Nortel Communication Server 1000

Nortel Converged Office Fundamentals

NN43001-525

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Sourced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Revision history

May 2007

Standard 01.01. This document is issued to support Nortel Communication Server 1000 Release 5.0. This document is renamed *Nortel Converged Office Fundamentals* (NN43001-525) and contains information previously contained in the legacy document, now retired: *Nortel Converged Office Implementation Guide* (553-3001-025).

December 2006

Standard 9.00. This document is up-issued to reflect changes in technical content and to address the following CRs:

- Q01298206,
- Q01501375

October 2006

Standard 8.00. This document is up-issued to reflect changes in technical content.

July 2006

Standard 7.00. This document is up-issued to reflect changes in technical content and to address the following CRs:

- Q01363480
- Q01377376

June 2006

Standard 6.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.

April 2006

Standard 5.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.

January 2006

Standard. 4.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.

January 2006

Standard 3.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.

January 2006

Standard 2.00. This document is up-issued with corrections related to CS 1000 Release 4.5 content.

December 2005

Standard 1.00. This document is a new NTP. It was created to support the new Nortel - Microsoft® Office Live Communications Server Converged Office project.

Contents

Procedures

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.

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

This document describes the various elements and processes involved in the Nortel - Microsoft® Office Live Communications Server Converged Office project to support the CS 1000 platform.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information about other products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Note: When you upgrade software, memory upgrades might be required on the Signaling Server, the Call Server, or both.

Intended audience

This document is intended for individuals who plan and configure the Nortel CS 1000 and Microsoft® Office Live Communications Server 2005 interworking.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)

The following systems are referred to generically as "Small System":

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000S (CS 1000S)

The following systems are referred to generically as "Large System":

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *New in This Release* (NN43001-115)
- *Transmission Parameters* (NN43001-282)
- *Signaling Server: Installation and Commissioning* (NN43001-312)
- *IP Peer Networking: Installation and Commissioning* (NN43001-313)
- *Features and Services* (NN43001-106)
- *Software Input/Output: Maintenance* (NN43001-711)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (NN43011-310)

- *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000S: Installation and Commissioning* (NN43031-310)
- *Communication Server 1000E: Installation and Configuration* (NN43041-310)

Microsoft® Documentation

Before you read this document, Nortel strongly recommends that you refer to the companion document, *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available on the Microsoft® web site:

www.microsoft.com

On the Microsoft® web site, go to the Downloads page. On the Downloads page, search on Office Communicator 2005. On the results page, select the Office Communicator 2005 Planning and Deployment Guide link.

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

http://www.nortel.com/

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Contents

This section contains information about the following topics:

Product Description

The multimedia strategy of many CS 1000 customers is based on deploying the Microsoft® Office Communicator soft clients and Live Communications Server. This strategy enables the introduction of multimedia capabilities using popular instant messenger (IM) clients without the need to install and support additional desktop software.

The Nortel Converged Office feature combines the business-grade telephony of the Communication Server 1000 with the real-time multimedia communication and the remote call control provided by Microsoft® Office Live Communications Server 2005 and Microsoft® Office Communicator 2005 products.

Technical Description

Nortel Converged Office is defined by the following two components:

- **Remote Call Control with Session Initiation Protocol (SIP) Computer Telephone Integration (CTI) TR/87** 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.

- **Telephony Gateway and Services** provides a basic SIP Telephony Gateway for connectivity between Private and Public Telephony networks and Live Communications Server 2005 clients.

Nortel offers a unique value with these two components by providing its telephony services to Office Communicator 2005 clients—in addition to providing connectivity between the Microsoft® Live Communications Server and the Nortel telephony network.

Release 5.0 enhancements

The Nortel Converged Office Solution supports the following enhancements for Release 5.0:

- **Do Not Disturb:** The "Do Not Disturb" feature is now offered through SIP CTI.

- **Video Calls:** Video calls are supported in the Microsoft Office Communicator to Office Communicator Session Initiation Protocol (SIP) Gateway call scenario. In Release 4.5, video calls were supported for SIP CTI only.

- **Transport Layer Security (TLS):** Both SIP Gateway and SIP CTI can now use TLS for signaling and Nortel’s Multimedia Convergence Manager (MCM) has been updated to support TLS.

  TLS provides secure calls from Office Communicator to the CS 1000 call server.

  TLS provides call signaling security between the Live Communications Server, the CS 1000 call server, and the SIP Proxy Server (SPS).

- **RFC2833:** DTMF digits dialed from Office Communicator or an IP telephone on the CS 1000 are now sent using the RFC2833 standard.

- **SIP Proxy Server (SPS):** The Converged Office Solution can now work with either the SPS or SIP Redirect Server (SRS).

ATTENTION

In this document, the use of the term Network Routing Service (NRS) implies both SPS and SRS.

NRS for CS 1000 Release 5.0 software is offered in two versions: a SIP Proxy NRS and a SIP Redirect Server NRS. For more information on NRS/SPS/SRS, refer to *Network Routing Service Installation and Commissioning* (NN43001-564).

- **Domain Name Server (DNS):** The Signaling Server SIP Stack now supports DNS configuration. As a result, the Host Table is not used for SIP CTI functionality in Release 5.0.

- **Enhanced Security:** SIP CTI now has an option that only accepts TLS end points. This feature enhances security by ensuring that only authorized hosts with TLS certificates can control a particular telephone.

- **G.723:** Both G.711 20 ms and G.723 are now supported in the Office Communicator to Telephone call scenario.

The Nortel Converged Office Solution also introduces several user interface and serviceability MCM enhancements to support new features for Release 5.0.

Remote Call Control with SIP CTI (TR/87)

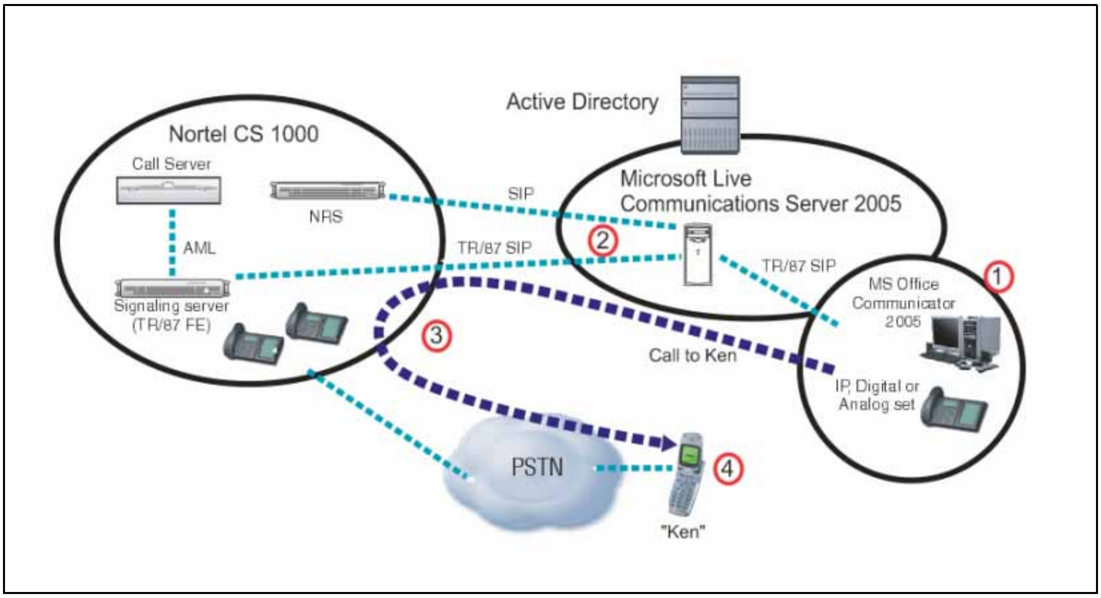
The Remote Call Control component (illustrated in Figure 1 "Remote Call Control with SIP CTI (TR/87)" (page 18)) provides convergence beyond the Microsoft® desktop IM client by moving into the full suite of Microsoft® Office applications and documents. By using Remote Call Control, enabled by the Office Communicator 2005 client, users can invoke many telephony features of the CS 1000 phones through the intuitive user interface of a PC client.

> ***Note:*** A feature which is not supported by the phone cannot be invoked through Office Communicator.

The example in "Remote Call Control with SIP CTI (TR/87)" (page 17) shows the following:

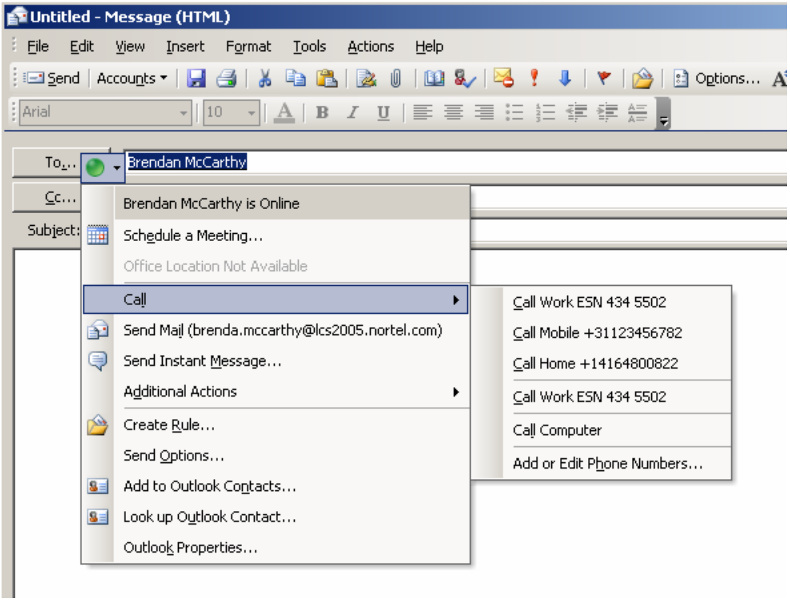
1. A user selects "Call" to Ken’s Mobile Phone number from his CS 1000 phone
2. The Live Communications Server sends a call request to the CS 1000
3. The CS 1000 sets up a call from the user’s phone to Ken’s mobile phone number
4. Ken answers his mobile phone and a media path is established between the two phones

Figure 1
Remote Call Control with SIP CTI (TR/87)



Users can, for example, operate the “Call” function from any contact icon visible within an e-mail or document in the Microsoft® Office suite (see the example in Figure 2 "Contact menu" (page 19)). This function is provided by support for the European Computer Manufacturer’s Association (ECMA) TR/87 protocol on the CS 1000 Signaling Server. TR/87 is the specification that Office Communicator 2005 uses to implement phone integration throughout the suite of Microsoft® Office applications.

Figure 2
Contact menu



To... Brendan McCarthy

The full set of business-grade telephony features available with CS 1000 phones is integrated with the Microsoft® Office Communicator client and can also be operated from a CS 1000 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 CS 1000 and Live Communications Server 2005 systems, the Office Communicator 2005 client compliments the voice communications between two users by offering the ability to add other media types, such as video, IM, file and application sharing to an existing voice call without the need to establish an independent session between users.

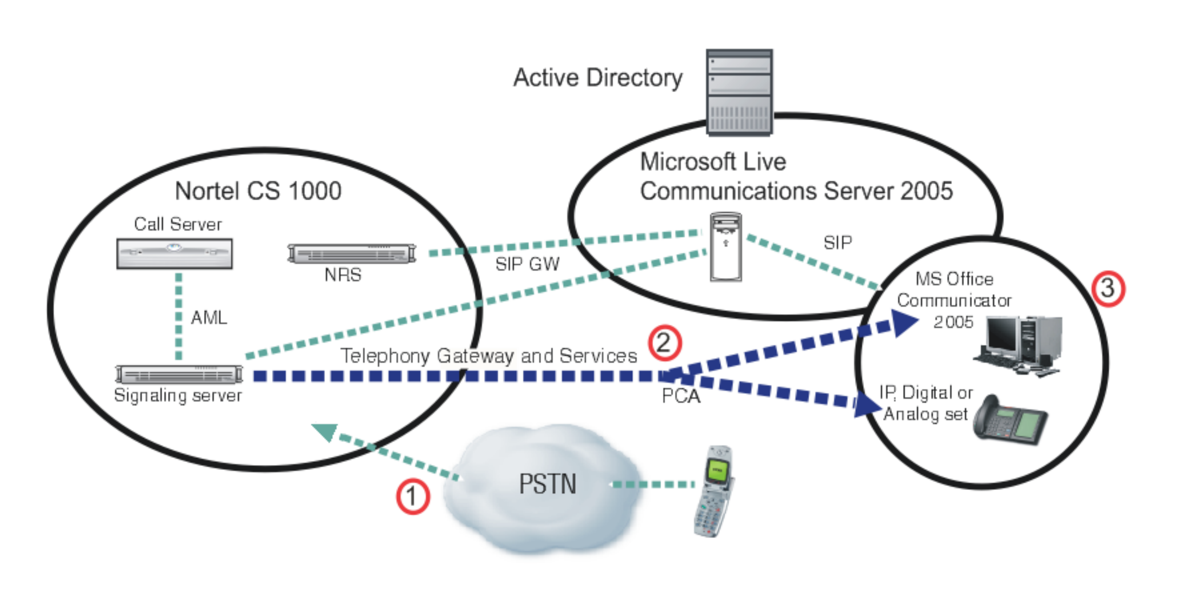
Telephony Gateway and Services

Using the Telephony Gateway and Services component, users can select Microsoft® Office Communicator 2005 as one of the clients they use when handling telephony calls. 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 the Microsoft® Office Communicator Client as a soft client.

This solution requires that a Personal Call Assistant (PCA) is configured on the CS 1000 for each user configured with this functionality. A phone is not required for configuration if Office Communicator is available to the user. The CS 1000 configured with the PCA 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.

Using the Telephony Gateway and Services component, Office Communicator 2005 can be configured as a Multiple Appearance Directory Number (MADN) member for users with the Personal Call Assistant (PCA) feature provided by CS 1000. With the PCA feature, calls to a user's phone number can be presented to both the desktop phone and to the Office Communicator 2005 client simultaneously. The user can then choose to answer on the device that makes the most sense at the time.

Figure 3
Telephony Gateway and Services



For 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 Office Communicator while traveling to locations that have network connectivity (for example, at hotels). Figure 3 "Telephony Gateway and Services" (page 20) illustrates the following example:

1. The CS 1000 system receives a PSTN call to the user's phone number
2. The CS 1000 uses the Personal Call Assistant (PCA) feature to provide simultaneous ringing to both the user's phone and the Office Communicator voice client
3. The user has the option of answering the call through the CS 1000 phone or the Office Communicator voice client

Consequently, users can be reached no matter where they are on the network and significant cost savings are incurred by using IP telephony through VPN access to their private network.

As part of the user’s telephony services, many features of incoming calls are available even when using Office Communicator as a telephony device. Features such as Call Forward No Answer, Unified Messaging, Call Detail Recording, and Attendant Recall are maintained within the CS 1000 system for calls presented to the Office Communicator.

Another key feature of Telephony Gateway and Services is the ability to access all of the telephony network resources using the Office Communicator client. Calls can originate from the Office Communicator client to the PSTN, phones, or services within the telephony network. Users can therefore 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 CS 1000 SIP Gateway with the Microsoft® Office Live Communications Server 2005 SIP gateway software.

Multimedia Convergence Manager

Nortel also introduces a software component called the Multimedia Convergence Manager (MCM) to ensure the proper interoperability between the two systems with respect to protocols, users, and phone numbers managed within the Microsoft® Active Directory®.

SIP CTI (TR/87) Protocol

The SIP CTI (TR/87) Front End (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.

> ***Note:*** Certain portions of the protocol are not supported at this time. Additional information about the SIP CTI (TR/87) protocol is available to Nortel partners upon request.

Feature operation

Contents

This section contains information about the following topics:

Introduction

This section describes the various features available to users of the Remote Call Control and Telephony Gateway and Services components.

ATTENTION

IMPORTANT!

Customers should **NOT** use their Microsoft® 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.

Remote Call Control functionality

This section provides an overview of the Remote Call Control feature functionality. Microsoft® uses the term Remote Call Control to describe the ability of Microsoft® Office Communicator 2005 to remotely control the features of the phones of an IP PBX, such as the CS 1000 from within the user interface of Office Communicator or other Microsoft® Office applications.

The Nortel Converged Office product supports Microsoft® Office Communicator Remote Call Control, which integrates of Live Communication Server multimedia capabilities (for example, application sharing, instant messaging, and video) with Nortel business-grade telephony through the CS 1000 system.

The Nortel Converged Office Solution is implemented through an open interface to ensure that any CS 1000 feature supported through Microsoft® Office Communicator is also accessible to applications from other vendors and application developers that support these interfaces.

Microsoft® Office Communicator 2005 features

This section provides an overview of the various Microsoft® Office Communicator 2005 features available through the Remote Call Control with SIP CTI component.

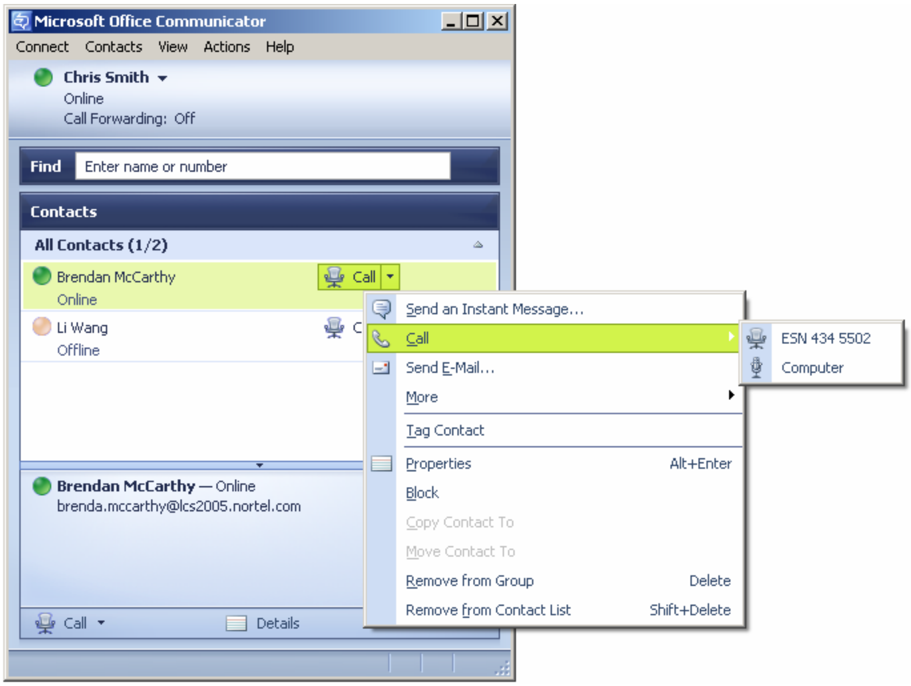
Make Call

Using the Make Call feature, accessible through the user interface of Office Communicator (see Figure 4 "Make Call From Contact" (page 25)), users can request that a call be made from their telephony device to a phone number. For example, a user can select the Call function associated with one of their contact icons to make a call from their CS 1000 phone to another user.

When a call is placed through Office Communicator, the default calling device can be either Phone or Computer (see Figure 18 "Default device option" (page 39)). If you select Phone, Remote Call Control is used to originate the call from the CS 1000 phone. If you select Computer, a SIP (or VoIP) call is originated from the PC itself using a headset or your computer's microphone and speakers.

> ***Note:*** Remote Call Control is only used for making calls if your default device in the Phones tab is set to Phone.

Figure 4
Make Call From Contact



The Make Call feature creates a new call and initiates a connection with the calling device. The Make Call feature assigns a ConnectionID to the calling device and returns it in positive acknowledgement. While establishing the connection with the calling device, the calling device may also be prompted to go off-hook (if necessary). When it does, either a call is placed to the called device, or the calling device is still in the process of dialing the called device.

The monitored device on-hook default path configuration setting defines whether the headset or hands-free operation is used. For phone types that do not support hands-free (M3905, i2001), it should be noted that in the absence of a headset, the speaker is used as the on-hook default path regardless of the on-hook default path configuration. Due to the absence of a microphone, only half-duplex is supported for the call.

If no speaker is available, Make Call is supported when the phone is off-hook.

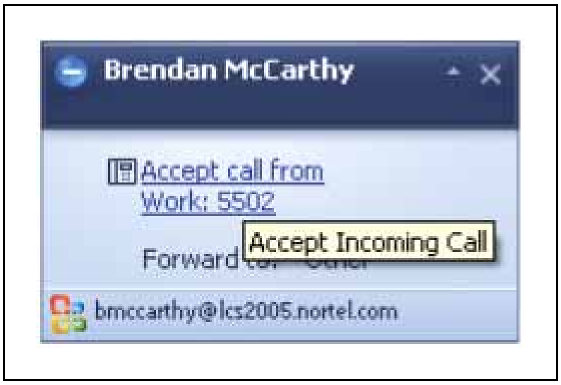
In the case of MADN, the MARP TN is used as the originating device. The Make Call service request can originate from a number of different user interfaces, such as the Office Communicator 2005 buddy list.

Answer Call

Using the Answer Call feature, a user can answer an incoming call to their CS 1000 phone by clicking an Accept call pop-up window (see Figure 5 "TR/87 Call Appearance pop-up window" (page 26)). A user may also start an instant message (IM) session with that caller by clicking the name of the caller in the window rather than accept the call.

For example, a user may receive an Accept call pop-up window, and click on the Accept call link to answer the call. If that same user is too busy to answer the call, they can click the name of the caller in the pop-up window to send the caller an instant message (for example: "Call you back in 10 minutes").

Figure 5
TR/87 Call Appearance pop-up window



The Answer Call service connects an alerting or queued call. This service is typically associated with devices that have attached speakerphone units and headset telephones to connect to a call using hands-free operation.

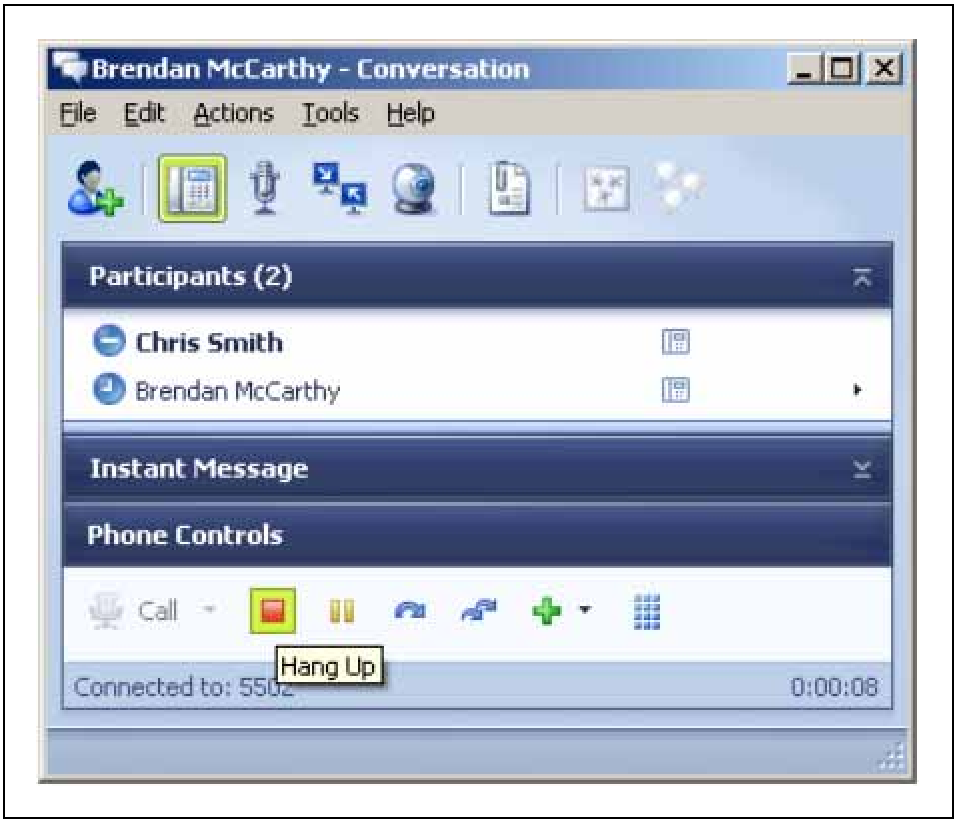
The monitored device on-hook default path configuration setting defines whether headset or hands-free operation is used. For phone types that do not support hands-free (M3905, i2001), note that in the absence of a headset, the speaker is used as the on-hook default path regardless of the on-hook default path configuration. Due to the absence of a microphone, this provides only half-duplex support for the call. If no speaker is available, Answer Call is not supported.

Where MADN is used, the MARP TN is used as the receiving device.

Clear Connection

Use Clear Connection (Release) to hang up from your soft client by clicking the Hang Up button on the user interface (see Figure 6 "Clear Connection UI window" (page 27)). You can also press the release button on your phone.

Figure 6
Clear Connection UI window



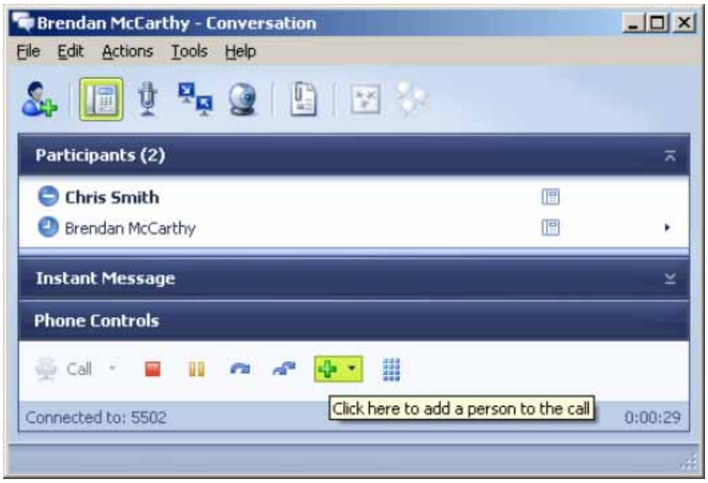
The Clear Connection service releases a specific device from a call. In the case of a two-party call, the call may be torn down. In the case of a conference call, a specific party may be removed from the conference.

The Clear Connection request is sent from the conversation dialog when a call is to be terminated from the client user interface. This is equivalent to pressing the release key on a phone keypad.

Conference Call

Using the Conference Call service, users can control a conference on their phone through their on-screen interface using Office Communicator 2005 (see Figure 7 "Conference Call UI window" (page 28)).

Figure 7
Conference Call UI window



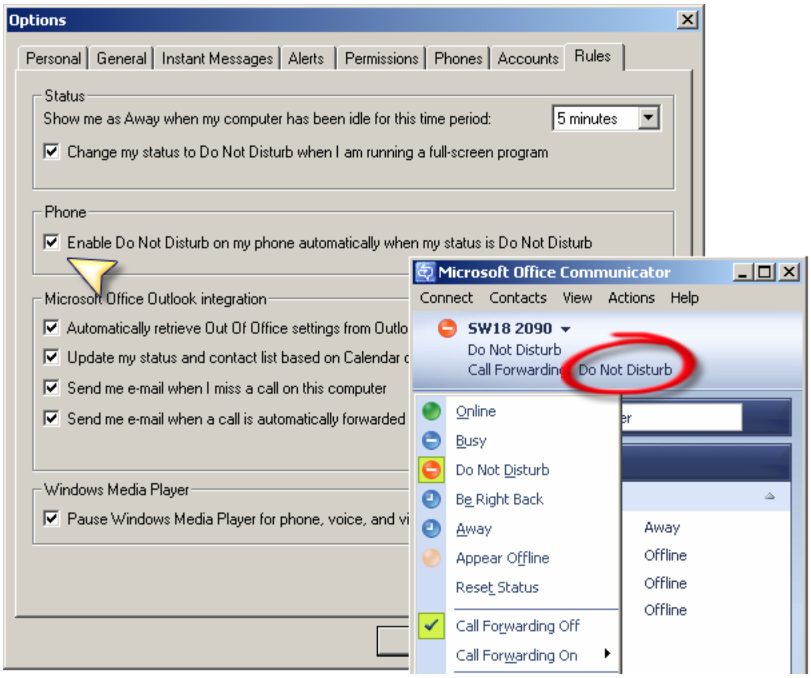
This service provides a conference of an existing held call and another active call at a conferencing device. The two calls are merged into a single call, and the two connections at the conferencing device are resolved into a single connection. The Connection IDs formerly associated with the conferenced connections are released, and a new Connection ID for the resulting connection is created. The existing held call may consist of two or more devices.

The use of the Conference Call service requires that an A03 or A06 key be configured on the TN where the CLS T87A resides. The conference service request is sent from a conversation dialog to add a caller to the existing call. These keys may be part of the default configuration.

Do Not Disturb

To enable the Do Not Disturb feature, the Make Set Busy key must be enabled on the phone and the “Enable Do Not Disturb” option must be selected in Office Communicator (see "Do Not Disturb" (page 28)). The Do Not Disturb feature enables the Make Set Busy key on a call by call basis. As a result, incoming calls are directed to a user’s voicemail or receive a busy signal.

Figure 8
Do Not Disturb



Status

Show me as Away when my computer has been idle for this time period: 5 minutes

☑ Change my status to Do Not Disturb when I am running a full-screen program

Phone

☑ Enable Do Not Disturb on my phone automatically when my status is Do Not Disturb

Microsoft Office Outlook integration

☑ Automatically retrieve Out Of Office settings from Outlo

☑ Update my status and contact list based on Calendar d

☑ Send me e-mail when I miss a call on this computer

☑ Send me e-mail when a call is automatically forwarded

Windows Media Player

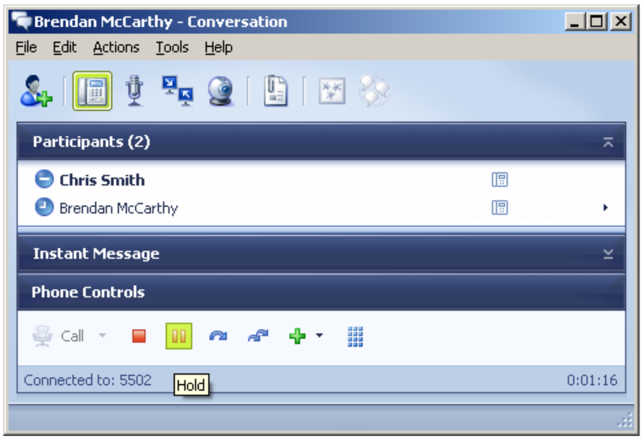
☑ Pause Windows Media Player for phone, voice, and vi

SW18 2090
Do Not Disturb
Call Forwarding Do Not Disturb

Hold Call

The Hold Call service places a connected call on hold at the same device. This service interrupts communication for an existing call at the device. Essentially, this is equivalent to pressing the Hold key on a phone. In this case, however, the hold button is part of the Office Communicator 2005 interface (see Figure 9 "Call Hold UI window" (page 29)).

Figure 9
Call Hold UI window



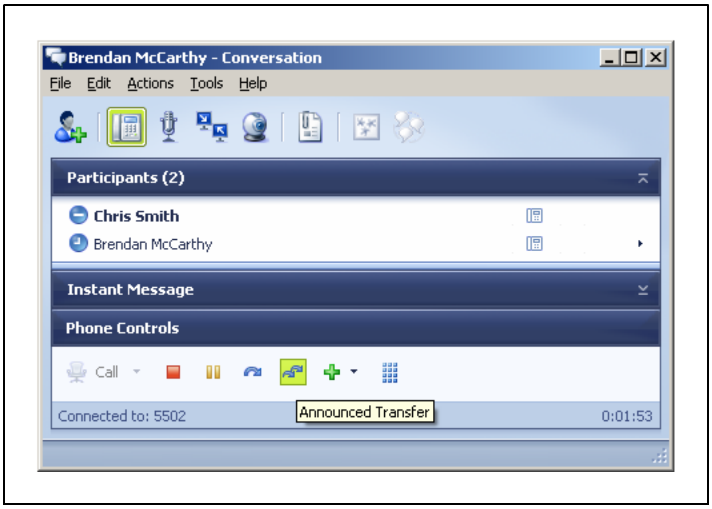
Connected to: 5502 0:01:16

Consistent with the behavior when initiated from a phone, a call on hold cannot be disconnected. The Hold Call service request is sent from the conversation dialog when a call is put on hold.

Transfer Call

The Transfer Call service transfers a call held at a device to an active call at the same device. The held and active calls at the transferring device are merged into a new call. For example, you receive a call that might be better handled by a coworker. By clicking the Transfer Call button, the caller is placed on hold while you call the number of the coworker to whom you are transferring the call.

Figure 10
Transfer Call UI window



The connections of the held and active calls at the transferring device become Null and their ConnectionIDs are released (in other words, the transferring device is no longer involved with the call).

The use of the Transfer Call feature requires that a TRN key be configured on the TN where the CLS T87A resides. This key may be part of the default set configuration.

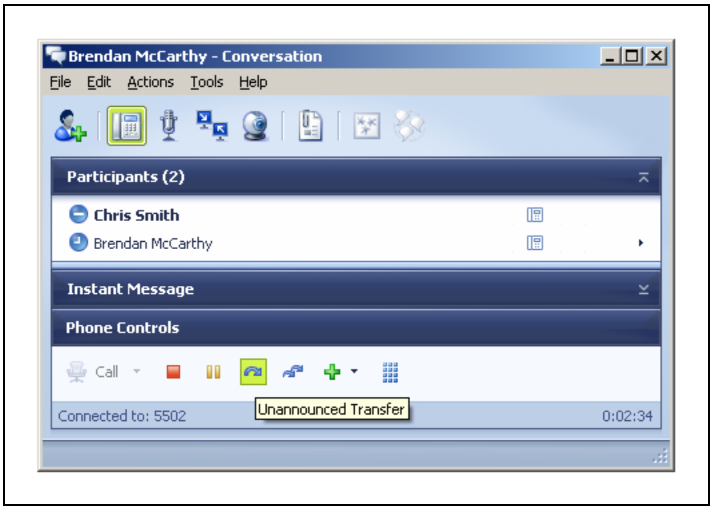
The Transfer Call service request is initiated from the conversation dialog when a call is to be transferred to another DN through the use of a consultation call.

Single Step Transfer Call

The Single Step (Blind) Transfer Call service (also known as Unannounced Transfer, see Figure 11 "Single Step Transfer UI window" (page 31)) transfers an existing connection at one device to another device. This transfer is performed in a single step to prevent the device performing the transfer from placing the existing call on hold.

The transferring connection may be in the Alerting, Connected, Failed, Held, or Queued state.

Figure 11
Single Step Transfer UI window



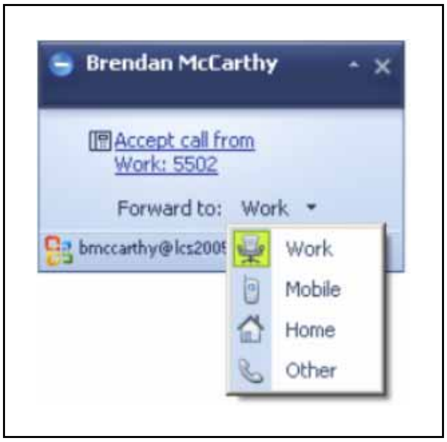
The use of this feature requires that a TRN key be configured on the TN where the CLS T87A resides.

The single step transfer call service request is initiated from the conversation dialog when a call is to be transferred directly to another DN. This is equivalent to the blind transfer function available from a phone.

Deflect Call

Using the Deflect Call feature, users can forward an incoming call in its ringing state to a number of their choosing. For example, a user may have their work phone number programmed in Office Communicator so it is in the drop-down list in the pop-up window (see Figure 12 "Deflect Incoming Call" (page 32)).

Figure 12
Deflect Incoming Call



Brendan McCarthy

Accept call from
Work: 5502

Forward to: Work

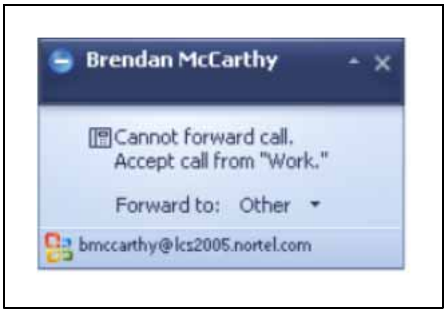
bmccarthy@lcs2005

Using the Deflect Call service, a user can divert a call to another destination that may be inside or outside the switching subdomain.

The Deflect Call service request is sent from the incoming call notification pop-up when an alternative destination is selected. This function is currently not available from the phone, and can be accessed only through the Office Communicator 2005 client. The deflect call service request is also used to implement the location-based forwarding service from Office Communicator 2005.

The deflect service request is supported for all call types. The deflect behaves as though the called device was configured with call forward to the target number. If a deflect fails, the call remains with the currently alerting device and the user is notified of the failure (see Figure 13 "Call Deflect Failure" (page 32)).

Figure 13
Call Deflect Failure



Brendan McCarthy

Cannot forward call.
Accept call from "Work."

Forward to: Other

bmccarthy@lcs2005.nortel.com

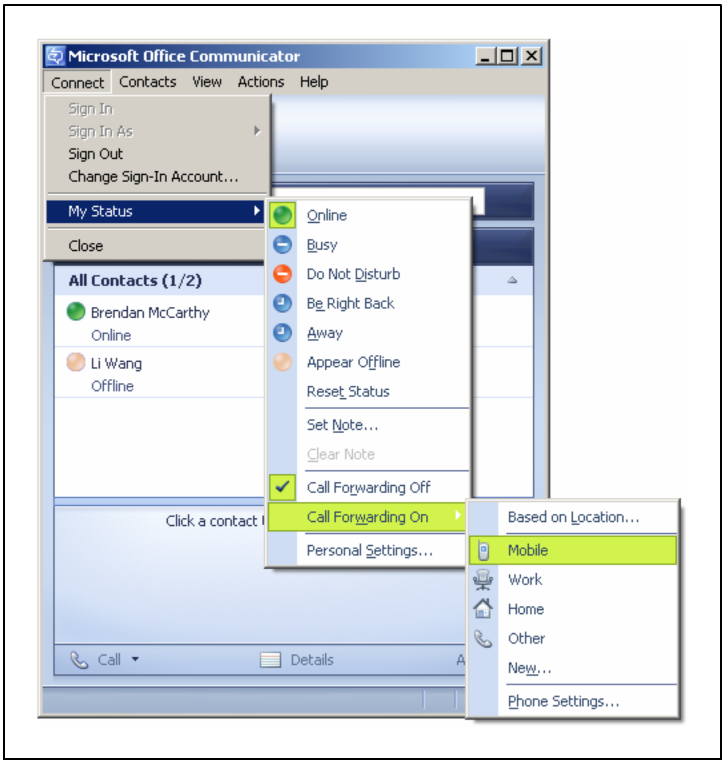
Call Forwarding

There are two methods of call forwarding. Users can forward all calls by selecting Call Forwarding On (see Figure 14 "Call Forwarding" (page 33)), and then select the number to which they want to forward calls.

The Call Forwarding service allows the computing function to control the forwarding feature at a specified device based on user-defined conditions. The forwarding feature is used to redirect calls that arrive at a specified device to an alternative destination.

Only one user-specified setting (the forwarding type and forward-destination combination) can be changed per service invocation.

Figure 14
Call Forwarding



The Call Forwarding service request is sent from Office Communicator 2005 when the call forwarding option is enabled. You can enable this option from a number of different locations within Office Communicator 2005. This function is equivalent to pressing the CFWD key on a phone.

This feature has a limitation. Refer to the section “Feature Limitations” for details.

WARNING

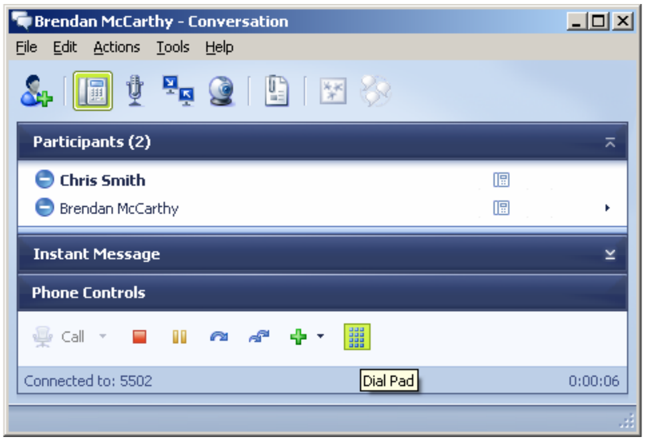
Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself. When Office Communicator is active and controlling a DN, all Call Forward changes should be made through Office Communicator to ensure that it is in the correct state.

When a user signs into Live Communications Server from their Office Communicator client, the forwarding status saved within Office Communicator overrides any forwarding status that may have been set from the phone. For example, if forwarding is off within Office Communicator, it is turned off following sign in, regardless of the phone forwarding status at the time.

Generate Digits

The Generate Digits feature provides users with a keypad to enter phone numbers on their computer screen (see Figure 15 "Generate Digits" (page 34)).

Figure 15
Generate Digits



The Generate Digits service causes a series of digits to be sent on behalf of a connection in a call. The digits may be sent in the form of Dual-tone Multifrequency (DTMF) tones. This service also:

- supports optional parameters to control digit generation
- generates end-to-end information that is to be sent to a device in a call (for example, not to address or select a device)
- does not affect the state or progress of a call
- supports analog, digital, and IP phone types and all trunk types

Note: In Release 5.0, if both ends support RFC2833, the digits are sent out-of-band.

There is one scenario, however, that is not supported: when the originating and terminating endpoints are IP sets. At this time, no known usage scenarios exist where this service is required between two IP sets.

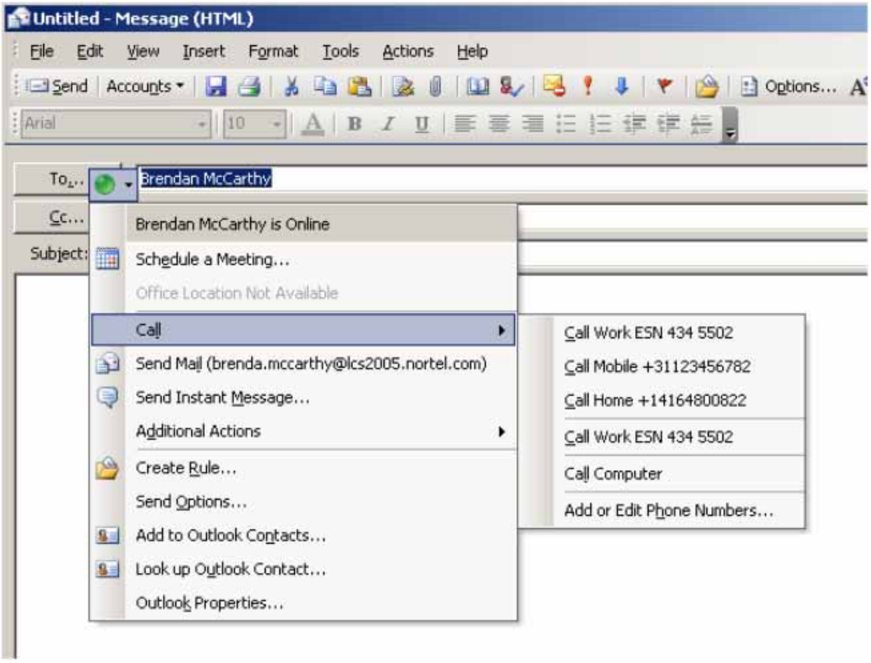
Within a service request, the characters 0 to 9, the pound sign (#), and the asterisk (*) are supported. You can insert a pause into the dialstring by using a comma (,). Up to 31 characters to be dialed are supported within a single service request.

The Generate Digits service request is sent to Office Communicator 2005 from the toolbar on the conversation dialog. This function is equivalent to pressing digits on the dial pad of a phone during a call (for example, to access voice mail or a conference bridge).

Contact Icons

The Remote Call Control component also provides, through the use of contact icons, the ability to call users directly from various Microsoft® Office applications (see Figure 16 "Contact icon" (page 35)) such as Outlook, Excel, and Word.

Figure 16
Contact icon



Telephony Gateway and Services functionality

The ability to connect between computers and phones is not natively provided by Microsoft® Office Live Communications Server 2005; however, the Telephony Gateway and Services component enables this functionality using the SIP gateway and Multimedia Convergence Manager (MCM) application.

With Telephony Gateway, users can choose how calls are made and received. For outgoing calls, users can make a call from their Office Communicator soft client instead of their CS 1000 phone. Incoming calls can be handled in one of two ways: through the computer, with Office Communicator, or through a phone.

CS 1000 Services

Many of the features provided by CS 1000 to traditional telephones are extended to Office Communicator clients configured with the Personal Call Assistant (PCA). For example, calls that remain unanswered may be forwarded using the "call forward - no answer" feature.

PCA

If a user wants to use the Office Communicator soft client for some of their voice calls using the Telephony Gateway and Services, a PCA 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 have configured with the same DN.

For outgoing calls from the Office Communicator, the user must have at least one TN configured on a CS 1000 Call Server. The MCM locates the Call Server associated with a user by their numbering plan entry in the NRS. This generates calls from Office Communicator clients using 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.

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 PCA when it is the only TN for the user.

With PCA and Remote Call Control configured, users receive a pop-up window for the incoming call to their phone and a second pop-up for their computer. Users can then choose the most convenient way to answer an incoming call.

MCM

Multimedia Convergence Manager (MCM) serves a number of functions, including:

- translation between telephony phone numbers and user IDs within Active Directory
- authentication of user phone numbers
- Numbering Plan normalization
- protocol interworking
- redundant connections to the CS 1000 network components (SRS, SPS, and redundant Signaling Servers)

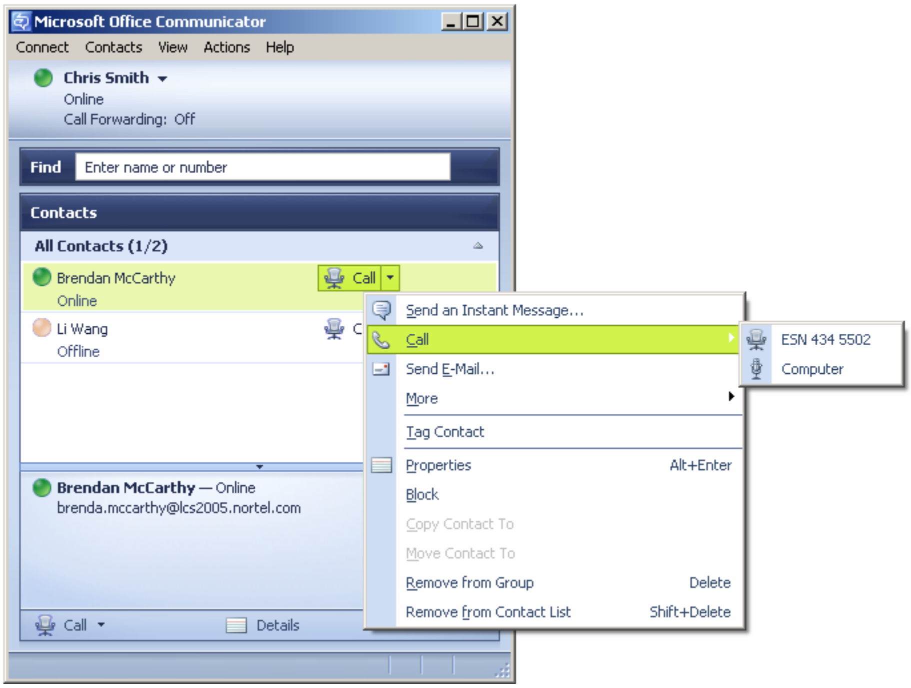
Microsoft® Office Communicator 2005 features

This section provides an overview of the various Microsoft® Office Communicator 2005 features available through the Telephony Gateway and Services component.

