be planned for the branch office IP phones in case they are in local mode.
  - — The UEXT TLSV service DNs must be planned for the TDM phones that are connected to the branch office.

Configuring the Mediation Server Routing table for Main and Branch Offices

Step	Action
1	From **MCM Configuration**, click **Routing Table**.

The Mediation Routing Table appears, as shown in the following figure.

Figure 59
Mediation routing table



2 Click **Add** to configure the Mediation Server pool IP address.

The Add Route page appears.

Use the following table to configure the Mediation Server pool information. For the topology, see Figure 58 "Topology of a main office and two branch offices" (page 165).

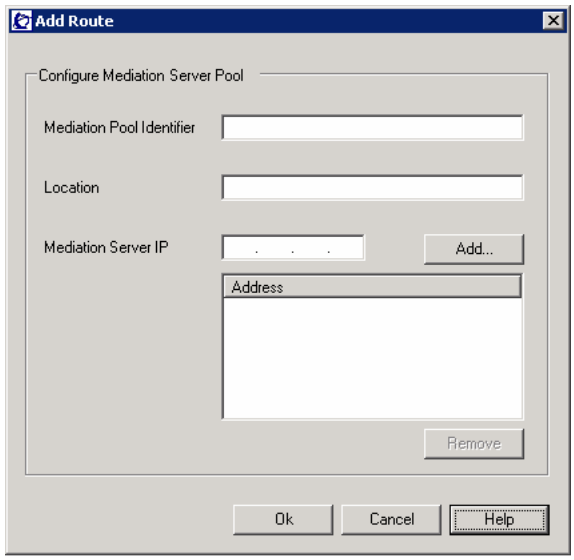
Table 34
Listing of Mediation Server IP addresses

Mediation Server Pool ID	Mediation Server IP address	Server count (increments automatically by MCM)
MOGW/7400	10.10.1.10	1
MOGW/7450	10.10.2.100	1
MOGW/7480	10.10.2.101	1
BO1GW/7450	10.10.2.100	1
BO2GW/7480	10.10.2.101	1

3 Configure the Mediation Server pool information, as shown in the following figure.

- Mediation Pool Identifier: Ensure this is the same as the sip-gw-id header.
- Location: Description of the pool.
- Mediation Server IP: Add the IP address of the Mediation Server and click **Add**.

Figure 60
Add Route



ATTENTION
When a new Mediation Server is added into the Mediation Server pool, the MCM configuration must be manually updated with the Mediation Server IP address because Mediation Servers do not support an auto discovery mechanism.

4 Click **Ok**.

--End--

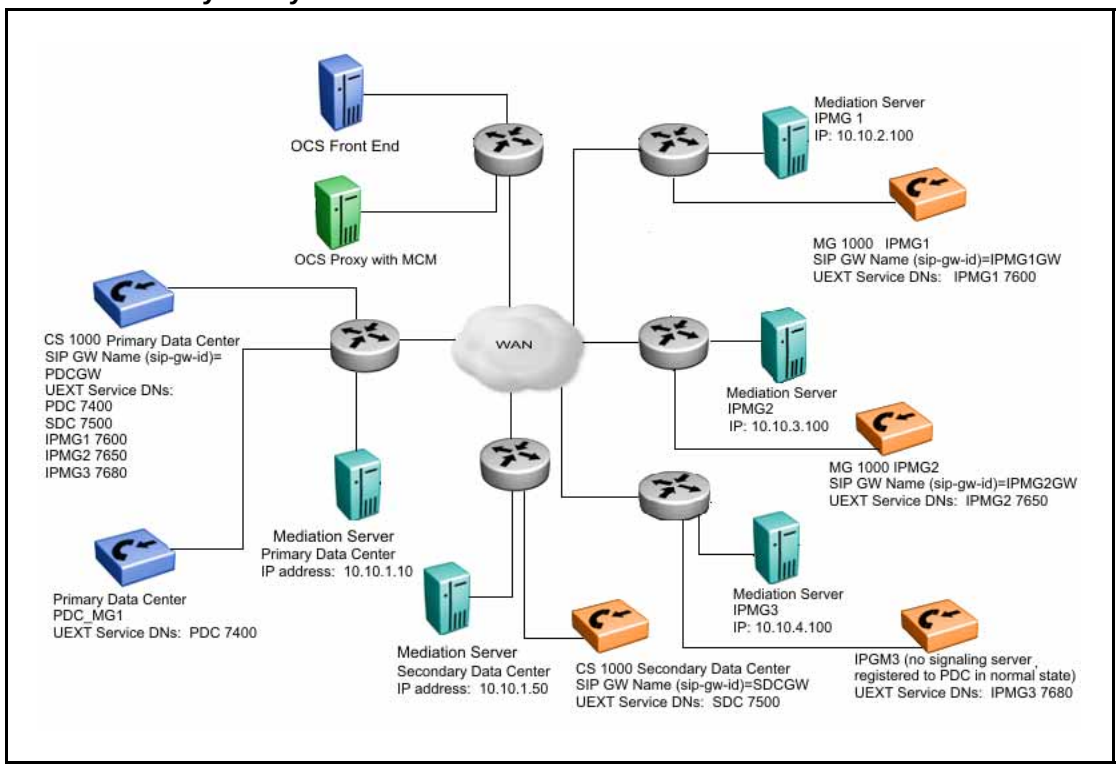
ATTENTION
To meet your site traffic requirements, add multiple Mediation Server IP addresses if your site has more than one Mediation Server.

MCM homing logic—Geographic Redundancy (N-way)

The following topology is an example configuration of geographic redundancy N-way setup where OC VoIP call redundancy and media stream localization is required. This topology depicts PDC_MG1 as part of the primary CS 1000 located at the Primary Data Center (PDC).

PDC_MG1 shares the same UEXT Service number and Mediation Server as the Primary CS 1000. One mediation server is required for each Data Center. IPMG1 and IPMG2 uses the same Signaling Server for IP phones redirection and survivability and SIP trunking. IPMG3 works similarly to an extension of the PDC running at a remote office location. For example, when the PDC is unreachable, the call attempts to register to the CS 1000 Secondary Data Center. The IPMG3 location is assigned its own Mediation Server and service DN.

Figure 61
Geo-redundancy N-way

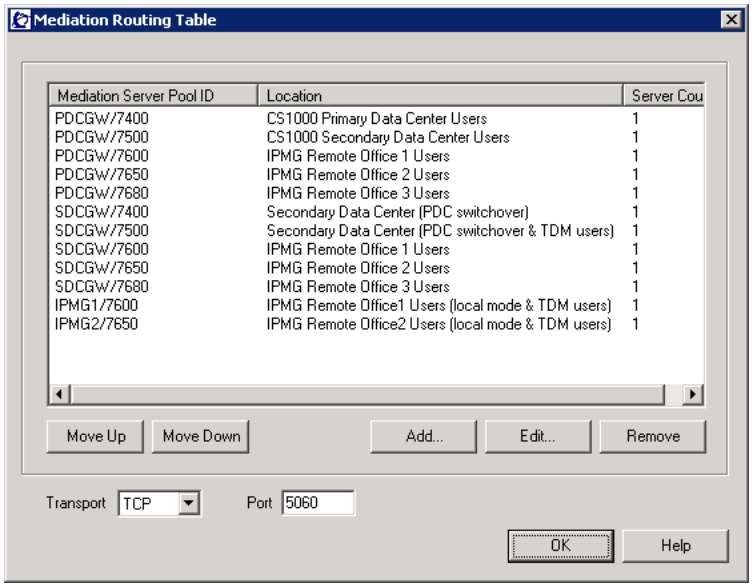


For prerequisite information, see “Prerequisites” (page 165).

Configuring the Mediation Server Routing table for Geo-redundancy (N-way)

Step	Action
1	From **MCM Configuration**, click **Routing Table**. The Mediation Routing Table appears, as shown in the following figure.

Figure 62
Mediation routing table



ATTENTION
The differences between a Main Office and Branch Office configuration are as follows:

- The Secondary Data Center functions like a geographic redundant CS 1000. It performs the functions of the Primary Data Center IP phone users that have switched over to the secondary side. Therefore, the pool ID for the Primary Data Center and all other remote office IPMGs are required.
- The MG 1000B can be deployed in remote office locations with or without Signaling Servers, depending on the following requirements:
  - IPMG1 and IPMG2 both have Signaling Servers and are capable of hosting IP phones in local mode and communicating with OCS through SIP trunks. Therefore, separate pool IDs are configured for IPMG1 and IPMG2 in survivable/local mode.
  - IPMG3 does not have a Signaling Server and therefore, cannot host survivable IP phones and SIP trunking. In a situation where the IPMG3 cannot contact the Primary and Secondary Data Centers, for example, a WAN outage, the IPMG3 cannot communicate with OCS. Therefore, a pool ID is not required to be configured for IPMG3 in survivable/local mode.

2 Click **Add** to configure the Mediation Server pool IP address. Use the following table to configure the Mediation Server pool

information. For the topology, see Figure 61 "Geo-redundancy N-way" (page 168).

Table 35
Listing of Mediation Server IP addresses

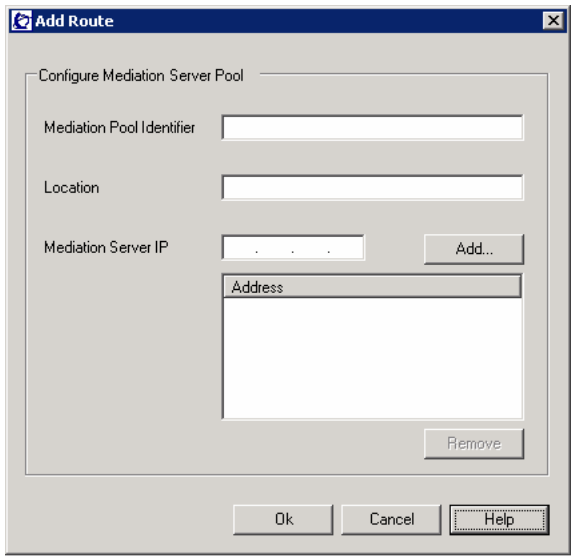
Mediation Server Pool ID	Mediation Server IP address	Server count (increments automatically by MCM)
PDCGW/7400	10.10.1.10	1
PDCGW/7500	10.10.1.50	1
PDCGW/7600	10.10.2.100	1
PDCGW/7650	10.10.3.100	1
PDCGW/7680	10.10.4.100	1
SDCGW/7400	10.10.1.50	1
SDCGW/7500	10.10.1.50	1
SDCGW/7600	10.10.2.100	1
SDCGW/7650	10.10.3.100	1
SDCGW/7680	10.10.4.100	1
IPMG1/7600	10.10.2.100	1
IPMG2/7650	10.10.3.100	1
IPMG3/7680	not required in survivable/local mode	N/A

ATTENTION
To meet your site traffic requirements, add multiple Mediation Server IP addresses if your site has more than one Mediation Server.

3 Configure the Mediation Server pool information, as shown in the following figure. Use the table Table 35 "Listing of Mediation Server IP addresses" (page 170).

- Mediation Pool Identifier: Ensure this is the same as the sip-gw-id header.
- Location: Description of the pool.
- Mediation Server IP: Add the IP address of the Mediation Server and click **Add**.

Figure 63
Add Route



ATTENTION
When a new Mediation Server is added into the Mediation Server pool, the MCM configuration must be manually updated with the Mediation Server IP address because Mediation Servers do not support an auto discovery mechanism.

4 Click **Ok**.

--End--

Enabling the Mediation Server zone selection (OCS 2007 R2 only)

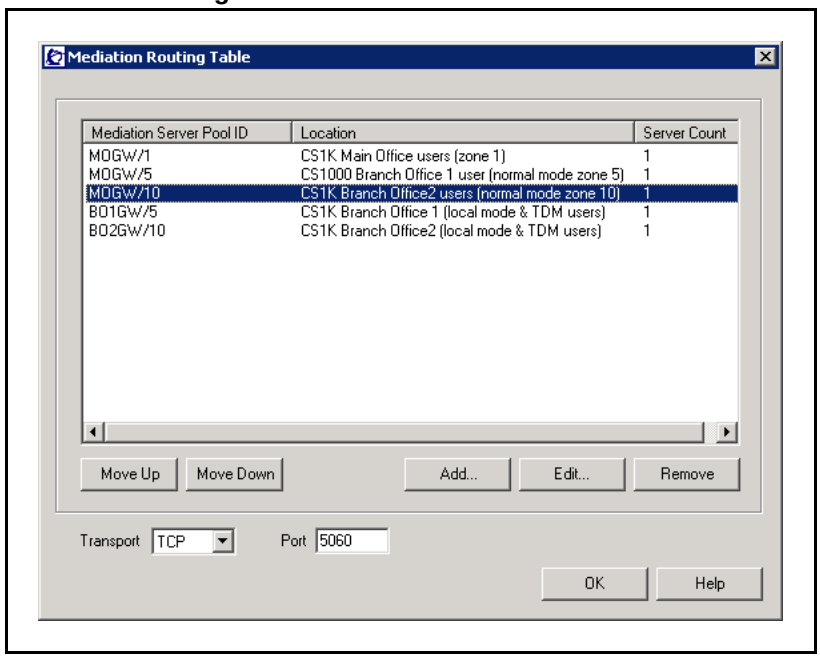
Enable the Mediation Server zone selection feature in LD 117 on the call server. This is part of the existing zone feature to assign all IP phones, virtual trunks, and DSP channels. The zone based routing to the Mediation Server applies a flag to each zone. You can enable this flag in LD 117 by typing ENL MEDS <zone number>, you can print by typing PRT MEDS <zone number/ALL/" ">, and you can disable by typing DIS MEDS <zone number>.

If you are calling to UEXT and MEDS flag is enabled for uext zone, then the zone number is passed from the Call Server to the Signaling Server and appended to the sip-gw-id for MCM routing to the appropriate pool. If you are calling to UEXT and MEDS flag is disabled for uext zone, then the zone number does not pass from the Call Server to the Signaling Server and it uses the SIP_Gateway_name/ServiceDn as

sip-gw-id field. For example, the Mediation Server enabled for zone 0 is **sip-gw-id=SIP_Gateway_name/0** and the Mediation server disabled for zone 0 is **sip-gw-id=SIP_Gateway_name/ServiceDn**.

Step	Action
1	For main office and remote locations, assume the IP phones are assigned to specific zones at the CS 1000 main office located at the Primary Data Center (PDC). Obtain a hard copy record of all zones for later reference.
2	Mediation Server zone selection feature must be enabled on LD 117.
3	On UEXT TLSV, configure all main and remote office users using UEXT TLSV key 1 HOT P DN to the CDP or ESN number designated for the MCM. You do not need to type in the individual service number for each user.
4	On the MCM Mediation Server routing table, configure the mediation pool ID as sip-gw-id/zone number.
5	From the **MCM configuration** window, click **Routing Table**. The Mediation Routing Table appears, as shown in the following figure.

Figure 64
Mediation routing table



The Mediation Routing Table must be configured with the Mediation Pool ID as sip-gw-id/zone number.

Click **Move Up** and **Move Down** to sort the list of SIP Gateway IDs. The main office sip-gw-id should go before the Branch Office sip-gw-id.

6 Click **Add**.

The Add Route page appears. Use the following table to configure the Mediation Server pool information.

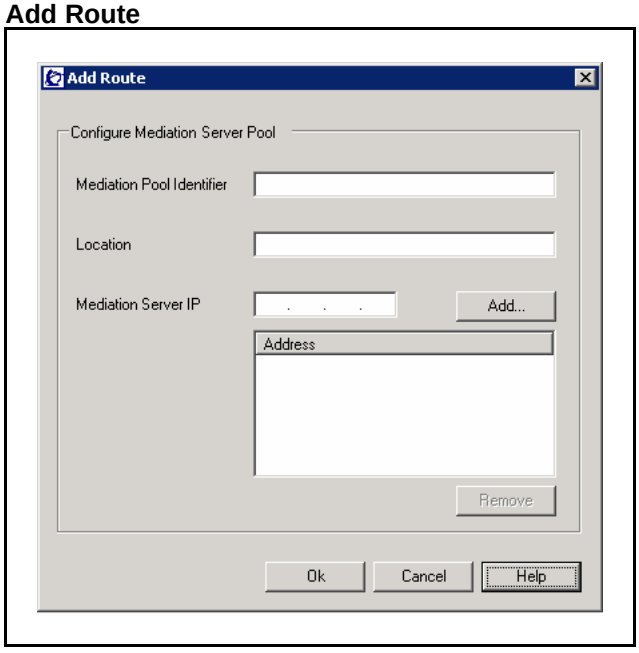
Table 36
Listing of Mediation Server IP addresses

Mediation Server Pool ID	Mediation Server IP address	Server count
MOGW/1	10.10.1.10	1
MOGW/5	10.10.2.100	1
MOGW/10	10.10.2.101	1
BO1GW/5	10.10.2.100	1
BO2GW/10	10.10.2.101	1

7 Configure the Mediation Server pool information, as shown in the following figure.

- Mediation Pool Identifier: Ensure this is the same as the sip-gw-id header.
- Location: Description of the pool.
- Mediation Server IP: Add the IP address of the Mediation Server and click **Add**.

Figure 65
Add Route



ATTENTION
The deployment topology and VoIP call homing logic is unchanged; however, the service DNs are replaced with zone numbers.

8 Click **Ok**.

--End--

In a sample user scenario, an incoming call from PSTN (off BO1) to OC twinned BO1 phone in normal mode, the OC client (BO1) answers. BO1 routes the call to MO through the vacant number routing. The BO1 phone rings. The twinning UEXT TLSV forks a SIP call to MCM with the sip-gw-id field configured to MOGW/5. MCM routes the call to the Mediation Server BO1, to the Front End, and then to the OC client (BO1).

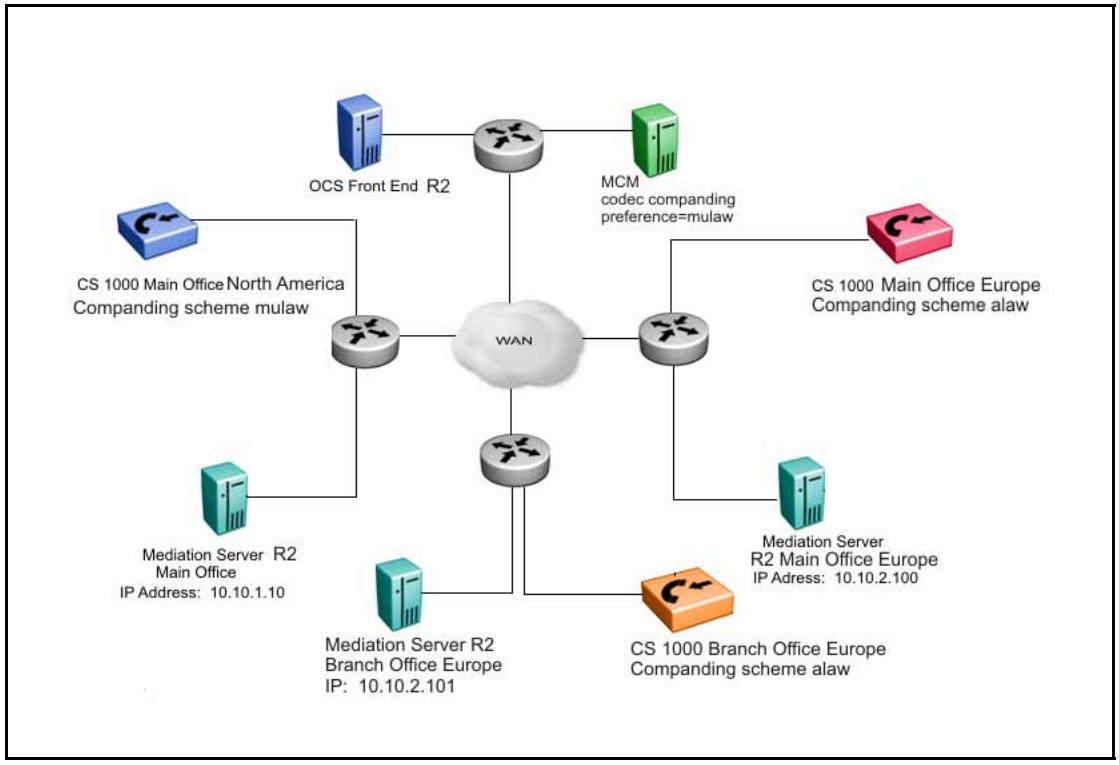
Mulaw and alaw companding preference setting

To resolve a codec selection issue with OCS 2007 Mediation Server, an mulaw and alaw companding preference setting was introduced as an upissue for MCM 3.5 and required a separate MCM to be placed in the mulaw and alaw codec regions on a customer Communication Server 1000 topology. This preference setting is still available for MCM 4.0.

Scenario 1

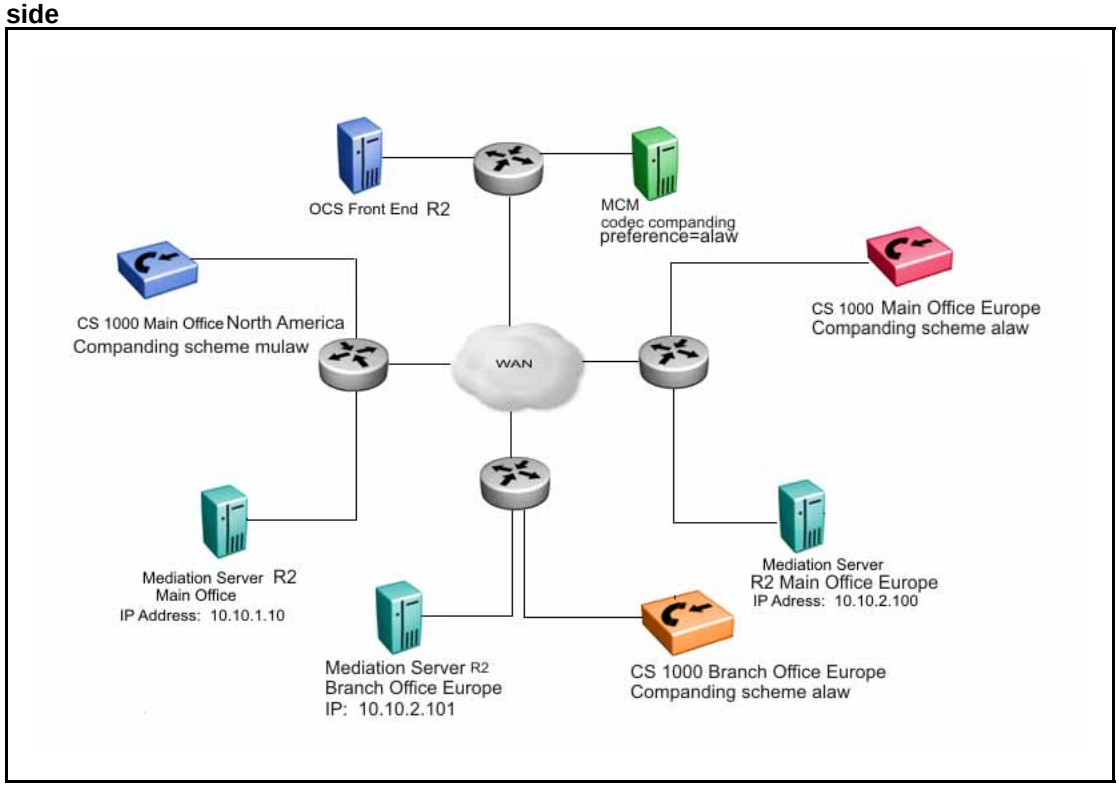
You have upgraded and deployed all Mediation Servers to OCS 2007 R2. One MCM is placed in either the mulaw or alaw region.

Figure 66
Topology 1—All Mediation Servers are deployed with OCS 2007 R2



The following figure depicts the MCM codec companding preferences configured to alaw on the European side of the network and all Mediation Servers deployed with OCS 2007 R2.

Figure 67
Topology 2—All Mediation Servers are deployed with OCS 2007 R2 and alaw on European side



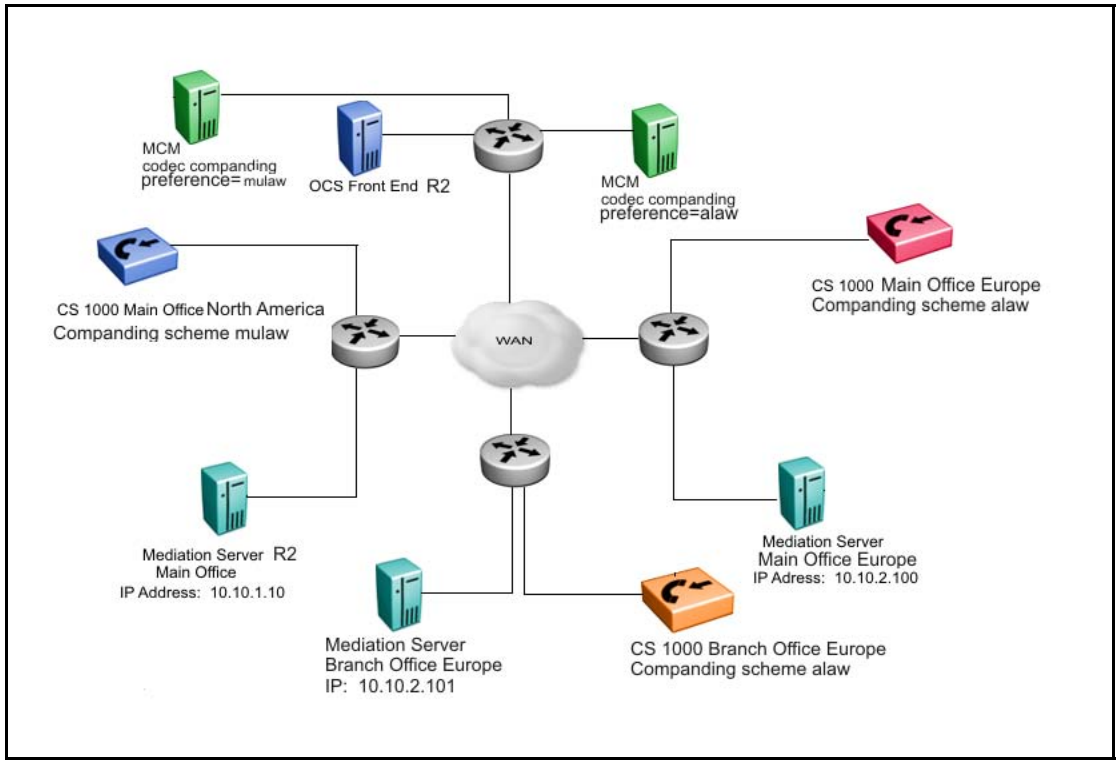
Scenario 2

You are in the process of transitioning your Mediation Servers to OCS 2007 R2. You have a network of OCS R2 Front End servers and have upgraded some Mediation Servers to OCS 2007 R2. In this scenario, separate MCMs must be deployed for the mulaw and alaw region until all OCS 2007 are upgraded to OCS 2007 R2.

The following figure depicts the following:

- A customer in North American has fully upgraded the Front End server, Mediation Server, and MCM to OCS 2007 RS.
- In Europe, the Mediation Servers are not upgraded and are still running OCS 2007

Figure 68
Topology 3—Two MCMs, mixed release of Mediation Servers



Incoming Call Processing Parameters section

This option refers to incoming CS 1000 calls to MCM that terminate on Office Communicator. You must specify the phone context. When the telephone context is defined, mapping is performed (using CDP or UDP). In the case of a large network, the telephone context used is UDP, while CDP is used for small networks. You can use Called Phone Prefix Delete and Insert fields to manipulate digits received from the CS 1000 prior to mapping.

Table 37
Incoming Call Processing parameters

Configuration field	Description
Called Phone Context	Phone Context of calls to be processed by MCM. This entry depends on the dial-plan (CDP or UDP) and must be the same as Private/CDP domain name entries in Element Manager.
Called Phone Prefix Delete	Number of prefix digits to be deleted from the called number for mapping to the user ID by MCM
Called Phone Prefix Insert	Prefix digits to be inserted in the called number for mapping to User ID by MCM.

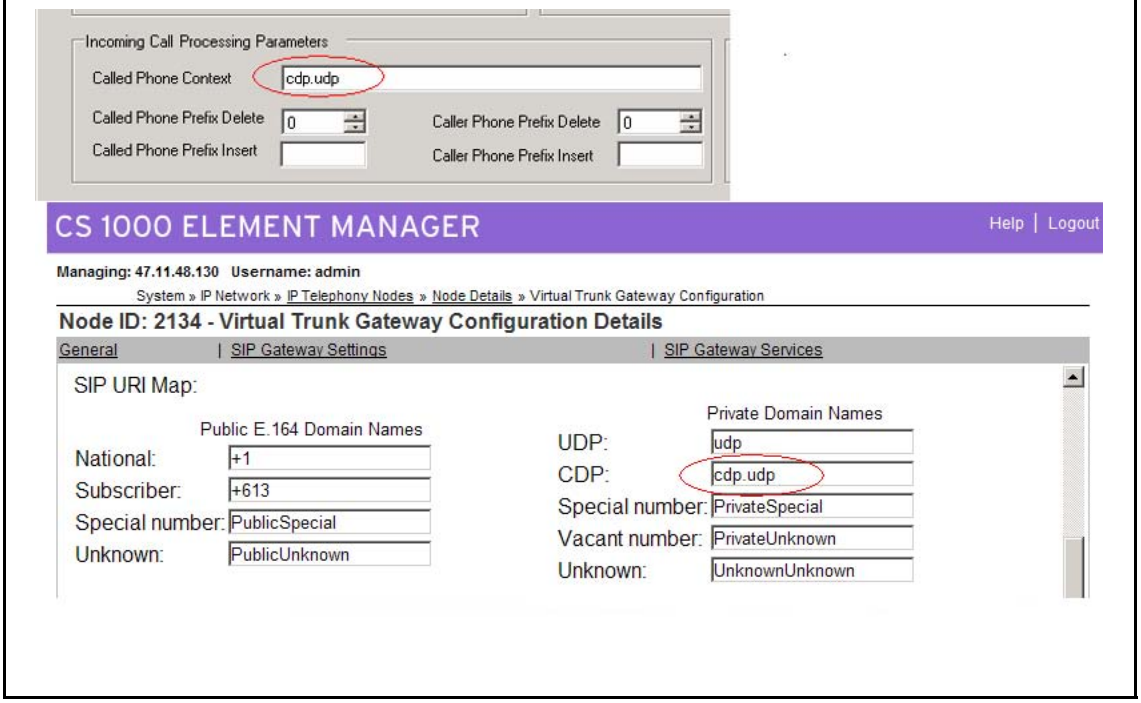
Configuration field	Description
Caller Phone Prefix Delete	Number of Prefix digits to be deleted from the caller number for mapping to a user ID by the Office Communicator client.
Caller Phone Prefix Insert	Prefix digits to be inserted in the caller number for mapping to a User ID by the Office Communicator client.

The Caller Phone Prefix Delete and Insert is used to manipulate the digits in the From header of the INVITE received from the CS 1000. These two kinds of manipulation are generally not necessary, but are available in case a scenario requires this type of manipulation.

The MCM requires access rights to certain directories (for example: “Program Files/ MCM…”). Ensure that the user has the Administrators rights to these directories.

The following figure depicts the Called Phone Context entry in the MCM configuration screen and the entries for UDP and CDP in Element Manager. These entries must match.

Figure 69
Element Manager SIP URI MAP



OCS Application parameters

By clicking the Critical check box, this option gives you the ability to enable MCM to register as a critical application on the OCS. If the MCM is registered as a critical application, the OCS Proxy service does not start

and MCM fails to start. This is useful in MCM redundancy deployment when the Load Balancer supports SIP health checking. When the MCM fails to start, health checking fails and the Load Balancer routes all the SIP messages to another functioning MCM.

Active Directory configuration section

There are two modes for Active Directory (AD) configuration: Realtime or Local Cache. Realtime mode is used for end-user ID mapping, which requires a Lightweight Directory Access Protocol (LDAP) query. Local Cache mode involves caching the Active Directory on the MCM server and using that cache information for queries.

Table 38
Active Directory configuration

Configuration Field	Description
Query server	Use this field for real-time LDAP AD queries.
Local Cache	AD queries are done to a local cache of the AD. The cache is synchronized daily at a preconfigured time. You can force it to synchronize by clicking the **Synchronize Now** button to start
Local Cache then Query Server	AD queries are done to a local cached of the AD. If the entry is not found in the local cache then the MCM queries the LDAP AD in real-time.
AD/LDAP SSL encryption	Use this option if LDAP over SSL is configured in your AD deployment and you want the AD queries to be encrypted. **ATTENTION** LDAP over SSL is not activated on the AD Domain Controller by default.For more information about how to enable LDAP over SSL with a third-party certification authority, go to the Microsoft Web site at www.microsoft.com.
Non default AD/LDAP Server	IP address and port of the LDAP server to be used if different from the default AD/LDAP server.

Active Directory query

The Active Directory Query tool is used to check Active Directory mapping configuration. It searches for a user-id (SIP URI) by a given telephone number, and vice versa. This tool is only used for maintenance, and emulates the same algorithm that is used by the MCM service in run-time.

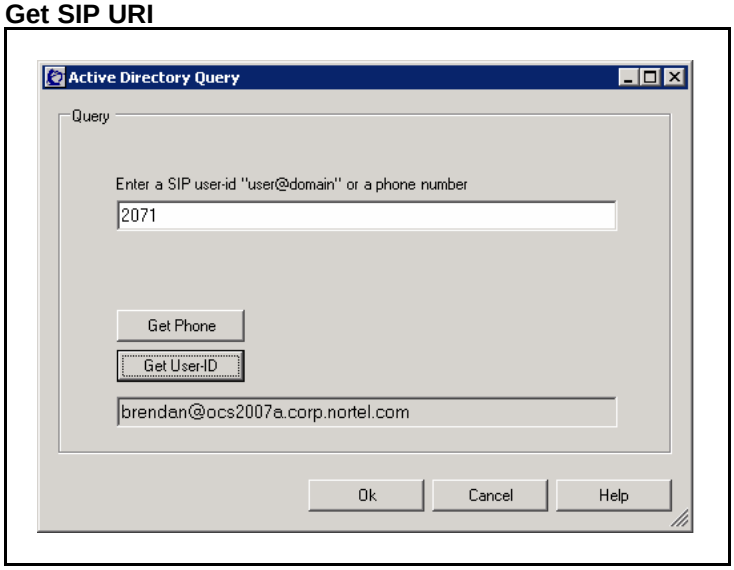
For example: user Brendan McCarthy is defined in the Active Directory as:

SIP URI: sip:brendan@ocs2007a.corp.nortel.com

Line URI: +16239675000;ext=2071

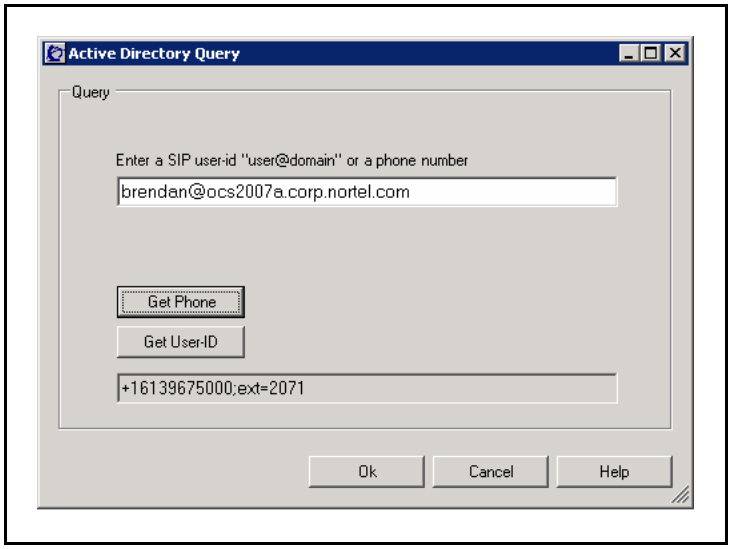
If you type the telephone number in the Query field and click the **Get User-ID** button, the SIP URI appears in the Result field, as shown in the following figure.

Figure 70
Get SIP URI



If you type the SIP URI in the Query field and press the Get Phone button, the Telephone number appears in the Result field (see Figure 71 "Get phone" (page 180)).

Figure 71
Get phone



Network Dialing Plan section

The following table describes the fields for Dial plan and Access code.

Table 39
Network dialing plan

Configuration field	Description
Dial plan	Use the dial plan to make calls between the CS 1000 and OCS (CDP or UDP). If the Line URI is configured as UDP, the dial plan will also be UDP.
Access code	Access code for the UDP plan. This code is added to the phone number stored in the OC user's Line URI.

ATTENTION
Only one dialing plan is supported at a time for Office Communication Server 2007 inter-working. All calls between nodes of CS 1000 deployment must be placed using the same dialing plan configured for the Nortel Converged Office feature.

Outgoing CLID Number Parameters section

The following table describes the fields for Prefix Delete and Prefix Insert.

Table 40
Outgoing CLID Number Parameters

Configuration field	Description
Prefix Delete	Number of prefix digits to be deleted from the CLID number sent by MCM to the CS 1000.
Prefix Insert	Prefix digits to be inserted in the CLID number sent by MCM to the CS 1000.

Outgoing CLID Name Parameters section

If an OC client does not have a UEXT defined in the CS 1000, the outgoing CLID Name Parameters manipulate the name string to display the name on a CS 1000 configured in the desired format. The name must be defined in the Active Directory in the format Last, First [additional info].

ATTENTION
When an OC client has a UEXT defined in the CS 1000, the name is displayed in accordance with the CPND configuration for the CS 1000 endpoint. The name is not displayed when CPND is not configured.

Table 41
Outgoing CLID Name Parameters

Configuration field	Description
FirstName LastName	First name Last name—display name format.
LastName, FirstName	Last name, First name—display name format.

Configuration field	Description
LastName FirstName	Last name First name—display name format.
AD Display Name	Click the check box to use the Display Name value from AD for the calling user name.

SIP CTI Authorization section

Click the Enable RCC Authorization check box to enable the authorization of SIP CTI INVITES from Office Communicator (OC). Only the OC user's phone that is configured in the Active Directory is controlled.

MCM for Remote Call Control

For Remote Call Control, the Nortel MCM application that resides within the Office Communications Server domain provides support for authorizing TR/87 service requests and redundancy.

Authorization of TR/87 service

MCM supports authorization of Remote Call Control service requests from Office Communicator clients. The following is a summary of the authorization algorithm:

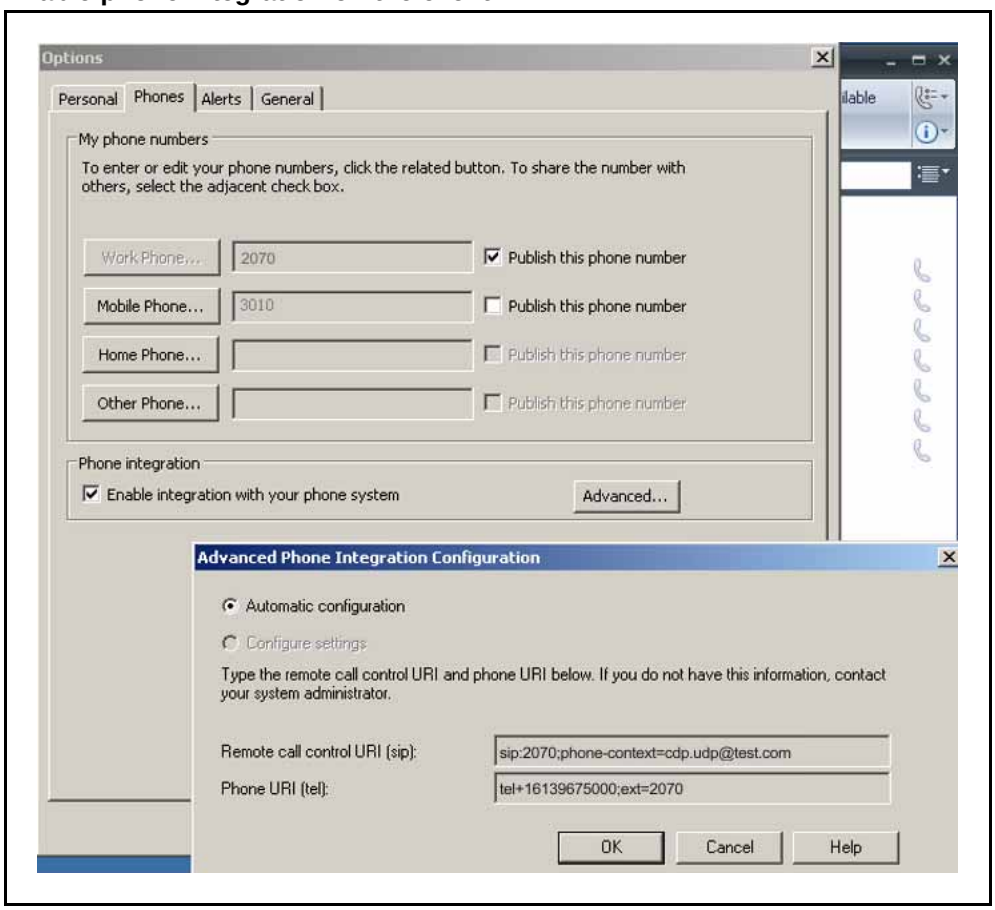
1. The SIP INVITE "from" header provides the **Requestor Identity** (for example, the Office Communications Server user identity).
2. The CSTA XML message provides the **Controlled Device Identity** (for example, the phone URI).
3. The **Owner Identity** is found by a reverse lookup using the Controlled Device Identity found in "Item 2" (page 182) as a query to Active Directory (Search Active Directory, Find the User whose msRTCSIP-Line equals "Controlled Device ID", then find the msRTCSIP-PrimaryUserAddress of that User).
4. If a result is found in "Item 3" (page 182) , the Owner Identity is equal to the Requestor Identity, and msRTCSIP-OptionFlags has RCC enabled, then approve the request. Otherwise, reject the request.

The primary function of MCM when authorization is enabled, is to ensure that an Office Communicator user can use Remote Call Control only for the phone URI, and that Remote Call Control SIP URI as configured in Active Directory for that user by the System Administrator as depicted in Figure 72 "Enable phone integration on the client" (page 183). Placing control in the hands of the System Administrator is necessary

in environments where users must not override their phone integration configuration through the manual phone integration option in Office Communicator.

Note: Disabling TR/87 authorization on the MCM is strongly discouraged. When this functionality is disabled, users can override their active directory configuration and control any DN in the system that is provisioned to support SIP CTI.

Figure 72
Enable phone integration on the client



Redundancy

Redundancy of the TR/87 interface is not provided natively with Office Communications Server 2007. Office Communicator does not support multiple Remote Call Control SIP URIs or SIP 300/302 redirection messages. To provide for redundancy of the TR/87 interface, the Nortel MCM application uses the redundancy of NRS and multiple FE endpoints.

MCM redundancy with Load Balancer

OCS Proxy with MCM redundancy is ensured by configuring a Load Balancer. The following must be configured:

- The Front-End server (static route) and Mediation Server (PSTN Gateway next hop) must point to the Load Balancer Virtual IP address (VIP).
- Each MCM is registered to the NRS with dynamic SIP (No Routing Entry configured).
- A static endpoint is configured for the MCM VIP on the NRS. Configure a Routing Entry to point to the static endpoint.

Telephony Gateway and Services configuration

This section describes the process to configure Telephony Gateway and Services.

Office Communications Server, Active Directory and MCM must be configured properly prior to configuring the Telephony Gateway and Services component.

Call Server configuration

CS 1000 configuration involves two separate functions: Signaling Server configuration and Call Server Configuration. All of the Signaling Server configuration is performed in Element Manager. Most of the Call Server configuration can also be done in Element Manager, although some can be done at the Call Server prompt. This document assumes that you are already familiar with how to configure a CS 1000.

In ESN networks, you must configure the correct HLOC in both LD 90 (required for ESN calls to work) and LD 15. If not, basic calling functionality does not work. Also, the Calling Line Identification (CLID) table, Home NPA, and LOC are required for outgoing calls to the Public network (PSTN) to correctly display the outgoing Calling Line Identification (CLID) in North America.

Package 408 is required for both Telephony Gateway and Services and Remote Call Control. Phones need not be configured as AST or have T87A enabled as a class of service; however, Package 408 must be added in order for Telephony Gateway and Services to work properly.

Configuring the Codec

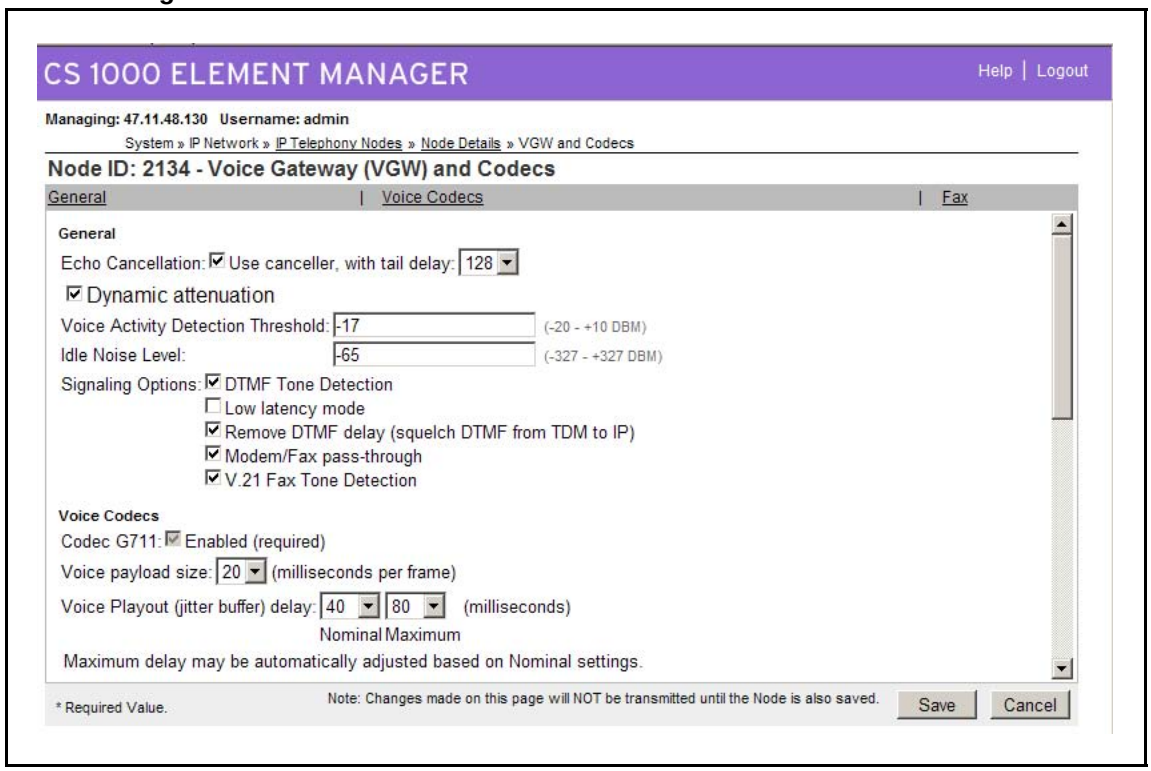
The Mediation Server supports the G.711 (20 milliseconds) codec. The G.711 codec must be enforced in the network by defining only the G.711 codec on the CS 1000. If G.711 is not the only codec used, calls to voice mail (such as CallPilot) or call conferencing bridges (such as MCS

MeetMe) do not work. The only codec supported for the short leg of a call (Mediation Server to Call Server) is G.711 and for the long leg (Mediation Server to Office Communications Server is RT audio.

Other codecs cannot be configured on the CS 1000, as Office Communicator calls that tandem through the CS 1000 to other endpoints cannot be allowed to select a codec other than G.711.

The codec is configured as described in *IP Peer Networking Installation and Commissioning* (NN43001-313). In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Voice Gateway (VGW) and Codecs, as shown in the following figure.

Figure 73
Codec configuration



Loss Plan configuration

In order for DTMF digits to be transmitted at the correct volume, especially for Office Communicator 2007 to PSTN communications, the Loss Plan for the CS 1000must be correctly configured. Calls from Office Communicator 2007 to a residential Voice Mail system (VoIP to PSTN) is an example of the necessity of Loss Plan configuration.

The DTI Data Block (DDB) must also be configured for the Loss and Level Plans to be configured correctly. For information about how to configure the Loss Plan and the DTI Data Block, see *Transmission Parameters* (NN43001-282) .

ATTENTION
When any kind of in-band signaling is to be used as payload audio packets (for example, DTMF tones) in the egress direction (IP to TDM), the Signal Limiter functionality must be disabled. If problems are encountered with DTMF tones from Office Communicator contact Nortel support to ensure the Signal Limiter functionality is disabled.

Dialing Plan configuration to route to MCM

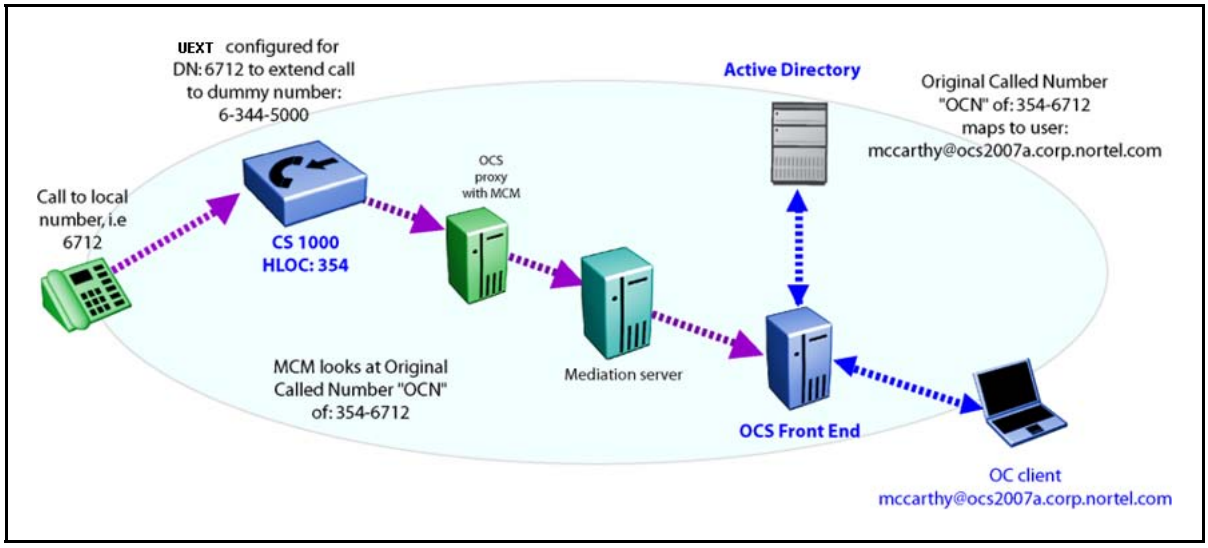
In order for calls to be extended using TLSV to the Office Communications Server, a dialing plan entry must be entered on the Call Server to send the call to the SIP trunk. This dialing plan entry does not correspond with any number that is dialable within a network, but rather is used to route the call to the MCM. The MCM service running on the OCS Proxy server handles the incoming call and directs the call to the correct Office Communicator client.

The reason for this is that the SIP Invite generated by TLSV has two fields:

- **To:** this field is used for the sole purpose of routing the invite to MCM.
- **Original Called Number (OCN):** this field is used to determine the original number called. The OCN maps to stored information about the Active Directory and sends the call to the correct Office Communicator client.

For example, the CS 1000 network can be configured, as shown in the following figure.

Figure 74
Dialing plan to route to MCM



In this figure, the CS 1000 has a HLOC of 354 and an LOC dialing plan entry of 344. The LOC dialing plan 344 is not dialable, however, calls to the DN: 6712 extend the call to the number 6-344-5000. By TLSV extending the call to 6-344-5000, a SIP Invite is sent to the OCS Proxy server.

The OCS Proxy server runs MCM, which handles the Invite and reads the Original Called Number as 354-6712. The call is sent to the Mediation server and To and RequestURI are mapped to the Line URI. In this diagram the user is mccarthy@ocs2007a.corp.nortel.com

The purpose of configuring is to ensure that the Office Communicator has the same phone number for both incoming and outgoing calls.

For more information about Dialing Plans, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

Configuring Telephony Services

Telephony Services (TLSV) is used to twin incoming calls so users can answer the calls on their desktop phone or Office Communicator 2007.

For incoming calls to be extended to the twinned Office Communicator client, a UEXT Terminal Number (TN) must be defined for that DN. A new Universal Extension TN is configured as a Telephony Services client. Telephony Services is defined as the prompt TLSV in response to UXTY. It cannot be changed once it has been set. To change UXTY, remove (OUT) and reconfigure (NEW).

Basic Client Configuration (BCC) can program the new TLSV subtype for UEXT TNs. The TLSV subtype will be the required value for all UEXTs associated with OCS 2007. For more information about BCC, see "Basic Client Configuration" (page 72).

The UEXT TN is configured to send the call to another number. In the case of twinning to Office Communicator, the call is sent to a number that is not dialable but routes the invite to the Office Communications Server. For more information, see "Dialing Plan configuration to route to MCM" (page 186).