Make Call

Using the Make Call feature, available from the user interface of Office Communicator (see Figure 17 "Make Call From Contact" (page 38)), users can request that a call be made from their telephony device to a phone number. For example, a user can select the Call function associated with one of their contact icons to make a call from their CS 1000 phone to another user.

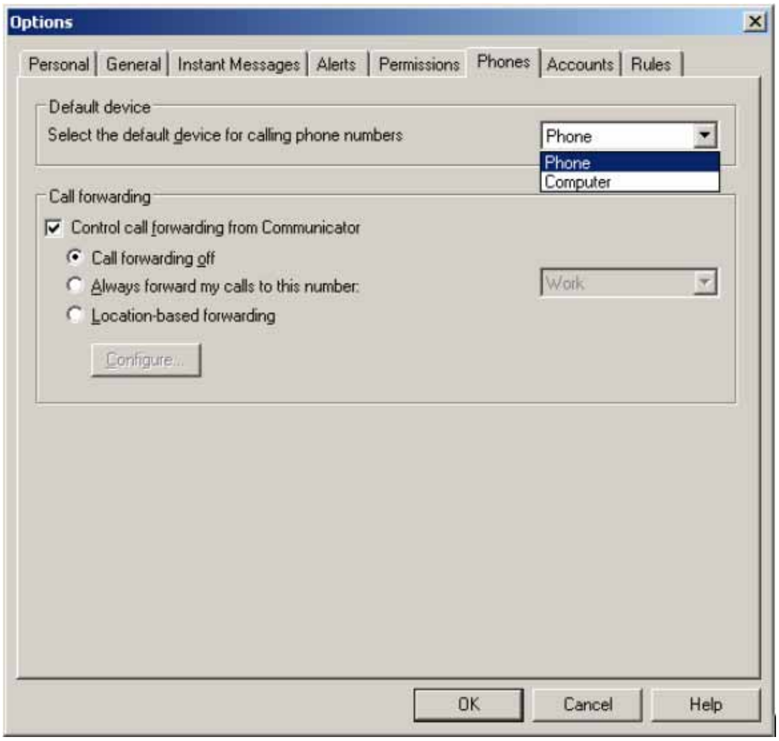
Figure 17
Make Call From Contact



When a call is placed through Office Communicator, the default calling device can be either Phone or Computer. If you select Phone, Remote Call Control is used to originate the call from the CS 1000 phone. If you select Computer, a SIP (or VoIP) call is originated from the PC itself using a headset or your computer's microphone and speakers.

Set this option by selecting the **Actions > Options > Phones** tab (see Figure 18 "Default device option" (page 39)).

Figure 18
Default device option



Default device

Select the default device for calling phone numbers: Phone

Phone
Computer

Call forwarding

☑ Control call forwarding from Communicator

● Call forwarding off

○ Always forward my calls to this number: Work

○ Location-based forwarding

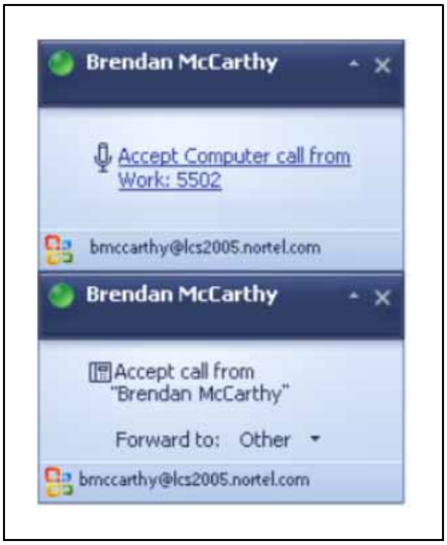
Configure...

Answer Call

Using the Answer Call feature, the user can answer an incoming call in one of two ways: through Remote Call Control of the CS 1000 phone clicking an Accept call pop-up window (as shown in the second pop-up in Figure 19 "PCA Call Appearance pop-up window" (page 40)), or through their computer.

With PCA enabled, users can accept calls to their computer. Selecting the Accept Computer call pop-up with the microphone icon allows users to answer the call as a computer, or VoIP, call on the PC itself.

Figure 19
PCA Call Appearance pop-up window



Brendan McCarthy

Accept Computer call from Work: 5502

bmccarthy@lcs2005.nortel.com

Brendan McCarthy

Accept call from "Brendan McCarthy"

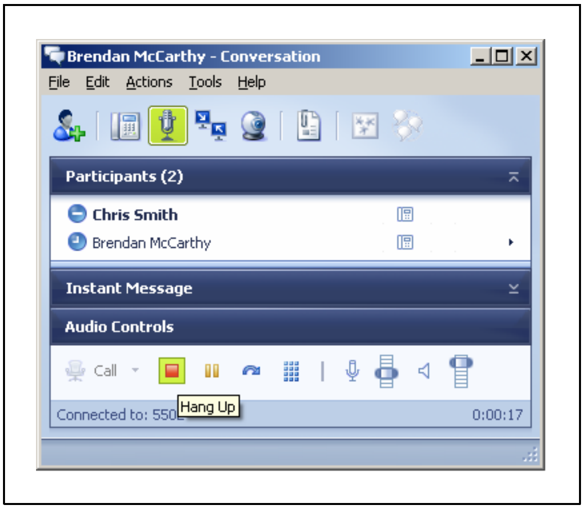
Forward to: Other

bmccarthy@lcs2005.nortel.com

Clear Connection

Using the Clear Connection (Release) feature, users can hang up from their soft client by clicking the Hang Up button (see Figure 20 "Clear Connection window" (page 40)).

Figure 20
Clear Connection window



Chris Smith

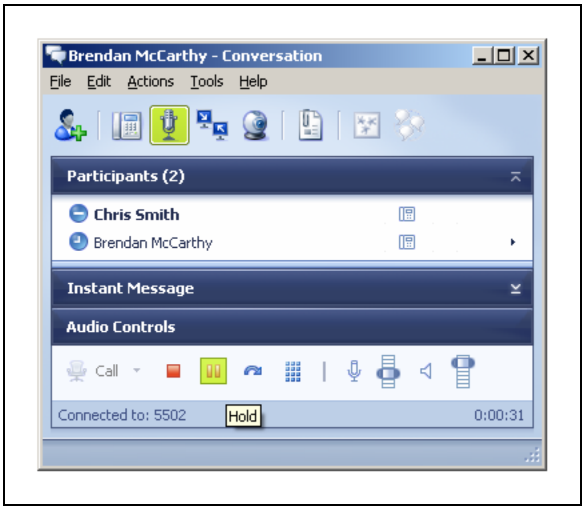
Brendan McCarthy

Connected to: 550 0:00:17

Hold Call

The Hold Call feature places a connection on hold at the same device. Clicking the Hold button once (see Figure 21 "Call Hold window" (page 41)) puts the call on hold and clicking the Hold button again restores the audio connection.

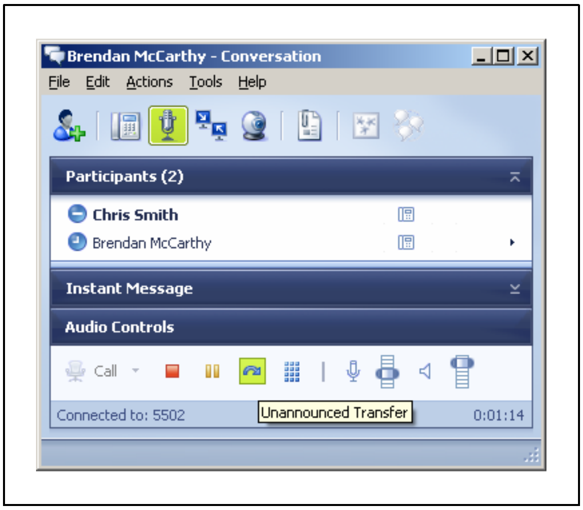
Figure 21
Call Hold window



Single Step Transfer Call

The Single Step (Blind) Transfer Call feature transfers an existing connection at one device to another device in a single step. The device performing the transfer does not place the existing call on hold before transferring the connection.

Figure 22
Single Step Transfer window



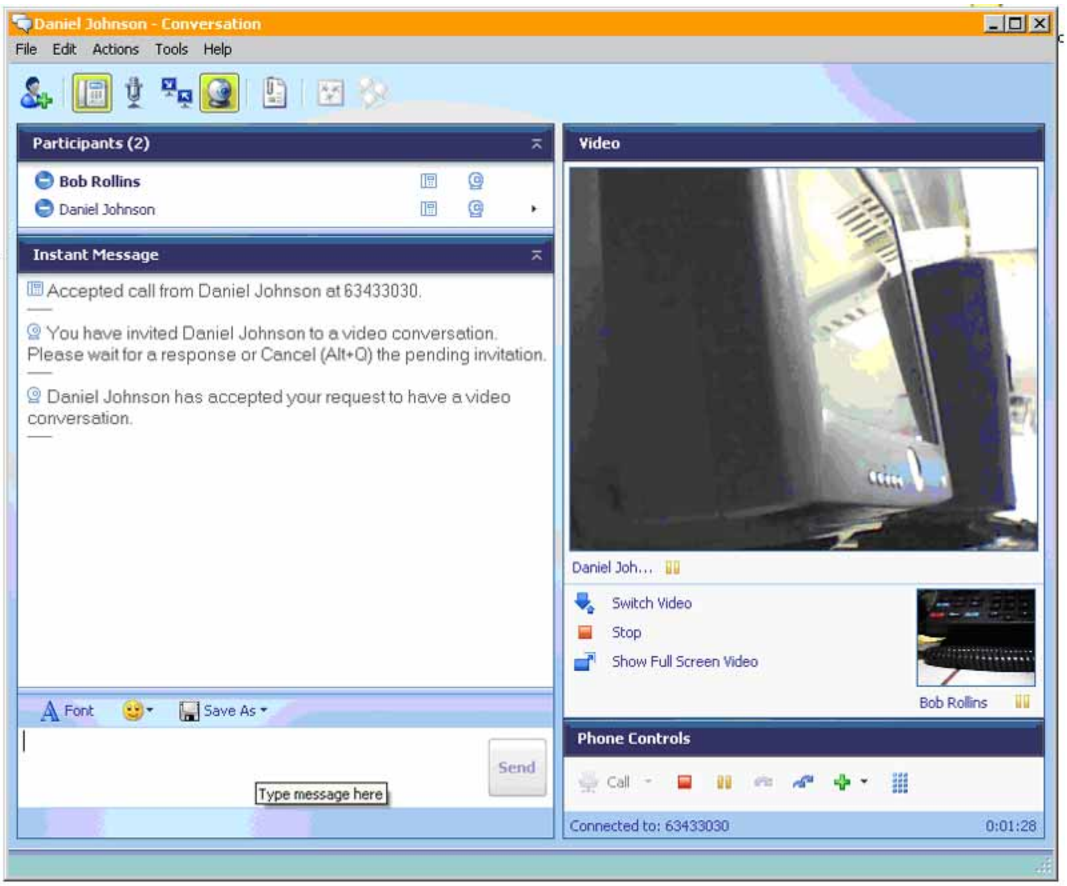
For Office Communicator SIP calls, Office Communicator 2005 supports "blind" no-hold transfers exclusively. For example, if computer A establishes a voice conversation with phone B, and computer A then transfers the call to phone C, the call is immediately presented to phone C.

Computer A cannot retrieve the call or talk to phone C, as the call releases from computer A when the call is presented to phone C. If phone C is busy or unavailable, the call terminates.

Establishing Multimedia Sessions

All Live Communications Server multimedia features are immediately available for use on the corresponding call dialog when the phone number for an active call is resolved to a Live Communications Server user identity by Office Communicator. This applies to both Remote Call Control and Telephony Gateway and Services calls.

Figure 23
Multimedia session



Accepted call from Daniel Johnson at 63433030.

You have invited Daniel Johnson to a video conversation. Please wait for a response or Cancel (Alt+Q) the pending invitation.

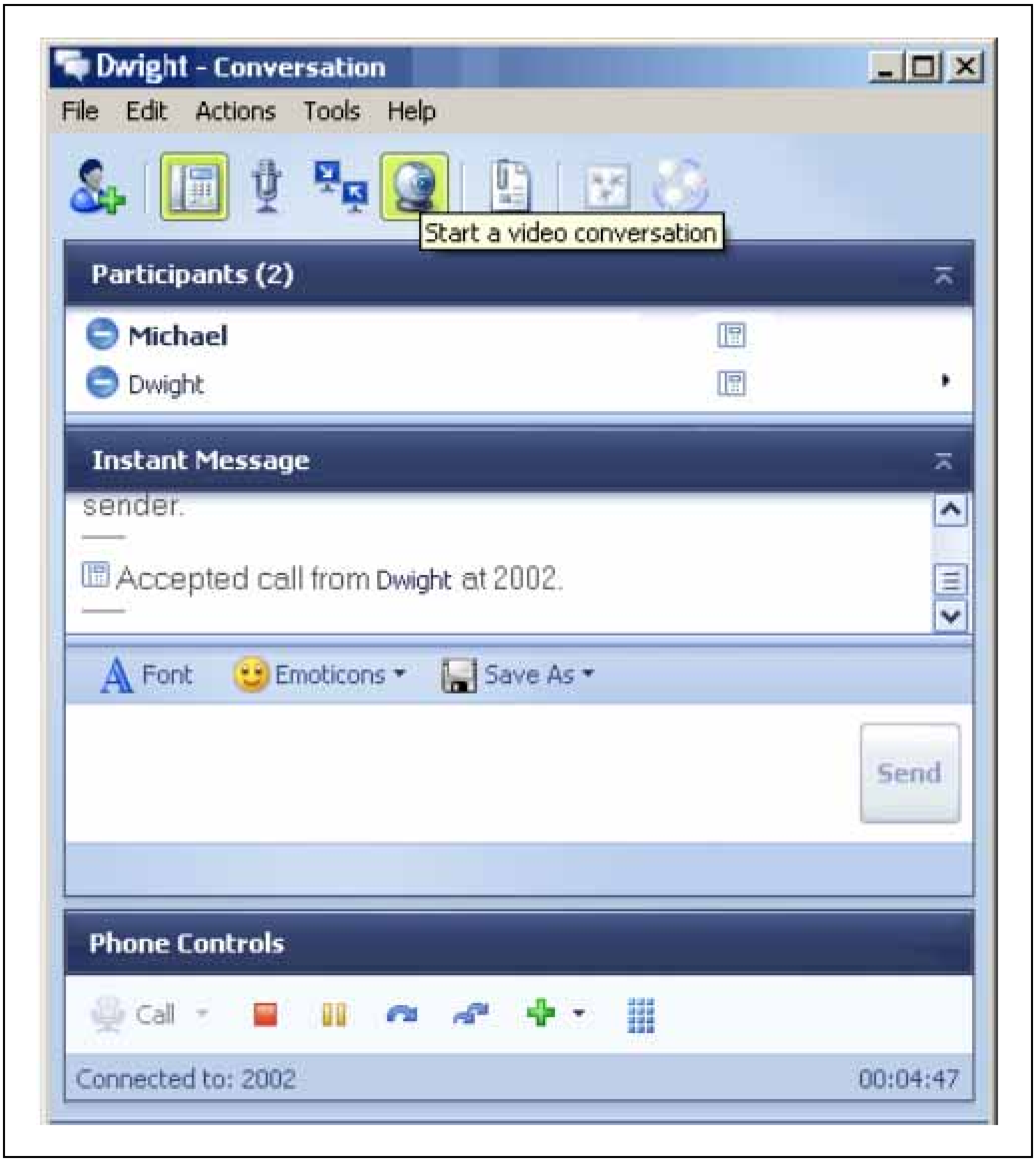
Daniel Johnson has accepted your request to have a video conversation.

For information on the process used to map phone numbers to Live Communications Server user identities from either SIP or TR/87 call events, refer to "Normalizing phone numbers" (page 158).

Video conferencing

Video is supported for SIP CTI Office Communicator to SIP CTI Office Communicator calls or SIP Gateway Office Communicator to SIP Gateway Office Communicator calls.

Figure 24
Starting a video conversation



sender.

Accepted call from Dwight at 2002.

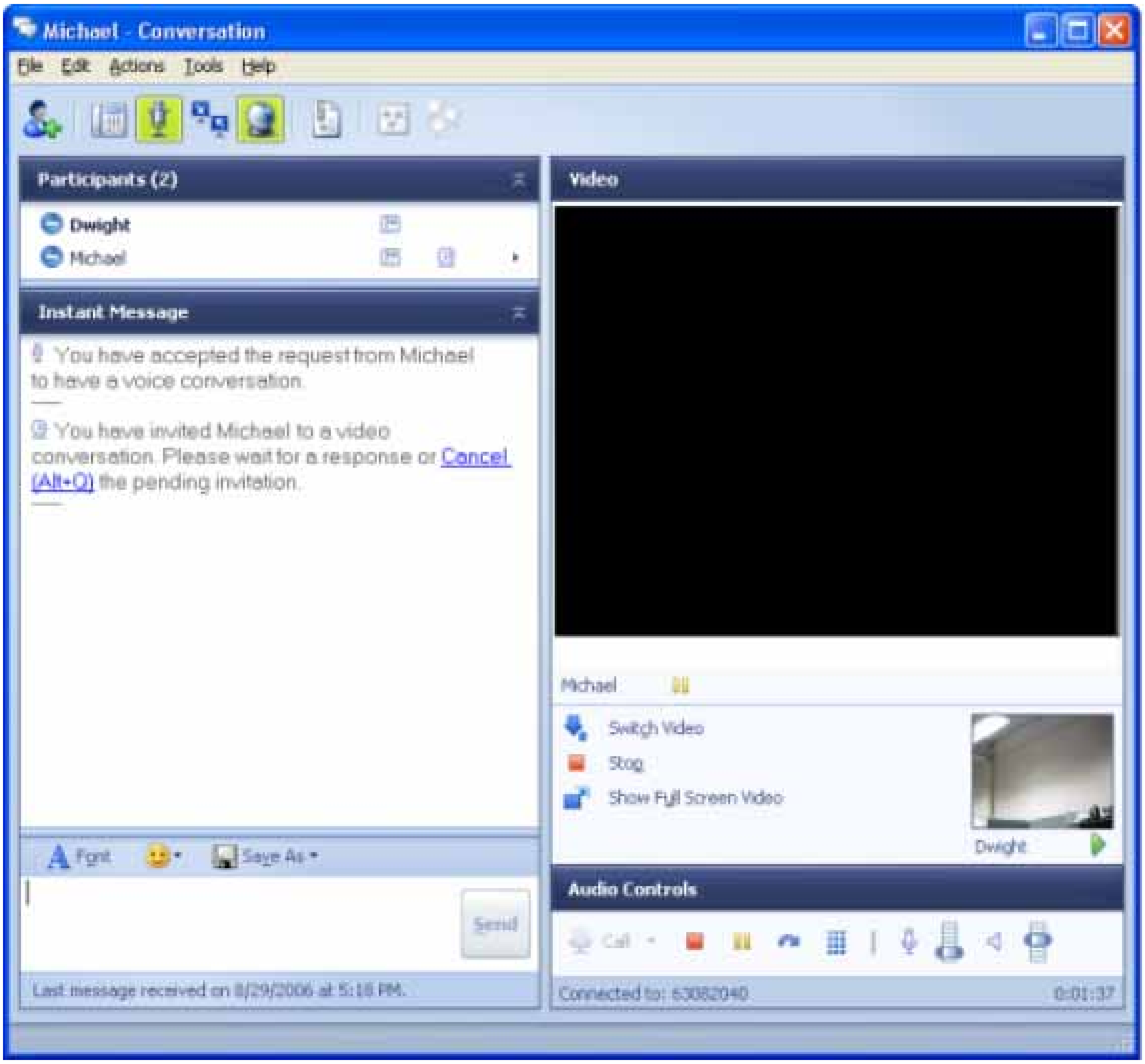
Connected to: 2002

00:04:47

By using Office Communicator as the actual phone instead of controlling the desktop phone, video calls are established by first establishing an active audio call between Office Communicator clients. Both endpoints must be using Office Communicator as a softphone (SIP Gateway). Once the audio call has been established, click the camera icon (see Figure 24 "Starting a video conversation" (page 43)) to initiate a video call. The following screen appears (Figure 25 "Establishing video" (page 44)):

> ***Note:*** A SIP Gateway Office Communicator to SIP Gateway Office Communicator call must be established as an audio call only to a phone number before adding video.

Figure 25
Establishing video



You have accepted the request from Michael to have a voice conversation.

You have invited Michael to a video conversation. Please wait for a response or Cancel (Alt+Q) the pending invitation.

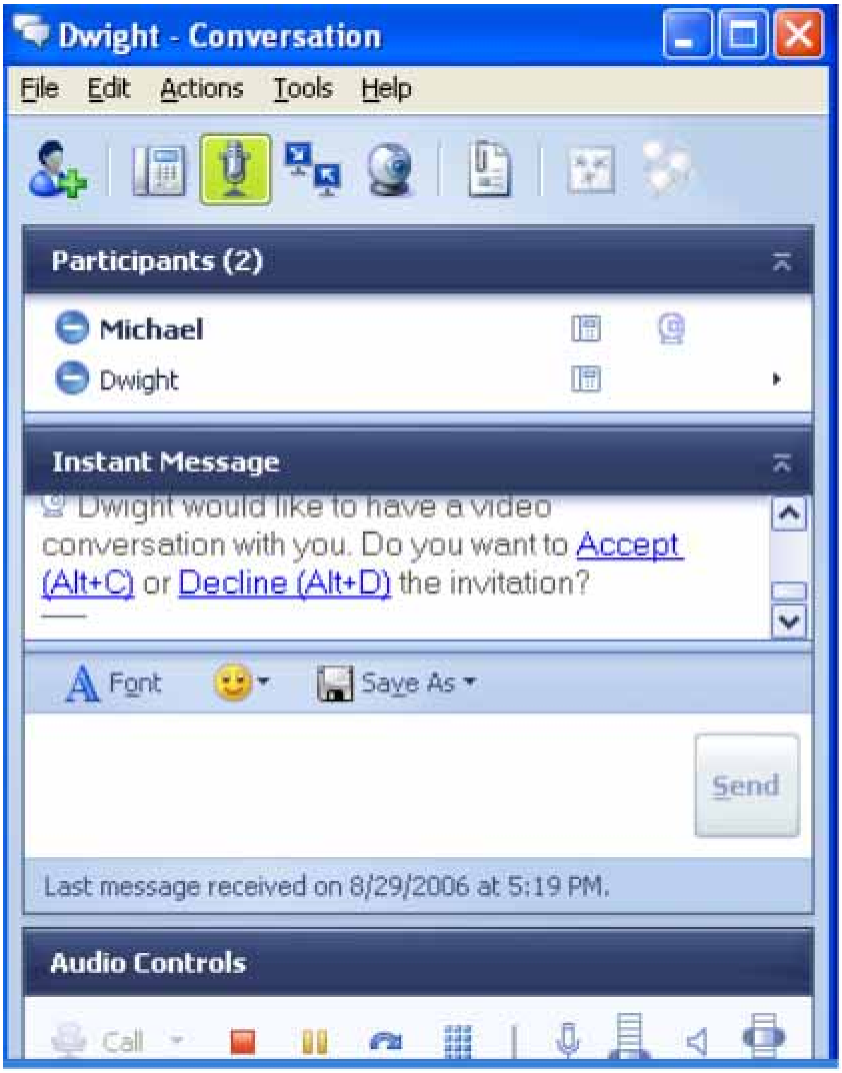
Last message received on 8/29/2006 at 5:18 PM.

Connected to: 63082040 0:01:37

In this example, you have invited Michael to a video conference, and are waiting for a reply. At this point, the main screen is black, and your image appears in the lower right hand corner.

On the other end of the call, Michael receives a request to accept or decline the video conference (see Figure 26 "Video conference request" (page 45)).

Figure 26
Video conference request

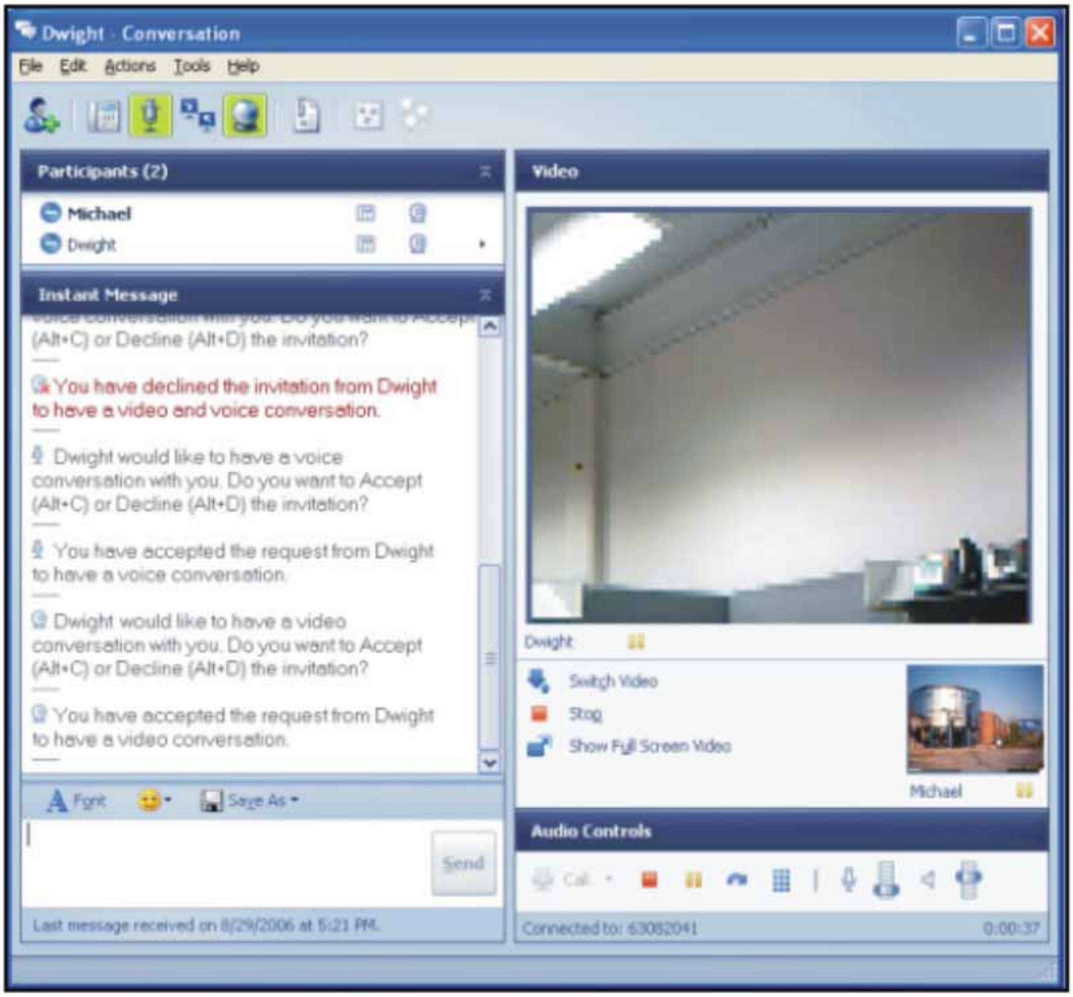


Dwight would like to have a video conversation with you. Do you want to Accept (Alt+C) or Decline (Alt+D) the invitation?

Last message received on 8/29/2006 at 5:19 PM.

When Michael accepts the request, a two-way video conference is initiated (see Figure 27 "Video conference (two-way video)" (page 46)). The other user appears in the larger screen, and your picture appears in the smaller screen in the lower right section of the window. At this point, both audio and video are going to Office Communicator.

Figure 27
Video conference (two-way video)



voice conversation with you. Do you want to Accept (Alt+C) or Decline (Alt+D) the invitation?

You have declined the invitation from Dwight to have a video and voice conversation.

Dwight would like to have a voice conversation with you. Do you want to Accept (Alt+C) or Decline (Alt+D) the invitation?

You have accepted the request from Dwight to have a voice conversation.

Dwight would like to have a video conversation with you. Do you want to Accept (Alt+C) or Decline (Alt+D) the invitation?

You have accepted the request from Dwight to have a video conversation.

Last message received on 8/29/2006 at 5:21 PM.

Connected to: 63082041 0:00:37

Planning and engineering

Contents

This section contains information about the following topics:

Introduction

Before you install and configure Nortel Converged Office, a number of issues must be addressed regarding network size and its impact on the type of software and hardware used. Also, because each Converged Office component has its own unique set of installation and configuration considerations, issues exist that are related specifically to both Remote Call Control with SIP CTI and Telephony Gateway and Services.

Note: In this chapter, and the one that follows, Telephony Gateway and Services is presented first, followed by Remote Call Control. During the implementation phase, it is recommended that the Telephony Gateway and Services component be implemented first to provide basic connectivity, (which can be more readily debugged), followed by Remote Call Control for more complex feature operation. Configuring both Telephony Gateway and Remote Call Control is only necessary in situations where both components are required. The Telephony Gateway and Services component is not required in situations where Remote Call Control is the only required component.

Network Design

The first consideration when you plan and engineer the Converged Desktop is the size of the network. Networks can be divided into three main categories: small, medium, and large, with each type requiring specific configurations.

The following sections describe typical network topologies you might consider depending upon your capacity and robustness requirements.

Note 1: The descriptions and graphical representations of the three network types are for illustration only, and are not intended to be actual configurations. The actual number of CS 1000s and Live Communications Servers will be based on the engineering guidelines found in this NTP and those provided by Microsoft®.

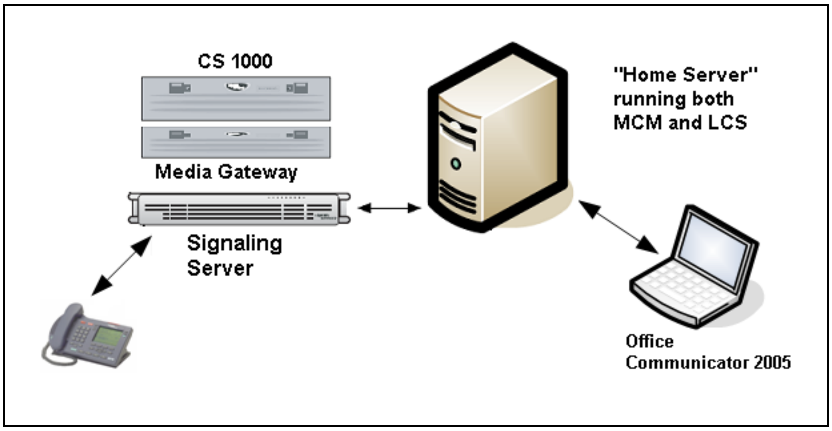
Note 2: Throughout this document, Live Communications Server 2005 Front End Enterprise Edition refers exclusively to Live Communications Server 2005 with Service Pack 1 (SP1).

Small network

Small networks require only a basic configuration, where MCM and Live Communications Server co-reside on the same Home Server. This configuration is recommended for small organizations that do not require redundancy.

Note: The recommended deployment requires that MCM reside on a separate Live Communications Server Application Proxy server; however, this is not required for small networks. Figure 28 "Small network configuration" (page 49), shows a typical Home Server configuration.

Figure 28
Small network configuration



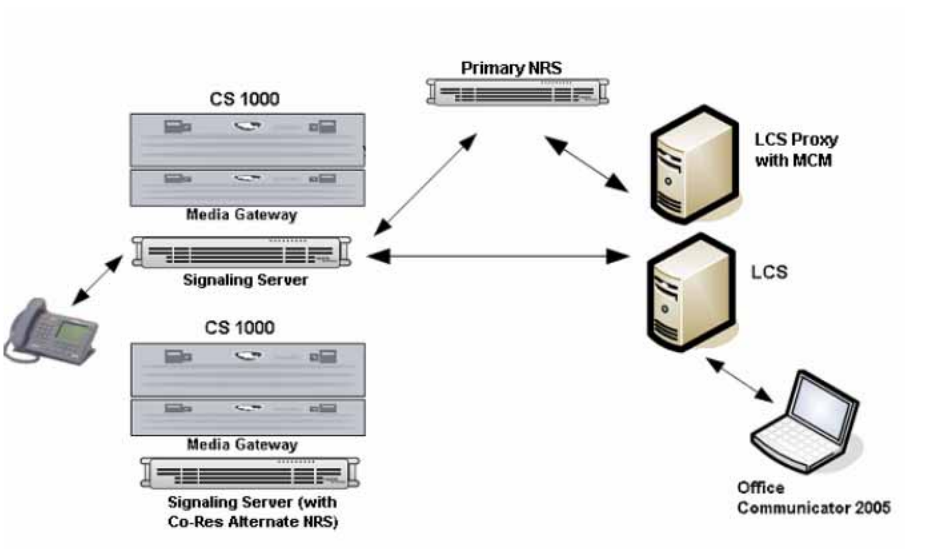
For small networks consisting of less than 500 users, you can install and operate Live Communications Server 2005 Standard Edition on a minimal hardware configuration. This configuration is not supported for large deployments or for the Enterprise Edition. The minimal hardware aligns with recommendations for hardware for Windows Server 2003 Standard Edition.

Medium network

A medium network may require the following components:

- multiple CS 1000 systems with Media Gateway and Signaling Server
- a Primary NRS with an Alternate NRS (co-residing on one of the Signaling Servers)
- Live Communication Server 2005 Standard Edition
- a Live Communication Server Proxy running MCM (the recommended deployment requires that MCM reside on a separate Live Communications Server Proxy server)

Figure 29
Medium network configuration



Note: SPS (Linux-based NRS) does not support co-residency.

Large network

A large network may require the following components:

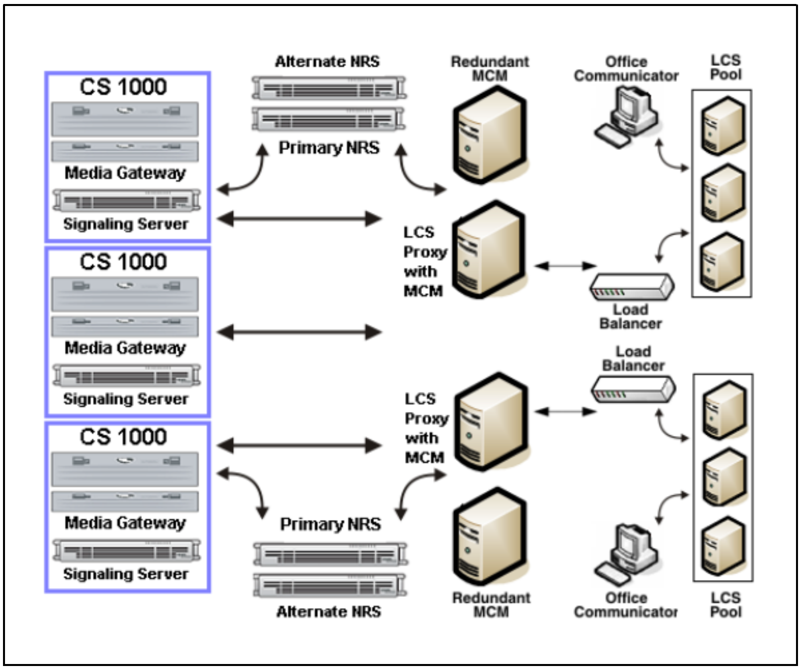
- multiple CS 1000 systems with Media Gateway and Signaling Server
- redundant Primary and Alternate NRS
- Live Communication Server 2005 Enterprise Edition (EE) with SP1 with a load balancer to front end the pool of Enterprise Edition Servers
- redundant Live Communication Server Proxies running MCM (the recommended deployment requires that MCM reside on a separate Live Communications Server Application Proxy server)
- multiple networks of CS 1000 systems can be configured using collaborative NRS

ATTENTION

If you are running the Enterprise Edition of Microsoft Live Communications Server 2005, **you must use a load balancer** even if only one server exists in the pool—per the Unified Communications Engineering Rules and Guidelines.

The load balancer ensures that the FQDN of the pool is not equal to the FQDN of any home server in the pool.

Figure 30
Large network configuration



Note 1: The redundant, primary, and alternate NRS can be either the VxWorks NRS or the Linux-based NRS (SPS/SRS).

Note 2: Microsoft requires, for Enterprise Edition, an SQL server as part of the network.

Load Balancer

Hardware IP Load Balancers (for example, Nortel Application Switches) are required for Live Communications Server 2005 Enterprise Edition deployments. The Load Balancer exposes a single virtual IP (VIP) address to clients to prevent direct access to individual Live Communications Server Enterprise Edition Servers. The Load Balancer uses a metric (for example, round robin, or fewest connections) to route new client requests to the Live Communications Servers.

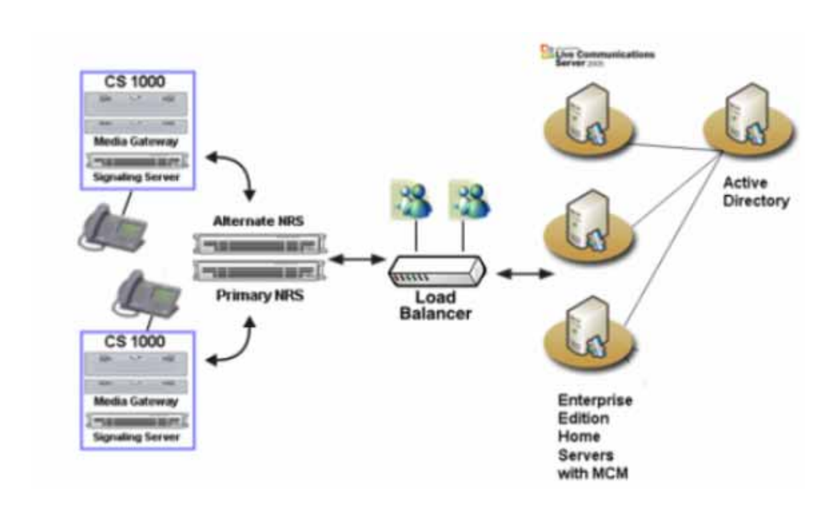
The Load Balancer can be configured in a number of ways depending on whether a Live Communications Server Application Proxy is deployed.

For more information about deployment of small, medium, and large networks, as well as Load Balancer requirements, refer to *Live Communications Server 2005 with SP1 Deployment Overview* from the Microsoft® site:

www.microsoft.com/office/livecomm

Using a Load Balancer between a pool of Enterprise Edition LCS Home Servers pool running MCM and the CS1000 It is possible to add redundancy to your network by placing a Load Balancer, such as a Nortel Application Switch, between a pool of Live Communications Server Home Servers and the CS1000. The role of this Load Balancer is to balance SIP invites from the CS1000 to the LCS Home Servers (which are part of Enterprise Edition pool). From the Home Servers, all SIP Invites are sent directly to the NRS and redirected to the appropriate CS1000. This configuration is depicted in Figure 31 "Single Load Balancer" (page 52).

Figure 31
Single Load Balancer



In order for the Load Balancer to work correctly, the following conditions must be met:

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: www.microsoft.com/office/livecomm
2. The Load Balancer can handle the balancing of TCP IP traffic
3. The Live Communications Server Home Servers adds the Virtual IP (VIP) address of the Load Balancer as well as all CS1000 as Authorized Hosts.
4. The NRS has the Virtual IP (VIP) of the Load Balancer configured as a static entry. All dialing plan entries are redirected to the Virtual IP address of the Load Balancer.
5. The MCM application running on all Home Servers should use the NRS for redirection must register with the NRS.

Using a Load Balancer between the LCS Home Server and Live Communications Server Application Proxy It is possible to add redundancy to your network by placing Load Balancers such as a Nortel Application Switch, between the Live Communications Server (LCS) Home Servers and Live Communications Server (LCS) Application Proxy.

The configuration depicted in Figure 32 "Redundancy with Load Balancers" (page 53) shows two Load Balancers. An Outgoing Load Balancer and an Incoming Load Balancer.

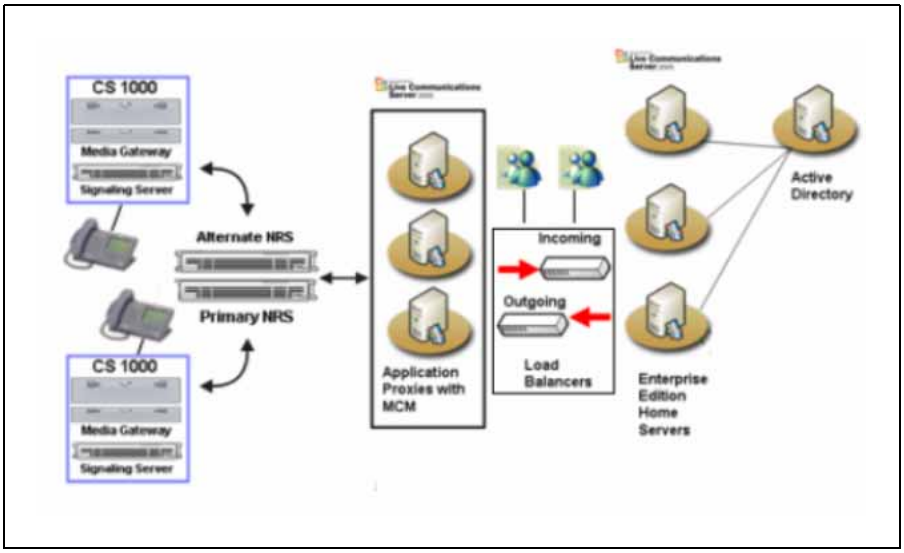
The role of the Outgoing Load Balancer is to balance SIP invites from the Home Servers to the Application Proxy. From the Home Servers, all SIP Invites are sent to the Virtual IP (VIP) of the Outgoing Load Balancer. The Load Balancer then sends the SIP Invite to the least busy Live Communications Server Application Proxy.

The role of the Incoming Load Balancer is to balance SIP invites from the Application Proxy to the least busy Home Server. The Application Proxy is configured to send all SIP invites to the Virtual IP (VIP) of the Incoming Load Balancer.

Redundancy is also ensured for calls to an Office Communicator user by having each LCS Application Proxy register to the MCM with a unique Registration ID and different cost factor. Therefore, if one of the LCS Application Proxy Servers is unavailable, the next one is selected.

It should be noted that the Outgoing and Incoming Load Balancers are viewed as two separate logical devices but can be one physical device configured to behave as two Load Balancers.

Figure 32
Redundancy with Load Balancers



In order for the Load Balancer to work correctly, the following conditions must be met:

Deployments with incoming Load Balancer only (TLS):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: www.microsoft.com/office/livecomm
2. TLS transport is used, exclusively, for all connections between Live Communications Server Home Servers and the Live Communications Server Application Proxy
3. The route added on the Live Communications Server Home Servers routes to the FQDN of the Live Communications Server Application Proxy using TLS
4. The route added on the Live Communications Server Application Proxy routes to the FQDN of Live Communications Server pool
5. The Live Communications Server Home Servers add the FQDN of the Live Communications Server Application Proxy Server as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the FQDN of Live Communications Server pool as Authorized Hosts.

Deployments with incoming Load Balancer only (TCP):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: www.microsoft.com/office/livecomm
2. TCP transport is used, exclusively, for all connections between Live Communications Server Home servers and the Live Communications Server Application Proxy.
3. The route added on the Live Communications Server Home Servers routes to the IP address of the Live Communications Server Application Proxy using TCP.
4. The route added on the Live Communications Server Application Proxy routes to the Virtual IP (VIP) address of incoming Load Balancer using TCP.
5. The Live Communications Server Home Servers add the IP address of the Live Communications Server Application Proxy Server and VIP address of incoming Load Balancer as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the IP addresses of all Live Communications Server Home Servers as Authorized Hosts.

Deployments with incoming and outgoing Load Balancers (TCP):

1. The Load Balancer meets all the criteria for a Load Balancer specified by Microsoft®. For more information, refer to: www.microsoft.com/office/livecomm
2. TCP transport is used, exclusively, for all connections between Live Communications Server Home servers and the Live Communications Server Application Proxy
3. The route added on the Live Communications Server Home Servers routes to the VIP address of outgoing Load Balancer using TCP.
4. The route added on the Live Communications Server Application Proxy routes to the VIP address of incoming Load Balancer using TCP.
5. The Live Communications Server Home Servers add the IP address of the Live Communications Server Application Proxy Server as Authorized Hosts.
6. The Live Communications Server Application Proxy adds the IP addresses of all Live Communications Server Home Servers as Authorized Hosts.

Deployments with incoming and outgoing Load Balancers (TLS):

Not supported

Deployments with mixed transport types (TCP in one direction and TLS in other):

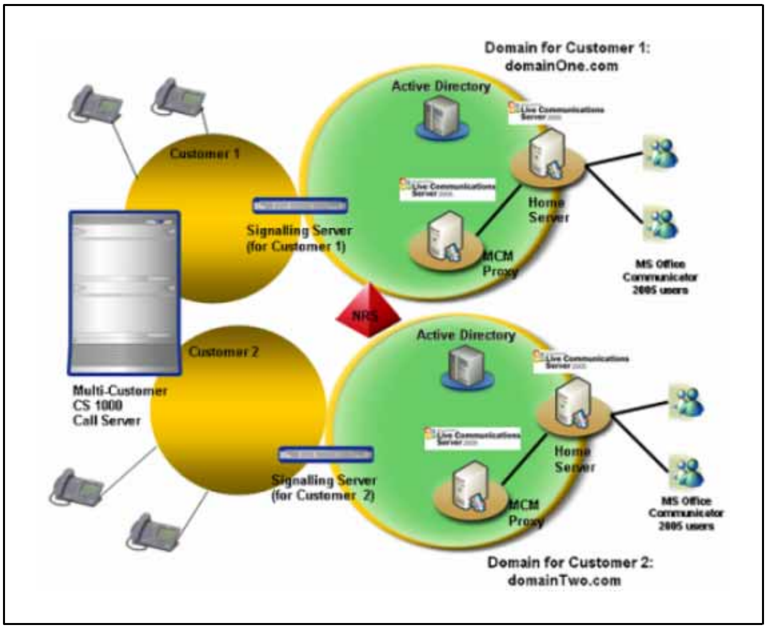
Not supported

Multiple Customer Network

A common feature in the Hosted Solution market, the CS 1000 can be configured with a number of customers. In this configuration, each of the customers on the CS 1000 have their own set of phones, trunks, features, restrictions, and numbering plans. In the Converged Office environment, as with the CS 1000 in general, each customer is treated as separate machine. Each customer has their own Node Number, Signalling Server, and SIP domain. For more information about the Multiple Customer environment, refer to the *Features and Services* (NN43001-106) NTP.

Figure 33 "SIP Gateway-only Network or SIP Gateway and SIP CTI Network" (page 56) provides an example of a Multiple Customer network. The figure shows two customers: Customer 1 and Customer 2, each with their own set of associated phones and Signalling Server(s). 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 33
SIP Gateway-only Network or SIP Gateway and SIP CTI Network



The Signalling Server(s) for Customer 1 are in the domainOne.com domain. For each customer, a separate Live Communications Server domain must be configured. The Live Communications Server domain used by Customer 1 is in the same domain as the Signalling Server(s) domainOne.com. Each Live Communications Server domain requires its own Active Directory.

The only equipment shared by Customer 1 and 2 is the Call Server 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 Signalling Server(s), Live Communications Server Application Proxy (which runs MCM), Live Communications Server Home Server, and Active Directory are completely separate. The number of Signalling Server(s), Live Communications Server Application Proxy, and Live Communications Server Home Servers required for each customer are the same as they would be if each customer were part of a single system. However, the total number of users allowed for the Call Server is the total number of users for all customers.

General Recommendations

The following sections describe in detail the recommended platform for deploying Live Communications Server 2005.

Operating System Required

Microsoft® Windows Server™ 2003 is the required operating system for Live Communications Server 2005 with SP1.

Live Communications Server 2005 running MCM

MCM must be loaded on a Live Communications Server Application Proxy.

ATTENTION
An Application Proxy is NOT an Access Proxy.

Live Communications Server 2005 Standard Edition

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB (front side bus)
- 2-GB DDR (double data rate), 266 MHz RAM
- 2 × 18-GB hard disks (15,000 rpm SCSI)
- 100-megabit network adapter
- Windows Server 2003, Standard Edition
- MSDE 2000 Service Pack 3a
- At least two disk drives are required for optimal performance: one for the database and the other for the database transaction log.

Note: Although Live Communications Server 2005 Standard Edition is compatible with Microsoft® Virtual Server 2005, it is not supported as part of the Nortel Converged Office feature. The Nortel software component Multimedia Convergence Manager (MCM) must not be installed on a Live Communications Server server running Microsoft® Virtual Server 2005. For additional information about Virtual Server 2005, visit the Virtual Server Web site at:

http://www.microsoft.com/windowsserversystem/virtualserver/default.mspxx

Live Communications Server 2005 Enterprise Edition Server

For each role of server that is part of the Live Communications Server 2005 Enterprise Edition, a low-end and a high-end hardware specification is provided.

A range is provided to accommodate the range of customer deployments that is supported:

- Low-end hardware supports between 0 to 50,000 clients.
- High-end hardware supports between 50,000 to 125,000 clients.

The low-end and high-end server platforms have different performance characteristics.

In general, a low-end computer does not mix with high-end computers in a deployment. An exception is components that are placed in the perimeter network (such as an Access Proxy) that provide service to a small percentage of the overall user base and, therefore, might make use of a lower-end computer while the remainder of the intranet deployment would contain higher-end computers.

Configuration for an Enterprise Pool

The following shows the recommended hardware configuration for Live Communications Server 2005, Enterprise pool.

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB
- 2-GB DDR, 266 MHz RAM
- 2 × 18-GB hard disks
- 100-megabit network adapter
- Windows Server 2003, Standard Edition
- For deployments in excess of 50,000 users, a one gigabit network adapter is required for the Enterprise Edition Server.

Live Communications Server 2005, Back-End Database

The following shows the low-end and high-end hardware configurations for Live Communications Server 2005, Back-End Database.

Low-end hardware configuration:

- Dual Intel Xeon 3.06 GHz, 1-MB Cache, 533 MHz FSB
- 2-GB DDR, 266 MHz RAM
- 2 SCSI Channels (split backplane)
- 5 × 18-GB hard disks, 15,000 rpm SCSI disk drives
- 1-gigabit network adapter
- Windows Server 2003 Standard Edition
- Windows SQL Server™ 2000 Service Pack 3a (SP3a)

High-end hardware configuration:

- Quad Intel Xeon 2.8 GHz, 2-MB Cache
- 8-GB DDR RAM
- 1-gigabit network adapter
- Windows Server 2003 Enterprise Edition
- SQL Server 2000 SP3a Enterprise Edition

SQL Server 2000 SP3a Enterprise Edition is required to take advantage of the 8 GB of RAM. SP3a is the minimum supported version of SQL for performance and security reasons. For more information about selecting the correct edition of SQL Server, refer to the following web site:

www.microsoft.com/sql/techinfo/planning/ChoosEd.doc

Storage

Internal hard disks used for operating system and executable software, data, and transaction files are assumed to be on separate storage. The storage can be:

- DASD (Direct access storage device)
- SAN (Storage Area Network)
- External RAID (redundant array of independent disks)

Onboard storage:

- 2 SCSI Channels (split backplane)
- 5 × 18-GB hard disks, 15,000 rpm SCSI disk drives

Optional SAN:

- 1 Fibre Channel HBA (host bus adapter)
- SAN unit

Application Proxy

For more information on Application Proxies, refer to "Application Proxy and MCM capacity" (page 82).

ATTENTION

IMPORTANT!

To ensure you have the most current platform information, refer to *Microsoft® Office Live Communications Server 2005 with Service Pack 1 Planning Guide* from the Microsoft® web site:

http://www.microsoft.com/office/livecomm

Signaling Server

To ensure that all Release 5.0 features work correctly, all signaling servers must be running the latest software version.

Trunking

To handle the traffic between the CS 1000 and the Live Communications Server 2005, you must configure sufficient SIP trunks and PCAs. The number of additional SIP trunks needed is determined by:

The number of Office Communicator Users using the SIP Gateway feature

multiplied by:

The percentage expected to be on the phone at any given time

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

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

PCA trunks are required for each Office Communicator user using the "Twinning" (for SIP Gateway) feature.

Calculating SIP access port and PCA requirements

Table 1 "Inputs" (page 60) defines the inputs used to calculate SIP access ports and PCA requirements.

Table 1
Inputs

Input	Description
TN_MO_Users	Total Number of Office Communicator users that use the SIP Access Ports for voice services
PCA_MO_Users	Number of Office Communicator users that utilize Personal Call Assistant (PCA). The value entered is in addition to the number you indicate on the Software screen.
P_PCA_SIP	Percentage of PCA calls that use the soft client to answer

Calculations The following formulas are used to calculate traffic requirements:

Traffic for PCAs = (PCA_MO_Users) x (CCS per user) x (1 - P_PCA_SIP) x 10%

Traffic for SIP ports = (TN_MO_Users - PCA_MO_Users) x (CCS per user) + (PCA_MO_Users x P_PCA_SIP) x (CCS per user)

Total SIP Traffic = (Traffic for PCAs) + (Traffic for SIP ports)

Number of MO SIP ports = Poisson (Total SIP Traffic) at P.01 Grade of Service

* - MO = Microsoft Office Communicator

Table 2 "Traffic figures" (page 61) shows traffic in CCS and number of ports calculated based on Poisson formula at P.01 Grade of Service.

Table 2
Traffic figures

Traffic (CCS)	Traffic (Erlang)	#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
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

Traffic (CCS)	Traffic (Erlang)	#Ports
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
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
10000	277.78	318
20000	555.56	611
30000	833.33	908
40000	1111.11	1205
50000	1388.89	1502

Traffic (CCS)	Traffic (Erlang)	#Ports
60000	1666.67	1799
70000	1944.44	2096

Port usage

The ports used between Live Communications Server and CS1000 are the ports related to TCP and TLS. These are:

- 5060: TCP
- 5061: TLS

The dynamic port range used by Microsoft® Office Communicator for SIP/RTP is:

1024 - 65535

The port range can be controlled (restricted) to a smaller range using the group policy settings as described on the Microsoft® site:

support.microsoft.com/default.aspx?scid=KB;EN-US;903056

Note: Port ranges must not overlap.

Security Considerations

When considering a Converged Office deployment, the following security concepts should be understood and integrated into deployment planning.

Authentication of Live Communications Server Clients

Authentication of Microsoft® Office Communicator clients is provided by the Live Communications Server. For more information, refer to the *Microsoft® Office Communicator 2005 Planning and Deployment Guide* on the Microsoft® site:

www.microsoft.com/office/livecomm

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 the ability for Office Communicator users to manually override the Phone Integration settings in Active Directory provisioned by an administrator. To ensure that each Live 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. Please refer to section "Configuring MCM for Remote Call Control" (page 110) for details on the authorization process and MCM configuration requirements.

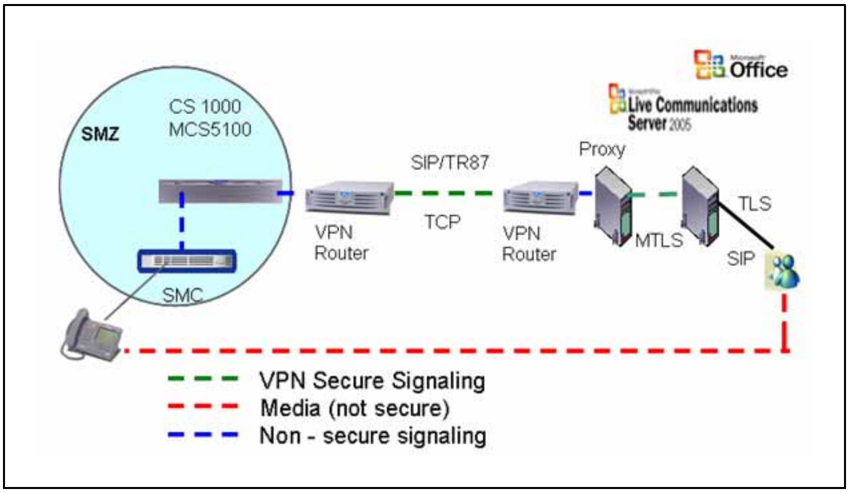
Signaling and Media Encryption

IP Connectivity between the Live Communications Server and the CS 1000 is provided by TCP. Similarly, Live Communications Server server-to-server traffic can also be TCP or TLS. TLS is the preferred option to provide signaling security between Live Communications Server and CS 1000.

> ***Note:*** For more information on TLS, refer to "Installation and Configuration" (page 89).

To provide signaling security between the Live Communications Server and the CS 1000 (see Figure 34 "Signaling Security" (page 64)), Nortel Contivity VPN routers can be used to tunnel SIP signaling between the Live Communications Server and the CS 1000. A single VPN router supporting Live Communications Server can service multiple individual VPN routers from multiple CS 1000 deployments.

Figure 34
Signaling Security



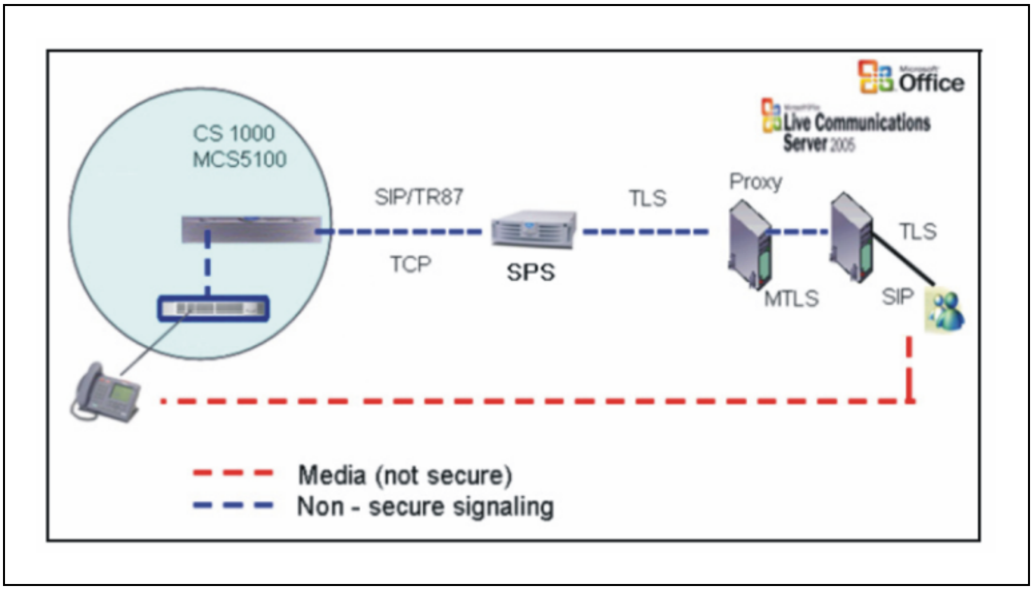
Secure Management Zone (SMZ) provides management access to local and remote devices over a secure connection. SMZ is a best practice that documents the LAN and WAN configurations required for secure management.

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.

Note: When configuring your security policies, please note that policy secure end-to-end is not supported with this application.

Figure 35
Signaling Security with TLS



Dial Plan Considerations

Overview

As discussed in previous sections, Microsoft® Converged Office consists of two components:

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

Whether a single or both components are chosen for deployment, an understanding of the existing dial plan and the mechanism through which it is exposed through Microsoft® Office Communicator is essential. This knowledge allows the existing dial plan (that users have become accustomed to with their existing telephony interfaces) to extend seamlessly to the Microsoft® Office Communicator client for either call type. This includes all existing CS 1000 dial plan features such as Coordinated Dial Plan (CDP), Uniform Dial Plan (UDP), and Group Dial Plan.

The following lists provide a summary of the features that contribute to the dial plan configuration for the Converged Office feature from the perspective of calls originated and received from Microsoft® Office Communicator.

Computer (SIP) Calls:

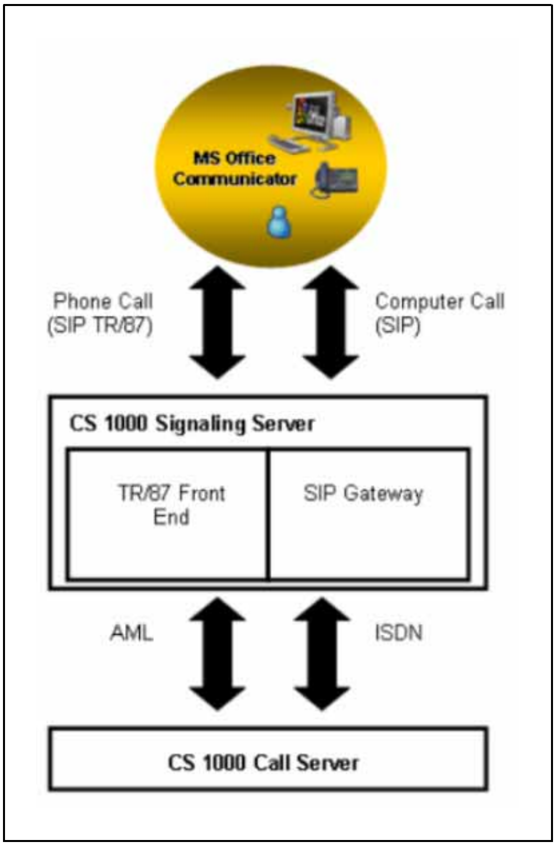
1. The format of the number itself entered in Active Directory or entered in Microsoft Office Communicator
2. Live Communications Server Address Book Service Normalization rules
3. The Network Redirect Service (NRS)
4. CS 1000 SIP Gateway Configuration
5. CS 1000 Call Server Configuration relating to the SIP Gateway

Phone (RCC or TR/87) Calls:

1. The format of the number itself entered in Active Directory or entered in Microsoft® Office Communicator
2. Live Communications Server Address Book Service Normalization rules
3. CS 1000 SIP CTI Services Configuration
4. CS 1000 Call Server Configuration relating to PBX phones

As highlighted by these lists, the number format and the normalization support provided by Live 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 CS 1000 is theTR/87 Front End and SIP Gateway respectively (as illustrated in Figure 36 "Signaling and media paths" (page 67)).

Figure 36
Signaling and media paths



Number Formats Supported by Microsoft® Office Communicator

In general, there are two types of numbers used by Microsoft® Office Communicator: **Dialstrings** and **E.164 International Format Numbers**. Both number formats apply to Computer and Phone calls with Microsoft® Office Communicator.

Dialstrings By default, any digits dialed from Microsoft® Office Communicator that are not fully qualified are sent as dialstrings. The sequence of digits entered in Microsoft® Office Communicator are sent directly to the Call Server to be dialed. This allows a user to dial all numbers that you would typically expect to dial from a phone local to the CS 1000.

E.164 International Format Numbers The recommended format of numbers stored in Microsoft® applications is the E.164 International format. This is a variable length number consisting of a '+' followed by a 1 to 3 digit country code and a national number that is 15-n digits long—where n is the length of the country code.

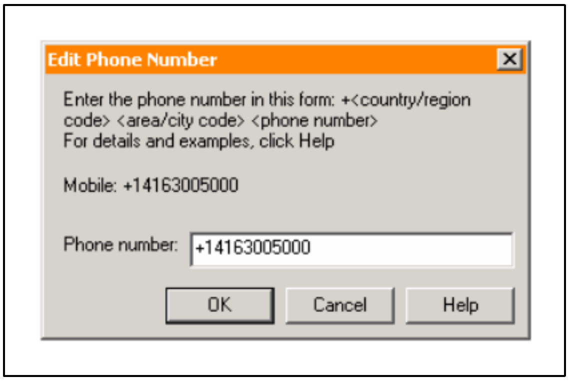
All E.164 numbers presented to the CS 1000, Computer, or Phone calls are expected to be in the following format:

+<country code><national number>

For example:

In North America, the Microsoft® Office Communicator Phone Number configuration input dialog would have the following entry (see Figure 37 "North American format" (page 68)).

Figure 37
North American format



Edit Phone Number

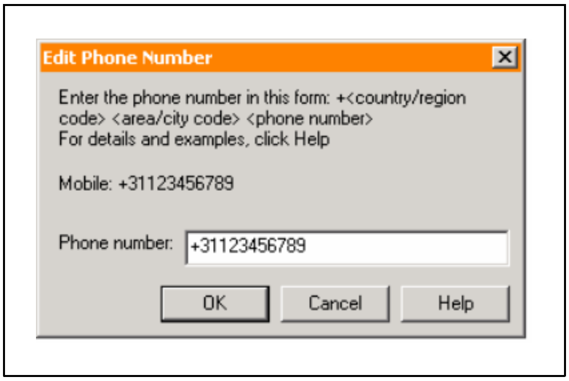
Enter the phone number in this form: +<country/region code> <area/city code> <phone number>
For details and examples, click Help

Mobile: +14163005000

Phone number: +14163005000

Outside North America, the Microsoft® Office Communicator Phone Number configuration input dialog would have the following entry (see Figure 38 "Outside North America format" (page 68)).

Figure 38
Outside North America format



Edit Phone Number

Enter the phone number in this form: +<country/region code> <area/city code> <phone number>
For details and examples, click Help

Mobile: +31123456789

Phone number: +31123456789

The Normalization feature, provided by the Microsoft® Live Communication Server Address Book Service, can be used to ensure that any formats used within a local deployment that do not conform to this convention can be converted without changes to the existing numbers themselves.

For example, in the Netherlands, numbers in Active Directory may be entered in the following format:

+31(0)123456789

A normalization rule can be used 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 on Normalization rules, refer to "Creating Normalization rules" (page 184).

Handling numbers called from Microsoft® Office Communicator in E.164 format requires that the call server be configured to ensure that the number requested is within the defined dial plans:

1. **Within North America**, various types of numbers can be recognized, including international, national, local (NPA, NXX, Free Calling Area Screening, and so on), or private, using one or two access codes and number translators (AC1 and AC2). The E.164 number entering 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 entering the Call Server are identified as international and outside of North America (for example, the country code is not 1), the translator used must contain entries that recognize these international numbers and route the call to the appropriate route list. These entries are generally within the existing AC1/AC2 translator, since they are used to route international calls that are dialed directly from phones.

   If calls entering the Call Server are national or local, the translation used must be able to recognize numbers with the national dialing prefix (for example, Converged Office calls) as well as numbers without the national prefix (for example, local calls dialed by users). To enable this 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 this HNPA entry within AC1, the translation software automatically begins using the AC2 translator to recognize the rest of the digits received.

2. **Outside North America**, various types of numbers are recognized, including international, national, local, or private, using one of two access codes and number translators (AC1 and AC2) and SPN entries. The E.164 number entering 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 entering the Call Server are identified as international and outside of the country of the caller, the translator used must contain entries that recognize these international numbers and route the call to the appropriate route list. These entries are generally within the existing AC1/AC2 translator, since they are used to route international calls that are dialed directly from phones.

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

The handling of E.164 international format numbers for SIP Gateway (Computer) calls is discussed in "Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls (SIP" (page 158).

The handling of E.164 international format numbers for SIP CTI (Phone) calls is discussed in "Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls (SIP CT" (page 181).

Telephony Gateway and Services

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

Table 3 "Systems, platforms, and applications" (page 70) identifies the systems, platforms, and applications supported by the Telephony Gateway and Services component.

Table 3
Systems, platforms, and applications

System, platform, or application	Supported
M1/CS 1000 Systems	
CS 1000S	Yes
CS 1000M Cabinet	Yes
CS 1000M Chassis	Yes
CS 1000M Small	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

Refer to "Capacity" (page 81) for capacity information relating to the Telephony Gateway and Services and Remote Call Control components.

Redundancy

Live Communications Server 2005 redundancy model is supported, with limitations, using Load Balancers.

NRS redundancy

NRS redundancy is similar to Converged Office redundancy; a heartbeat mechanism between MCM 2.0 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 their "twinned" phone. A user may have a phone number in Active Directory associated with their account (in Figure 39 "SIP Routing" (page 72), the number used is 231-3052). Calls made from a user to any endpoint (Public number or Private) are directed to their CS 1000 first. The CS 1000 then tandems the call to the other CS 1000, if necessary.

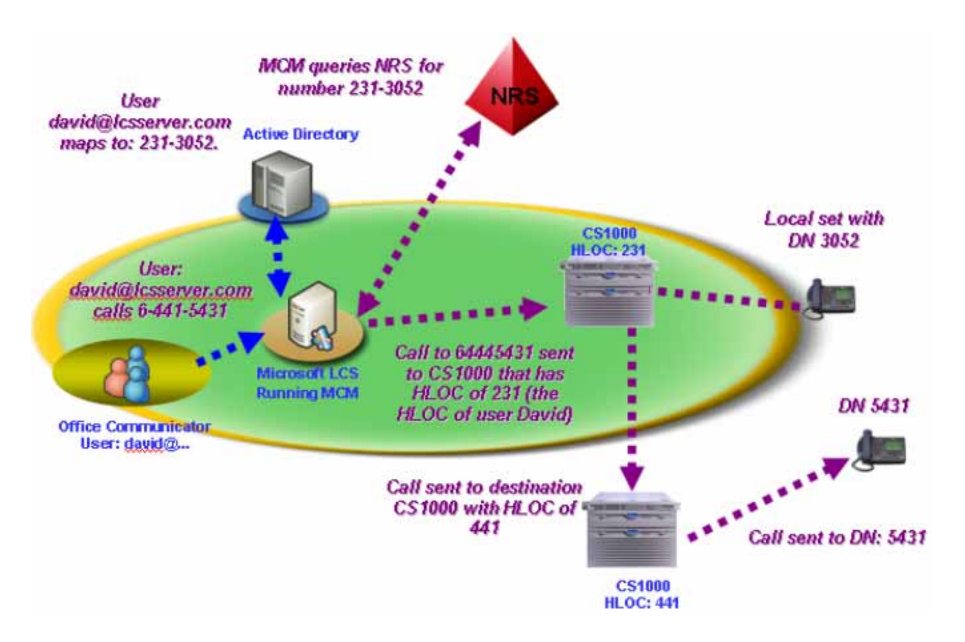
SIP routing ensures that:

1) All outgoing Office Communicator calls made by a "twinned" client can be tracked by Call Detailed Record (CDR)

2) Calls from Office Communicator to incompatible systems can be made

In Figure 39 "SIP Routing" (page 72) the user "david" calls 6-441-5431 (AC1-LOC-DN). The MCM application queries the Active Directory for the number associated with the originator "david", which comes back as 231-3052. MCM then uses the NRS to resolve the CS 1000 associated with the number 231-3052. MCM then directs the call to the CS 1000 that has the number of 231-3052. This CS 1000 then directs the call to the CS 1000 that has the destination number of 441-5431. This CS 1000 then directs the call to the CS 1000 that has the number 441-5431.

Figure 39
SIP Routing


MCM queries NRS for number 231-3052
NRS
User david@lcsserver.com maps to: 231-3052.
Active Directory
User: david@lcsserver.com calls 6-441-5431
CS1000 HLOC: 231
Local set with DN 3052
Microsoft LCS Running MCM
Call to 64445431 sent to CS1000 that has HLOC of 231 (the HLOC of user David)
Office Communicator User: david@...
DN 5431
Call sent to destination CS1000 with HLOC of 441
Call sent to DN: 5431
CS1000 HLOC: 441

It is important to understand the behavior of MCM when calculating the number of required SIP Trunks required by each CS 1000. Calls made to a CS 1000 that the "twinned" phone is not based off of use two SIP trunks: one incoming and one outgoing.

If users commonly call between CS 1000 systems, additional SIP trunks may be needed.

The number of required SIP trunks is sufficiently covered through the use of the calculations described in "Trunking" (page 59) and the platform-specific Planning and Engineering document.

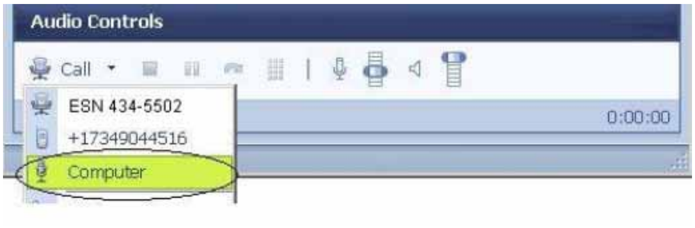
Feature Limitations

The following sections describe the limitations of the Telephone Gateway feature.

Call transfers for Office Communicator direct Computer to Computer calls

If a call is set up from an Office Communicator user in Computer mode to another Office Communicator user directly, the call is made to a "Computer" instead of a phone number (see Figure 40 "Computer call" (page 73)). As a result, the CS 1000 is not involved in the call and this type of call cannot then be transferred to a phone number.

Figure 40
Computer call



Office Communicator-initiated Call Transfer in Computer/Telephony Gateway mode

To handle a call transferred by Office Communicator, 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/Call Restriction controlling the transfer is only that of the SIP trunk itself.

Multi-Customer operation

Multi-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 Multi-Customer environment please refer to "Multiple Customer Network" (page 55).

Deployment

All information required to support Live Communications Server 2005 and Microsoft® Office Communicator deployment can be found on the Microsoft® Live Communications Server site:

www.microsoft.com/office/livecomm

MCM 2.0 uses LDAP queries to the Active Directory server for user-id/DN lookup. The Active Directory server must be engineered properly to provide the expected performance for the LDAP queries (less than 25 milliseconds). Live Communications Server and Active Directory APIs are used for queries and mapping.

Live Communications Server 2005 availability

Live Communications Server 2005 availability is up to 99.99% as described on the Microsoft® web site. (This is a Microsoft® limitation.)

Live Communications Server 2005 redundancy

The Live Communications Server 2005 redundancy model is supported, with limitations, using Load Balancers. For more information, refer to "Load Balancer" (page 51).

Microsoft Office Communicator Web Access

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

Microsoft Office Communicator Mobile (COMO)

Converged Office requires that the client support SIP Gateway. The Mobile version of Office Communicator, Microsoft Office Communicator Mobile, has limited support for SIP Gateway. SIP Gateway is only supported when the device is running Windows Mobile 5.0. Also, SIP Gateway calls/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 phone numbers for Microsoft Office Communicator Mobile are not supported.

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 set is translated into a signaling packet (or packets) that flow with the VoIP stream to the far end. These signaling packets are in fact 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 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. As well, the VGW TN can receive an RFC2833 packet on the VoIP side and generates a tone on the TDM side.

The correct Loss Values must be configured for in-band DTMF. For more information about correctly configuring the CS 1000 to support in-band DTMF tones, refer to "Configuring the Call Server" (page 136).

Support of Multimedia Communicator Server (MCS) MeetMe Conference

In Release 5.0 there are no limitations for Office Communicator calls to the MCS MeetMe bridge as long as all tandem nodes are running Release 5.0 software.

Codecs

G.711 A/MU law and G.723 are codecs supported for Office Communicator 2005. CS 1000 configuration no longer restricts the use of G.723 (out-of-band DTMF digits are now supported).

> ***Note:*** The G.711 codec must use a 20-ms payload at this time, due to the Microsoft® Office limitation.

IPDR/CDR capability

Live Communications Server 2005 does not support IPDR/CDR capability. CDR captures are supported on CS 1000 systems.

Office Communicator 2005 video support

Office Communicator video is is supported for both Remote Call Control and SIP Gateway. The video setup is exclusively Office Communicator client to Office Communicator client.

Note: For video calls to work, both users must be using the same form of Office Communicator (both are using either SIP CTI Office Communicator or SIP Gateway Office Communicator).

Video Calls

Office Communicator calls made in "Computer" mode can only establish video when connected in a call to another Office Communicator that is also in "Computer" mode (through CS 1000s running Release 5.0).

Video Call Transfer

Office Communicator calls made in "Computer" mode that have established video can be transferred to another Office Communicator user in "Computer" mode—although the new call is audio only. The transferred Office Communicator user will experience the call becoming audio only. Once 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," meaning that the call is immediately transferred to the new party.

Re-establishing Voice for Office Communicator Telephony Gateway to Office Communicator Telephony Gateway Video calls

Voice and Video calls that are established in Computer mode from one Office Communicator to another Office Communicator cannot drop the voice part of the call and then add back it again.

Local Tones

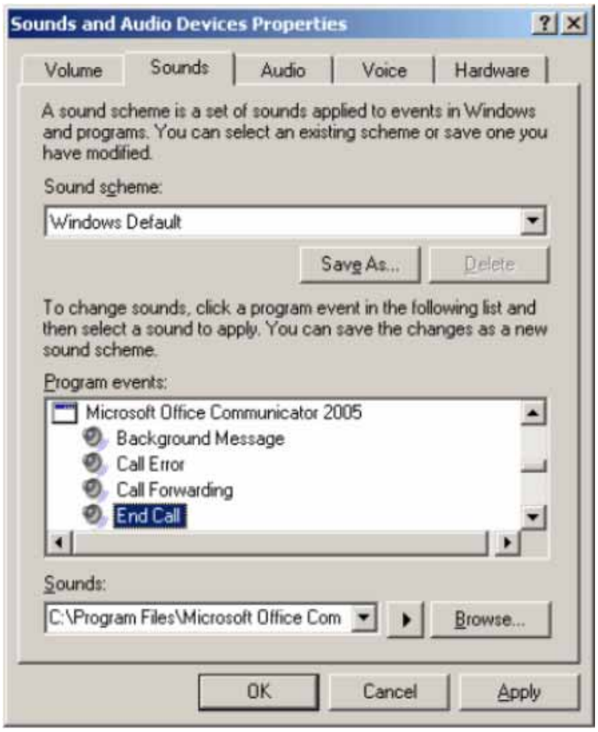
Office Communicator 2005 does support the generation of local tones (for example, "Ringback"), but the tones generated by Office Communicator are unique tones that are not specific to any country. Also, ringback is only generated for a set number of cycles — after which the other end continues to ring, but there is no audible ringback.

To change the ringback, or any tone, perform the following:

Procedure 1
Changing local tones

Step	Action
1	On the PC, select **Control Panel > Sounds and Multimedia**.
2	Select the **Sounds** tab.
3	Scroll down to the **Microsoft® Office Communicator 2005** section and select a tone (see Figure 41 "Sounds and Multimedia Properties" (page 76)).

Figure 41
Sounds and Multimedia Properties



A sound scheme is a set of sounds applied to events in Windows and programs. You can select an existing scheme or save one you have modified.

Sound scheme:
Windows Default

To change sounds, click a program event in the following list and then select a sound to apply. You can save the changes as a new sound scheme.

Program events:
Microsoft Office Communicator 2005
Background Message
Call Error
Call Forwarding
End Call

Sounds:
C:\Program Files\Microsoft Office Com

—End—

Quality of Service (QoS)

Office Communicator 2005 does not support QoS (L2: 802.1p/q or L3: diffserv).

Voice mail

Voice mail is not supported for direct Office Communicator calls. Voice mail is supported only with PCA/SimRing/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/ extension associated with the Office Communicator user. For example, if user david@lcsuser.com has a number/extension of 3052, david@lcsuser.com can call the same long distance and overseas numbers that the number/extension 3052 can on the CS 1000.

For more information refer to "Configuring the Call Server" (page 136).

MCS 5100

MCS 5100 interoperability and federation with Live Communications Server 2005 requires that a CS 1000 reside between the two, and is limited to voice in this feature.

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 Live Communications Server 2005.

For more information, refer to "Trunking" (page 59).

SIP CTI mode (phone mode)

Office Communicator 2005 supports SIP CTI mode (phone mode) where it controls the desktop phone to originate or answer calls and the non-CTI mode where voice calls can be originated or answered in the client.

Hold and Transfer

Office Communicator 2005 supports Hold and Transfer in stand-alone or non-CTI mode.

ipDialog Ethernet Phone

Office Communicator 2005 clients can only work with the ipDialog Ethernet Phone if it is tandemed through a CS 1000.

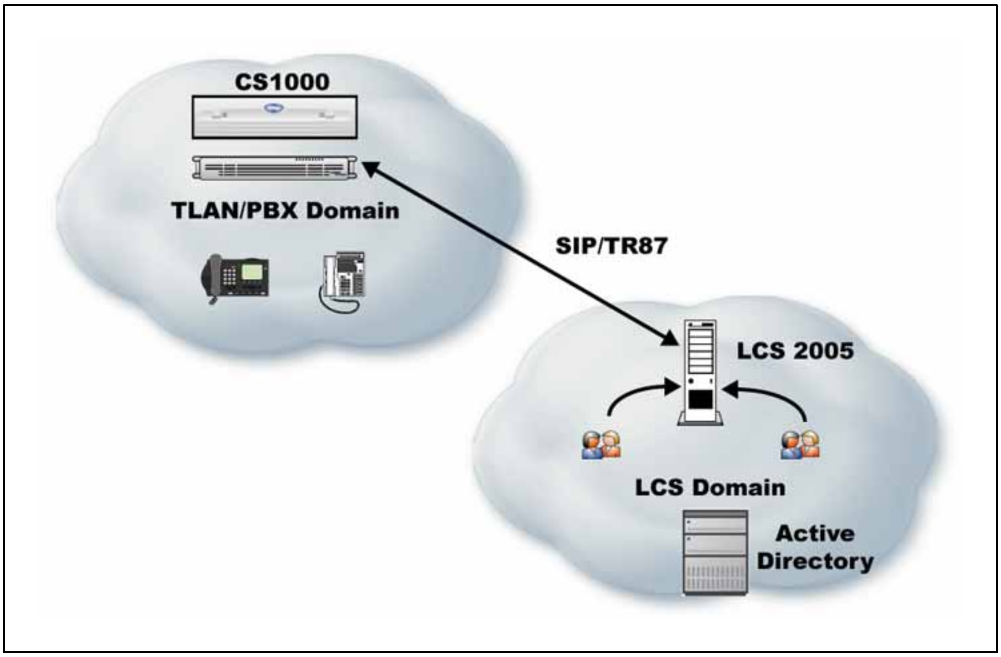
Country or region tone configuration

Country or region tone configuration is not supported by Live Communications Server 2005 and Office Communicator 2005.

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 phone types.

Figure 42
Simple network diagram



Microsoft® Office Communicator 2005 is the first soft client to use the ECMA TR/87 specification. Figure 42 "Simple network diagram" (page 78) shows a sample customer network deploying Active Directory, Live Communications Server Home Server, and CS 1000. Figure 42 "Simple network diagram" (page 78) does not show a Live Communications Server Application Proxy that can be inserted between a Live Communications Server Home Server Pool and CS 1000 servers for easy network configuration.

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 Microsoft® Office Communicator 2005 within a Live Communications Server 2005 deployment.

You can configure the TR/87 FE as a static routing rule within each pool of Live Communications Server Home Servers, or you can use the NRS to route TR/87 association requests.

CS 1000 is supported in both the Live Communications Server 2005 Standard Edition and Enterprise Edition network configurations subject to the capacity restrictions defined in this document.

Table 4 "Supported systems, platforms, and applications" (page 79) identifies the various systems, platforms, or applications that are interoperable or supported by the Remote Call Control component.

Table 4
Supported systems, platforms, and applications

System, Platform or Application	Interoperable	Supported
M1/CS 1000 Systems		
Option 11C Cabinet	N	N
Option 11C Chassis	N	N
Option 51C	N	N
Option 61C (CP3/4)	N	N
Option 61C (CP PIV)	N	N
Option 81C (CP3/4)	N	N
Option 81C (CP PIV)	N	N
CS 1000S	Y	Y
CS 1000M Cabinet	Y	Y
CS 1000M Chassis	Y	Y
CS 1000M Small	Y	Y
CS 1000M HG	Y	Y
CS 1000M SG (CP3/4)	Y	Y
CS 1000M SG (CP PIV)	Y	Y
CS 1000M MG (CP3/4)	Y	Y
CS 1000M MG (CP PIV)	Y	Y
CS 1000E	Y	Y
MG 1000B	Y	Y
Other Systems, Call Servers and Gateways		
CS 2000	N/A	N/A
CS 2100	N/A	N/A
MCS 5100	N/A	N/A
SRG 1.0	N/A	N/A
SRG 505	N/A	N/A

System, Platform or Application	Interoperable	Supported
M1/CS 1000 Systems		
BCM 50	N/A	N/A
BCM 200/400	N/A	N/A
Nortel Applications		
IP Clients	N/A	N/A
CDR	N/A	N/A
Telephony Manager (TM)	N/A	N/A
Element Manager	N/A	N/A
IP Call Recording	N	N
(See 9.1.1) Call Pilot	N/A	N/A
Call Pilot Mini	N/A	N/A
Meridian Mail	N/A	N/A
Meridian Mail Card Option	N/A	N/A
Meridian / Succession Companion DECT (DMC8 version)	N/A	N/A
VoIP - 802.11 Wireless IP Gateway	N/A	N/A
Remote Gateway 9150	N/A	N/A
Remote Office 9110/9115/ IP Adaptor	N/A	N/A
Mini Carrier Remote	N/A	N/A
Carrier Remote	N/A	N/A
Fiber I and Fiber II	N/A	N/A
Symposium Desktop TAPI Service Provider for MCA	N/A	N/A
Meridian Link Services [MLS]	Y	Y
Symposium TAPI Service Provider	N/A	N/A
Symposium Agent	N/A	N/A
Symposium Agent Greeting	N/A	N/A
Symposium Express Call Center (SECC)	N/A	N/A
Symposium Call Center Server [SCCS]	N/A	N/A
Symposium Web Centre Portal (SWCP)	N/A	N/A
Periphonics Open IVR (VPS/is)	N/A	N/A
Periphonics Integrated Package for Meridian Link (IPML) – VPS	N/A	N/A
Periphonics Multimedia Processing Server (MPS) 100	N/A	N/A

System, Platform or Application	Interoperable	Supported
M1/CS 1000 Systems		
Periphonics Multimedia Processing Server (MPS) 500	N/A	N/A
Integrated Call Assistant (MICA)	N/A	N/A
Integrated Conference Bridge (MICB)	N/A	N/A
Integrated Recorded Announcer (MIRAN)	N/A	N/A
Integrated Call Director (MICPD)	N/A	N/A
Hospitality Integrated Voice Services (HIVS)	N/A	N/A
Enterprise Data Networking	N/A	N/A
Third party applications		
AML based applications	Y	Y
Net6	N/A	N/A
Competitors		
Cisco H.323 GW	N/A	N/A
Avaya H.323 GW	N/A	N/A
Cisco SIP GW	N/A	N/A
Avaya SIP GW	N/A	N/A

Capacity

When planning for capacity with SIP CTI services, there is a fundamental restriction that must be observed:

- For a single call server that supports multiple nodes, each with SIP CTI services enabled, multiple SIP CTI(TR/87) sessions can be established for a given DN through the same node—but not through different nodes.

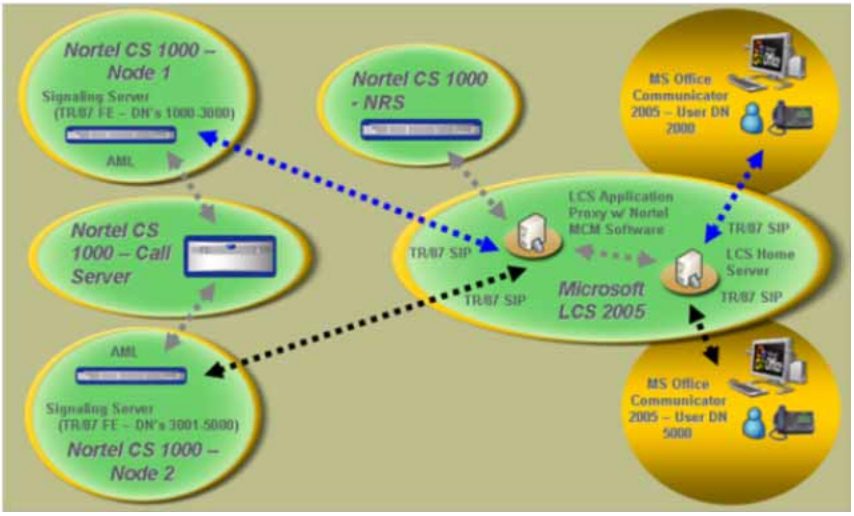
To illustrate this restriction, consider the following high level example:

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's session through Node 1.

To solve this issue when planning for capacity, SIP routing must ensure that all TR/87 sessions for a given DN always terminate on the same node when there are multiple nodes for a single call server (see Figure 43 "Capacity example" (page 82)).

Figure 43
Capacity example


Nortel CS 1000 – Node 1
Signaling Server (TR/87 FE – DN's 1000-3000)
AML
Nortel CS 1000 - NRS
MS Office Communicator 2005 – User DN 2000
Nortel CS 1000 – Call Server
LCS Application Proxy w/ Nortel MCM Software
TR/87 SIP
TR/87 SIP
LCS Home Server
TR/87 SIP
TR/87 SIP
Microsoft LCS 2005
AML
Signaling Server (TR/87 FE – DN's 3001-5000)
Nortel CS 1000 – Node 2
MS Office Communicator 2005 – User DN 5000

This situation may arise in cases where there is an expectation that a single user has multiple clients logged in simultaneously (for example, a client at home, a client in the office, and a mobile client all with TR/87 capability).

Impact on Signaling Server

The maximum number of SIP CTI/TR87 users on a single Signaling Server is 5000. For Release 5.0 a Standard Signaling Server memory of 1GB is required.

Impact on Call Server

For different CPUs, the number of users supported is:

- CPP PII 7000 users
- CPP PIV 15000 users
- CP PM: 15000 users

Application Proxy and MCM capacity

The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain, and endorse a standardized set of relevant benchmarks that can be applied to the newest generation of high-performance computers.

MCM capacity numbers depend on the hardware platform this application runs on, and the unit used to identify the platform is SPECint.

A single MCM can support 20000 calls per hour (this is a projected value of 4000 users averaging 5 calls per hour - check this using Windows Performance Monitor), per box, with a SPECint of 18.6.

Since MCM co-resides with Microsoft® Live Communications Server on different platforms, the formula for different hardware platforms is:

Number of calls per hour supported = (20000 x SPECint for a box) / 18.6

Note: This formula is based on SPECint_rate2000. The SPECint for each box can be found at www.spec.org.

Redundancy

SIP CTI services are supported (with limitations) in the following scenarios:

- Single node redundancy
- Campus redundancy
- Geographic redundancy

Redundancy within a single node

The same master/follower mechanism used for VTRK and TPS applications is used to support redundancy within a node for Remote Call Control. Once the master of the node goes down, one of the followers takes over the node IP and continues to deliver service. No SIP CTI session state is preserved when a new master is elected.

Redundancy across multiple nodes is possible using the least cost routing feature of NRS.

> ***Note:*** When considering a multi-node redundant configuration, refer to the restrictions on establishing TR/87 sessions from multiple nodes that have AML links to a single call server (see "Capacity" (page 81)).

Campus redundancy

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

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 GW SIP traffic. The main impacts are:

1. During transition periods, situations may arise where IP sets are registered to a call server different from the call server providing support for the TR/87 FE. In this case, TR/87 support is undefined. TR/87 clients are allowed to register successfully, however the status of the IP phone is impacted by any actions performed on the phone itself, or TR/87 client, since the FE and IP Phone are interfacing different call servers.

   Note: NRS is required to support redundancy.

2. Once an event has occurred that causes the IP Phones to register to a server other than their home server (and then to return to their home server), the Office Communicator 2005 client does not automatically follow the IP Phone registration. In order for the TR/87 sessions to be directed back to the TR/87 FE corresponding to the home TPS, one of the following actions must be taken:

   a. Users must log out and log back into the TR/87 client (for example, Office Communicator 2005) to force the previous SIP dialog to terminate so that a new dialog can be established, which NRS then redirects to the correct TR/87 FE.

   b. An administrator issues the "SIPCTIStop all" command on the Signaling Server (see Table 5 "SIPCTIStop all Command" (page 84)) to which the TR/87 sessions currently reside to terminate the SIP dialogs and force the clients to send another association request (for example, SIP INVITE) which the NRS then redirects to the correct TR/87 FE.

Table 5
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 sets in Local mode (registered in the Branch Office) only when the following conditions are met:

- Branch Office has SIP CTI and Telephony Gateway and Services enabled and properly configured and has a Signaling Server (SS) dedicated to each branch.
- The network dialing plan is a Coordinated Dial Plan (CDP).

- The IP set (Branch User) has the same domain name (DN) configured in Main Office and Branch Office.
- The Branch Office has access the Network Redirect Service (NRS) and Live Communications Server (LCS). If access is disrupted, failure cases may not be supported if the NRS and LCS 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 LCS 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 timeout (30 minutes) or manually log out and log in again after the IP sets go to Local mode.

Digital and analog sets in the Branch Office can have SIP CTI support and Telephony Gateway and Services when the Branch Office has access to the NRS and LCS.

Feature Limitations

The following sections describe the limitations of the Remote Call Control with SIP CTI component.

Call Forwarding

Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself.

WARNING

Microsoft® Office Communicator does not reflect call forward state changes made to the CS 1000 phone itself. When Office Communicator is active and controlling a DN, all Call Forward changes should be made through Office Communicator to ensure that it is in the correct state.

When a user signs into Live Communications Server from their Office Communicator client, the forwarding status saved within Office Communicator overrides any forwarding status that may have been set from the phone. For example, if forwarding is off within Office Communicator, it is turned off following sign in, regardless of the phone forwarding status at the time.

Analog phone usage

As a general rule, Office Communicator in SIP CTI mode can only control and invoke telephony features supported by the phone being controlled. If a feature is not supported or configured on a particular phone (whether it be

Analog, IP, or Digital) that feature is not supported by Office Communicator. Office Communicator in SIP CTI mode supervising an analog phone (2500) has the following limitations:

- **Make Call**: cannot be made Office Communicator if the analog phone (2500) phone does not go off hook prior to placing the call
- **Answer Call:** cannot be performed through Office Communicator. Answer Call must be performed through the analog phone (2500)
- **Call Conference:** cannot be performed through Office Communicator
- **Call Hold:** can be performed through Office Communicator
- **Call Transfer:** Analog phones do not support the Conference and Transfer feature keys. As a result, Call Conference and Call Transfer (Announced and Blind) cannot be performed through Office Communicator.

  Note: Flexible Feature Code (FFC) is not supported by AML and SIP CTI.

- **Send DTMF digits:** DTMF digits work with both Voicemail and Conferencing

Multi-Customer operation

Multi-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 please refer to "Multiple Customer Network" (page 55).

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.

AML limitation

CS 1000 has an AML limitation where only one application may acquire a DN/TN at any time. For example, the TR/87 FE application and IP Call Recording cannot co-exist on the same DN/TN. This also applies to the interaction between Symposium and Microsoft® Office Communicator Remote Call Control. Symposium uses the Application Module Link (AML) to acquire and control phones on CS 1000 Call Server.