ATTENTION
If SIP CTI control is also enabled for that telephone, the UEXT TN cannot be MARP 0.

When you use a UEXT, the MARP must be on the DN key of the phone itself, not the UEXT. If the MARP is on the UEXT, CTI clients (such as Office Communicator) do not receive Remote Call Control call pop-ups for incoming calls (in addition to other problems).

Note that MARP is assigned to the first DN key created, so if you create the UEXT first and assign a DN key, it becomes the MARP by default. If you add a phone later with the same DN (to twin the phone with Office Communicator) the MARP stays on the UEXT and you encounter this exact situation. The following is an example of a supported configuration:

Table 42
LD 22

Prompt	Response	Description
REQ	prt	
TYPE	dnb	
CUST	0	
DN	2070	
DATE		
PAGE		
DES		

Screen output

```
DN 2070
TYPE I2002
TN > 096 9 08 15 V t y
KEY 00 MARP DES I2002 i F m > 16 APR 2008
(I2002 )
```

```
TN 061 0 00 00 KEY 00 DES I2002 16 APR 2008
(UEXT)
```

Table 43
LD 20

Prompt	Response	Description
REQ	prt	
TYPE	tnb	
TN	096 0 08 15	

Screen output

```
DES OCS
TN 096 0 08 15 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY TLSV
NUID
NHTN
ERL 0
ECL 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SFLT NO
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD DSX VMD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
```

```
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND FLXD FTTC DNDY FDSD
NOVD VOLA VOUD CDMR ICRD MCDD T87D MSNV FRA PKCH
CPND_LANG ENG
HUNT
PLEV 02
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 2070 0
ANIE 0
01 HOT P 4 8888
ANIE 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
```

```
31
DATE 16 APR 2008
```

Calling Line ID table configuration

The Calling Line Identification (CLID) table is used to correctly build the CLID for both Private network and Public network calls from a number/extension. The CLID table is used by all CS 1000 telephones and is required for Office Communicator calls to work.

In Private network calls where the Uniform Dialing Plan (UDP) is used, the Location Code (LOC) is normally prefixed to the Called and Calling number. Therefore, the Active Directory for all users must include the LOC for their number. A telephone number of ESN 354-6712, has an LOC of 354 and an extension of 6712.

For TLSV twinning to work correctly in a UDP environment, the full Original Called Number (OCN) must be sent by the CS 1000 to the Office Communications Server. To have the full OCN sent, the CLID table must be configured with the Home Location (HLOC) of the CS 1000.

Outgoing Office Communicator calls to the Public network must have the CLID table used by the associated MARP TN (a TN with the same extension used by Office Communicator marked as MARP) correctly configured. The associated MARP TN must point to a CLID table that has the International Country Code configured. The International Country Code is the prompt INTL (in North America the value is 1). In North America the associated MARP TN must point to a CLID table that also has the Home Exchange configured. The Home Exchange is the prompt HLCL and is the ‘967’ in 1-800-967-2070.

For example, a phone with an extension of 2070, an ESN number of 231-2070, and a Public Number of 967-2070 in North America is configured in the following manner:

Table 44
LD 11

Prompt	Response	Description
REQ	prt	
TYPE	i2002	
TN	061 0 00 00	
DATE		
PAGE		

The following is a portion of the screen output:

```
DNDR 0
KEY 00 SCR 2070 0 MARP
DPND_LANG ROMAN
NAME Chris Smith
```

This user is configured to use the default CLID table entry of 0 (the CLID table number is always next to the extension). The CLID table entry 0 must have the correct HLOC of 354, HLCL of 967, and INTL of 1.

The CLID table entry of 0 with an HLOC of 354 is configured in the following manner:

Table 45
LD 15

Prompt	Response	Description
REQ	chg	
TYPE	net	
TYPE NET_DATA		
CUST	0	
OPT		
AC2		
FNP		
CLID	yes	
SIZE	5	
INTL	1	
ENTRY	0	
HNTN		
HLCL	967	
HLOC	354	
...		

The response to SIZE must be a number greater than 0. The response to ENTRY must match the CLID table entry for the target telephones. Generally the default is 0.

Home LOC and Home NPA configuration

In order for the correct Calling Line Identification (CLID) to be correctly displayed for Office Communicator calls to the Public network, both the HLOC and HNPA can require configuration. All Office Communicators that are part of an ESN network require HLOC configuration. All Office Communicators that make calls to the Public network in North America require that the Area Code be configured.

For more information about the HLOC and HNPA, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

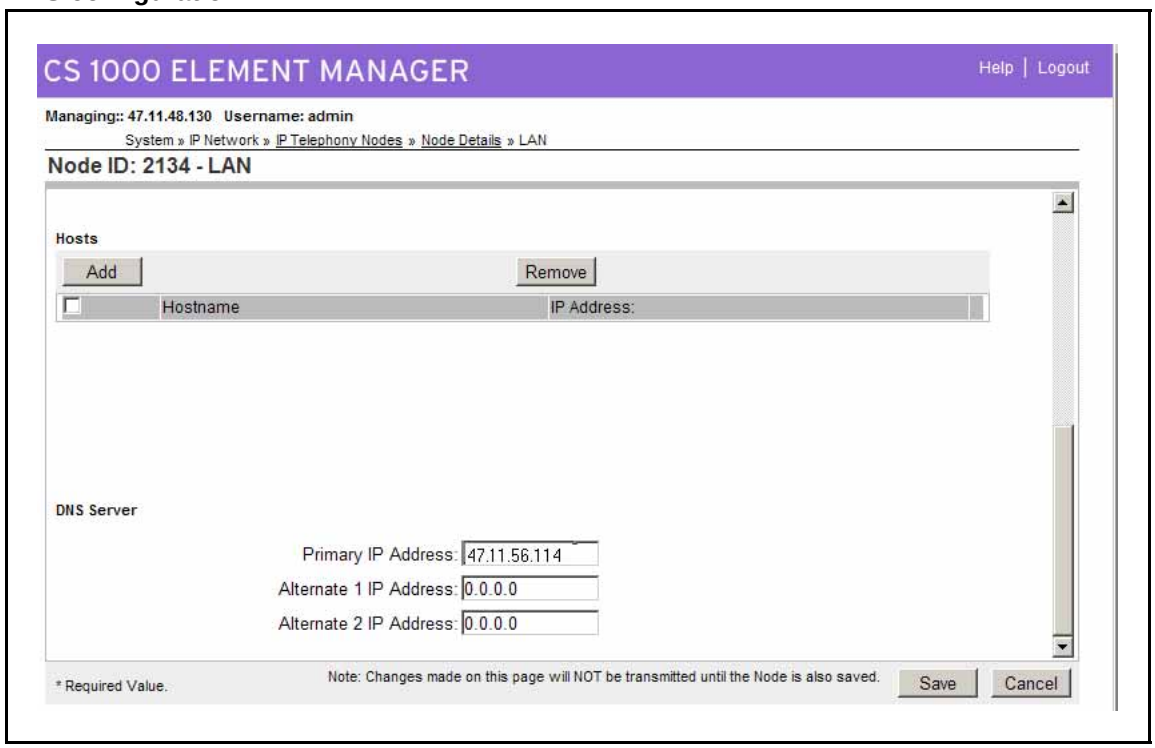
DNS Server configuration

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click LAN, you can enter up to three DNS server IP addresses. The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all OCS and Enterprise Edition Pools. Also, the FQDN must resolve to the IP address of the OCS for all types of DNS queries (not just for the SIP service type).

DNS server must respond with the correct IP for a generic DNS query. There are a number of different types of DNS queries that can be performed.

ATTENTION
The Signaling Server must be rebooted to ensure that all DNS server configurations take effect.

Figure 75
DNS configuration



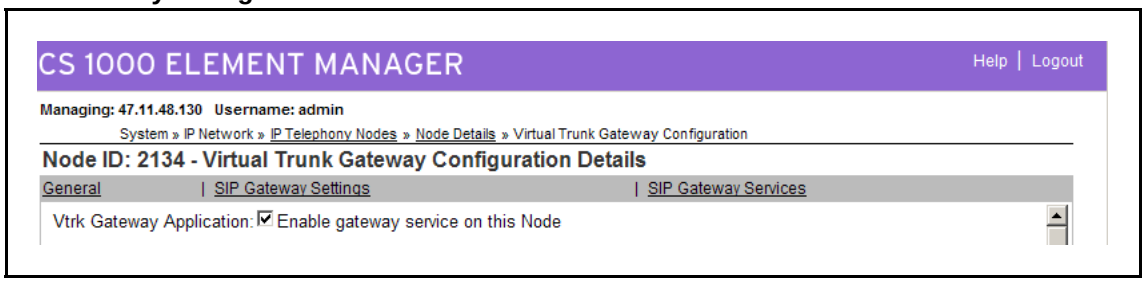
SIP Trunk configuration

For an Office Communications Server to use a CS 1000 as a SIP Gateway, SIP Trunks must be configured on the CS 1000. The configuration of the SIP Trunk requires that configuration be done on both the Call Server and the Signaling Server. For more information about how to configure SIP trunks, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

A CS 1000 with existing SIP trunks requires a configuration change to be compatible with Office Communications Server. In order for a SIP Trunk to communicate with Office Communications Server, the SIP Transport Protocol must be configured as TCP, not UDP (see Figure 76 "SIP Gateway configuration window" (page 194)). However, this is not valid when SPS in Proxy All mode is used, since everything goes through SPS.

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw). The default Local SIP Port of 5060 is required.

Figure 76
SIP Gateway configuration window



ATTENTION
The Route Data Block (RDB) must have the prompts NCNA and NCRD configured to Yes. Otherwise, calls that are Twinned to Office Communicator using TLSV do not work.

ATTENTION
The Route Data Block (RDB) must not have a value configured for the prompt INST. Otherwise, incoming calls from Office Communicator to the CS 1000 do not work.

ATTENTION
When configuring the D Channel used by the SIP Trunk for Converged Office Telephony Gateway and Services, configure the NASA prompt to Yes. Failure to do so can result in limited call transfers through Office Communicator.

The CS 1000 SIP trunk that receives Office Communicator calls must be configured to ESN5, and all associated Virtual trunks must be configured to WNK/WNK. These settings are required so that Office Communicator calls to the Public Network display the correct CLID and have the same Network Class of Service (NCOS) as a call from the associated CS 1000 IP Phone.

The Virtual trunk is WNK/WNK if the output from Element Manager, or a terminal window, is:

DES IPTIE
TN 081 0 00 02 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 000
TRK ANLG
NCOS 0
RTMB 10 3
CHID 3
TGAR 0
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0 *
CLS UNR DIP WTA LPR APN THFD XREP P10 NTC MID
TKID *
AACR NO

ATTENTION
All of the SIP Virtual Trunks must be configured to WNK WNK.

The Route Data Block is ESN5 if the output from Element Manager, or a terminal window, is:

TYPE RDB
CUST 00
DMOD
ROUT 10
DES IPROUTE

TKTP TIE
VTRK YES
ZONE 100
PCID SIP
... ANTK
SIGO ESN5
STYP SDAT

ATTENTION
If the Route Data Block (RDB) already has associated Virtual Trunks and is configured to SIGO STD, all Virtual Trunks must be removed before the RDB can be changed to ESN5.

Route list data block

The Route List Data Block that is used for Office Communicator SIP trunks must have the prompt DORG configured to No. Otherwise, Office Communicator in dual mode will receive two toasts instead of a merged one. One is with CLID information of the transferring telephone and the other is with CLID information of the original caller. This occurs in some transfer and conference scenarios. The default value for DORG is No.

Changing the value to DORG=YES offers new ISDN CLID enhancements. For more information about this feature, see *New in this Release* (NN43001-115) document.

The Route List Data Block can be checked in LD 86. See Table 46 "LD 86" (page 196).

Table 46
LD 86

Prompt	Response	Description
REQ	PRT	
CUST	00	
FEAT	RLB	
RL1	10	
...		
DORG	NO	
...		

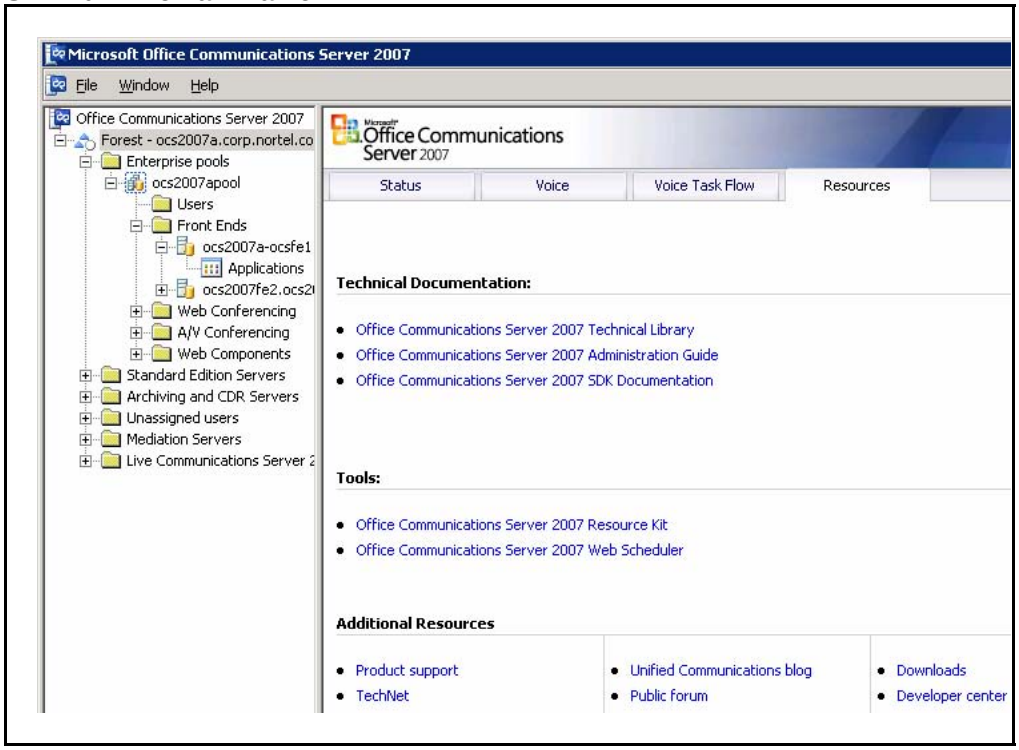
Domain naming

In most configurations where the CS 1000 acts as a SIP Gateway for a Office Communications Server, it is recommended that the SIP Trunk Domain name and the Office Communications Server Domain name be an exact match.

In situations where both the OCS and the CS 1000 have already both been assigned a domain name, and the domain names do not match, there is an alternative. MCM can be configured to register to the NRS using an End_Point_Name@Service_Domain_Name.

The domain is listed under the Domains folder in the Management console for Office Communications Server. For example, in the following figure, the Office Communications Server Domain is ocs2007a-ocsfe1.ocs2007a.corp.nortel.com.

Figure 77
SIP Trunk Domain name

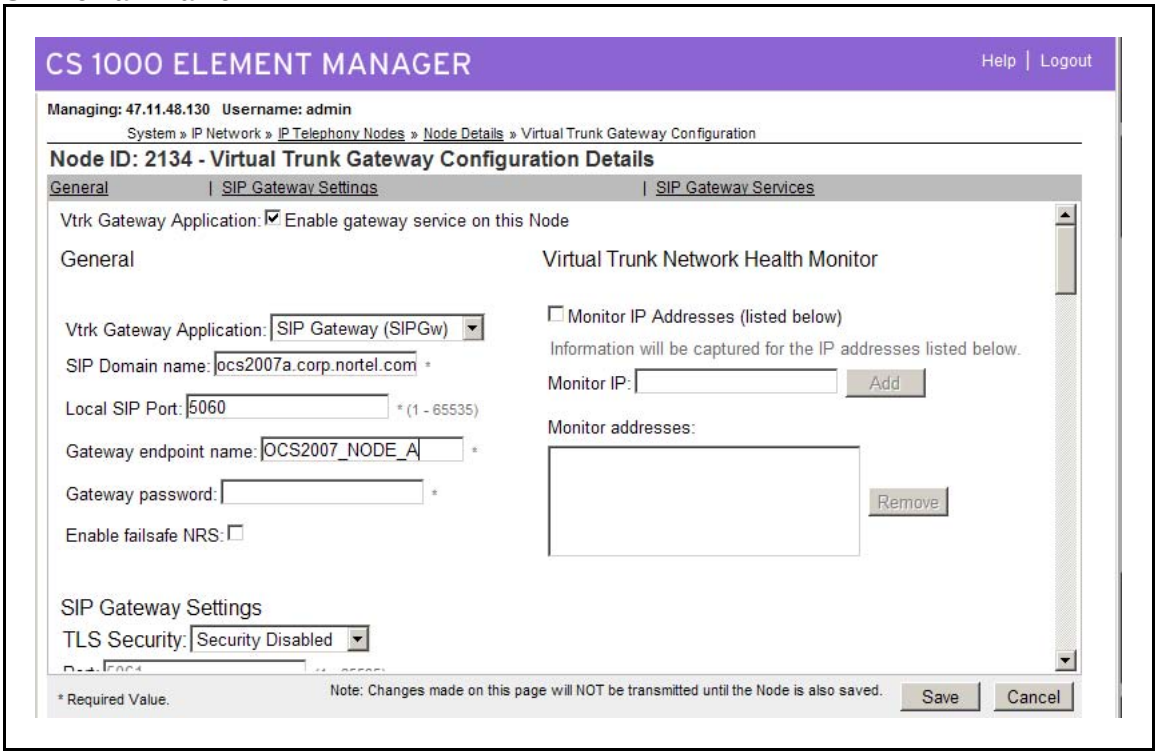


Configuring the SIP Trunk Domain name

The configuration of the SIP Trunk Domain name describes how to configure the SIP Trunk domain name to match the Office Communications Server domain name. In Element Manager on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a

node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw), as shown in the following figure

Figure 78
SIP Domain Name

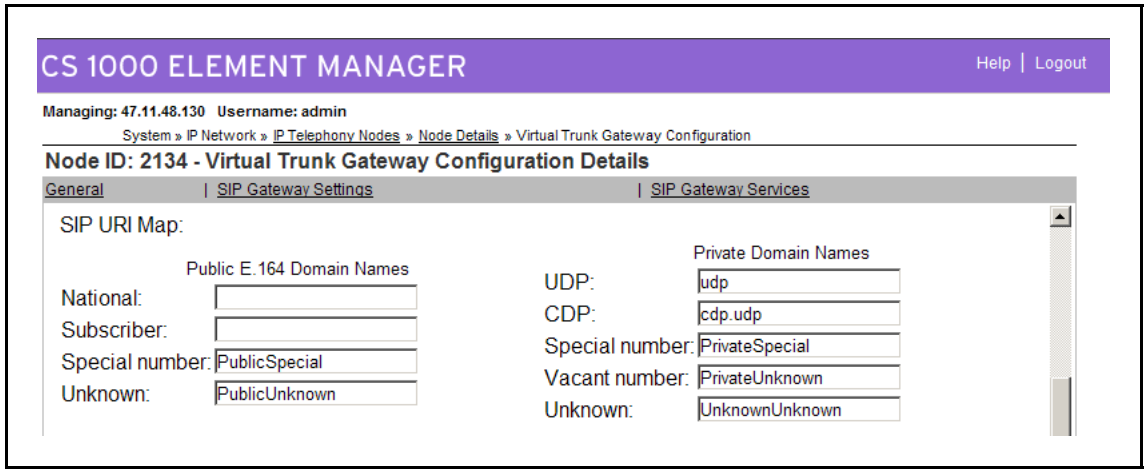


URI Mapping

The SIP URI Map must be configured in order to correctly register with the NRS. The Private/UDP domain name or Private/CDP domain name is used by MCM to obtain the correct context of the Calling Number.

The SIP URI Map is also configured in Element Manager. On the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw), as shown in the following figure.

Figure 79
SIP URI Map



The SIP URI Map must match the NRS server configuration in the following manner:

- The Private/UDP domain name maps to the L0 Domain on the NRS
- The Private/CDP domain name maps to the L1 Domain on the NRS

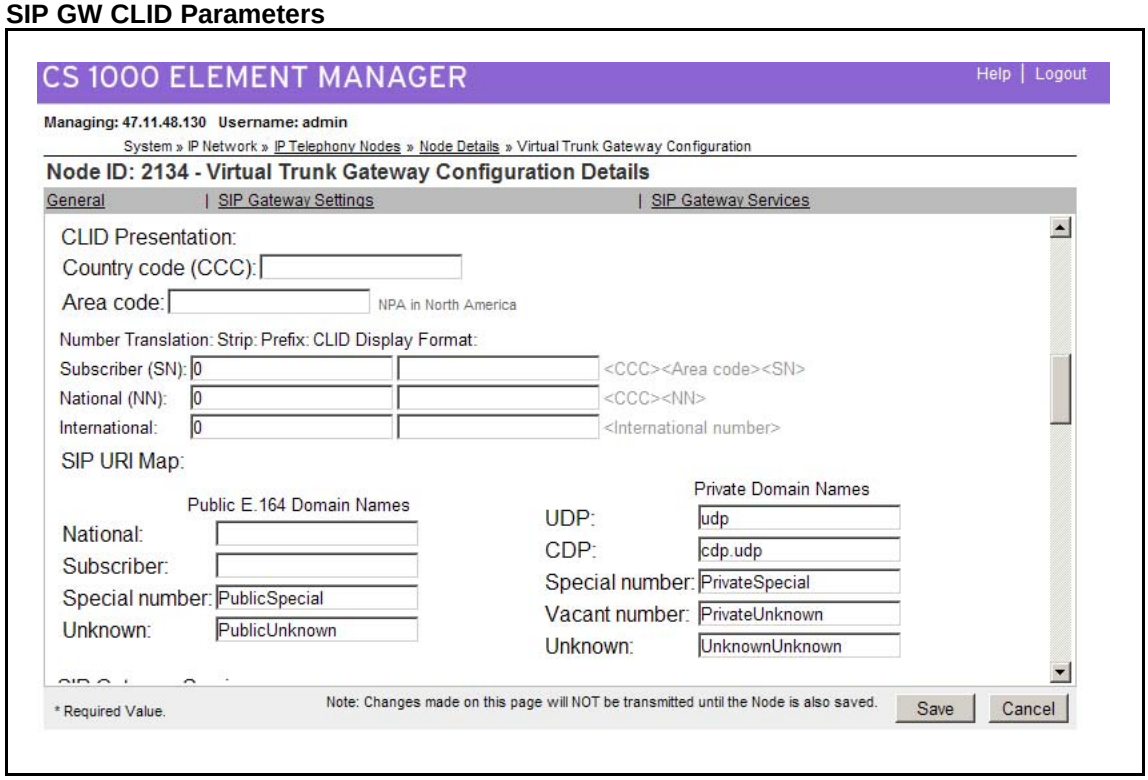
MCM must be configured to match one of the domain names. For example, in a UDP network, the configured domain name is OCS2007_UDP in MCM. Mediation server supports Mediation server routing and Mediation server load balancing. MCM 4.x manipulates the SIP URI for VoIP and Device URI for RCC to seamlessly integrate with OCS 2007 and the CS 1000. The mapping phone number into SIP URI user id is not required because it is processed internally by the Mediation server. MCM 4.x should only process “x-nt-ocn-id” header of incoming messages in the same manner as before.

SIP Gateway CLID Parameters configuration

The SIP Gateway CLID parameters are used to adjust the format of telephone numbers for incoming call appearances. For Office Communicator, these settings impact the format of numbers that appear on the incoming call pop-up for Telephony Gateway and Services (the SIP call leg for Office Communicator clients that are twinned with a CS 1000 DN through a TLSV).

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw) and scroll down to the CLID Presentation section, as shown in the following figure.

Figure 80
SIP GW CLID Parameters



Note: These settings are independent of the similar SIP CTI CLID parameters to allow independent control of the format of numbers on the incoming call pop-up for telephony gateway and services.

For all public calls (subscriber (for example, NXX in North America), national (for example, NPA in North America), or international) E.164 fully qualified numbers are used to represent the caller. This is possible through the use of the following parameters:

- Country Code
- Area Code
- Subscriber/Number of Digits to strip
- Subscriber/Prefix to insert
- National/Number of Digits to strip
- National/Prefix to insert

The E.164 format of subscriber calls (for example, NXX in North America) is:

+<countrycode><area code><subscriber number>.

The parameters Subscriber/Number of digits to strip and prefix to insert are used to modify the format of subscriber numbers presented from the PSTN due to region specific requirements.

The E.164 format of national calls (for example, NPA in North America) is:

- +<countrycode><national number>.

The parameters National / Number of digits to strip and prefix to insert are used to modify the format of national numbers presented from the PSTN due to region specific requirements.

Parameter: Country Code
This parameter defines the country code to be used in CLID generation.

Parameter: Area Code
This parameter defines the area code to be used in CLID generation.

Parameter: Subscriber / Number of Digits to strip
For incoming subscriber (NXX) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: Subscriber / Prefix to insert
For incoming subscriber (NXX) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

Parameter: National / Number of Digits to strip
For incoming national (NPA) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: National / Prefix to insert
For incoming national (NPA) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

SPS configuration

SIP Proxy Server (SPS) is configured through MCM (see Figure 55 "MCM configuration window" (page 160)).

SPS options include:

- **Primary and Secondary IP addresses**
- **Three different modes**: Proxy All, Redirect, and Proxy SIP Gateway Calls
- **Transport**: TLS (5061) and TCP (5060)

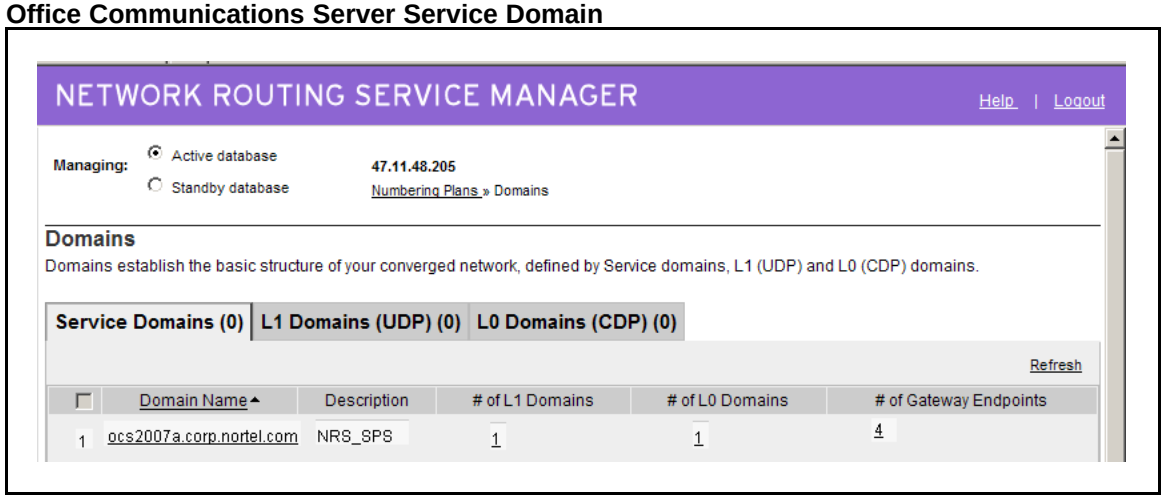
NRS configuration

The Server IP running the MCM application (generally an Office Communications Server 2007 Proxy) must be configured on the NRS as a dynamic SIP endpoint, or gateway, and not as a collaboration server.

An Office Communications Server Service Domain must be created for the Signaling Server and MCM. The Signaling Server and MCM register to the Office Communications Server Service Domain on the NRS. The Service Domain between the NRS and the Office Communication Server may or may not match the domain name of the Office Communications Server.

The MCM is configured to register with End_Point_Name@Service_Domain_Name, where the Service Domain Name matches the Service Domain configured on the NRS. In the Network Routing Service Manager navigation tree, click Numbering Plans and Domains. The Service Domains tab appears, as shown in the following figure.

Figure 81
Office Communications Server Service Domain



In Figure 81 "Office Communications Server Service Domain" (page 202), the NRS is configured with the matching Service Domain of ocs2007a.corp.nortel.com.

The L1 and L0 Domains must also be configured and match what the CS 1000is configured under SIP URI Map. Dynamic Gateway endpoints must be configured for the CS 1000 and the MCM with appropriate dialing plan entries.

The NRS must have the same UDP or CDP dialing plan prefix to route calls to the MCM endpoint. This UDP or CDP dialing plan prefix is the same one configured for the TLSV calls.

For example, the Location Code (LOC) 354 from the TLSV example appears as:

01 HOT P 8 63545000

The NRS must be configured to analyze and qualify numbers dialed from the Office Communications Server (for example, if you configure prefixes to identify the call type, then you might use 6011 for International, 61 for National, and 6 for UDP).

For more information about how to configure the NRS, see *IP Peer Networking Installation and Commissioning* (NN43001-313) .

CDR configuration

Call Detail Recording (CDR) is supported for outgoing calls from Office Communicator. Office Communicator CLID is included in the CDR record. From Office Communicator, when you make a call, the Office Communicator CLID (extracted from the Active Directory) is identified.

The following is an example of an outgoing call:

N 024 00 A030 001 T012 023 09/12 10:48:23 00:00:02.0 614165558888&2452070XXXXXXXXX

The dialed number appears at the end (XXXXXXXXX) and the Office Communicator CLID and the CDR records appear after the ampersand (&); a location code of 245 is followed by 2070 (a location code of 245 followed by 2070). Again, MCM supports redundant NRS configurations.

E.164 International Format Numbers from Office Communicator - Computer Calls (SIP Gateway)

The dialed number sent from Office Communicator to the CS 1000 for SIP GW calls follows the same format as those dialed on the station. There is no distinction within or outside North America for the handling of computer (SIP Gateway) calls.

Calls to International format numbers are handled by the SIP Gateway and arrive with a request URI in the SIP INVITE for the following call:

sip: +CCCXXXXXXXX@domain; user=phone

In order to support these calls, placed through the SIP Gateway, you must configure the parameters CNTC, NATC, and INTC in LD 15. These parameters ensure that fully qualified numbers within the same country are dialed as national numbers by stripping the country code and adding the national dial prefix.

Example 1 (Outside of North America)
AC1=0, CNTC=31, NATC=0, INTC=00
The URI incoming for the SIP INVITE for the call is:
sip:+31123456789@domain.com;user=phone
The digits sent to the outgoing trunk are: 00123456789
The digits seen on the DCH for the outgoing trunk are: 0123456789

Example 2 (North America)
AC1=8, CNTC=1, NATC=1, INTC=011
The URI incoming for the SIP INVITE for the call is:
sip: +12125551212@domain.com;user=phone
The digits sent to the outgoing trunk are: 812125551212
The digits seen on the DCH for the outgoing trunk are: 12125551212

Phone number normalization

Now that you have completed the installation and configuration of Telephony Gateway and Services, proceed directly to the next step in the process: “Normalizing phone numbers” (page 244).

Remote Call Control configuration

This section describes the process to configure the Remote Call Control with the SIP CTI component.

Office Communications Server, Active Directory and MCM must be configured properly prior to configuring the Remote Call Control component.

Enabling Remote Call Control and PBX integration

By default users are configured for PC-to-PC communications. Configuring Remote Call Control and PBX integration is done from the User properties in Active Directory and on the Office Communicator client.

Use the following procedures to enable RCC and PBX integration.

Step	Action
1	On the OCS configuration console, go to Users.
2	Choose a user, right-click and select **Properties**.

3 In the properties window, in the **Advanced Options** section, click the **configure** button.

4 Choose **Enable Remote call control** to enable clients control of the PBX phone or **Enable Enterprise Voice** and click the **Enable PBX integration** box to enable both Remote Call Control and Enterprise Voice.

--End--

Enabling RCC and PBX integration on the OC client

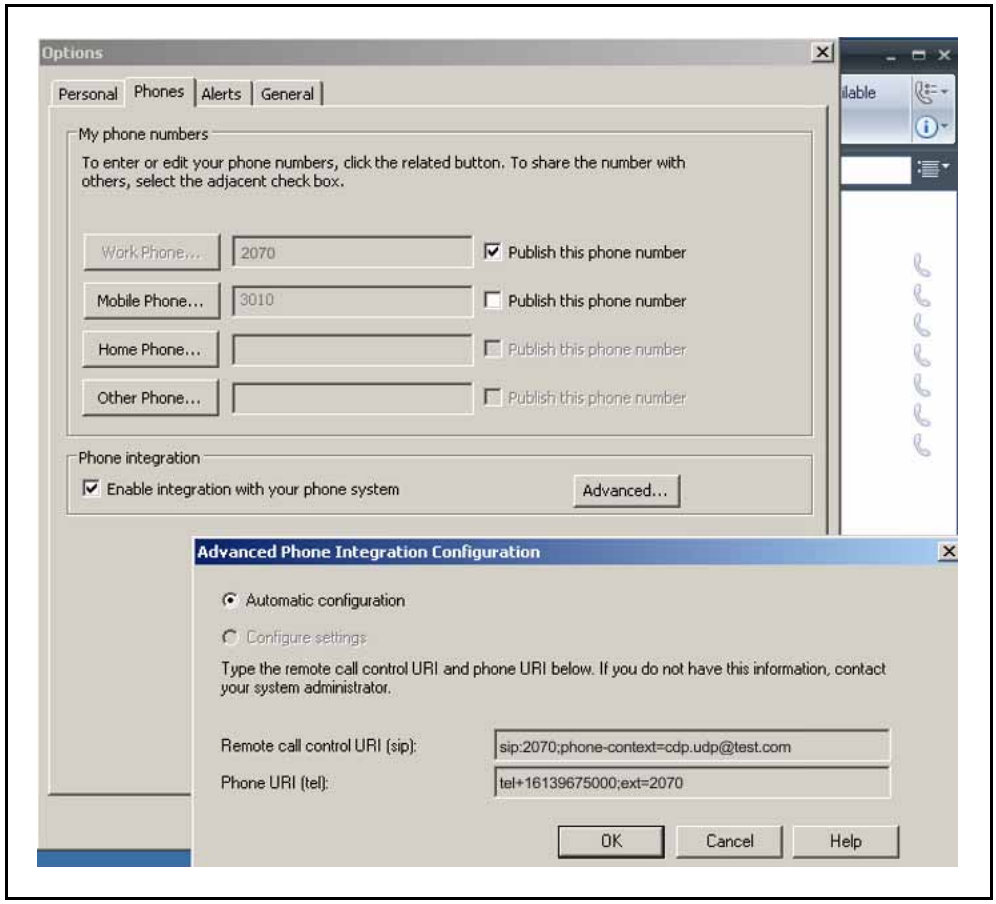
After phone integration options are enabled for a user on the server, they are enabled on the OC client.

Use the following procedures for enabling RCC and PBX integration on the OC client.

Step	Action
1	Go to the **Office Communicator** menu.
2	Choose **Tools** and then select **Options**.
3	Go to the **Phones** tab.
4	Click **Enable integration with your phone system** box to integrate Communicator to control your desktop phone. See Figure 82 "Enable integration with your phone system" (page 206).
5	Click **Advanced** and select **Automatic configuration**. Click **OK**.

--End--

Figure 82
Enable integration with your phone system



CS 1000 configuration

Application Module Link (AML) is the main interface used to support call control requests from SIP CTI clients between the SS TR/87 FE application and the CS 1000.

Per-TN configuration is required to define which TNs are used for SIP CTI and to define the specific DN keys on each TN that are available for control by SIP CTI applications.

Configuring the AML

The following tables (“Configuring the AML” (page 206) and Table 48 "LD 17: Configure VAS (Value Added Server)" (page 207)) display the prompts used for AML link configuration:

Table 47
LD 17: Configure AML Link

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	
ADAN	<new ELAN #>	A new AML link; the link is an ELAN type. The link number can be from 32 and 127 on a large system. An AML link number within the above range implies that the transport is over a TCP link.
CTYP	ELAN	Card Type: ELAN

To verify that the AML link is up and running, use the STAT ELAN command from LD 48:

LD 48
STAT ELAN
ELAN #: 032 DES: CDLCS
APPL_IP_ID: 47 .164 .116 .43 : 0000F600 LYR7: **ACTIVE** EMPTY
APPL **ACTIVE**

For more information about the STAT ELAN command, see *Software Input Output Reference — Maintenance* (NN43001-711) .

ATTENTION
For redundancy, one AML link is required for each Front End within the node, regardless of whether the Front End is a leader or a follower.

Table 48
LD 17: Configure VAS (Value Added Server)

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	VAS	Value Added Server
VAS	NEW	
VSID	<VAS#>	VAS ID, ranges from 32 to 127 on a large system
ELAN	<LINK #>	AML ELAN link number provisioned when the AML link was created
SECU	YES	Security For Meridian Link Applications. Enable this for the TR/87 FE application on the Signaling Server to acquire DNs

TLSV ISM

Incremental Software Management (ISM) is a flexible mechanism that allows the telephone provider company to charge for the Telephony Services feature independently of other related available features. The

ISM also gives the telephone service provider the flexibility to charge for the Telephony Services units that are configured on the system on per user basis.

A new ISM for the TLSV type of UEXT is available. The TLSV ISM count will be incremented when UXTY prompt is configured as TLSV.

Configuring the SIP CTI TR/87 ISM limit

Incremental Software Management (ISM) (SIP CTI TR/87) is used to define the number of TNs that can be configured with the T87A class of service. The TR/87 configuration for a given TN requires that in addition to the existence of the CLS T87A, the controlled line itself must also be identified as an AST DN. This implies that AST ISMs are also required.

As part of the ordering process, a corresponding AST license is provided for each SIP CTI TR/87 license. This ISM limit is prompted only if package 408 (MS_CONV) is unrestricted (requires level 2 packages).

The SIP CTI TR87 ISM is an instant ISM and does not require a cold start of the Call Server to take effect (see Figure 83 "ISM Limit printout" (page 208))

Table 49
LD 22

Prompt	Response	Description
REQ	prt	
TYPE	slt	

Figure 83
ISM Limit printout

```
    TYPE                 slt                Print System Limits

<…>
PCA                    32767    LEFT 32767    USED      0
ITG ISDN TRUNKS        32767    LEFT 32767    USED      0
H.323 ACCESS PORTS     32767    LEFT 32767    USED      0
AST                    32767    LEFT 32767    USED      0
SIPCONVERGED DESKTOPS  32767    LEFT 32767    USED      0
SIP CTI TR_87          32767    LEFT 32767    USED     11
RAN CON                32767    LEFT 32767    USED      0
MUS CON                32767    LEFT 32767    USED      0
SURVIVABILITY              0    LEFT     0    USED      0
<…>
```

Configuring a station

SIP CTI control of a DN key can be supported on IP, digital, and analog stations.

ATTENTION
Features such as Make Call and Answer Call depend on the hands-free capability of the station and the on-hook default path configuration on the station. Therefore the use of certain features on stations without hands-free support is limited.

A new CLS (T87A) is introduced to allow a TN to support the SIP CTI application.

The AST prompt is used to configure which DN key on the TN is controlled or monitored by the SIP CTI application. A maximum of two keys per TN can be configured as AST keys.

CLID information is sent, or suppressed, to Office Communicator based on the CLS CNDA/CNDD consistent with the presentation of the CLID information about the station display itself.

This affects whether CLID information (that can be available for calls that do not map to Active Directory users) appears on the Office Communicator call toast (for example, PSTN calls).

Considering MADN (Multiple Appearance DN)

When you configure a station, you must consider certain issues if Office Communicator is used in a MADN environment:

- When multiple TNs exist in a MADN group, the T87A CLS and AST configuration are configured only on the MARP TN
- When twinning a station with Office Communicator using a TLSV, the MARP TN within the MADN group must be on a station and not on the TLSV. For more information, see Table 50 "LD 11–Twinning a station" (page 209).

Table 50
LD 11–Twinning a station

Prompt	Response	Description
REQ	prt	
TYPE	dnb	
CUST	0	
dn	2070	

Screen Output

DN 2070
CPND
XPLN 15
DISPLAY_FMT FIRST,LAST
TYPE SL1

TN 100 0 03 04 V KEY 00 MARP DES DLOCS2 3 DEC 2007 (2004P2)
TN 100 0 03 05 V KEY 00 DES OCS 16 APR 2008 (UEXT)
NACT

- Any Remote Call Control service request sent by Office Communicator, such as Make Call or Answer Call, always apply to the device defined as the MARP TN.
- For SCR keys telephony, presence updates such as On the Phone, are supported for all TNs within a MADN group. For example, answering a call on a wireless station SCR key on a non-MARP TN shows the Office Communications Server user as On the Phone.
- For MCR keys telephony, presence is supported only for the MARP TN within a MADN group. For example, answering a call on a wireless station MCR key on a non-MARP TN does not show the Office Communications Server user as On the Phone. Only calls answered on the MARP TN affect the presence status of that user.
- Incoming calls to a Multiple Appearance Directory Number (MADN) in the Make Set Busy (MSB) mode, are signified by an indicator next to the Directory Number (DN) key. These incoming calls can be answered while MSB is active. Calls to any Single Appearance Directory Number on the telephone receives a busy indicator. For more information, see *Features and Services Fundamentals* (NN43001-106).

NRS configuration

Using NRS is optional. If NRS is used, MCM and TR/87 FE must be configured on the NRS as the Gateway Endpoints.

The corresponding Routing Entries must be defined to support SIP gateway calls.

Signaling Server configuration

The TR/87 FE application shares the TPS master/follower mechanism to provide redundancy within a node. The TR/87 FE application shares one instance of the SIP stack with the SIP GW and correspondingly uses some of the existing SIP GW configuration parameters:

- SIP Transport Protocol, Local SIP Port, SIP Domain Name
- The SIP URI map

The IP address and domain name of any Office Communications Server proxy responsible for forwarding TR/87 traffic to the Signaling Server must be added to the Signaling Server Host Table in Element Manager. Configure SIP CTI-specific parameters in Element Manager.

ATTENTION
When the SIP CTI service is enabled and any dependent configuration parameter is modified in Element Manager, all active SIP CTI sessions are terminated so the configuration data can be updated.

Node parameter configuration

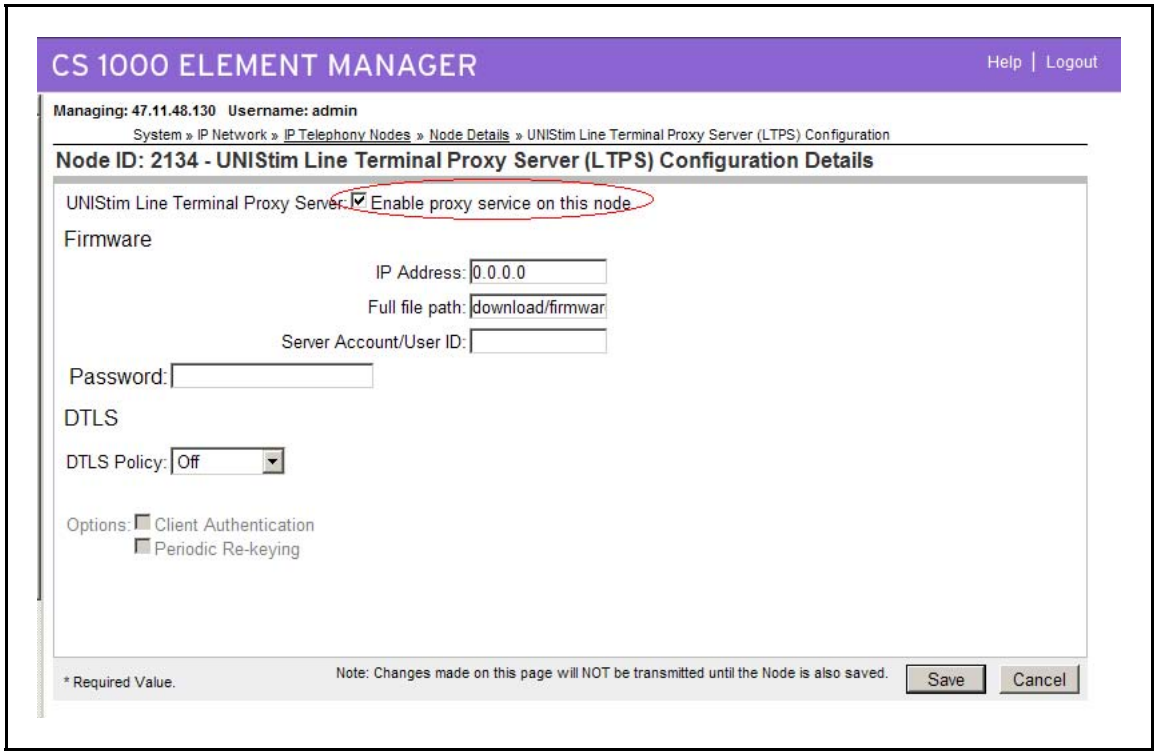
The node IP is the IP address of the TR/87 FE:

- You can configure multiple nodes to support TR/87 applications for additional capacity. The Remote Call Control SIP URI of users determines which node they use.
- An AML restriction dictates that only one application can acquire a given DN on a Call Server.

ATTENTION
When you add additional nodes to balance TR/87 load, SIP routing must be configured so that all clients that attempt to control a DN terminate on the same node.

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Terminal Proxy Server (TPS). The UNIStim Line Terminal Proxy Server page appears, as shown in the following figure. The TR/87 FE application can run within a TPS node or a non-TPS node.

Figure 84
TR/87 Node configuration



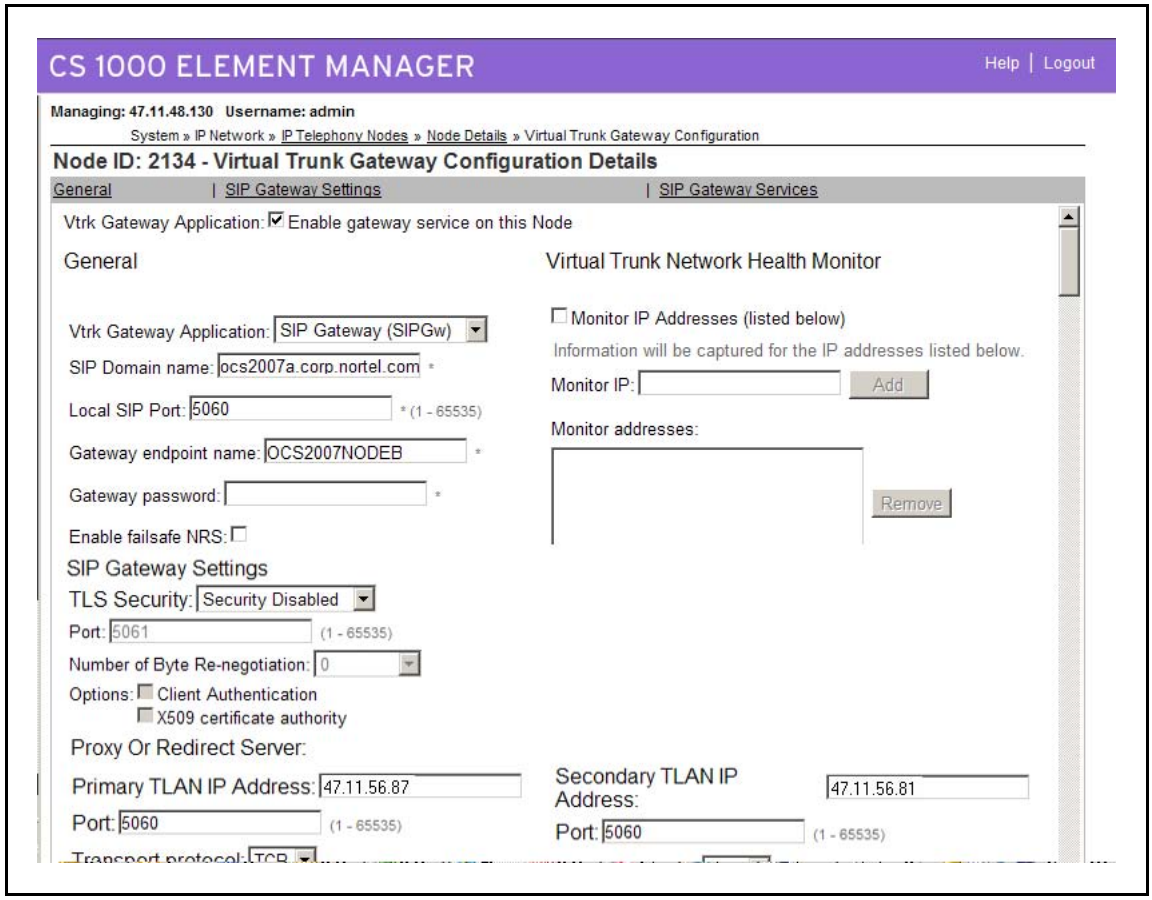
SIP Gateway parameter configuration

The SIP Gateway application must be enabled. To enable the SIP Gateway, TR/87 FE uses the following SIP Gateway configuration parameters, as shown in the following figure.

- SIP Transport Protocol (must be TCP for Office Communications Server 2007 deployment)
- Local SIP Port (default 5060)
- SIP Domain Name

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw). The Virtual Trunk Gateway Configuration Details page appears, as shown in the following figure.

Figure 85
SIP Gateway configuration



DNS Server configuration

The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all OCS servers and Enterprise Edition Pools. Also, the FQDN must resolve to the IP address of the OCS server for all types of DNS queries (not just for the SIP service type).

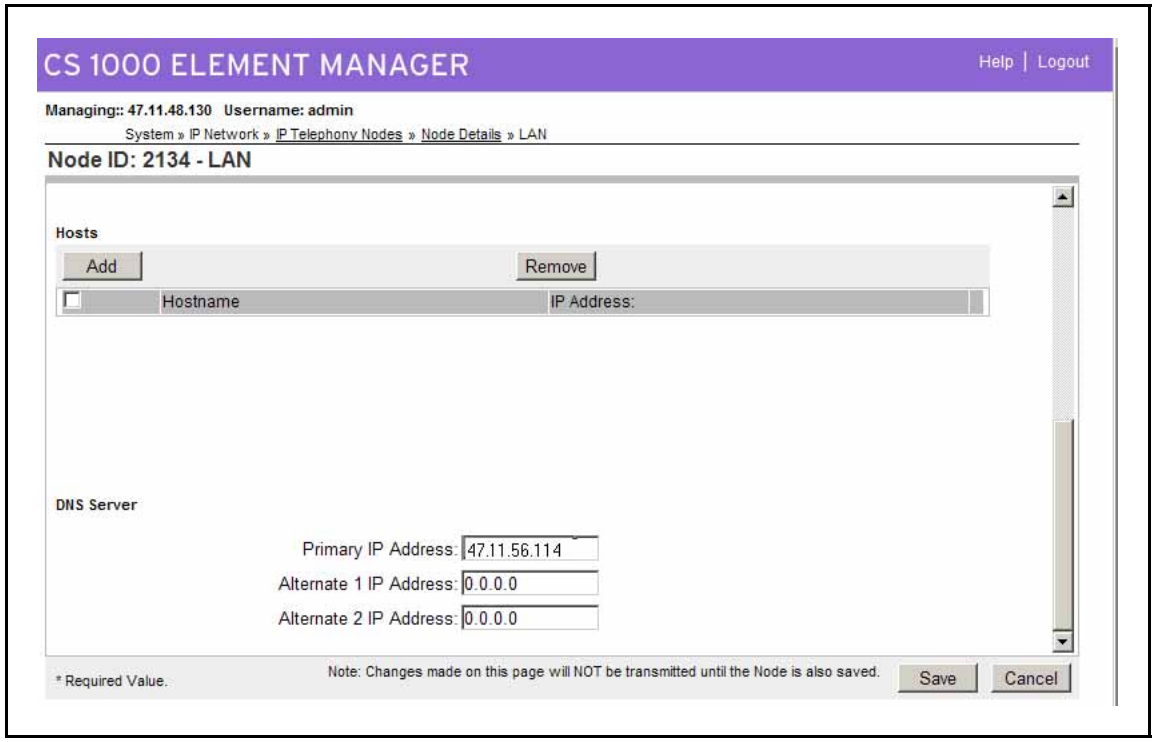
DNS server must respond with the correct IP for a generic DNS query. There are a number of different types of DNS queries that can be performed.

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click LAN, as shown in the following figure.

Step	Action
1	Log on to Element Manager and navigate to LAN configuration.
2	Enter the FQDN of up to three DNS servers.

--End--

Figure 86
DNS configuration



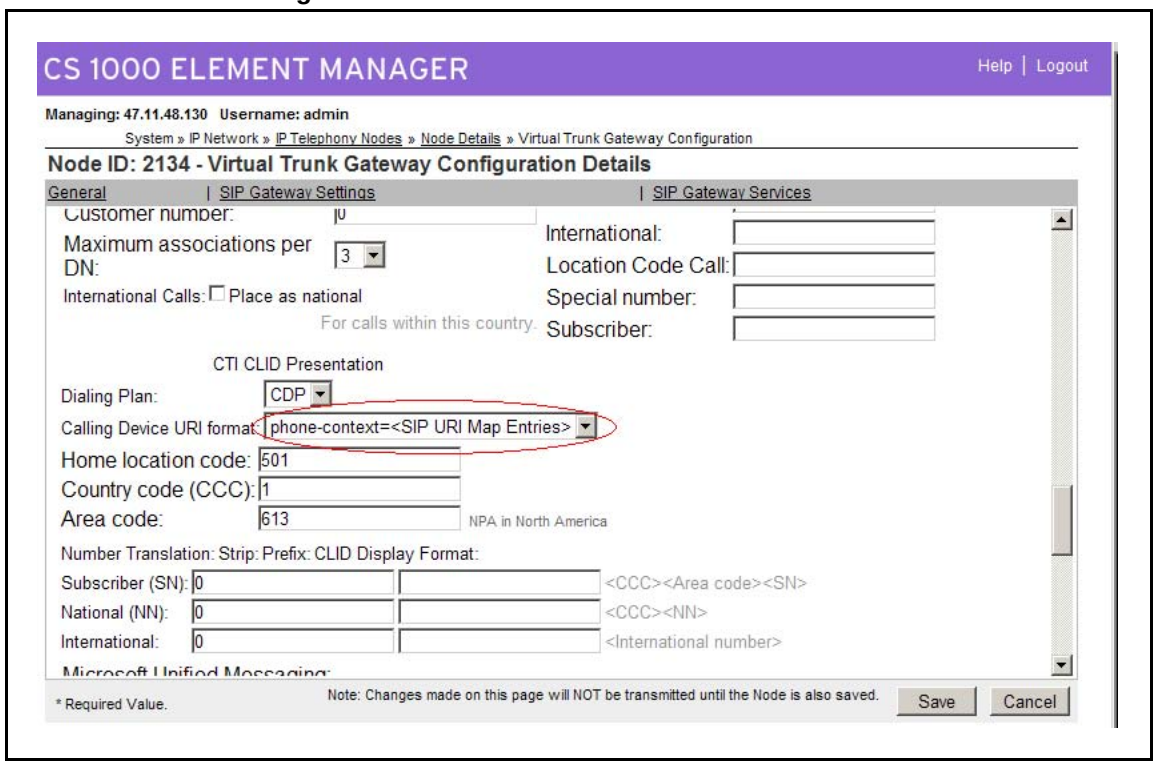
SIP CTI Services configuration settings

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw), as shown in the following figure. The Calling Device URI Format must be configured as **phone-context=<SIP URI Map Entries>** to support OCS 2007 RCC. Ensure the **Dial Plan prefix** section values under SIP CTI Services are configured. Click **Save and Transfer** the configuration and then reboot the Signaling Server.

For each of the SIP CTI settings, if you make a configuration change and a save and transfer is performed, all active SIP CTI sessions are terminated to apply the change. Office Communicator automatically reestablishes the session without user intervention.

There is a limitation where you cannot configure SIP CTI for two or more customers on a single node.

Figure 87
SIP CTI Services settings



Parameter: Service Enabled

The default state of the SIP CTI service is disabled. If the state of this parameter is changed, you must reboot. The SIP CTI service consumes approximately 140 MB of RAM on the Signaling Server when enabled.

ATTENTION
The configuration change to enable or disable the SIP CTI service is propagated to all Signaling Servers within the node. Ensure that engineering guidelines are considered for all Signaling Servers within the node before you enable this feature.

Parameter: Customer Number

The customer number parameter defines the customer on the Call Server to which SIP CTI service requests apply. Each TR/87 FE can support one customer number. Additional customers can be supported by adding additional Signaling Servers.

Parameter: Maximum Associations Per DN

This parameter defines the maximum number of simultaneous TR/87 SIP dialogs that can be active for a single DN. Multiple instances of Office Communicator (for example, home, office, laptop) are active and each of them can have its own active TR/87 session. This parameter limits the number of simultaneous client sessions for a single DN.

Parameter: International Calls As National

This parameter is used in combination with the following parameters:

- SIP CTI Dial Plan Prefix - National Prefix
- SIP CTI Dial Plan Prefix - International Prefix
- SIP CTI CLID Parameters - Country Code

When enabled this feature monitors all SIP CTI calls made using the E.164 international number format. For E.164 called numbers that are within the local country the SIP CTI national dial prefix is used to originate the call from the Call Server. For E.164 called numbers that are outside the local country the international dial prefix is used to originate the call from the Call Server.

When this feature is disabled all SIP CTI calls made using the E.164 number format uses the international dial prefix when originating the call from the Call Server.

Two scenarios are provided using the following example parameters:

- SIP CTI Settings - International Calls As National = Enabled
- SIP CTI Dial Plan Prefix - National Prefix = 61
- SIP CTI Dial Plan Prefix - International Prefix = 6011
- SIP CTI CLID Parameters - Country Code - 1
- AC1 = 6

Scenario 1 A call is placed from Office Communicator to +14167008000. The TR/87 Front End application on the Signaling Server uses the above SIP CTI settings to determine that the E.164 destination is within the local country. The call originates through AML from the Call Server using the national dial string 614167008000.

Scenario 2 A call is placed from Office Communicator to +31123456789. The TR/87 Front End application on the Signaling Server uses the preceding SIP CTI settings to determine that the E.164 destination is not within the local country. The call originates through AML from the Call Server using the international dial string 601131123456789.

SIP CTI Dial Plan prefixes

The SIP CTI dial plan prefixes configuration settings are used to prefix phone numbers sent to the Call Server as a result of SIP CTI call attempts.

Parameter: National Prefix When calls are made to E.164 fully qualified numbers this parameter is used in combination with the “International Calls as National” setting in the CTI IP settings section. When a call to an E.164 destination contains the same country code as the local country the call is placed from the Call Server as a national call using this prefix rather than the international call prefix.

This parameter is also used to prefix calls that are made with a URI that contains a phone-context equal to the Public E.164/National domain in the SIP URI map.

Refer to the section “Parameter: International Calls As National” (page 216) for an example of the use of this parameter.

Parameter: International Prefix When calls are made to E.164 fully qualified numbers this parameter is used in combination with the International Calls as National setting in the CTI settings section. If the International Calls as National feature is disabled, all calls to any E.164 number are prefixed with this prefix. If the International Calls as National feature is enabled, only calls to E.164 destinations outside of the local country are dialed with this prefix.

Refer to the section “Parameter: International Calls As National” (page 216) for an example of the use of this parameter.

Parameter: Location Code Call Prefix This parameter is used to prefix calls that are made with IRAs with a phone-context equal to the Private/UDP domain in the SIP URI map.

This parameter is also used in conjunction with the Calling Device URI Format setting. Refer to the section “Parameter: Calling Device URI Format” (page 219) for an example of the use of this parameter.

Parameter: Special Number Prefix This parameter is used to prefix calls that are made with a URI that contains a phone-context equal to the Public/E.164 Special Number domain in the SIP URI map.

Parameter: Subscriber Prefix This parameter is used to prefix calls that are made with a URI that contains a phone-context equal to the Public E.164/Subscriber domain in the SIP URI map.

SIP CTI CLID configuration parameters

The SIP CTI CLID parameters are used to adjust the format of phone numbers for incoming call appearances. For Office Communicator these settings impact the format of numbers that appear on the incoming call pop-up for Remote Call Control.

ATTENTION
These settings are independent of the similar SIP GW CLID parameters to allow independent control of the format of numbers on the incoming call pop-up for Remote Call Control.

For all public calls (subscriber (for example, NXX in North America), national (for example, NPA in North America), or international) E.164 fully qualified numbers are used to represent the caller. This is possible through the use of the following parameters:

- Country Code
- Area Code
- Subscriber/Number of Digits to strip
- Subscriber/Prefix to insert
- National/Number of Digits to strip
- National/Prefix to insert

The E.164 format of subscriber calls (NXX) is:

+<countrycode><area code><subscriber number>.

The parameters Subscriber/Number of digits to strip and prefix to insert are used to modify the format of subscriber numbers presented from the PSTN due to region specific requirements.

The E.164 format of national calls (NPA) is:

+<countrycode><national number>.

The parameters National/Number of digits to strip and prefix to insert are used to modify the format of national numbers presented from the PSTN due to region specific requirements.

Parameter: Dialing Plan

When configured to CDP, no changes are made to CDP numbers from the Call Server. However, when configured to UDP, the location code prefix and location code are added as a prefix to CDP numbers to aid in normalization. When this setting is enabled all user phone numbers in the active directory can be entered using the home location code to ensure a consistent unique format throughout the enterprise. Two scenarios are provided using the following example parameters:

- SIP CTI Dial Plan Prefix - Location Code Call Prefix = 6
- SIP CTI CLID Parameters - Home Location Code = 343

Scenario 1 - SIP STI Dial Plan = CDP

A call is placed to the DN controlled by Office Communicator for RCC from DN 3000 on the same Call Server. The call pop-up that appears on the users desktop shows call from 3000.

Scenario 2 - SIP CTI Dial Plan = UDP

A call is placed to the DN controlled by Office Communicator for RCC from DN 5000 on the same Call Server. The call pop-up that appears on the users desktop shows call from 634353000.

Parameter: Calling Device URI Format

This configuration setting defines the phone-context=<SIP URI Map Entries>.

ATTENTION
For Office Communications Server installations, phone-context=<SIP URI Map Entries> must be used to ensure compatibility with Office Communicator.

The combination of the URIs generated by the TR/87 FE and the normalization rules available to Office Communicator 2007 define the ability for Office Communicator to match incoming phone numbers to Office Communications Server user identities (for example, on the incoming call pop-up window).

The CSTA-delivered event contains a parameter called callingDevice that notifies the Office Communicator when a call is presented to the Remote Call Control controlled line. This field contains a TEL URI that is generated based on the combination of the SIP CTI dialing plan and Calling Device URI format parameters. Four scenarios are provided where a call is placed to the DN controlled by Office Communicator for RCC from DN 5000 using the following example parameters:

- SIP CTI Dial Plan Prefix - Location Code Call Prefix = 6
- SIP CTI CLID Parameters - Home Location Code = 343

Scenario 1, Dial Plan = UDP, Calling Device URI Format = phone-context= SIP GW URI map entries:
The TEL URI generated for the caller is:
"tel:3435000;phone-context=udp.nortel.com"

Scenario 2, Dial Plan = CDP, Calling Device URI Format = phone-context= SIP GW URI map entries:
The TEL URI generated for the caller is:
"tel:3000;phone-context=cdp.nortel.com"

Parameter: Home Location Code
This parameter defines the home location code to be used in CLID generation in combination with the SIP CTI dial plan setting.

For an example of this parameter, see “Parameter: Dialing Plan” (page 219).

Parameter: Country Code
This parameter defines the country code to be used in CLID generation.

Parameter: Area Code
This parameter defines the area code to be used in CLID generation.

Parameter: Subscriber/Number of Digits to strip
For incoming subscriber (for example, NXX in North America) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: Subscriber/Prefix to insert
For incoming subscriber (for example, NXX in North America) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

Parameter: National/Number of Digits to strip
For incoming national (for example, NPA in North America) calls this parameter defines the number of digits to strip from the incoming phone number prior to conversion to E.164 format.

Parameter: National/Prefix to insert
For incoming national (for example, NPA in North America) calls this parameter defines the prefix to insert after stripping any digits necessary from the incoming phone number prior to conversion to E.164 format.

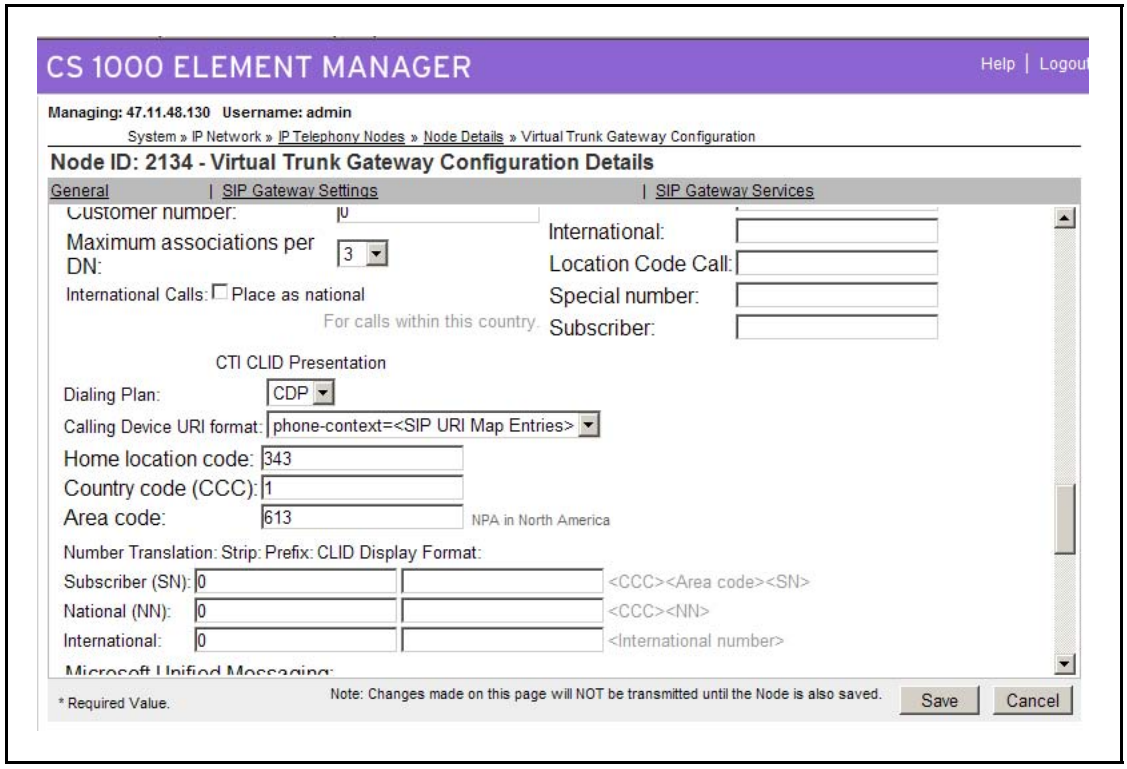
North American SIP CTI configuration example

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw), as shown in the following figure. With the configuration defined, the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces tel:+16134005000 on the Office Communicator incoming call pop-up.
- An incoming National Call with phone number 4169008000 produces tel:+14169008000 on the Office Communicator incoming call pop-up.
- An RCC call from Office Communicator to the E.164 number +16135006000 produces a call from the controlled DN to 616135006000.

An RCC call from Office Communicator to the E.164 number +3312345678 9 produces a call from the controlled DN to 601133123456789.

Figure 88
North American CLID manipulation

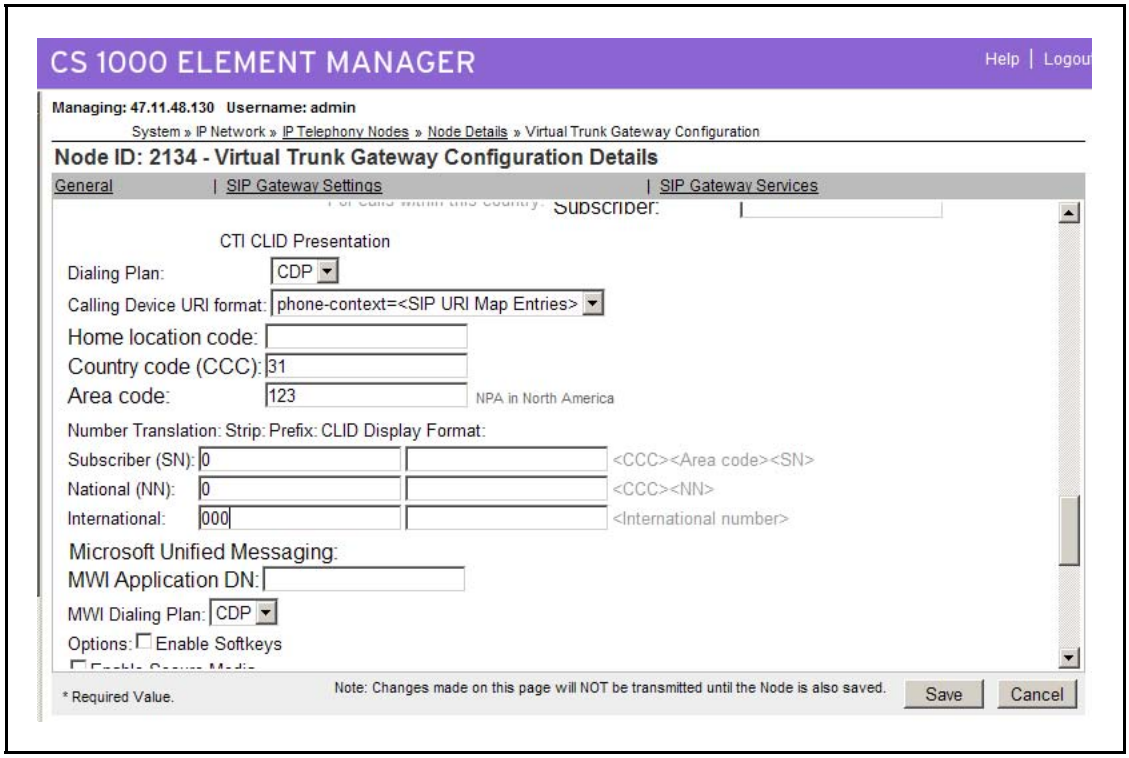


Non-North American SIP CTI configuration example

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw). The Virtual Trunk Gateway Configuration Details page appears, as shown in the following figure. With the configuration defined, the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces +311234005000 on the Office Communicator incoming call pop-up.
- An incoming National Call with phone number 00123456789 produces +31123456789 on the Office Communicator incoming call pop-up.
- An RCC call from Office Communicator to the E.164 number +31123456789 produces a call from the controlled DN to 00123456789.
- An RCC call from Office Communicator to the E.164 number +33123456789 produces a call from the controlled DN to 00033123456789.

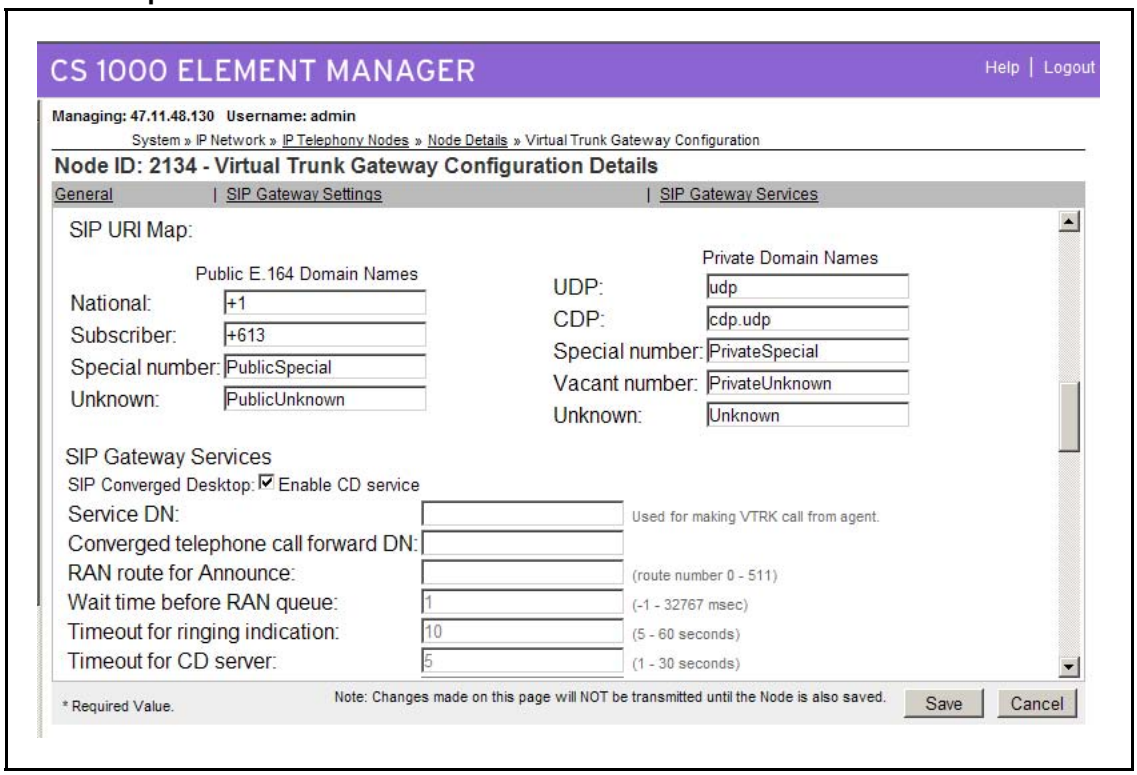
Figure 89
Non-North American CLID Manipulation



Configuring the SIP URI Map

In Element Manager, on the navigation pane, select IP Network, Nodes: Server, Media Cards. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the IP Telephony Node Properties Applications section, click Gateway (SIPGw). The Virtual Trunk Gateway Configuration Details page appears, as shown in the following figure. The existing SIP URI map configured for SIP GW application is also used by the TR/87 FE application to parse incoming URIs within SIP CTI service requests.

Figure 90
SIP URI Map



Configuring CDR

Call Detail Recording (CDR) records are produced for calls controlled using the Remote Call Control feature. The format of these CDR records is the same as those of calls dialed directly from a telephone's keypad.

Dialing E.164 International Format Numbers from Office Communicator - Phone Calls (SIP CTI)

When a call is originated from Office Communicator to an E.164 number (such as +14163005000) through Remote Call Control, the make call service request arrives at the TR/87 FE within a SIP INFO message as per the TR/87 specification. See Figure 91 "SIP INFO message" (page 224).

Figure 91
SIP INFO message

```
<?xml version="1.0" encoding="UTF-8"?><DeliveredEvent
xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
<monitorCrossRefID>37</monitorCrossRefID>

<connection>
        <callID>19806</callID>
        <deviceID>tel:+16139675000;ext=3050</deviceID>
</connection>

<alertingDevice>
        <deviceIdentifier>tel:+16139675000;ext=3050</deviceIdentifier>
</alertingDevice>

<callingDevice>
        <deviceIdentifier>tel:+16139675000;ext=2014</deviceIdentifier>
</callingDevice>

<calledDevice>
        <deviceIdentifier>tel:+16139675000;ext=3050</deviceIdentifier>
</calledDevice>

<lastRedirectionDevice>
        <notRequired />
</lastRedirectionDevice>

<localConnectionInfo>alerting</localConnectionInfo>

<cause>normal</cause>

</DeliveredEvent>
01/21/2008|15:02:18.898 1E498:1E494 INFO  :: End of Data Received -
47.11.56.51:5061 (To Local Address: 47.11.56.165:2968) 2113 bytes
```

The TR/87 FE that resides on the Signaling Server contains a feature to insert the appropriate dial plan prefix, either national or international, depending on the location of the Call Server and destination of the call. This ensures calls within the country use the national dial format and calls outside the country use the international dial format. This feature is enabled or disabled in Element Manager in the SIP CTI Settings section. When “All International Calls As National” is enabled, any calls within the local country have the country code stripped from the E.164 number and the national dial prefix applied. The format of the number presented by the TR/87 FE to the Call Server through AML in this scenario is:

<SIP CTI national prefix><national subscriber number>.

Any calls outside the country have only the international dial prefix applied to the E.164 phone number. The format of the number presented by the TR/ 87 FE to the Call Server through AML in this scenario is:

<SIP CTI international prefix><international number>.

When “All International Calls As National" is disabled, all calls to any E.164 destination use the international dial format. See section “Parameter: International Calls As National” (page 216) for additional detail on the configuration of this feature and an illustrative example.

Transport Layer Security (TLS) configuration between the OCS Proxy with MCM and CS 1000

For more information about TLS in the CS 1000, see *Security Management* (NN43001-604). For more information about how to enable or configure TLS on the OCS server, go to www.microsoft.com.

Interactions and requirements

The following provides information about product interactions and requirements.

End-to-end security

End-to-end security is not supported for Converged Office solution and CS 1000 node configuration.

Issue To (subject) parameter

The Issued To (subject) parameter must be a Fully Qualified Domain Name (FQDN) for all certificates used by Converged Office solutions. For example, Office Communications Server, SPS, SIP Gateway).

Security options

The Security Option “System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing” must be enabled on the Office Communications Server that talks to the CS 1000 using TLS. This option is automatically enabled by MCM if TLS transport is configured. Enabling this option affects other system components (Terminal Services, Encrypting File System Service). For example, Remote Desktop Client cannot connect to the server from a Windows 2000 PC because it does not support FIPS. New Remote Desktop Client must be installed on the Windows XP PC (Windows 2003 Server %SystemRoot%\System32\Clients\tsclient).

Local host IP Address

Local host IP Address 127.0.0.1 must be authorized on the Office Communications Server that talks to the CS 1000 using TLS. Authorization is performed by MCM automatically if TLS transport is configured.

DNS server

The DNS server used by Office Communications Server must resolve the SPS FQDN to its IP address and vice versa.

Private Certificate Authority (Nortel UCM)

Certificates signed by the Private CA (Nortel UCM) cannot be used on the Office Communications Server. For example, certificates for OCS servers must be issued by either Microsoft CA or another external CA. For more information about Microsoft security and the Microsoft Office Communications Server Security Guide, go to the Microsoft Web site at www.microsoft.com.

OCS certificate

Certificates used by OCS for TLS connection has to meet the following requirements:

- Enhanced Key Usage (EKU): Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
- Key Usage (KU): Digital Signature, Key Encipherment, Data Encipherment (b0)

For more information about configuring the OCS certificate and how to configure a certificate that is compliant with the above requirements, see "OCS certificate configuration" (page 235).

Using the OCS certificate wizard to request a certificate for the OCS Application Proxy with MCM is not supported if the Microsoft Enterprise CA is used. Microsoft Enterprise CA running Microsoft Windows Server 2003 in Standard or Web Edition are not supported.

Example TLS configuration

- OCS Proxy server running MCM:
  - IP address – 47.11.56.54
  - FQDN – ocs2007a-proxy.ocs2007.corp.nortel.com
  - SIP address: mcm@ocs2007a.corp.nortel.com
- SIP Proxy Server (SPS):
  - IP address – 47.11.56.24
  - FQDN – ocs2007asps.ocs2007a.corp.nortel.com
- Office Communications Server uses certificates issued by the Microsoft Certification Authority. CS 1000 components use the Private CA (Nortel Unified Communications Management (UCM)) signed certificates.

Configuring TLS for Converged Office

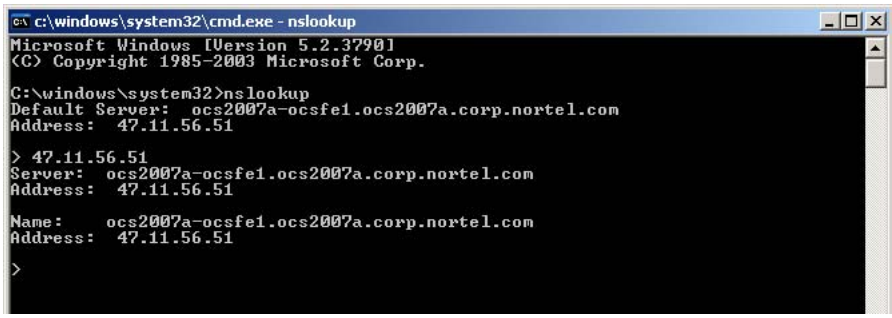
The following section describes the TLS configuration procedures for Converged Office.

ATTENTION
The network addresses used in the example figures in this section are different than the examples used throughout this document.

Step	Action
1	Configure the DNS server used by Office Communications Server to resolve SPS FQDN to its IP Address and vice versa. See Figure 92 "nslookup" (page 227).

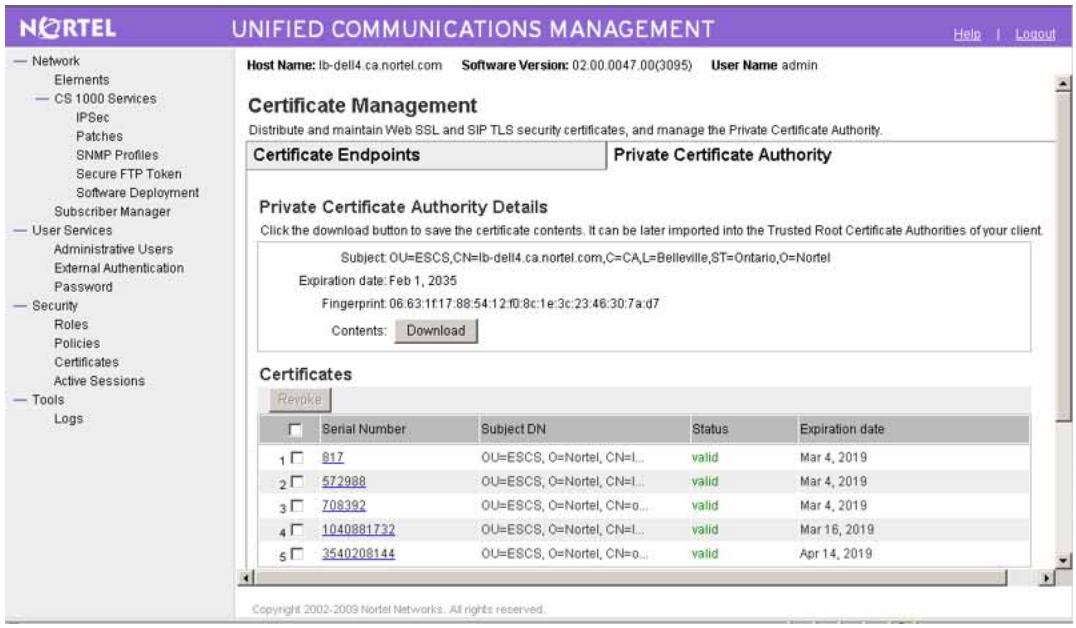
Note: If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP, and Redirect SIP-CTI) then FQDNs of all SIP Gateways with TLS enabled must be resolved to IP Addresses by DNS and vice versa.

Figure 92
nslookup



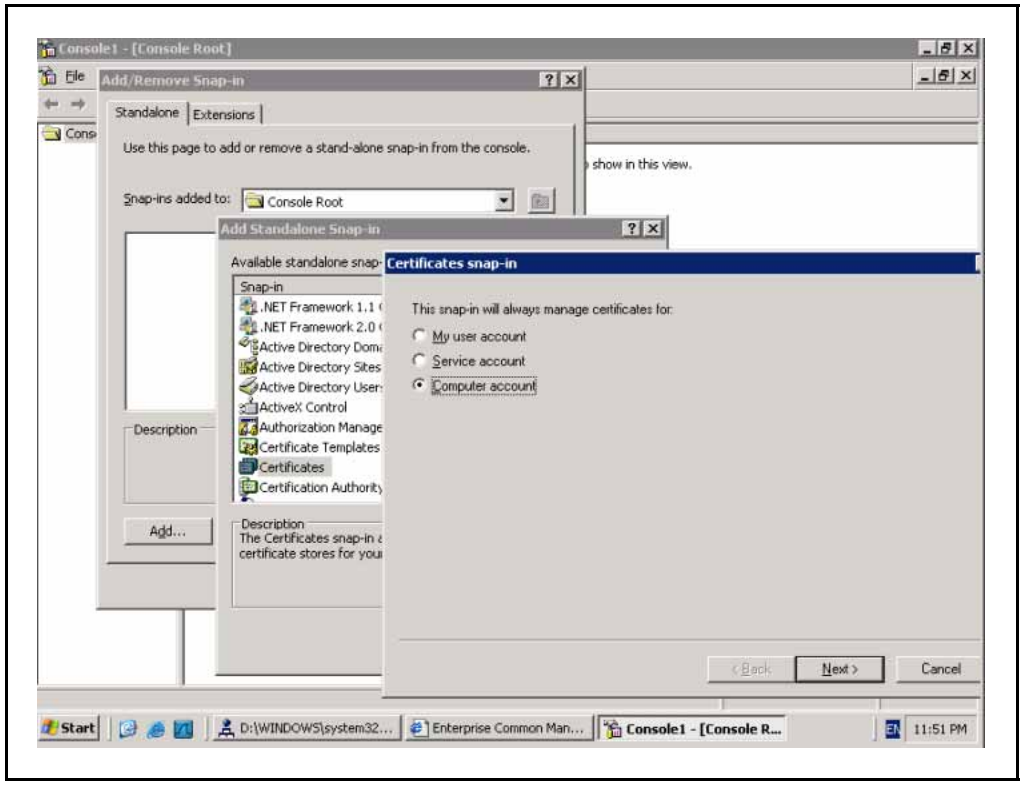
2	Add Private CA certificate to the Trusted Root Certification Authorities. Click Download and Save Private CA certificate to a file on the OCS server, as shown in the following figure.

Figure 93
Private Certificate Authority



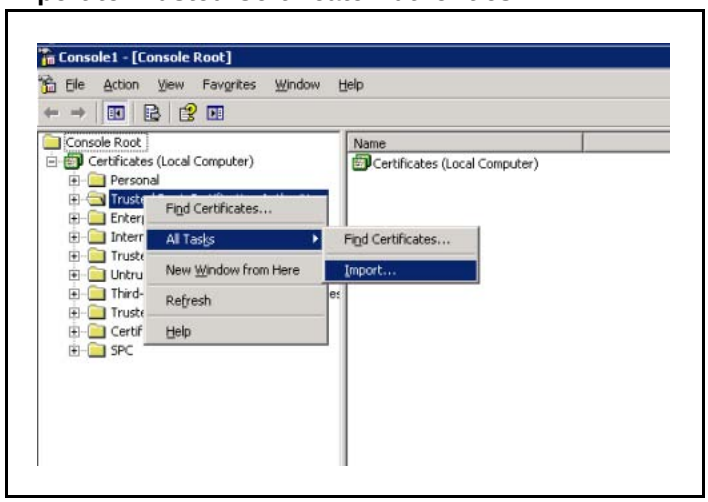
3 Open MMC on the Office Communication Server and add the Certificates (local computer) snap-in, as shown in the following figure.

Figure 94
Certificate snap-in



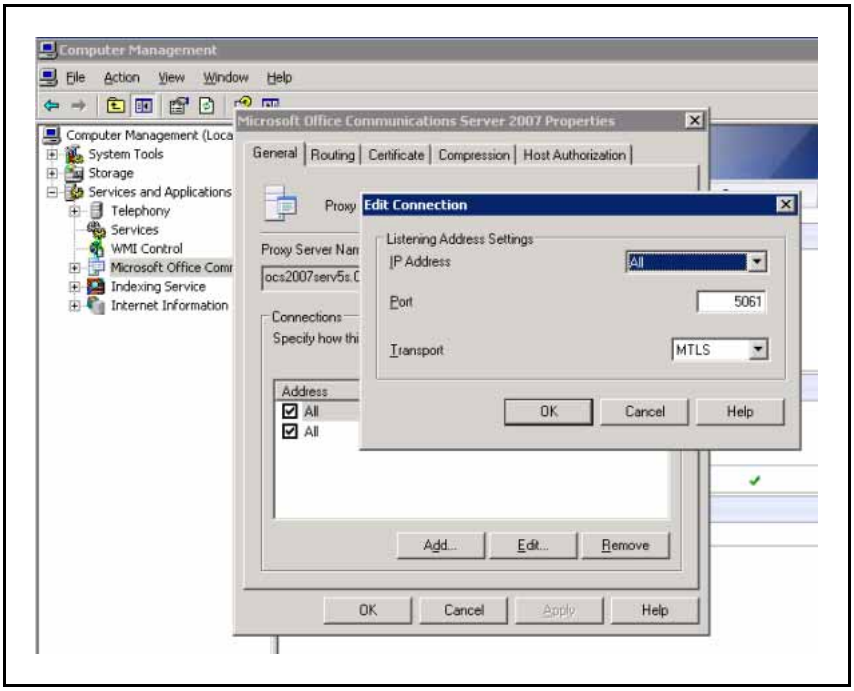
4 Import the saved file to the Trusted Root Certification Authorities, as shown in the following figure.

Figure 95
Import to Trusted Certificate Authorities



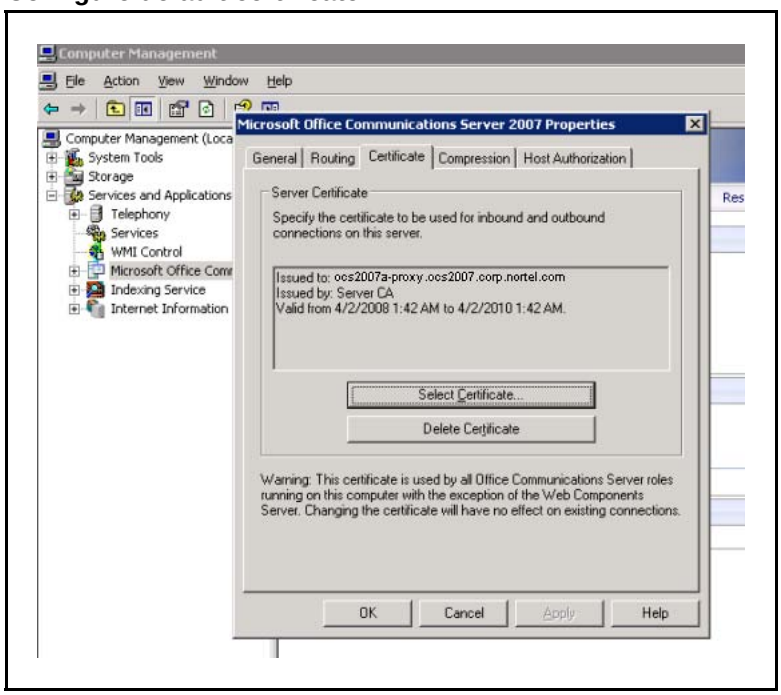
5 Enable incoming TLS connections on the Office Communications Server, as shown in the following figure.

Figure 96
Enable incoming TLS connections



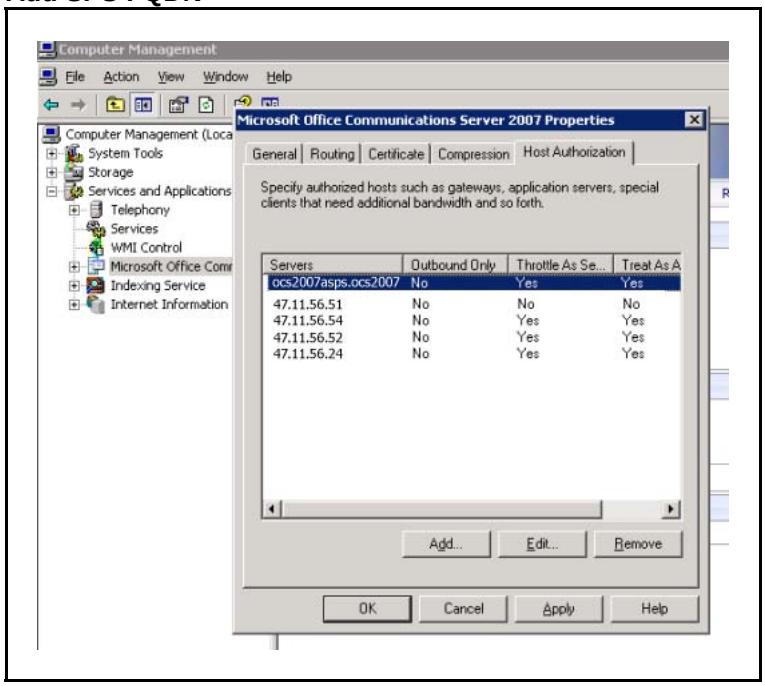
6 Configure the default certificate used for TLS connections by the Office Communications Server, as shown in the following figure.

Figure 97
Configure default certificate



7 Click **Add** to add the SPS FQDN to the Host Authorization table on the Office Communication Server, as shown in the following figure.

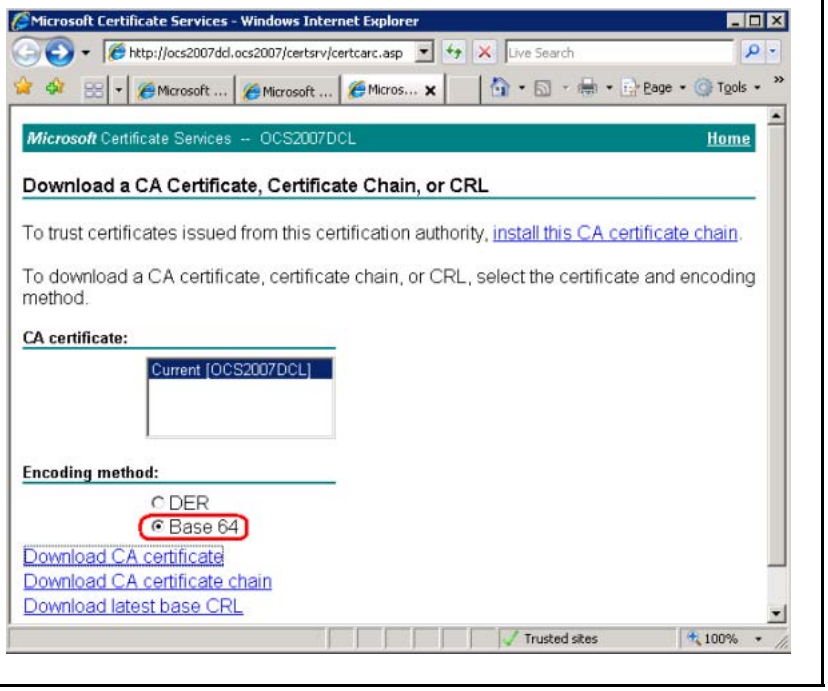
Figure 98
Add SPS FQDN



Note: If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP, and Redirect SIP-CTI) the FQDNs of all SIP Gateways with TLS enabled must be added to the table.

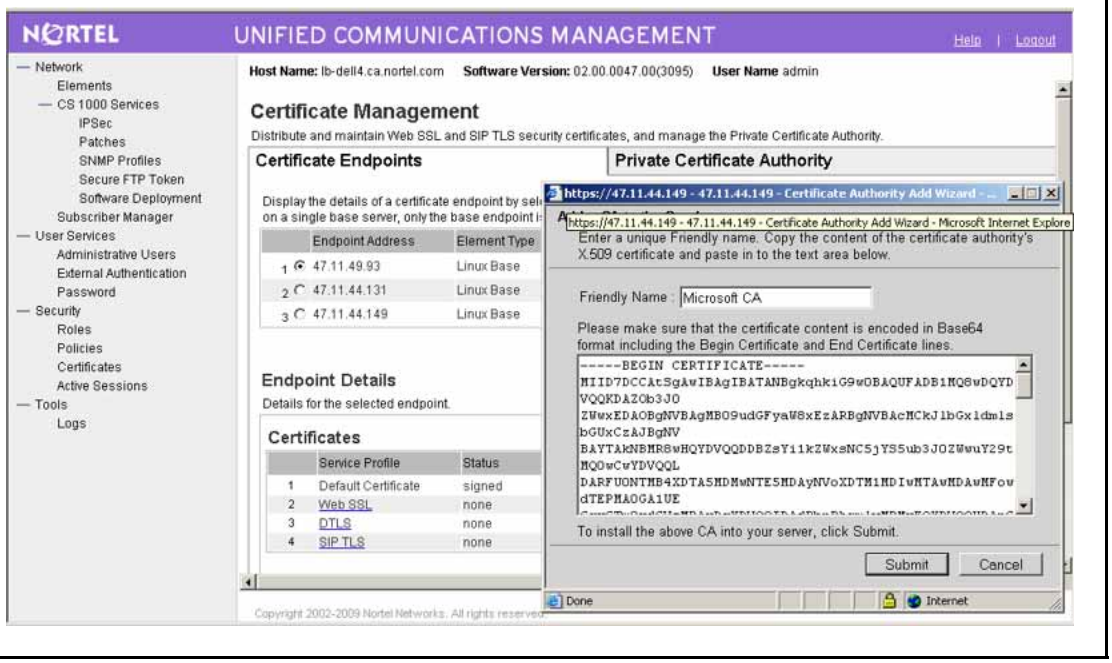
8 Add Microsoft CA certificate to the Trusted Certificate Authorities on SPS. See Figure 99 "Add Microsoft CA Certificate" (page 232). Download Microsoft CA certificate and save it to file on the Office Communications Server in Base-64 encoding.

Figure 99
Add Microsoft CA Certificate



9 Open the saved file in Notepad and copy its content to the clipboard. Add the copied content to the Trusted Certificate Authorities, as shown in the following figure. Click **Submit**.

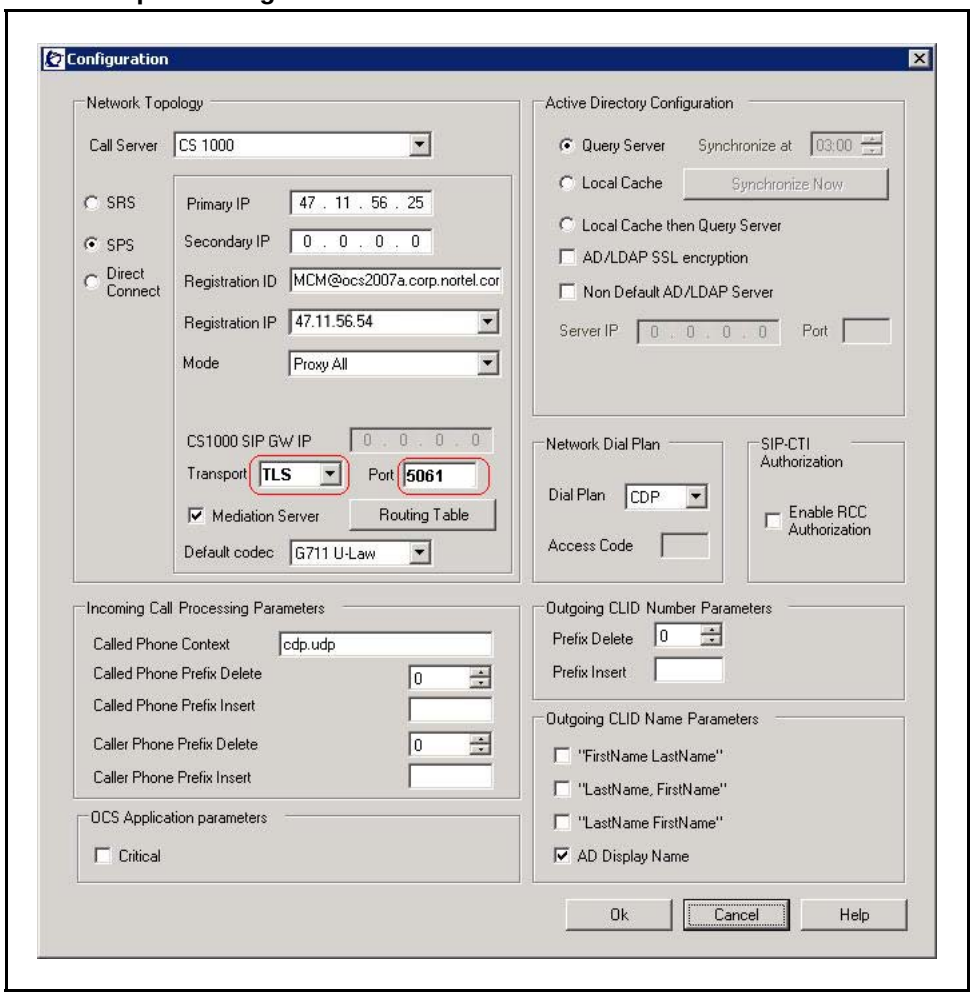
Figure 100
Add a CA to the service



The refreshed screen shows the newly added Certificate Authority.

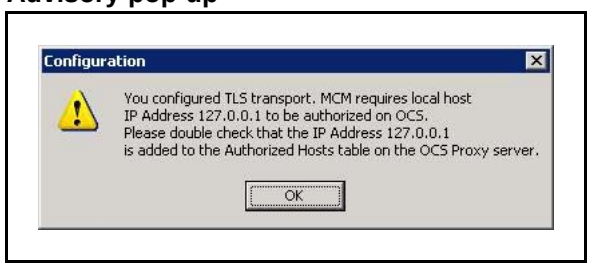
10 Configure Transport on the MCM from TCP to TLS, as shown in the following figure.

Figure 101
TLS Transport configuration



11 The following advisory pop-up appears requesting you to take note and perform a manual configuration. Click **OK** to close the advisory pop-up.

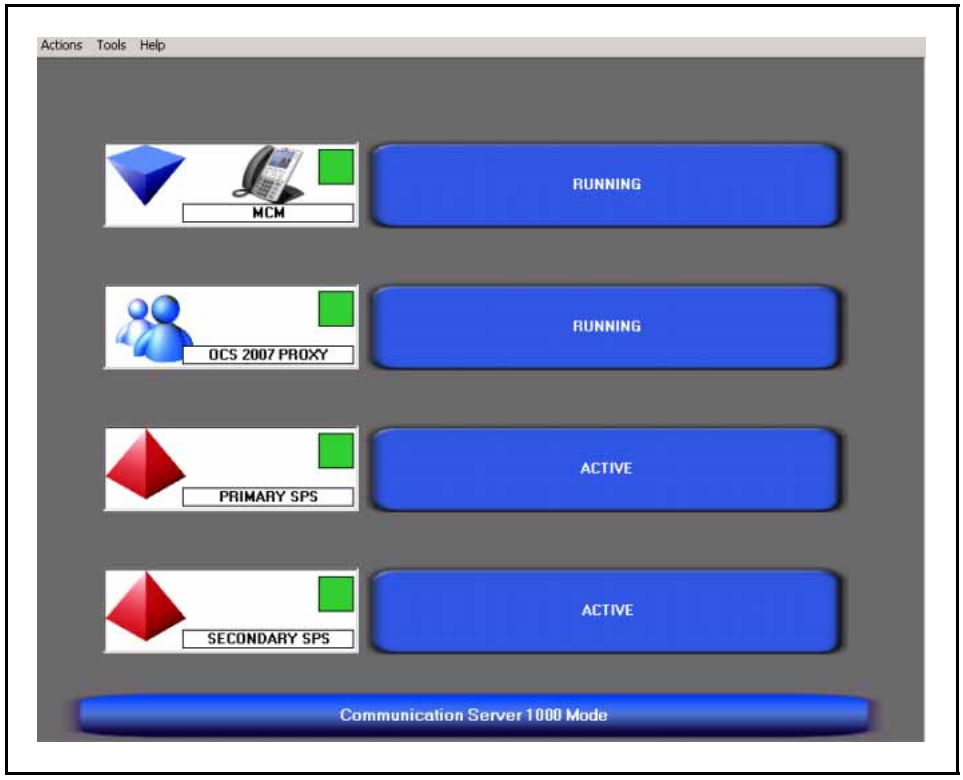
Figure 102
Advisory pop-up



12 On the main MCM configuration page, click **OK** to save the configuration changes.

13 Check that MCM is registered with SPS, as shown in the following figure.

Figure 103
MCM status



If the SPS status is not responding, it may take up to five minutes until all the Office Communications Server changes are applied.

14 On the OCS Proxy server properties, open the Host Authorization table and add the IP address 127.0.0.1 as the authorized host.

--End--

For more information about TLS, see the following Nortel and Microsoft documents:

- *Nortel Security Management Fundamentals* (NN43001-604) document
- *Microsoft Office Communications Server 2007 Security Guide*

ATTENTION

- Microsoft Enterprise CA running Microsoft Windows Server 2003 either Standard or Web Editions are not supported.
- Using OCS Certificate wizard to request certificate for OCS Proxy server, where MCM runs, is not supported.

OCS certificate configuration

This section covers the following topics for configuring the certificate used by the OCS Proxy server for TLS connection to the CS 1000.

- "Step 1: Configuring (duplicating) the Web certificate template" (page 235)
- "Step 2: Downloading the CA certification path" (page 237)
- "Step 3: Installation of the CA certification path" (page 237)
- "Step 4: Requesting a certificate" (page 238)
- "Step 5: Configuring OCS to use the certificate" (page 239)

Enterprise CA

Use the following procedures for configuration certificates for an Enterprise configuration.

Step 1: Configuring (duplicating) the Web certificate template

To duplicate the Computer certificate template for a Windows Server 2003 Enterprise CA, perform the following steps.

Step	Action
1	Log on to the CA server as a member of the **DomainAdmins** group.
2	Click **Start** and select **Run**. In the Open box, type **mmc**, and then click **OK**.
3	On the **File** menu, click **Add/Remove Snap-in**.
4	Click **Add**.
5	In the Add Standalone Snap-in dialog box, click **Certificate templates**, and then click **Add**.
6	Click **Certification Authority**, and then click **Add**.
7	In Certification Authority, accept the default option, Local computer (the computer this console runs).
8	Click **Finish**.
9	Click **Close**, and then click **OK**.

10 The console pane of MMC, verify that the Certificate Templates and Certification Authority snap-ins appear.

11 Click **Certificate Templates**.

12 In the details pane, right-click **Web Server**, and then click **Duplicate Template**.

13 On the **General** tab, change the template name to a meaningful name for your organization.

14 In the **Validity period** box, verify that the validity period meets your organization's requirements.

15 On the **Request Handling** tab, select the **Allow private key to be exported** check box.

16 On the **Subject name** tab, in the **Request** area, click **Supply**.

17 Click the **Security** tab.

18 Grant **Enroll** permissions for the following groups in all domains: Authenticated users, Domain Admins, Domain Computers, and Enterprise Admins.