Microsoft Office Communicator Web Access

Converged Office requires that the client support SIP CTI. The web version of Office Communicator, Microsoft Office Communicator Web Access, does not support SIP CTI.

Microsoft Office Communicator Mobile (COMO)

Converged Office requires that the client support SIP CTI. The Mobile version of Office Communicator, Microsoft Office Communicator Mobile, has limited support for SIP CTI.

Outgoing VoIP calls to phone numbers for Microsoft Office Communicator Mobile are not supported. SIP CTI (Remote Call Control) only permits the phone status to be updated (for example, on a call or not) when using Microsoft Office Communicator Mobile. SIP CTI supports Call Forward with COMO.

Office Communicator 2005 Call Forward On feature

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 2005 acquires a MADN which is not the Prime DN then the call is not forwarded, even if Call Forwarding On is enabled. For more information, refer to *Features and Services* (NN43001-106).

Live Communications Server/MCS co-existence

A user cannot have both Live Communications Server and MCS enabled for their extension (all TN’s that have a particular number/extension). If any of the TN’s have CLS CDMV or CLS CDMO configured, then the extension is treated as having MCS enabled. When MCS (SIP CD) is enabled on an extension, Live Communications Server Converged Office is not supported for that extension in Release 4.5B.

> **ATTENTION**
>
> **IMPORTANT!**
>
> All Converged Office users must have their extension configured as CLS CDMR.

Call Pilot configuration

In order for Telephony Gateway (Computer mode) calls to CallPilot to be able to access their mailbox by just pressing the "#" key, every mailbox needs to have the optional messaging network configured. In a normal CS1000 - CallPilot, this configuration is optional and may not be configured. For Telephony Gateway (Computer Mode) calls to CallPilot to work properly, this extra configuration is required. More information about the configuration of CallPilot can be found in *Callpilot network planning guide*(NN44200-201) in the section "Message Network Configuration Description".

Installation and Configuration

Contents

This section contains information about the following topics:

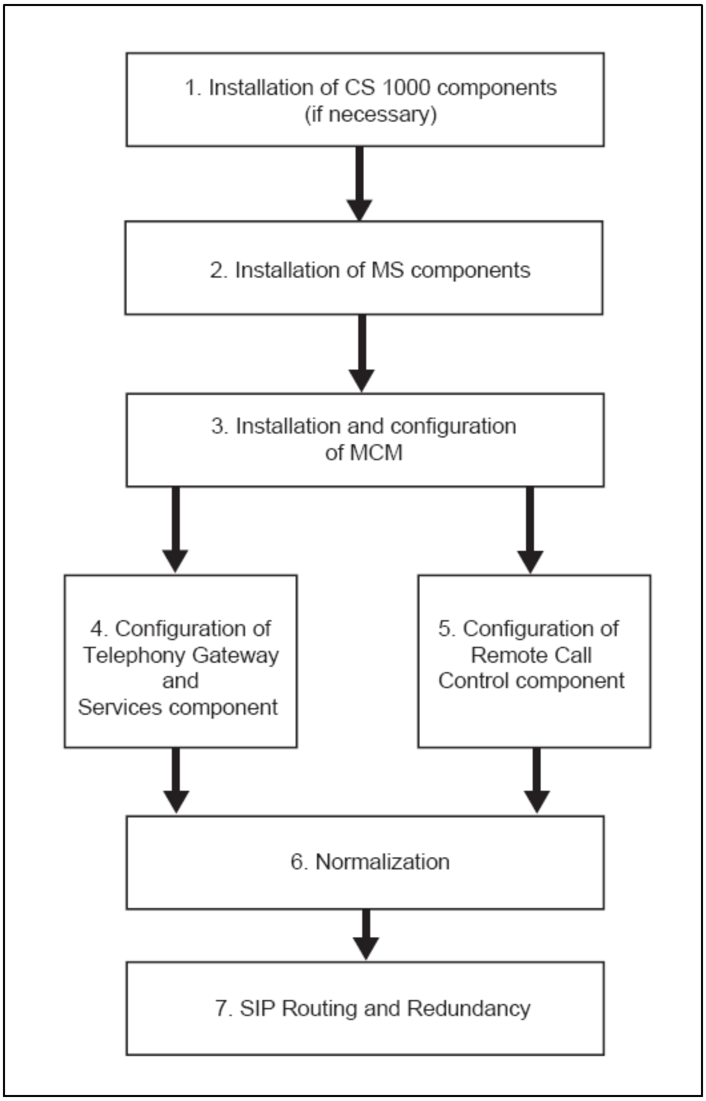
Overview

This chapter contains the procedures necessary to install and configure Microsoft® Office Live Communications Server 2005 on a CS 1000 system.

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

Once configuration is complete, normalization of phone numbers, SIP routing, and redundancy help you integrate the Nortel and Microsoft® Live Communications Server 2005 domains. Figure 44 "Installation and configuration process" (page 90) illustrates this process.

Figure 44
Installation and configuration process


1. Installation of CS 1000 components (if necessary)
2. Installation of MS components
3. Installation and configuration of MCM
4. Configuration of Telephony Gateway and Services component
5. Configuration of Remote Call Control component
6. Normalization
7. SIP Routing and Redundancy

The following steps describe the installation and configuration process in greater detail.

1. "Installing CS 1000 components" (page 93)
   a. "Installing the Call Server" (page 93) (release 5.0 or later), including all DEP list PEPs and Converged Office PEPs.
   b. "Installing the Signaling Server" (page 93) (release 5.0 or later), including all DEP list PEPs and Converged Office PEPs
2. "Installing Microsoft Live® Communications Server components" (page 94)
   a. "Installing Active Directory" (page 94)

   b. "Installing Live Communications Server 2005 Service Pack 1 (SP1)" (page 94)

3. "Installing and configuring MCM" (page 96)
   a. "Installing MCM software" (page 96)
   b. "Configuring MCM" (page 99)

4. "Configuring Telephony Gateway and Services" (page 112)
   a. "Configuring Live Communications Server" (page 112)
      - "Configuration of Static Routes on all intermediate Live Communications Servers" (page 122)
      - "Configuring Host Authorization" (page 123)

   b. "Configuring Active Directory" (page 174)
   c. "Configuring the Call Server" (page 136)
      - "Configuring the SIP Trunk" (page 137)
      - "Configuring the Codec" (page 138)
      - "Configuring the Loss Plan" (page 140)
      - "Configuring the Dialing Plan to route to MCM" (page 140)
      - "Configuring the Personal Call Assistant" (page 141)
      - "Configuring the Call ID Table" (page 144)
      - "Configuring Home LOC and Home NPA" (page 146) (if necessary)

   d. "Configuring the Signaling Server" (page 146)
      - "Configuring the DNS Server" (page 146)
      - "Configuring the SIP Trunk" (page 147)

   e. "Configuring SIP Gateway CLID Parameters" (page 151)
      - "Configuring NRS" (page 153)

   f. "Configuring Microsoft® Office Communicator 2005" (page 155)

      Note: Requires phone integration enabled (Microsoft® Knowledge Base article KB 910790)

   g. "Configuring CDR" (page 157)
   h. "Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls (SIP Gateway)" (page 158)

   i. "Normalizing phone numbers" (page 158)

5. "Configuring Remote Call Control" (page 159)
   a. "Configuring the Call Server" (page 136)
      - "Configuring the AML" (page 159)
      - "Configuring the SIP CTI TR/87 ISM Limit" (page 160)
      - "Configuring a station" (page 161)
      - "Considering MADN (Multiple Appearance DN)" (page 161)
      - "Configuring NRS" (page 162) (optional)
   b. "Configuring the Signaling Server" (page 162)
      - "Configuring Node Parameters" (page 163)
      - "Configuring SIP Gateway Parameters" (page 163)
      - "Configuring the DNS Server" (page 164)
   c. "Configuring SIP CTI Settings" (page 165)
   d. "Configuring SIP CTI Dial Plan Prefixes" (page 167)
   e. "Configuring SIP CTI CLID Parameters" (page 168)
   f. "Configuring Live Communications Server" (page 173)
   g. "Configuring Active Directory" (page 174)
      - "Enabling the Remote Call Control Flag" (page 175)
      - "Defining the Remote Call Control Controlled Line (Device URI of the phone of the user)" (page 176)
      - "Defining the Remote Call Control SIP URI" (page 177)
      - "Configuring the SIP URI Map" (page 178)
   h. "Configuring Microsoft® Office Communicator 2005" (page 178)
      - "Configuring Phone Integration settings" (page 178)
      - Procedure 8 "Configuring account details" (page 179)
   i. "Configuring CDR" (page 181)
   j. "Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Phone Calls (SIP CTI)" (page 181)

6. "Normalizing phone numbers" (page 182)
   a. "Normalizing Offline (Recommended)" (page 183)

  b. "Normalizing using the Address Book Service" (page 184)
  c. "Creating Normalization rules" (page 184)

7. "Configuring SIP Routing and Redundancy" (page 188)
   a. "Configuring Remote Call Control SIP Routing Using Phone Addressing" (page 189)
   b. "Configuring Remote Call Control SIP Routing Using a Gateway Endpoint Name" (page 189)
   c. "Configuring Redundancy" (page 190)

8. "Deploying Live Communications Server Client PC application to end users" (page 190)

Installing CS 1000 components

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

Installing the Call Server

If you do not have a CS 1000 system installed and configured, refer to the following NTPs for detailed instructions:

- *Communication Server 1000M and Meridian 1: Small System Installation and Commissioning* (NN43011-310)
- *Communication Server 1000M and Meridian 1: Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000S: Installation and Configuration* (NN43031-310)
- *Communication Server 1000E: Installation and Configuration* (NN43041-310)

ATTENTION

IMPORTANT!

PEPs, from the PEPs library, are required for both Call Server and Signaling Server installation for the Converged Office feature to operate.

Refer to 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, refer to *Signaling Server: Installation and Commissioning* (NN43001-312).

Configuring the Signaling Server is covered later in this chapter.

Installing Microsoft Live® Communications Server components

After all CS 1000 components are installed, install the Microsoft® components, beginning with the Active Directory.

Installing Active Directory

The Live Communications Server and Communicator 2005 environment have a strong dependency on Active Directory. Active Directory is used for authenticating, authorizing, provisioning, and configuring Live Communications Server 2005.

With Office Communicator 2005, Active Directory is also used to supply the enterprise address list to facilitate search-based lookups.

It is assumed at this stage that Active Directory has been installed in accordance with Microsoft® documentation. For more information about Active Directory planning, refer to the *Live Communications Server 2005 Active Directory Preparation* document in the Deployment Resources area of the Microsoft® site:

www.microsoft.com/office/livecomm

Installing Live Communications Server 2005 Service Pack 1 (SP1)

Microsoft® Office Live Communications Server 2005 Standard Edition

Live Communications Server 2005 Standard Edition provides a simple way to enable presence and IM services for small, simple networks. Standard Edition Server is completely self-contained and does not require Microsoft® SQL Server® 2000 to operate. It does; however, require Microsoft® Database Engine (MSDE).

Microsoft® Office Live Communications Server Enterprise Edition

For deployments that require higher availability or a large degree of scalability, the concept of a Home Server is divided into two distinct parts:

- Live Communications Server 2005, Enterprise Edition (manages client connections, presence, and other real-time communication features like instant messaging)
- Live Communications Server 2005, Back-End Database (a back-end server, running Microsoft® SQL Server 2000 Service Pack 3a (SP3a), which can be clustered)

Together, the Enterprise Edition Server and the Back-End Database form a pool.

Microsoft® Office Live Communications Server 2005 Enterprise Pool

Live Communications Server 2005, Enterprise pool is a collection of Enterprise Edition Servers that are connected to a central Live Communications Server 2005, Back-End Database.

Users (clients) register on an Enterprise pool. Users are directed to a specific server within the pool by a hardware load balancer that distributes the load to these servers. 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. 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. A client can register on multiple servers at the same time. Each device to which the user is logged on (called an endpoint) can be connected through a different server at the same time.

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. Live Communications Servers within the pool are networked to the back-end server using a high-speed network. These Live Communications Servers also run User Replicator (UR) software to provide a connection to the Microsoft® Active Directory® directory service so that user account information can be synchronized between the Microsoft® Back-End Database Server and the Active Directory.

You can deploy Live Communications Server 2005 SP1 using one of the following methods:

- The deployment tool launched by Setup.exe. The deployment tool provides a set of wizards that guides you through each deployment task.
- Command-line tools provided on the Live Communications Server 2005 CD.

For more information about Live Communications Server 2005 SP1 installation, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

www.microsoft.com/office/livecomm

Installing and configuring MCM

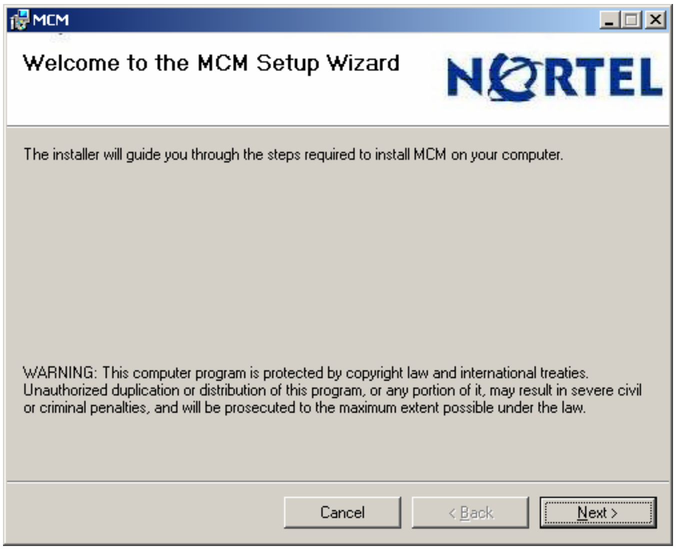
> **ATTENTION**
> If configuring for TLS, refer to "Configuring TLS" (page 192) for TLS-specific information.

Installing MCM software

> ***Note:*** If upgrading to MCM 2.0, refer to "Upgrading MCM" (page 99).

MCM 2.0 software installation involves the use of a standard installation wizard (see Figure 45 "MCM Setup Wizard" (page 96)). You need to create an account for the installation (see Figure 46 "MCM Login" (page 97)) of MCM and you must define this user name and password in Active Directory before you install MCM.

Figure 45
MCM Setup Wizard



Welcome to the MCM Setup Wizard

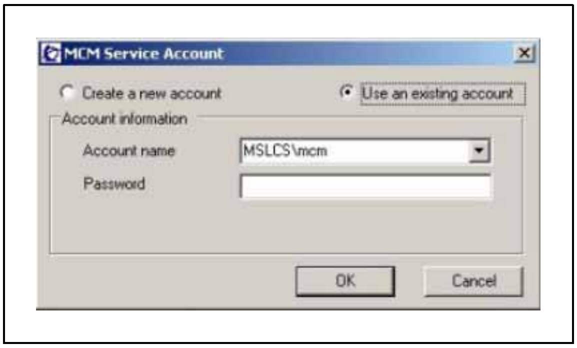
The installer will guide you through the steps required to install MCM on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

The correct user name and password are required for MCM to run as a service. The user entered must be a member of two groups that are local to the Live Communications Server (the groups are not listed in Active Directory). The user must be part of the "RTC Server Application" group and the "Administrator" group. MCM cannot not be configured or run as a service unless the user has been properly created (listed in Active Directory and a member of the correct local groups).

MCM 2.0 allows for the automatic creation of new MCMService accounts with required permissions and groups. The MCM installer can create a new user and configure it automatically—no additional configuration is required. If a user already exists, MCM verifies the user’s configuration and the password provided during setup.

Figure 46
MCM Login



○ Create a new account ● Use an existing account

Account name: MSLCS\mcm

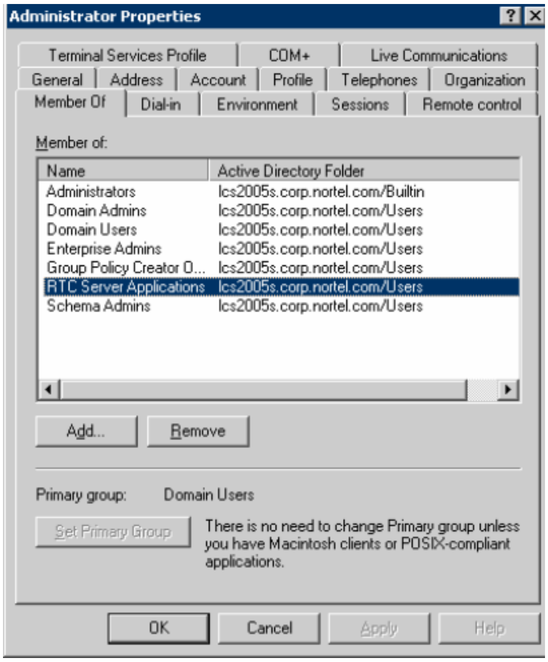
Password:

Note: Figure 46 "MCM Login" (page 97) shows the login screen for the MCM service account. The Username field must include the domain (for example, "Domain\MCMService" must be used, as "MCMService" on its own does not work). The username may take the form of "MCMService@full_domain"; however, the user account cannot be specified in this form if:

1. There is only one DNS server in the deployment
2. MCM runs on the same server as DNS Server

Figure 47 "Member Of tab in Active Directory" (page 98) shows the "Member Of" tab in the Active Directory Administrator Properties window. This user is a member of the RTC Server Application

Figure 47
Member Of tab in Active Directory



Name	Active Directory Folder
Administrators	lcs2005s.corp.nortel.com/Builtin
Domain Admins	lcs2005s.corp.nortel.com/Users
Domain Users	lcs2005s.corp.nortel.com/Users
Enterprise Admins	lcs2005s.corp.nortel.com/Users
Group Policy Creator O...	lcs2005s.corp.nortel.com/Users
RTC Server Applications	lcs2005s.corp.nortel.com/Users
Schema Admins	lcs2005s.corp.nortel.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

MCM is installed on a Home Server for small deployments of 500 users or fewer with low traffic.

For large networks with multiple home servers or high traffic, MCM must run on top of a Live Communications Server Proxy to ensure Nortel support. This installation results in an easy deployment that can serve multiple Home Servers.

This installation also requires that you add a host authorization entry in the Application Proxy/MCM Proxy for the Enterprise Edition pool fully qualified directory number (FQDN), as well as every Enterprise Edition Home Server FQDN sitting behind the Load Balancer.

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.

The MCM Service User account may be removed from the Administrators group if it meets the following additional requirements:

1. The account must be a member of the "RTC Local Administrators" local group.
2. The account must have read/write access to its folder ("%ProgramFiles%\Nortel Networks\MCM" by default). It may be

configured after the MCM installation, but access must be established prior to the first MCM Service startup.

> ***Note:*** A reboot of the server is required to complete the installation of MCM.

Uninstalling MCM

Use the Windows Add/Remove Programs utility to uninstall MCM. Be sure you stop MCM before you uninstall it.

Upgrading MCM

Upgrading MCM involves uninstalling the old version of MCM and then installing the new version.

Patching

Patching is supported by deploying an MCM up-issue. MCM uninstall/install is required for this up-issue.

Configuring MCM

The Multimedia Convergence Manager (MCM) is one of the software components provided by Nortel to enable voice connectivity between CS 1000 clients and the Live Communications Server 2005 clients. MCM consists of the following modules:

- Call Processing Service
- Management Console

The MCM Call Processing Service handles the SIP telephony traffic between the CS 1000 and the Live Communications Server. The Management Console provides real-time status of the MCM, Live Communications Server, Primary NRS, and Secondary NRS. It also provides Administrative, Maintenance, and Configuration tools.

Microsoft® Live Communications Server 2005 SP1 provides multimedia and collaboration features such as Video, IM, Presence, White Board, Application Sharing, and VoIP capability. MCM enables the SIP VoIP connectivity between the CS 1000 and the Live Communications Server 2005 in addition to the TR/87 authorization functionality required for the Office Communicator 2005 Remote Call Control capability.

Phones in a CS 1000 system can make direct SIP calls to Live Communications Server clients where the dialed number is mapped to the corresponding user ID using LDAP queries to the corporate Active Directory. MCM also allows the Live Communications Server clients to originate ESN and trunk calls to corporate and external users.

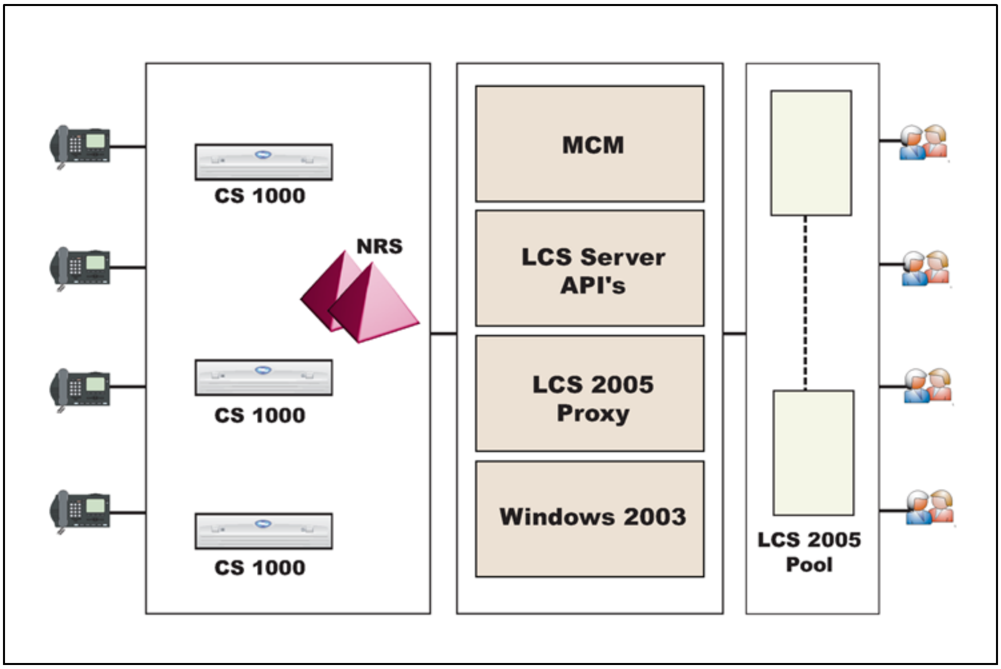
MCM architecture

MCM resides between the Live Communications Server and CS 1000. As shown in Figure 48 "MCM architecture" (page 100), MCM runs on top of the Live Communications Server 2005 Proxy which, in turn, runs on top of Windows 2003. MCM must run on top of a Live Communications Server 2005 Proxy server (the only exception is small networks where only one Home Server is required). The Live Communications Server Proxy is required for handling traffic if you run multiple Home Servers.

At this time, installation of the MCM on an Live Communications Server 2005 Enterprise Edition Server (Home Server) within an Enterprise Pool is not supported. For Converged Office solutions with Live Communications Server Enterprise Edition deployments, the following is recommended:

- addition of a Live Communications Server 2005 Proxy server
- installation of the MCM application on the Proxy server rather than on a Home Server within the pool

Figure 48
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 determine how it should be configured.

Example 1: Outgoing calls from Office Communicator

In this example, an invite travels from the client to the Live Communications Server Home Server and then on to the Live Communications Server MCM Proxy. MCM checks to see which NRS is active, and then sends an invite to that NRS. In this case, the invite is not qualified (using a sample number of 6 231 5555).). To return from the NRS, 302 is used.

The invite is now sent unqualified to the CS 1000 associated with the originator's location code and DN.

Example 2: incoming calls to Office Communicator with PCA

In this example, the user has a desktop phone and a PCA pointing to a Live Communications Server 2005 server. The PCA sends a DN or Routing DN. The call was originally going to 6 231 3052, but the PCA 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, 8214) should also be configured by a DSC (for example, 82). 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, look for a special header injected by the invite. That header, called x-nt-ocn, contains the actual number called. Use this header to compare against the Active Directory map for the user ID. This method is used to prevent you from having to program the hot key for each user to determine the correct DN upon which to terminate the call.

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

MCM Direct configuration

For small CS 1000 deployments (without SRS), 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.

> ***Note:*** MCM does not check CS 1000 availability in Direct mode configuration.

For a complete description of the various MCM configuration screen fields, refer to "MCM Configuration screen" (page 104).

The MCM management console

The following is a list of possible statuses for the various MCM components:

MCM

- Running
- Pending
- Stopped

LCS

- Running
- Pending
- Stopped

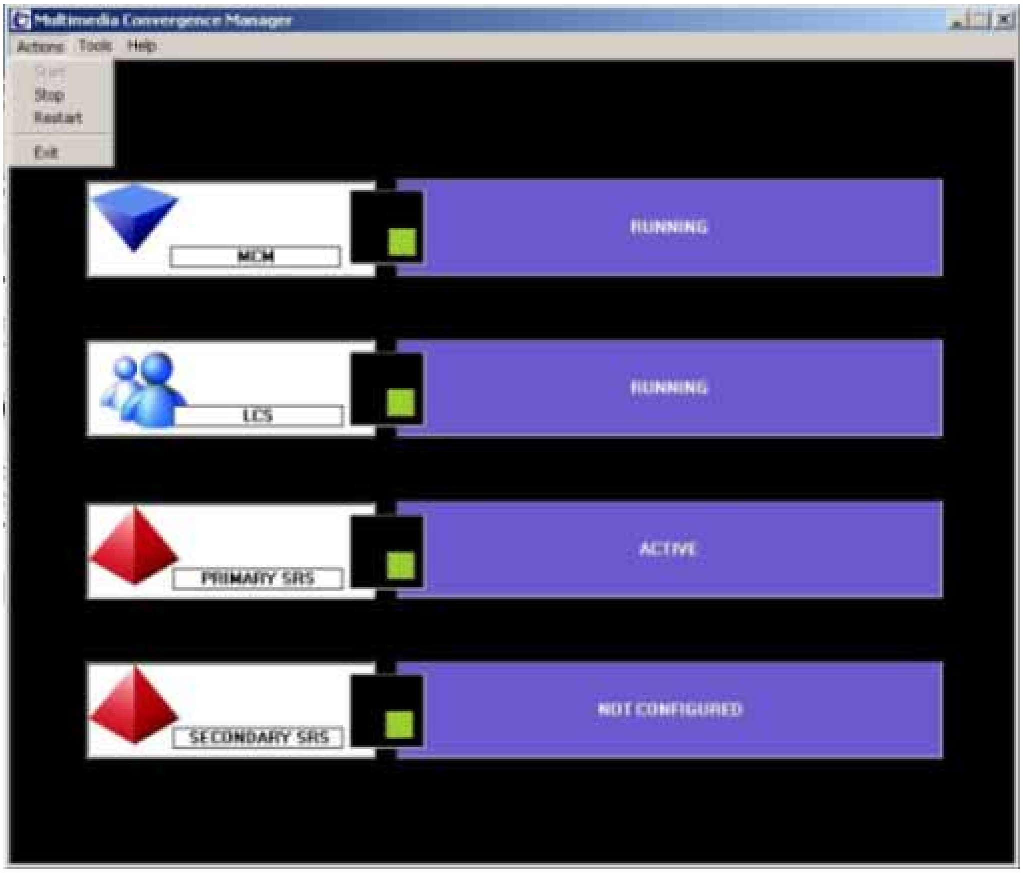
Primary SRS (the IP address of the Primary SRS server)

- **Active** - Primary SRS is active. All messages are sent through the Primary NRS.
- **Standby** - Primary SRS is alive. The Secondary SRS is active.
- **Down** - Primary SRS is down. For normal processing, the Secondary SRS should be switched to Active state.

Secondary SRS (the IP address of the Secondary SRS server)

- **Active** - Secondary SRS is active, which is possible only if the Primary SRS is down.
- **Standby** - Secondary SRS is alive, which is the normal state if the Primary SRS is active.
- **Down** - Secondary SRS is down. It is not possible to switch to it.

Figure 49
MCM Management Console



MCM menu options

MCM has three menu options: Actions, Tools, and Help. The following describes the function of each menu item:

Actions menu:

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

Tools menu:

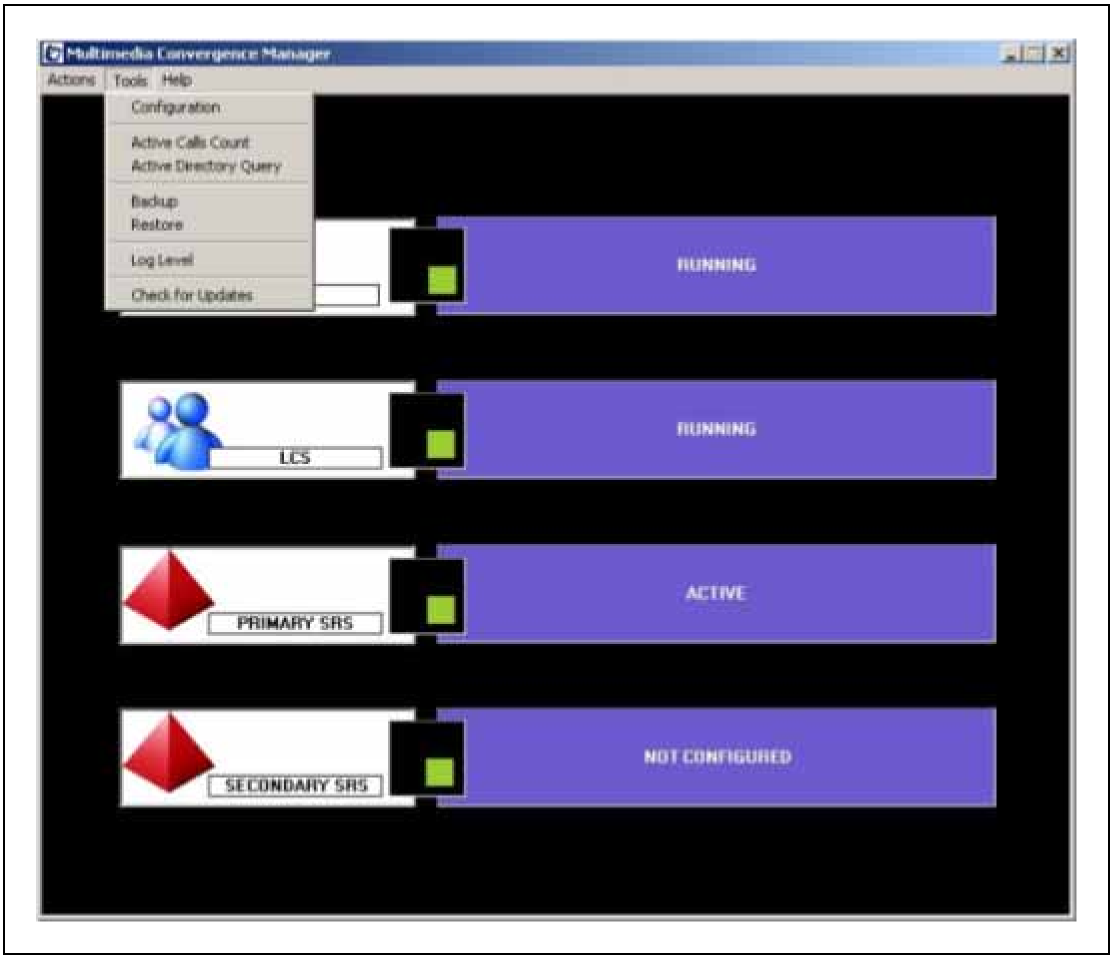
- Configuration
- Active Calls Count
- Active Directory Query

- Backup
- Restore
- Set Log Level

Help menu:

Get Help information and general information about MCM.

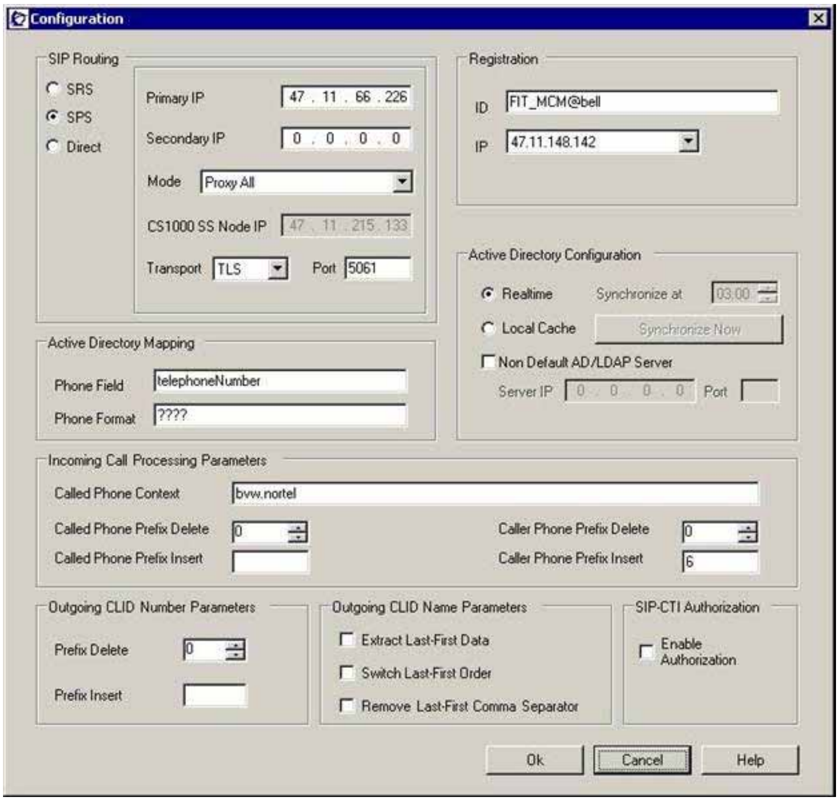
Figure 50
MCM menu options



MCM Configuration screen

This section describes the various fields in the MCM Configuration screen (Figure 51 "MCM Configuration" (page 105)).

Figure 51
MCM Configuration



SIP Routing
○ SRS
● SPS
○ Direct
Primary IP: 47 . 11 . 66 . 226
Secondary IP: 0 . 0 . 0 . 0
Mode: Proxy All
CS1000 SS Node IP: 47 . 11 . 215 . 133
Transport: TLS
Port: 5061

Registration
ID: FIT_MCM@bell
IP: 47.11.148.142

Active Directory Configuration
● Realtime
Synchronize at: 03:00
○ Local Cache
□ Non Default AD/LDAP Server
Server IP: 0 . 0 . 0 . 0
Port:

Active Directory Mapping
Phone Field: telephoneNumber
Phone Format: ????

Incoming Call Processing Parameters
Called Phone Context: bvw.nortel
Called Phone Prefix Delete: 0
Called Phone Prefix Insert:
Caller Phone Prefix Delete: 0
Caller Phone Prefix Insert: 6

Outgoing CLID Number Parameters
Prefix Delete: 0
Prefix Insert:

Outgoing CLID Name Parameters
□ Extract Last-First Data
□ Switch Last-First Order
□ Remove Last-First Comma Separator

SIP-CTI Authorization
□ Enable Authorization

SIP Routing The SIP Routing options are SIP Redirect Service (SRS), which is similar to NRS in Release 4.5, SIP Proxy Server (SPS), and Direct. If you have only one system (as opposed to a network), select Direct and enter the CS 1000 IP address to point directly to the CS 1000 (the Node IP of the SIP CTI Signaling Server).

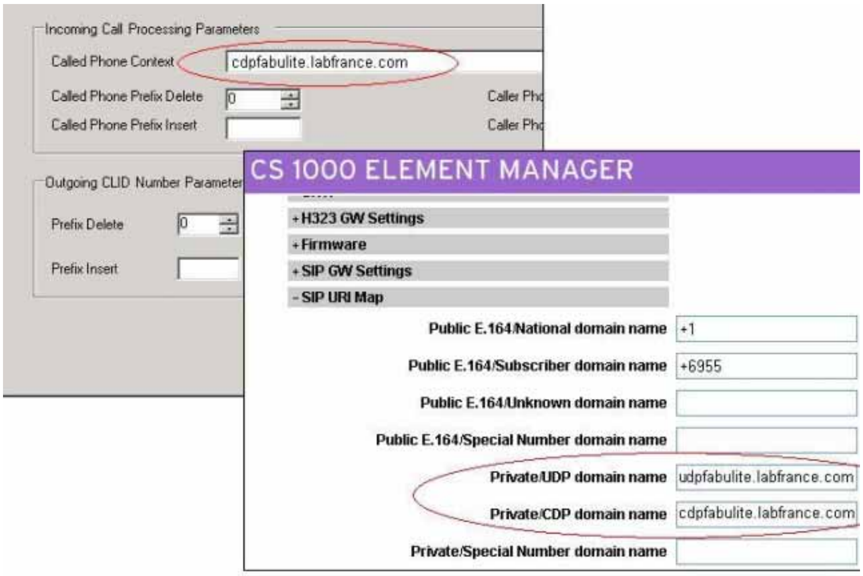
> ***Note 1:*** The name configured on the SRS (Gateway endpoint) and the name entered inside the MCM configuration file must match. The name is case sensitive.
>
> ***Note 2:*** The MCM requires access rights to certain directories (for example: “Program Files/ MCM…”). Ensure that the user has the Administrators rights to these directories.

ATTENTION

IMPORTANT!

The Called Phone Context entry in the MCM Configuration screen and the entries for UDP and CDP in the Signalling Server Element Manager must the same, as shown in Figure 52 "Element Manager SIP URI MAP" (page 106). Entries are case sensitive.

Figure 52
Element Manager SIP URI MAP



Incoming Call Processing Parameters

Called Phone Context: cdpfabulite.labfrance.com

Called Phone Prefix Delete: 0

Called Phone Prefix Insert:

Outgoing CLID Number Parameter

Prefix Delete: 0

Prefix Insert:

CS 1000 ELEMENT MANAGER

Public E.164/National domain name: +1

Public E.164/Subscriber domain name: +6955

Public E.164/Unknown domain name:

Public E.164/Special Number domain name:

Private/UDP domain name: udpfabulite.labfrance.com

Private/CDP domain name: cdpfabulite.labfrance.com

Private/Special Number domain name:

Registration Registration ID can be configured in two forms:

1. **End_Point_Name@Service_Domain_Name**, where End_Point_Name is the MCM End Point Name configured on the NRS and Service_Domain_Name is the service domain name configured on the NRS where the MCM End Point belongs.
2. **End_Point_Name**, where End_Point_Name is the MCM End Point Name configured on the NRS. In this case, the first domain name served by Live Communications Server (configured in the properties of the domain forest of the Live Communications Server snap-in) is used by MCM.

If you choose the NRS, then this justifies the registration ID of the MCM. Imagine the MCM as another CS 1000 endpoint in the network. The MCM requires a registration IP ID and IP (if that the server runs as multiple IPs, you need to specify which IP).

Note: Authentication is not supported for MCM configuration in the NRS.

Active Directory Mapping The Active Directory Mapping field allows you to define which phone field you use for mapping. In the Active Directory, a user may have a business phone number, an IP phone number, and so on. This field defines which phone you are using. For the Phone Format field, the actual phone number stored in the Active Directory can be similar to the format in Figure 51 "MCM Configuration" (page 105). The format in this field must match the format in Active Directory exactly to correctly map the phone number for incoming calls.

Digits received by MCM from a CS 1000 are mapped into ??????? fields—for example, the number 5703334 maps into ESN 570-3334 for lookup in the Active Directory Phone Field. There are two main formats in Active Directory Mapping: **UDP** and **CDP**. For example:

- with UDP, if the Phone Field contains numbers like **ESN 570-3334**, the Phone Format field should be **ESN ???-????.**
- with CDP, if the Phone Field contains numbers like **3334**, the Phone Format field should be **????.**

Active Directory Configuration There are two modes for Active Directory Configuration: Realtime or Local Cache. Realtime mode is used for end-user ID mapping, which requires an LDAP query. Local Cache mode involves caching the Active Directory on the MCM server and using that cache information for queries.

This cache updates every day by default at the same time. You can force it to synchronize by clicking the Synchronize Now button. During the synchronization, which generally takes 20 to 25 seconds, a switch to Realtime mode occurs.

> ***Note:*** Microsoft® recommends placing a GC Controller inside every network site. Nortel's GC LDAP server contains about 50 000 user records. The synchronization with local GC takes about 20-25 seconds. The GC LDAP server provides access to the Active Directory Global Catalog (GC) through the Lightweight Directory Access Protocol (LDAP). If the user is unfamiliar with GC, it is preferable to leave the default values in place.

The Local Cache is then used for mapping. The Non Default Active Directory/LDAP Server option is used for non-default active directories configured for Windows 2003 and Live Communications Server deployment.

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

The non-default LDAP server configuration may be used to:

1. specify GC LDAP server (the Port field is 3268 or blank) if there are multiple GC Domain Controllers in the Active Directory forest and only this server should be used.
2. specify non-GC LDAP server to reduce the search scope to only one domain.

To propagate an Active Directory field to GC, MCM uses the default telephoneNumber field. If this field is already in use for other purposes, the otherTelephone field may be used. Note, however, that the otherTelephone field is not replicated to Active Directory.

Active Directory Query The Active Directory Query tool allows users to check Active Directory mapping configuration. It searches for a user-id (SIP URI) by a given phone 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 Chris Smith is defined in the Active Directory as:

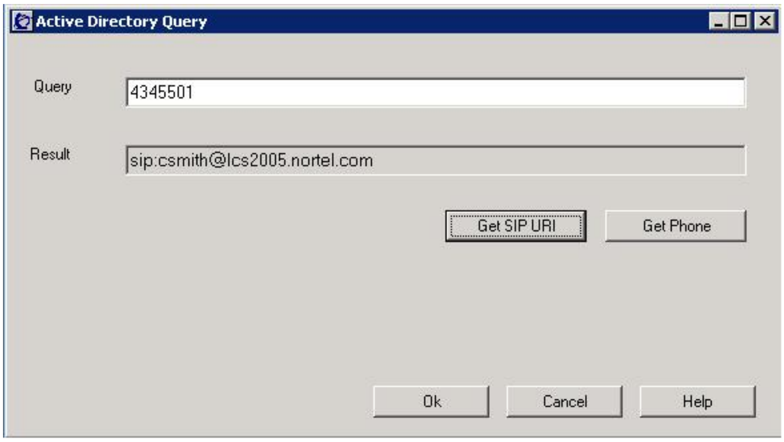
SIP URI: sip:csmith@lcs2005.nortel.com

Telephone number: ESN 434-5501

The phone format is defined as ESN ???-???? in MCM configuration.

If you type the phone number in the Query field and press Get SIP URI button, the SIP URI appears in the Result field (as shown in Figure 53 "Get SIP URI" (page 108)).

Figure 53
Get SIP URI

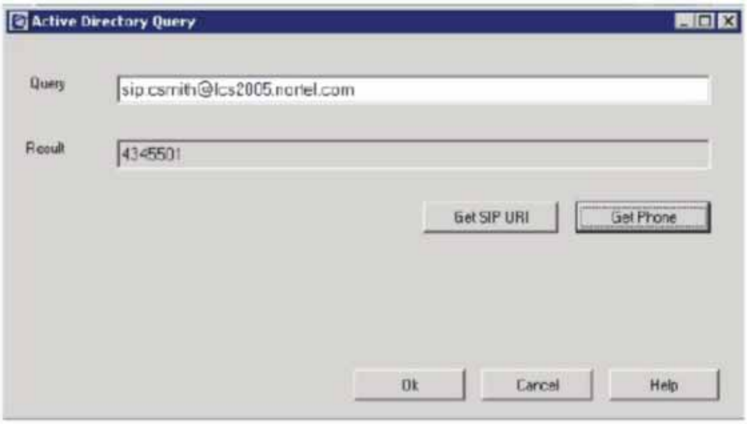


Query 4345501

Result sip:csmith@lcs2005.nortel.com

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 54 "Get phone" (page 109)).

Figure 54
Get phone



Query: sip:csmith@lcs2005.nortel.com

Result: 4345501

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

This manipulation is generally not necessary, but is available in case a scenario requires this type of manipulation. The Caller Phone Prefix Delete and Insert is used when Office Communicator maps to a user ID. When a CS 1000 phone calls MCM and then Office Communicator, a pop-up window appears, and that pop-up displays the caller's user ID. This pop-up takes place on Office Communicator, and results from mapping the caller phone number to a user ID.

The origin of this mapping is the From header in the invite that comes to MCM and then to Office Communicator (for example, Office Communicator cannot map a number like 343 8888, because those numbers are normalized and stored in Office Communicator in the following format: X 343 8888 (a dialable number). In this scenario, insert 6 so that it matches a dialable number. Office Communicator can then map it to a user ID. So, when A calls B on a CS 1000, and the call terminates on the Live Communications Server, Office Communicator can see who originated the call. B answers the call from A, and once the connection is established, B can also use IM, whiteboard, and other tools to communicate with A.

This information is configured on the Signaling Server and the NRS. For more information, refer to "URI Mapping" (page 151).

Outgoing CLID Number Parameters You can inject identity headers for calls going from Office Communicator to a CS 1000. Then, when a call is made from Office Communicator to a CS 1000 phone, you see the Calling Line ID (CLID) number and name. The first field, Prefix Delete, is not used often, but is available in case a CLID number needs to be manipulated.

Outgoing CLID Name Parameters Outgoing CLID Name Parameters manipulate the name string to display the name on a CS 1000 phone in the desired format. The name must be defined in the Active Directory in the following format: Last, First [additional info].

Extract Last-First Data This field extracts the Last and First names and removes the rest from the name string.

Switch Last-First Order This field switches the order of the Last and First names in the name string.

Remove Last-First Comma Separator This field removes the comma separator between the Last and First names.

TR/87 Authorization TR/87 Authorization enables the authorization of the TR/87 (SIP-CTI) INVITEs from the Office Communicator to ensure that an Office Communicator user has control only over their own phone (as defined in Active Directory).

Configuring MCM for Remote Call Control

For Remote Call Control, the Nortel MCM application that resides within the Live 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 Microsoft® Communicator clients. The following is a summary of the authorization algorithm:

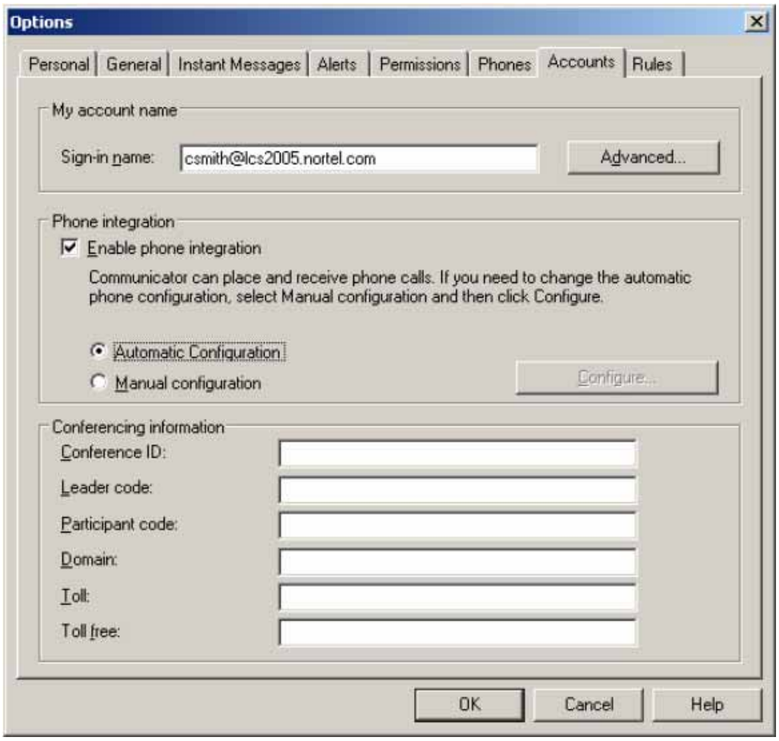
1. The SIP INVITE or INFO "from" header provides the **Requestor Identity** (for example, the Live Communications Server user identity).
2. The CSTA XML message provides the **Controlled Device Identity** (for example, the phone URI).
3. The **Owner Identity** is found by a reverse lookup using the Controlled Device Identity found in Step 2 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 Step 3, the Owner Identity is equal to the Requestor Identity, and msRTCSIP-OptionFlags (RCC bit - 5th bit) is set to **equal 1**, then approve the request. Otherwise, reject the request.

The primary function of MCM (when authorization is enabled, see Figure 55 "Enable phone integration" (page 111)) 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 is configured in Active Directory for that user by the system administrator. 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 55
Enable phone integration



My account name

Sign-in name: csmith@lcs2005.nortel.com

Phone integration

☑ Enable phone integration

Communicator can place and receive phone calls. If you need to change the automatic phone configuration, select Manual configuration and then click Configure.

● Automatic Configuration

○ Manual configuration

Conferencing information

Conference ID:

Leader code:

Participant code:

Domain:

Toll:

Toll free:

Redundancy

Redundancy of the TR/87 interface is not provided natively with Live Communications Server 2005. 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.

Select component for configuration

If you have elected to configure Telephony Gateway and Services, continue reading. If, however, you are configuring for Remote Call Control, proceed to "Configuring Remote Call Control" (page 159).

Configuring Telephony Gateway and Services

This section describes the process you must follow to properly configure the Telephony Gateway and Services component.

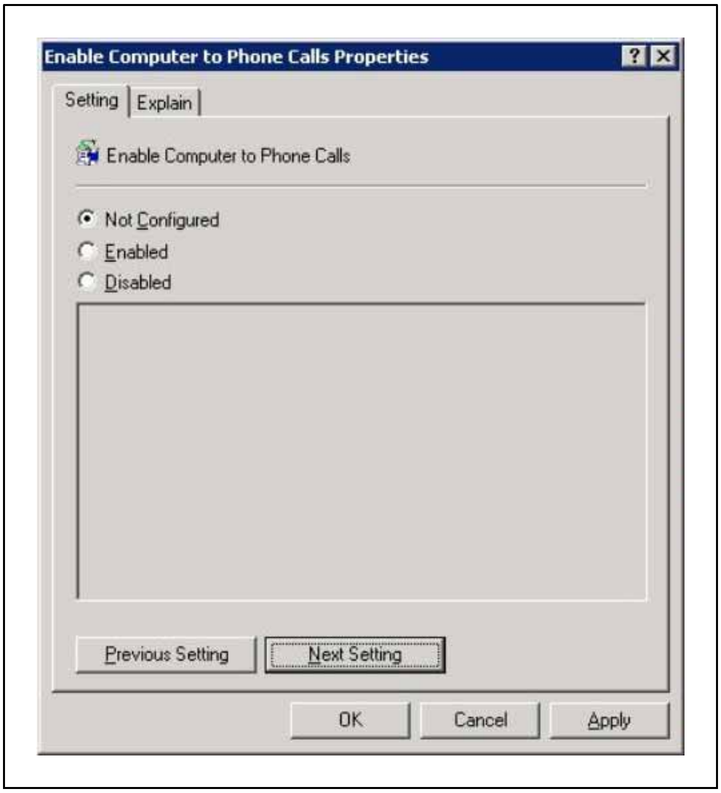
Configuring Live Communications Server

The starting point for Telephony Gateway and Services configuration is the Live Communications Server 2005 component.

Group Policy

For Telephony Gateway and Services to operate properly, each Office Communicator 2005 user’s group policy must have Computer-to-Phone calling enabled (see Figure 56 "Group policy settings" (page 113)). Procedure 2 in Procedure 2 "Enabling a group policy" (page 113) describes the process required to add/change a group policy.

Figure 56
Group policy settings



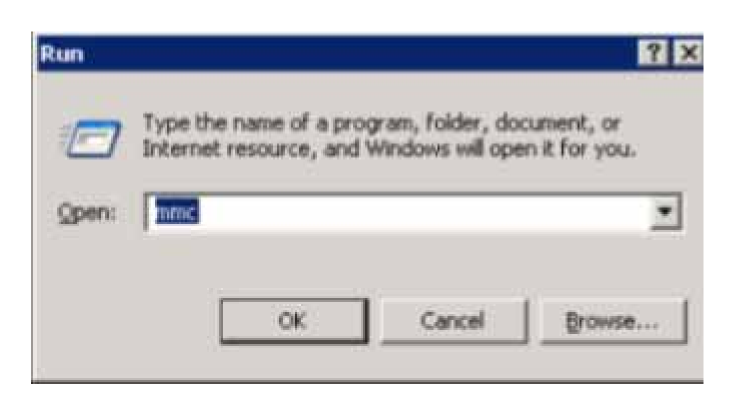
Enable Computer to Phone Calls

● Not Configured
○ Enabled
○ Disabled

Procedure 2
Enabling a group policy

Step	Action
1	Choose **Start/Run > MMC** (see Figure 57 "Start/Run" (page 113))

Figure 57
Start/Run

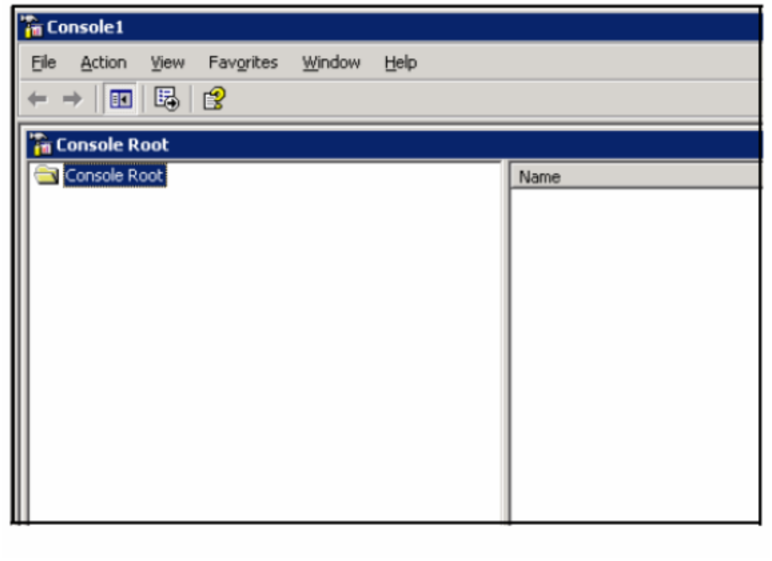


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

2	Choose **File > Add-remove snap-in** for Console1.

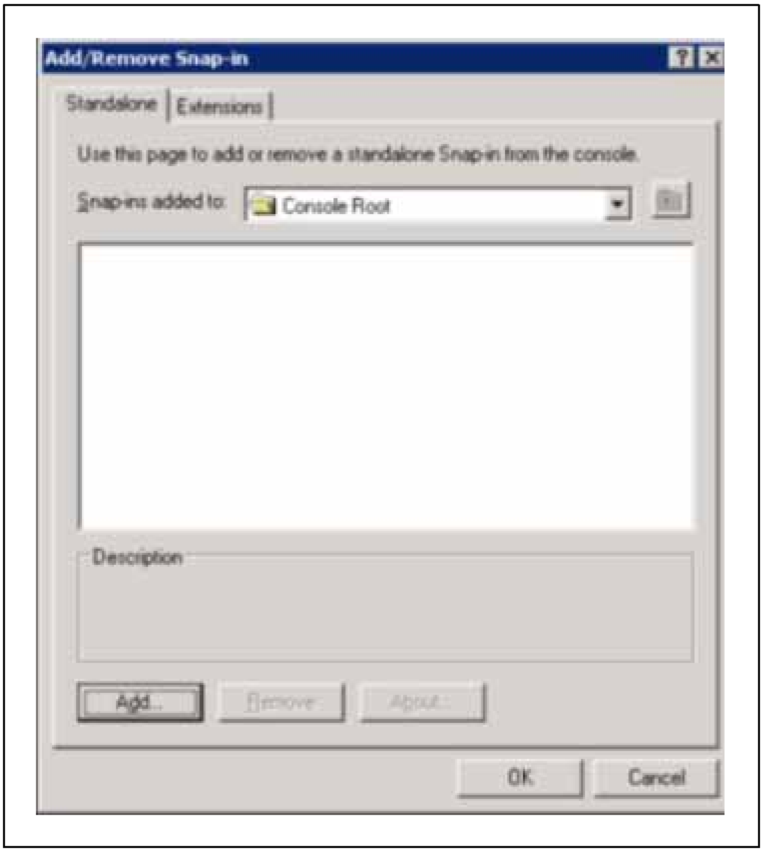
Figure 58
Console 1



3 Select Console Root from the "Snap-ins added to" menu (see Figure 59 "Add/Remove Snap-in" (page 115)).

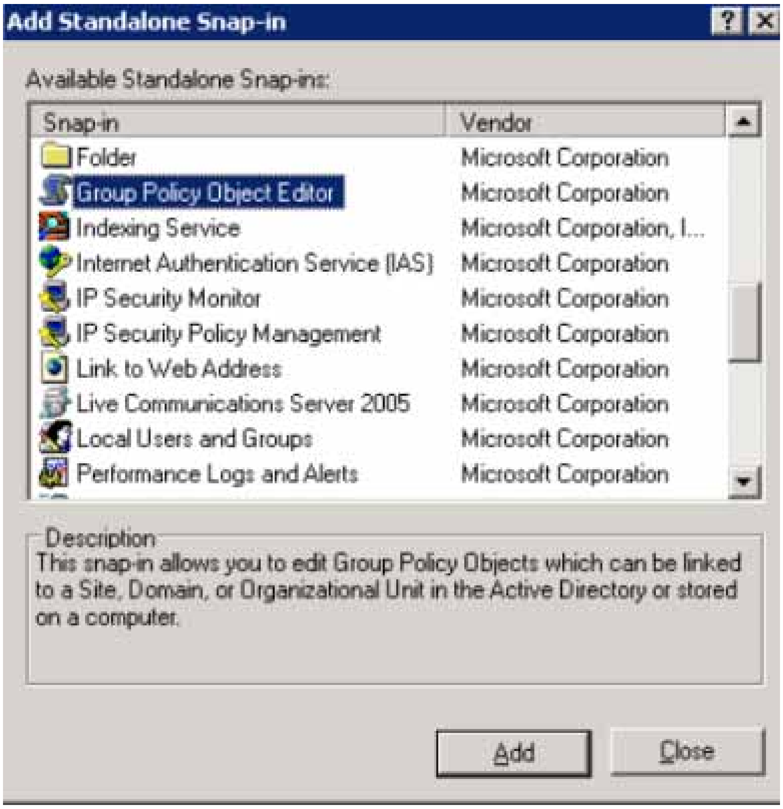
4 Click **Add**.

Figure 59
Add/Remove Snap-in



5 Select Group Policy Object Editor and click Add (see Figure 60 "Add Standalone Snap-in" (page 116)).

Figure 60
Add Standalone Snap-in

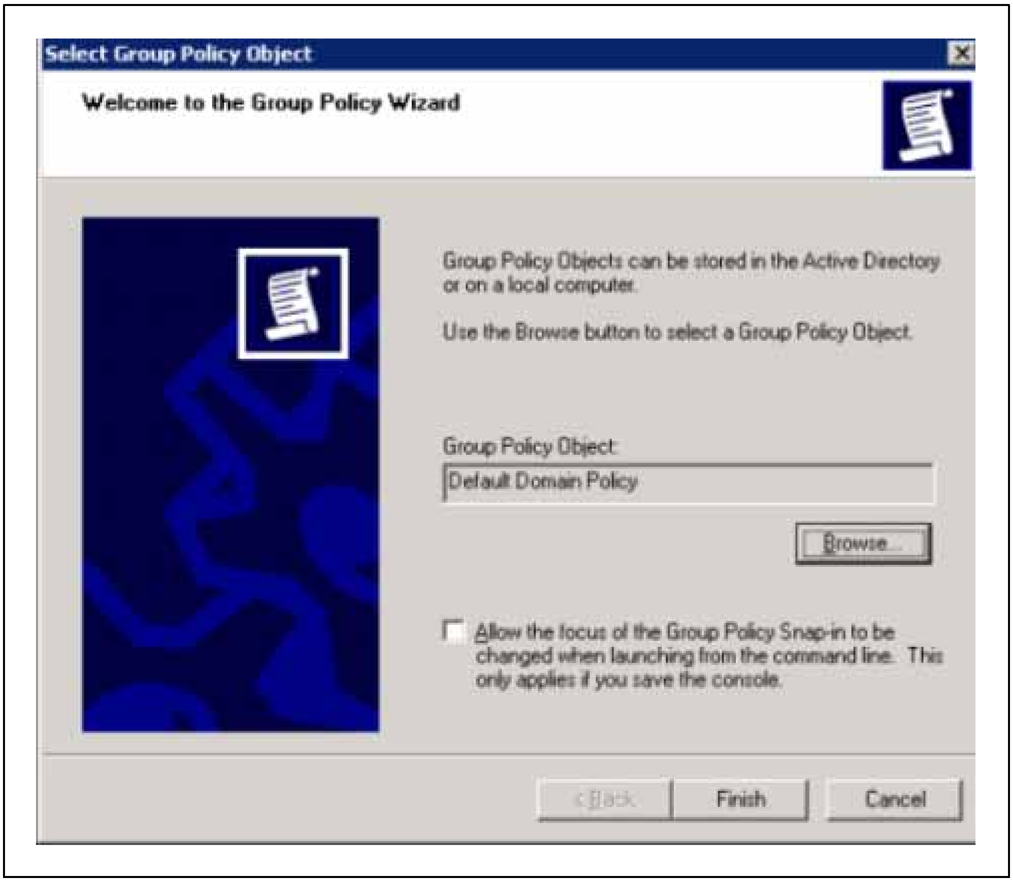


Snap-in	Vendor
Folder	Microsoft Corporation
Group Policy Object Editor	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
Internet Authentication Service (IAS)	Microsoft Corporation
IP Security Monitor	Microsoft Corporation
IP Security Policy Management	Microsoft Corporation
Link to Web Address	Microsoft Corporation
Live Communications Server 2005	Microsoft Corporation
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation

Description
This snap-in allows you to edit Group Policy Objects which can be linked to a Site, Domain, or Organizational Unit in the Active Directory or stored on a computer.

6 The Group Policy object should be the local computer and handled on a per-computer basis. It is recommended that group policies also be handled on a per-domain basis (as shown in Figure 61 "Select Group Policy Object" (page 117)). Click **Finish** and then **Close**.

Figure 61
Select Group Policy Object



Select Group Policy Object

Welcome to the Group Policy Wizard

Group Policy Objects can be stored in the Active Directory or on a local computer.

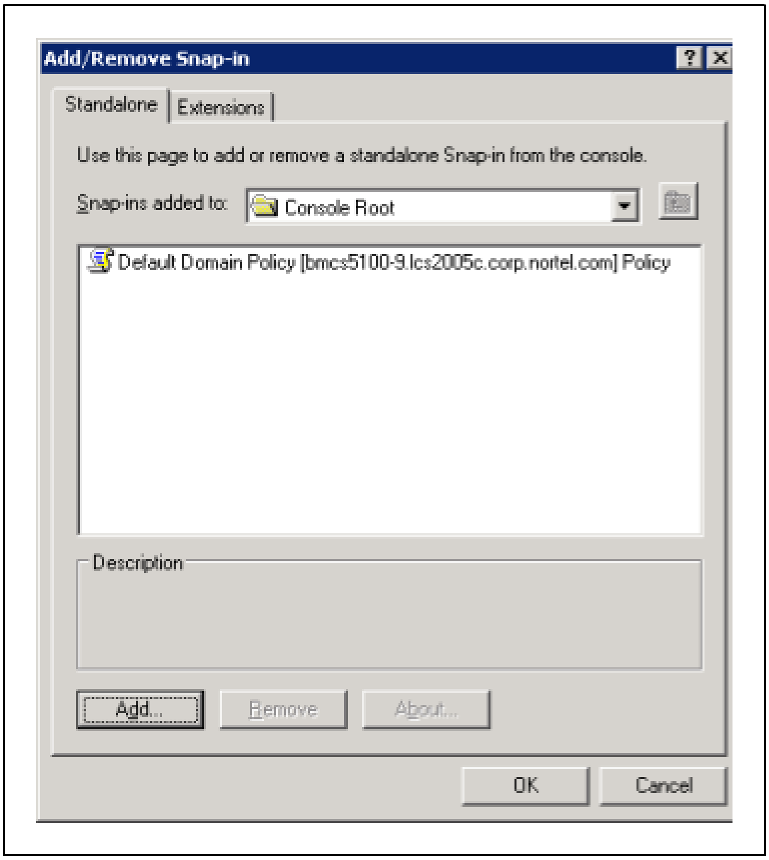
Use the Browse button to select a Group Policy Object.

Group Policy Object:
Default Domain Policy

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

7 Click **OK**, with the local computer policy showing as “added” (see Figure 62 "Add/Remove Snap-in" (page 118)).

Figure 62
Add/Remove Snap-in



Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

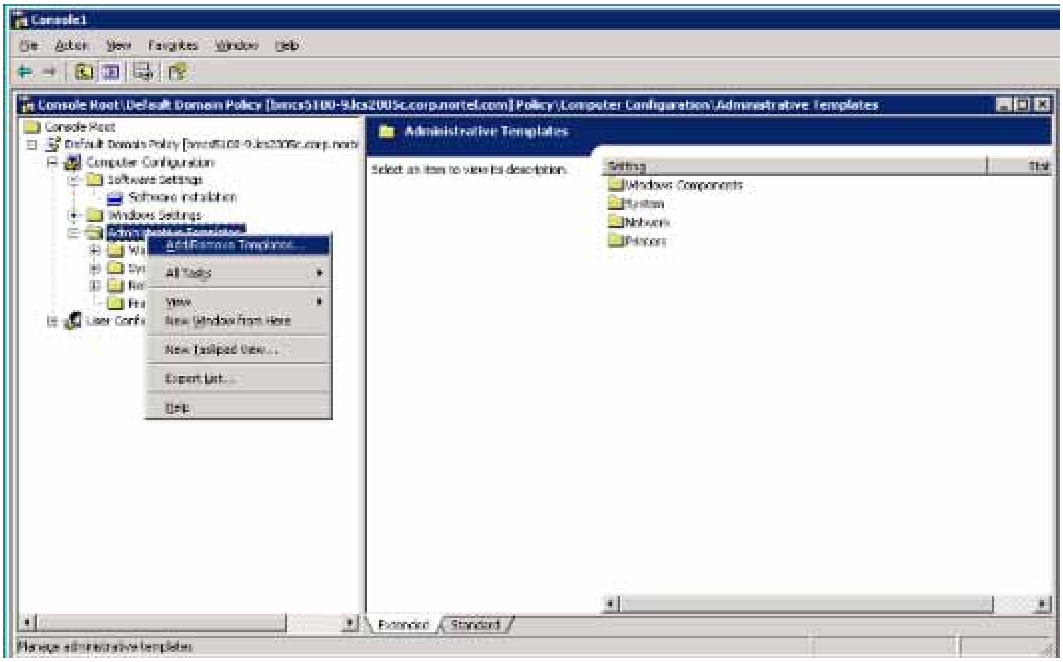
Snap-ins added to: Console Root

Default Domain Policy [bmcs5100-9.lcs2005c.corp.nortel.com] Policy

Description

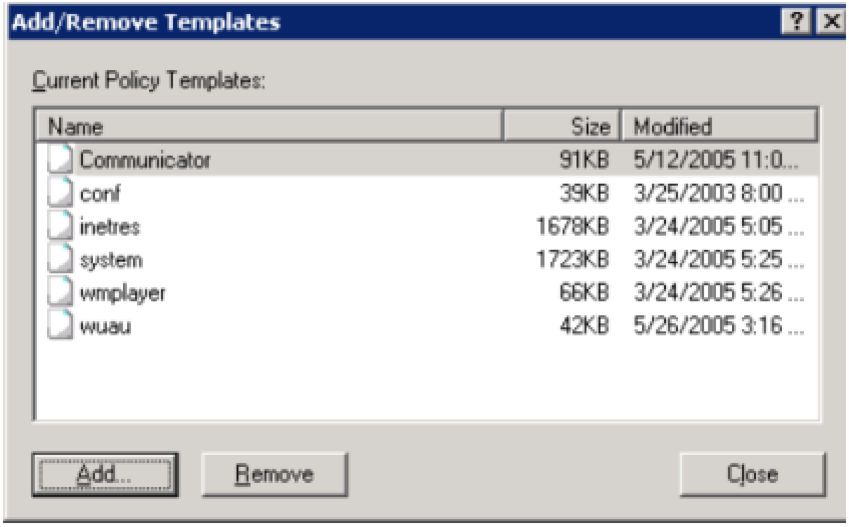
8 In the Console Root frame (see Figure 63 "Console Root" (page 119)), expand the **Local Computer Policy** (in this case, the Default Domain Policy). Expand **Computer Configuration** and right-click **Administrative Templates**. Select **Add/ Remove Templates**.

Figure 63
Console Root



9 Click **Add**.

Figure 64
Add/Remove Templates

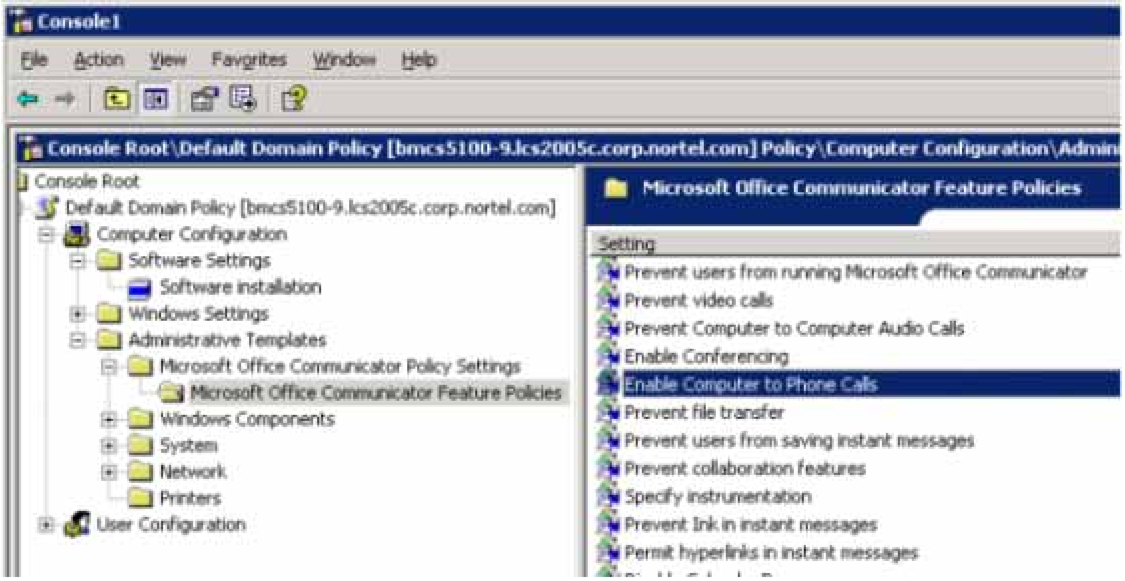


Name	Size	Modified
Communicator	91KB	5/12/2005 11:0...
conf	39KB	3/25/2003 8:00 ...
inetres	1678KB	3/24/2005 5:05 ...
system	1723KB	3/24/2005 5:25 ...
wmplayer	66KB	3/24/2005 5:26 ...
wuau	42KB	5/26/2005 3:16 ...

10 Browse to find and click **Communicator.adm** (in the install directory of Office Communicator). During the installation of Office

Communicator, Communicator.adm is included as one of the files. Press **Close**.

Figure 65
Console Root



Console Root\Default Domain Policy [bmcs5100-9.lcs2005c.corp.nortel.com] Policy\Computer Configuration\Admin

- Console Root
  - Default Domain Policy [bmcs5100-9.lcs2005c.corp.nortel.com]
    - Computer Configuration
      - Software Settings
        - Software installation
      - Windows Settings
      - Administrative Templates
        - Microsoft Office Communicator Policy Settings
          - Microsoft Office Communicator Feature Policies
        - Windows Components
        - System
        - Network
        - Printers
    - User Configuration

Microsoft Office Communicator Feature Policies

Setting
Prevent users from running Microsoft Office Communicator
Prevent video calls
Prevent Computer to Computer Audio Calls
Enable Conferencing
Enable Computer to Phone Calls
Prevent file transfer
Prevent users from saving instant messages
Prevent collaboration features
Specify instrumentation
Prevent Ink in instant messages
Permit hyperlinks in instant messages

11 In the Console Root frame, the Administrative Templates have a new subfield. To access this new subfield, expand **Local Computer Policy > Computer Configuration > Administrative Templates > Microsoft Office Communicator Policy Settings** (see Figure 65 "Console Root" (page 120)).

12 Click **Microsoft Office Communicator Feature Policies**.

13 In the frame on the right, right-click **Prevent Video Calls** and select **Properties**. Click **Disable > Ok**.

14 Right-click **Prevent Computer to Computer Audio Calls** and select **Properties**. Click **Disable > Ok**.

15 Right-click **Enable Computer to Phone Calls** and select **Properties**. Click **Enable > Ok**.

16 Right-click **Prevent Collaboration Features** and select **Properties**. Click **Disable > Ok**.

17 Right-click **Enable Phone Control** and select **Properties**. Click **Enable > Ok**.

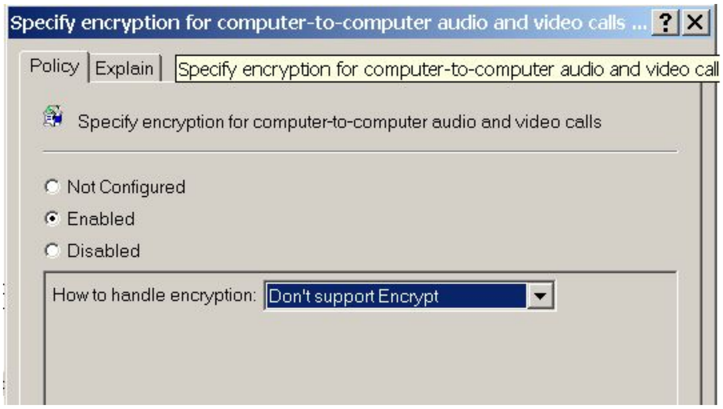
18 Right-click **Disable Call Presence** and select Properties. Click **Disable > Ok**.

19 All other features should be set to “Not configured” at this time.

20 Close the Console Root window. When asked to save Console1 settings, click **No**. The settings are saved to the registry, there is no need to save them to an external file.

> ***Note:*** In order for SIP Gateway Office Communicator-to-SIP Gateway Office Communicator video calls to work, the group policy for "Specify encryption for computer-to-computer audio and video calls" must be enabled and match for Office Communicator clients. To enable these calls, select **Enabled**, in the Policy tab. In the **How to handle encryption:** menu, select **Don’t support Encryption** (see Figure 66 "Specify encryption for computer-to-computer audio and video calls" (page 121)).

Figure 66
Specify encryption for computer-to-computer audio and video calls


Specify encryption for computer-to-computer audio and video calls ...
?
Policy
Explain
Specify encryption for computer-to-computer audio and video call

Specify encryption for computer-to-computer audio and video calls

○ Not Configured
● Enabled
○ Disabled

How to handle encryption: Don't support Encrypt

—End—

Live Communications Server configuration procedures

For the specific Live Communications Server configuration procedures, refer to the Live Communications Server 2005 Deployment Resources page on the Microsoft® site:

www.office.microsoft.com

On the Microsoft® Office web site, search on **Assistance > Live Communications Server 2005 Deployment Resources**. On the results page, select the **Live Communications Server 2005 Deployment Resources** link.

Configuration of Static Routes on all intermediate Live Communications Servers

Configuration of the Live Communications Server involves the configuration of static routes on the Live Communications Server, and configuration of host authorization.

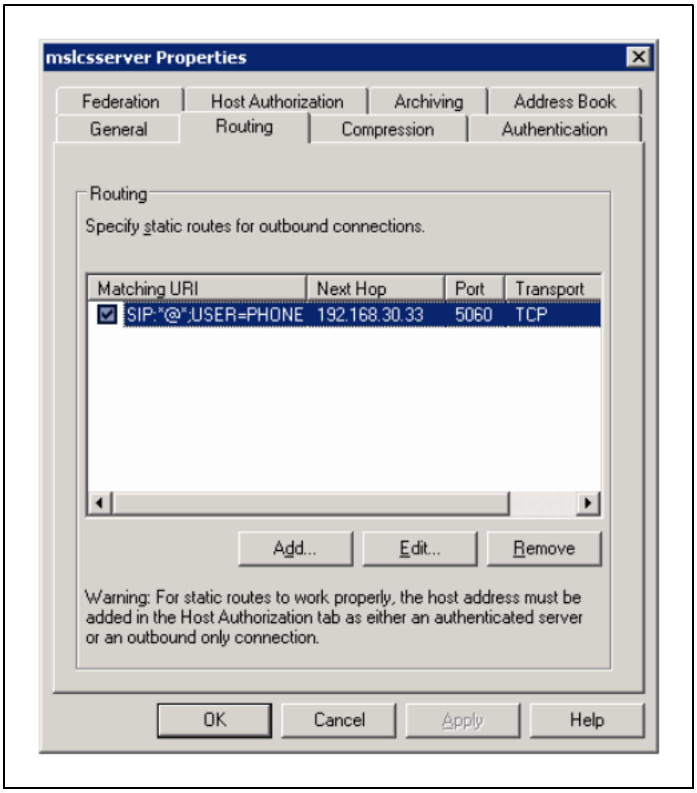
You must configure static routes between the client and server. For information about configuring static routes (Enterprise Edition pool behind a Load Balancer), see *Live Communications Server 2005 Planning Guide*, and the *Live Communications Server 2005 Enterprise Edition Deployment Guide* on the Microsoft® site:

www.microsoft.com/office/livecomm

Routing configuration on Live Communications Server 2005 servers When a call is made using Office Communicator, the home server needs to know where to route the call (for example: is it routed to another Live Communications Server proxy?). The route must be defined using the Routing tab (see Figure 67 "Routing configuration on Live Communications Server 2005 servers" (page 123)). When it terminates on the proxy, the MCM handles the routing by performing a check to determine which NRS is active (usually the primary NRS), and then sends an invite to the active NRS. At this point, it receives a 302 and redirects the call to the correct CS 1000.

> ***Note:*** In small deployments where there is only one Live Communications Server, and it is running MCM, routing entries are not required.

Figure 67
Routing configuration on Live Communications Server 2005 servers



Routing

Specify static routes for outbound connections.

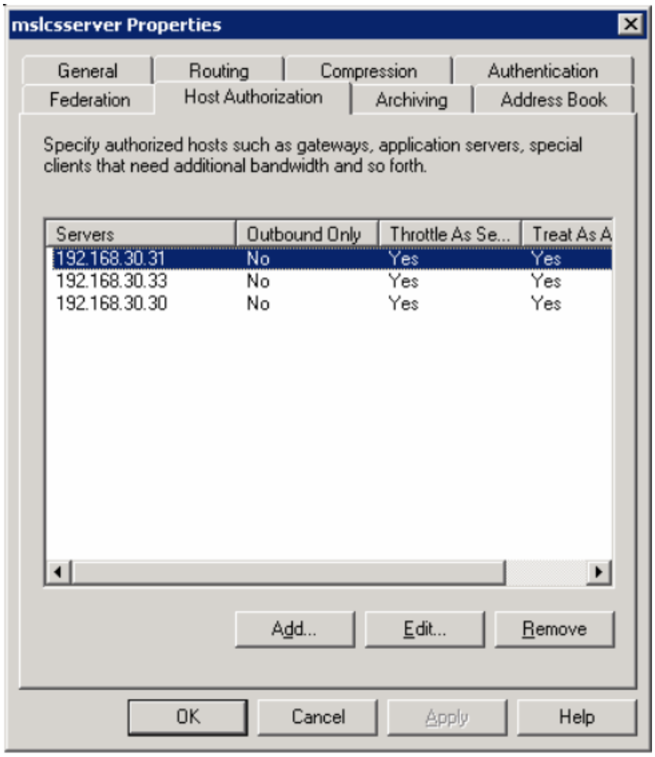
	Matching URI	Next Hop	Port	Transport
☑	SIP:*@*;USER=PHONE	192.168.30.33	5060	TCP

Warning: For static routes to work properly, the host address must be added in the Host Authorization tab as either an authenticated server or an outbound only connection.

Configuring Host Authorization

For one Live Communications Server to communicate with another Live Communications Server, each Live Communications Server must have authorization to speak to the other. The Host Authorization page (see Figure 68 "Host Authorization: Live Communications Server-Live Communications Server, Live Communications Server-CS 1000" (page 124)) is where you establish this authorization.

Figure 68
Host Authorization: Live Communications Server-Live Communications Server, Live Communications Server-CS 1000



Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth.

Servers	Outbound Only	Throttle As Se...	Treat As A
192.168.30.31	No	Yes	Yes
192.168.30.33	No	Yes	Yes
192.168.30.30	No	Yes	Yes

The Host Authorization page (found in a Live Communications Server running MCM), is where all CS 1000 endpoints are configured. These endpoints must be configured as authorized endpoints in the Live Communications Server MCM Proxy. Configure the CS 1000 IP addresses which, in turn, talk to the Live Communications Server server. The same authorization must take place for both Live Communications Server to Live Communications Server authorization and Live Communications Server to CS 1000 authorization.

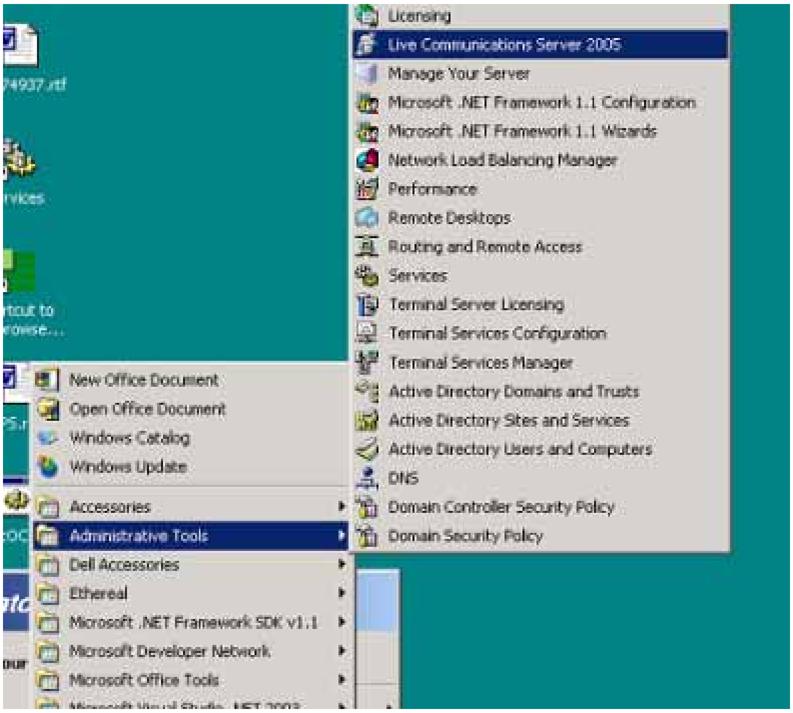
For each Live Communications Server running MCM, Host Authorization is required for the Node IP address of all CS 1000 servers the Live Communications Server interacts with, as well as the TLAN IP address of the Primary, Secondary, and all possible collaborative NRS.

Procedure 3
Configuring a static route and host authorization for the Application Proxy

Step	Action
1	Open the Live Communications Server Management Console. The console is accessed on the Windows server running Live

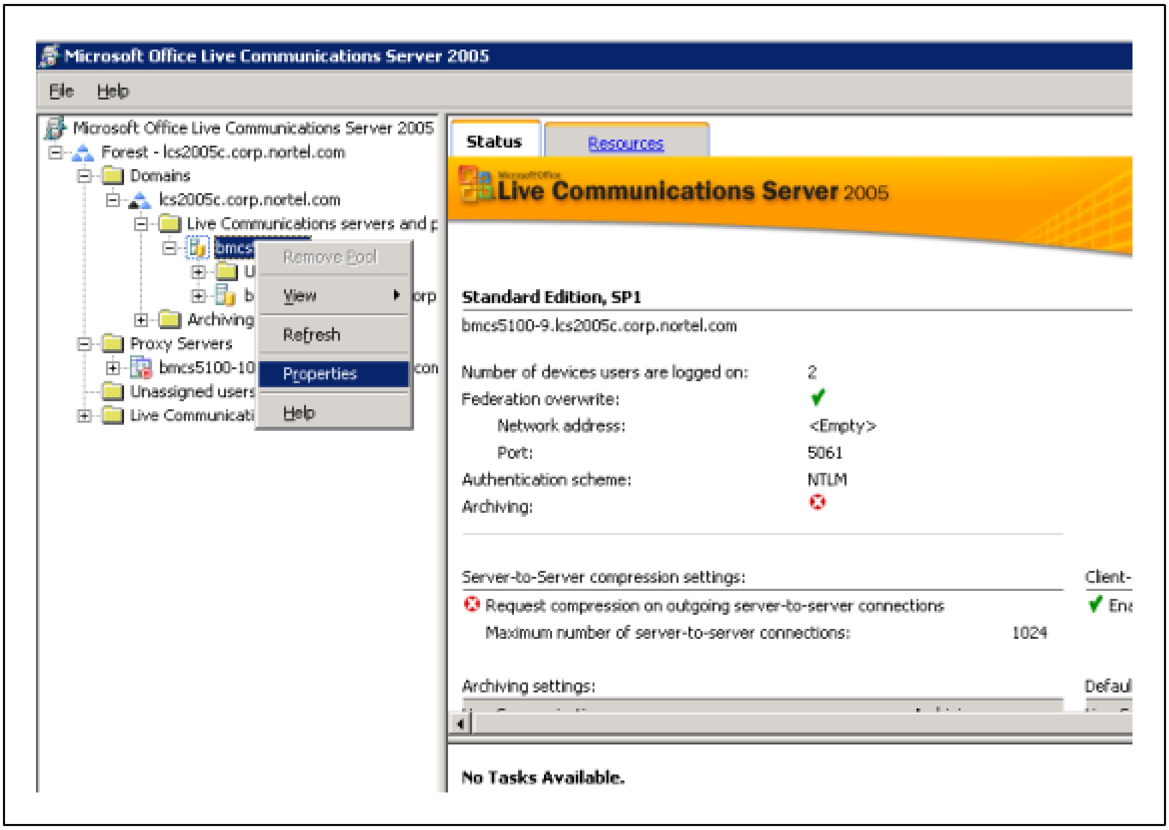
Communications Server, as shown in Figure 69 "Opening the Live Communications Server Management Console" (page 125), by selecting **Start > Program > Administrative Tools > Live Communications Server 2005**.

Figure 69
Opening the Live Communications Server Management Console


74937.rtf
rvices
rtcut to
rowse...
New Office Document
Open Office Document
Windows Catalog
Windows Update
Accessories
Administrative Tools
Dell Accessories
Ethereal
Microsoft .NET Framework SDK v1.1
Microsoft Developer Network
Microsoft Office Tools
Licensing
Live Communications Server 2005
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
DNS
Domain Controller Security Policy
Domain Security Policy

2 In the Live Communications Server Management Console, select the Live Communications Server (the server to which you are adding Host Authorization and changing the Routing) and right-click on that server. From the drop-down menu, select **Properties**. See Figure 70 "Live Communications Server Management Console" (page 126).

Figure 70
Live Communications Server Management Console


Microsoft Office Live Communications Server 2005
File
Help
Microsoft Office Live Communications Server 2005
Forest - lcs2005c.corp.nortel.com
Domains
lcs2005c.corp.nortel.com
Live Communications servers and p
bmcs
U
b
Archiving
Proxy Servers
bmcs5100-10
Unassigned users
Live Communicati
orp
con
Remove Pool
View
Refresh
Properties
Help
Status
Resources
Live Communications Server 2005

Standard Edition, SP1

bmcs5100-9.lcs2005c.corp.nortel.com

Number of devices users are logged on: 2
Federation overwrite: ✓
Network address: <Empty>
Port: 5061
Authentication scheme: NTLM
Archiving: ☒

Server-to-Server compression settings:
☒ Request compression on outgoing server-to-server connections
Maximum number of server-to-server connections: 1024

Client-
✓ Ena

Archiving settings:

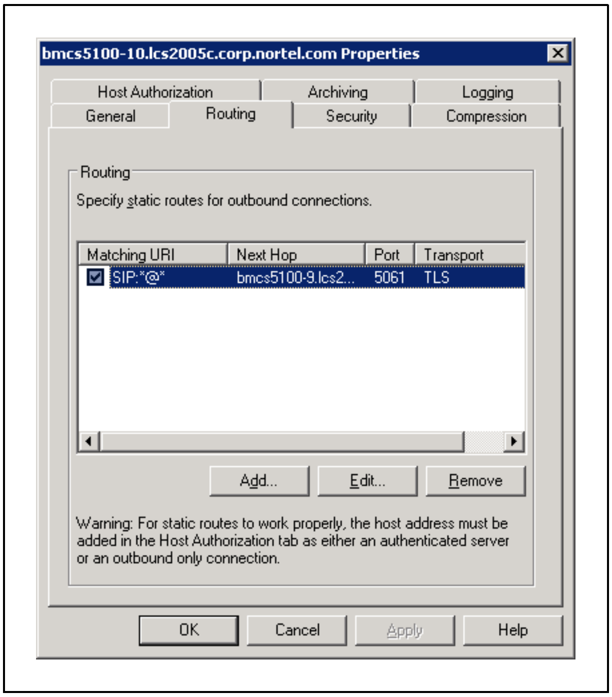
Defaul

No Tasks Available.

3 For the Application Proxy, route all incoming SIP requests to the Live Communication Server Home Server. This routes all incoming calls from CS 1000S to the Home Server, which then routes the call on to the appropriate Office Communicator user. Routing outgoing calls from the Live Communications Server Home Server on to the CS 1000 is not necessary as the MCM application is responsible for this task. Therefore, no routes from the Application Proxy to the CS 1000 need to be configured on the Application Proxy.

In Figure 71 "Routing configuration on Live Communications Server Application Proxy" (page 127), all incoming SIP requests are routed to the Home Server "bmcs5100-9.lcs2.." over TLS.

Figure 71
Routing configuration on Live Communications Server Application Proxy



bmcs5100-10.lcs2005c.corp.nortel.com Properties

Routing

Specify static routes for outbound connections.

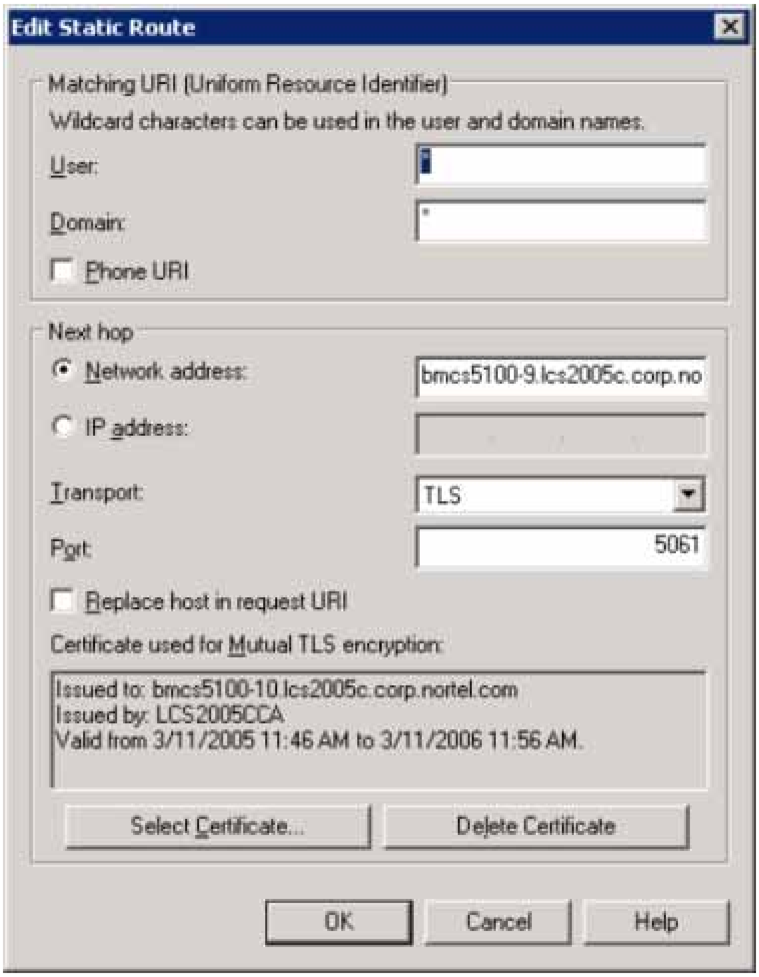
Matching URI	Next Hop	Port	Transport
☑ SIP:*@*	bmcs5100-9.lcs2...	5061	TLS

Warning: For static routes to work properly, the host address must be added in the Host Authorization tab as either an authenticated server or an outbound only connection.

4 On the Add Static Route dialog box (see the next figure), enter the user and route information.

> ***Note:*** Do not enable User equals phone on the static route configured on the application proxy.

Figure 72
Add Static Route



Matching URI (Uniform Resource Identifier)

Wildcard characters can be used in the user and domain names.

User: *

Domain: *

□ Phone URI

Next hop

● Network address: bmcs5100-9.lcs2005c.corp.no

○ IP address:

Transport: TLS

Port: 5061

□ Replace host in request URI

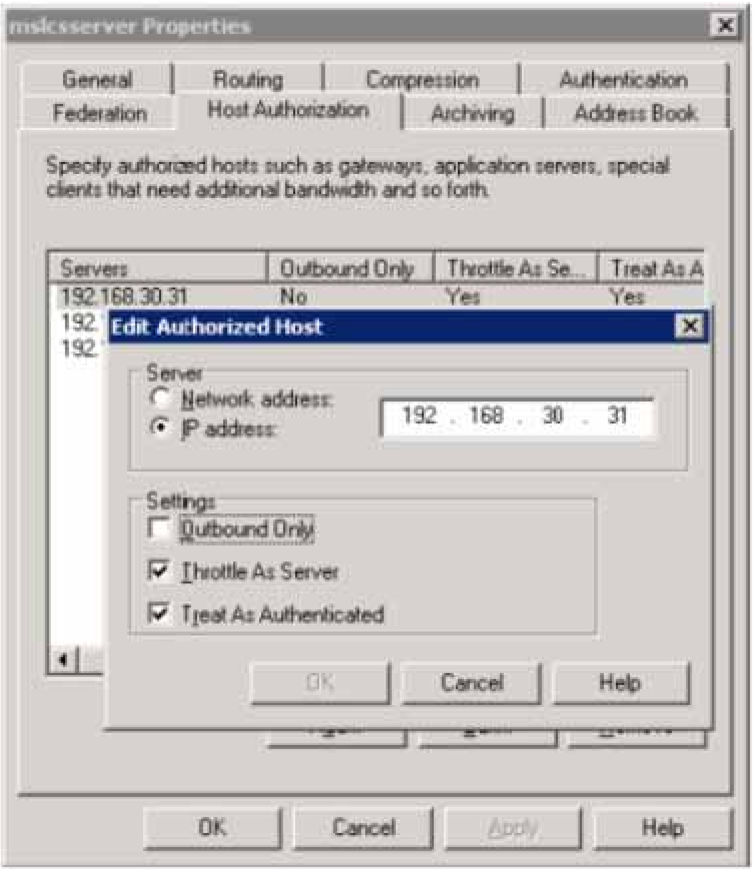
Certificate used for Mutual TLS encryption:

Issued to: bmcs5100-10.lcs2005c.corp.nortel.com
Issued by: LCS2005CCA
Valid from 3/11/2005 11:46 AM to 3/11/2006 11:56 AM.