19 Click **Apply**, and then click **OK**.

20 To verify settings, expand **Certificate Templates**.

21 In the details pane, right-click the template that you configured. Click **Properties** and verify your settings, and then click **OK**.

22 Expand **Certification Authority (local)**, and then expand your **CA**.

23 In the console tree, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.

24 Select the new template, and then click **OK**.

25 Verify that the new template appears in the details pane, then under Intended Purpose, verify that **Server Authentication** and **Client Authentication** appear, and under Key Usage, verify that Digital signature, **Allow key exchange only with key encryption** and **Allow encryption of user data** appear.

26 Close MMC.

27 Click **Start**, and then click **Run**. In the Open box, type **gpupdate /force**, and then click **OK**. The gpupdate program forces an update of the Group Policy on the domain controller and replicates these changes throughout the forest.

28 28. Click Start, and then click Run. In the Open box, type **http://***<domain controller name>***/certserv**, and then click **OK**.

29 Enter the user name and password of an account that is a member of the **DomainAdmins** group.

30 On the Certificate Services Web page, under **Select a task**, click **Request a certificate**.

31 Click **Advanced certificate request**.

32 Click **Create and submit a request to this CA**.

33 Verify that your new certificate template appears in the **Certificate template** list.

--End--

Step 2: Downloading the CA certification path

Use the following procedures to download the CA certification path.

Step	Action
1	With the enterprise root CA offline and the enterprise subordinate (issuing) CA Server online, log on to Office Communications Server. Click **Start**, **Run**, and then type **http://***<name of your Issuing CA Server>***/certsrv** and then click **OK**.
2	Under **Select a task**, click **Download a CA certificate, certificate chain, or CRL**.
3	Under **Download a CA Certificate, Certificate Chain, or CRL**, click **Download CA certificate chain**.
4	In the **File Download** dialog box, click **Save**.
5	Save the file to the hard disk drive on your server. This file has an extension of .p7b. If you open this .p7b file, the chain will have the following two certificates: • *<name of enterprise root CA>* certificate. • *<name of enterprise subordinate CA>* certificate

--End--

Step 3: Installation of the CA certification path

Use the following procedures for installation of the CA certification path.

Step	Action
1	Click **Start**, **Run**, type **mmc**, and then click **OK**.
2	On the File menu, click **Add/Remove Snap-in**.
3	In the **Add/Remove Snap-in** dialog box, click **Add**.

4 In the list of **Available Standalone Snap-ins**, select **Certificates**.

5 Click **Add**.

6 Select **Computer account** and click **Next**.

7 In the **Select Computer** dialog box, ensure **Local computer: (the computer this console runs)** is selected, and then click **Finish**.

8 Click **Close**, and then click **OK**.

9 In the left pane of the Certificates console, expand **Certificates (Local Computer)**.

10 Expand **Trusted Root Certification Authorities**.

11 Right-click **Certificates**, point to **All Tasks**, and then click **Import**.

12 In the Import Wizard, click **Next**.

13 Click **Browse** and go to where you saved the certificate chain, select the p7b file, and then click **Open**.

14 Click **Next**.

15 Leave the default value **Place all certificates in the following store** and ensure **Trusted Root Certification Authorities** appears under the Certificate store.

16 Click **Next**.

17 Click **Finish**.

--End--

Step 4: Requesting a certificate

Use the following procedures to request a certificate.

Step	Action
1	Open a Web browser, type the URL **http://***<name of your Issuing CA server>***/certsrv**, and then press ENTER.
2	Click **Request a Certificate**.
3	Click **Advanced certificate request**.
4	Click **Create and submit a request to this CA**.
5	In **Certificate Template**, select the name you gave to your duplicated Web certificate template.
6	In **Identifying Information for Offline Template**, type the FQDN of either the pool or the server.

7	In **Key Options**, click the **Store certificate in the local computer certificate store** check box.
8	Click **Submit**.
9	Click **Yes** on the potential scripting violation dialog.
10	After the requested certificate is issued by the CA go to the URL **http://***<name of your Issuing CA server>***/certsrv** again.
11	Click **View the status of a pending certificate request**.
12	Click the request you just submitted.
13	Click **Install this certificate**.
14	Click **Yes** on the potential scripting violation dialog.

--End--

Step 5: Configuring OCS to use the certificate

Use the following procedures to configure OCS to use the certificate.

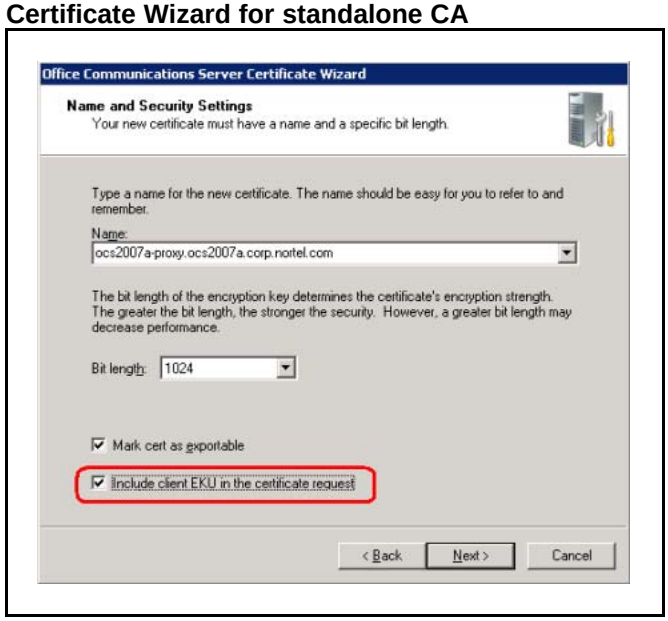
Step	Action
1	Open **Computer Management** snap-in.
2	Navigate and right-click **Microsoft Office Communications Server 2007**.
3	Click **Properties**.
4	Click **Certificate** tab.
5	Click **Select Certificate**.
6	Select the certificate you just installed.
7	Click **OK**.
8	Click **Apply**.

--End--

Standalone CA

OCS Certificate wizard can be used in case of Standalone CA but client EKU must be included.

Figure 104
Certificate Wizard for standalone CA



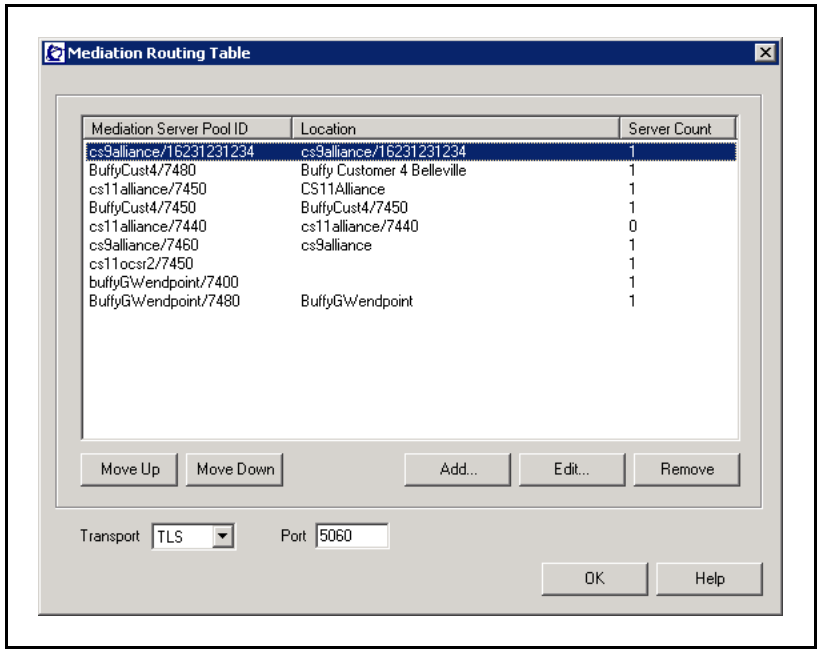
For more details about certificate configuration, see the Microsoft Office Communications Server 2007 Security Guide. Download Microsoft documentation from the Microsoft Web site at www.microsoft.com.

Configuring TLS between OCS Proxy with MCM and Mediation Server (OCS R1 only)

Follow these steps to configure the Mediation Server.

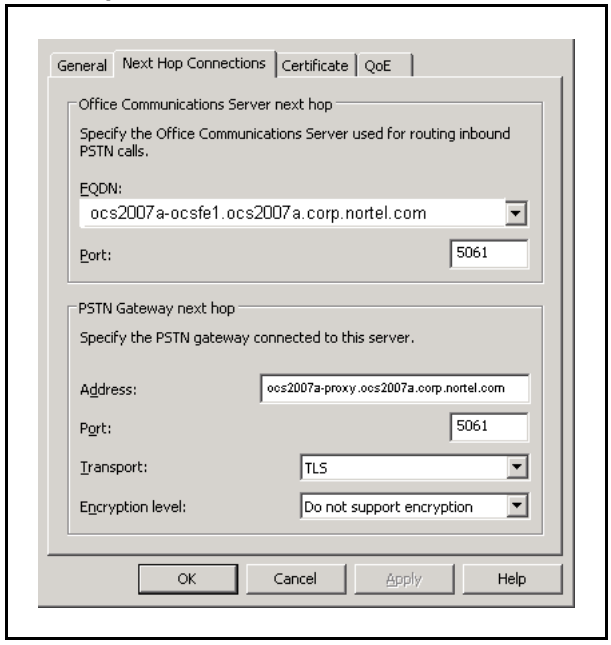
Step	Action
1	Ensure the procedures in "Configuring TLS for Converged Office" (page 226) have been completed prior to completing the next steps.
2	On the MCM, click **Routing Table**. The Mediation Routing Table window opens, as shown in the following figure.

Figure 105
Mediation Routing Table



3 Configure 5061 for PSTN Gateway next hop port, as shown in the following figure.

Figure 106
Next hop tab



4 Create a text file with name MediationServerSvc.exe.config in the Mediation Server directory. For example, C:\Program Files\Microsoft Office Communications Server 2007\Mediation

Server\ MediationServerSvc.exe.config. This file should have the following content:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<appSettings>
<add key="GatewayTLS" value="On" />
<add key="GatewayFqdn" value="OCS-Proxy.FQDN" />
</appSettings>
</configuration>
```

Where OCS-Proxy.FQDN is FQDN of your OCS Proxy server. This FQDN has to be resolved to the IP Address configured as PSTN Gateway Next hop.

5 Restart the Mediation Server.

--End--

For more information, see the Technet home page on the Microsoft Web site www.microsoft.com.

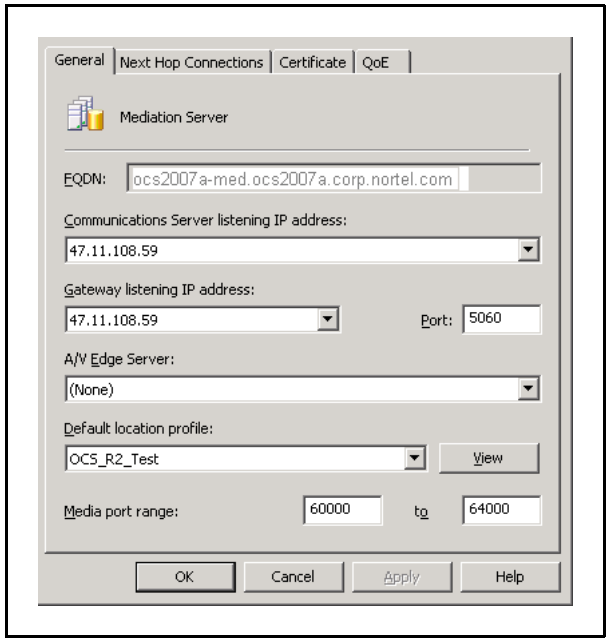
Configuring the TLS between OCS Proxy with MCM and Mediation Server using secure signaling (OCS R2 only)

With OCS 2007 R2, the Mediation Server has an improved interface for enabling secure signaling with TLS. The XML configuration file is no longer required. Certificate configuration remains the same.

Step	Action
1	Ensure the procedures in “Configuring TLS for Converged Office” (page 226) have been completed prior to completing the next steps.
2	Enable the TLS to communicate with the Mediation Server. Ensure **Port** is configured to 5060.
3	On the OCS R2 Administration tool, right-click on Mediation Server and select **Properties**.
4	Click the General tab and ensure the Gateway listening IP address port is configured to 5060, as shown in the following figure.

ATTENTION
Ensure the TLS port on the Mediation Routing Table and the Mediation Server Properties screen are both configured to port 5060.

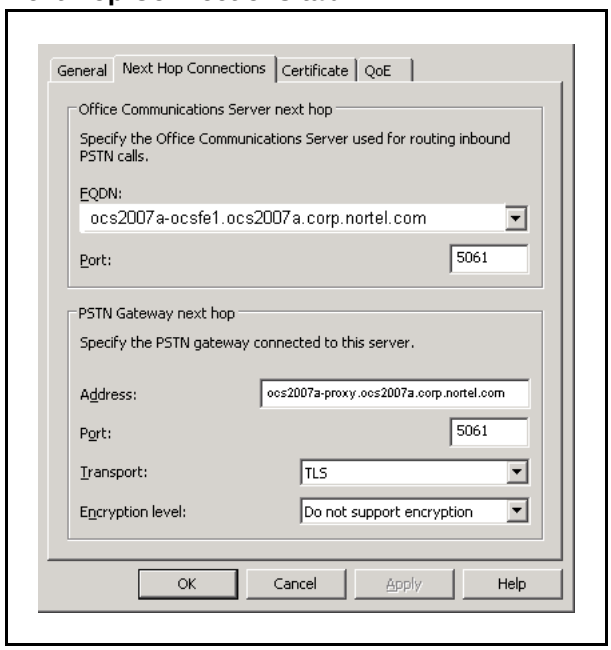
Figure 107
Mediation Server Properties



5 Click the **Next Hop Connections** tab.

The Next Hop Connections window appears, as shown in the following figure.

Figure 108
Next Hop Connections tab



6 In the PSTN Gateway next hop section, configure the following and click **Ok**.

- Address: FQDN of the OCS R2 Proxy with MCM server. For example, ocs2007a-proxy.ocs2007a.corp.nortel.com
- Port: 5061
- Transport: TLS
- Encryption level: Do not support encryption

7 Restart the Mediation Server.

--End--

Configuring the OCS Proxy server

Use the following procedure for configuring the OCS Proxy server.

Step	Action
1	Add the Mediation Server FQDN to the Authorized hosts on OCS Proxy.
2	Configure the Transport field on the MCM for the Mediation Server connections (MCM Console\Configuration\Routing table).

--End--

ATTENTION
OCS Mediation Server listens to the TCP port 5060 for incoming connections from Gateway even if TLS is configured. The same 5060 port should be configured on the MCM.

Normalizing phone numbers

Office Communicator 2007 requires that all phone numbers be in standard TEL URI format as defined in RFC 3966 for dialing and for reverse number lookup.

Office Communicator 2007 uses phone numbers that are provisioned (Active Directory and Outlook) and that are adhoc from the user through the user interface. All sources can be free format—a convention that is not in compliance with TEL URI.

The phone numbers configured for the Office Communicator user in the Active Directory are normalized. The PBX private dialing plan phone number is normalized to the Line URI format. For example, E.164;ext=CDP number or UDP number, based on the dialing plan.

The following lists some examples of normalization:

- ESN 343-5555 would be normalized to +16139620100;ext=3435555
- +1 (425) 7066340 would be normalized to +14257066340
- 1-800-368-3908 would be normalized to +18003683908

Phone numbers are normalized in Active Directory. Each user can have multiple phone numbers such as Office, Mobile, and Home. Two options are available to normalize these numbers: Offline and Address Book Service. For more information about normalization, see *Microsoft Office Communications Server 2007 Planning Guide* . Download Microsoft documentation from the Microsoft Web site www.microsoft.com.

ATTENTION
All normalization rules must be in Generic script.

Normalizing offline (recommended)

The user phone number is read from the Active Directory user object, original fields. These numbers are normalized offline to TEL URI format and stored in Active Directory in a different field named proxy address (multi value). Microsoft provides a reference on how to build a tool for this task.

If you use this option, then Address Book Service must not normalize the phone numbers and must instead publish only normalized phone numbers in the proxy address.

Each number in the proxy address is attached with an attribute that describes the phone number (for example: Office, Home, and so on).

For example:

tel:+14255551212;ext=5551212;ad-rdn=telephoneNumber;displayName =(425)555-1212

The ad-rdn = telephoneNumber is a proprietary parameter describes the type of the phone number and displayName, which is a proprietary parameter that holds the display format of this phone number (by default, the original phone number before normalization).

By default, the msRTCSIP-RCC Line is copied from the proxy address (attribute ad-rdn=telephoneNumber). The phone number is copied without ad-rdn and display name parameters.

For example:

tel:+14257771234;ext=1234;ad-rdn=telephoneNumber;display-name="(425) 7771234 * 1234"

is shown as:

tel:+14257771234;ext=1234

Normalizing using the Address Book Service

The Run time: Address Book service normalizes the original phone numbers in Active Directory. In this case, the normalized phone numbers are not stored in Active Directory and the output cannot be analyzed before it is used by Office Communicator. Having Address Book Service properly setup for an OC client is essential in receiving correct CLID info on call pop-ups.

Creating Normalization rules

Matching incoming calling numbers to the phone numbers for a Office Communications Server user, and transforming free-form dialstrings to URIs that can be called through TR/87, is performed by Office Communications Server 2007 and Office Communicator 2007 through a process called Normalization.

Normalization rules, according to Microsoft guidelines, must be defined to make use of the integration of Office Communicator 2007 Remote Call Control and Office Communications Server 2007 Multimedia functionality.

Each Office Communications Server user that uses Office Communicator Remote Call Control capability must have appropriate Office Communications configuration (in addition to the per-TN configuration discussed previously).

You must consider and define SIP routing for TR/87 sessions for each Office Communications Server user.

MCM provides authorization of Remote Call Control service requests based on the configuration defined in Active Directory for each Office Communications Server user.

Office Communicator requires that all phone numbers be in the standardized TEL URI format (RFC 3966) for reverse number lookup (matching the phone number of an incoming call to a known Office Communications Server user) and for dialing (either through an adhoc interface or through a menu from a user object).

Matching an incoming phone number to a Office Communications Server user identity is used to establish multimedia sessions. If the Office Communications Server user identity cannot be determined from a phone number, then Office Communications Server multimedia sessions cannot be established with the calling or called party.

See the *Microsoft Office Communicator Planning and Deployment Guide*. Download Microsoft technical documentation from the Download Center at www.microsoft.com.

For more in-depth information about deploying the Address Book Service, see the *Address Book Service Planning and Deployment Guide*. Microsoft documentation can be found at the Download Center, www.microsoft.com.

Example

A Office Communications Server user accesses an Active Directory phone number for Jim (in Outlook, for example) to make a Remote Call Control phone call. Office Communicator uses normalization to map the free-form phone number to a TEL URI prior to sending the TR/87 Make Call service request. You can assume the following points for normalizing phone numbers:

- The normalization method chosen is Address Book Service – Run time as opposed to using the offline method
- An Active Directory entry exists for Jim with business phone number ESN 343-2356
- A normalization rule exists that defines a regular expression (as defined in Figure 109 "Normalization rule example for UDP dial plan" (page 247)) to map ESN 343-2356 to +16239675000;ext=3432356.

Figure 109
Normalization rule example for UDP dial plan

```
#
# ESN ddd-dddd
#

.*ESN\s*  (\d\d\d)[\s()\-\./]*(\d\d\d\d)
   +16139675000;ext=$1$2
```

Result

The normalized version (tel:+16139675000;ext=$1$2) of the business number in Active Directory entries is stored in the Global Address List (GAL) and downloaded at logon by the Office Communicator 2007 client from the Address Book Service.

When you use a contact in a buddy list for Jim, or any other Microsoft Office Application that makes use of Active Directory phone numbers, the URI sent to the TR/87 FE for a TR/87 Make Call service request is:

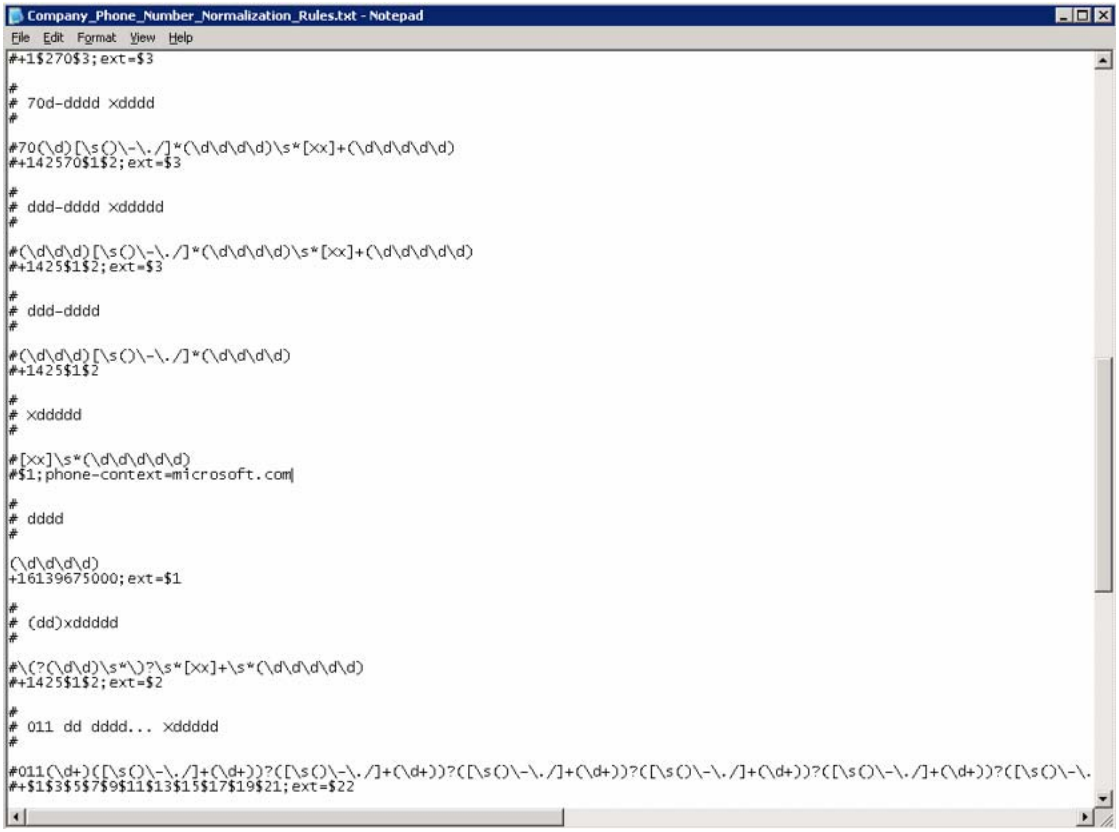
tel:+16139675000;ext=$1$2

Adding a new normalization rule

The following procedure describes the process of adding a new normalization rule.

Step	Action
1	Add an appropriate rule to the beginning of the “% ProgramFiles%\Microsoft OC 2007\Address Book Service"\Company_Phone_Number_Normalization_Rules.txt” file. This ensures that the e-mail notification provides the correct link.

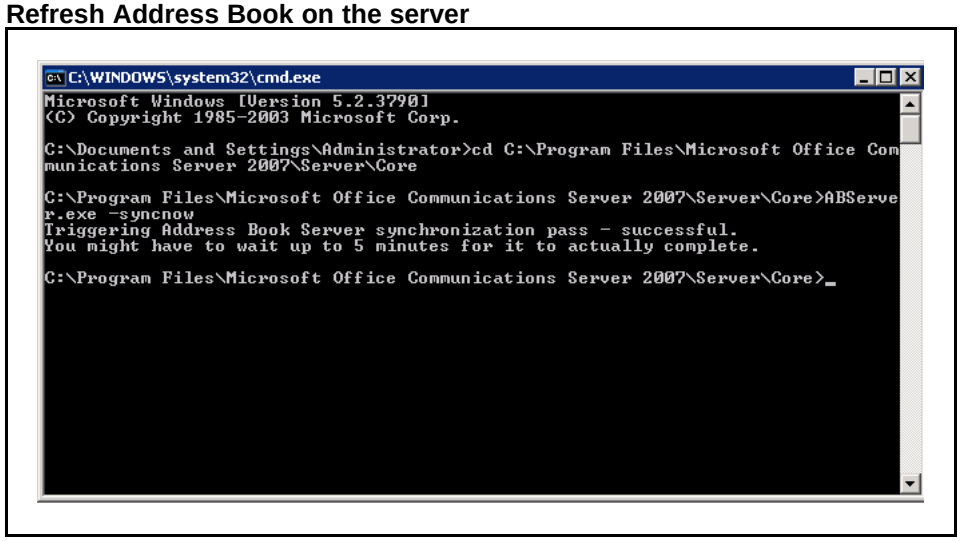
Figure 110
Company phone number normalization rules for CDP



2 Refresh the Address Book on the server by issuing the following command on the server running ABService, as shown in the example Figure 111 "Refresh Address Book on the server" (page 250):

%ProgramFiles%\Microsoft Office Communications 2007\Server\Core\ABServer.exe -syncNow

Figure 111
Refresh Address Book on the server

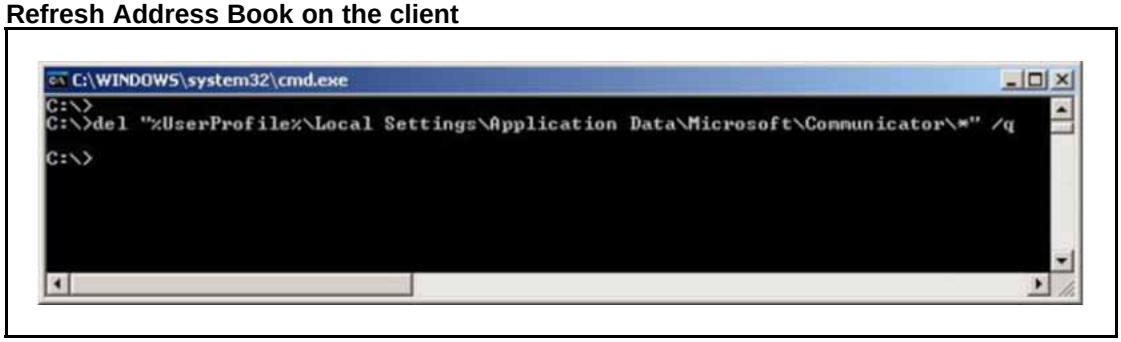


3 Exit from Office Communicator 2007.

4 Refresh Address Book on the client, as shown in Figure 112 "Refresh Address Book on the client" (page 250). Issue the following command on the PC running Office Communicator 2007:

Del “%UserProfile%\Local Settings\Application Data\Microsoft\Communicator*" /q

Figure 112
Refresh Address Book on the client



5 Start Office Communicator 2007.

--End--

SIP Routing and Redundancy configuration

Office Communicator is a soft phone application as well as a SIP User Agent (UA). Office Communications Server Front End server (Standard Edition Server or Enterprise Edition Server) hosts Office Communicator.

The TR/87 FE within the Communication Server 1000 is also a SIP UA. Office Communicator 2007 establishes a SIP dialog in one direction only: from the application to the TR/87 FE. The Office Communications Server Front End, which functions as a SIP Proxy, is a required component. The Nortel Multimedia Convergence Manager (MCM) is also required to provide support for authorization and the use of an NRS.

ATTENTION
Due to the inability of the Office Communicator client to support the SIP 302 redirect message (a fundamental requirement for the basic operation of the NRS), the MCM application installed on the Office Communications Server to support Telephony Gateway and Services functionality is also a required component for Remote Call Control support when using Office Communicator. The MCM application handles the 302 redirect message on behalf of Office Communicator clients.

Configuring Remote Call Control SIP Routing Using Phone Addressing

When an NRS is used with SIP addressing, based on the phone address format, the Communication Server 1000 TR/87 FE used to support a Remote Call Control session for a user must be co-resident with the SIP GW. This is essential, as the URI that is present in the INVITE to establish a TR/87 session is identical to the URI used to place a SIP call to the user. Thus, the NRS redirects the INVITE based on the request URI only (and not the mime content type within the INVITE).

The TR/87 FE recognizes the TR/87 mime type within an INVITE and intercepts the TR/87 INVITE if it is co-resident with the SIP Gateway. This ensures that both TR/87 sessions and phone calls with the same request URI are handled appropriately—either by the TR/87 FE or SIP Gateway, on the same Signaling Server.

Redundancy configuration

For information about Redundancy, see “Redundancy” (page 94).

OCS 2007 users using UM 2007 in integrated mode

Use the following procedures for OCS 2007 users using Unified Messaging (UM) 2007 in integrated mode—Option 1 or Option 2.

Prerequisites

The procedures in this section assume the following:

- The installation procedures for Exchange UM integrated mode have already been completed. For more information, see the *Microsoft Office Communications Server 2007 Document: Enterprise Voice*

Planning and Deployment Guide from Microsoft. Download Microsoft documentation from the Download Center at www.microsoft.com.

- You have access to the Exchange UM server.
- You have access to the Nortel technical document for configuring Exchange UM for the OCS user, see CS 1000 with Microsoft Exchange Server 2007 UM (NN43001-122).

Option 1—integrated mode

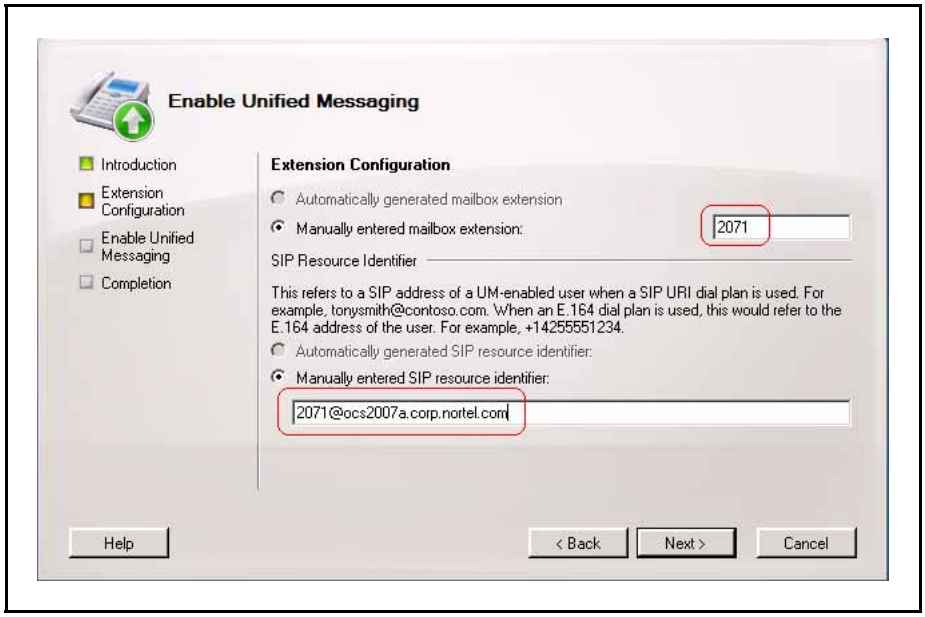
Use the following procedures for OCS 2007 users using Unified Messaging (UM) 2007 in integrated mode for Option 1.

Configuring a basic mailbox for the UM user

Configure a basic mailbox for the UM user. For more information, see *CS 1000 with Microsoft Exchange Server 2007 UM* (NN43001-122).

Step	Action
1	Create a new SIP URI dialing plan in Exchange UM.
2	Configure the OCS user mailbox in Exchange UM.
3	On the **Exchange Management Console** screen, click **Recipient Configuration**. The Mailbox window appears in the right pane.
4	Right-click a user in the right pane and select **Enable Unified Messaging**. The Enable Unified Messaging window opens.
5	Enable the OCS user for UM by manually configuring the SIP URI. Click **Manually entered SIP resource identifier** and type CS1000DN@domain.com, as shown in the following figure. For example, 2071@ocs2007a.corp.nortel.com.

Figure 113
Enable Unified Messaging integrated



6 Click **Next**.

7 Continue to follow the instructions from the *CS 1000 with Microsoft Exchange Server 2007 UM* (NN43001-122).

--End--

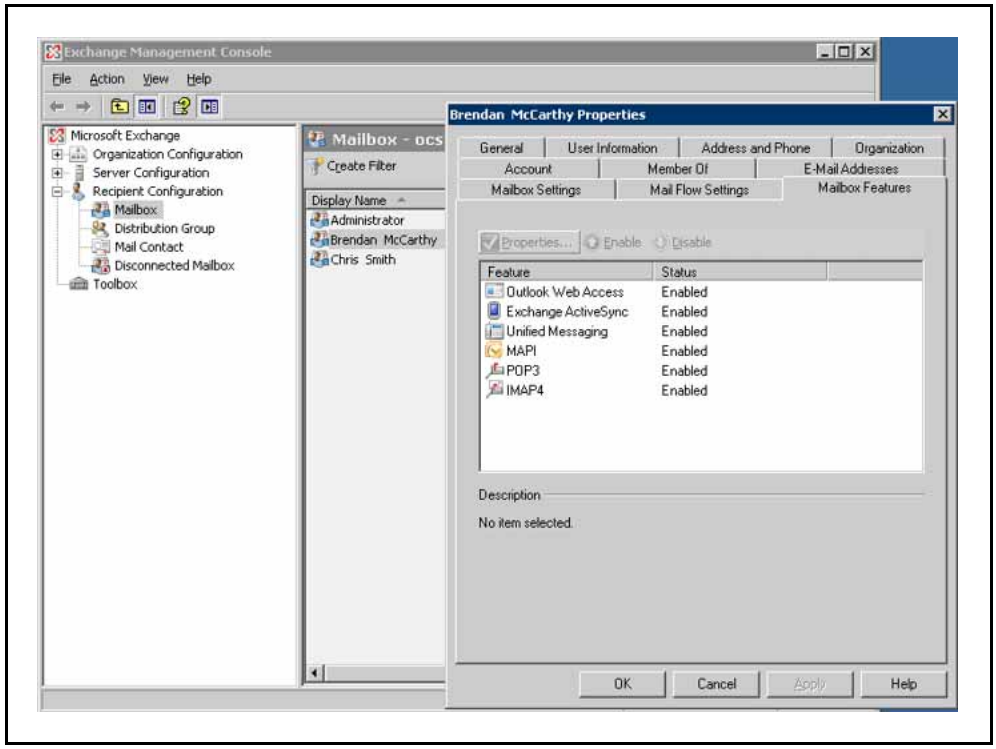
ATTENTION
An Exchange UM Extension (EUM) must be created for every user configured for Exchange UM. For example CS1000DN@domain.

Adding a user alias as Exchange UM

Add a user alias in Exchange UM.

Step	Action
1	From the Exchange Management Console, click **Recipient Configuration**, and select **Mailbox**.
2	Select a user. For example, Brendan McCarthy
3	Right-click the user and select **User Properties**, as shown in the following figure.

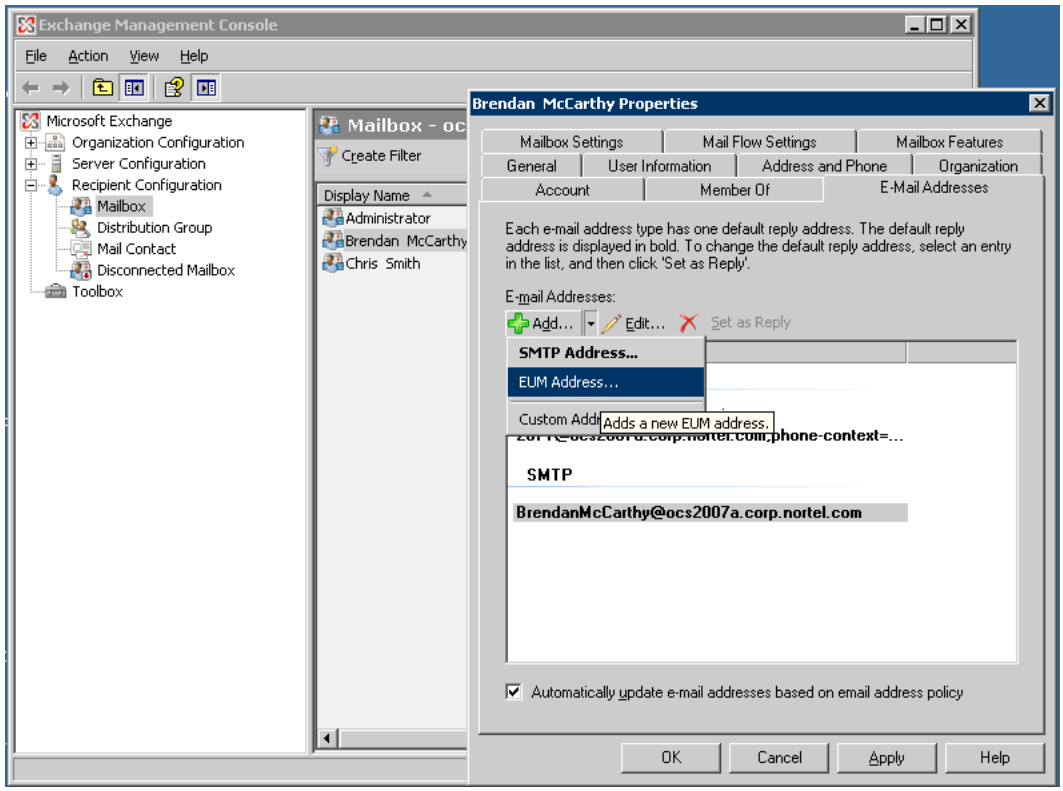
Figure 114
User Properties window for Exchange UM



4 Click the **E-mail Addresses** tab.

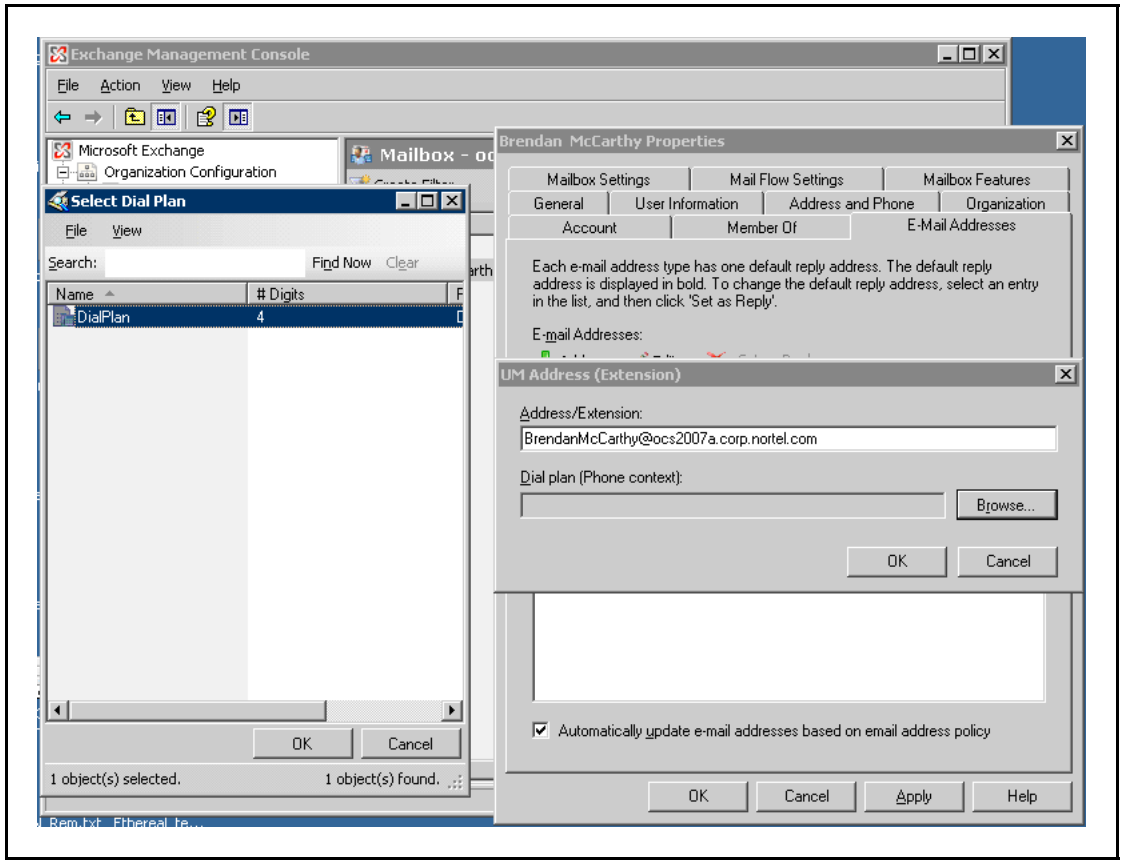
5 Click **Add** and select **EUM Address**, as shown in the following figure.

Figure 115
UM Address



6 In the **UM Address (Extension)** window, type the useralias@domain of the user in the **Address/Extension** field, as shown in the following figure. For example, BrendanMcCarthy@ocs2007a.corp.nortel.com

Figure 116
Dialing plan window



7 Click **Browse** to find the associated dialing plan for the user. Click **OK**.

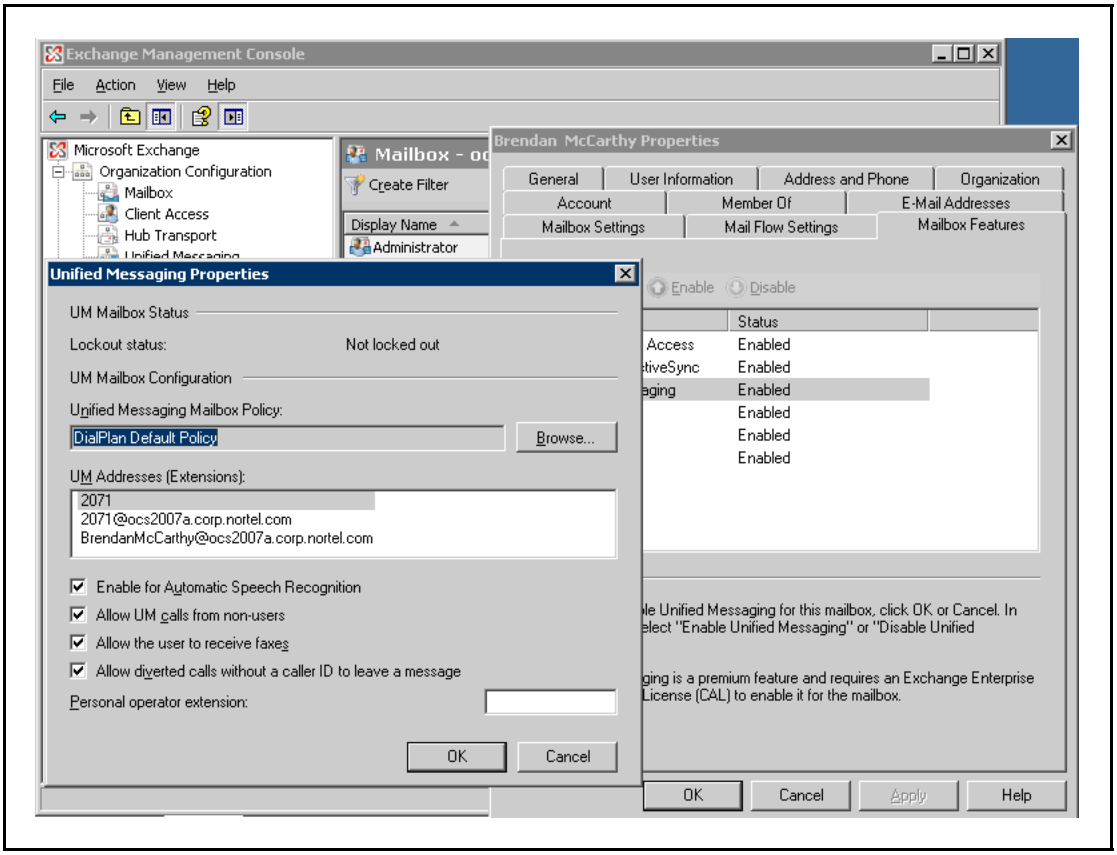
8 From the **E-Mail Addresses** tab, click **Apply**.

9 The new EUM address is added. To find the new UM Extension, click the **Mailbox Features** tab, right-click **Unified Messaging**, and select **Unified Messaging Properties**, as shown in the following figure.

In the **UM Addresses (Extensions)** field, you can see three addresses.

- CS1000 DN
- CS1000DN@domain.com
- useralias@domain.com

Figure 117
Unified Messaging Properties window



10 Click **OK**.

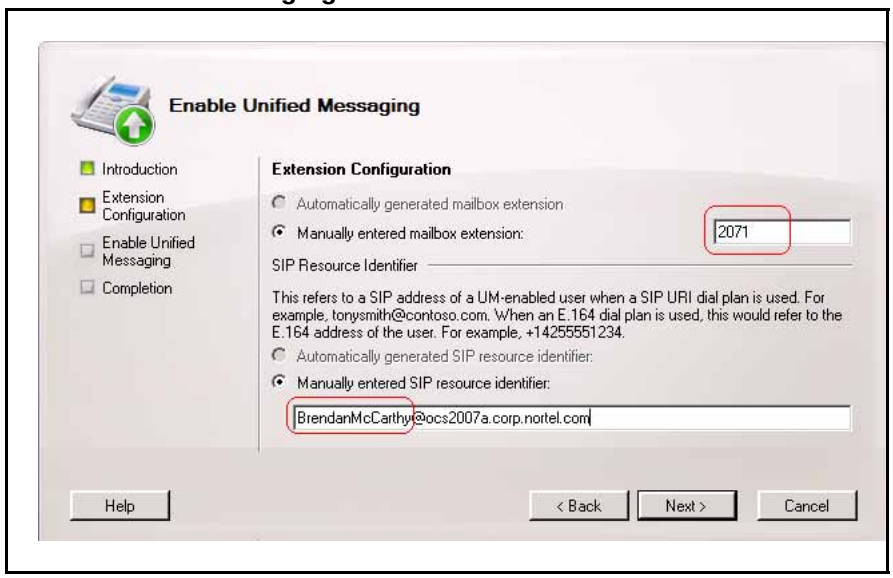
--End--

Option 2—integrated mode

Use the following procedures for OCS 2007 users using Unified Messaging (UM) 2007 to manually configure the user alias in integrated mode for Option 2. You can choose the automated default value if you do not need to change the user alias. The automated default value ensures the Active Directory and the OCS have the same user alias. For more information on configuring Exchange UM for the OCS user, see *CS 1000 with Microsoft Exchange Server 2007 UM* (NN43001-122).

Configuring a basic mailbox for the UM user

Configure a basic mailbox for the UM user. For more information, see "Prerequisites" (page 251).

Step	Action
1	Create a new SIP URI dialing plan in Exchange UM.
2	Configure the OCS user mailbox in Exchange UM.
3	On the **Exchange Management Console** screen, click **Recipient Configuration**. The Mailbox window appears in the right pane.
4	Right-click a user in the right pane and select **Enable Unified Messaging**. The Enable Unified Messaging window opens.
5	Enable the OCS user for UM by manually configuring the SIP URI. Click **Manually entered SIP resource identifier** and type useralias@domain.com, as shown in the following figure. For example, BrendanMcCarthy@ocs2007a.corp.nortel.com. **Figure 118** **Enable Unified Messaging** 
6	Click **Next**.
7	Continue to follow the instructions from the *CS 1000 with Microsoft Exchange Server 2007 UM* (NN43001-122).

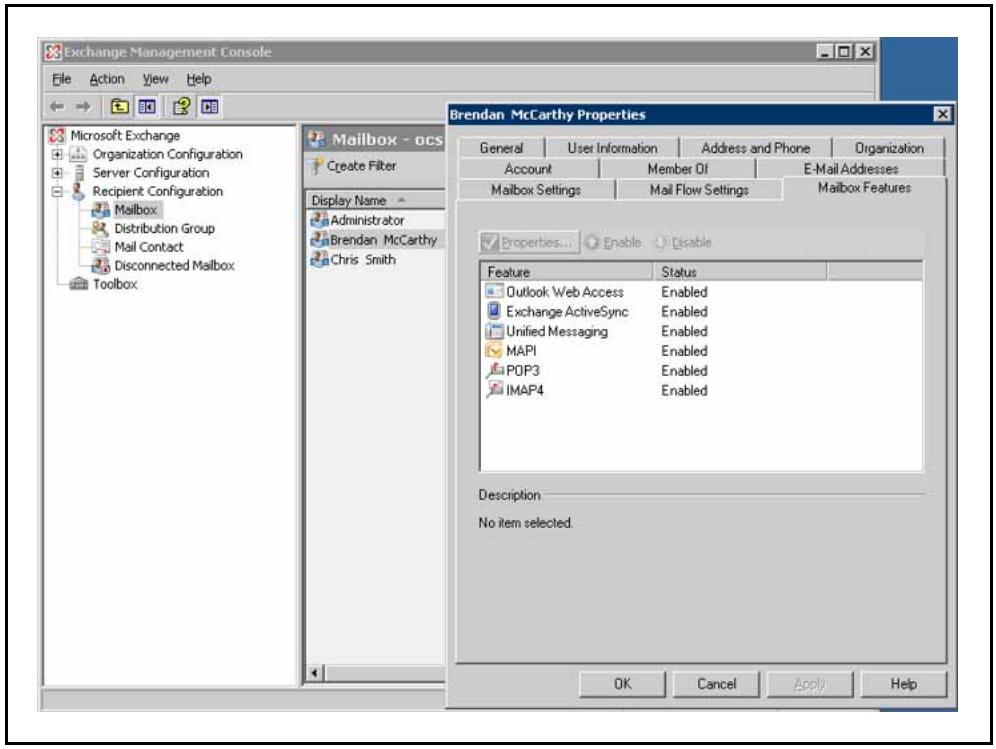
--End--

Adding Exchange UM

Add Exchange UM.

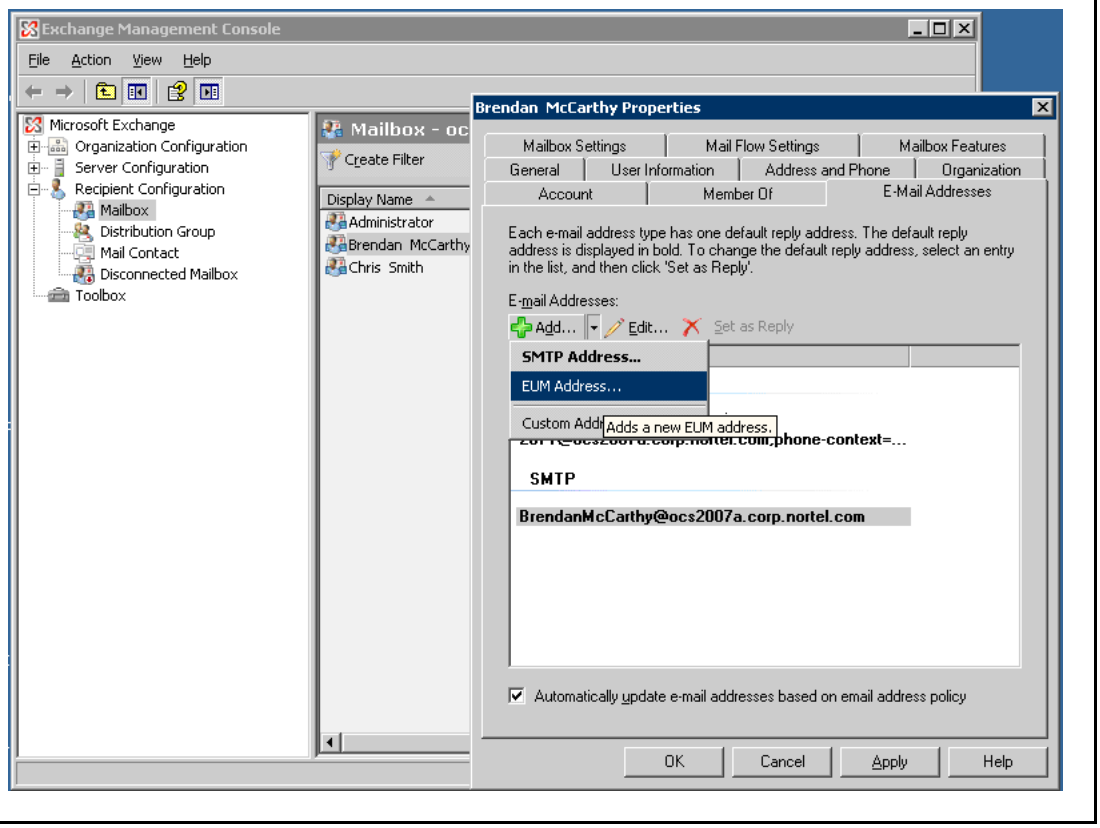
Step	Action
1	From the Exchange Management Console window, click **Recipient Configuration** and **Mailbox**.
2	Right-click a user in the right pane and choose **Properties**, as shown in the following figure.

Figure 119
User Properties window for Exchange UM



3	Click the **E-mail Addresses** tab, as shown in the following figure.

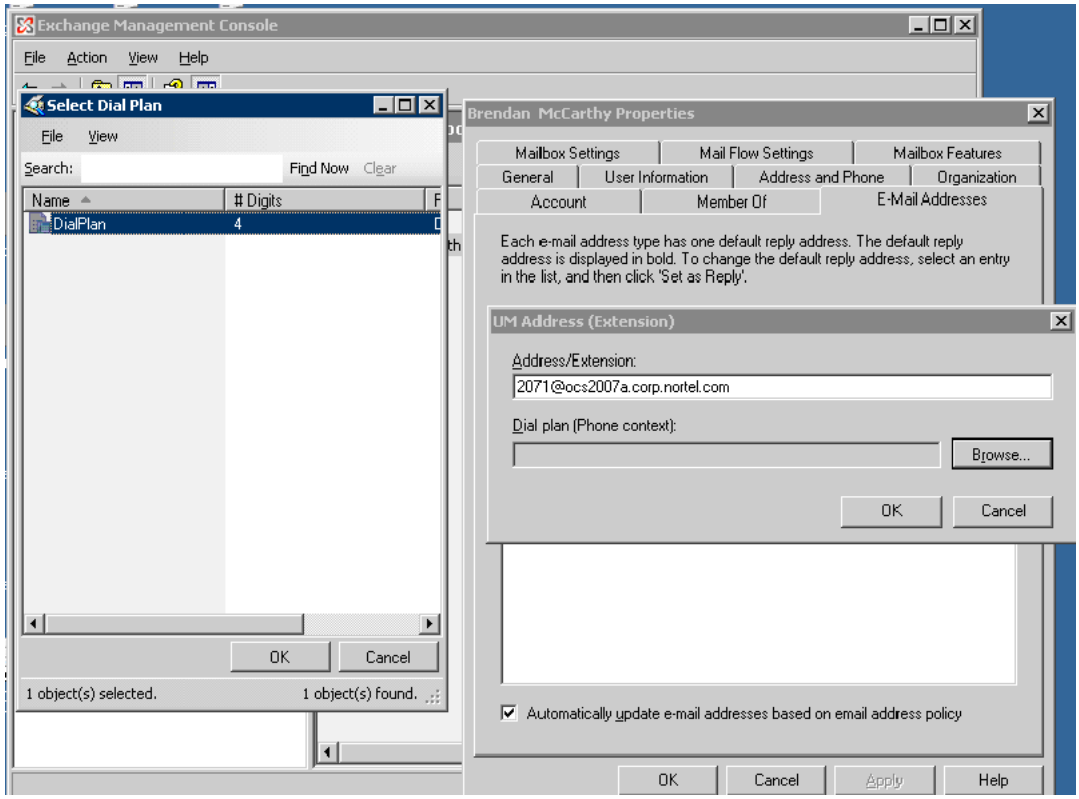
Figure 120
UM Address



4 Click the **Add** menu and select **EUM Address**.

5 In the UM Address (Extension) window, enter the CS1000DN@domain of the user in the **Address/Extension** field, as shown in the following figure. For example, 2071@ocs2007a.corp.nortel.com

Figure 121
Dialing plan window



6 Click **Browse** to find the associated dialing plan for the user. Click **OK**.

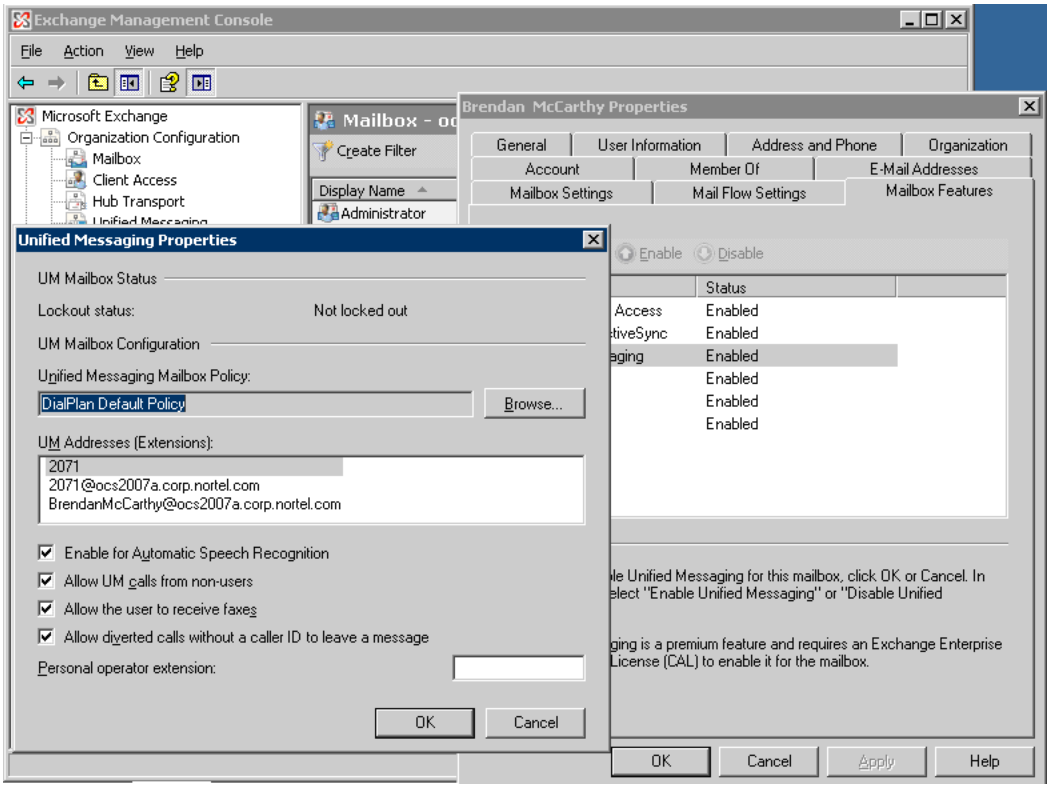
7 From the **E-Mail Addresses** tab of the Properties window, click **Apply**.

8 The new EUM address is added. To find the new UM Extension, click the **Mailbox Features** tab, right-click **Unified Messaging**, and select **Unified Messaging Properties**.

In the **UM Addresses (Extensions)** field, you see three addresses.

- CS1000 DN
- CS1000DN@domain.com
- useralias@domain.com

Figure 122
Unified Messaging Properties window



9 Click **OK**.

--End--

Maintenance

The following are maintenance tips for the CS 1000, MCM, and RCC. For information about troubleshooting tips, see the “Troubleshooting” (page 271) section.

Navigation

Communication Server 1000

No new SIP tracing capabilities are available on the Communication Server 1000. Existing SIP Trunk and Gateway tracing capabilities are used.

MCM

MCM provides the following maintenance features:

Tools

MCM provides the following commands on the Tools menu:

- Active Directory Query: Check phone to user-id mapping. DNs can be entered, and found user-ids are displayed
- Backup Data: Back up a configuration file to the user specified location.
- Restore Data: Restore configuration files from user specified location.
- Set Log Level: Determine (configure) which information is logged in the MCM log file.
- Get Active Calls Count: Show how many calls are connected through Office Communications Server. You can use the Traffic tool to capture SIP and SIP CTI calls and transactions per hour.

— The Multimedia Convergence Manager 3.0 service provides a test capability to retrieve user ID by phone number.

— The Primary and Secondary NRS status utility is available from the application main window.

— You can deploy Ethereal software on the OCS Proxy to provide call traces. MCM also provides full SIP-tracing capability. MCM SIP tracing is important particularly when MTLS (Mutual Transport Layer Security) is enabled in future Communication Server 1000 releases- where SIP traces cannot be captured by a tool like Ethereal. MCM SIP tracing can be filtered by DN number. MCM SIP tracing is implemented as part of the application logging functionality. Special commands are not required. For more information about tracing, see “Capturing traces and logs” (page 283)

— You can remotely access the Office Communications Server application using the Windows 2003 server remote access capability.

— Task Manager is supported in Windows 2003 Server for MCM.

Patches and upgrades

Patching is not supported in MCM 4.x. Fixes are provided in up-issues and maintenance releases.

ATTENTION
All customer configured MCM application data is retained during an MCM application upgrade.

Remote Call Control

Use the following Signaling Server OAM Level CLI commands to query active TR/87 sessions and to turn on tracing at the SIP level.

Signaling Server OAM Level CLI Commands

You can use these commands to terminate either a session for a specific DN or to terminate all TR/87 sessions that are currently active on the server.

Table 51
Signaling Server OAM Level CLI commands

Prompt	Command/User Response	Description
>	SIPCTISessionShow tSSG	Show the total number of TR87 SIP sessions.

Table 51
Signaling Server OAM Level CLI commands (cont'd.)

Prompt	Command/User Response	Description
>	SIPCTITraceShow	Display the trace settings for SIP CTI application, including the trace filter setting and output setting.
>	SIPCTIShow tSSG	Show SIP CTI application status and configuration.
>	SIPCTIClientShow	Show information about the all the soft clients associated.
>	SIPCTITraceLevel <level>	Configure the TR87 SIP message Trace Level. The level can be one of the following: 0 –TR87 SIP message body (ECMA 323) only 1 – TR87 SIP message body (ECMA 323) and message headers
>	SIPCTITrace on	Turn on SIP CTI trace for all soft clients in both incoming and outgoing directions.
>	SIPCTITrace off	Turn off SIP CTI trace for all soft clients in both incoming and outgoing directions.
>	SIPCTITrace <MsgRcv> <MsgSend>	Turn on SIP CTI trace for all soft clients in incoming and/or outgoing. The parameter is either on or off.
>	SIPCTITrace sc <soft client SIP/Tel URI/DN> <MsgRcv><MsgSend>	Turn on SIP CTI trace for a specific soft client in incoming and/or outgoing direction(s). This may result in a number of sessions as a single URI could be used for multiple active sessions.
>	SIPCTIOutput <Dest> <"fileName">	Redirecting the SIP CTI trace to a specific output destination. The destination can be one of the following: • TTY • RPTLOG • File

Table 51
Signaling Server OAM Level CLI commands (cont'd.)

Prompt	Command/User Response	Description
		If File is selected as the output destination, the filename must be given.
>	SIPCTIStop all	De-acquire all AST DNs and terminate all the TR87 SIP sessions.
>	SIPCTIStop <dn>	De-acquire one specific AST DN and terminate all the TR87 SIP sessions associated with this AST DN.
OAM>	amlAcquiredTNShow <"TN"> where the TN is a string in quotation marks. For example: <TN>="4010"	Displays the contents of the Acquired DN list for the given <TN>. For example: If a DN of a given <TN> is acquired by one or more application links, the output is as follows: The DN1 of the <TN> is acquired by: <Application ID1> <Application ID2> ..... The DN2 of the <TN> is acquired by: <Application ID1> <Application ID2> ..... If no DN of the given <TN> is acquired by any application, the following appears: **The TN <TN> is not acquired by any application through the AML Front End.**
OAM>	amlApplLinkShow [<Application ID>] where Application ID is an optional parameter and is equal to a string If it is not given, all records (up to five) are displayed in the Application Link table.	Displays the record in the Application Link table with the given Assigned Application ID. The , For example: If there is a record in the Application Link table with the given Assigned Application ID, the output is as follows: **<Application ID>** **IP Address: ###.###.###.###**

Table 51
Signaling Server OAM Level CLI commands (cont'd.)

Prompt	Command/User Response	Description
		Message Filter Bitmap: 0x## (in Hex) **Feature Control Bitmap: 0x## (in Hex)** **Number of Acquired DNs: ####** If there is no record in the Application Link table with the given Assigned Application ID, the following appears: **No record for the application link with the given Application ID.**
OAM	amlAcquiredTNClearAll	Clears the following: • Acquired TN table • Acquired DN lists • Application ID lists • and updates the Application Link table The value for the NumberofAcquiredDNs is set to zero. If there is a minimum of one telephone that is acquired by at least one application, the acquired resources on the Call Server are not de-acquired. For the Call Server to de-acquire all the resources acquired through the AML FE, the following output appears **OK. Please issue command DACR ALL <#> in overlay 48 on the CS.** Where # is equal to the AML Link number for the AML FE. If no telephone is acquired, the following is displayed: **No phone is acquired through the AML FE.**

Operational Measurements for SIP CTI

The following Operational Measurements (OM) details are collected for SIP CTI:

- SIPCTITotalSoftClientLoginAttempts
- SIPCTITotalSoftClientLoginSuccesses
- SIPCTITotalAnswerCallRequests
- SIPCTITotalAnswerCallSuccesses
- SIPCTITotalClearConnectionRequests
- SIPCTITotalClearConnectionSuccesses
- SIPCTITotalConsultationCallRequests
- SIPCTITotalConsultationCallSuccesses
- SIPCTITotalDeflectCallRequests
- SIPCTITotalDeflectCallSuccesses
- SIPCTITotalHoldCallRequests
- SIPCTITotalHoldCallSuccesses
- SIPCTITotalMakeCallRequests
- SIPCTITotalMakeCallSuccesses
- SIPCTITotalRetrieveCallRequests
- SIPCTITotalRetrieveCallSuccesses
- SIPCTITotalSingleStepTransferRequests
- SIPCTITotalSingleStepTransferSuccesses
- SIPCTITotalTransferCallRequests
- SIPCTITotalTransferCallSuccesses
- SIPCTITotalMonitorStartRequests
- SIPCTITotalMonitorStartSuccesses
- SIPCTITotalMonitorStopRequests
- SIPCTITotalMonitorStopSuccesses
- SIPCTITotalConferenceCallRequests
- SIPCTITotalConferenceCallSuccesses
- SIPCTITotalSetForwardingRequests
- SIPCTITotalSetForwardingSuccesses
- SIPCTITotalGetForwardingRequests

- SIPCTITotalGetForwardingSuccesses
- SIPCTITotalSessionTerminated

For information about how to access OM through Element Manager, see *Element Manager System Reference — Administration* (NN43001-632) .

Signaling Server Expert Level CLI Commands

Use Signaling Server Expert Level CLI commands, as shown in the following table. You can trace AML commands that are sent by the TR/87 FE to the Call Server on behalf of the Office Communicator clients that may be active.

Table 52
Signaling Server Expert Level CLI commands

Prompt	Response	Description
	SIPCTIAmlTrace level	Configure AML Trace level for SIP CTI application. The level can be one of the following: • 0—Turn off trace. • 1—Print all input and output AML data buffer. • 2—Print all input and output AML data buffer except POLLING message. • 3—Print all input and output AML data buffer except POLLING message, with IE type decoding. • 4—Print all input and output AML data buffer except POLLING message with IE type and data decoding. **ATTENTION** This trace prints out AML messages to and from CS at the transport layer. Because sending and receiving AML messages are per AML link instead of per DN or TN, no good solution exists to filter on this AML trace tool. Nortel recommends that you do not turn on the trace in a busy system.

Troubleshooting

Use the following procedures to assist in troubleshooting general Converged Office problems.

Navigation

Checking Telephony Gateway (SIP Gateway) configuration

Use the following procedure for checking the Telephony Gateway configuration.

Step	Action
1	Check all required Communication Server 1000 resources (packages, license, and Communication Server 1000 patches).
2	Check the DN, telephone TN and TLSV configuration.
3	Check the DNS on the Signaling Server.
4	Verify the Signaling Server SIP and the MCM endpoint registration on the NRS.
5	Ensure that MCM is registered to the NRS.
6	Verify the Host Authorization and Certificates for Office Communications Servers and Pool.

ATTENTION
Improper configuration of Host Authorization and Certificates for Office Communications Servers and Pool is the primary reason Converged Office does not function properly in the Enterprise Edition configuration.

--End--

Checking Remote Call Control (SIP CTI) configuration

Use the following procedure for checking the Remote Call Control configuration.

Step	Action
1	Check all required Communication Server 1000 resources (packages, license, and Communication Server 1000 patches).
2	Check the DN, telephone TN, and TLSV configuration.
3	Verify that AST, IAPG, and CLS (CDMR/TR87A) are configured correctly (SIP CTI only).
4	Verify that the AML Link status is up. Make sure that the ELAN ID is greater or equal to 32 (SIP CTI only).
5	Check the SIP CTI status (on the Signaling Server at the prompt, issue the command SIPCTIShow). Make sure the SIP CTI status reads **Application status: Active** (SIP CTI only).
6	Check the DNS on the Signaling Server.
7	Verify the Signaling Server SIP and the MCM endpoint registration on the NRS.
8	Ensure that MCM is registered to the NRS.

9 Verify the MCM configuration for the Called Phone Context and check it against the Signaling Server configuration for the SIP URI map and Private/CDP domain name parameter (SIP CTI only).

10 Verify the Routing, Host Authorization, and Certificates inside OCS servers and Pool.

Note: Improper configuration of Routing, Host Authorization, and Certificates on OCS Servers and Pool is the primary reason Converged Office does not function properly in the Enterprise Edition configuration.

11 If the problem still exists, go to the section "Capturing traces and logs" (page 283)to assist further.

--End--

Lack of memory on Signaling Server

Problem:
Lack of memory on Signaling Server.

Symptom:
After SIP CTI services are activated, you are unable to log on to the Signaling Server through Element Manager. When rebooting, some HTTP tasks are not up.

Possible cause:
Insufficient memory.

Solution:
Check the memory and upgrade the memory to 1 gigabyte (GB), if required. The Signaling Server (running Converged Office) requires 1 GB of memory. Release 4.5 only required 512 megabytes (MB).

SIP CTI services does not come up

Use the following for troubleshooting purposes.

SIP Dialog not established

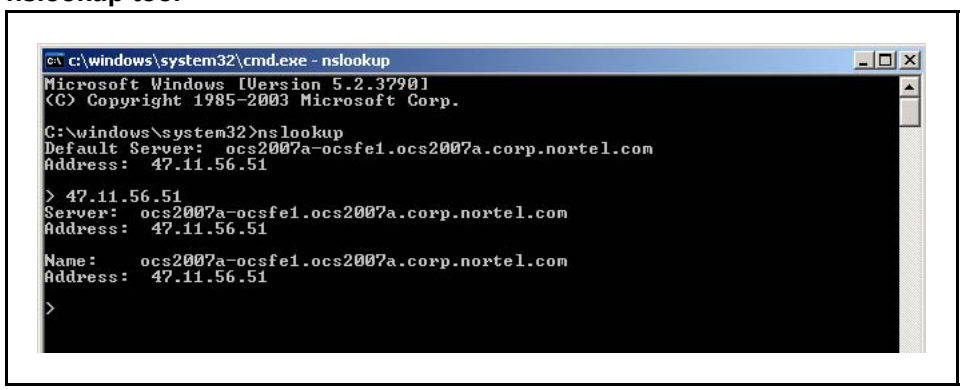
Problem:
Phone integration is enabled in Office Communicator and a SIP dialog for TR/87 was attempted and not established successfully.

Symptom:
When logged into the Office Communicator, the phone icon is not displayed.

Possible cause 1:
The Server URI or the Line URI is incorrect.

Possible cause 2:
Use the Microsoft nslookup tool to verify the DNS configuration on the Signaling Server and the Host Name resolution for each IP address. For more information about the nslookup tool, see Figure 123 "nslookup tool" (page 274)or go to the Microsoft Web site at www.microsoft.com.

Figure 123
nslookup tool



Solution 1: Check configuration parameters in AD

Check the configuration parameters in Active Directory for this user. Run a SIPCTITrace on the Signaling Server and check the MCM logs. For more information about activating the trace, see “SIP CTI traces on the Signaling Server” (page 284).

Solution 2: Confirm FQDN and the IP address are correct

Solution 2:
Confirm that the FQDN (case sensitive) and the IP address are correct.

For causes (not mentioned), the following actions may help identify the problem:

- Activate AML traces on the Call Server to check if the IACR/IACS (TN acquire) is correct. For more information about capturing traces, see “AML traces on the Call Server (SIP CTI only)” (page 283)
- Activate SIPCTITrace. For more information about traces, see Table 56 "SIP CTI trace" (page 284)
- Activate OCS Front End server and Proxy server traces
- Activate MCM logs
- Capture Ethereal traces

SIP CTI service is down

Problem:
SIP CTI service down.

Symptom:
After SIP CTI services are activated, SIP CTI services does not come up.

Possible cause:
VSID or ELAN ID is lower than 32.

Solution:
Use the following procedure to resolve this issue.

Reconfiguring SIP CTI service

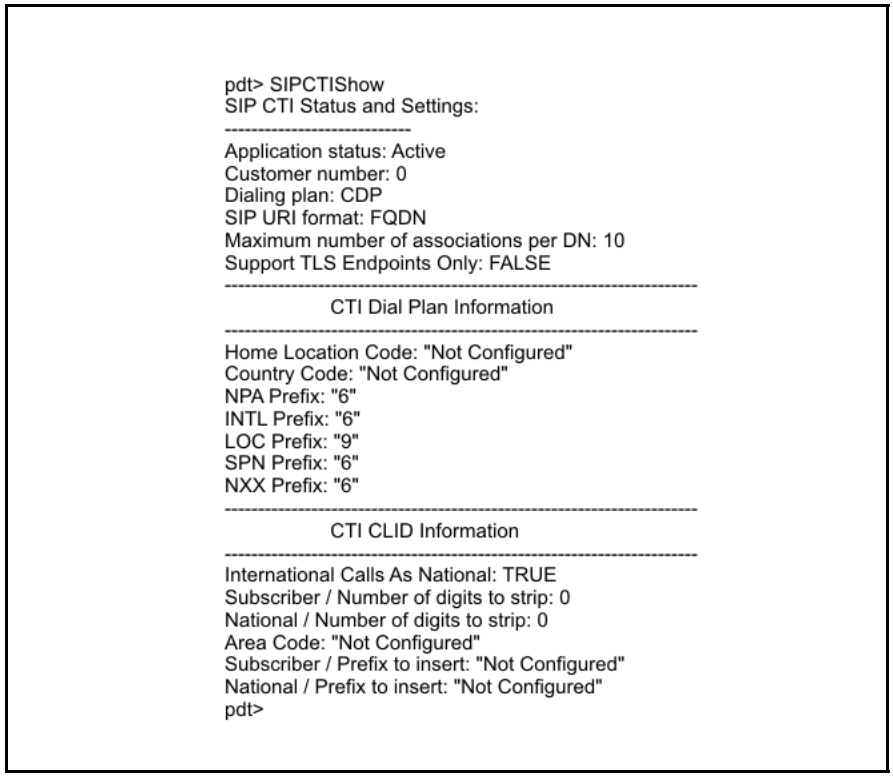
Step	Action
1	Reconfigure the VSID and ELAN IDs so both are greater than 32. Confirm that the SIP CTI service is up.
2	Check the SIP CTI status on the Signaling Server.

Table 53
Check the SIP CTI status

Prompt	Response	Description
	SIPCTIShow tSSG	show SIP CTI status and settings

See Figure 124 "Screen output example for SIP CTI status" (page 276).

Figure 124
Screen output example for SIP CTI status



3 In LD 48, check the ELAN status on the Call Server

Table 54
LD 48

Prompt	Response	Description
.stat	elan	Check the ELAN status on the Call Server

Screen output:
SERVER TASK: ENABLED
ELAN #: 032 DES: CDLCS
APPL_IP_ID: 47.11.157.112 : 0000F600 LYR7: ACTIVE EMPTY APPL ACTIVE

--End--

MCM not synchronizing new users in AD Cache mode

Problem:
MCM cannot synchronize new users in AD Cache Mode.

Symptom:
Several new users are configured in AD, but MCM did not download them to its AD Cache during synchronization and cannot find them.

Possible cause 1:
The changes made to those users in AD is not replicated to the Global Catalog (GC) server used by MCM.

Possible cause 2:
MCM Service credentials are not sufficient to view the msRTCSIP properties.

Possible cause 3:
The Active Directory field is not enabled for propagation to the Global Catalog.

Solution 1: Checking the Global Catalog content manually

Consult with the Network Administrator about the schedule of replications between Domain Controllers (DC).

Use the following procedure to check the Global Catalog (GC) content.

Step	Action
1	Install the Operating System Support Tools on the server (usually the Tools setup is on the MS Windows 2003 Server setup disk).
2	Run the LDP tool (%ProgramFiles%\Support Tools\ldap.exe).
3	Connect to the GC server IP address at the port 3268 (Connection -> Connect …).
4	Bind with the MCM service account credentials (Connection -> Bind …).
5	Download the AD structure tree (View -> Tree).
6	Navigate to the object of one of those just configured users.
7	Confirm that the object contains the properties: • msRTCSIP-UserEnabled and it is configured to TRUE • msRTCSIP-PrimaryUserAddress and it is configured with correct User • SIP URI • with correct phone number • msRTCSIP-OptionFlags

- msRTCSIP-Line
- msRTCSIP-LineServer

If some of those properties are not presented, or configured with old values, then the GC server is not replicated. The user must wait for the next automatic replication or run the replication manually.

If you are unsure that the replication is complete, or that the properties msRTCSIPUserEnabled and/or msRTCSIP-OptionFlags are not presented, see Possible cause 2 and “Solution 2: Accessing permissions for the AD object properties” (page 278).

--End--

Solution 2: Accessing permissions for the AD object properties

Solution 2:

Use the following procedures to check the access permissions for the AD object properties.

Step	Action
1	Install the Operating System Support Tools on the server (usually the Tools setup is on the MS Windows 2003 Server setup disk).
2	Run the ADSIEdit tool (%ProgramFiles%\Support Tools\adsiedit.msc).
3	Navigate to the users object container or the specific user object.
4	Right-click the item and open **Properties**.
5	Go to the **Security** tab and click the **Advanced** button.
6	Search for the permission entry specific for the msRTCSIP properties group or RTCPropetySet. If there is a specific user group that has access rights to that property group, then the best solution is to add the MCM service account to this user group. Otherwise, you have to allow MCM Service account to read the properties **msRTCSIP-UserEnabled, msRTCSIP-PrimaryUserAddress, msRTCSIPOptionFlags, msRTCSIP-Line,** and **msRTCSIP-LineServer**.
7	Click **Add**.
8	Choose the **MCM service account** and click **OK**.
9	Go to the **Properties** tab.
10	Select **User objects** in the field **Apply onto**.

11	In the **Permissions** list box select the Allow check boxes across the Read permission of necessary properties and RTCPropetySet.
12	Click **OK**.

--End--

Solution 3: Enabling propagation of the AD to the Global Catalog

Enable propagation of the Active Directory field to the Global Catalog. Be sure to specify a Domain Controller LDAP server (port 389) to reduce the search scope to only one domain. Use the following procedure.

Step	Action
1	Open the Active Directory Schema snap-in.
2	Select the Attributes folder on the left pane.
3	Find and the right-click the necessary field (**otherTelephone**).
4	Click the **Property** menu item.
5	Enable **Replicate this attribute to the Global Catalog.**
6	Click **OK**.

--End--

OC client not registered

The following is a list of areas to troubleshoot when only one client is unable to register:

- Check to ensure that all clients are registered.
- Look in the client options for Active Directory for a mistake in SIP URI or Line URI.
- For RCC enabled user, ensure that the T87A class of service is configured for this client and a session is established.
- Remove RCC to see if VOIP functionality is present.

The following is a list of areas to troubleshoot when all clients are unable to register:

- Ensure all component configuration information is correct on the Front End server, Mediation Server, MCM, Signaling Server, SPS, Call Server, and DNS.
- Capture logs starting with the client logs. SIP messages between the Mediation Server and the Front End server cannot be seen as this is a secure leg.

Pop-up not displayed

Problem:
Pop-up not displayed.

Symptom:
When a Office Communicator user receives a call, the called telephone rings, but no pop-up appears for the user to click to answer the call.

Possible causes:
The Phone Context may be not correct. Address Book Service may not be properly setup. Phone integration is not activated.

Solutions:

- Ensure that the user's name is in Active Directory, the MCM, and the Signaling Server (L1 parameter) have the correct Phone Context.
- Ensure Address Book Service properly setup for an OC client is essential in receiving correct CLID info on call pop-ups
- Ensure PBX Integration is marked for an OC client in Active Directory and Server URI line is filled with valid info
- Ensure User has activated Phone integration on OC client
- Ensure TLSV is configured properly for the called user.

Two pop-ups are displayed

Problem:
Two toasts appear.

Symptom:
In some transfer and conference scenarios, the user receives two toasts instead of a merged one. One is with CLID information of the transferring telephone and the other is with CLID information of the original caller.

Solution:
The Route List Data Block must have the prompt DORG configured to No. The default value for DORG is No. For more information, see "Route list data block" (page 196).

Delay for a SIP Gateway call

Problem:
Delay for a SIP Gateway call.

Symptom:
Office Communicator users observe a delay at the beginning of a call.

Possible cause:
Missing Office Communicator patch.

Solution:
Ensure that the Office Communicator patch is up-to-date.

Call Forward is cancelled by Office Communicator

Problem:
Office Communicator cancels the Call Forward configured on the telephone.

Symptom:
The telephone is on Call Forward to another number. When the Office Communicator user who is associated to this telephone logs in (this telephone is controlled by the Office Communicator user through SIP CTI), the Office Communicator cancels the Call Forward.

Possible cause:
This is a Microsoft issue that Nortel has escalated to Microsoft.

Solution:
No solution yet.

Office Communicator disconnecting from the network

Problem:
Office Communicator user cannot control the telephone after having been disconnected several times.

Symptom:
Customers using smart telephones or Mobile Communicators cannot take control of the telephone after having been disconnected abruptly three or more times. This disconnection could be due to your network (for example, GPRS or WLAN).

Possible cause:
This problem occurs because the SIP CTI link is disconnected abnormally and the Association is out of service for 30 minutes (1800 seconds). This timer is hard-coded by Office Communicator and cannot be changed.

Solution:
Increase the **Maximum Associations per DN** on the Signaling Server through Element Manager. This field is configured to 3 by default. Increase this parameter to allow more network disconnections.

Anonymous Calling Line Identification on incoming call toast (OCS R2 only)

Problem:
Incoming call to a fully converged Office Communicator R2 client, where the Calling Line Identification (CLID) is blocked or the trunk type does not support CLID.

Symptom:
OC R2 client gets the incoming call toast "Unidentified Caller" but cannot answer the call either by phone or by computer.

Workaround Solution:
The MCM 4.x has bundled commands to replace the anonymous CLID into a predefined number before presenting the call to the OC client.

1. Collect and investigate MCM or Wireshark traces. Analyze VoIP FROM header and RCC <callingDevice> attribute field. For example, for an incoming call from PSTN through DTI trunk you have:
   VoIP address: sip:anonymous@anonymous.invalid
   RCC number: tel:anonymous
2. Using MCMConsole CLI define VoIP and RCC mapping to a defined number. On the MCM server, open a command prompt window. Change to the MCM directory, for example, C:\Program Files (x86)\Nortel\MCM). For this example, type the following two commands to change the anonymous CLID into +16135550000:
   MCMConsole "/VoIPChange:<sip:anonymous@anonymous.invalid><sip:+16135550000@domain.com;user=phone>
   MCMConsole "/RCCChange:<tel:anonymous><tel:+16135550000>
3. Open and check MCM.ini file in MCM program directory. The following two lines should be visible:
   VoIP_replace=<sip:anonymous@anonymous.invalid><sip:+161355500

00@domain.com;user=phone>
RCC_replace=<tel:anonymous><tel:+16135550000>

4. Make a test call to OC client. An incoming toast displaying "+16135550000" appears. You can answer the call on phone or computer as usual.

Capturing traces and logs

Use the following procedures to capture traces and logs to assist in troubleshooting Converged Office problems. When a problem is encountered, traces and logs can be activated on different components.

- Communication Server 1000 traces
- MCM logs
- OCS logs
- OC logs

ATTENTION
MCM logs are used for debugging purposes only. Use the Event Viewer to determine if any Error Events were logged. A detailed description of an Event can be seen by right-clicking on the Event and selecting Properties from the pop-up menu. Report any problems listed in the Event description.

Communication Server 1000 traces

Use the following procedures for capturing traces.

AML traces on the Call Server (SIP CTI only)

In LD 48, activate AML traces on the Call Server (SIP CTI only):

Table 55
LD 48

Prompt	Response	Description
EDD000	enl msgi 32	Enable incoming AML traces for ELAN 32
EDD000	enl msgo 32	Enable outgoing AML traces for ELAN 32

Screen output:

ELAN32 I MTYP=3B IACR TN=0 TIME=18:07:34
ELAN32 IN B1B1BE7A OUT B1B1BE7C QSIZE 00000000
ELAN32 03 20 00 00 00 00 1E 3B 00 0B 00 00 95 01 05 36 02 72 14 E6
ELAN32 0C BF EE 01 FF FF FF 00 00 0F FF 00 00