5 On the Edit Authorized Host dialog box (see Figure 73 "Edit Authorized Host" (page 129)), enter the **IP address**, click both the **Throttle As Server** and **Treat As Authenticated** check boxes, and then click **OK**. The IP addresses that require authorization on the Application Proxy are the Node IP addresses of all the CS 1000s in the network.

> ***Note:*** In Release 5.0, MCM adds a loopback address to the authorized host table automatically during startup. Therefore, users must not manually remove that entry.

Figure 73
Edit Authorized Host



Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth.

Servers	Outbound Only	Throttle As Se...	Treat As A
192.168.30.31	No	Yes	Yes
192.			
192.			

Server
○ Network address:
● IP address: 192 . 168 . 30 . 31

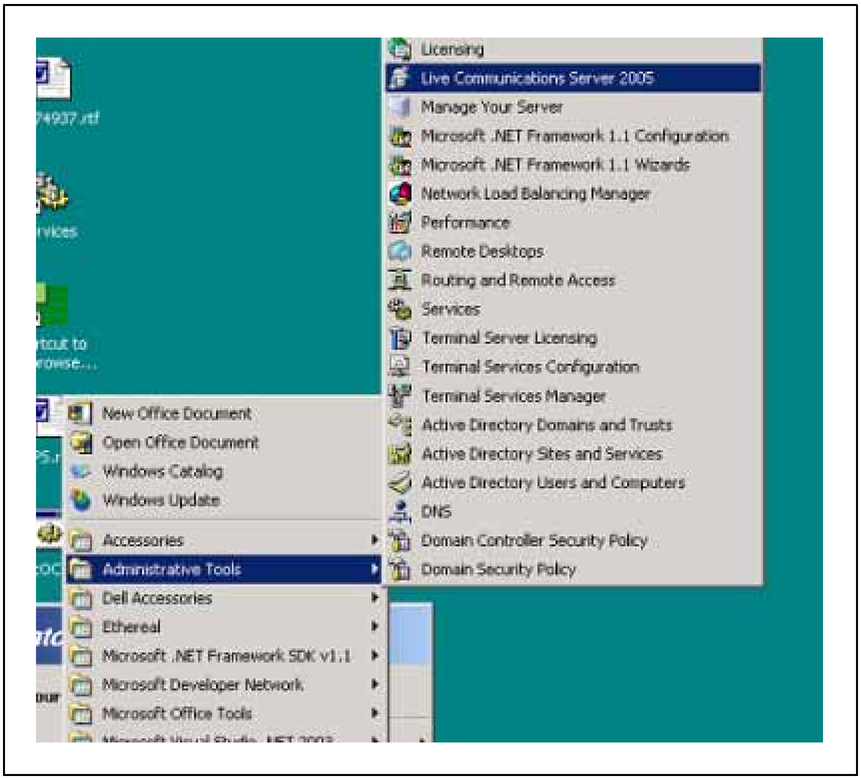
Settings
☐ Outbound Only
☑ Throttle As Server
☑ Treat As Authenticated

—End—

Procedure 4
Configuring a static route for the Home Server

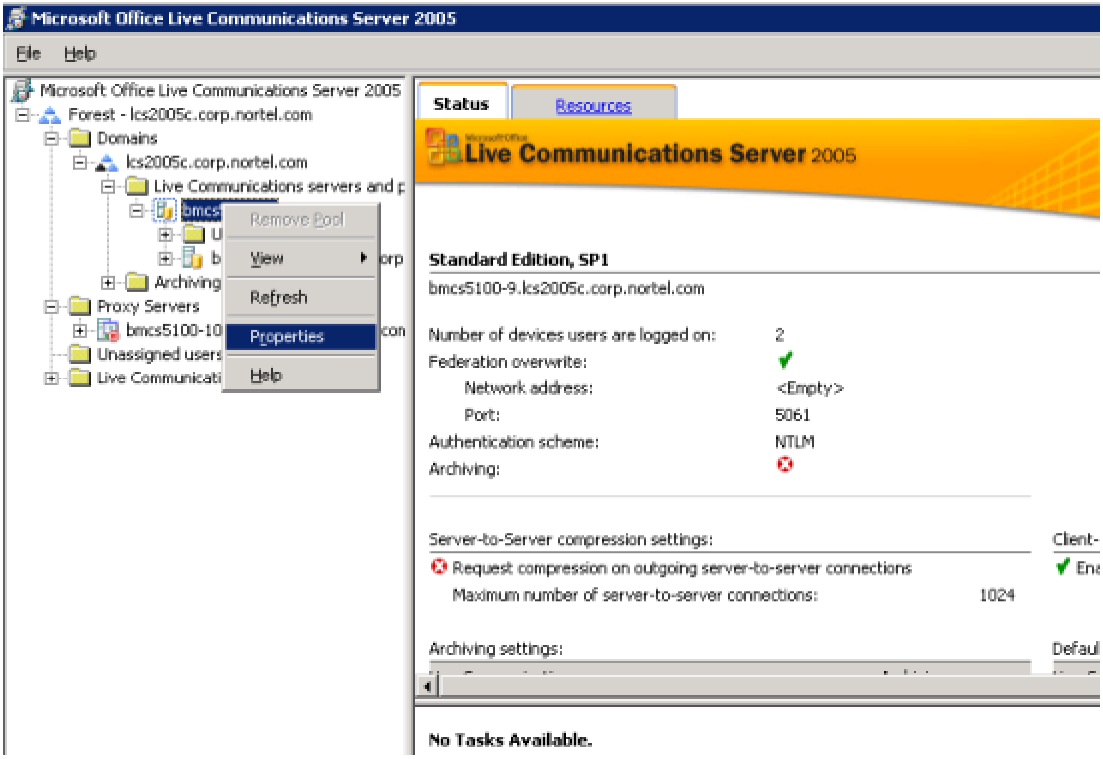
Step	Action
1	Open the Live Communications Server Management Console. The console is accessed on the Windows server running Live Communications Server, as shown in Figure 74 "Opening the Live Communications Server Management Console" (page 130), by selecting **Start > Program > Administrative Tools > Live Communications Server 2005**.

Figure 74
Opening the Live Communications Server Management Console


74937.rtf
rvices
rtcut to
rowse...
Licensing
Live Communications Server 2005
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
DNS
Domain Controller Security Policy
Domain Security Policy
New Office Document
Open Office Document
Windows Catalog
Windows Update
Accessories
Administrative Tools
Dell Accessories
Ethereal
Microsoft .NET Framework SDK v1.1
Microsoft Developer Network
Microsoft Office Tools

2 In the Live Communications Server Management Console, select the Live Communications Server (the server to which you are adding Host Authorization and changing the Routing) and right-click on that server. From the drop-down menu, select **Properties**. See Figure 75 "Live Communications Server Management Console" (page 131).

Figure 75
Live Communications Server Management Console


Microsoft Office Live Communications Server 2005
File
Help
Microsoft Office Live Communications Server 2005
Forest - lcs2005c.corp.nortel.com
Domains
lcs2005c.corp.nortel.com
Live Communications servers and p
bmcs
U
b
orp
Archiving
Proxy Servers
bmcs5100-10
com
Unassigned users
Live Communicati
Remove Pool
View
Refresh
Properties
Help
Status
Resources
Microsoft Office
Live Communications Server 2005

Standard Edition, SP1

bmcs5100-9.lcs2005c.corp.nortel.com

Number of devices users are logged on: 2
Federation overwrite: ✓
Network address: <Empty>
Port: 5061
Authentication scheme: NTLM
Archiving: ✗

Server-to-Server compression settings:
✗ Request compression on outgoing server-to-server connections
Maximum number of server-to-server connections: 1024

Client-
✓ Ena

Archiving settings:

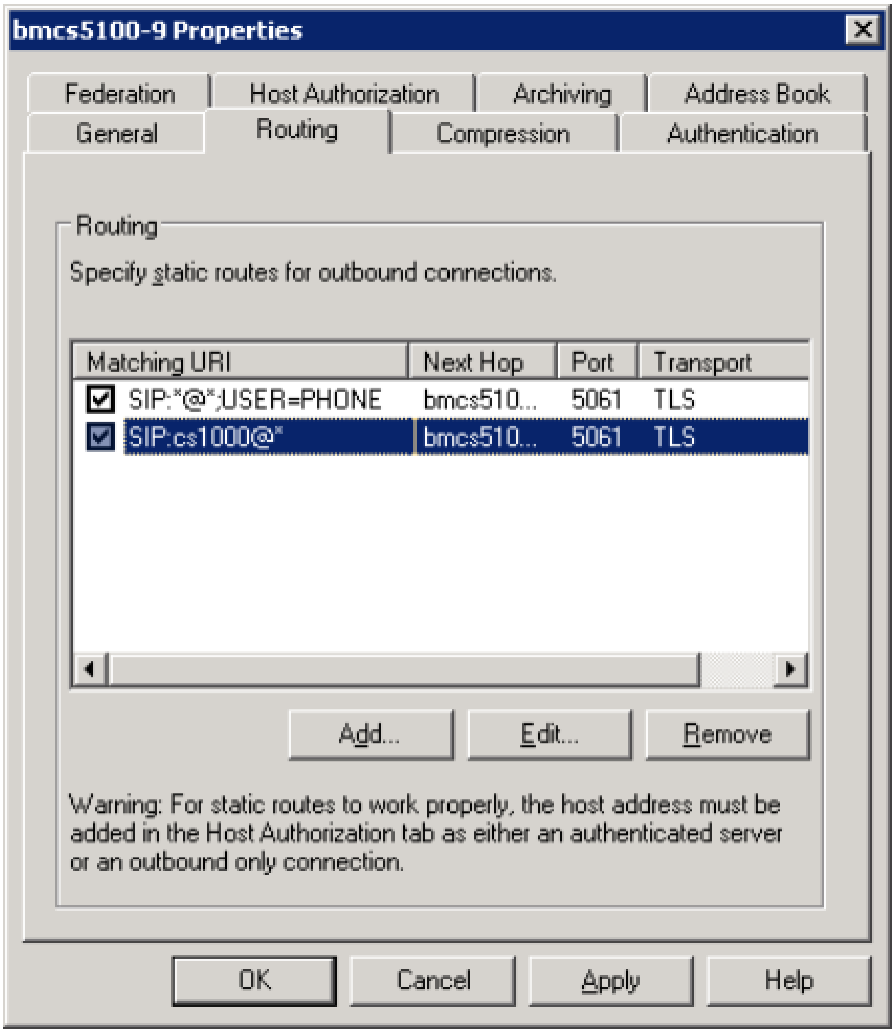
Defaul

No Tasks Available.

3 On the Routing page of the Home Server, route all SIP messages to the appropriate Application Proxy. With MCM running on the Application Proxy, the SIP invite is sent to the correct CS 1000.

See Figure 76 "Routing tab" (page 132), all incoming SIP requests are routed to the Home Server "bmcs5100-9.lcs2..." over TLS.

Figure 76
Routing tab



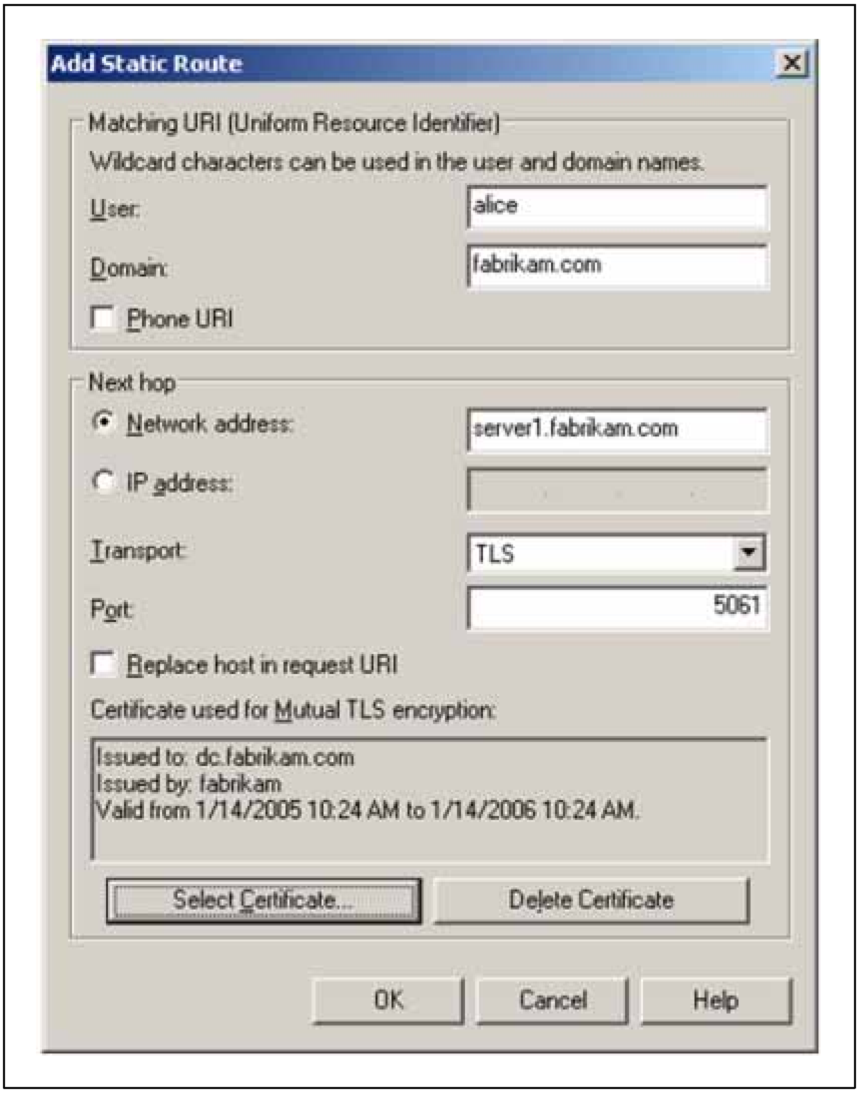
Specify static routes for outbound connections.

	Matching URI	Next Hop	Port	Transport
☑	SIP:*@*;USER=PHONE	bmcs510...	5061	TLS
☑	SIP:cs1000@*	bmcs510...	5061	TLS

Warning: For static routes to work properly, the host address must be added in the Host Authorization tab as either an authenticated server or an outbound only connection.

4 On the Add Static Route dialog box (see Figure 77 "Add Static Route" (page 133)), enter the user and route information.

Figure 77
Add Static Route



Add Static Route

Matching URI (Uniform Resource Identifier)

Wildcard characters can be used in the user and domain names.

User: alice

Domain: fabrikam.com

□ Phone URI

Next hop

● Network address: server1.fabrikam.com

○ IP address:

Transport: TLS

Port: 5061

□ Replace host in request URI

Certificate used for Mutual TLS encryption:

Issued to: dc.fabrikam.com
Issued by: fabrikam
Valid from 1/14/2005 10:24 AM to 1/14/2006 10:24 AM.

—End—

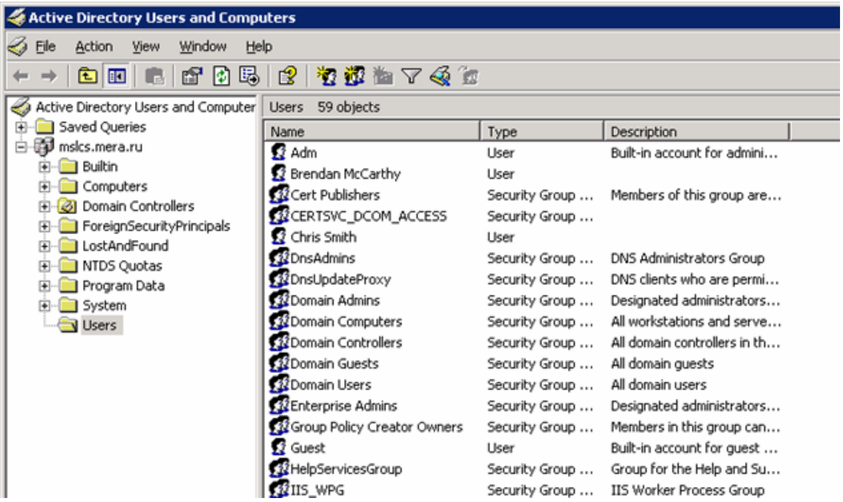
Configuring Active Directory

Active Directory configuration takes place in the Active Directory Users and the Computers (ADUC) window. Selecting the Users folder reveals the list of users (see Figure 78 "Active Directory (Microsoft® LDAP server)" (page 134)). All users are defined in this folder.

> ***Note:*** 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 made in the Active Directory User’s configuration ("Active Directory Sites and Services" snap-in).

Figure 78
Active Directory (Microsoft® LDAP server)



Name	Type	Description
Adm	User	Built-in account for admini...
Brendan McCarthy	User	
Cert Publishers	Security Group ...	Members of this group are...
CERTSVC_DCOM_ACCESS	Security Group ...	
Chris Smith	User	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group

Procedure 5
Defining users

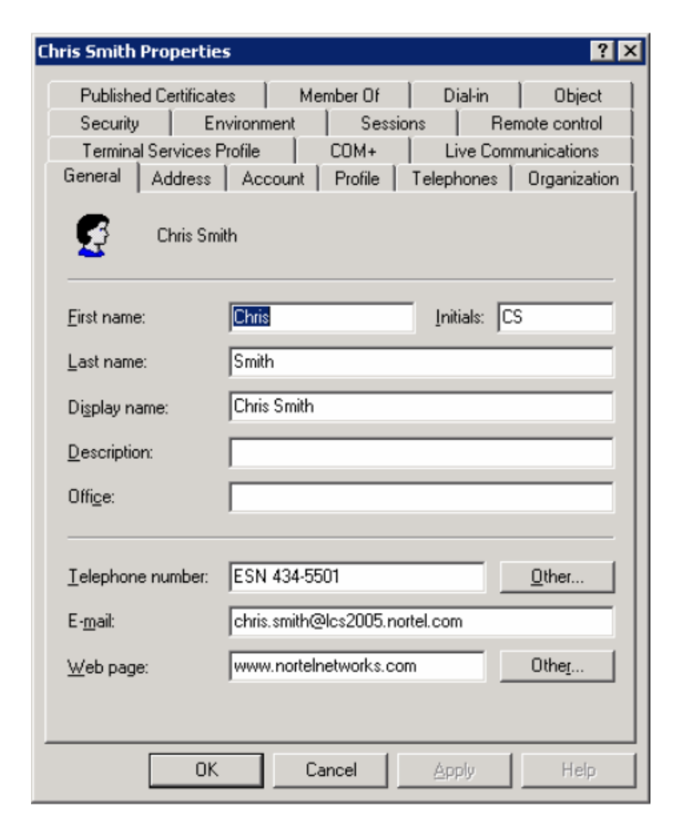
Step Action

1 Select a user from the list in the Users folder.

2 Right-click the user, and select **Properties**.

3 The Properties dialog box opens (see Figure 79 "User properties" (page 135)).

Figure 79
User properties



Chris Smith

First name: Chris
Initials: CS
Last name: Smith
Display name: Chris Smith
Description:
Office:
Telephone number: ESN 434-5501 Other...
E-mail: chris.smith@lcs2005.nortel.com
Web page: www.nortelnetworks.com Other...

4 Enter the user’s information (first name, last name, telephone number, and so on) in the appropriate fields in the General page.

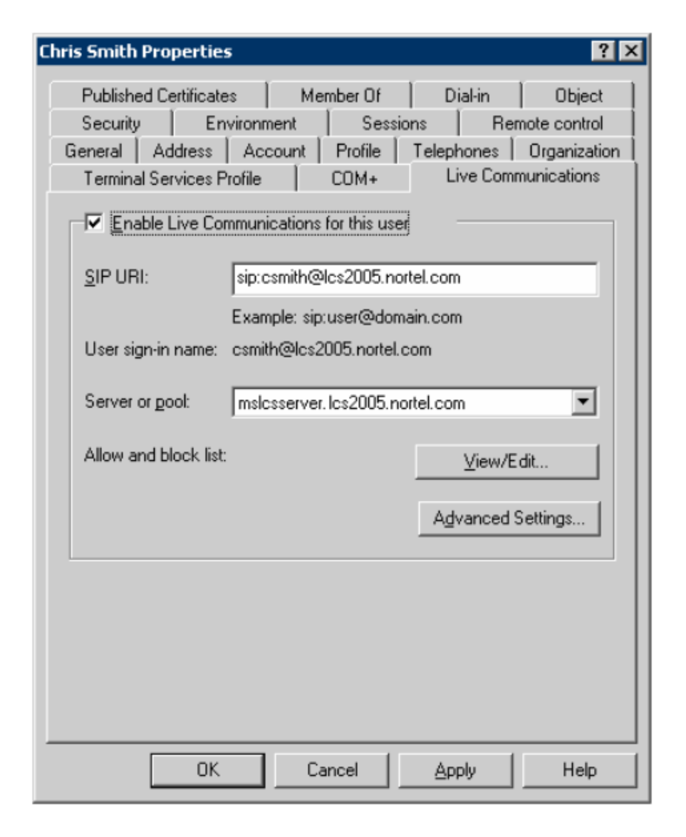
> ***Note:*** The "Telephone number" field is the preferred field to enter the phone number used for the Twinning feature. It is extremely important that:
>
> - The phone number is entered in the same field and in the exact same format for all users.
> - The field and format used matches what is configured in MCM. Typical configuration involves using the Phone Number field, which maps to telephoneNumber in MCM and then puts the number in the format of "ESN 445-8888" which maps to "ESN ???-????" in MCM.

5 Select the Live Communications tab (see Figure 80 "Enable Live Communications Server connectivity for a user in Active Directory" (page 136)).

6 Click the check box next to **Enable Live Communications for this user**.

7 In the fields provided, define the user **SIP URI** and the **Server or Pool** (see Figure 80 "Enable Live Communications Server connectivity for a user in Active Directory" (page 136)). Office Communicator 2005 uses these addresses to place calls.

Figure 80
Enable Live Communications Server connectivity for a user in Active Directory



Chris Smith Properties

☑ Enable Live Communications for this user

SIP URI: sip:csmith@lcs2005.nortel.com

Example: sip:user@domain.com

User sign-in name: csmith@lcs2005.nortel.com

Server or pool: mslcsserver.lcs2005.nortel.com

Allow and block list:

—End—

Configuring the Call Server

CS 1000 configuration involves two separate functions: Signaling Server configuration (covered in the next section) 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 may need to be done at the Call Server prompt. This document assumes that you are already familiar with how to configure a CS 1000.

It is important in ESN networks that the correct HLOC is configured in both Overlay 90 (required for ESN calls to work) and Overlay 15. If not, basic calling functionality does not work. Also, the Caller ID table (explained in this section), Home NPA, and LOC are required for outgoing calls to the Public network (PSTN) to correctly display the outgoing Caller Line ID (CLID) in North America.

Configuring the SIP Trunk

In order for a Live Communications Server 2005 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.

> ***Note:*** Both can be done through Element Manager. For more information on how to create the required components on the Call Server, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313).

ATTENTION

IMPORTANT!

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

ATTENTION

IMPORTANT!

The Route Data Block (RDB) must have no value configured for the prompt "INST". Otherwise, incoming calls from Office Communicator to the CS 1000 do not work.

ATTENTION

IMPORTANT!

When configuring the D Channel used by the SIP Trunk for Converged Office Telephony Gateway and Services, ensure that NASA=yes in LD 17 for DCH 79. Failure to do so will result in limitations to Call Transfers that involve Office Communicator.

The CS 1000 SIP trunk that receives Office Communicator calls must be set to ESN5, and all associated Virtual trunks must be set 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 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
```

> ***Note:*** All of the SIP Virtual Trunks must be set 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
```

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

Configuring the Codec

Office Communicator 2005 supports the G.711 (20 milliseconds) codec. While the G.723 is supported, it should not be used. The G.711 codec should be enforced in the network by defining only the G.711 codec on the CS 1000. As DTMF digits are sent in-band by Office Communicator

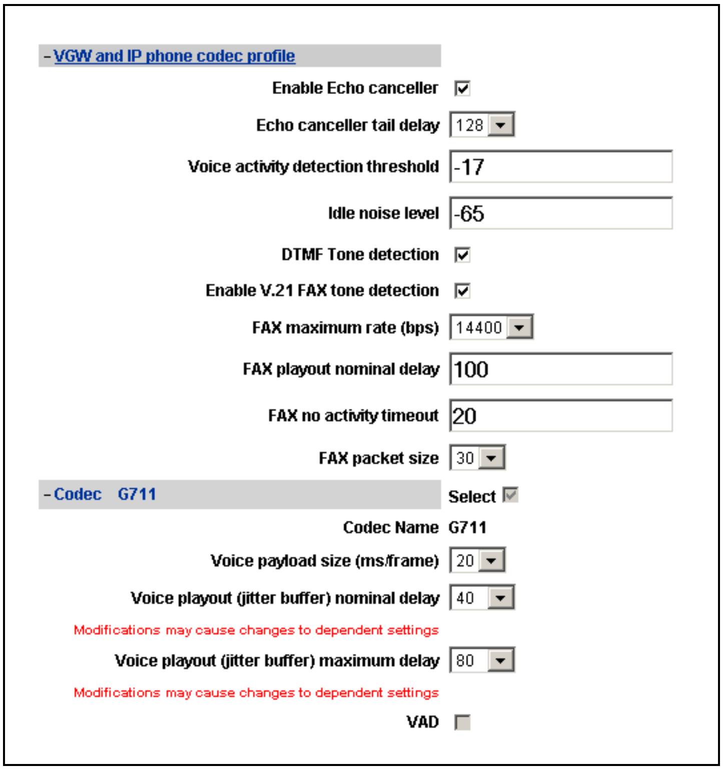
2005, the G.711 codec should be the only codec used. If G.711 is not the only codec used, calls to voice mail (such as CallPilot) or call conferencing bridges (such as MCS MeetMe) do not work.

> ***Note:*** G.723 is supported in Release 5.0. However, it should only be enabled on the CS 1000 when the system has been set up so that DTMF tones are not used for DTMF digit handling. Otherwise, calls from Office Communicator to voice mail (such as CallPilot) or call conferencing bridges (such as MCS MeetMe) do not work.

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). Figure 81 "Codec configuration" (page 139) demonstrates the correct location of Element Manager in which to configure the codec.

Figure 81
Codec configuration



- VGW and IP phone codec profile

Enable Echo canceller	☑
Echo canceller tail delay	128
Voice activity detection threshold	-17
Idle noise level	-65
DTMF Tone detection	☑
Enable V.21 FAX tone detection	☑
FAX maximum rate (bps)	14400
FAX playout nominal delay	100
FAX no activity timeout	20
FAX packet size	30

- Codec G711 Select ☑

Codec Name	G711
Voice payload size (ms/frame)	20
Voice playout (jitter buffer) nominal delay	40
Modifications may cause changes to dependent settings	
Voice playout (jitter buffer) maximum delay	80
Modifications may cause changes to dependent settings	
VAD	☐

Configuring the Loss Plan

In order for DTMF digits to be transmitted at the correct volume, especially for Office Communicator 2005 to PSTN communications, the Loss Plan for the CS 1000 must be correctly configured. Calls from Office Communicator 2005 to a residential Voice Mail system (VoIP to PSTN) is an example of the necessity of Loss Plan configuration. For information on how to configure the Loss Plan refer to *Transmission Parameters* (NN43001-282).

It is important to not just configure the Loss Plan values, but also the DTI Data Block (DDB), in order that the Loss and Level Plans be set correctly. For more information, refer to the "Loss values for Voice Gateway Media Card" section in *Transmission Parameters* (NN43001-282).

ATTENTION

IMPORTANT!

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.

Configuring the Dialing Plan to route to MCM

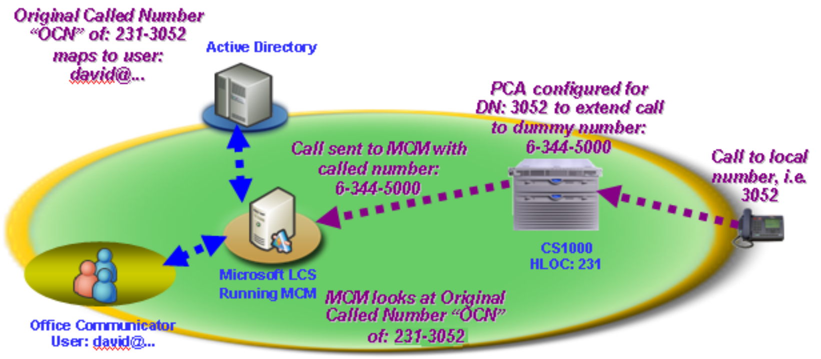
In order for calls to be extended using PCA to the Live Communications Server, a dialing plan entry must be entered on the Call Server to send the call to the SIP trunk. This dialing plan entry does not correspond with any number that is "dialable" within a network, but rather is used to route the call to the Live Communications Server. The MCM service running on the Live Communications 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 PCA 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 on the Active Directory and sends the call to the correct Office Communicator client.

For example, the CS 1000 network may be configured as shown in Figure 82 "Dialing plan to route to MCM" (page 141).

Figure 82
Dialing plan to route to MCM


Original Called Number "OCN" of: 231-3052 maps to user: david@...
Active Directory
PCA configured for DN: 3052 to extend call to dummy number: 6-344-5000
Call sent to MCM with called number: 6-344-5000
Call to local number, i.e. 3052
CS1000 HLOC: 231
Microsoft LCS Running MCM
MCM looks at Original Called Number "OCN" of: 231-3052
Office Communicator User: david@...

In this figure, the CS 1000 has a HLOC of 231 and an LOC dialing plan entry of 344. The LOC dialing plan 344 is not "dialable", but calls to the DN: 3052 extends the call to the number 6-344-5000. By PCA extending the call to 6-344-5000, a SIP Invite is sent to the Live Communications Server.

The Live Communications Server runs MCM, which handles the Invite and reads the Original Called Number as 231-3052. The call is then sent to the user and is mapped to 231-3052. In this diagram the user is "david@...."

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 on Dialing Plans, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313).

Configuring the Personal Call Assistant

Personal Call Assistant (PCA) is used to "twin" incoming calls so users can answer the calls on either their desktop phone or Office Communicator 2005.

In order for the incoming calls to be extended to the "twinned" Office Communicator client, a PCA TN must be defined for that DN. PCA is configured as shown in *Features and Services* (NN43001-106).

The PCA 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 Live Communication Server. For more information, refer to "Dialing Plan to route to MCM" (page 140).

ATTENTION

IMPORTANT!

If SIP CTI control is also enabled for that set, the PCA TN cannot be MARP 0.

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

Note that MARP is assigned to the first DN key created, so if you create the PCA 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 PCA and you encounter this exact situation. The following is an example of an unsupported configuration:

```
REQ: prt
TYPE: dnb
CUST 0
DN a r l 2002
DATE
PAGE
DES

DN 2002
TYPE SL1
TN > t T 061 0 00 00 V t y KEY 00 MARP DES I2002 i F m > 28 AUG 2005
(I2002 )
TN 061 0 00 00 V KEY 00 DES I2002 28 AUG 2005
(PCA)
```

For more information about PCA, refer to the *Features and Services* (NN43001-106) NTP.

The following is an example of a correctly configured PCA:

```
DES PCA
TN 097 0 00 01 VIRTUAL
TYPE PCA
CDEN 8D
CUST 0
ZONE 000
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SFLT NO
```

```
CAC_CIS 3
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFA CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE
DRG1
POD DSX VMD CMSD 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 HSPD ABDD CFHD FICD NAID DNAA RDLA BUZZ
AGRD MOAD
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD
NRCD NROD DRDD EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD
FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR ICRD MCDD T87D
CPND_LANG ENG Note: All TNs for a DN used for Converged Office must
have CLS CDMR
HUNT
PLEV 02
CSDN
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 3052 0 Note: "Twinned" DN of 3052, CLID Table 0 (that is
covered later)
ANIE 0
01 HOT P 8 63445000 Note: HOT P key points to a "FAKE" number that just
directs the call to the MCM/LCS server. In this example the call is directed to:
AC1 ("6")+ LOC ("344") of MCM + Dummy DN of 5000

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
```

Configuring the Call ID Table

The Caller ID table is used to correctly build the Caller ID (CLID) for both Private network and Public network calls from a number/extension. The Caller ID table is used by all CS 1000 phones 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 231-3052, has an LOC of 231 and an extension of 3052.

For PCA Twinning to work correctly in a UDP environment, the full Original Called Number (OCN) must be sent by the CS 1000 to the Live 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 Call ID 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 should point to a Call ID 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 should point to a Call ID table that also has the Home Exchange configured. The Home Exchange is the prompt HLCL and is the ‘967’ in 1-800-967-3052.

For example, a phone with an extension of 3052, an ESN number of 231-3052, and a Public Number of 967-3052 in North America is configured in the following manner:

```
>ld 11
REQ: prt
TYPE: i2004
TN 61 00
DATE
PAGE

...

DNDR 0
KEY 00 SCR 3052 0 MARP
CPND
CPND_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 231, HLCL of 967, and INTL of 1.

The CLID table entry of 0 with an HLOC of 231 is configured in the following manner:

```
>ld 15
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
AC2
FNP
CLID yes
SIZE 5
INTL 1
ENTRY 0

HNTN

...
HLCL 967
...

HLOC 231
```

...

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

Configuring Home LOC and Home NPA

In order for the correct Caller Line ID (CLID) to be correctly displayed for Office Communicator calls to the Public network, both the HLOC and HNPA may 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 on the HLOC and HNPA, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313).

Configuring the Signaling Server

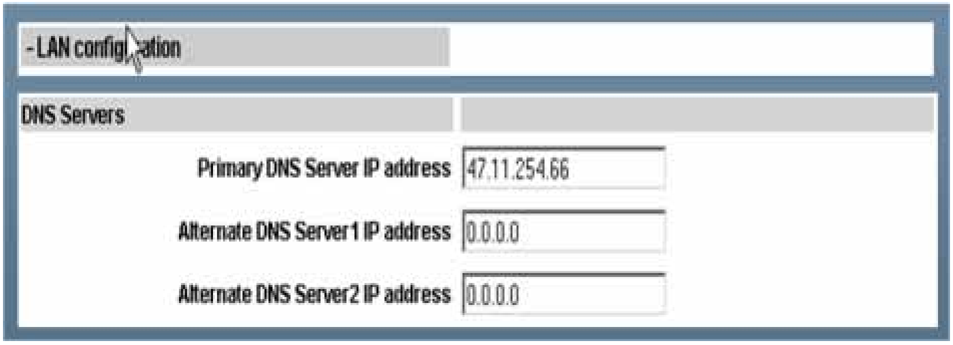
Configuring the DNS Server

Host Table configuration is replaced in Release 5.0 with DNS configuration. In Element Manager, under LAN configuration (see Figure 83 "DNS configuration" (page 147)), you have the option of entering up to three DNS server IP addresses. The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all LCS Servers and Enterprise Edition Pools. Also, the FQDN must resolve to the IP address of the LCS 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.

> ***Note:*** Users upgrading from Release 4.5 to Release 5.0 still see Host Table configuration in Element Manager, but that information is no longer used.

Figure 83
DNS configuration



- LAN configuration

DNS Servers

Primary DNS Server IP address: 47.11.254.66

Alternate DNS Server1 IP address: 0.0.0.0

Alternate DNS Server2 IP address: 0.0.0.0

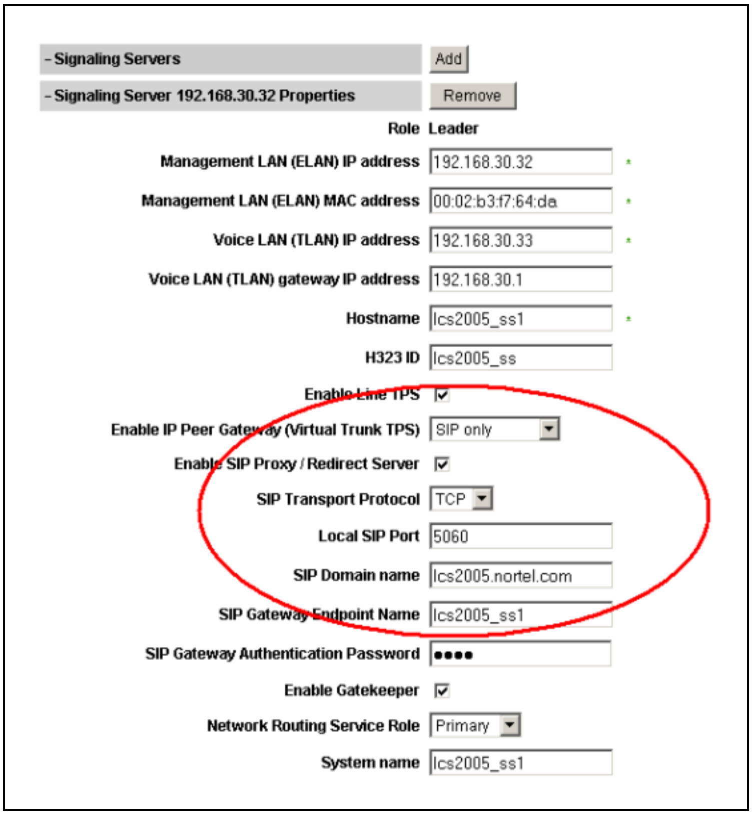
Configuring the SIP Trunk

In order for calls to be made between the CS 1000 and Office Communicator 2005, you must configure the SIP trunks. For more information on how to configure SIP trunks, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313).

A CS 1000 with existing SIP trunks requires a configuration change to be compatible with Microsoft® Live Communications Server 2005. In order for a SIP Trunk to communicate with Live Communications Server 2005, the SIP Transport Protocol must be configured as TCP, not UDP (see Figure 84 "SIP Gateway configuration" (page 148)).

> ***Note:*** The default Local SIP Port of 5060 is required.

Figure 84
SIP Gateway configuration



- Signaling Servers

- Signaling Server 192.168.30.32 Properties

Role	Leader
Management LAN (ELAN) IP address	192.168.30.32 *
Management LAN (ELAN) MAC address	00:02:b3:f7:64:da *
Voice LAN (TLAN) IP address	192.168.30.33 *
Voice LAN (TLAN) gateway IP address	192.168.30.1
Hostname	lcs2005_ss1 *
H323 ID	lcs2005_ss
Enable Line TPS	☑
Enable IP Peer Gateway (Virtual Trunk TPS)	SIP only
Enable SIP Proxy / Redirect Server	☑
SIP Transport Protocol	TCP
Local SIP Port	5060
SIP Domain name	lcs2005.nortel.com
SIP Gateway Endpoint Name	lcs2005_ss1
SIP Gateway Authentication Password	●●●●
Enable Gatekeeper	☑
Network Routing Service Role	Primary
System name	lcs2005_ss1

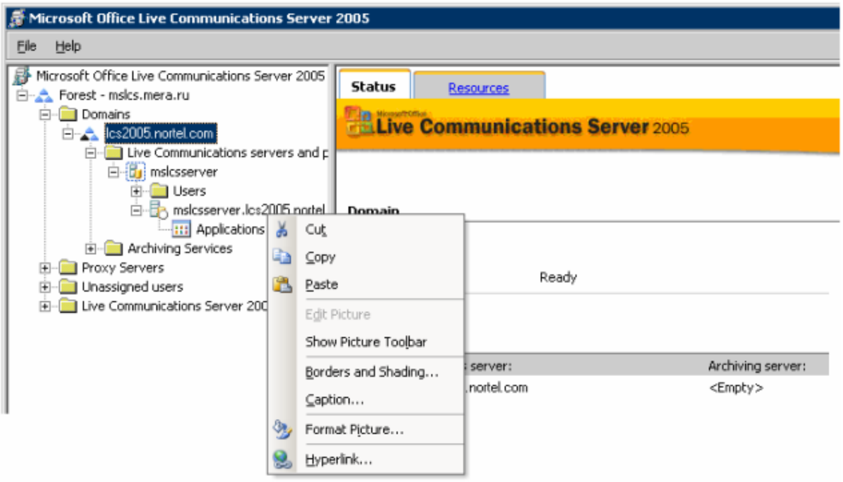
Domain naming

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

In situations where both the LCS 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. For more information, please refer to "Registration" (page 106)

The domain is listed under the Domains folder in the Management console for Live Communications Server. For example, in the next figure, the Live Communications Server Domain is lcs2005s.corp.nortel.com.

Figure 85
SIP Trunk Domain name

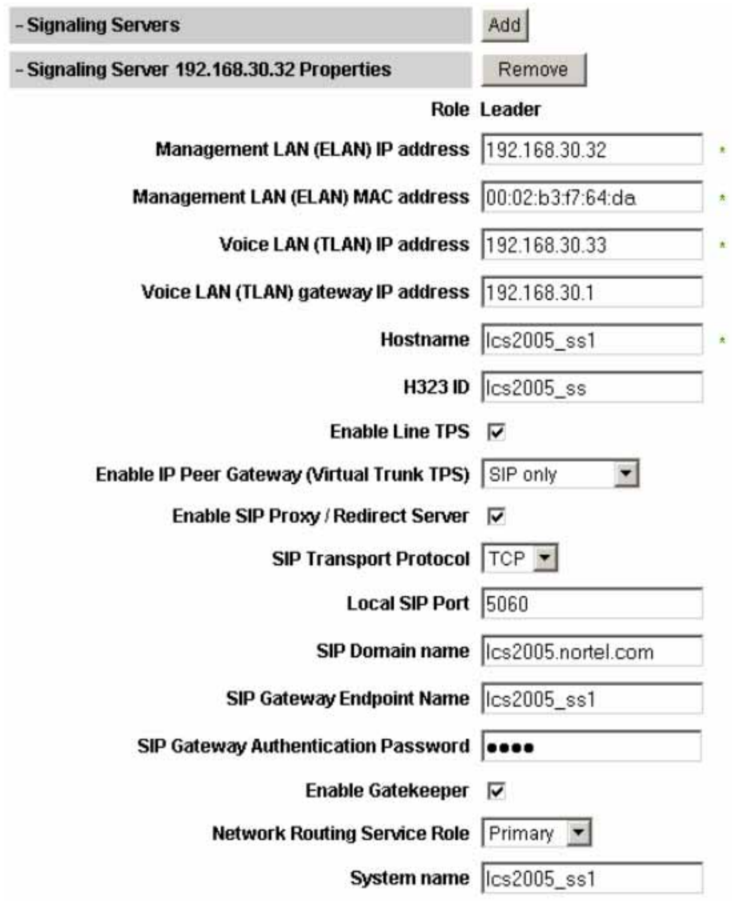


Procedure 6 "Configuring the SIP Trunk Domain name" (page 149) describes how to configure the SIP Trunk domain name to match the Live Communications Server domain name.

Procedure 6
Configuring the SIP Trunk Domain name

Step	Action
1	Log into the Element Manager page for the Signaling Server.
2	Go to **IP Telephony**.
3	Click **Nodes > Servers, Media Cards**.
4	Select **Configuration**.
5	Click **Edit** next to the correct node.
6	Open the **Signaling Server Properties** (see Figure 86 "Element Manager Signaling Server Properties" (page 150)).

Figure 86
Element Manager Signaling Server Properties



- Signaling Servers [Add]

- Signaling Server 192.168.30.32 Properties [Remove]

Role	Leader
Management LAN (ELAN) IP address	192.168.30.32 *
Management LAN (ELAN) MAC address	00:02:b3:f7:64:da *
Voice LAN (TLAN) IP address	192.168.30.33 *
Voice LAN (TLAN) gateway IP address	192.168.30.1
Hostname	lcs2005_ss1 *
H323 ID	lcs2005_ss
Enable Line TPS	☑
Enable IP Peer Gateway (Virtual Trunk TPS)	SIP only
Enable SIP Proxy / Redirect Server	☑
SIP Transport Protocol	TCP
Local SIP Port	5060
SIP Domain name	lcs2005.nortel.com
SIP Gateway Endpoint Name	lcs2005_ss1
SIP Gateway Authentication Password	●●●●
Enable Gatekeeper	☑
Network Routing Service Role	Primary
System name	lcs2005_ss1

7 In most cases, the value for the field SIP Domain Name must match the domain of the Live Communications Server. In Figure 86 "Element Manager Signaling Server Properties" (page 150) the SIP Domain name is lcs2005c.corp.nortel.com. Only in situations where the MCM is configured to register to the NRS using End_Point_Name@Service_ Domain_Name can the two SIP Domain Names not match. For more information, please refer to "Registration" (page 106).

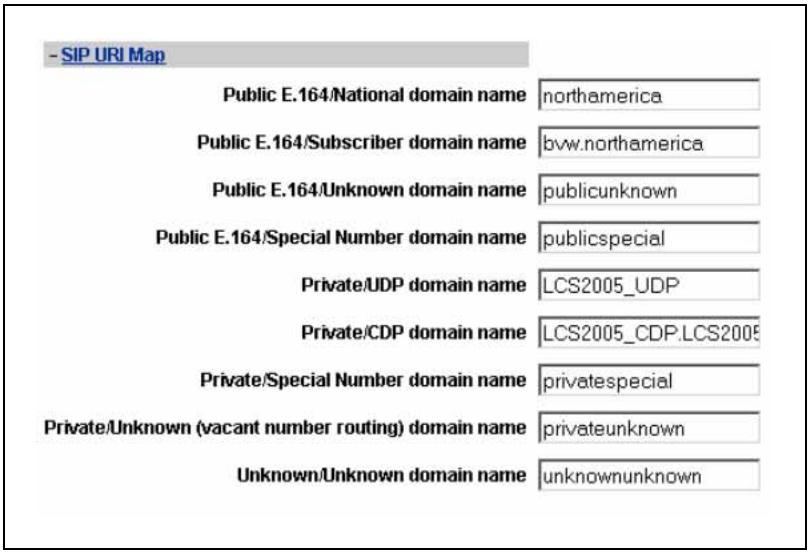
—End—

URI Mapping

The SIP URI Map must be configured in order to correctly register with the NRS. Also, the SIP URI map information is required for configuration of the MCM Service running on the Live Communications Server. 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 (see Figure 87 "SIP URI Map" (page 151)) is also configured in Element Manager under Node Configuration.

Figure 87
SIP URI Map



- SIP URI Map

Public E.164/National domain name: northamerica

Public E.164/Subscriber domain name: bvw.northamerica

Public E.164/Unknown domain name: publicunknown

Public E.164/Special Number domain name: publicspecial

Private/UDP domain name: LCS2005_UDP

Private/CDP domain name: LCS2005_CDP.LCS2005

Private/Special Number domain name: privatespecial

Private/Unknown (vacant number routing) domain name: privateunknown

Unknown/Unknown domain name: unknownunknown

The SIP URI Map must match the NRS server configuration in the following manner:

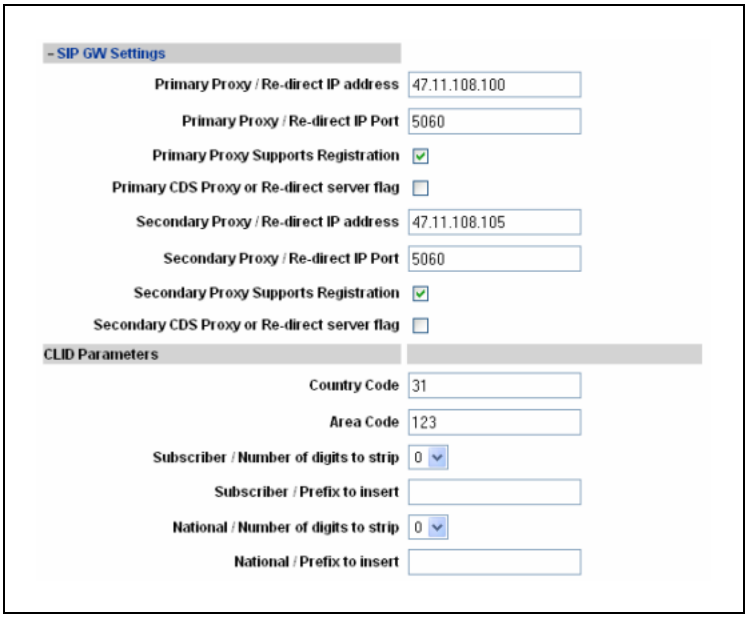
- The Private/UDP domain name maps to the L0 Domain on the NRS
- The Private/CDP domain name maps to the L1 Domain on the NRS

MCM must be configured to match one of the domain names. For example, in a UDP network, the configured domain name is LCS2005_UDP in MCM.

Configuring SIP Gateway CLID Parameters

The SIP Gateway CLID parameters are used to adjust the format of telephone numbers for incoming call appearances. For Microsoft® Office Communicator these settings impact the format of numbers that appear on the incoming call popup for Telephony Gateway and Services (the SIP call leg for Microsoft® Office Communicator clients that are twinned with a CS 1000 DN through a PCA).

Figure 88
SIP GW CLID Parameters



- SIP GW Settings

Primary Proxy / Re-direct IP address	47.11.108.100
Primary Proxy / Re-direct IP Port	5060
Primary Proxy Supports Registration	☑
Primary CDS Proxy or Re-direct server flag	□
Secondary Proxy / Re-direct IP address	47.11.108.105
Secondary Proxy / Re-direct IP Port	5060
Secondary Proxy Supports Registration	☑
Secondary CDS Proxy or Re-direct server flag	□

CLID Parameters

Country Code	31
Area Code	123
Subscriber / Number of digits to strip	0
Subscriber / Prefix to insert	
National / Number of digits to strip	0
National / Prefix to insert	

> ***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 popup 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 made 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.

Configuring SPS

SIP Proxy Server (SPS) is configured through MCM (see Figure 51 "MCM Configuration" (page 105)). In Release 4.5, the SIP Routing section of the MCM Configuration screen had two main options: NRS and Direct. In Release 5.0, Direct is still supported in addition to SPS.

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)

Configuring NRS

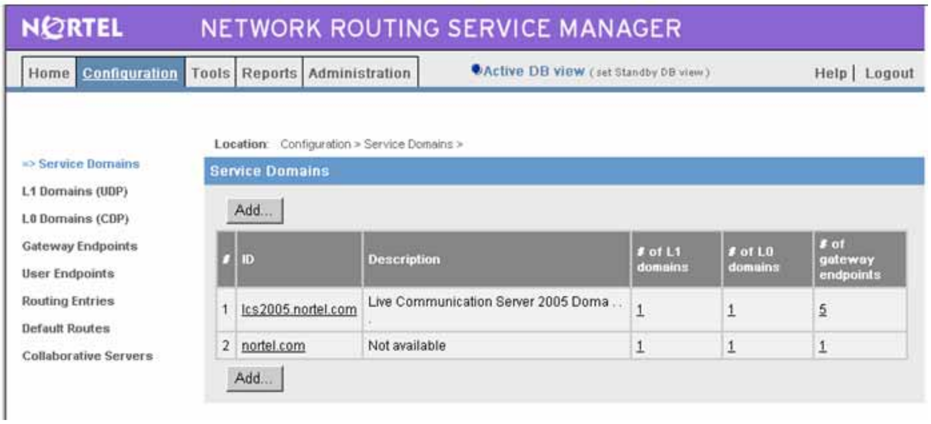
The Server IP running the MCM application (generally a Live Communications Server 2005 Proxy) must be configured on the NRS as a dynamic SIP endpoint, or gateway, and not as a collaboration server.

Note: NRS configuration is the legacy method.

A Live Communications Server Service Domain must be created for the Signaling Server and MCM. The Signaling Server and MCM register to the Live Communications Server Service Domain on the NRS. This Live Communications Server Service Domain must also match the domain name of the Live Communications Server.

The Service Domain between the NRS and the Live Communication Server must also match—or 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.

Figure 89
Live Communications Server Service Domain



Location: Configuration > Service Domains >

Service Domains

#	ID	Description	# of L1 domains	# of L0 domains	# of gateway endpoints
1	lcs2005.nortel.com	Live Communication Server 2005 Doma . . .	1	1	5
2	nortel.com	Not available	1	1	1

In Figure 89 "Live Communications Server Service Domain" (page 154), the NRS is configured with the matching Service Domain of lcs2005c.nortel.com.

The L1 and L0 Domains must also be configured and match what the CS 1000 is 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 PCA calls.

For example, the Location Code (LOC) 344 from the PCA example appears as:

01 HOT P 8 63445000

The NRS must be configured to analyze and qualify numbers dialed from the Live 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 on how to configure the NRS, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313).

Configuring Microsoft® Office Communicator 2005

The following figures demonstrate how to configure a SIP account in Office Communicator 2005.

Figure 90
Office Communicator 2005 Main Window

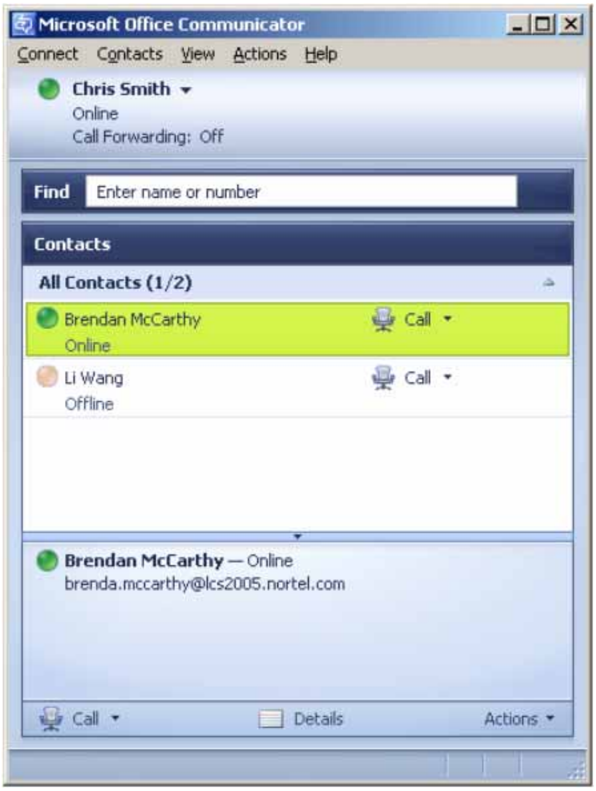
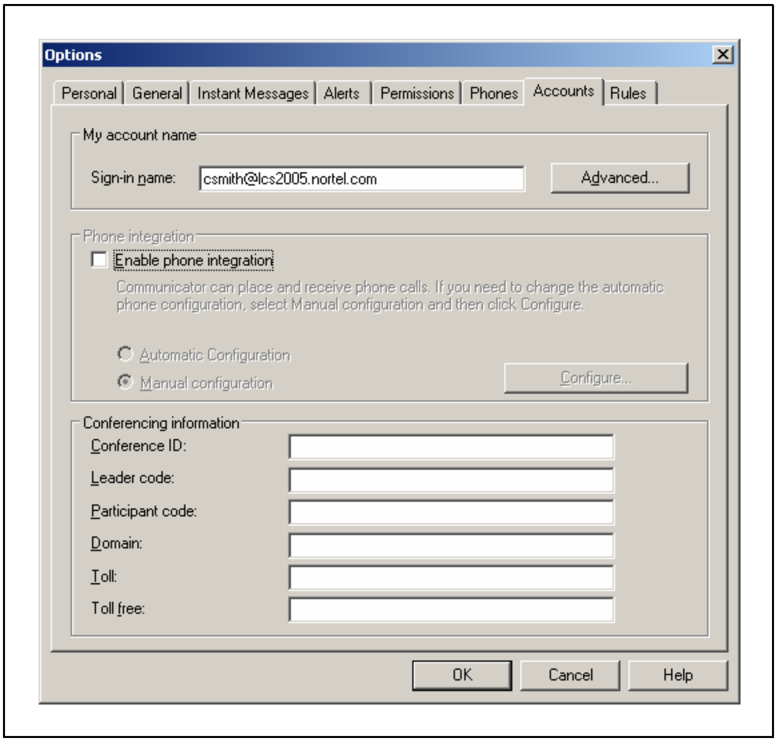


Figure 91
Account Configuration Window in Office Communicator 2005



My account name

Sign-in name: csmith@lcs2005.nortel.com

Phone integration

☐ Enable phone integration

Communicator can place and receive phone calls. If you need to change the automatic phone configuration, select Manual configuration and then click Configure.

○ Automatic Configuration

● Manual configuration

Conferencing information

Conference ID:

Leader code:

Participant code:

Domain:

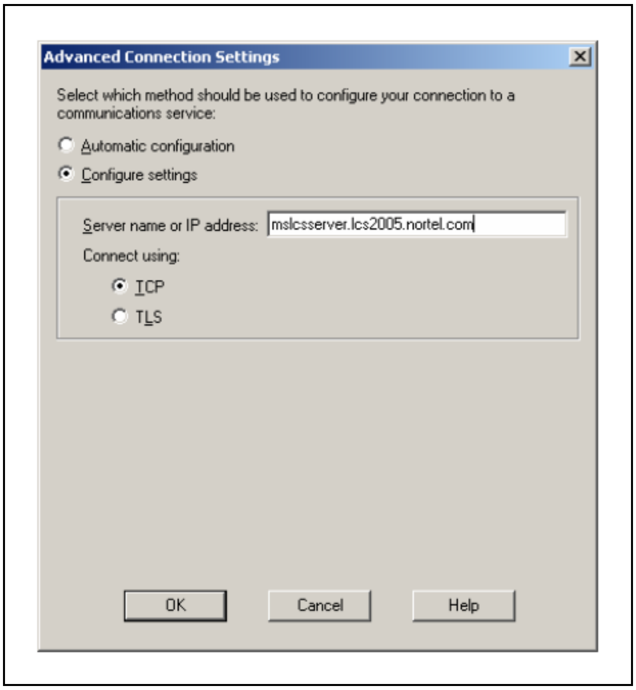
Toll:

Toll free:

Note: The Enable phone integration box must be checked for the Office Communicator "blind" transfer feature to work. For more information, refer to the following Microsoft® Knowledge Base Article:

www.support.microsoft.com/kb/910790

Figure 92
Server Connection Configuration Window


Advanced Connection Settings

Select which method should be used to configure your connection to a communications service:

○ Automatic configuration

● Configure settings

Server name or IP address: mslcsserver.lcs2005.nortel.com

Connect using:

● TCP

○ TLS

Although you can select UDP as a transport protocol in Office Communicator 2005, Live Communications Server 2005 does not support UDP.

Client-to-server and server-to-client communication can be achieved only through TCP or TLS in the following manner:

- within the internal network perimeter
- outside the internal network perimeter, or
- across the internal network perimeter.

The use of TLS is recommended for communicating outside or across the network perimeter, as this protocol provides high security levels. TLS requires PKI and certificates, whereas TCP does not.

Configuring CDR

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 a call is made, 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&2452336XXXXXXXXX
```