```
ELAN32 O MTYP=3C IACS TN=0 TIME=18:07:34
ELAN32 IN B1B1BE8B OUT 00000000 QSIZE 00000000
ELAN32 03 27 00 00 00 00 1E 3C 00 0B 00 00 95 01 05 36 02 72 14 E6
ELAN32 0C BF EE 01 FF FF FF 00 00 0F FF 00 00 37 02 98 C2 AA 01 00

ELAN32 I MTYP=1D SETFTR TN=0 TIME=18:07:34
ELAN32 IN B1B1C6E8 OUT B1B1C6EA QSIZE 00000000
ELAN32 03 16 00 00 00 00 16 1D 00 0B 00 00 46 01 08 36 02 72 14 3F
ELAN32 02 00 00

ELAN32 O MTYP=1D SETFTR TN=0 TIME=18:07:34
ELAN32 IN B1B1C6EE OUT 00000000 QSIZE 00000000
ELAN32 03 1D 00 00 00 00 16 1D 00 0B 00 00 3F 02 98 C2 46 01 08 36
ELAN32 02 72 14 71 01 01 78 02 20 0E
```

SIP CTI traces on the Signaling Server

Activate **SIP CTI** traces on the Signaling Server.

Table 56
SIP CTI trace

Prompt	Response	Description
	SIPCTITrace on	activate SIP CTI trace
	SIPCTITraceLevel 1	

Figure 125
Example of screen output for SIP CTI Traces on the Signaling Server

```
=~=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2008.01.23 22:37:58
=~=~=~=~=~=~=~=~=~=~=~=~=~=
[SIPCTITrace:] (23/01/08 23:39:39) <?xml version="1.0" encoding="UTF-
8"?>
[SIPCTITrace:] (23/01/08 23:39:39) <DeliveredEvent
xmlns="http://www.ecma-international.org/standards/ecma
[SIPCTITrace:] (23/01/08 23:39:39) -323/csta/ed3">
[SIPCTITrace:] (23/01/08 23:39:39)
<monitorCrossRefID>37</monitorCrossRefID>
[SIPCTITrace:] (23/01/08 23:39:39)
<connection><callID>19797</callID><deviceID>tel:+16139675000;ext=3050</
[SIPCTITrace:] (23/01/08 23:39:39) deviceID></connection>
[SIPCTITrace:] (23/01/08 23:39:39)
<alertingDevice><deviceIdentifier>tel:+16139675000;ext=3050</deviceIden
[SIPCTITrace:] (23/01/08 23:39:39) tifier></alertingDevice>
[SIPCTITrace:] (23/01/08 23:39:39)
<callingDevice><deviceIdentifier>tel:2014;phone-context=cdp.udp</device
[SIPCTITrace:] (23/01/08 23:39:39) Identifier></callingDevice>
[SIPCTITrace:] (23/01/08 23:39:39)
<calledDevice><deviceIdentifier>tel:+16139675000;ext=3050</deviceIdenti
[SIPCTITrace:] (23/01/08 23:39:39) fier></calledDevice>
[SIPCTITrace:] (23/01/08 23:39:39)
<lastRedirectionDevice><notRequired/></lastRedirectionDevice>
[SIPCTITrace:] (23/01/08 23:39:39)
<localConnectionInfo>alerting</localConnectionInfo><cause>normal</cause
[SIPCTITrace:] (23/01/08 23:39:39) >
[SIPCTITrace:] (23/01/08 23:39:39) </DeliveredEvent>
[SIPCTITrace:] (23/01/08 23:39:46) <?xml version="1.0" encoding="UTF-
8"?>
[SIPCTITrace:] (23/01/08 23:39:46) <ConnectionClearedEvent
xmlns="http://www.ecma-international.org/standa
[SIPCTITrace:] (23/01/08 23:39:46) rds/ecma-323/csta/ed3">
[SIPCTITrace:] (23/01/08 23:39:46)
<monitorCrossRefID>37</monitorCrossRefID>
[SIPCTITrace:] (23/01/08 23:39:46)
<droppedConnection><callID>19797</callID><deviceID>tel:+16139675000;ext
[SIPCTITrace:] (23/01/08 23:39:46) =3050</deviceID></droppedConnection>
[SIPCTITrace:] (23/01/08 23:39:46)
<releasingDevice><deviceIdentifier>tel:+16139675000;ext=3050</deviceIde
[SIPCTITrace:] (23/01/08 23:39:46) ntifier></releasingDevice>
[SIPCTITrace:] (23/01/08 23:39:46)
<localConnectionInfo>null</localConnectionInfo><cause>normal</cause>
[SIPCTITrace:] (23/01/08 23:39:46) </ConnectionClearedEvent>
```

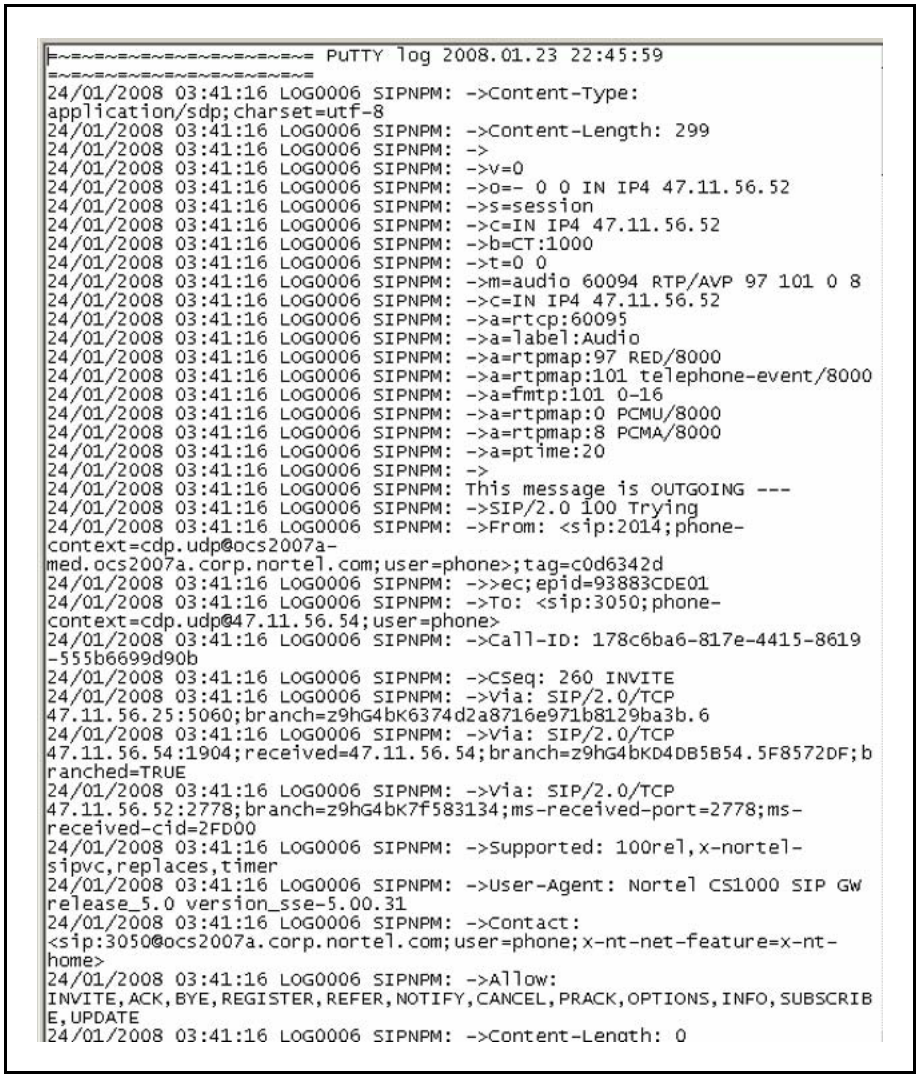
SIP Gateway traces on the Signaling Server

Activate **Gateway** traces on the Signaling Server.

Table 57
SIP Gateway trace

Prompt	Response	Description
	SIPCallTrace on	
	SIPTraceLevel 1	

Figure 126
Example of screen output for SIP Gateway trace



```
=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2008.01.23 22:45:59
=~=~=~=~=~=~=~=~=~=~=~=~=
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Content-Type:
application/sdp;charset=utf-8
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Content-Length: 299
24/01/2008 03:41:16 LOG0006 SIPNPM: ->
24/01/2008 03:41:16 LOG0006 SIPNPM: ->v=0
24/01/2008 03:41:16 LOG0006 SIPNPM: ->o=- 0 0 IN IP4 47.11.56.52
24/01/2008 03:41:16 LOG0006 SIPNPM: ->s=session
24/01/2008 03:41:16 LOG0006 SIPNPM: ->c=IN IP4 47.11.56.52
24/01/2008 03:41:16 LOG0006 SIPNPM: ->b=CT:1000
24/01/2008 03:41:16 LOG0006 SIPNPM: ->t=0 0
24/01/2008 03:41:16 LOG0006 SIPNPM: ->m=audio 60094 RTP/AVP 97 101 0 8
24/01/2008 03:41:16 LOG0006 SIPNPM: ->c=IN IP4 47.11.56.52
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=rtcp:60095
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=label:Audio
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=rtpmap:97 RED/8000
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=rtpmap:101 telephone-event/8000
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=fmtp:101 0-16
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=rtpmap:0 PCMU/8000
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=rtpmap:8 PCMA/8000
24/01/2008 03:41:16 LOG0006 SIPNPM: ->a=ptime:20
24/01/2008 03:41:16 LOG0006 SIPNPM: ->
24/01/2008 03:41:16 LOG0006 SIPNPM: This message is OUTGOING ---
24/01/2008 03:41:16 LOG0006 SIPNPM: ->SIP/2.0 100 Trying
24/01/2008 03:41:16 LOG0006 SIPNPM: ->From: <sip:2014;phone-
context=cdp.udp@ocs2007a-
med.ocs2007a.corp.nortel.com;user=phone>;tag=c0d6342d
24/01/2008 03:41:16 LOG0006 SIPNPM: ->>ec;epid=93883CDE01
24/01/2008 03:41:16 LOG0006 SIPNPM: ->To: <sip:3050;phone-
context=cdp.udp@47.11.56.54;user=phone>
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Call-ID: 178c6ba6-817e-4415-8619
-555b6699d90b
24/01/2008 03:41:16 LOG0006 SIPNPM: ->CSeq: 260 INVITE
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Via: SIP/2.0/TCP
47.11.56.25:5060;branch=z9hG4bK6374d2a8716e971b8129ba3b.6
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Via: SIP/2.0/TCP
47.11.56.54:1904;received=47.11.56.54;branch=z9hG4bKD4DB5B54.5F8572DF;b
ranched=TRUE
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Via: SIP/2.0/TCP
47.11.56.52:2778;branch=z9hG4bK7f583134;ms-received-port=2778;ms-
received-cid=2FD00
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Supported: 100rel,x-nortel-
sipvc,replaces,timer
24/01/2008 03:41:16 LOG0006 SIPNPM: ->User-Agent: Nortel CS1000 SIP GW
release_5.0 version_sse-5.00.31
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Contact:
<sip:3050@ocs2007a.corp.nortel.com;user=phone;x-nt-net-feature=x-nt-
home>
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIB
E,UPDATE
24/01/2008 03:41:16 LOG0006 SIPNPM: ->Content-Length: 0
```

MCM logs

MCM generates a daily log file with no maximum size restrictions and no cleanup procedures are implemented. The contents of the existing log file remain in all cases.

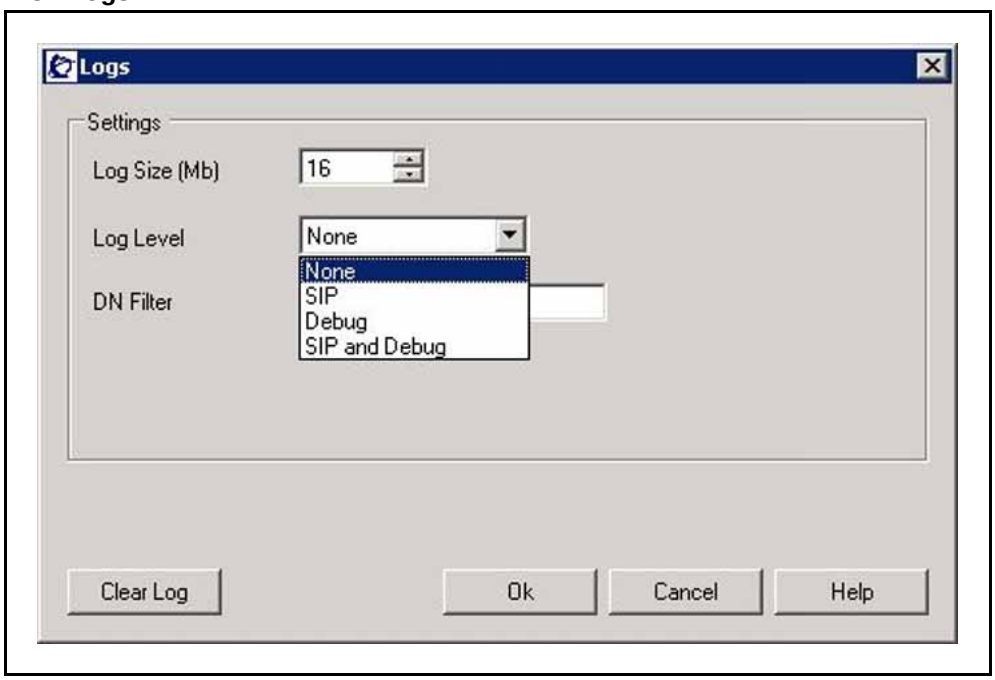
SNMP is not supported on the MCM application. Alarms are logged to an MCM log file in addition to the Windows 2003 Event Viewer.

MCM logging has the following levels:

- **None**: No messages or alarms are logged to the file. (Alarms are still logged to Windows Event Viewer).
- **SIP**: SIP messages (filtered by distinct DN) are logged further to alarms. Only one DN can be specified at the same time in MCM.
- **Debug**: Debug information is logged to the MCM log file.
- **SIP and Debug**

To clear a log, click **Clear Log**. The backup file is stored as MCMlog.bak. See Figure 127 "MCM logs" (page 287) for an example of the Logs window.

Figure 127
MCM logs



Activating MCM logging

The following section details how to turn on MCM logging. MCM Logs can be enabled from MCM Console. Log files are stored in MCM.log file which is located in the MCM application installation directory (?:\Program Files\Nortel\MCM\MCM.log).

Step	Action
1	On the MCM console interface, to activate MCM logs, select **Tools** and then choose **Logs** from the menu.

2 Go to **Log Level** and choose **Debug**.

--End--

To turn off MCM logging, see "Resetting MCM debug trace" (page 289).

MCM log file output

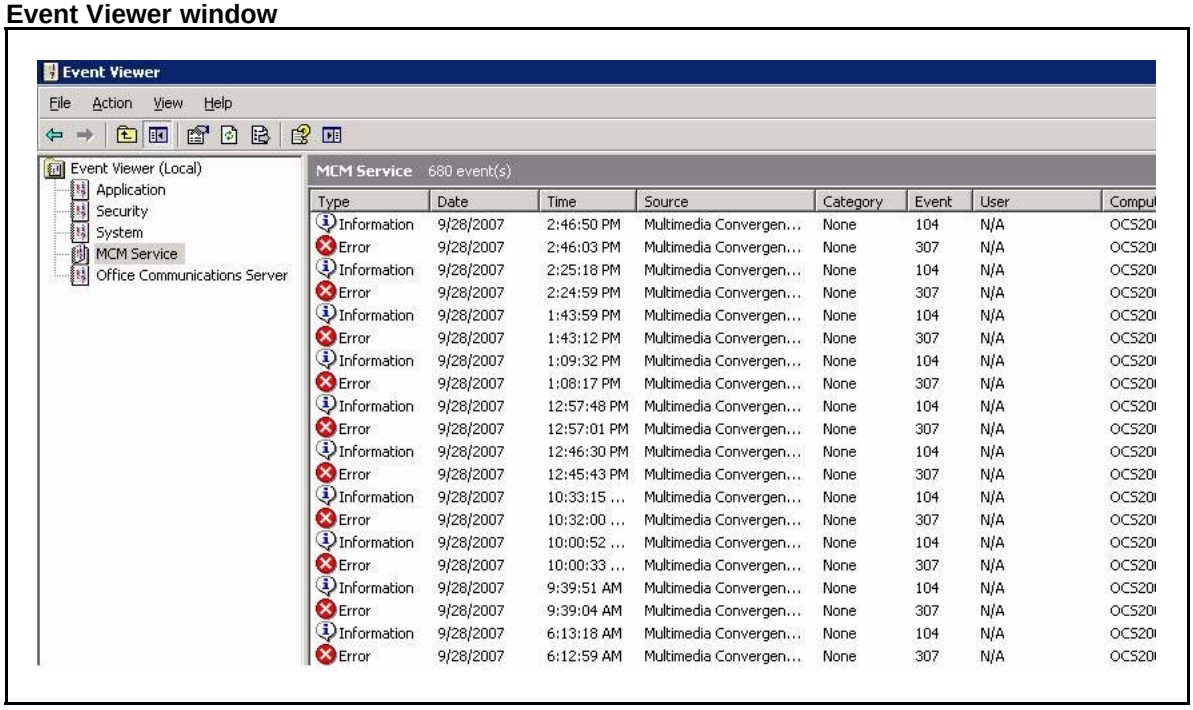
The following shows a snippet from the log output file:

```
12/14/2007 11:11:37 AM: 3.0.1.76:  Debug:  OnCustomCommand
:  got command:
update config data
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  ConfigurationDa
ta:
ReadConfigFile:  Invalid secondary NRS address:  0.0.0.0
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  ConfigurationDa
ta:
ReadConfigFile:  Invalid LDAP server IP address:  0.0.0.0
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  ServerEventHand
ler:  got Event #2
12/14/2007 11:11:38 AM: 3.0.1.76:  SIP and Debug:
NRSPolling:
sendPolling:  request sent to the Primary NRS
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  AD Cache:
turning off
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  AD Cache:  it
has been turned off
12/14/2007 11:11:38 AM: 3.0.1.76:  Debug:  ServerEventHand
ler:  got Event #3
12/14/2007 11:11:38 AM: 3.0.1.76:  SIP and Debug:
NRSPolling:  pollingResponseHandler
SIP/2.0 200
via:  SIP/2.0/TCP 47.11.56.54:4616;branch=z9hG4bK-422726
df-8d69b1-2ac0;received=47.11.56.54
from:  <sip:MCM@ocs2007a.corp.nortel.com>;tag=a7fdb8be-c
10b-44ef-9bf8-b9f6233cecb5
to:  <sip:MCM@ocs2007a.corp.nortel.com>;tag=18892
call-id:  0000000-00000000-0000-00000000-000002-0000
cseq:  6 REGISTER
contact:  < sip:MCM@ocs2007a.corp.nortel.com:5060>;expir
es=300;maddr=47.11.56.54;Transport=TCP
expires:  300
content-length:  0
```

MCM Event log

MCM Exceptions and failures are reported in System Event Log. The following shows an example event log:

Figure 128
Event Viewer window



Resetting MCM debug trace

Use the following procedures to reset the MCM debug trace.

Step	Action
1	On the MCM interface, select **Tools** and then choose **Logs** from the menu.
2	Go to **Log Level** and choose **None**.
3	Delete the MCM.log file from the directory where MCM is installed.

--End--

OCS logs

Use the following procedures to activate an OCS log.

Activating OCS logs

Step	Action
1	Right-click the OCS pool and select **Logging Tool** and then choose **New Debug Session**.

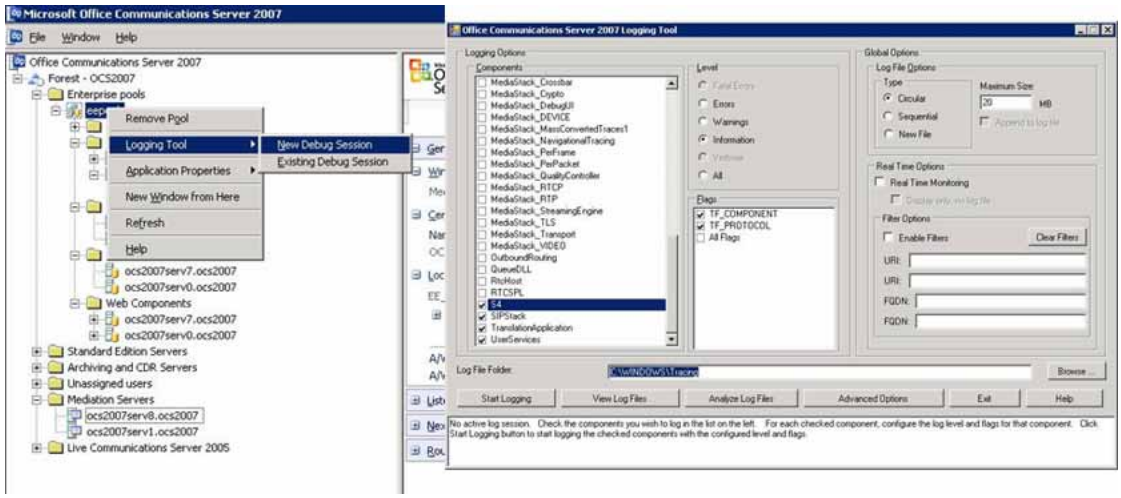
2 In the OCS 2007 Logging Tool window, specify the Components to trace, Severity level, and other log file options. See example Figure 129 "OCS debugging tool" (page 290).

3 Click the **Start Logging** button.

4 To view the log file, click the **Analyze Log Files** button. The log file is stored as a .txt file in c:\WINDOWS\Tracing folder.

--End--

Figure 129
OCS debugging tool



Enabling OC logs

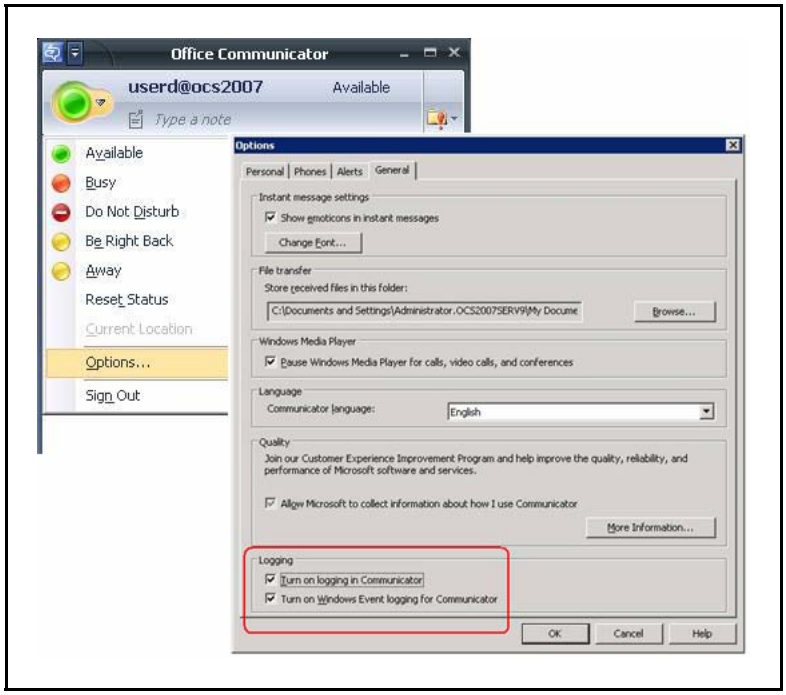
The following procedures describe how to enable logs for OC client. The tracing log folder is stored in the user Documents and Settings sub folder with the .uccplog extension.

Step	Action
1	From the OC client, select the **Options** menu.
2	Choose the **General** tab.
3	Select the **Turn on logging in Communicator** and the **Turn on Windows Event Logging for Communicator** check boxes. See Figure 130 "Turn on Logging and Windows Event Logging" (page 291).

4 Click OK.

--End--

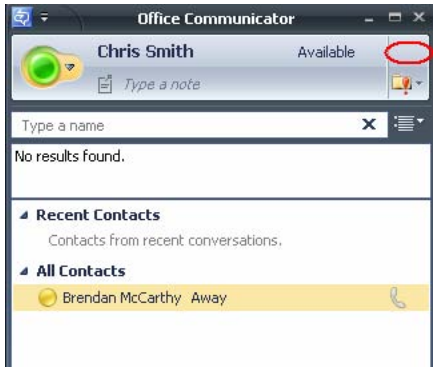
Figure 130
Turn on Logging and Windows Event Logging



OC client start-up debugging

To determine if there is a PBX connection, a handset icon will be present in the upper right of the OC client window. The example in Figure 131 "No PBX connection for OC client" (page 292) shows an OC client window where the handset icon is not present. For more information about troubleshooting an OC client registration, see “OC client not registered” (page 279).

Figure 131
No PBX connection for OC client



Case checklists

Use the following checklists prior to opening a case to ensure that all relevant information is collected:

Table 58
Signaling Server information

	Check
The patches list installed on the Signaling Server: At the prompt type: mdp issp	
The configuration on the Signaling Server: • cd /u/config • copy config.ini	
Have you ssh to the Signaling Server and logged on to Nortel account? At the prompt type: • SIPCTIShow tSSG	

Table 59
Call Server information

	Check
Provide the patches list installed on the Call Server • LD 22 • issp	
Capture the print out for the user DN in LD 11	
Capture the print out for the TN configured for this DN (do both for all TNs, including the TLSV)	
Capture the DSC configuration for the TLSV (configured for the Hot P 1)	
In LD 48, perform the command stat elan	
Provide the print out for the SIP Route and all related RLI/DMI	

Table 60
NRS configuration information

	Check
NRS configuration	
Print capture of the Signaling Server endpoint configuration	
Print capture of the MCM endpoint configuration	
Print capture of the Routing Entries for the MCM endpoint	

Table 61
MCM configuration information

	Check
Send the MCM.ini file	

Table 62
OCS configuration information

	Check
The FQDN name of the Proxy server and the IP address	
The FQDN name of the Pool and the IP name	
The VIP of the Load Balancer	
On the Proxy Server capture Routing and for each route, Edit it and capture the screen	
On the Pool, capture **Routing** for each route, Edit it and get a screen capture	
On the Proxy Server, get a screen capture of **Host Authorization**	
On the Pool, get a screen capture of **Host Authorization**	
Front End server Properties, General tab, Mutual TLS/TLS row, Edit	
Front End server Properties, Security tab	
OCS Proxy Properties, General tab, Mutual TLS/TLS row, Edit	
OCS Proxy Properties, Security tab	

Table 63
Active Directory configuration information

	Check
Print Capture of the OCS user for the General Tab	
Print Capture of the OCS user for the Office Communications Server	
Print Capture of the OCS user for the Office Communication, Advanced Settings	

Table 64
Tracing information

	Check
An example AML trace on the Call Server (if it is a problem regarding the RCC feature not able to control the telephone	
An example Signaling Server trace: SIPCallTrace (For problem related to SIP Gateway)	
An example Incoming and Outgoing SIP registration messages: SIPGwRegTrace	
An example Signaling Server trace: SIPCTITrace (For problem related to SIP CTI)	
An example MCM.log with the log level = SIP + Debug for the failed call scenario (to reset the trace: put the trace level to none, delete the MCM.log file and put back the level to Debug)	

Appendix
Call Flow and protocol details

This section contains information about call flows.

Navigation

Overview

The Converged Office feature provides interworking between Nortel and Microsoft products. It addresses the market need of our customers who want to use Microsoft client software for their multimedia needs while continuing to use the Business Grade Telephony of the Nortel IP PBX.

The software component introduced to implement this functionality is the TR/87 Front End application that resides on the Signaling Server.

The same TR/87 FE that supports the Office Communicator client also serves as a core component of the SIP Contact Center architecture.

From the perspective of the TR/87 FE, all client types are transparent, whether Office Communicator, a TR/87 session initiated by the Contact Center Manager server (CCMS), or some other SIP UA.

Within the scope of Communication Server 1000 TR/87 supported services and events noted in this document, all operations performed on the telephone are directly reflected in the client and vice versa. Similarly, all phone restrictions applicable to a physical TN also apply to the soft client that is issuing commands on behalf of a controlled DN.

Message sequence

TR/87(4) is an ECMA Technical Report that describes the use of SIP as a transport of service requests and events defined by the ECMA-269(5) specification as XML bodies within SIP messages. The ECMA-323(6) specification defines the XML format of ECMA-269 services and events.

The Front End (FE) application conforms to the minimum subset of the TR/87 specification defined for Office Communications Server 2007 interworking and those components necessary to support the next generation SIP Contact Center requirements.

Figure 132 "Message sequence diagram - CSTA Session Establishment and Monitor Start" (page 296) shows the expected message flow for establishing and monitoring a CSTA session as defined by TR/87.

Figure 132
Message sequence diagram - CSTA Session Establishment and Monitor Start

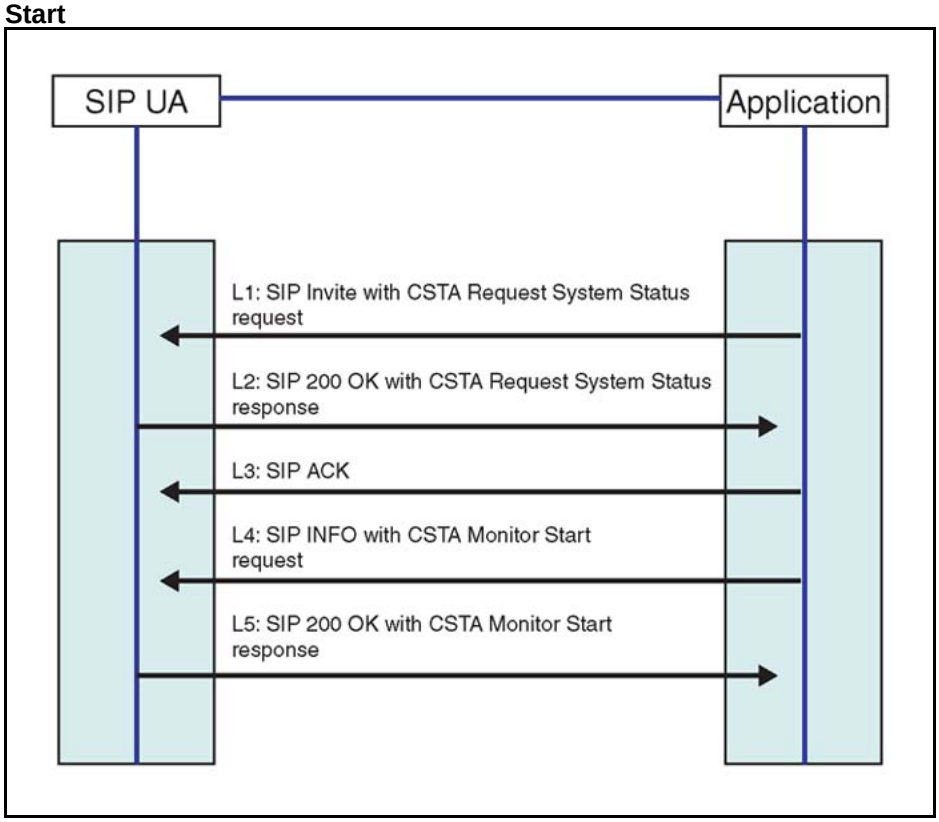


Figure 133 "SIP INFO message with ECMA-323 content" (page 297) is an example of a SIP INFO message with ECMA-323 content.

Figure 133
SIP INFO message with ECMA-323 content

```
INFO fe1_cs1000@lcs2005s.corp.nortel.com
Via: SIP/2.0/TCP 157.56.66.156:16714
Max-Forwards: 70
From:<sip:alice@microsoft.com>;tag=0d9280080ada4a1ea504f7d78d434336;epid=5fc88
0096d
To:<sip:fe1_cs1000@lcs2005s.corp.nortel.com>;tag=3f181801fc9d4fabb27ef7d8
9bd28f9f
Call-ID: fdbcb6a6184a4e92a5f001865f84a2c6@157.56.66.156
CSeq: 2 INFO
Contact: <sip:alice@microsoft.com:16714
Contact:<sip:alice@microsoft.com:9609;maddr=47.130.16.136;transport=tcp>;proxy
=replace
User-Agent: RTC/1.2
Content-Type: application/csta+xml
Content-Disposition: signal; handling=required
Content-Length: 189
<?xml version="1.0" encoding="UTF-8"?>
<MakeCall
xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3.">
<callingDevice>tel:+14257777777</callingDevice>
<calledDirectoryNumber>tel:65000;phone
context=microsoft.com</calledDirectoryNumber>
</MakeCall>
```

Call flow

This section illustrates the call flow sequence for the Telephony Gateway and Services and Remote Call Control with Mediation Server present.

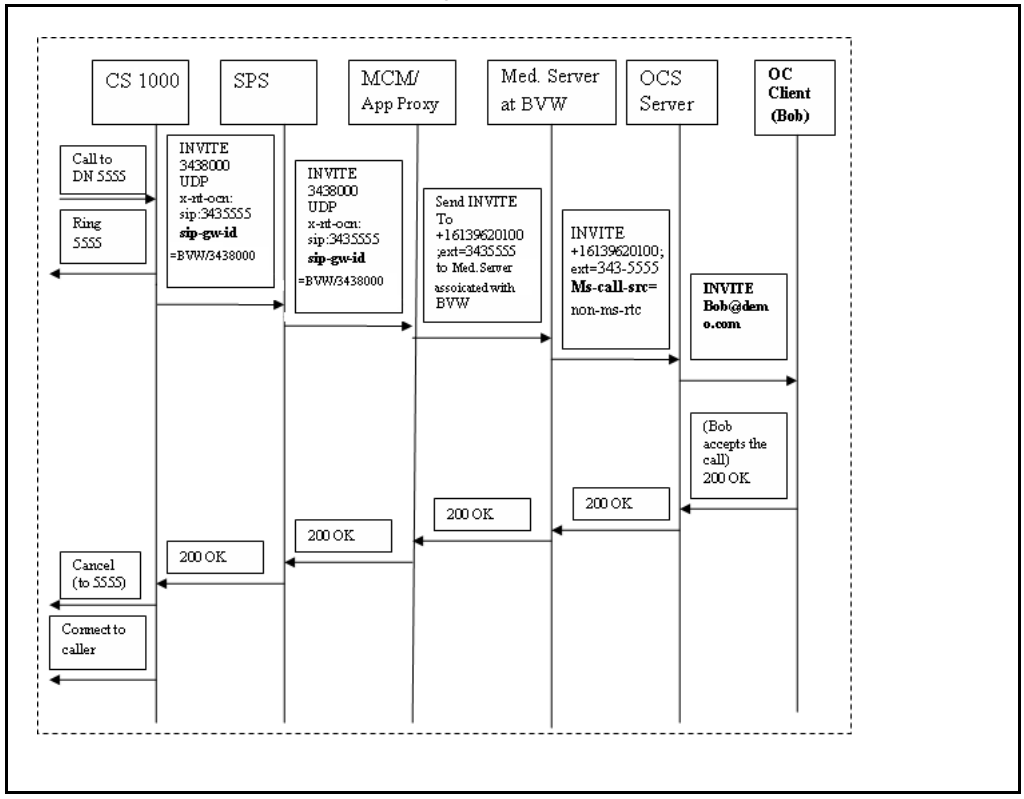
Telephony Gateway and Services call flow

This section explores dual forking call flows in different scenarios when Mediation Server is present.

This scenario as illustrated in Figure 134 "Inbound call to OC client with SPS, OC client answers" (page 298) depicts a configuration of a UDP dialing plan on the Communication Server 1000 and the presence of an SPS component on the network. A Communication Server 1000 user dials 5555 which is the phone belonging to user Bob in the demo.com domain. Bob accepts the call from his OC client.

Note: This scenario would also apply if the inbound call originated from the PSTN.

Figure 134
Inbound call to OC client with SPS, OC client answers



Incoming calls to OC 2007 can originate directly from a phone behind the Communication Server 1000 where the request URI represents the destination.

Incoming calls can also come from a TLSV, where the Request URI is a service DN used to route the call to OCS 2007, and the actual destination is determined by a special header (x-nt-ocn) that contains the destination DN. MCM checks for the x-nt-ocn and routes the call accordingly.

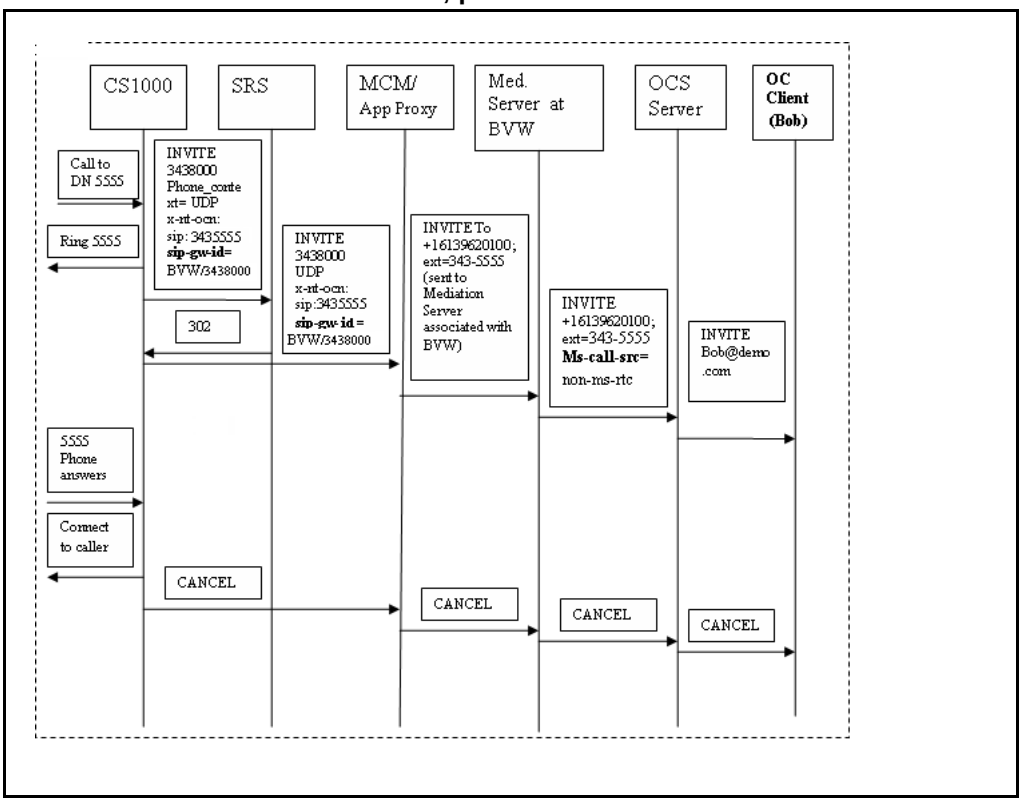
Telephony Services (TLSV) configuration provides additional Office Communicator features such as forwarding to voice mail, and so on. Configuration of TLSV is performed through station administration tools.

This scenario as illustrated in Figure 135 "Inbound call to OC client with SRS, phone answers" (page 299) depicts the presence of an SRS component on the network (instead of SPS).

For example, A Communication Server 1000 user dials 5555 which is the phone belonging to user Bob in the demo.com domain. Bob accepts the call from his phone (instead of the OC client).

ATTENTION
This scenario would also apply if the inbound call originated from the PSTN.

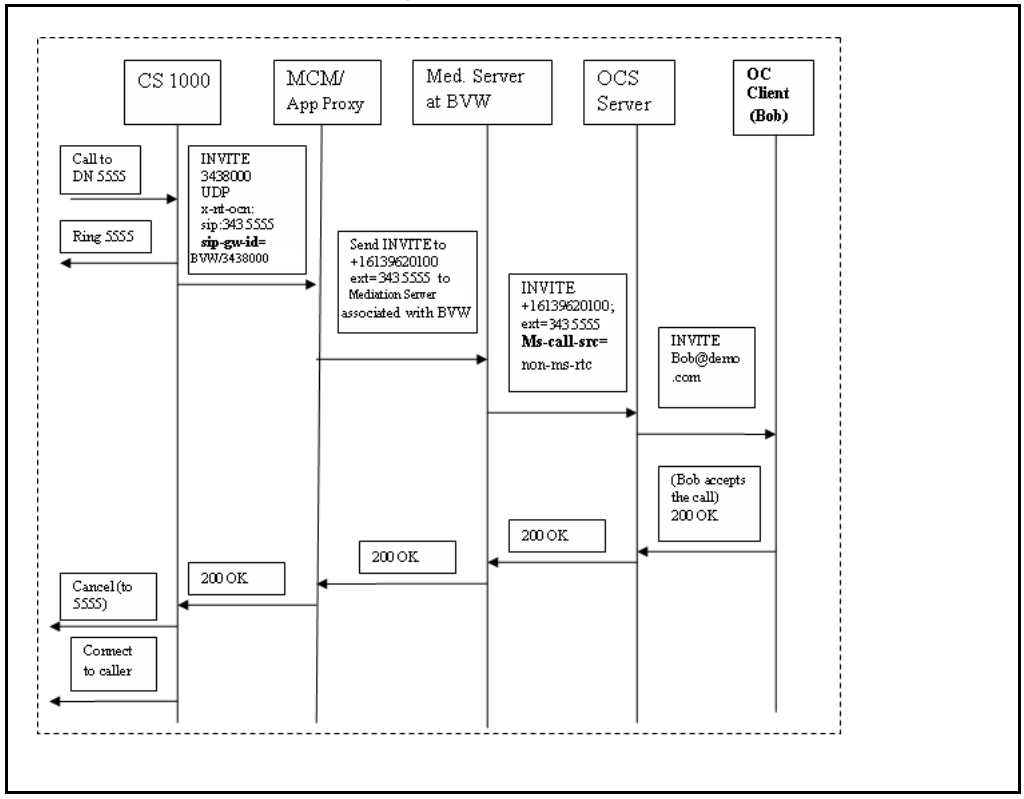
Figure 135
Inbound call to OC client with SRS, phone answers



The next scenario as illustrated in Figure 136 "Direct inbound call to OC client, OC client answers" (page 300) depicts a limited deployment configuration where the MCM is pointing directly to the Communication Server 1000. The deployment of SPS or SRS are not present. A Communication Server 1000 user dials 5555 which is the phone belonging to user Bob in the demo.com domain. Bob accepts the call from his OC client.

ATTENTION
This scenario would also apply if the inbound call originated from the PSTN.

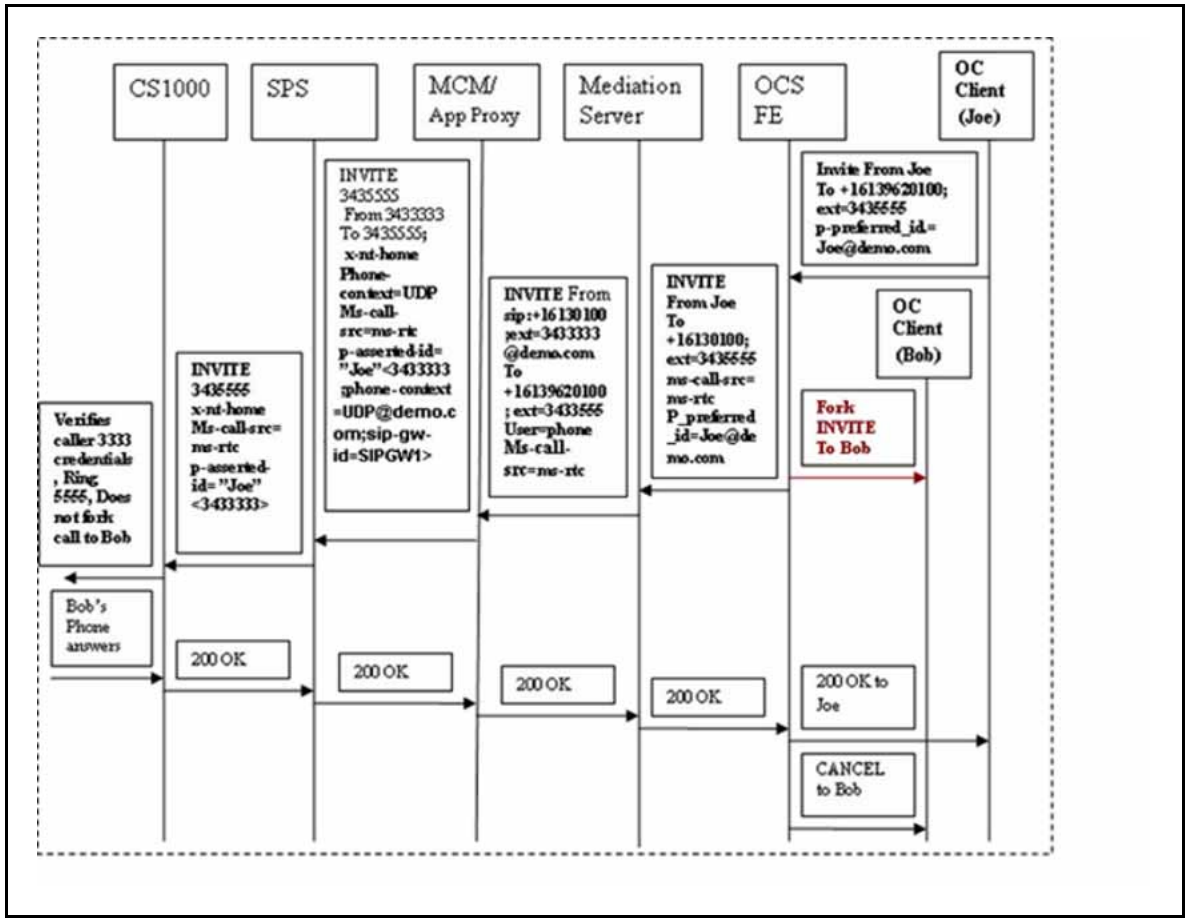
Figure 136
Direct inbound call to OC client, OC client answers



This scenario as illustrated in Figure 137 "Outbound call from OC client to another client, phone answers" (page 301) depicts the prevention of dual forking in a configuration where both users are registered to the same Communication Server 1000 with the presence of SPS. Joe calls Bob from his OC client. Bob accepts the call from his phone.

ATTENTION
In this call flow scenario, homing operation is performed on the Communication Server 1000 to validate the caller's (Joe) permissions before proceeding with the call.

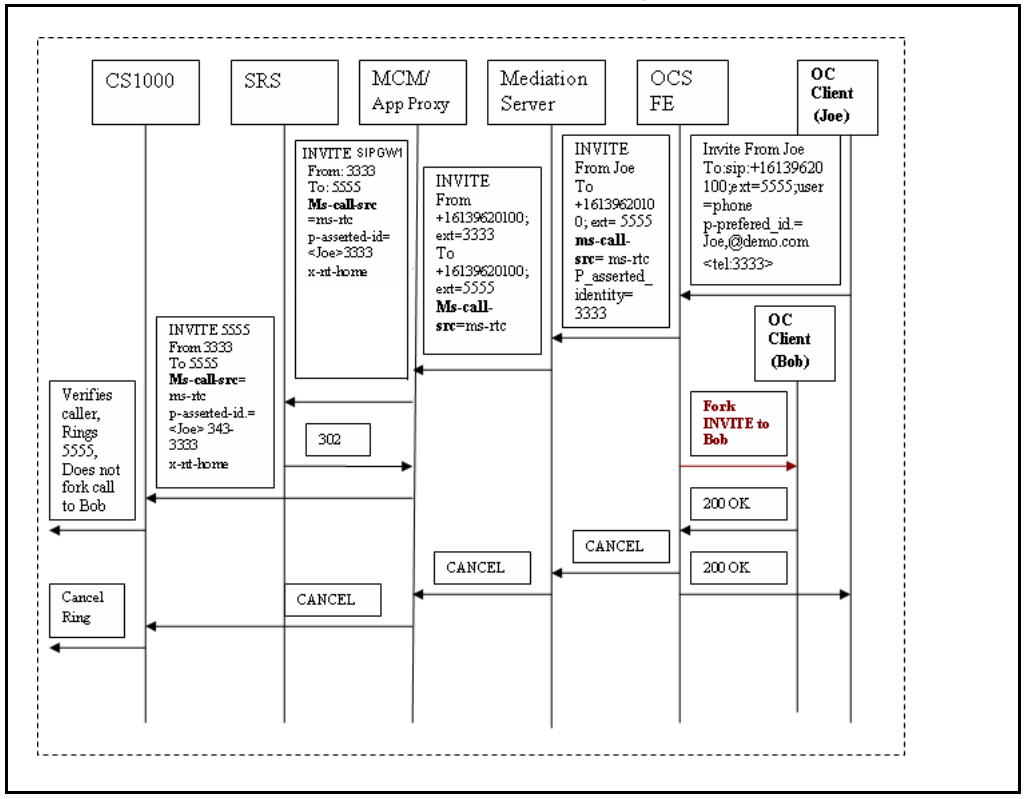
Figure 137
Outbound call from OC client to another client, phone answers



This scenario as illustrated in Figure 138 "Outbound call from OC client to another OC client, OC client answers" (page 302) depicts a configuration with a CDP dialing plan and the presence of the SRS component on the network. Joe calls Bob from his OC client. Bob accepts the call from his OC client.

ATTENTION
For the CDP dialing plan to work, the entire network must be configured with CDP. Therefore, it can only be deployed on small networks.

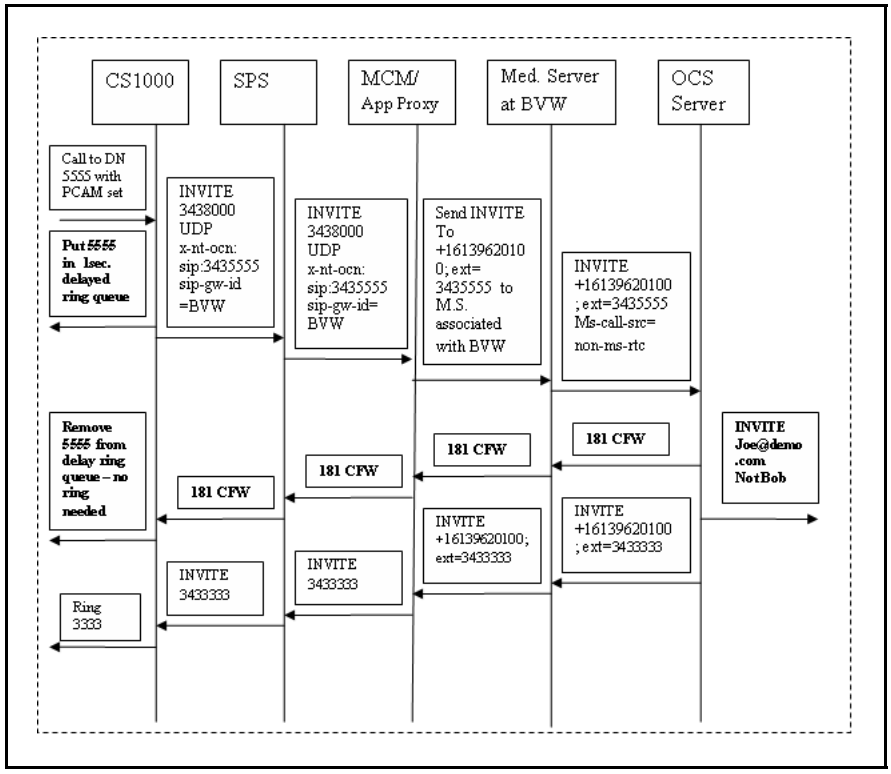
Figure 138
Outbound call from OC client to another OC client, OC client answers



Call Forward by OC client

This scenario depicts a situation where the Communication Server 1000 phone dials the phone number of an OC client Bob and is forwarded to another client Joe. Bob's twin phone number is x5555 and Joe's number is X3333.

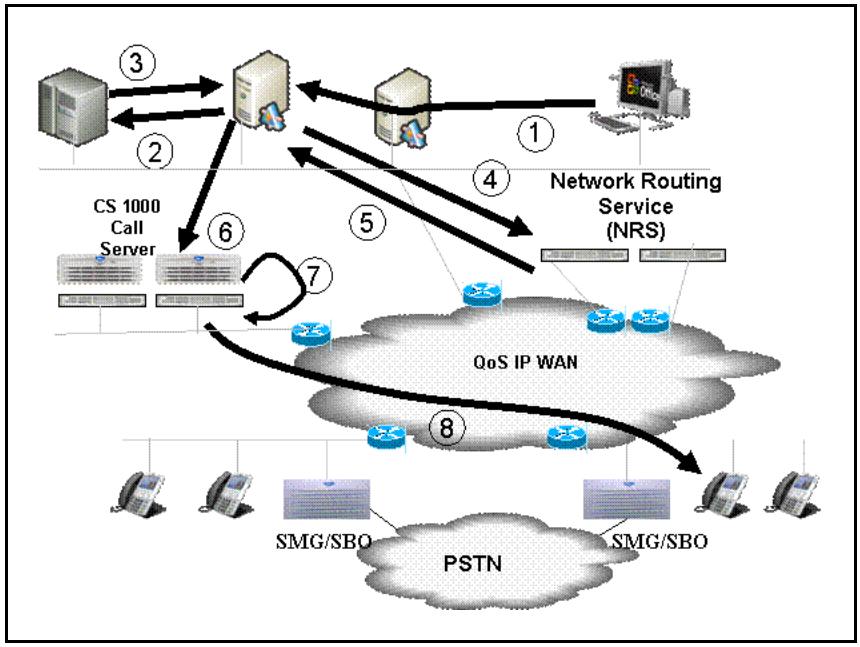
Figure 139
Call Forward call flow by OC client



Outgoing OC client SIP Gateway call to on-net private number using IP WAN

The following figure depicts the outgoing OC client SIP Gateway call to on-net private number using IP WAN.

Figure 140
Outgoing OC client SIP Gateway call to on-net private number using IP WAN



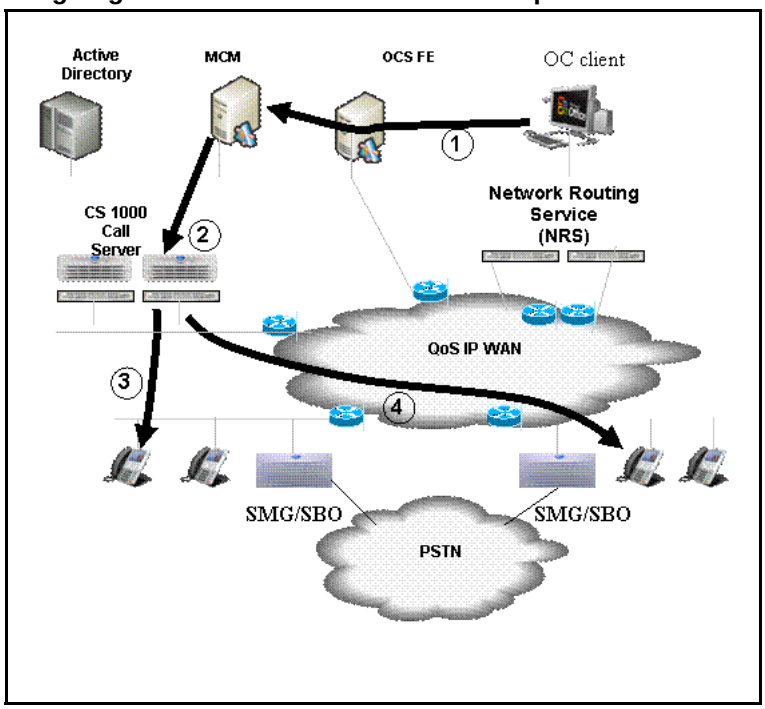
Within an outgoing OC client SIP Gateway call to on-net private number using IP WAN scenario, the following occurs:

1. The OC client user dials a private number.
2. The Multimedia Convergence Manager (MCM) queries the Active Directory for the phone number of the OC client user.
3. The Active Directory responds with the matching number.
4. The MCM sends the caller number to the Network Routing Service (NRS).
5. The NRS responds with the matching Communication Server 1000 associated with the caller.
6. The call is sent to Communication Server 1000 used by the caller.
7. The zone prefix is inserted, based on numbering zone configuration, for all dialed digits from the OC SIP Gateway and Services. Introduction of the zone prefix (PREF) avoids the necessity for the pretranslation table configuration.
8. The Call Server determines the availability of adequate bandwidth and alerts the appropriate stations. The Calling Line Identification (CLID) is changed from a 7 digit to 3-5 digit local DN and Name Display for intrazone calls. For interzone calls, the CLID is 7-digits.

Outgoing SIP CTI OC client call to on-net private number using IP WAN

The following figure depicts the SIP CTI client call to on-net private number using IP WAN.

Figure 141
Outgoing SIP CTI OC client call to on-net private number using IP WAN



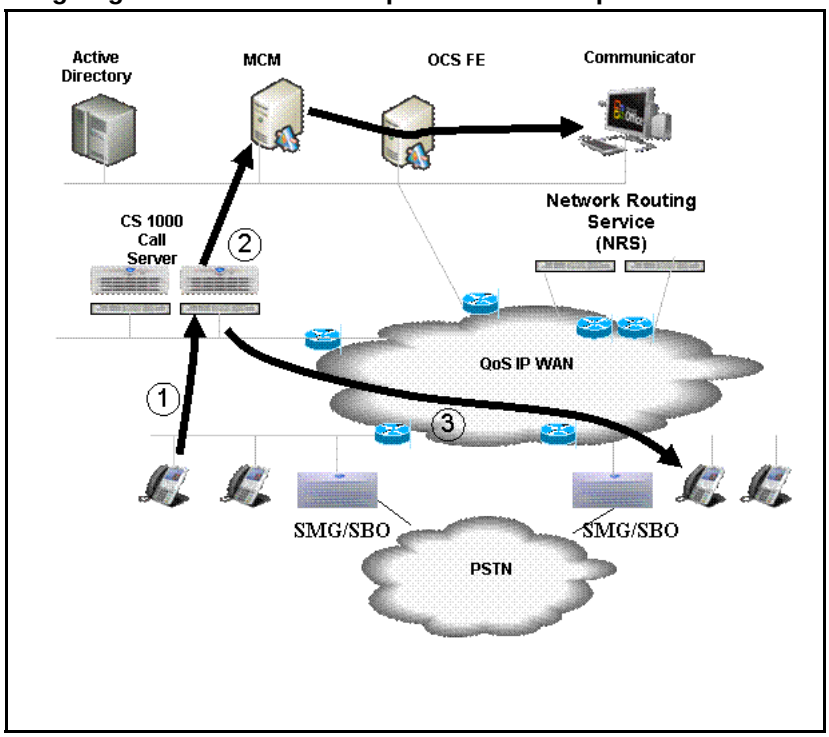
Within an outgoing OC client SIP Gateway call to on-net private number using IP WAN scenario, the following occurs:

1. The OC client user dials a private number.
2. The SIP CTI message is sent to the CS 1000.
3. The zone prefix (PREF) is introduced to avoid need for pretranslation table configuration. Zone prefix is inserted based on numbering zone configuration for all dialed digits from the OC using Remote Call Control of CS 1000 phones. Call Server takes controlled phone off-hook and initiates call.
4. Call Server determines that adequate bandwidth is available and alerts appropriate stations. CLID is changed from 7-digits to 3-5 digits local DN and Name Display for intrazone calls. For interzone calls CLID is 7-digits.

Outgoing SIP CTI call from IP phone to on-net private number using IP WAN

The following figure depicts the outgoing SIP CTI call from IP phone to on-net private number using IP WAN.

Figure 142
Outgoing SIP CTI call from IP phone to on-net private number using IP WAN



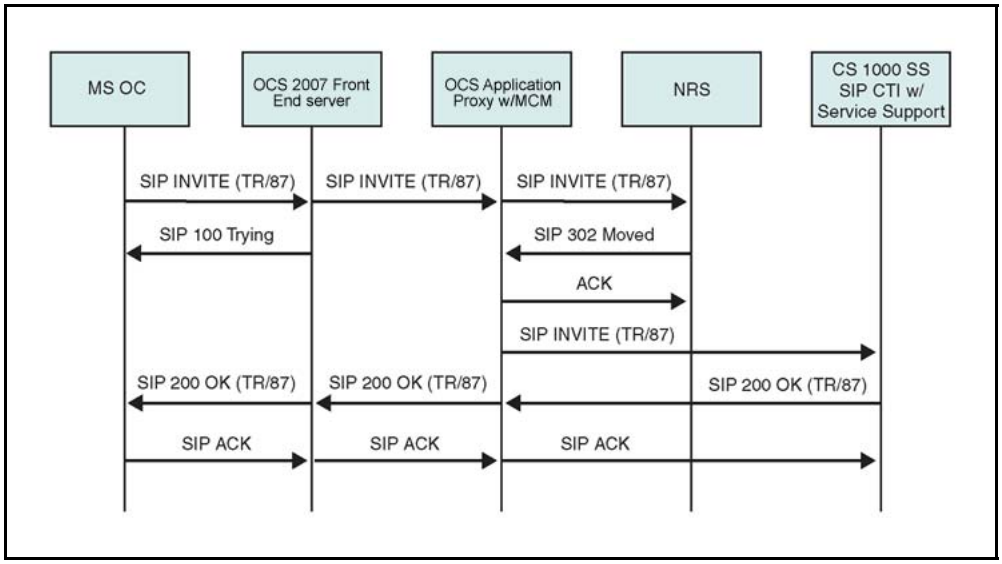
Within an outgoing SIP CTI call from IP phone to on-net private number using IP WAN scenario, the following occurs:

1. The IP phone user dials a private number.
2. Zone prefix (PREF) is introduced to avoid the need for a pretranslation table configuration. Zone prefix is inserted base don the numbering zone configuration for all dialed digits.
3. Call Server determines that adequate bandwidth is available and alerts the appropriate stations. CLID is changed from 7-digits to 3-5 digits local DN and Name Display for intrazone calls, based upon length of zone prefix (PREF). For interzone calls CLID is 7-digits.

Remote Call Control Call Flow

Figure 143 "Remote Call Control Session Establishment through SRS" (page 307) illustrates the Remote Call Control Session Establishment through SRS.

Figure 143
Remote Call Control Session Establishment through SRS



Supported features

Table 65
SIP CTI supported features

Feature	Supported by CS 1000 TR/87 FE	Supported by Office Communicator 2007
Call Control Events		
17.2.3 - Conference	X	X
17.2.4 - Connection Cleared	X	X
17.2.5 - Delivered	X	X
17.2.7 - Diverted	X	X
17.2.8 - Established	X	X
17.2.9 - Failed	X	X
17.2.10 - Held	X	X
17.2.14 - Originated	X	X
17.2.16 - Retrieved	X	X
17.2.18 - Transferred	X	X
Call Associated Services		
18.1.4 - Generate Digits	X	X

Table 65
SIP CTI supported features (cont'd.)

Feature	Supported by CS 1000 TR/87 FE	Supported by Office Communicator 2007
Call Associated Events		
18.2.5 - Service Completion Failure	X	X
Logical Device Features		
22.1.9 - Get Do Not Disturb	X	
22.1.10 - Get Forwarding	X	X
22.1.17 - Set Do Not Disturb		
22.1.18 - Set Forwarding	X	X
Logical Device Feature Event		
22.2.12 - Do Not Disturb	X	
22.2.13 - Forwarding	X	X
Capability Exchange Services		
13.1.1 - Get CSTA Features	X	X
System Services		
14.2.1 - Request System Status	X	X
Monitoring Services		
15.1.2 - Monitor Start	X	X
15.1.3 - Monitor Stop	X	X
Call Control Services		
17.1.2 - Alternate Call		X
17.1.3 - Answer Call	X	X
17.1.8 - Clear Connection	X	X
17.1.9 - Conference Call	X	
17.1.10 - Consultation Call	X	X

Table 65
SIP CTI supported features (cont'd.)

Feature	Supported by CS 1000 TR/87 FE	Supported by Office Communicator 2007
17.1.11 - Deflect Call	X	X
17.1.15 - Hold Call	X	X
17.1.18 - Make Call	X	X
17.1.21 - Reconnect Call		X
17.1.22 - Retrieve Call	X	X
17.1.25 - Single Step Transfer Call	X	X
17.1.26 - Transfer Call	X	X

Appendix Configuration Examples

As described in the Planning and Engineering chapter, small, medium, and large networks require different editions of Office Communications Server (OCS) 2007. This appendix contains configuration examples for both Standard Edition and Enterprise Editions of OCS 2007.

Navigation

Standard Edition

This section provides information about how to configure and troubleshoot the Converged Office solution running the Standard Edition OCS 2007. This sample configuration is for a small network deployment.

Setting up the lab

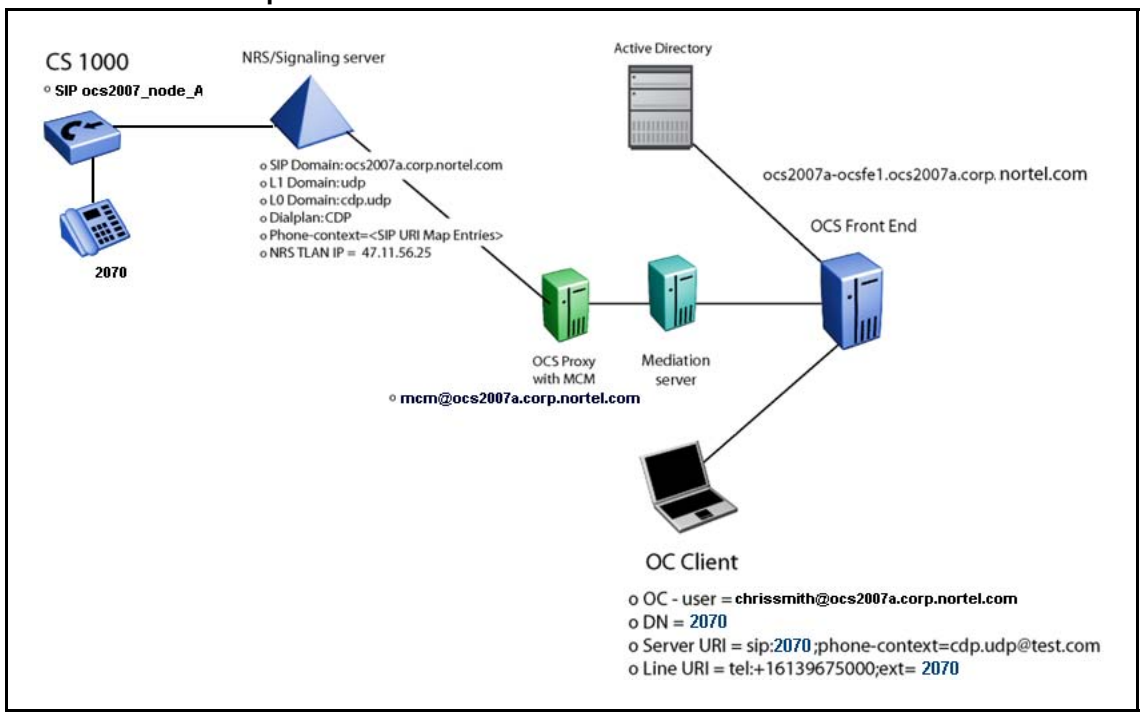
Use the following procedures to ensure the lab is set up correctly.

Step	Action
1	Confirm that the CS 1000 server is version 6.0.
2	Confirm that the Signaling Server is version 6.0 with the required patches as identified in the Product Bulletin.
3	Confirm that you have the OCS 2007 Standard Edition server.
4	Confirm that you have MCM 4.x.

--End--

Figure 144 "Overview of lab setup" (page 312) illustrates how to set up a lab for Converged Office.

Figure 144
Overview of lab setup



Collecting required data

Collect the required data listed in the following three tables before you begin to configure the Converged Office solution. The information entered here can be used to verify configuration settings later on.

Table 66
Microsoft Active Directory

Required information	Record your information	For example
User SIP URI		chrissmith@ocs2007a.corp.nortel.com
Server URI		sip:2070;phone-context=cdp.udp@test.com
Line URI		tel:+16139675000;ext=2070

Table 67
Network Routing Service (NRS)

Required information	Record your information	For example
IP-address Primary SPS		47.11.56.25
IP-address Secondary SPS		Not used
Node IP-address		47.11.56.24
MCM endpoint name		mcm@ocs2007a.corp.nortel.com
Communication Server 1000 SIP gateway endpoint name		ocs2007_node_A@ocs2007a.corp.nortel.com
Routing Entry for UEXT		CDP: 888-MCM CDP: 20 and 21 > OCS2007_node A
Service domain		ocs2007a.corp.nortel.com
Level 1 domain		udp
Level 0 domain		cdp.udp

Table 68
Element Manager for Signaling Server

Required information	Record your information	For example
Communication Server 1000 SIP gateway endpoint name		ocs2007_node_A@ocs2007a.corp.nortel.com
SIP Domain name		ocs2007a.corp.nortel.com
SIP URI map, Private/UDP domain name		udp
SIP URI map, Private/CDP domain name		cdp.udp
SIP CTI Service, Service enabled		Yes
SIP CTI Service, Customer Number		0

SIP CTI Service, International Calls As National		Yes
SIP CTI Service, National Prefix		0
SIP CTI Service, International Prefix		00
SIP CTI Service, Dialing Plan		cdp
SIP CTI Service, Calling Device URI Format		sip:2070;phone-context=cdp.udp@test.com
SIP CTI Service, Country Code		33
SIP CTI Service, National/ Number of digits to strip		1

Table 69
MCM

Required Information	Record your information	For example
Registration ID		mcm@ocs2007a.corp.nortel.com
Called Phone Context		cdp.udp

Checking the Call Server configuration

Use the following procedure to check the configuration of the Call Server.

Step	Action
1	Check to make sure the version of the Communication Server 1000 Call Server is Release 6.0.
2	Check the Product Bulletin.
3	In LD 22, confirm that AST, TLSV, and **SIP CTI TR87** licenses are available.

Table 70
LD 22––check for licenses

Prompt	Response	Description
REQ	slt	

Screen output:

```
ANALOGUE TELEPHONES 32767 LEFT 32767 USED 0
CLASS TELEPHONES 32767 LEFT 32767 USED 0
DIGITAL TELEPHONES 32767 LEFT 32767 USED 0
DECT USERS 32767 LEFT 32767 USED 0
IP USERS 32767 LEFT 32756 USED 11
BASIC IP USERS 32767 LEFT 32767 USED 0
TEMPORARY IP USERS 32767 LEFT 32767 USED 0
DECT VISITOR USER 10000 LEFT 10000 USED 0
ACD AGENTS 32767 LEFT 32767 USED 0
MOBILE EXTENSIONS 32767 LEFT 32767 USED 0
TELEPHONY SERVICES 32767 LEFT 32761 USED 6
CONVERGED MOBILE USERS 32767 LEFT 32767 USED 0
NORTEL SIP LINES 32767 LEFT 32767 USED 0
THIRD PARTY SIP LINES 32767 LEFT 32767 USED 0
PCA 32767 LEFT 32762 USED 5

AST 32767 LEFT 32756 USED 11
ITG ISDN TRUNKS 32767 LEFT 32767 USED 0
H.323 ACCESS PORTS 32767 LEFT 32767 USED 0
AST 32767 LEFT 32761 USED 6
SIP CONVERGED DESKTOPS 32767 LEFT 32767 USED 0
SIP CTI TR87 32767 LEFT 32760 USED 7
SIP ACCESS PORTS 32767 LEFT 32753 USED 14
RAN CON 32767 LEFT 32767 USED 0
MUS CON 32767 LEFT 32767 USED 0
TNS 32767 LEFT 32639 USED 128
ACDN 24000 LEFT 24000 USED 0
AML 16 LEFT 14 USED 2 IDLE_SET_DISPLAY NORTEL
LTID 32760 LEFT 32760 USED 0
RAN RTE 512 LEFT 512 USED 0
ATTENDANT CONSOLES 32767 LEFT 32767 USED 0
BRI DSL 10000 LEFT 10000 USED 0
MPH DSL 100 LEFT 100 USED 0
DATA PORTS 32767 LEFT 32767 USED 0
PHANTOM PORTS 32767 LEFT 32767 USED 0
TRADITIONAL TRUNKS 32767 LEFT 32767 USED 0
DCH 255 LEFT 254 USED 1
```

4 Also in LD 22, confirm that the MS_CONV and TLSV package is present (this package is required).

Table 71
LD 22–MS_CONV and TLSV packages

Prompt	Response	Description
REQ	prt	
TYPE	pkg 408	
TYPE	pkg 413	

Screen output:

```
MS_CONV 408
```

```
TLSV 413
```

5 Ensure that the VSID and the ELAN ID are **greater than or equal to 32** and that the SECU parameter is configured to **YES** for ELAN and for VAS configuration.

Table 72
LD 22–Check VSID and ELAN ID configuration

Prompt	Response	Description
REQ	prt	
TYPE	vas	

Screen output:

```
ELAN 032
SECU YES
INTL 0001

MCNT 9999
```

6 In LD 20, confirm that STRI/STRO is **WNK** for SIP Trunk configuration.

ATTENTION
The screen output shown here may differ, depending on the setup used.

Table 73
LD 20–SIP Trunk configuration

Prompt	Response	Description
REQ	prt	
TYPE	tnb	
TN	156 0 0 0	
DATE	<enter>	
PAGE	<enter>	
DES	<enter>	

Screen output:

```
DES SIP
TN 156 0 00 00 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 000
TRK ANLG
NCOS 0
RTMB 62 1
```

```
CHID 1
TGAR 0
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0
CLS UNR DTN WTA LPR APN THFD XREP P10 NTC
TKID
AACR NO

DATE 5 DEC 2006
```

7 In LD 21, check that NCNA and NCRD are configured to **YES** and that SIGO is **ESN5** in the SIP Route Configuration. For example:

Table 74
LD 21–SIP Route configuration

Prompt	Response	Description
REQ	prt	
TYPE	rdb	
CUST	0	
ROUT	62	

Screen output:

```
TYPE RDB
CUST 00
ROUT 62
DES SIP
TKTP TIE
NPID_TBL_NUM 0
ESN NO
RPA NO
CNVT NO
SAT NO
RCLS EXT
VTRK YES
ZONE 000
PCID SIP
CRID YES
NODE 81
DTRK NO
ISDN YES
MODE ISLD
DCH 63
IFC SL1
PNI 00001
NCNA YES
NCRD YES
```

```
TRO YES
FALT NO
CTYP UKWN
INAC YES
ISAR NO
DAPC NO
PTYP ATT
...
DEXT NO
ANTK
SIGO ESN5
MFC NO

...
```

8 For TN configuration in LD 20, confirm configuration of **AST, TR87A, TLSV, and CDMR Class of Service**. Confirm configuration of **MARP** for the telephone.

ATTENTION
The screen output shown here may differ depending on the setup used.

Table 75
LD 20–TN configuration

Prompt	Response	Description
REQ	prt	
TYPE	dnb	
CUST	0	
DN	2070	
DATE	<enter>	
PAGE	<enter>	
DES	<enter>	

Screen output:

```
DN 2070
CPND
CPND_LANG ROMAN
XPLN 16
DISPLAY_FMT FIRST,LAST
TYPE SL1
TN 100 0 03 04 V KEY 00 MARP DES DLOCS2 3 DEC 2007
(2004P2)
TN 100 0 03 05 V KEY 00 DES OCS 16 APR 2008
(UEXT)
NACT
```

Table 76
LD 20

Prompt	Response	Description
REQ	prt	
TYPE	tnb	
TN	152 0 0 14	
DATE	<enter>	
PAGE	<enter>	
DES	<enter>	

Screen output:

```
DES CDLCS
TN 152 0 00 14 VIRTUAL
TYPE I2004
CDEN 8D
CTYP XDLC
CUST 0
ZONE 000
FDN
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST 0
SCPW 2070
SFLT NO
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD DSX VMD CMSD SLKD CCSA-CSI SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXD ARHD FITD CLTD ASCD
CPFA CPTA HSPD ABDD CFHD FICD NAID BUZZ
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD
NROD
DRDD EXR0
USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC
DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87A KEM2
CPND_LANG ENG
BFTN 152 0 01 00
HUNT
PLEV 02
```

```
CSDN
AST 00

IAPG 0
```

9 Check LD 20 to confirm that UEXT with TLSV subtype is activated. If not, configure LD 15 to PCA **ON** This allows the incoming call to twin the UEXT and make the SIP Gateway call work. Use LD 11 to configure each user with UEXT.

Table 77
LD 20–Confirm UEXT is activated

Prompt	Response	Description
REQ	prt	
TYPE	FTR_DATA	
CUST	0	

Screen output

```
...
PCA ON
...
```

Table 78
LD 11–Confirm configuration of UEXT with TLSV subtype for SIP Gateway

Prompt	Response	Description
REQ	prt	
TYPE	UEXT	
TN	96 0 8 15	
UXTY	TLSV	
DATE	<enter>	
PAGE	<enter>	
DES	<enter>	

The screen output shown here may differ depending on the setup used.

Screen output:

```
DES OCS
TN 096 0 08 15 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY TLSV
UXID
NUID
NHTN
```

```
CFG_ZONE 000
CUR_ZONE 000
NCOS 0
ERL 0
ECL 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SFLT NO
CAC_CIS 0
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFD CRPD MWD LMPN RMMD
SMWD AAD IMD XHD IRD NID OLD VCE DRG1 POD DSX VMD SLKD CCSD
SWD LND CNDD CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED
RCBD ICDD CDMD LLCN MCTD CLBD AUTU GPUD DPUD DNDD CFXD
ARHD CLTD ASCD CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZUDI
RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD UDI
RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD DRDD
EXR0USMD USRD ULAD CCBD RTDD RBDD RBHD PGND FLXD FTTC DNDY
DNO3 MCB FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87D MSNV FRA
PKCH
CPND_LANG ENG
HUNT
PLEV 02
DANI NO
AST
IAPG 0
AACS NO
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 2070 0
CPND
ANIE 0
01 HOT P 3 888
02
03
04
05
06
07
08
```

```
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31

Date 16 APR 2008
```

Table 79
LD 11 — Configure UEXT with subtype TLSV

Prompt	Response	Description
REQ	CHG/NEW	Change or create a new mobile universal extension.
TYPE	UEXT	Universal Extension–This parameter indicates this is a universal extension unit.
TN	L S C U	Universal Extension TN
CUST	0-99	Customer number
UXTY	TLSV	UEXT subtype, this is prompted only for TYPE=UEXT. TLSV – Telephony Services unit ***Note:*** the UXTY cannot be changed for a UEXT. The unit must be removed and reconfigured. MOBX units cannot be copied.

Prompt	Response	Description
KEY 0 SCR	<SCR DN>	Prime DN can be up to seven-digits
KEY 01 HOT P	nn yyyzzzz	<nn> is the maximum number of digits for HOTP DN yyyzzzz is the access code and phone number of OCS target DN. This can be up to 31-digits.

Screen Output:

```
....
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY TLSV
....
KEY 00 SCR 2070 0
01 HOT P 3 888
```

10 Confirm that AST is not configured.

11 Configure TR87D and CDMR Class Of Service.

12 Confirm that this UEXT is not configured as MARP.

13 Configure Hot P for SIP Gateway calls.

14 Configure CLS PCAM.

15 Confirm **DSC** configuration. Create a DSC to route the call to the SIP route using the RL1.

Table 80
LD 87–Confirm DSC configuration

Prompt	Response	Description
REQ	prt	
CUST	0	
FEAT	cdp	
TYPE	dsc	
DSC	888	

ATTENTION
The screen output shown here may differ depending on the setup used.

Screen Output

```
FLEN 3
DSP LSC
```

```
RRPA NO
RLI 1
CCBA NO
NPA

NXX
```

--End--

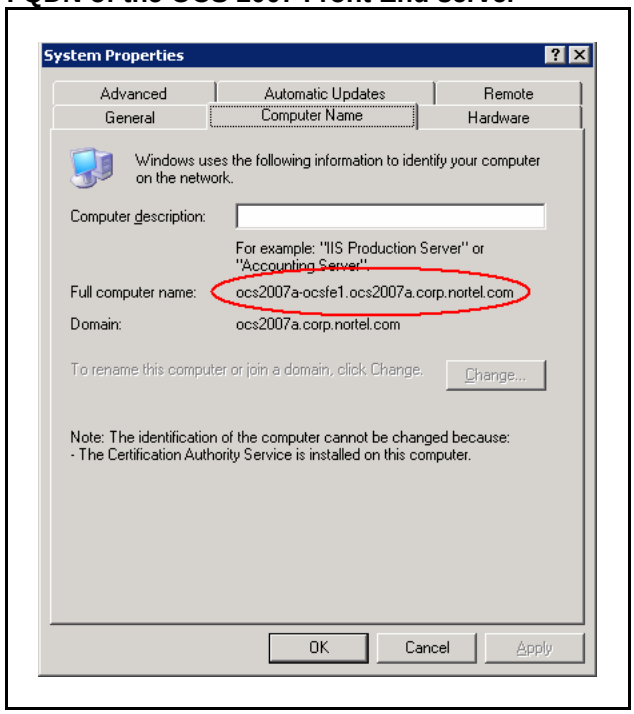
Signaling Server checklist

Use the following procedure to confirm the correct configuration of the Signaling Server.

Checking the configuration of the Signaling Server

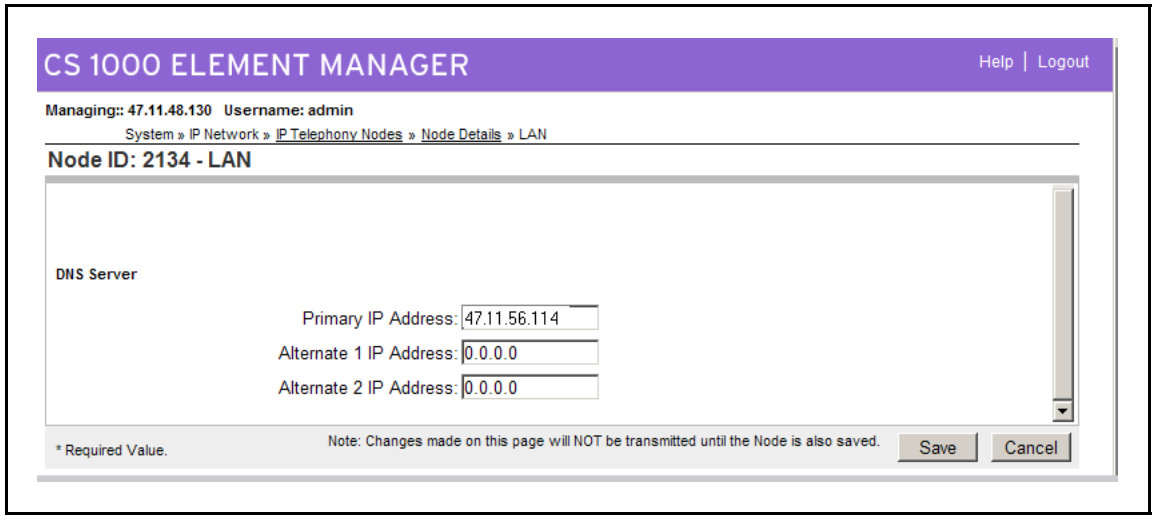
Step	Action
1	Confirm that the Signaling Server is version 6.0. Refer to the Product Bulletin for any required patches for Converged Office.
2	Confirm that your installation meets the memory requirements. The maximum number of SIP CTI/TR87 users on a single Signaling Server is 5000. The Standard Signaling Server memory is 1 gigabyte (minimum requirement) and is required in the following scenarios: **a** if SIP CTI/TR87 is co-resident with PD/RL/CL application **b** if SIP CTI/TR87 is co-resident with H.323/SIP GW serving more than 200 ports, or co-resident with Terminal Proxy Server serving more than 1000 IP users
3	Confirm the configuration of the Front End server and OCS Proxy server. Right-click **My Computer** and choose the **Computer Name** tab. For more information, see Figure 145 "FQDN of the OCS 2007 Front End server" (page 325).

Figure 145
FQDN of the OCS 2007 Front End server



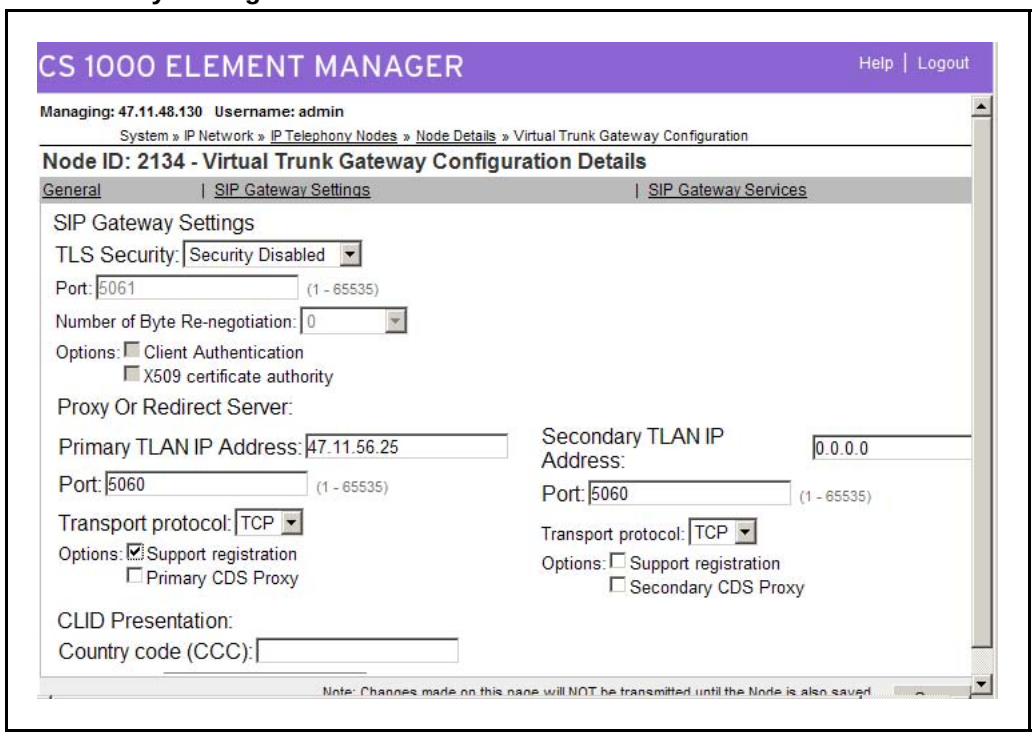
4 In Element Manager, on the navigation pane, select **IP Network, Nodes: Server, Media Cards**. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the **IP Telephony Node Properties Applications** section, click **LAN**, as shown in the following figure. Define the IP address of the server acting as DNS. For example, IP address is **47.11.56.114**.

Figure 146
DNS configuration on the Signaling Server



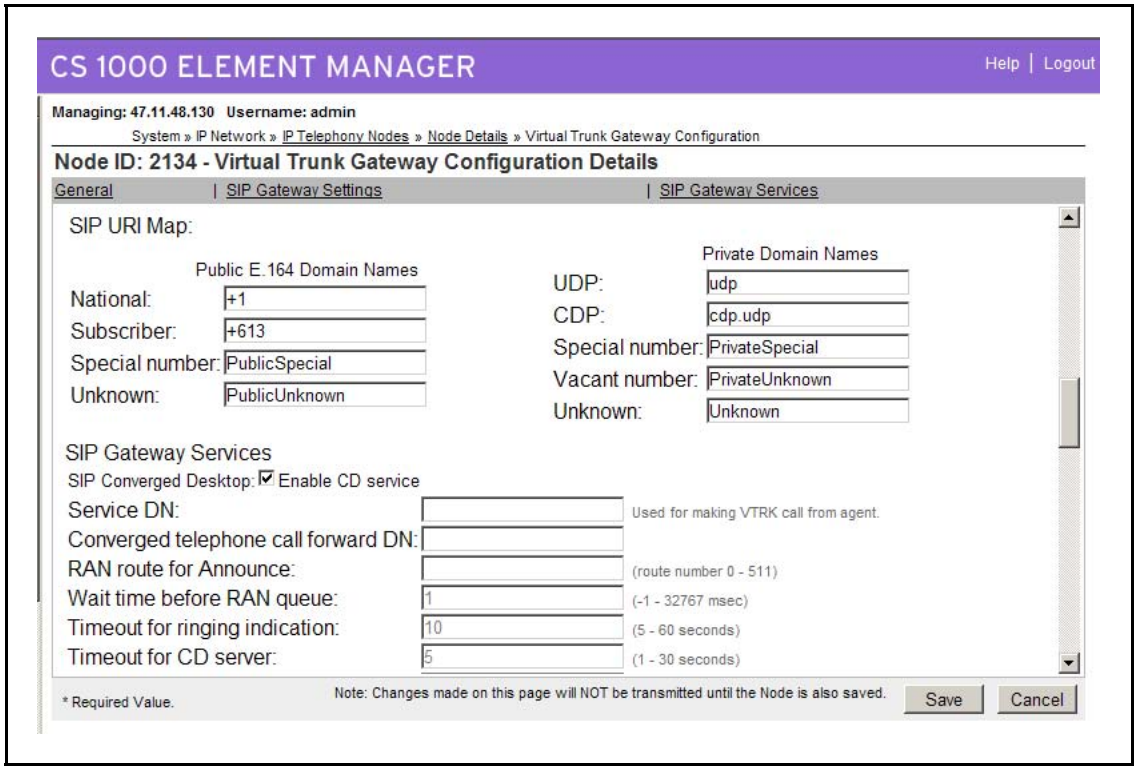
5 In the **IP Telephony Node Properties Applications** section, click **Gateway (SIPGw)**. Ensure that the SIP Gateway settings match the settings, as shown in the following figure.

Figure 147
SIP Gateway settings



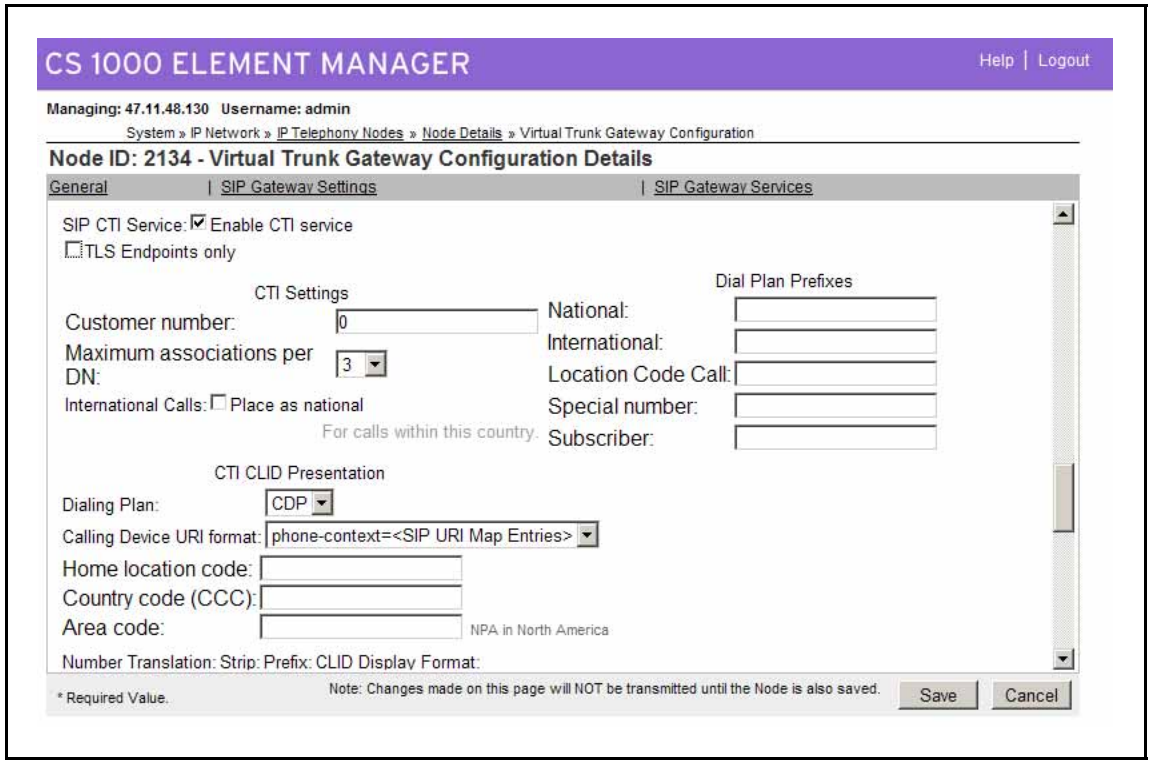
6 Confirm that the SIP URI Map settings match the settings, as shown in the following figure.

Figure 148
SIP URI Map



7 Confirm that the SIP CTI Services settings match the settings, as shown in the following figure.

Figure 149
SIP CTI Services



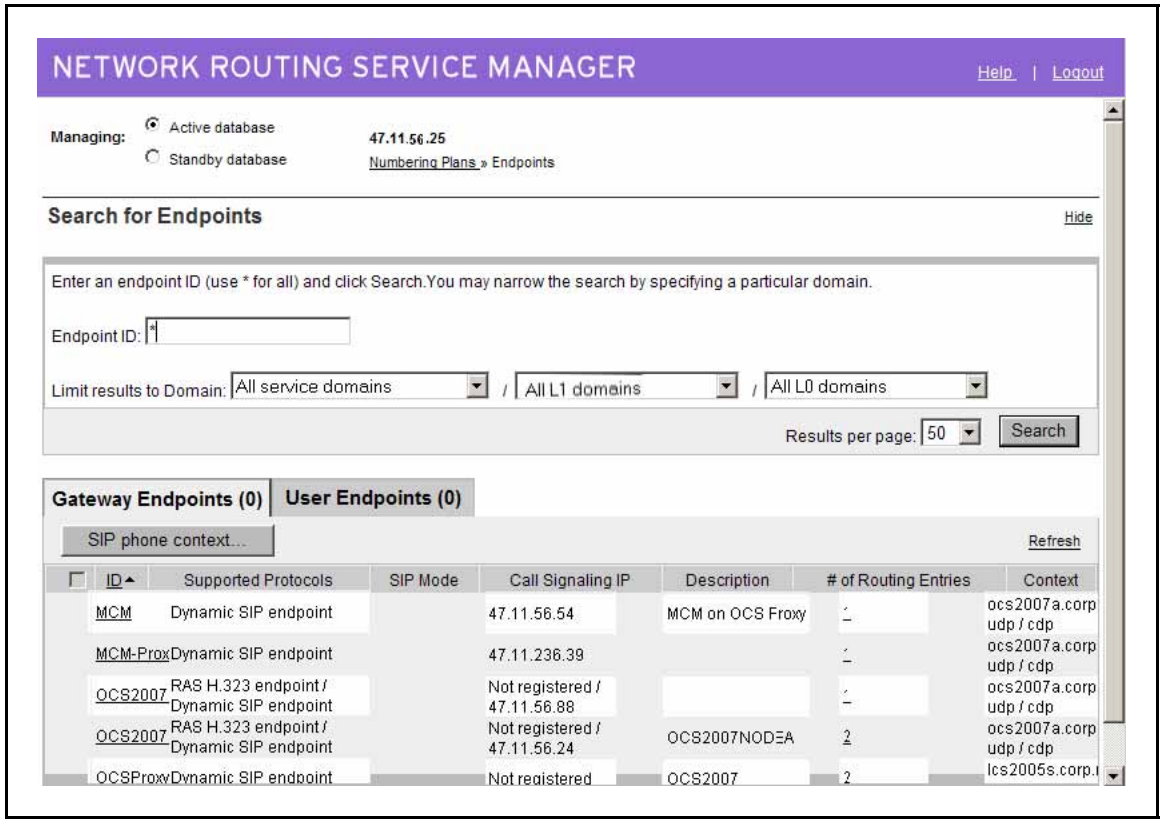
--End--

Checking the Network Routing Service (NRS) configuration

Use the following procedure to check the configuration of NRS.

Step	Action
1	In Network Routing Service Manager, on the navigation tree click **Numbering Plans** and then **Endpoints**. Check the Signaling Server and MCM Endpoints status, as shown in the following figure.

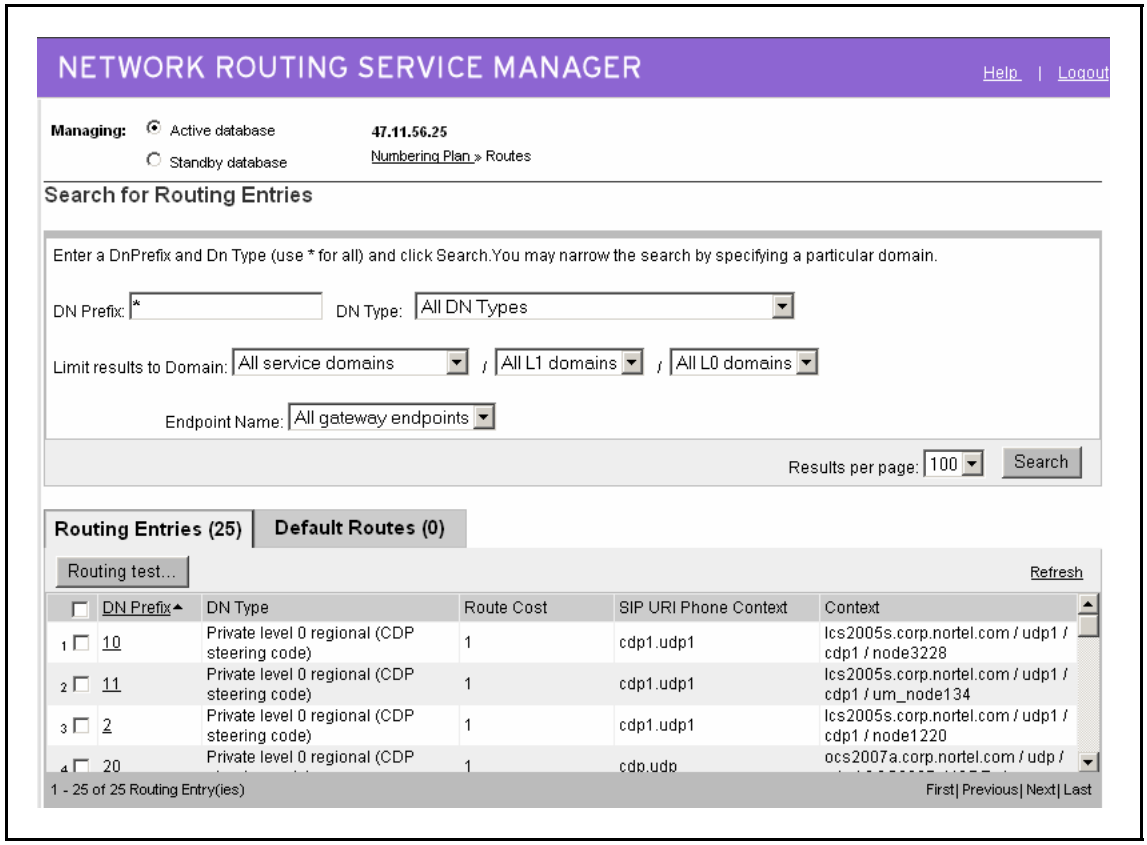
Figure 150
Signaling Server and MCM Endpoints status on NRS



Ensure that all the endpoints are registered (the endpoints must be listed as "Dynamic Sip" under the Supported Protocols column and have an IP address under the Call Signaling IP column in Figure 150 "Signaling Server and MCM Endpoints status on NRS" (page 329).

2 In the Network Routing Service navigation tree, click **Numbering Plans** and **Routes**. Check the UEXT Routing Entry, as shown in the following figure (refer to the information you recorded in Table 67 "Network Routing Service (NRS)" (page 313)).

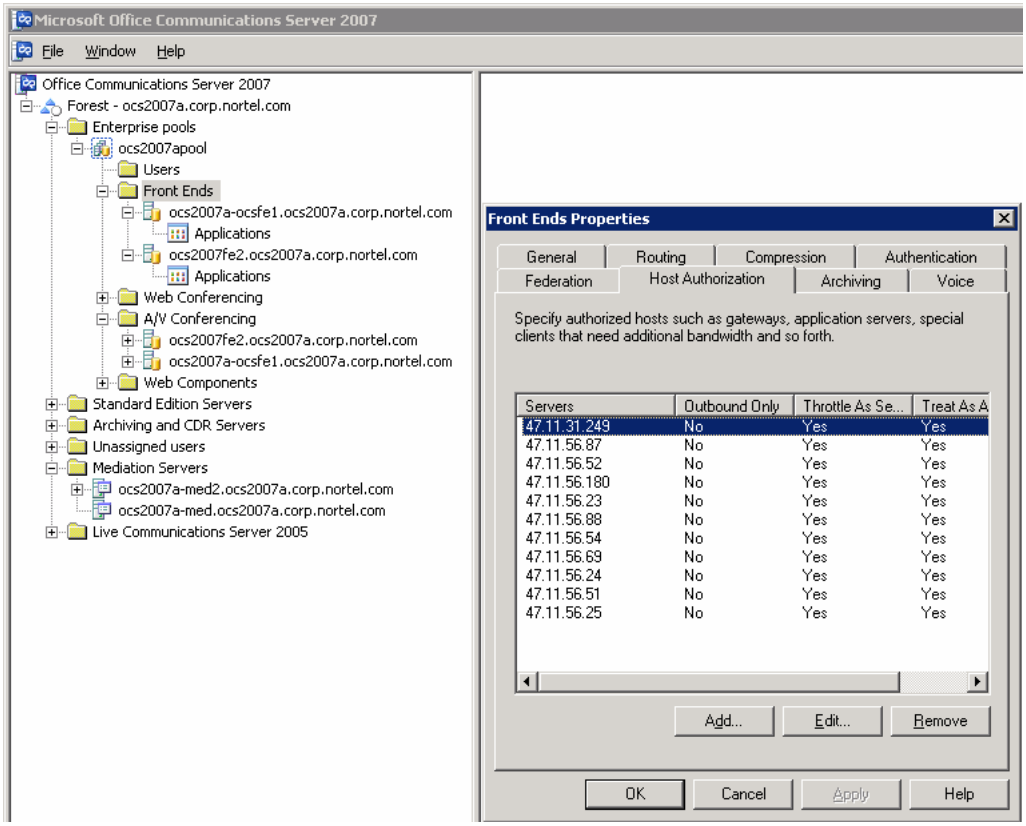
Figure 151
Routing Entry



3 Check the OCS 2007 Standard Edition configuration.

In Host Authorization for an OCS 2007 Standard Edition, configure the IP Address of the OCS Proxy server. See Figure 152 "Host Authorization" (page 331).

Figure 152
Host Authorization



4 Check the OCS Proxy server configuration. See Table 67 "Network Routing Service (NRS)" (page 313), the OCS Proxy IP is 47.11.56.54, and the Node IP is 47.11.56.24.

--End--

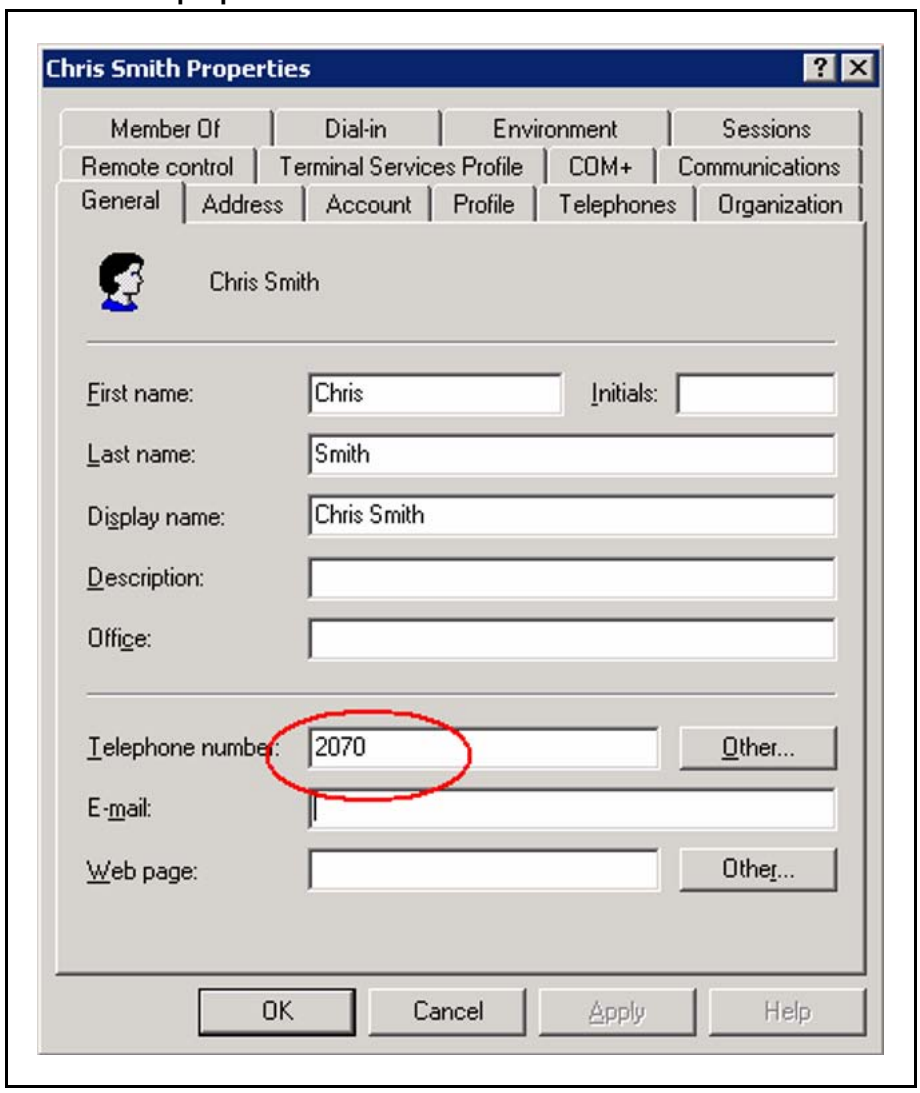
Checking the settings of Active Directory user configuration

Use the following procedure to check the Active Directory user configuration.

Step	Action
1	Check the user configuration by going to Active Directory, select the user and right-click **User Properties**. Select the **General** tab. Complete the following actions:
	a Compare and match your user properties settings with those in Figure 153 "General user properties" (page 332). The telephone number in the Telephone Number field must be

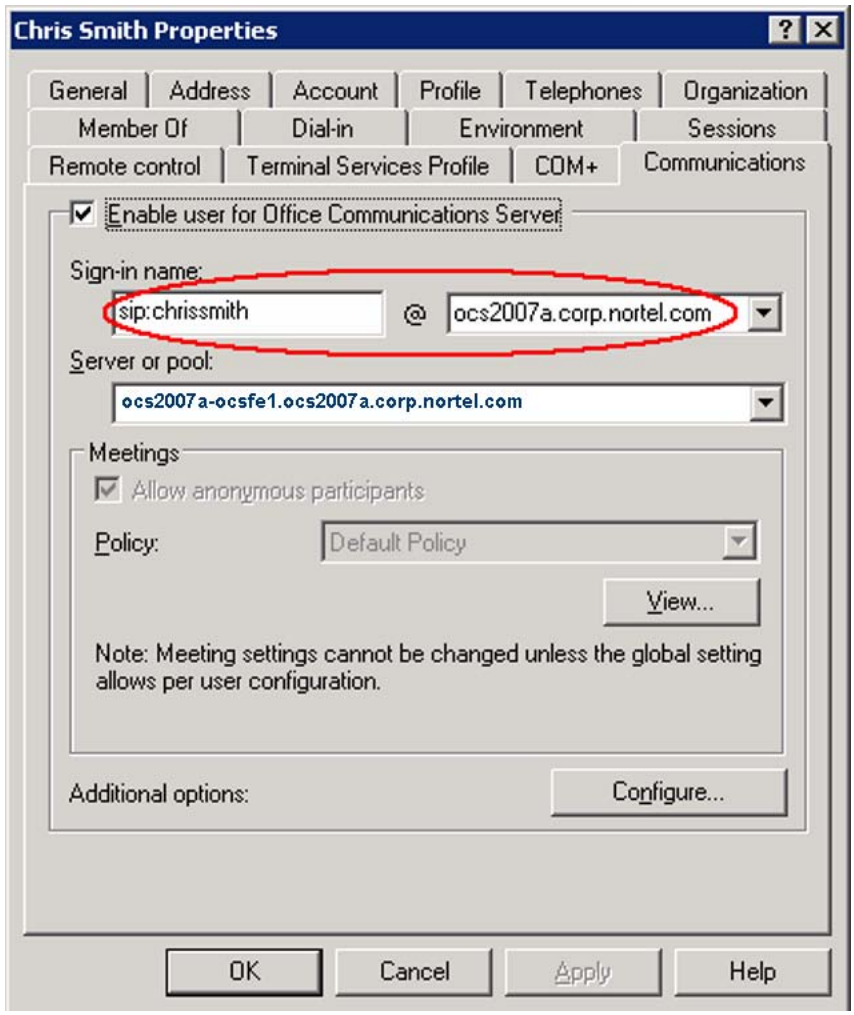
the same as the information recorded in Table 66 "Microsoft Active Directory" (page 313).

Figure 153
General user properties



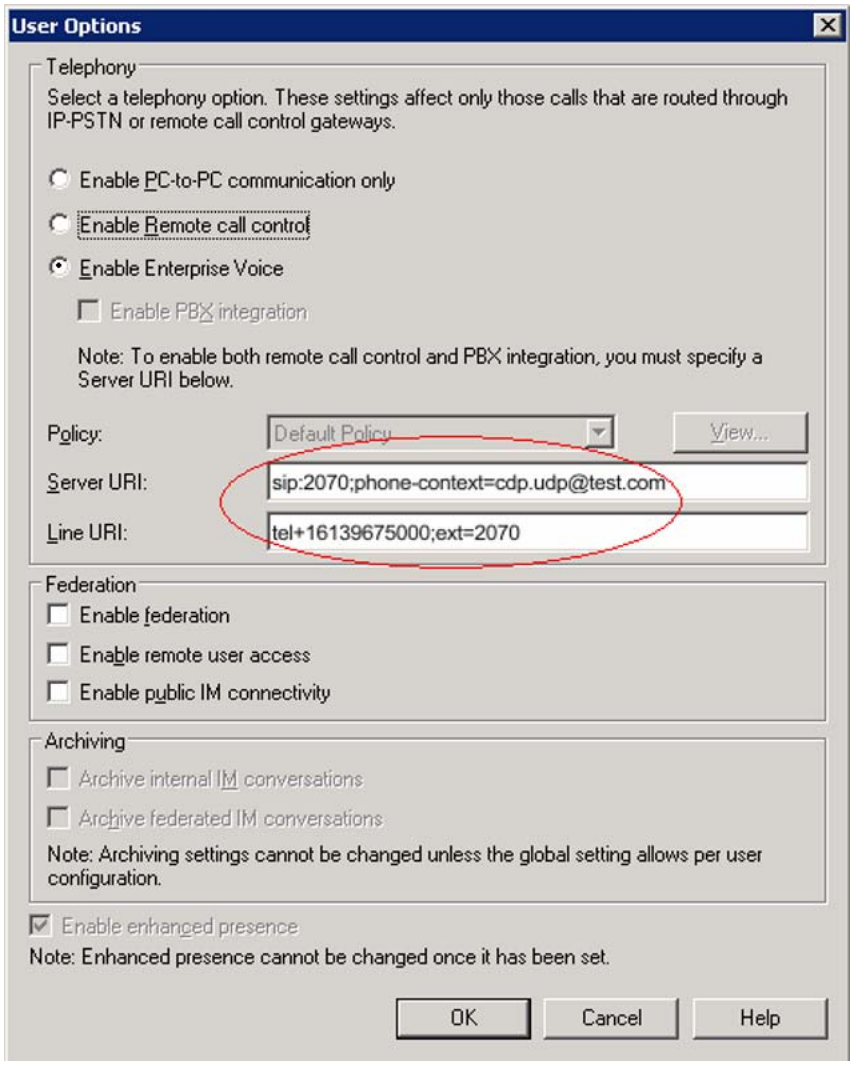
b Click the **Communications** tab. Compare and match your settings in OCS 2007 Office Communications user properties with those in Figure 154 "Communications properties" (page 333). Ensure the SIP Sign-in name is the same as the information recorded in Table 66 "Microsoft Active Directory" (page 313)).

Figure 154
Communications properties



c Click the **Communications** tab and click the Configure button. Compare and match your settings with those in Figure 155 "User Options" (page 334). The Server URI and the Line URI must be the same as the information recorded in Table 66 "Microsoft Active Directory" (page 313)).

Figure 155
User Options



Checking the MCM installation and configuration

Check that the MCM is properly installed and configured.

Step	Action
1	On the MCM, check that the user is a member of the RTC Server Applications and RTC Server Local Group.
2	For MCM Application, confirm that MCM running and for the Default OCS applications, confirm that IM URL Filter and Routing

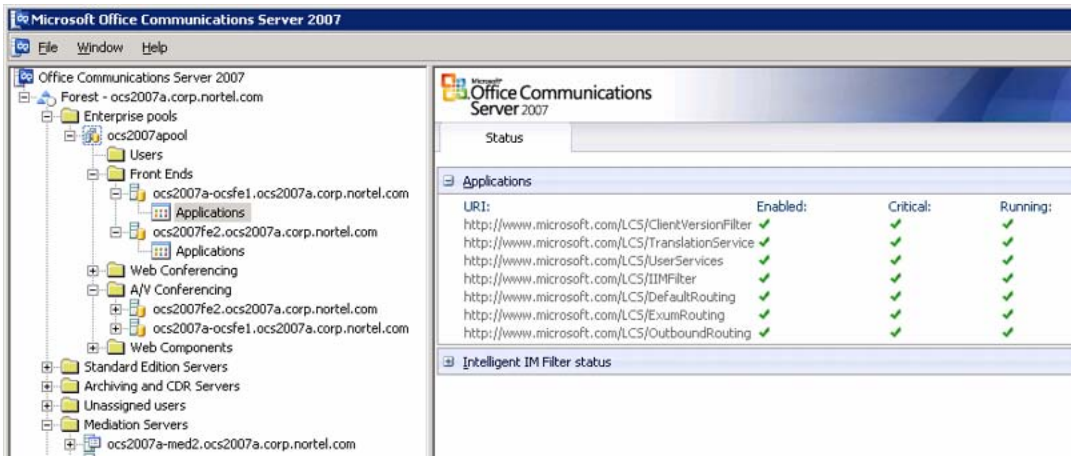
Application are running (see Figure 156 "MCM Application" (page 335).

If the MCM application is not running:

Confirm that MCM is configured with the MCM user groups RTC Server Local Group and RTC Server Applications.

- Confirm that the MCM user password is correct.
- Check the Event logs to find out why MCM is not running.

Figure 156
MCM Application



3 See Figure 157 "MCM Gateway Endpoint configuration" (page 336) and Figure 158 "MCM Configuration screen" (page 337) to check for proper MCM configuration on NRS.

--End--

Figure 157
MCM Gateway Endpoint configuration

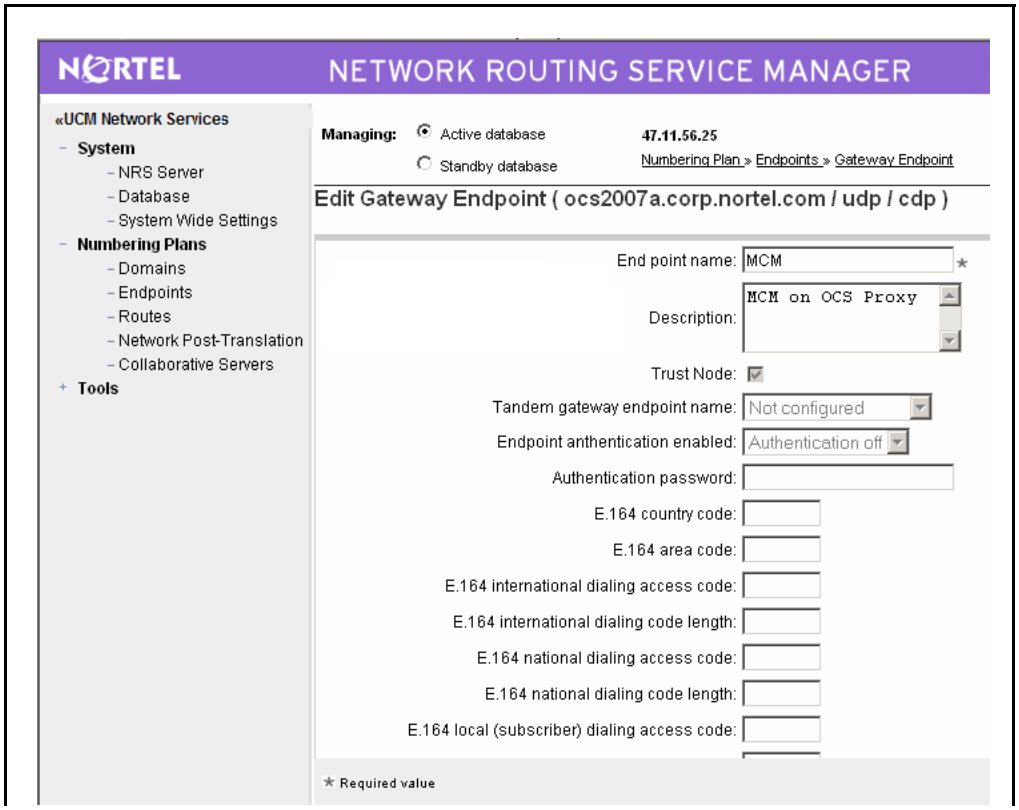
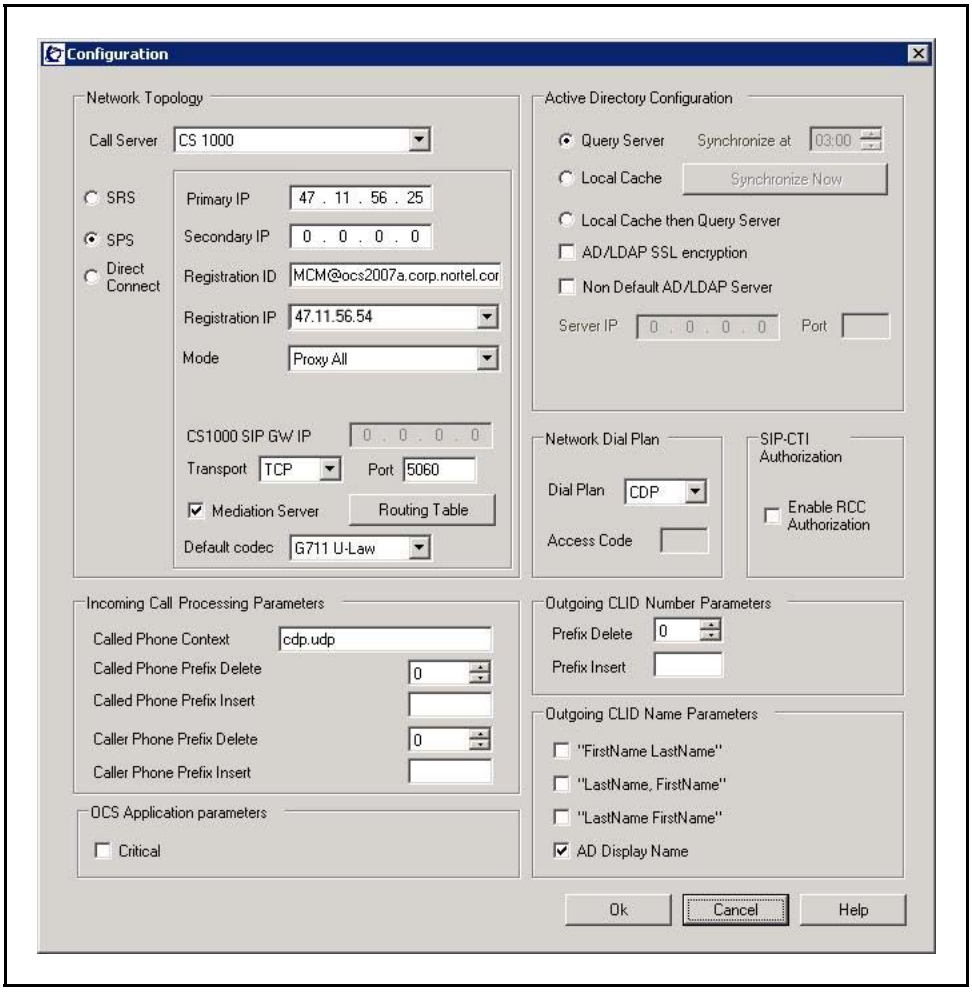


Figure 158
MCM Configuration screen



Enterprise Edition

This section describes the configuration of the OCS Enterprise Edition.

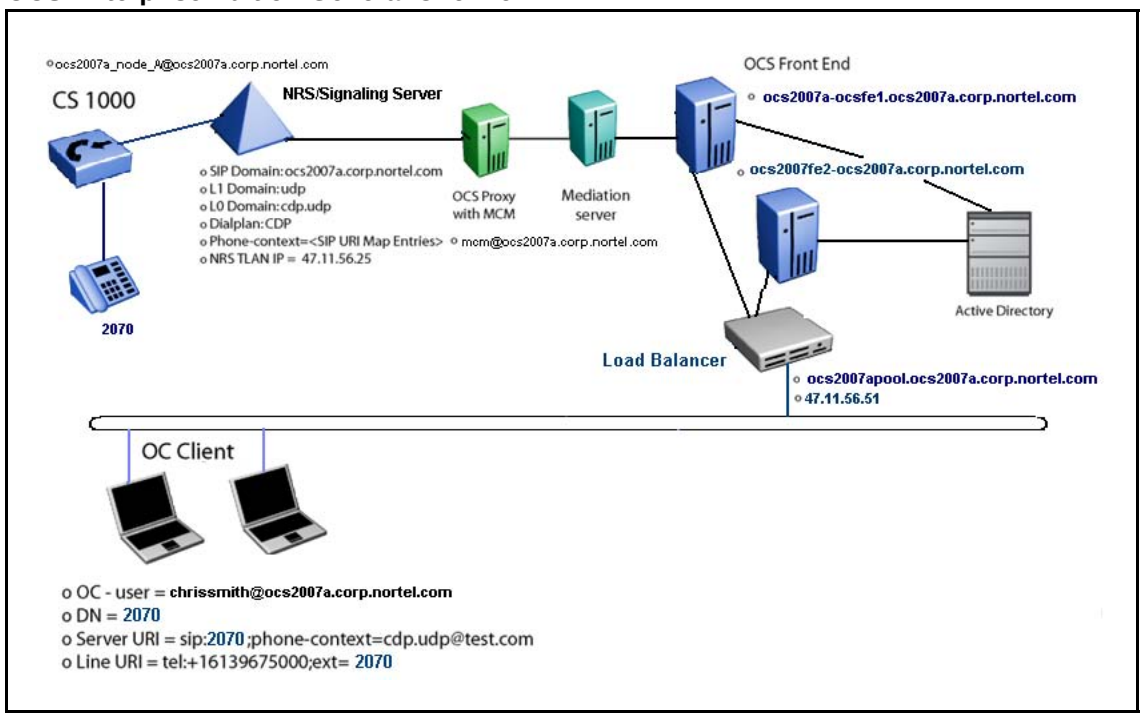
Overview of general lab set-up

Figure 159 "OCS Enterprise Edition General Overview" (page 338), illustrates the lab configuration, which includes:

- Call Server version 6.0
- Signaling Server version 6.0
- MCM version 4.x
- 1 DNS/Active Directory Server
- Mediation Servers

- OCS FE Server with a Pool and a Microsoft Software Load Balancer
- 1 OCS Proxy server

Figure 159
OCS Enterprise Edition General Overview



Collecting Data for Enterprise Edition

Collect the required data listed in the following four tables before you begin to configure the Converged Office solution.

ATTENTION
The FQDN field is case sensitive. Enter the exact FQDN.

ATTENTION
The Certificate is complex and its correct configuration is not described in this section. Confirm that you have configured the Certificate correctly.

Table 81
Microsoft Active Directory

Required information	Record your information	For example
User SIP URI		chrissmith@ocs2007a.corp.nortel.com
Server URI		sip:2070;phone-context=cdp.udp@test.com

Line URI		tel:+16139675000;ext=2070
Telephone number		2070

Table 82
OCS

Required information	Record your information	For example
OCS 2007 Proxy server		ocs2007a-proxy.ocs2007a.corp.nortel.com 47.11.56.54
Load Balancer Pool		ocs2007apool 47.11.56.51
OCS Enterprise Edition Front End server 1		ocs2007a-ocsfe1.ocs2007a.corp.nortel.com 47.11.56.51
OCS Enterprise Edition Front End server 2		ocs2007ocsfe2.ocs2007a.corp.nortel.com 47.11.56.52

Table 83
NRS

Required information	Record your information	For example
IP-address Primary SPS		47.11.56.25 (standalone)
IP-address Secondary SPS		Not used
Node IP-address		47.11.156.24
OCS endpoint name		mcm@ocs2007a.corp.nortel.com
Communication Server 1000 SIP gateway endpoint name		ocs2007_node_A
Routing Entry for UEXT		LOC: CDP: 888 - MCM LOC: 20 and 21 - OCS2007_node_A
Service domain		ocs2007asps.ocs2007a.corp.nortel.com
Level 1 domain		udp
Level 0 domain		cdp.udp

Table 84
Element Manager

Required information	Record your information	For example
LAN configuration, FQDN (OCS Proxy and OCS Pool)		ocs2007a-proxy.ocs2007a.corp.nortel.com
LAN configuration, IP Address (OCS Proxy and OCS Pool)		47.11.56.54

Communication Server 1000 SIP gateway endpoint name		ocs2007_node_A
SIP Domain name		ocs2007a.corp.nortel.com
SIP Gateway Endpoint name		ocs2007_node_A
SIP URI map, Private/UDP domain name		udp
SIP URI map, Private/CDP domain name		cdp.udp
SIP CTI Service, Service enabled		Yes
SIP CTI Service, Customer Number		0
SIP CTI Service, International Calls As National		Yes
SIP CTI Service, National Prefix		0
SIP CTI Service, International Prefix		00
SIP CTI Service, Dialing Plan		CDP
SIP CTI Service, Calling Device URI Format		Phone-context=<sip URI map entries)
SIP CTI Service, Country Code		33
SIP CTI Service, National/ Number of digits to strip		1

OCS Management Console

The OCS Management Console, shown in Figure 160 "OCS Management Console" (page 341), provides an overview of OCS configuration:

- The OCS Enterprise Edition Pool: **ocs2007apool**
- The OCS Enterprise Edition FE server(s): **ocs2007a-ocsfe1.ocs2007a.corp.nortel.com**

  The Enterprise edition can have multiple FE Servers.
- The OCS Enterprise Edition Proxy Server: **ocs2007a-proxy-ocs2007a.corp.nortel.com**

ATTENTION
The OCS GUI is always displayed in lower case. To determine the correct FQDN, right-click pool, and the correct FQDN displays under Display Name as depicted in Figure 161 "Determining the exact FQDN of the pool" (page 342).

Figure 160
OCS Management Console

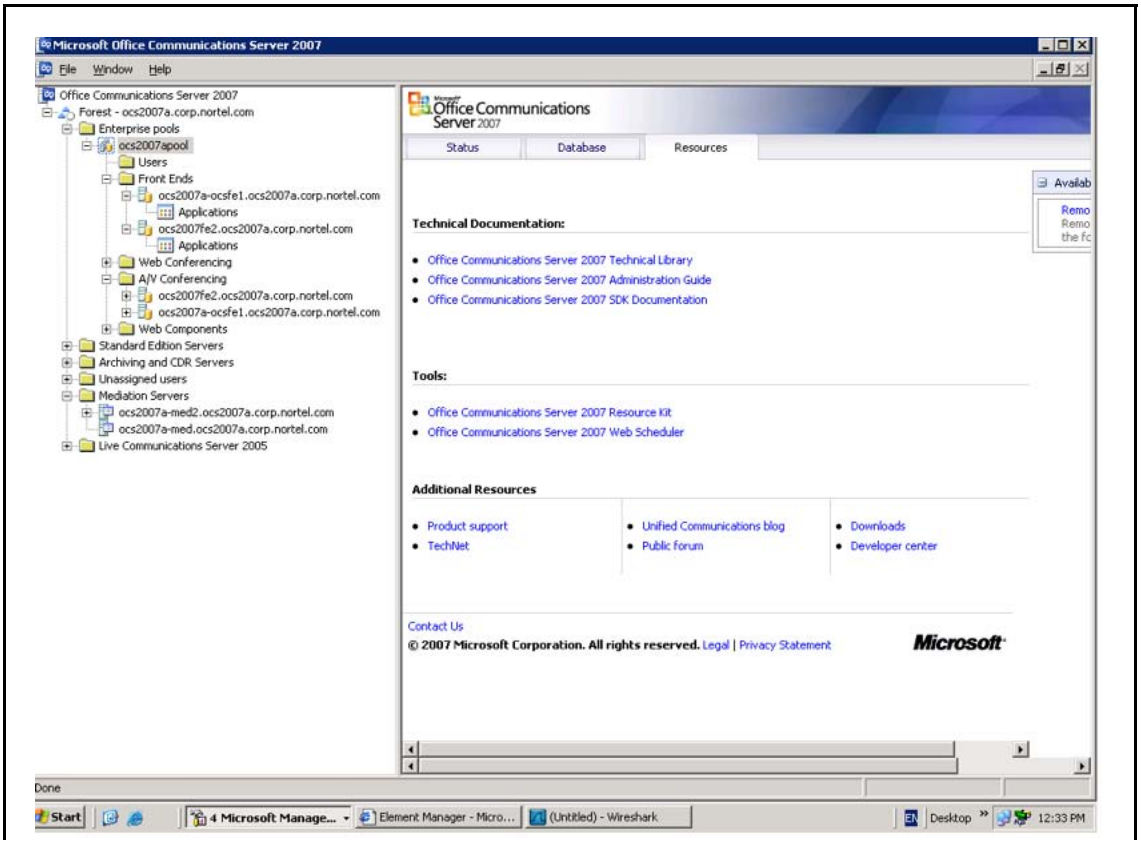
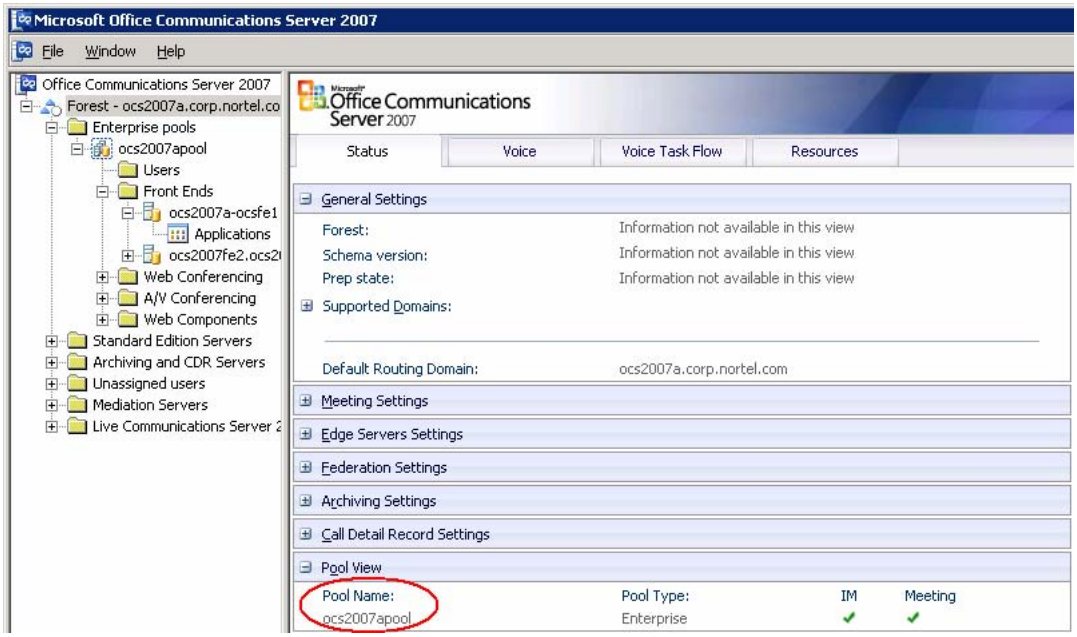


Figure 161
Determining the exact FQDN of the pool

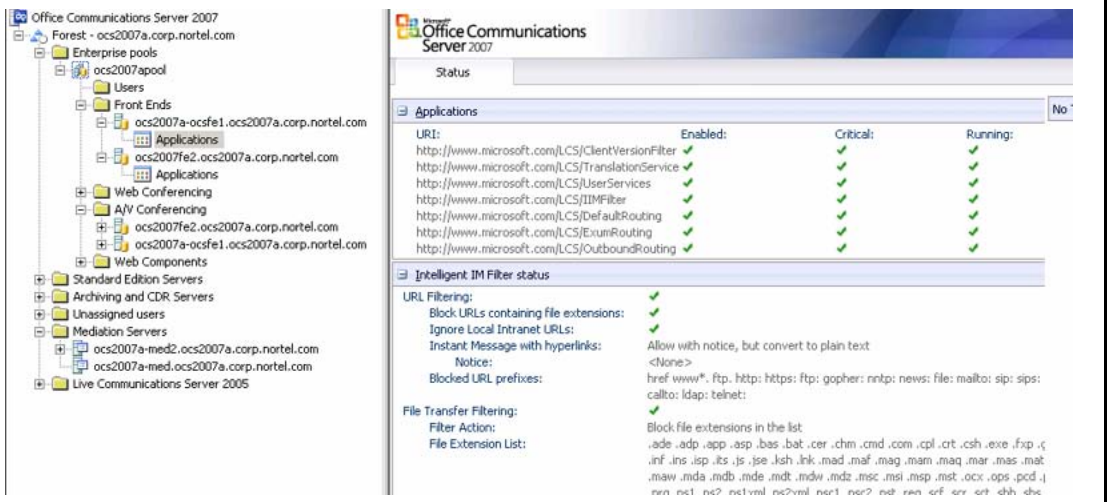


Identifying the active OCS default applications

Use the following procedure to determine which default applications are running.

Step	Action
1	To determine the exact FQDN of Pool, confirm that the two default applications, IM URL Filter Application Setting and Routing Application Setting are running.
2	In OCS 2007, click Applications. See Figure 162 "Default applications" (page 343) for an example window.

Figure 162
Default applications



--End--

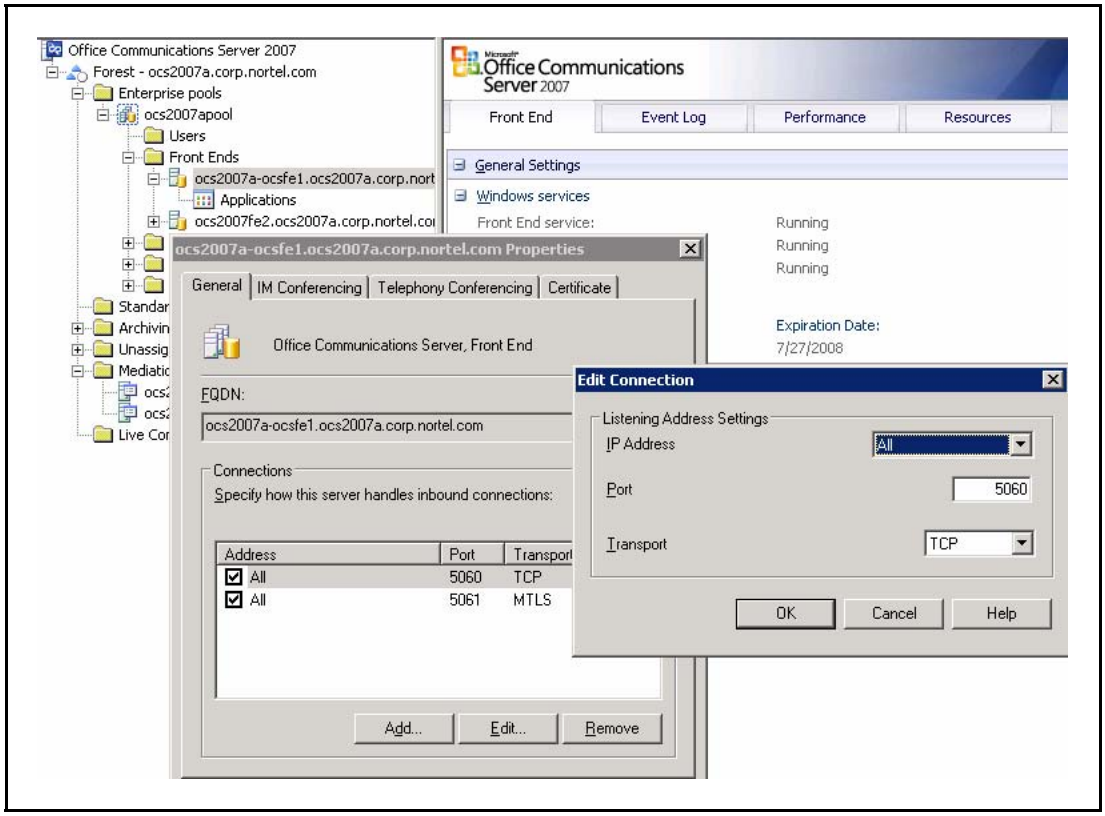
Confirming the General tab settings

Use the following procedure to confirm the correct settings in the General tab.

Step	Action
1	Right-click OCS 2007 Front End server and select **Properties**.
2	Choose the **General** tab and click the **Edit** button. Confirm you have the correct settings for the Front End server. For an example, see Figure 163 "General settings" (page 344).

--End--

Figure 163
General settings



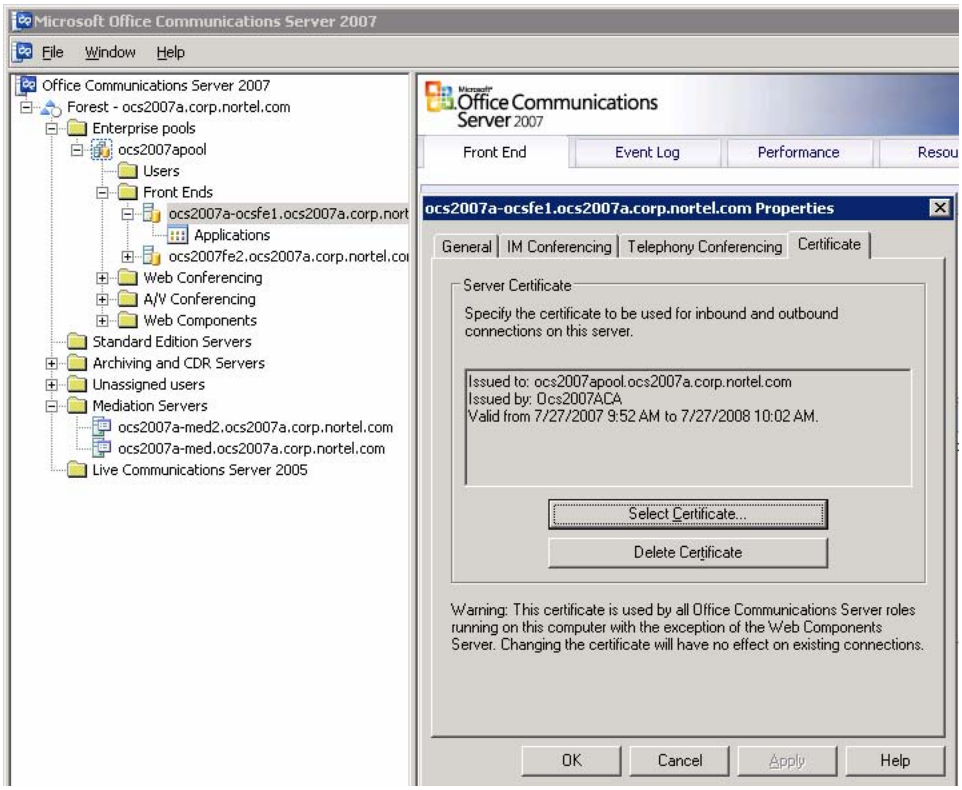
Checking the configuration of Certificates

Prior to the setup of Converged Office, configure certificates.

Use the following procedure to check your configuration settings of Certificates.

Step	Action
1	Right-click the OCS 2007 Front End server, select **Properties**.
2	Choose the **Certificate** tab. The Certificate must be issued to the FDQN of the Pool, not to FQDN of the Front End server (see Figure 164 "Front End server Certificate" (page 345)).
3	Click the **Select Certificate** button to confirm the settings of the Front End server Certificate.

Figure 164
Front End server Certificate



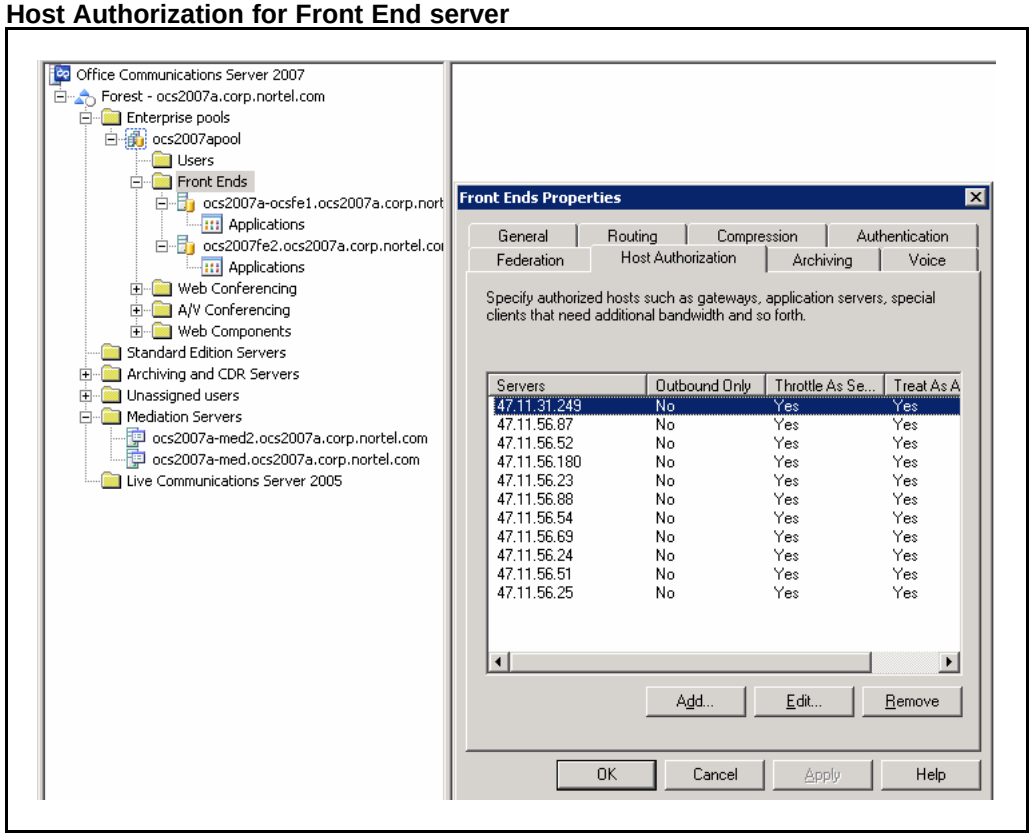
--End--

Checking the configuration of Host Authorization

Use the following procedure to check your configuration settings of Host Authorization.

Step	Action
1	Right-click the OCS 2007 Front End server and select **Properties**.
2	Choose the **Host Authorization** tab.
3	Click **Edit** to confirm the settings of the Host Authorization for the Front End server (see Figure 165 "Host Authorization for Front End server" (page 346)).

Figure 165
Host Authorization for Front End server



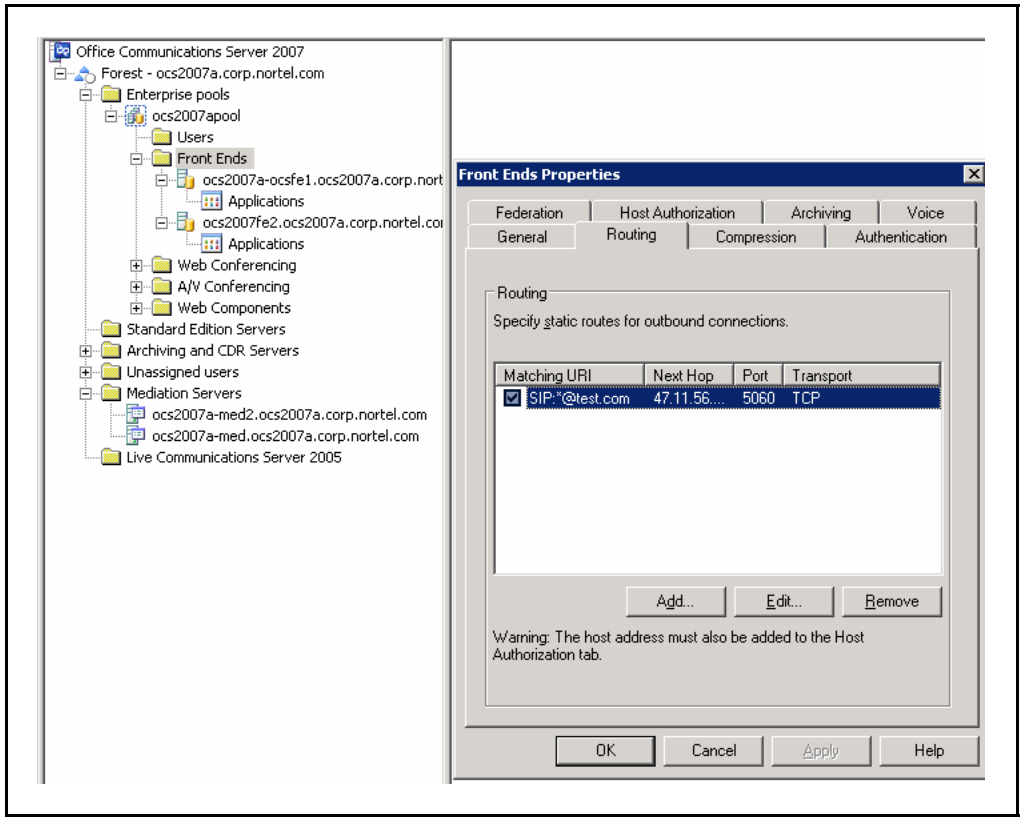
--End--

Checking that Routing is correctly configured

Use the following procedure to check that Routing is correctly configured.

Step	Action
1	Right-click Front Ends and select **Properties**. Compare the Routing settings of the Front End server Enterprise Pool with the Routing settings in Figure 166 "Routing for Enterprise Pool" (page 347).

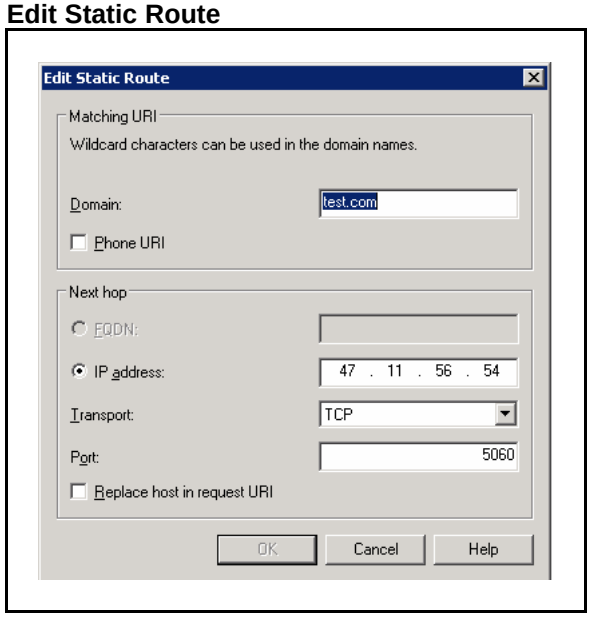
Figure 166
Routing for Enterprise Pool



2 Choose the **Routing** tab.

3 Click the **Edit** button to confirm the Matching URI and Next hop settings. (see Figure 167 "Edit Static Route " (page 348)). Forward all requests with the specified Domain.

Figure 167
Edit Static Route



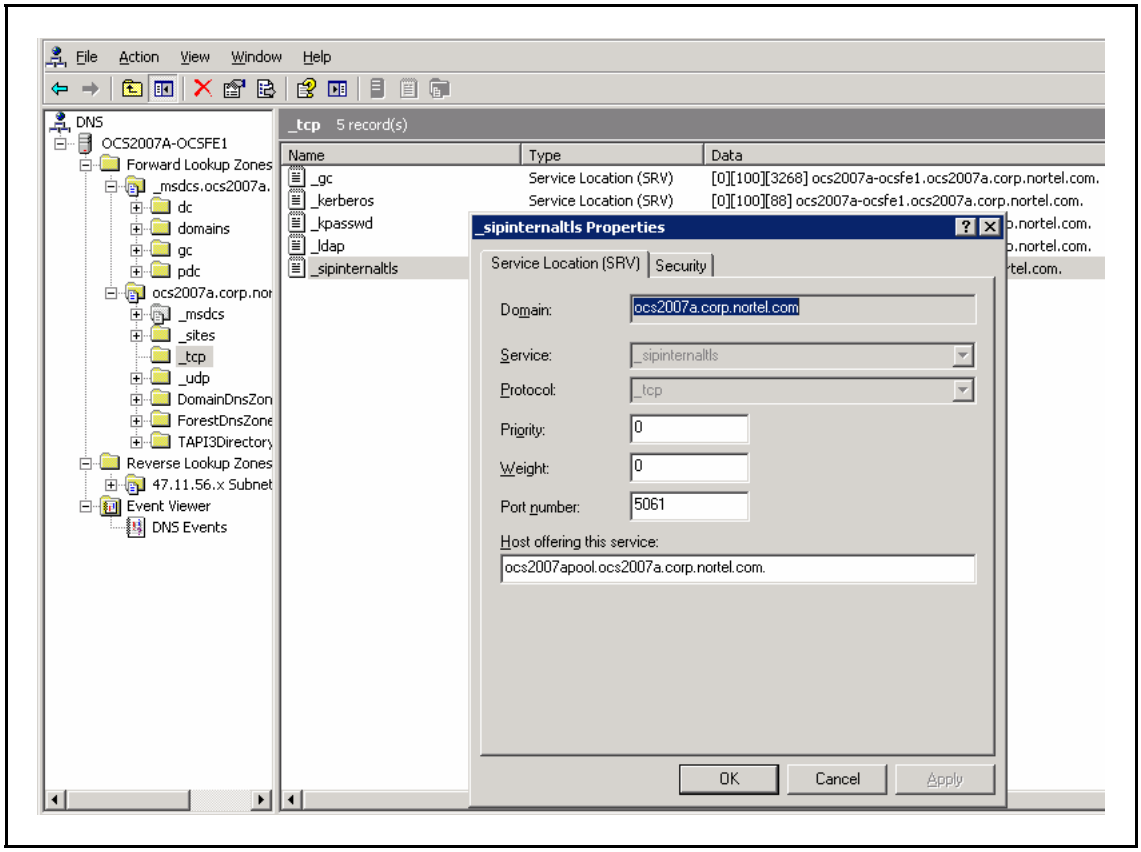
--End--

Checking that DNS is correctly configured

Use the following procedure to check the settings for DNS Configuration. Checking these settings assumes that the DNS service is enabled on the Windows 2003 server. The OCS servers are also using this DNS server.

Step	Action
1	On the DNS server, select _**tcp**.
2	Select _**sipinternaltls**.
3	Right-click and select **Properties**.
4	Click the **Service Location (SRV)** tab.
5	Check that the sipinternal SRV records are configured properly. See example Figure 168 "sipinternaltls SRV records" (page 349) for the settings for sipinternaltls SRV records.

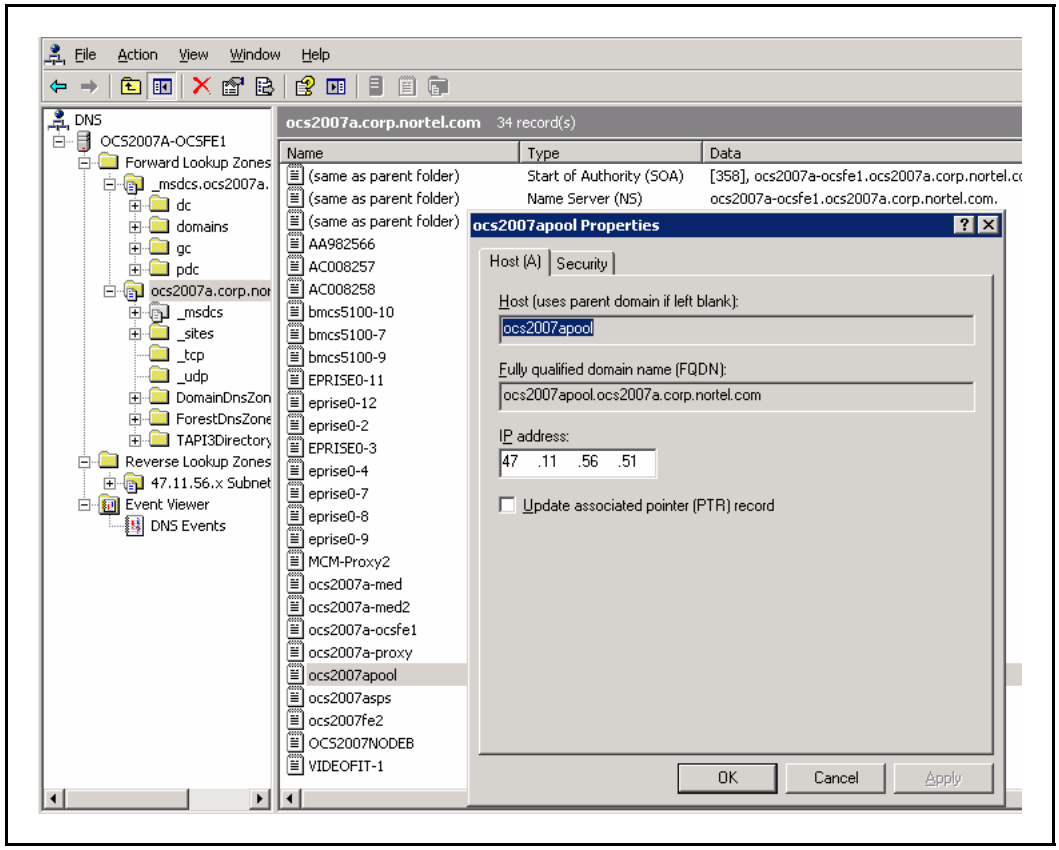
Figure 168
sipinternaltls SRV records



6 On the DNS server, right-click **ocs2007apool** and select **Properties**.

7 Select the **Host (A)** tab and check the Host A record for the Pool (see Figure 169 "Host (A) record for the Pool" (page 350)).

Figure 169
Host (A) record for the Pool



For more information about these configurations, see the *Microsoft Office Communications Server 2007 Enterprise Edition Deployment Guide* . Download Microsoft documentation from the Download Center at www.microsoft.com.

--End--

Checking Active Directory configuration

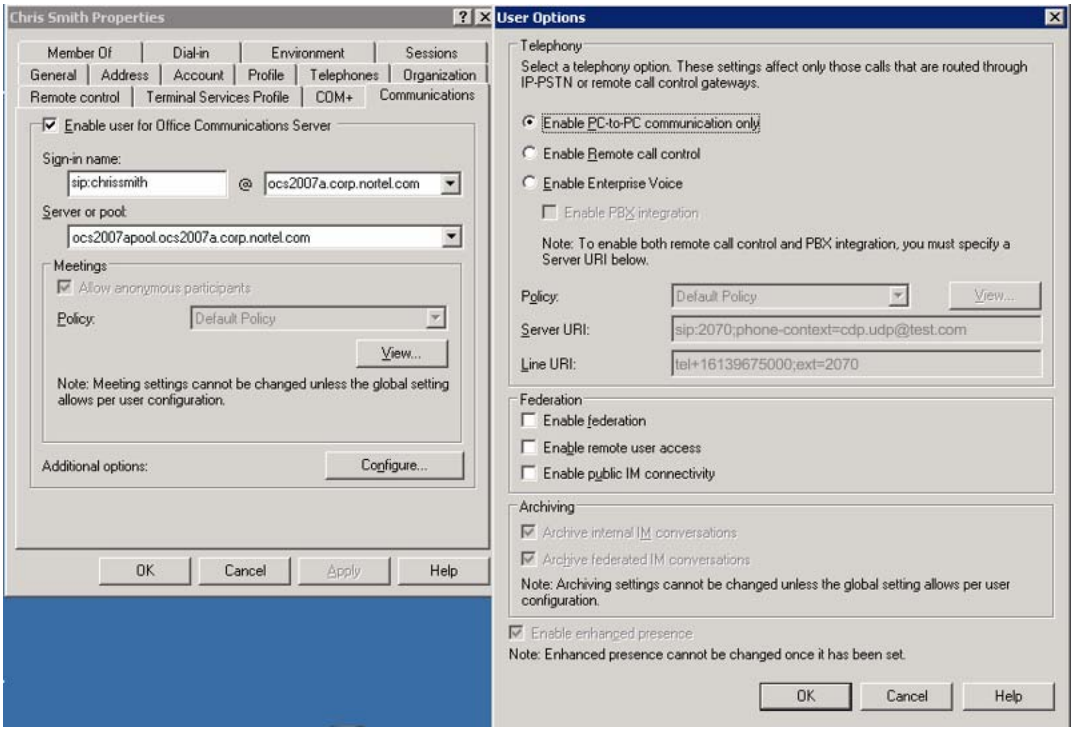
Step	Action
1	On the Active Directory server, right-click **Users** and select the name of the user to configure in the right pane.
2	Right-click and select **Properties**.
3	Choose the **Communications** tab.

4 Click the **Configure** button.

--End--

See Figure 170 "User Advanced Settings" (page 351) to check the settings for Server URI and Line URI.

Figure 170
User Advanced Settings



ATTENTION
For more information about the user configuration of Active Directory, see the Standard Edition section "Checking the settings of Active Directory user configuration" (page 331).

Checking the installation and configuration of MCM

Use the following procedure to check that MCM is correctly installed and configured.

Step	Action
1	Assign the required Local group to the MCM user.

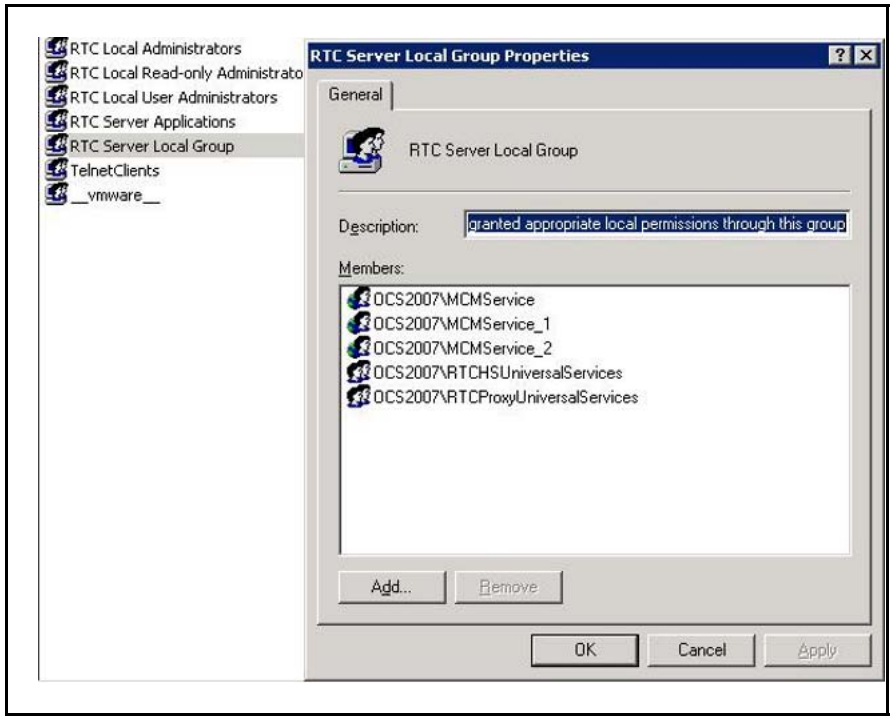
Prior to installation of MCM, an MCM user inside the Active Directory is created and the RTC Server Local Group and RTC Server Application local group is assigned to this user.

2 On the Proxy Server, right-click **My Computer** and choose **Manage**. This assigns the MCM user to the RTC Server Local Group and RTC Server Application.

3 Under Local Users and Groups, select **Groups**.

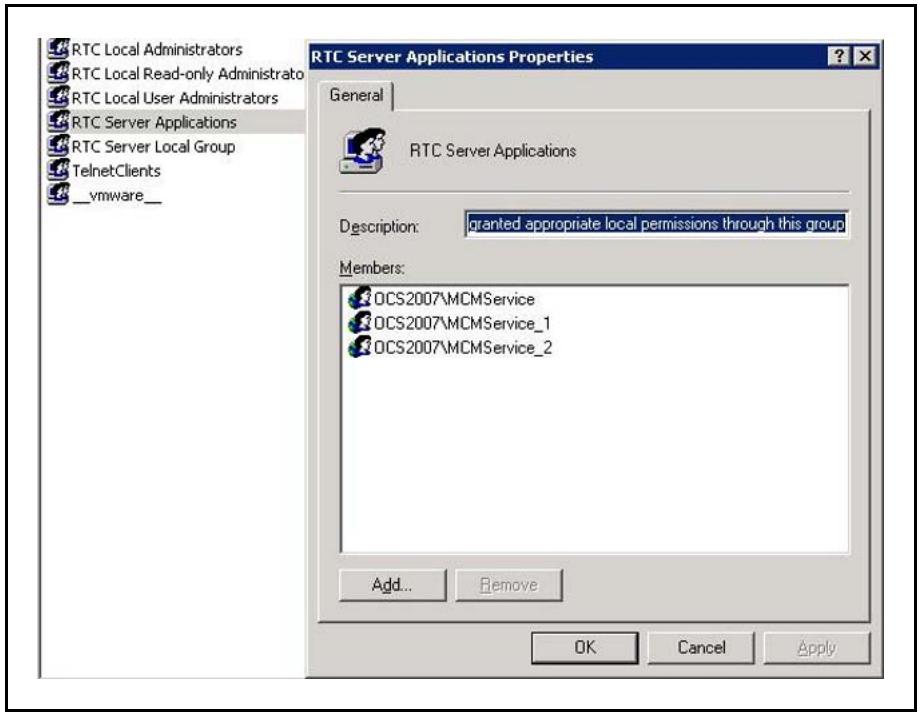
4 Right-click **RTC Server Local Group** and select **Properties**. Confirm that the settings are correct . See Figure 171 "RTC Server Local Group" (page 352) for an example.

Figure 171
RTC Server Local Group



5 Right-click **RTC Server Applications** and select **Properties**. Confirm that the settings of the RTC Server Application group are correct (see Figure 172 "RTC Server Application group" (page 353)).

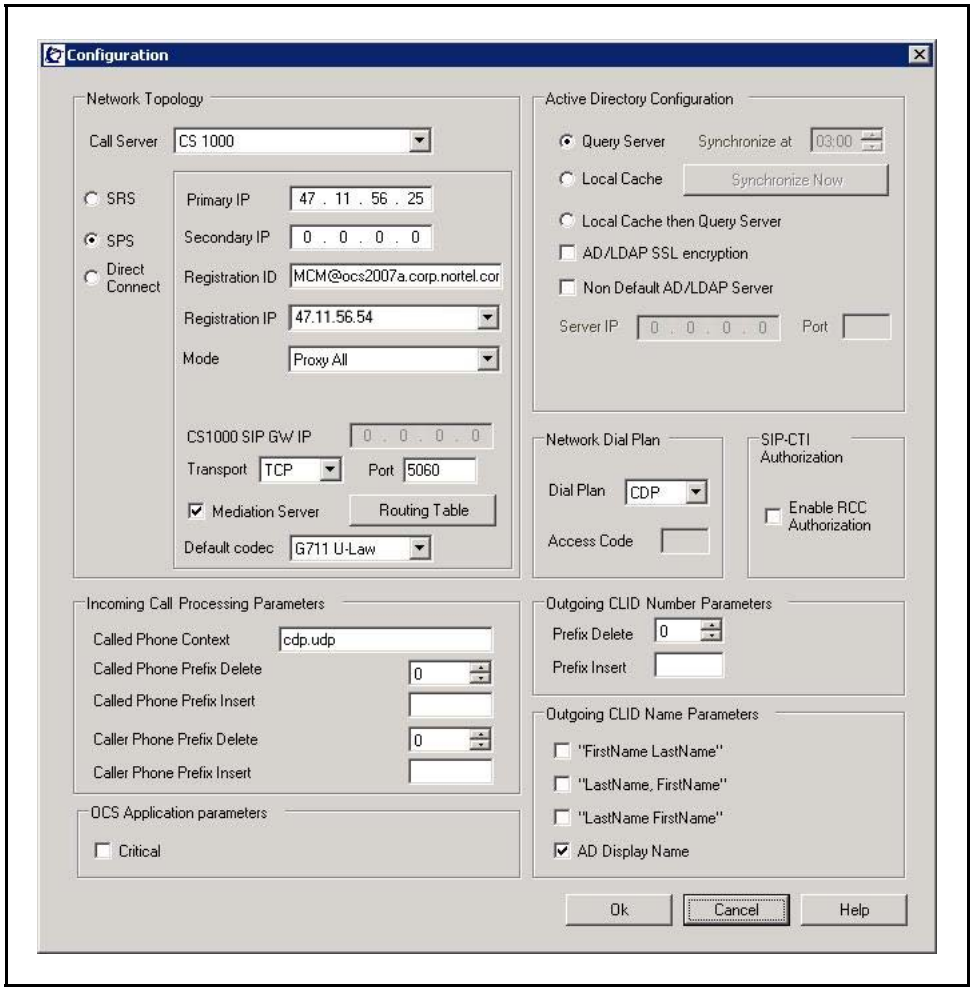
Figure 172
RTC Server Application group



ATTENTION

- MCM may not run if the MCM user is not configured to belong to the required groups.
- MCM may not run if an incorrect password is entered during the MCM installation.

6 On the MCM server, choose the **Tools** menu and select **Configuration**. See the following figure for an example of a configuration window.



7	Ensure that the correct **Called Phone Context** is entered. The Called Phone Context must correspond to what is configured for the **user inside Active Directory** and the **SIP URI map** (Private/CDP or UDP domain name) configured in Element Manager.

--End--

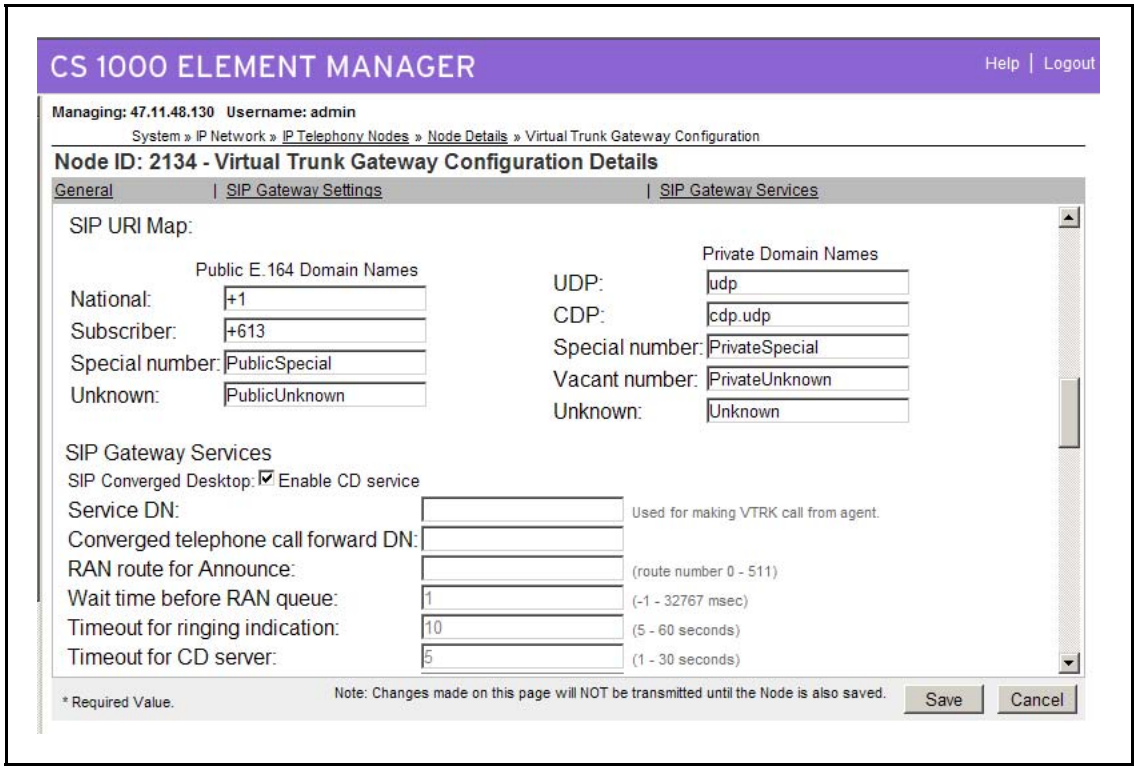
Checking the Signaling Server configuration

Use the following procedure to check that the Signaling Server is correctly configured.

Step	Action
1	In Element Manager, on the navigation pane, select **IP Network, Nodes: Server, Media Cards**. Click a node under the NodeID column. The window refreshes with the selected Node Details. In the **IP Telephony Node Properties Applications** section, click

Gateway (SIPGw). The Virtual Trunk Gateway Configuration Details page appears, check the settings of **SIP URI** .

Figure 173
SIP URI



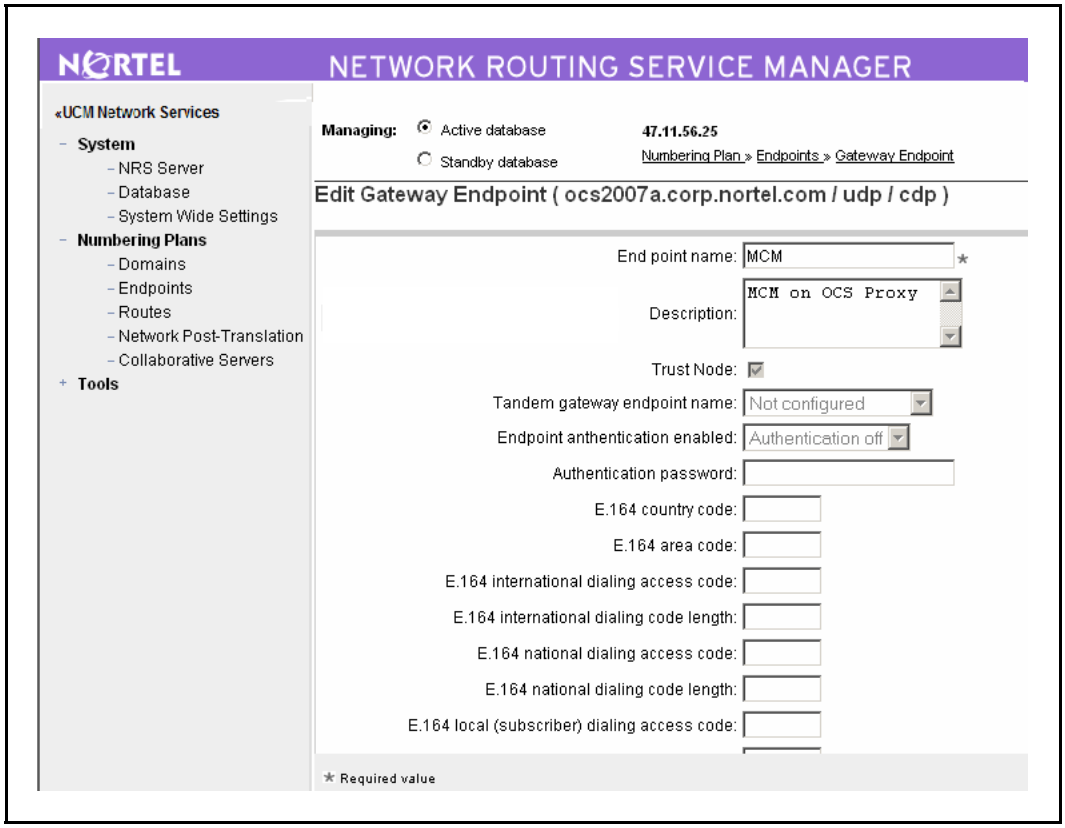
--End--

Checking the configuration of NRS

Use the following procedure to check that the NRS is correctly configured.

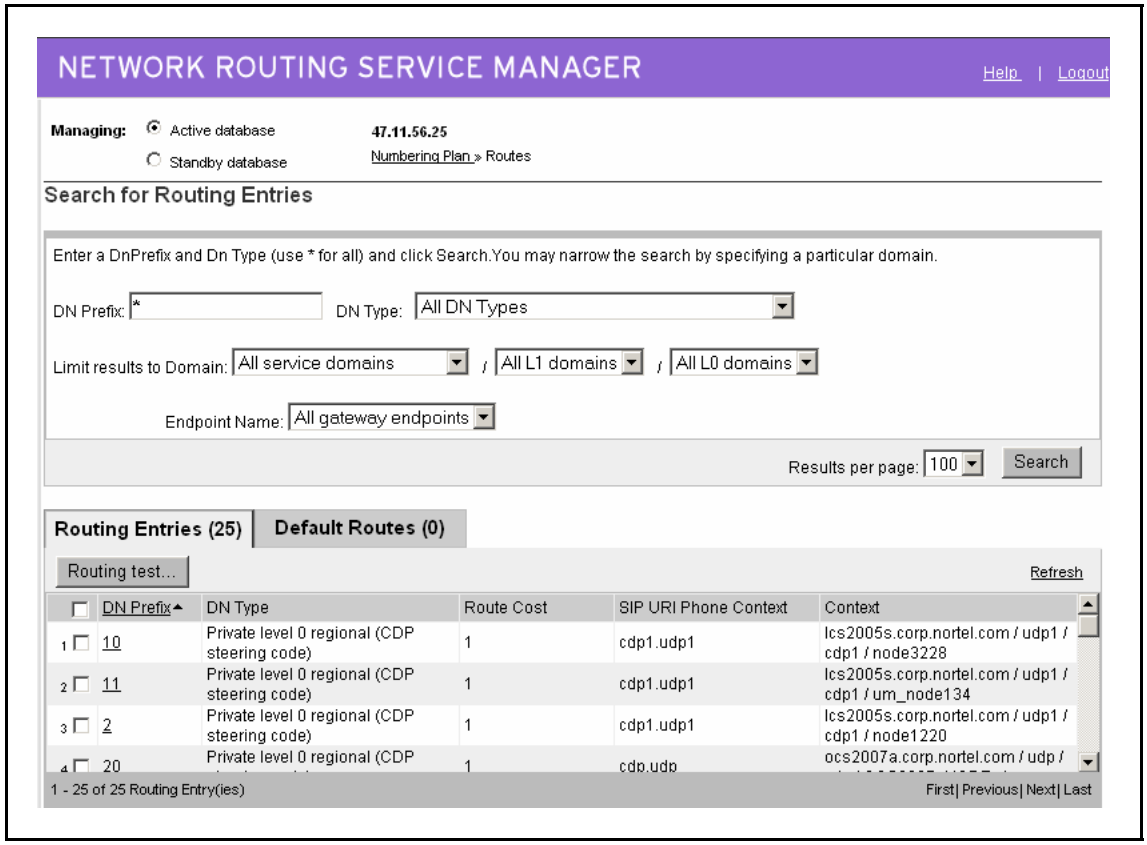
Step	Action
1	On the Network Routing Service Manager (NRSM) navigation pane, click **Numbering Plans** and then **Endpoints**. Select the endpoint name. Confirm that the settings are correct, as shown in the following figure.

Figure 174
MCM endpoints



2 On the Network Routing Service Manager (NRSM) navigation pane, click **Numbering Plans** and then **Routes**. The Search for Routing Entries page appears, confirm the settings are correct, as shown in the following figure.

Figure 175
Routing Entries for Endpoints



--End--

Normalizing Phone Numbers

When normalizing phone numbers, the **Telephone Number** field can be different from what is configured in the OCS user configuration for the **Line URI** field. However, a corresponding normalization rule should be defined in the Company_Phone_Number_Normalization_Rules.txt file to convert the Telephone Number to the Line URI format.

For example:
##
CDP 4 digits
##
(\d\d\d\d)
+16139675000;ext=$1

If the Telephone Number is normalized to the Line URI format, you can use the "Click to Call" feature to show the caller's user name when the Address Book Service is available.

Appendix Abbreviations

ACD
Automatic Call Distribution

AD
Active Directory

AML
Application Module Link

ATS
Activity Tracking System

AUX
Auxiliary

B2BUA
Back 2 Back User Agent

BCC
Basic Client Configuration

BRSC
Basic Rate Signaling Concentrator

CAST
Customer Assurance and Serviceability Test

CCMS
Contact Center Manager Server

CCR
Customer Controlled Routing

CDP
Coordinated Dialing Plan

CDR
Call Detail Recording

CNDP
Calling Number Dialing Plan

CRL
Certificate Revocation List

CS
Communication Server

CSTA
Computer Supported Telecommunications Applications

DC
Domain Controllers

DIDN
Direct Inward Dial Number

DMI
Desktop Management Interface

DORG
Display Call Originator Information

DRAM
Dynamic Random Access Memory

DN
Directory Number

DNIS
Dialed Number Identification Services

EC
Enterprise Configurator

EMS
Enterprise Multimedia Systems

EPROM
Erasable Programmable Read-Only Memory

FS
Feature Specification

FQDN
Fully Qualified Domain Name

GC
Global Catalog

GNTS
Global Network Technical Support

HLCL
Home Local number

HLOC
Home Location Code

HNTN
Home National number

IP
Internet Protocol

IPSec
Secure Internet Protocol

IVR
Interactive Voice Response

LDAP
Lightweight Directory Access Protocol

LSC
Local Steering Code

MISP
Multipurpose ISDN Signaling Processor

MCM
Multimedia Convergence Manager

MLS
Meridian Link Services

MMC
Microsoft Management Console

MNM
Meridian Network Management

MSDL
Multi-purpose Serial Data Link

MWI
Message Waiting Indicator

NAS
Nortel Application Switch

NCR
Number of Call Registers

NPA
Numbering Plan Area

NPI
Numbering Plan Index

NRS
Network Routing Service

NRSM
Network Routing Service Manager

OC
Office Communicator

OCS
Office Communications Server

P
Pentium

PEM
Privacy Enhanced Mail

PSTN
Public Switched Telephone Network

PRD
Product Requirements Document

RCC
Remote Call Control
Provides full Microsoft Office integration of telephony to control business-grade telephony phones from within Microsoft Office applications, as well as support for a standards-based CTI interface defined by the TR/87 protocol.

RDB
Route Data Block

RTP
Real-Time Transport Protocol

SA
Subscriber Access

OR

SA
StrongARM

SDP
Session Description Protocol

SIP CTI
Session Initiation Protocol Computer Telephony Integration
The SIP CTI (TR/87) protocol is on the Communication Server 1000 Signaling Server. TR/87 is the specification that OC 2007 uses to implement phone integration throughout the suite of Microsoft Office applications.

SPN
Special Number

SPS
SIP Proxy Server

SRS
SIP Redirect Service

sRTP
Secure Real-Time Transport Protocol

TLSV
Telephony Services

TN
Terminal Number

TON
Type of Number

UEXT
Universal Extension

URI
Uniform Resource Identifier

VIP
Virtual Internet Protocol

VoIP
Voice over Internet Protocol

VTRK
Virtual Trunk

XPEC
Expanded Peripheral Equipment Controller Pack

ZBD
Zone Based Dialing

Nortel Communication Server 1000

Nortel Converged Office Fundamentals — Microsoft Office Communications Server 2007

Release: 6.0
Publication: NN43001-121
Document revision: 03.09
Document release date: 1 February 2010

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com