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 2336 (a location code of 245 followed by 2336). Again, MCM supports redundant NRS configurations.

Dialing E.164 International Format Numbers from Microsoft® Office Communicator - Computer Calls (SIP Gateway)

It is important to note that the dialed number sent from Microsoft® Office Communicator to the CS 1000 for SIPGW calls follows the same format as those dialed on the station. As such, 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: +CCCXXXXXXXXX@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 on 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 on the outgoing trunk are: 812125551212

Normalizing phone numbers

Now that you have completed the installation and configuration of Telephony Gateway and Services, you may proceed directly to the next step in the process: "Normalizing phone numbers" (page 182).

Configuring Remote Call Control

This section describes the process to configure the Remote Call Control with SIP CTI component.

Configuring the CS 1000

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.

Incremental Software Management (ISM) defines the number of TNs that can be accessed through SIP CTI by the CLS T87A.

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 ("LD 17 – Configure AML Link" (page 159) and "LD 17 – Configure VAS (Value Added Server)" (page 160)) display the prompts used for AML link configuration:

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 to 47 on a small system and 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
```

Refer to *Software Input/Output: Maintenance* (NN43001-711) for more information on the STAT ELAN command.

Note: 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.

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 47 on a small system and 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

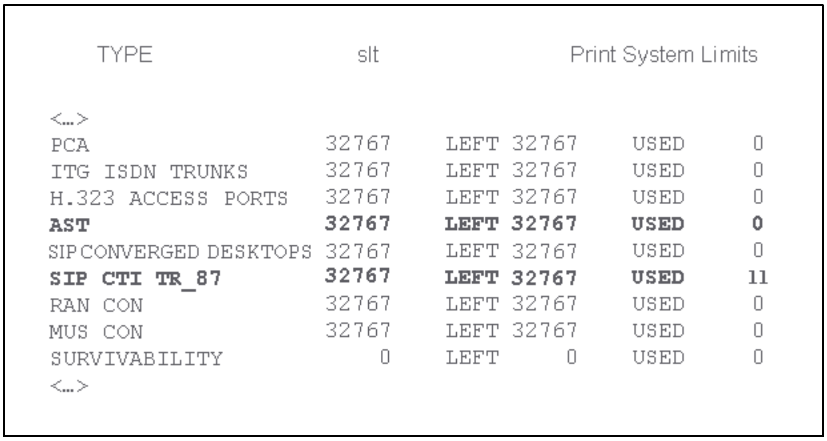
Configuring the SIP CTI TR/87 ISM Limit

A new ISM (SIP CTI TR/87) is introduced to define the number of TNs that may 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 93 "LD 22 – ISM Limit printout" (page 161)).

Figure 93
LD 22: 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
SIP CONVERGED 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.

> ***Note:*** 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 on the station display itself.

This affects whether CLID information (that may be available for calls that do not map to Active Directory users) appears on the Microsoft® 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 PCA, the MARP TN within the MADN group must be on a station and not on the PCA. From LD 11 prt dnb:

  ```
  DN 2002
  TYPE SL1
  TN 061 0 00 00 V KEY 00 MARP DES I2002 28 AUG 2005
  (I2002 )
  TN 061 0 00 21 V KEY 00 DES PCA 28 AUG 2005
  (PCA )
  ```

- Any Remote Call Control service request sent by Microsoft® Office Communicator 2005, such as Make Call or Answer Call, always apply to the device defined as the MARP TN.
- For SCR keys telephony, presence updates (for example, on the phone) are supported for all TNs within a MADN group
  Example: Answering a call on a wireless station SCR key on a non-MARP TN shows the Live Communications Server user as "On the Phone".
- For MCR keys telephony, presence is supported only for the MARP TN within a MADN group.
  Example: Answering a call on a wireless station MCR key on a non-MARP TN does not show the Live Communications Server user as "On the Phone". Only calls answered on the MARP TN affect the presence status of that user.

Configuring NRS

Use of the NRS is optional. However, if you use the NRS, 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.

Configuring the Signaling Server

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 Live 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. A new section is introduced to Element Manager to configure SIP CTI-specific parameters.

Note: 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.

Configuring Node Parameters

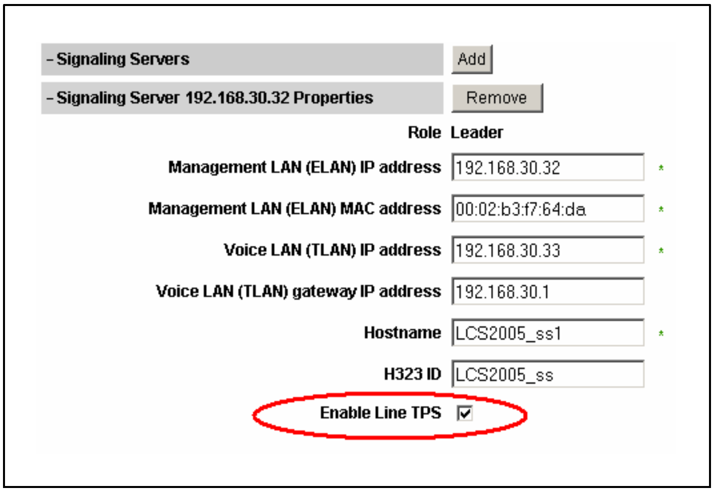
The node IP is the IP address of the TR/87 FE:

- 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.

  Note: 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.

The TR/87 FE application can run within a TPS node as well as a non-TPS node (see Figure 94 "TR/87 Node configuration" (page 163)).

Figure 94
TR/87 Node configuration



- Signaling Servers

- Signaling Server 192.168.30.32 Properties

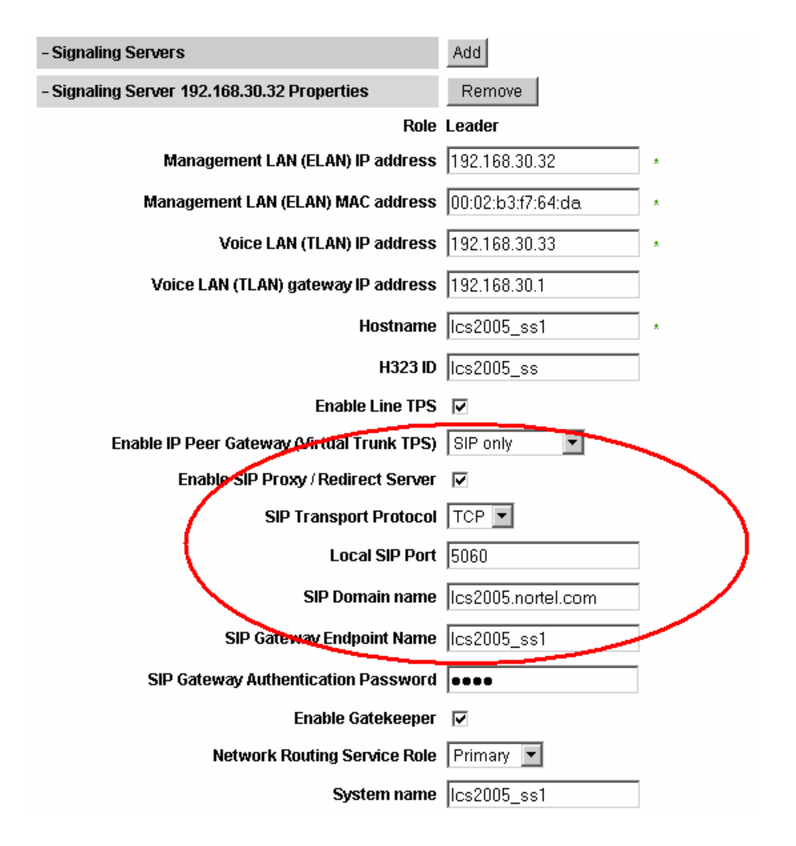
Role	Leader	
Management LAN (ELAN) IP address	192.168.30.32	*
Management LAN (ELAN) MAC address	00:02:b3:f7:64:da	*
Voice LAN (TLAN) IP address	192.168.30.33	*
Voice LAN (TLAN) gateway IP address	192.168.30.1	
Hostname	LCS2005_ss1	*
H323 ID	LCS2005_ss	
Enable Line TPS	☑	

Configuring SIP Gateway Parameters

The SIP Gateway application must be enabled. To enable the SIP Gateway, TR/87 FE uses the following SIP Gateway configuration parameters (see Figure 95 "SIP Gateway configuration" (page 164)):

- SIP Transport Protocol (must be TCP for Live Communications Server 2005 deployments)
- Local SIP Port (default 5060)
- SIP Domain Name

Figure 95
SIP Gateway configuration



- Signaling Servers

- Signaling Server 192.168.30.32 Properties

Role	Leader	
Management LAN (ELAN) IP address	192.168.30.32	*
Management LAN (ELAN) MAC address	00:02:b3:f7:64:da	*
Voice LAN (TLAN) IP address	192.168.30.33	*
Voice LAN (TLAN) gateway IP address	192.168.30.1	
Hostname	lcs2005_ss1	*
H323 ID	lcs2005_ss	
Enable Line TPS	☑	
Enable IP Peer Gateway (Virtual Trunk TPS)	SIP only	
Enable SIP Proxy / Redirect Server	☑	
SIP Transport Protocol	TCP	
Local SIP Port	5060	
SIP Domain name	lcs2005.nortel.com	
SIP Gateway Endpoint Name	lcs2005_ss1	
SIP Gateway Authentication Password	●●●●	
Enable Gatekeeper	☑	
Network Routing Service Role	Primary	
System name	lcs2005_ss1	

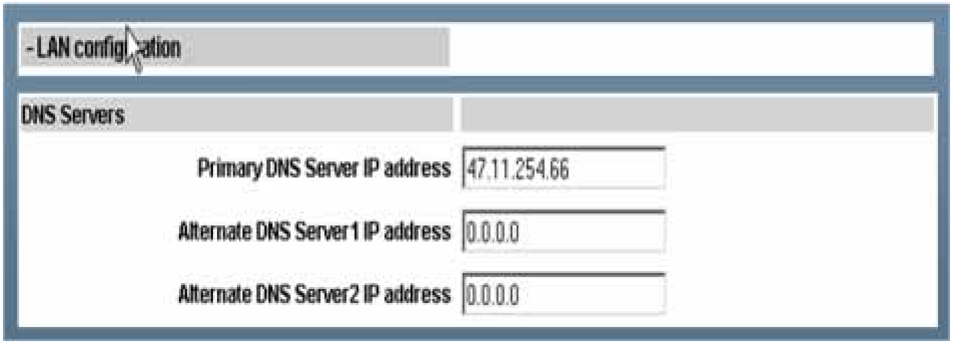
Configuring the DNS Server

Host Table configuration is replaced in Release 5.0 with DNS configuration. In Element Manager, under LAN configuration (see Figure 96 "DNS configuration" (page 165)), you have the option of entering up to three DNS server IP addresses. The DNS server must be correctly configured with the Fully Qualified Domain Name (FQDN) of all LCS Servers and Enterprise Edition Pools. Also, the FQDN must resolve to the IP address of the LCS 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.

> ***Note:*** Users upgrading from Release 4.5 to Release 5.0 still see Host Table configuration in Element Manager, but that information is no longer used.

Figure 96
DNS configuration



- LAN configuration

DNS Servers

Primary DNS Server IP address: 47.11.254.66

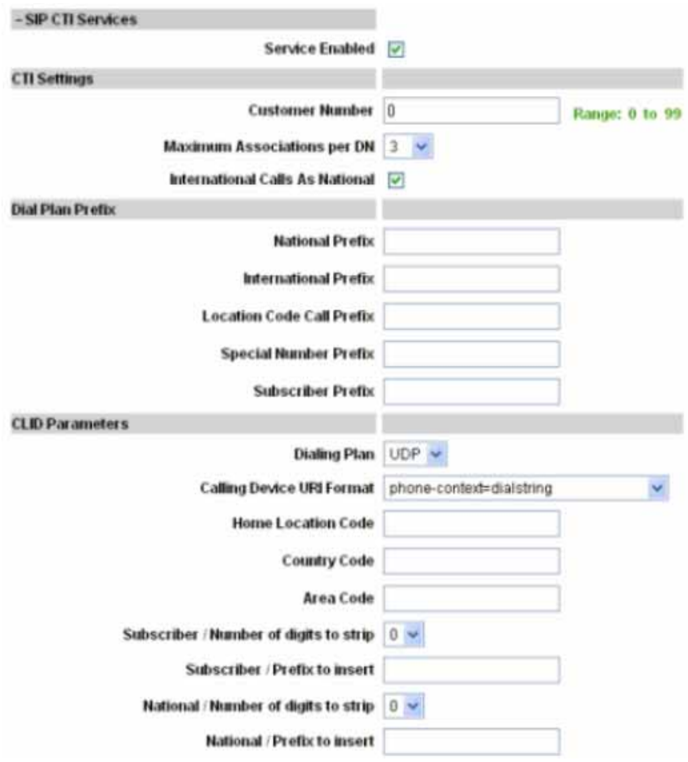
Alternate DNS Server1 IP address: 0.0.0.0

Alternate DNS Server2 IP address: 0.0.0.0

Configuring SIP CTI Settings

All SIP CTI configuration parameters can be configured in Element Manager. See Figure 97 "SIP CTI configuration" (page 165).

Figure 97
SIP CTI configuration



- SIP CTI Services

Service Enabled: ☑

CTI Settings

Customer Number: 0 Range: 0 to 99

Maximum Associations per DN: 3

International Calls As National: ☑

Dial Plan Prefix

National Prefix:

International Prefix:

Location Code Call Prefix:

Special Number Prefix:

Subscriber Prefix:

CLID Parameters

Dialing Plan: UDP

Calling Device URI Format: phone-context=dialstring

Home Location Code:

Country Code:

Area Code:

Subscriber / Number of digits to strip: 0

Subscriber / Prefix to insert:

National / Number of digits to strip: 0

National / Prefix to insert:

Note: For each of the SIP CTI settings, if a configuration change is made and a save and transfer is performed, all active SIP CTI sessions are terminated to apply the change. Microsoft® Office Communicator automatically reestablishes the session without user intervention.

Parameter: Service Enabled

The default state of the SIP CTI service is disabled. To enforce the change of state for this parameter, you must reboot. The SIP CTI service consumes approximately 140 MB of RAM on the Signaling Server when enabled.

> ***Note:*** The configuration change to enable or disable the SIP CTI service is propagated to all Signaling Servers within the node. Ensure that engineering guidelines have been 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 may 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. This parameter relates to the Office Communicator 2005 location-based forwarding feature that is based on the assumption that multiple instances of Office Communicator are active, each with their own active TR/87 session (for example, home, office, laptop). 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 Microsoft® 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 Microsoft® 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.

Configuring 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 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 "Parameter: International Calls As National" (page 166) 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 166) 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 169) 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.

Configuring SIP CTI CLID Parameters

The SIP CTI CLID parameters are used to adjust the format of phone numbers for incoming call appearances. For Microsoft® Office Communicator these settings impact the format of numbers that appear on the incoming call popup for Remote Call Control.

> ***Note:*** Note: These settings are independent of the similar SIP GW CLID parameters to allow independent control of the format of numbers on the incoming call popup 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 made 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 set to CDP, no changes are made to CDP numbers from the Call Server. However, when set 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 Microsoft® Office Communicator for RCC from DN 5000 on the same call server. The call popup that appears on the users desktop shows call from 5000.

Scenario 2 - SIP CTI Dial Plan = UDP

A call is placed to the DN controlled by Microsoft® Office Communicator for RCC from DN 5000 on the same call server. The call popup that appears on the users desktop shows call from 63435000.

Parameter: Calling Device URI Format

This configuration setting defines whether phone-context=dialstrings or the SIP Gateway URI map is used to qualify the TEL URIs used for TR/87.

> ***Note:*** For Live Communications Server installations, phone-context=dialstring must be used to ensure compatibility with Microsoft® Office Communicator.

It may be desirable to use the SIP GW URI map to qualify TEL URIs for non-Converged Office implementations as this removes the need to interpret dial plan digits outside of the Call Server.

The combination of the URIs generated by the TR/87 FE and the normalization rules available to Office Communicator 2005 define the ability for Office Communicator to match incoming phone numbers to Live 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 Microsoft® 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=dialstring:

The TEL URI generated for the caller is:
"tel:63435000;phone-context=dialstring"

Scenario 2, 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 3, Dial Plan = CDP, Calling Device URI Format = phone-context= phone-context=dialstring: The TEL URI generated for the caller is:
"tel:5000;phone-context=dialstring"

Scenario 4, Dial Plan = CDP, Calling Device URI Format = phone-context= SIP GW URI map entries:

The TEL URI generated for the caller is:
"tel:5000;phone-context=cdp.nortel.com"

When Office Communicator receives notification of an incoming call, this TEL URI is matched against all known phone numbers (after normalization) to determine if the caller is a known Live Communications Server user.

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.

Please refer to section "Parameter: Dial Plan" for an example of the use of this parameter.

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.

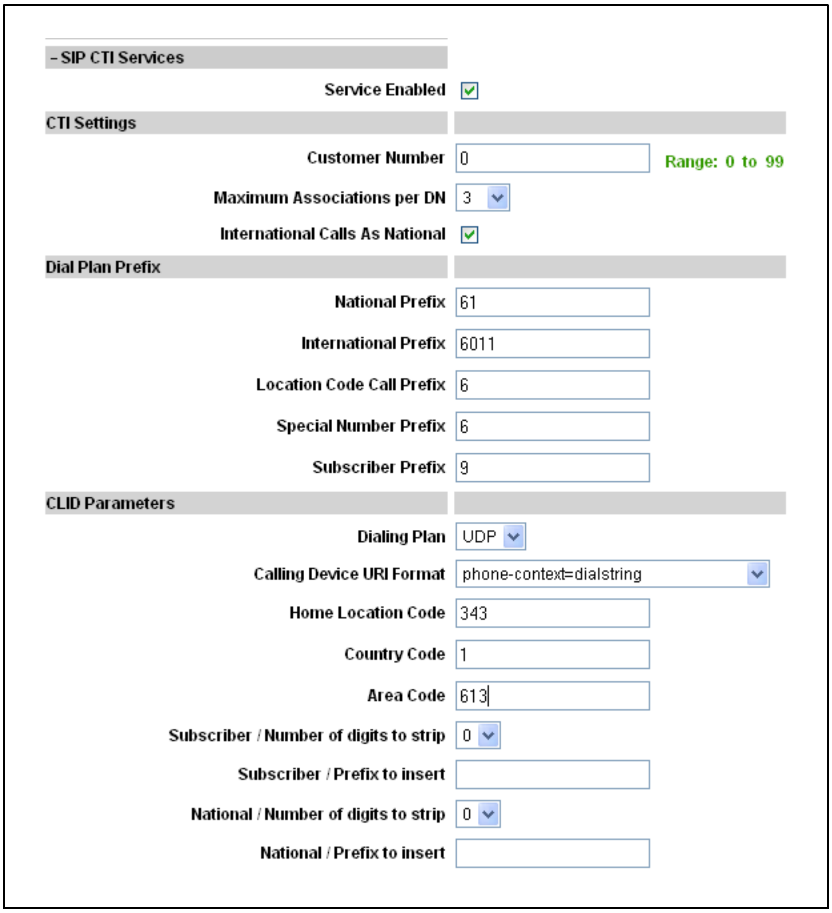
North American SIP CTI Configuration Example

With the configuration defined as in Figure 98 "North American CLID Manipulation" (page 172), the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces tel:+16134005000 on the Microsoft® Office Communicator incoming call popup.
- An incoming National Call with phone number 4169008000 produces tel:+14169008000 on the Microsoft® Office Communicator incoming call popup.
- An RCC call from Microsoft® Office Communicator to the E.164 number +16135006000 produces a call from the controlled DN to 616135006000.

An RCC call from Microsoft® Office Communicator to the E.164 number +33123456789 produces a call from the controlled DN to 601133123456789.

Figure 98
North American CLID Manipulation



- SIP CTI Services

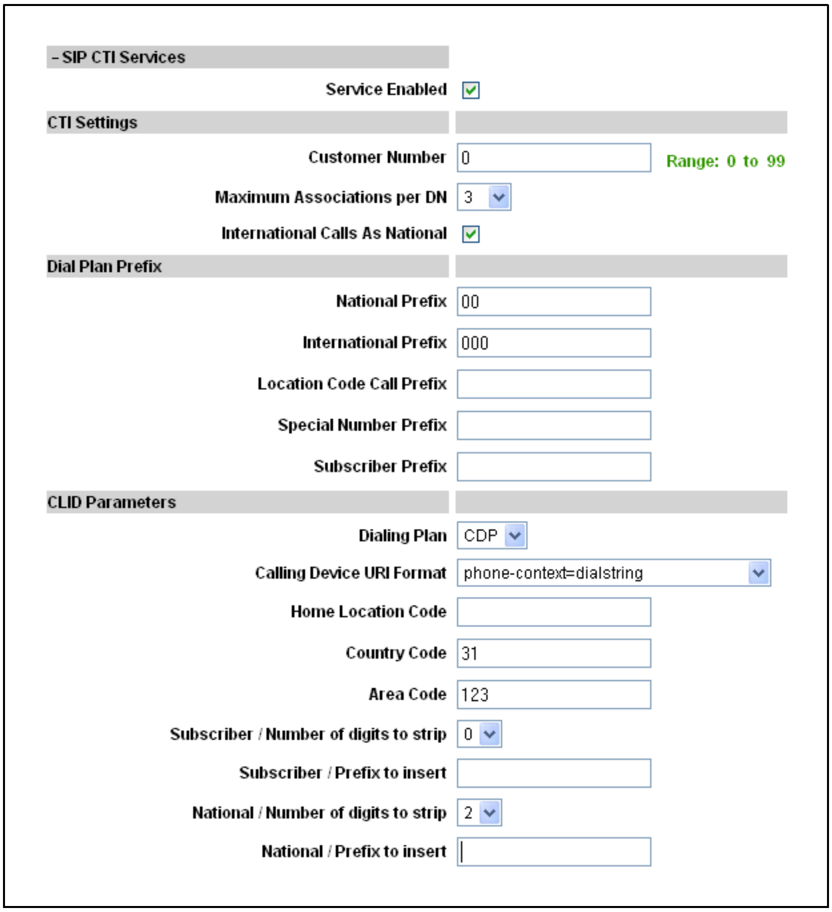
Service Enabled	☑
CTI Settings	
Customer Number	0 Range: 0 to 99
Maximum Associations per DN	3
International Calls As National	☑
Dial Plan Prefix	
National Prefix	61
International Prefix	6011
Location Code Call Prefix	6
Special Number Prefix	6
Subscriber Prefix	9
CLID Parameters	
Dialing Plan	UDP
Calling Device URI Format	phone-context=dialstring
Home Location Code	343
Country Code	1
Area Code	613
Subscriber / Number of digits to strip	0
Subscriber / Prefix to insert	
National / Number of digits to strip	0
National / Prefix to insert	

Non-North American SIP CTI Configuration Example

With the configuration defined as in Figure 99 "Non-North American CLID Manipulation" (page 173) the following occurs:

- An incoming Subscriber Call with phone number 4005000 produces +311234005000 on the Microsoft® Office Communicator incoming call popup.
- An incoming National Call with phone number 00123456789 produces +31123456789 on the Microsoft® Office Communicator incoming call popup.
- An RCC call from Microsoft® Office Communicator to the E.164 number +31123456789 produces a call from the controlled DN to 00123456789.
- An RCC call from Microsoft® Office Communicator to the E.164 number +33123456789 produces a call from the controlled DN to 00033123456789.

Figure 99
Non-North American CLID Manipulation



- SIP CTI Services		
Service Enabled	☑	
CTI Settings		
Customer Number	0	Range: 0 to 99
Maximum Associations per DN	3	
International Calls As National	☑	
Dial Plan Prefix		
National Prefix	00	
International Prefix	000	
Location Code Call Prefix		
Special Number Prefix		
Subscriber Prefix		
CLID Parameters		
Dialing Plan	CDP	
Calling Device URI Format	phone-context=dialstring	
Home Location Code		
Country Code	31	
Area Code	123	
Subscriber / Number of digits to strip	0	
Subscriber / Prefix to insert		
National / Number of digits to strip	2	
National / Prefix to insert		

Configuring Live Communications Server

Configuration of Live Communications Server for Remote Call Control has the same requirements and procedures as those documented for Telephony Gateway and Services. See "Configuring Live Communications Server" (page 112).

When configuring static routing on any Live Communications Server, the request-URI used by Microsoft Office Communicator to establish a TR/87 dialog with CS 1000 is the Remote Call Control SIP URI configured on a per-user basis in Active Directory. Information on the configuration of the Remote Call Control SIP URI can be found in"Defining the Remote Call Control SIP URI" (page 177).

There must be a static routing rule on each Live Communications Server to define the SIP routing path between the Microsoft Office Communicator client and the MCM application.

Also note that Authorization of TR/87 service requests is provided by the MCM application based on the per-user Active Directory configuration. Refer to "Configuring MCM for Remote Call Control" (page 110) for a description of this feature. If the manual configuration option is used in Microsoft Office Communicator to define the Remote Call Control SIP URI and Phone URI, please ensure that TR/87 authorization is disabled on the MCM. Without the corresponding Active Directory configuration to allow the authorization to succeed, the TR/87 SIP messages generated by Microsoft Office Communicator is rejected by the MCM.

Configuring Active Directory

This section is based on the assumption that a Live Communications Server 2005 user account is created, and that all SIP CTI configuration on the CS 1000 is complete.

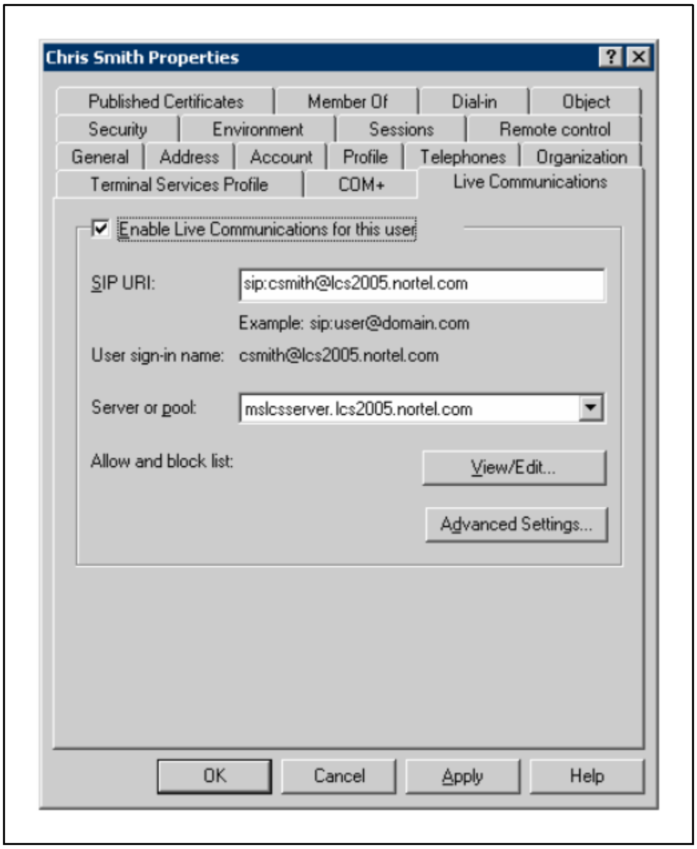
> ***Note:*** By default MCM uses GC LDAP server which contains partial information about all objects in the Active Directory domain forest. It requires replication from all Domain controllers to the GC domain controller to be performed after changes made in the Active Directory User's configuration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

Procedure 7

Active Directory configuration

Step	Action
1	In the Active Directory Users and Computers (ADUC) window, expand **Users**, right-click the user, and select **Properties**.
2	Select the **Live Communications** tab (see Figure 100 "Active Directory configuration" (page 175)).
3	On the Live Communications page, click **Advanced Settings**.
4	On the User Advanced Settings dialog box, click **Enable Remote Call Control** to enable remote control of a PBX line (see Figure 101 "User Advanced Settings" (page 176)).
5	Specify the user's **SIP URI** or **TEL URI**, and the **Destination URI** in their respective text boxes.
6	If you specified a SIP URI for the user, specify the SIP URI for the telephony gateway to which the user's calls are routed.
7	Click **OK**.

Figure 100
Active Directory configuration



Chris Smith Properties

☑ Enable Live Communications for this user

SIP URI: sip:csmith@lcs2005.nortel.com

Example: sip:user@domain.com

User sign-in name: csmith@lcs2005.nortel.com

Server or pool: mslcsserver.lcs2005.nortel.com

Allow and block list:

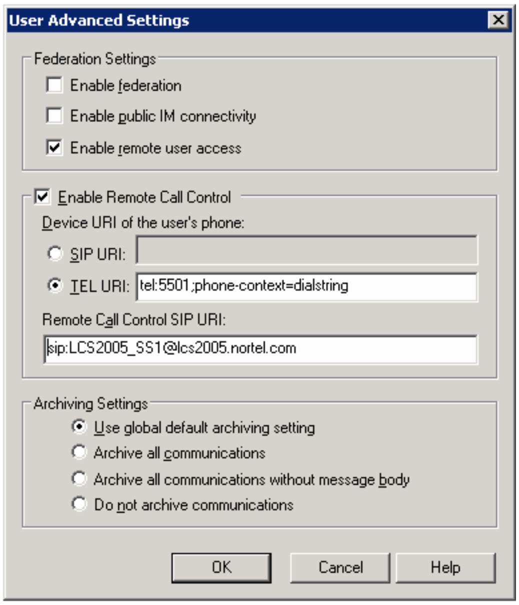
—End—

Enabling the Remote Call Control Flag

The status of the Enable Remote Call Control flag (see Figure 101 "User Advanced Settings" (page 176)), either enabled or disabled, is enforced by MCM as a part of the authorization process.

If this flag is disabled, all attempts to use Remote Call Control through automatic or manual configuration in Microsoft® Office Communicator when authorization is enabled on MCM fail due to the status of this flag.

Figure 101
User Advanced Settings



User Advanced Settings

Federation Settings

□ Enable federation

□ Enable public IM connectivity

☑ Enable remote user access

☑ Enable Remote Call Control

Device URI of the user's phone:

○ SIP URI:

● TEL URI: tel:5501;phone-context=dialstring

Remote Call Control SIP URI:

sip:LCS2005_SS1@lcs2005.nortel.com

Archiving Settings

● Use global default archiving setting

○ Archive all communications

○ Archive all communications without message body

○ Do not archive communications

Defining the Remote Call Control Controlled Line (Device URI of the phone of the user)

This configuration defines the DN to be controlled, which depends on the LD 11 configuration for the TN on which the DN key resides.

CS 1000 SIP CTI services support the following URI formats to define the controlled line (DN) for Remote Call Control:

TEL URI with a phone-context attribute If the phone-context descriptor matches the UDP domain as configured in the SIP GW URI map, the HLOC is stripped from the telephone subscriber portion of the URI prior to issuing the AML IACR request.

In all other cases, the phone-context descriptor is ignored. Examples of this are:

- tel:3432330;phone-context=LCS2005S_UDP
- tel:2330;phone-context=LCS2005S_CDP.LCS2005S_UDP
- tel:2330;phone-context=logicalDevice

TEL URI without a phone-context attribute For a TEL URI without a phone-context attribute, the number is assumed to be an E.164 number. For controlled lines, an ext attribute must be present for this to be considered a valid URI representing a controlled line.

The ext attribute value is used as the DN to acquire in the AML IACR request. For example:

tel:+16139712330;ext=2330

SIP URI A SIP URI derived from a TEL URI has the entire telephone-subscriber portion of the TEL URL, including any parameters, placed into the userinfo part of the SIP or SIPS URI.

If the SIP URI is derived from a TEL URI, then the equivalent TEL URI is handled according to the first two cases above.

> ***Note:*** The Remote Call Control SIP URI must be the same as the Signaling Server endpoint name configured on the NRS. For example, in the case of the Remote Call Control SIP URI entry sip:LCS2005_SS1@lcs2005.nortel.com, “lcs2005.nortel” is the domain name while “LCS2005_SS1” is the Signaling Server endpoint definition on the NRS.

Examples

- sip:3432330;phone-context=LCS2005S_UDP@cs1kdomain.corp.nortel.com:5060;user=phone
- sip:2330;phone-context=LCS2005S_CDP.LCS2005S_UDP@cs1kdomain.corp.nortel.com:5060;user=phone
- sip:2330;phone-context=logicalDevice@cs1kdomain.corp.nortel.com:5060;user=phone
- sip:+16139712330;ext=2330@cs1kdomain.corp.nortel.com:5060;user=phone

If the no user=phone attribute exists within the URI, the URI is not derived from a Tel URI. Therefore, the user portion must represent a user on the local PBX.

- The only users that are recognized on the CS 1000 are DNs.
- The user portion of the SIP URI is used as the DN in the AML IACR request. For example:

  sip:2330@cs1kdomain.corp.nortel.com

Defining the Remote Call Control SIP URI

The Remote Call Control SIP URI is the per-client configuration parameter that defines the content of the request URI header field in the SIP INVITE sent from Microsoft® Office Communicator to the Live Communications Server home server to establish a TR/87 SIP dialog for Remote Call Control. For example:

sip:sw18_FE@lcs2005.nortel.com

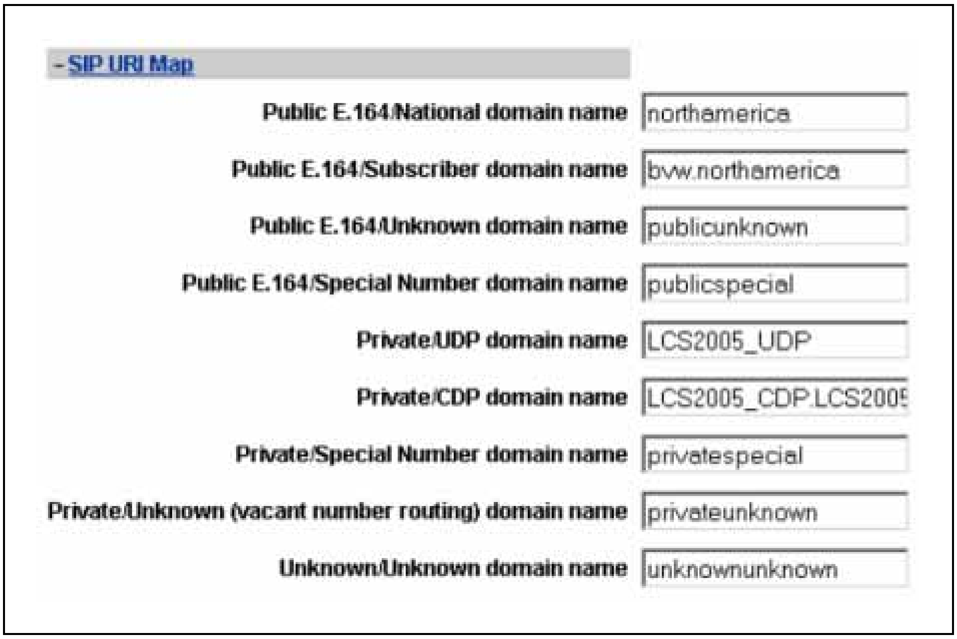
The routing configuration on the Live Communications Server Home Server defines how the TR/87 INVITE is routed based on the request URI:

- For example, the next hop for a Live Communications Server Home Server can be the proxy upon which the MCM resides.
- The MCM can be configured to route the request to an NRS or directly to a specific node with TR/87 support.

Configuring the SIP URI Map

The existing SIP URI map (see Figure 102 "SIP URI Map" (page 178)) configured for SIP GW application is also used by the TR/87 FE application to parse incoming URIs within SIP CTI service requests.

Figure 102
SIP URI Map



- SIP URI Map

Public E.164/National domain name	northamerica
Public E.164/Subscriber domain name	bvw.northamerica
Public E.164/Unknown domain name	publicunknown
Public E.164/Special Number domain name	publicspecial
Private/UDP domain name	LCS2005_UDP
Private/CDP domain name	LCS2005_CDP.LCS2005
Private/Special Number domain name	privatespecial
Private/Unknown (vacant number routing) domain name	privateunknown
Unknown/Unknown domain name	unknownunknown

Configuring Microsoft® Office Communicator 2005

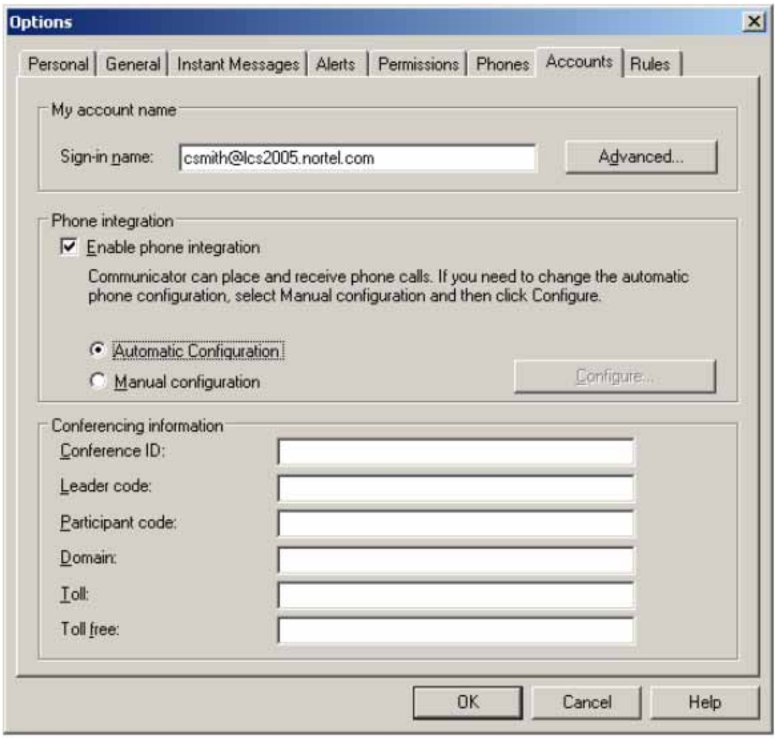
Configuring Phone Integration settings

Phone integration must be enabled on the Office Communicator 2005 client to enable the client to establish a Remote Call Control session at start-up.

Automatic configuration uses the Remote Call Control settings defined for this Live Communications Server user in Active Directory.

Using manual configuration, the settings in Active Directory can be defined locally on a per-client basis (see Figure 103 "Phone Integration settings" (page 179)).

Figure 103
Phone Integration settings



My account name

Sign-in name: csmith@lcs2005.nortel.com

Phone integration

☑ Enable phone integration

Communicator can place and receive phone calls. If you need to change the automatic phone configuration, select Manual configuration and then click Configure.

● Automatic Configuration

○ Manual configuration

Conferencing information

Conference ID:

Leader code:

Participant code:

Domain:

Toll:

Toll free:

Configuring Account details

To configure your account details, perform the following:

Procedure 8
Configuring account details

Step	Action
1	Open **Office Communicator 2005**.
2	On the Actions menu, select **Options**.
3	In the Options dialog box, click the **Accounts** tab.
4	Click **Advanced**.
5	Click **Configure settings**.

6 In Server Name or IP address, type the fully qualified domain name (FQDN) of the SIP server.

7 Select **TCP** or **TLS**.

8 Click **OK**.

—End—

Configuring the Do Not Disturb feature

To enable the Do Not Disturb feature (see Figure 104 "Enable Do Not Disturb" (page 181)), perform the following:

Procedure 9

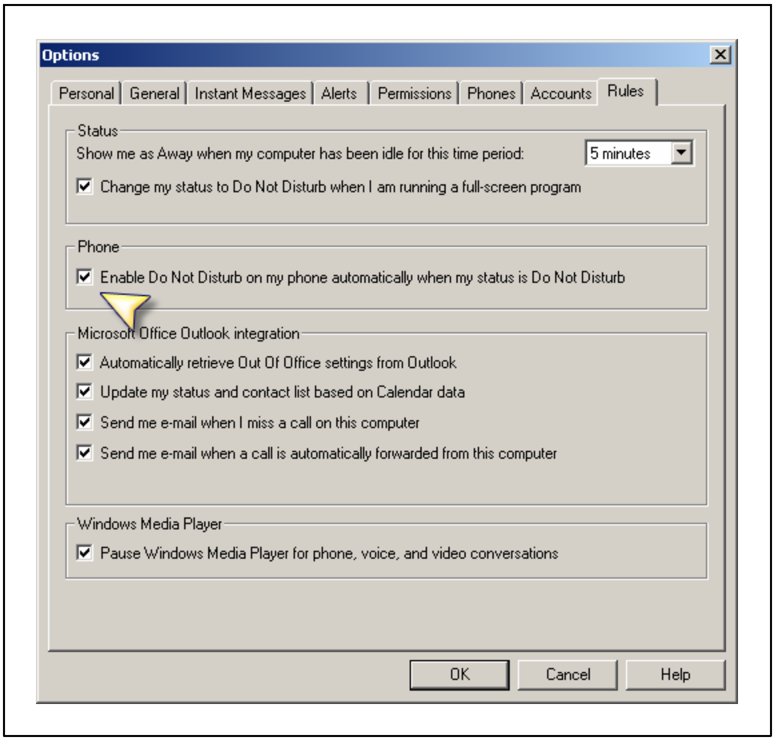
Configuring Do Not Disturb

Step	Action
1	Open **Office Communicator 2005**.
2	On the Actions menu, select **Options**.
3	In the Options dialog box, click the **Rules** tab.
4	Select **Enable Do Not Disturb on my phone automatically when my status is Do Not Disturb**.
5	Click **OK**.

> ***Note:*** Enabling the Do Not Disturb feature also requires configuration of the “Make Set Busy” key on the phone.

—End—

Figure 104
Enable Do Not Disturb



Status

Show me as Away when my computer has been idle for this time period: 5 minutes

☑ Change my status to Do Not Disturb when I am running a full-screen program

Phone

☑ Enable Do Not Disturb on my phone automatically when my status is Do Not Disturb

Microsoft Office Outlook integration

☑ Automatically retrieve Out Of Office settings from Outlook

☑ Update my status and contact list based on Calendar data

☑ Send me e-mail when I miss a call on this computer

☑ Send me e-mail when a call is automatically forwarded from this computer

Windows Media Player

☑ Pause Windows Media Player for phone, voice, and video conversations

For more information about configuring Office Communicator, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available on the Microsoft® Live Communications Server site:

www.microsoft.com/office/livecomm

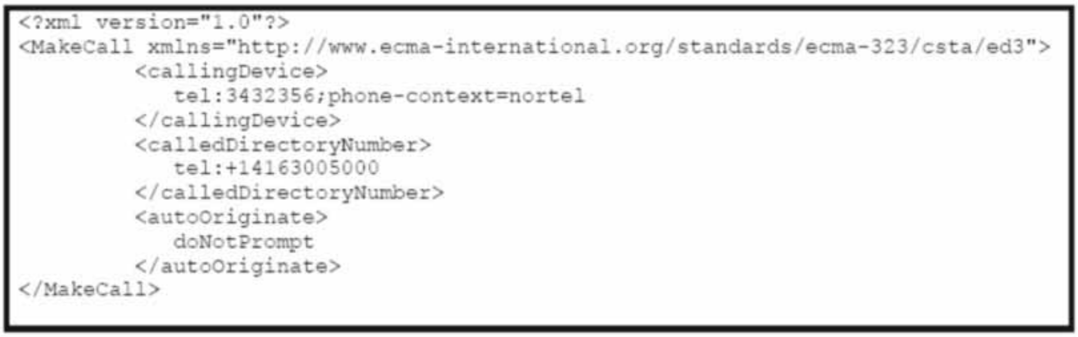
Configuring CDR

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 Microsoft® Office Communicator - Phone Calls (SIP CTI)

When a call is originated from Microsoft® 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 105 "SIP INFO message" (page 182).

Figure 105
SIP INFO message



```
<?xml version="1.0"?>
<MakeCall xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
         <callingDevice>
            tel:3432356;phone-context=nortel
         </callingDevice>
         <calledDirectoryNumber>
            tel:+14163005000
         </calledDirectoryNumber>
         <autoOriginate>
            doNotPrompt
         </autoOriginate>
</MakeCall>
```

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 the setting “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 the setting “All International Calls As National" is disabled all calls to any E.164 destination use the international dial format. Refer to the section "Parameter: International Calls As National" (page 166) for additional detail on the configuration of this feature and an illustrative example.

Normalizing phone numbers

Office Communicator 2005 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 2005 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.

For example:

(425) 7712345 x 12345

425-7712345

Phone numbers are normalized in Active Directory. Each user may have multiple phone numbers such as Office, Mobile, and Home. Two options are available to normalize these numbers: **Offline** and **Address Book Service**.

Note: All normalization rules should be in Company script.

Normalizing Offline (Recommended)

The user’s 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 should not normalize the phone numbers and should 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;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.

Creating Normalization rules

Matching incoming calling numbers to the phone numbers for a Live Communications Server user, and transforming free-form dialstrings to URIs that can be called through TR/87, is performed by Live Communications Server 2005 and Office Communicator 2005 through a process called Normalization.

Normalization rules, according to Microsoft® guidelines, must be defined to make use of the integration of Office Communicator 2005 Remote Call Control and Live Communications Server 2005 Multimedia functionality.

Each Live Communications Server user that uses Office Communicator Remote Call Control capability must have appropriate Live Communications configuration (in addition to the per-TN configuration discussed previously).

You must consider and define SIP routing for TR/87 sessions for each Live Communications Server user.

MCM provides authorization of Remote Call Control service requests based on the configuration defined in Active Directory for each Live Communications Server user.

Microsoft® 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 Live 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 Live Communications Server user identity is used to establish multimedia sessions. If the Live Communications Server user identity cannot be determined from a phone number, then Live Communications Server multimedia sessions cannot be established with the calling or called party.

Most Microsoft® interfaces and applications accept phone numbers as free-form strings. For example:

- Entering 3000 from Microsoft® Office Communicator
- Using an existing number in active directory such as ESN 343-2356
- Using an Outlook contact wizard that creates +1(613)971-2356

Normalization is the process by which a free-form string is mapped to a TEL URI. Some sample mappings for the numbers above to TEL URIs (with appropriate rules) might be:

- tel:3000;phone-context=dialstring
- tel:63432356;phone-context=dialstring
- tel:+16139712356

Refer to the *Microsoft® Office Communicator Planning and Deployment Guide* on the Microsoft® support site for further details:

www.microsoft.com/office/livecomm

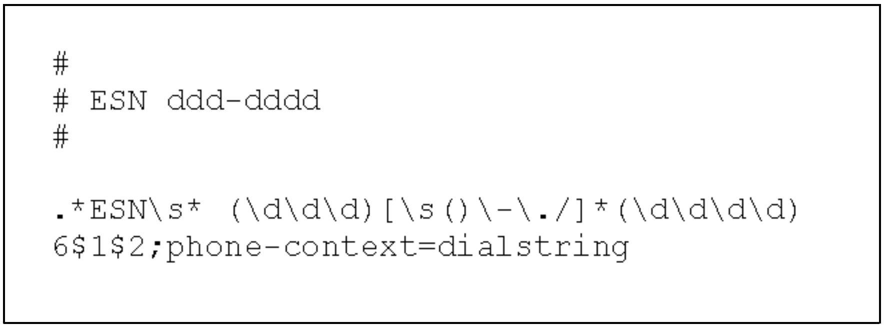
For more in-depth information about deploying the Address Book Service, refer to the *Address Book Service Planning and Deployment Guide*, also available on the Microsoft® support site.

Example

A Live 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 106 "Normalization rule example" (page 185)) to map ESN 343-2356 to tel:63432356;phone-context=dialstring

Figure 106
Normalization rule example



```
#
# ESN ddd-dddd
#

.*ESN\s*  (\d\d\d)[\s()\-\./]*(\d\d\d\d)
6$1$2;phone-context=dialstring
```

Result

- The normalized version (tel:63432356;phone-context=dialstring) of the business number in Active Directory entries is stored in the Global Address List (GAL) and downloaded at login by the Office Communicator 2005 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:63432356;phone-context=dialstring

Adding a new Normalization rule

The procedure, "Adding a new Normalization rule" (page 186), describes the process of adding a new normalization rule.

Procedure 10

Adding a new normalization rule

Step Action

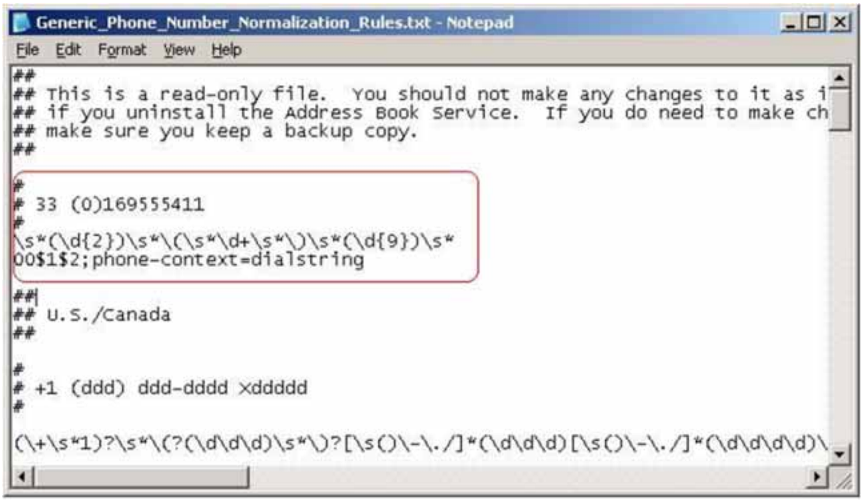
1 Add an appropriate rule to the beginning of the “%ProgramFiles%\Microsoft LC 2005\Address Book Service"\Generic_Phone_Number_Normalization_Rules.txt” file (see Figure 107 "Generic phone number normalization rules" (page 187)). A description of the language used in the Address Book Normalization rules can be found in:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpgenref/html/cpconregularexpressionslanguageelements.asp

The rules file uses a format of: 1) Regular expression; 2) Replacement pattern.

2 As in Step 1, add an appropriate rule to the beginning of the “%ProgramFiles%\Microsoft LC 2005\Address Book Service"\Company_Phone_Number_Normalization_Rules.txt” file. This ensures that the email notification provides the correct link.

Figure 107
Generic phone number normalization rules



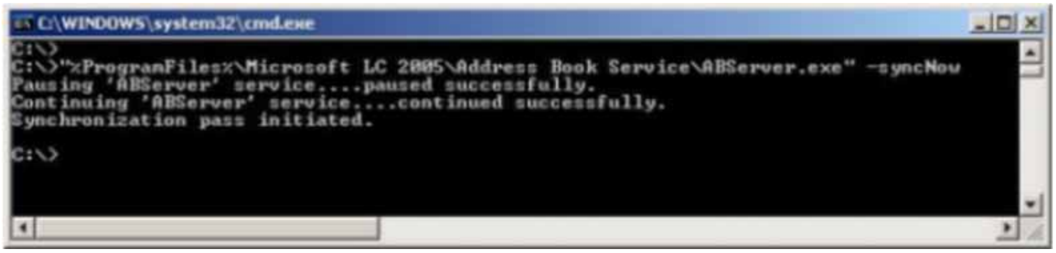
Generic_Phone_Number_Normalization_Rules.txt - Notepad
File Edit Format View Help

```
##
## This is a read-only file.  You should not make any changes to it as i
## if you uninstall the Address Book Service.  If you do need to make ch
## make sure you keep a backup copy.
##

#
# 33 (0)169555411
#
\s*(\d{2})\s*\(\s*\d+\s*\)\s*(\d{9})\s*
00$1$2;phone-context=dialstring

##
## U.S./Canada
##

#
# +1 (ddd) ddd-dddd xddddd
#

(\+\s*1)?\s*\(?(\d\d\d)\s*\)?[\s()\-\./]*(\d\d\d)[\s()\-\./]*(\d\d\d\d)\
```

3 Refresh the Address Book on the server (as shown in Figure 108 "Refresh Address Book on the server" (page 187)) by issuing the following command on the server running ABService:

“%ProgramFiles%\Microsoft LC 2005\Address Book Service\ABServer.exe -syncNow”

Figure 108
Refresh Address Book on the server



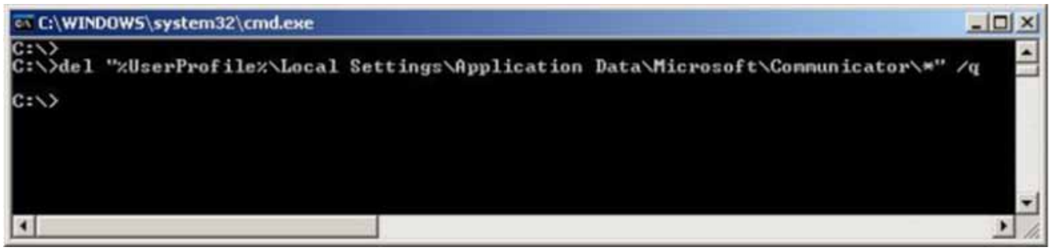
```
C:\>
C:\>"%ProgramFiles%\Microsoft LC 2005\Address Book Service\ABServer.exe" -syncNow
Pausing 'ABServer' service....paused successfully.
Continuing 'ABServer' service....continued successfully.
Synchronization pass initiated.

C:\>
```

4 Exit from Office Communicator 2005.

5 Refresh Address Book on the client (as shown in Figure 109 "Refresh Address Book on the client" (page 188)). Issue the following command on the PC running Office Communicator 2005:

Del “%UserProfile%\Local Settings\Application Data\Microsoft\Communicator\*" /q

Figure 109
Refresh Address Book on the client



```
C:\>
C:\>del "%UserProfile%\Local Settings\Application Data\Microsoft\Communicator\*" /q

C:\>
```

6 Launch Office Communicator 2005.

—End—

Configuring SIP Routing and Redundancy

Microsoft® Office Communicator 2005 is a soft phone application as well as a SIP User Agent (UA). Live Communications Server Home Server (Standard Edition Server or Enterprise Edition Server) hosts Office Communicator 2005.

The TR/87 FE within the CS 1000 is also a SIP UA. Office Communicator 2005 establishes a SIP dialog in one direction only: from the application to the TR/87 FE. The Live Communications Server home server, which functions as a SIP Proxy, is a required component. The Nortel Multimedia Communications Manager (MCM) is also required to provide support for authorization and the use of an NRS.

> ***Note:*** Due to the inability of the Office Communicator 2005 client to support the SIP 302 redirect message (a fundamental requirement for the basic operation of the NRS), the MCM application installed on the Live Communications Server to support Telephony Gateway and Services functionality is also a required component for Remote Call Control support when using Microsoft® Office Communicator 2005. The MCM application handles the 302 redirect message on behalf of Office Communicator 2005 clients.

When Office Communicator 2005 establishes a dialog with the TR/87 FE, it also retrieves the SIP address for the TR/87 FE from the Active Directory (Automatic) or from a specific server using the specified protocol (Manual).

The SIP address for the Remote Call Control Gateway can be in phone address format. Table 6 "SIP Examples" (page 189) shows examples of these addresses:

Table 6
SIP Examples

Item	Example
SIP From header	sip:alice@nortel.com
SIP To header (using a gateway endpoint name)	sip:tr87fe1@nortel.com
SIP To header (using a phone address)	sip:2356;phone-context=cdp.domain@nortel.com;user=phone
Device ID (Phone URI)	tel:2356; phone-context=cdp.domain

Configuring Remote Call Control SIP Routing Using Phone Addressing

When an NRS is used with SIP addressing, based on the phone address format, the CS 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.

Configuring Remote Call Control SIP Routing Using a Gateway Endpoint Name

If NRS is used, you must configure MCM and the TR/87 FE on the NRS as Gateway Endpoints. You can use the gateway endpoint name as the Remote Call Control URI to define the TR/87 FE that is used to service a group of users. Given that the gateway endpoint name is independent of the URI used to address a user to place a SIP call, no dependency exists on the choice of a gateway endpoint name and URIs that may be used to place SIP calls to the user. If this addressing method is used, the TR/87 FE may or may not be co-resident on the SIP gateway.

The SIP Request URI and the To: headers are populated with msRTCSIP-LineServer, provisioned in Active Directory. Office Communicator sends an INVITE message to the Live Communications Server 2005 Home Server, which hosts Office Communicator. The Home Server is identified by settings entered on the Advanced Connection Setting dialog, which is accessible from the Accounts page of the Options dialog in Office Communicator 2005.

The Live Communications Server 2005 SP1 home server forwards the INVITE message to the Next Hop FQDN, based on a static routing rule for the URI in the INVITE Request URI addressTo. The Next Hop FQDN defines a path for the INVITE that eventually leads to the proxy on which the MCM resides, or to the signaling server, which defines the TR/87 FE that supports the Remote Call Control session for this user.

If the Next Hop is not a Live Communications Server 2005 server, the Next Hop device must be provisioned as a secure link. When the SIP dialog is initially established, the same dialog path is used in both directions to route subsequent SIP messages. For information about setting static routes, refer to the next section: "Configuring Static Routes on Live Communications Server 2005".

> ***Note:*** Geographic Redundancy is supported only with the Phone Addressing format, as the alternate routing logic used to provide Geographic Redundancy for virtual trunk calls is also used for TR/87. For more information on alternate routing logic, refer to *IP Peer Networking: Installation and Commissioning* (NN43001-313)

Configuring Redundancy

For information on Redundancy, refer to "Redundancy" (page 71).

Deploying Live Communications Server Client PC application to end users

The following installations are performed once all other components have been configured and tested.

Installing Windows Messenger 5.1

Windows Messenger 5.1 must be installed on the user’s desktop before you install Office Communicator. Installing Messenger is required for "presence" in Microsoft® Office applications.

> ***Note:*** Although Windows Messenger 5.1 is not supported for the Nortel Converged Office feature, it is required to support Office Communicator 2005.

For information about Windows Messenger 5.1 installation, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

www.microsoft.com/office/livecomm

Installing Microsoft® Office Communicator 2005 client software

This section guides you through the steps to install the client component of Microsoft® Office Communicator 2005 (version 1.0) on a user's desktop.

To ensure that Office Communicator 2005 operates properly, a number of group policies must be set, and they must be set in the correct order. There are a number of deployment methods available. For a full description of the deployment options, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

www.microsoft.com/office/livecomm

Installing the Client

Use the following procedures to install the client component of Office Communicator 2005.

Procedure 11
Installing Office Communicator 2005

Step	Action
1	Double-click **Communicator.msi**.
2	Follow the instructions in the Office Communicator 2005 Setup wizard.

—End—

Procedure 12
Silent installation of Office Communicator 2005

Step	Action

1 Use the following script to silently install Office Communicator 2005:

```
%SERVERPATH%\Communicator.msi /q
```

2 After it is installed, launch Office Communicator 2005 using the following script:

```
%Program Files%\ Microsoft Office Communicator\
communicator.exe
```

—End—

ATTENTION

IMPORTANT!
The following hotfixes are required when using Office Communicator 2005 with CS 1000, and can be found under `C:\Program Files\Microsoft Office Communicator`:

- Communicator.exe
- Lcmedia.dll

At the time of publication, version 1.0.559.212 is the most current for each of these files. Refer to support.microsoft.com and search for hotfixes for Office Communicator 2005 (search "1.0.559").

For more hotfix information, refer to the following MS Knowledge Base Article:

www.support.microsoft.com/kb/928606

For a full description of the Office Communicator installation process, refer to the *Microsoft® Office Communicator 2005 Telephony Planning and Deployment Guide*, available at:

www.microsoft.com/office/livecomm

Installing Microsoft® Office 2003 and Windows XP

For full Live Communications Server integration, you must install Microsoft® Office 2003 (or later) and Windows XP (full integration). For information about how full integration may be achieved with earlier versions of Microsoft® Office, refer to the Live Communications Server site:

www.microsoft.com/office/livecomm

Configuring Transport Layer Security (TLS)

Limitations and requirements

End to End security

“End To End Security” is not supported for Converged Office solution/CS1000 Node configuration.

Issued To (subject) parameter

The Issued To (Subject) parameter must be FQDN for all certificates used by Converged Office solutions (for example: Live 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 Live 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 Live 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 Live Communications Server must resolve SPS FQDN to its IP address—and vise versa.

Private Certificate Authority (Nortel ECM)

Certificates signed by the Private CA (Nortel ECM) cannot be used on the Live Communications Server. For example, certificates for LCS servers must be issued by either Microsoft CA or another external CA (refer to Microsoft’s Live Communications Server 2005 Configuring Certificates: office.microsoft.com/en-us/FX011450741033.aspx

Configuring TLS

The next procedure describes how to configure TLS for Converged Office. For this procedure, the following is assumed:

A Live Communications Server SE Home Server running MCM with:

- IP Address – 192.168.60.9
- FQDN – mslcsserver.mslcs.mera.ru

A SIP Proxy Server (SPS):

- IP Address – 192.168.29.100
- FQDN – aknv-4221.mera.ru

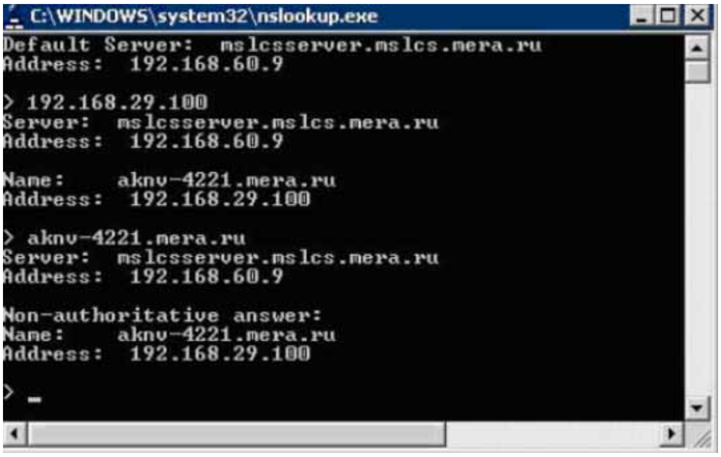
Live Communications Server uses certificates issued by the Microsoft Certification Authority. CS 1000 components use the Private CA (Nortel ECM) signed certificates.

Procedure 13
Configuring TLS

Step	Action
1	Configure the DNS server (see Figure 110 "Configure the DNS server" (page 194)) used by Live Communications Server to resolve SPS FQDN to its IP Address and vice versa.

> ***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 110
Configure the DNS server

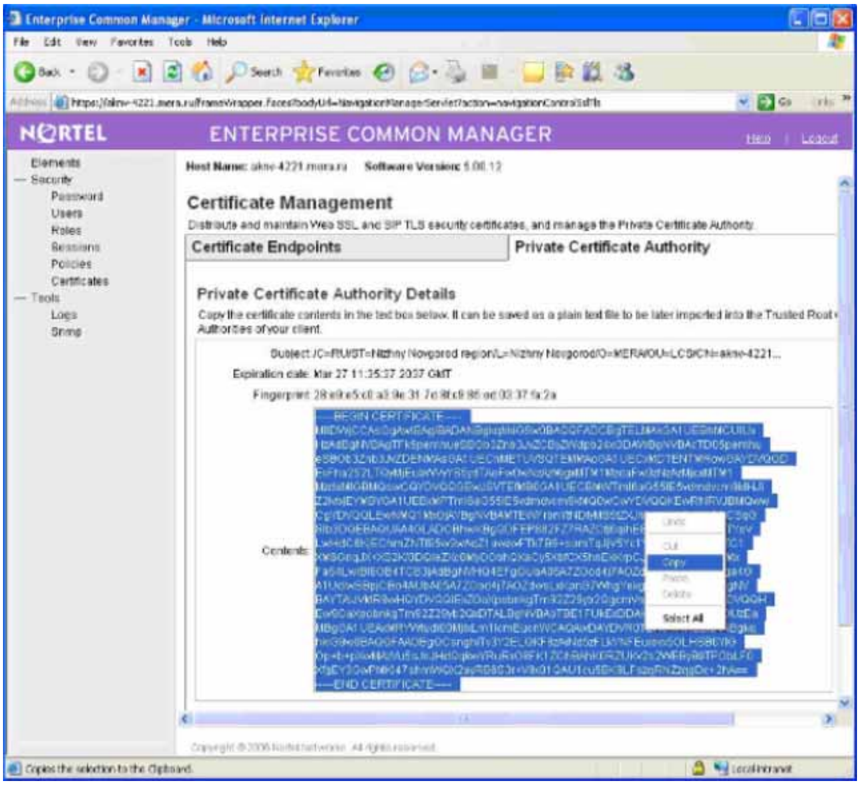


```
Default Server:  mslcsserver.mslcs.mera.ru
Address:  192.168.60.9

> 192.168.29.100
Server:  mslcsserver.mslcs.mera.ru
Address:  192.168.60.9

Name:    aknv-4221.mera.ru
Address:  192.168.29.100

> aknv-4221.mera.ru
Server:  mslcsserver.mslcs.mera.ru
Address:  192.168.60.9

Non-authoritative answer:
Name:    aknv-4221.mera.ru
Address:  192.168.29.100

> _
```

Step	Action
2	Add Private CA certificate to the Trusted Root Certification Authorities

Copy and Save Private CA certificate to a file on the LCS server (see Figure 111 "Private Certificate Authority" (page 195)).

Figure 111
Private Certificate Authority



Enterprise Common Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://akne-4221.mera.ru/frameWrapper.faces?bodyUrl=NavigationManagerServlet?action=navigationControl&sf%
Go Links
NORTEL ENTERPRISE COMMON MANAGER
Help | Logout
Elements
— Security
Password
Users
Roles
Sessions
Policies
Certificates
— Tools
Logs
Snmp
Undo
Cut
Copy
Paste
Delete
Select All
Local intranet

Host Name: akne-4221.mera.ru Software Version: 5.00.12

Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority

Certificate Endpoints | Private Certificate Authority

Private Certificate Authority Details

Copy the certificate contents in the text box below. It can be saved as a plain text file to be later imported into the Trusted Root Authorities of your client.

Subject /C=RU/ST=Nizhny Novgorod region/L=Nizhny Novgorod/O=MERA/OU=LCS/CN=akne-4221...

Expiration date Mar 27 11:35:37 2037 GMT

Fingerprint 28:e9:e5:c0:a3:9e:31:7c:8f:c9:86:ec:03:37:fa:2a

Contents

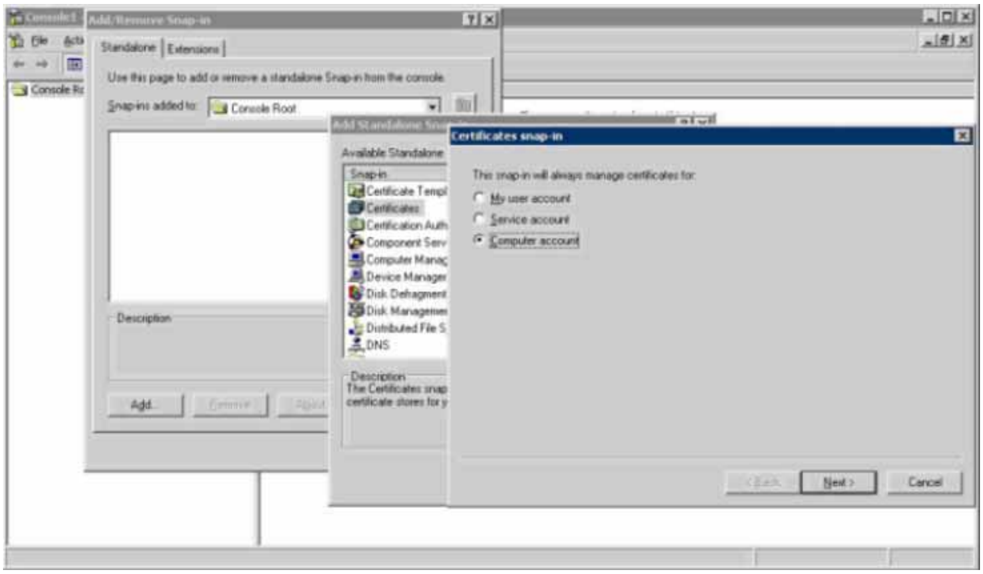
```
-----BEGIN CERTIFICATE-----
[illegible]
-----END CERTIFICATE-----
```

Copyright © 2006 Nortel Networks. All rights reserved.

Copies the selection to the clipboard.

3 Open MMC on the Live Communication Server server and add the Certificates (Local Computer) snap-in (see Figure 112 "Certificates snap-in" (page 196)).

Figure 112
Certificates snap-in



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

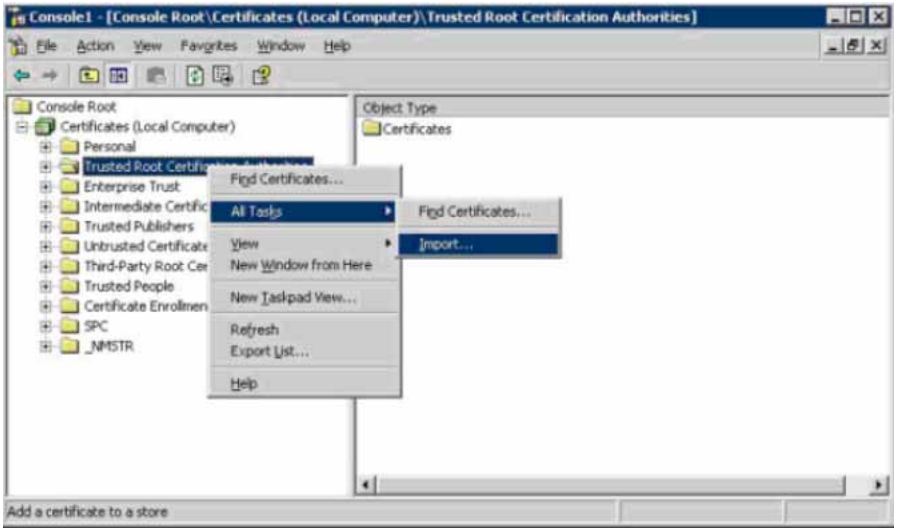
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

4 Import the saved file to the Trusted Root Certification Authorities (see Figure 113 "Import to Trusted Root Certificate Authorities" (page 196)).

Figure 113
Import to Trusted Root Certificate Authorities

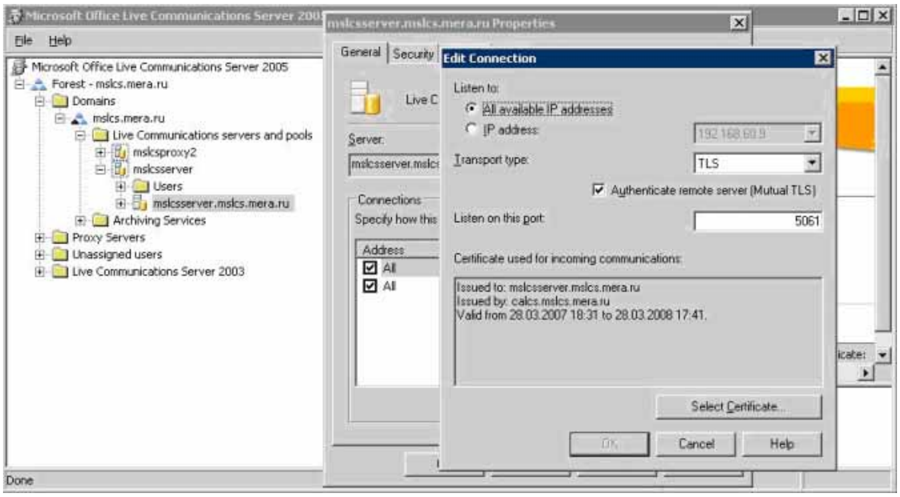


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities]

Add a certificate to a store

5 Enable incoming TLS connections on the Live Communication Server (see Figure 114 "Enable Incoming TLS connections" (page 197)).

Figure 114
Enable Incoming TLS connections


Microsoft Office Live Communications Server 2005
File Help
Microsoft Office Live Communications Server 2005
Forest - mslcs.mera.ru
Domains
mslcs.mera.ru
Live Communications servers and pools
mslcsproxy2
mslcsserver
Users
mslcsserver.mslcs.mera.ru
Archiving Services
Proxy Servers
Unassigned users
Live Communications Server 2003
Done
mslcsserver.mslcs.mera.ru Properties
General Security
Server:
Connections
Address
All
All

Edit Connection

Listen to:
● All available IP addresses
○ IP address: 192.168.60.9

Transport type: TLS

☑ Authenticate remote server (Mutual TLS)

Listen on this port: 5061

Certificate used for incoming communications:

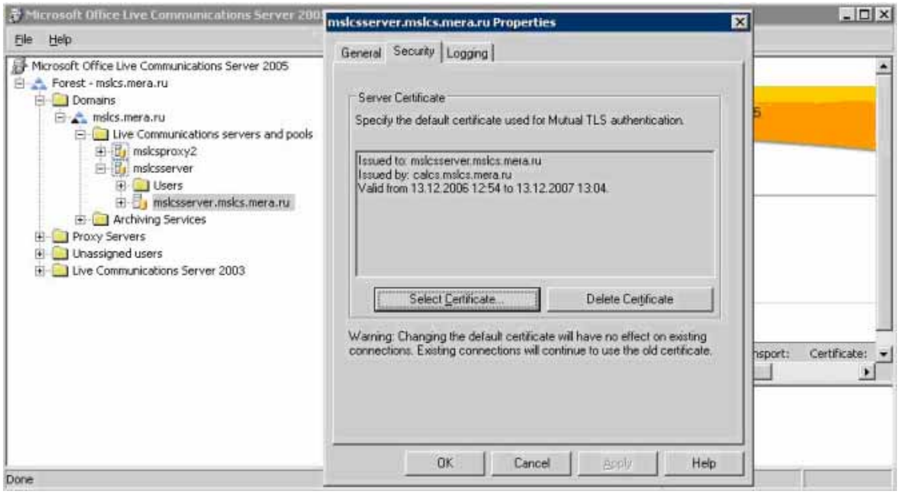
Issued to: mslcsserver.mslcs.mera.ru
Issued by: calcs.mslcs.mera.ru
Valid from 28.03.2007 18:31 to 28.03.2008 17:41.

Select Certificate...

OK Cancel Help

6 Configure the default certificate used for outgoing TLS connections by the Live Communications Server (see Figure 115 "Configure default certificate" (page 197)).

Figure 115
Configure default certificate


Microsoft Office Live Communications Server 2005
File Help
Microsoft Office Live Communications Server 2005
Forest - mslcs.mera.ru
Domains
mslcs.mera.ru
Live Communications servers and pools
mslcsproxy2
mslcsserver
Users
mslcsserver.mslcs.mera.ru
Archiving Services
Proxy Servers
Unassigned users
Live Communications Server 2003
Done

mslcsserver.mslcs.mera.ru Properties

General Security Logging

Server Certificate

Specify the default certificate used for Mutual TLS authentication.

Issued to: mslcsserver.mslcs.mera.ru
Issued by: calcs.mslcs.mera.ru
Valid from 13.12.2006 12:54 to 13.12.2007 13:04.

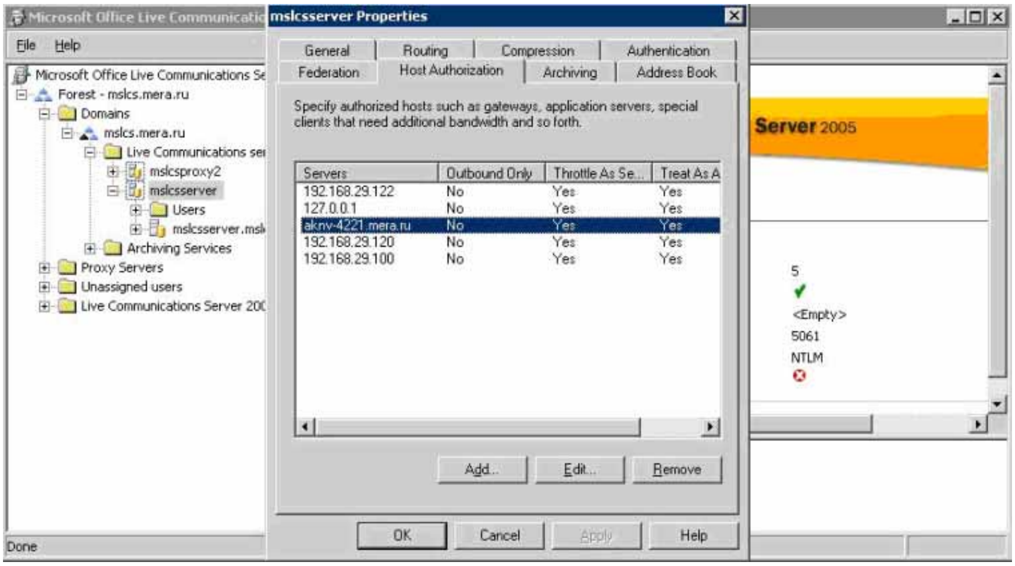
Select Certificate... Delete Certificate

Warning: Changing the default certificate will have no effect on existing connections. Existing connections will continue to use the old certificate.

OK Cancel Apply Help

7 Add **SPS FQDN** to the Host Authorization table on the Live Communication Server (see Figure 116 "Add SPS FQDN" (page 198)).

Figure 116
Add SPS FQDN



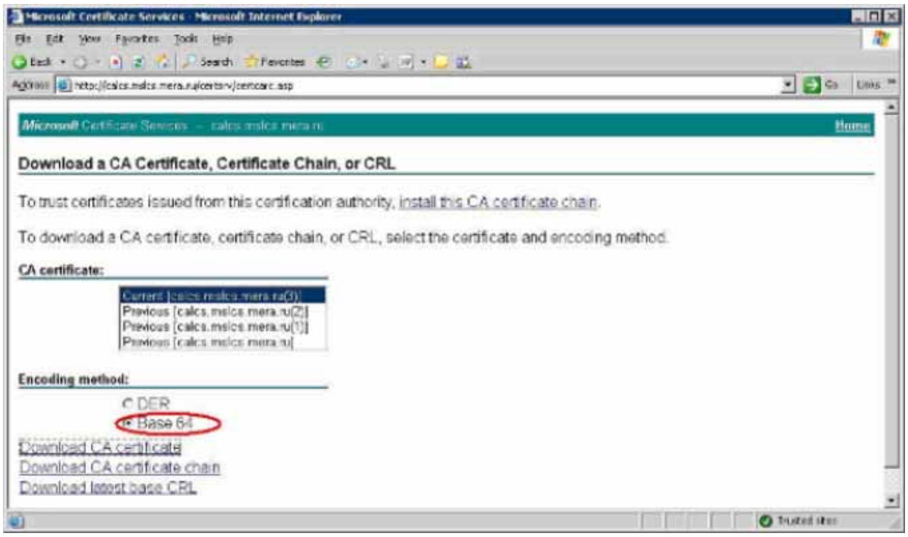
Specify authorized hosts such as gateways, application servers, special clients that need additional bandwidth and so forth.

Servers	Outbound Only	Throttle As Se...	Treat As A
192.168.29.122	No	Yes	Yes
127.0.0.1	No	Yes	Yes
aknv-4221.mera.ru	No	Yes	Yes
192.168.29.120	No	Yes	Yes
192.168.29.100	No	Yes	Yes

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 have to be added to the table.

8 Add Microsoft CA certificate to the Trusted Certificate Authorities on SPS (see Figure 117 "Add Microsoft CA Certificate" (page 199)). Download Microsoft CA certificate and save it to file on the Live Communication Server in Base-64 encoding

Figure 117
Add Microsoft CA Certificate


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://calcs.mslcs.mera.ru/certsrv/certcarc.asp
Go Links
Microsoft Certificate Services -- calcs.mslcs.mera.ru
Home
Trusted sites

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [calcs.mslcs.mera.ru(3)]
Previous [calcs.mslcs.mera.ru(2)]
Previous [calcs.mslcs.mera.ru(1)]
Previous [calcs.mslcs.mera.ru]

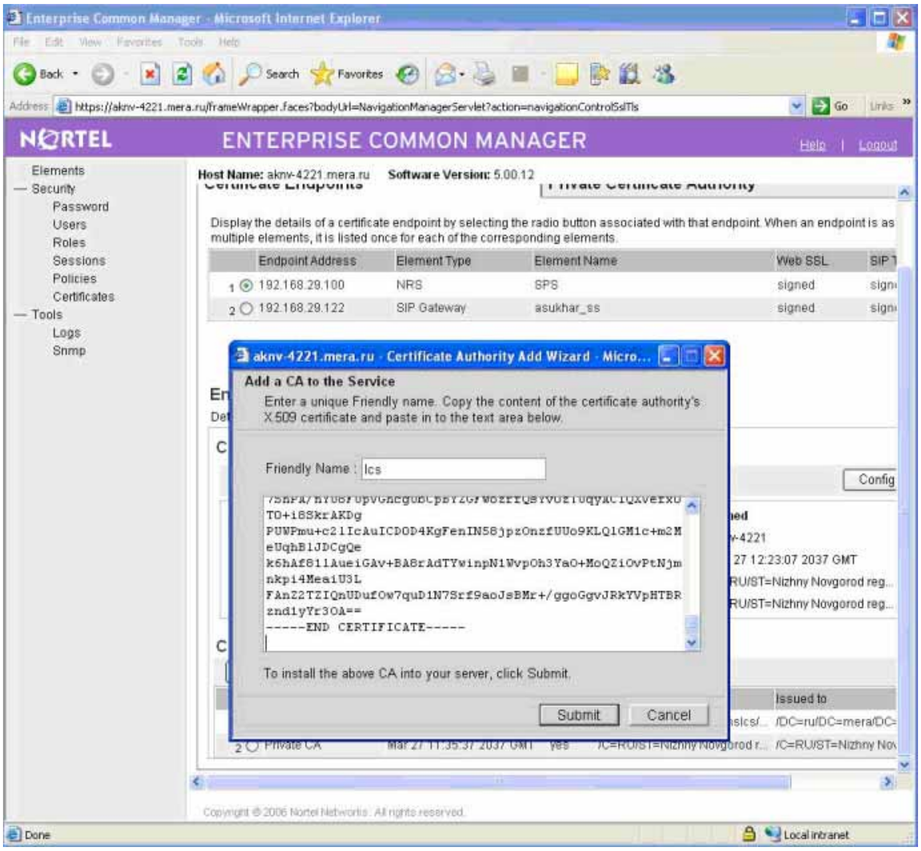
Encoding method:

○ DER
● Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL

9 Open the saved file in Notepad and copy its content to clipboard. Add the copied content to the Trusted Certificate Authorities (see Figure 118 "Add a CA to the Service" (page 200)).

Figure 118
Add a CA to the Service



Enterprise Common Manager - Microsoft Internet Explorer

Address: https://aknv-4221.mera.ru/frameWrapper.faces?bodyUrl=NavigationManagerServlet?action=navigationControlSslTls

ENTERPRISE COMMON MANAGER

Host Name: aknv-4221.mera.ru Software Version: 5.00.12

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is as multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Web SSL	SIP T
1 ●	192.168.29.100	NRS	SPS	signed	sign
2 ○	192.168.29.122	SIP Gateway	asukhar_ss	signed	sign

aknv-4221.mera.ru - Certificate Authority Add Wizard - Micro...

Add a CA to the Service

Enter a unique Friendly name. Copy the content of the certificate authority's X.509 certificate and paste in to the text area below.

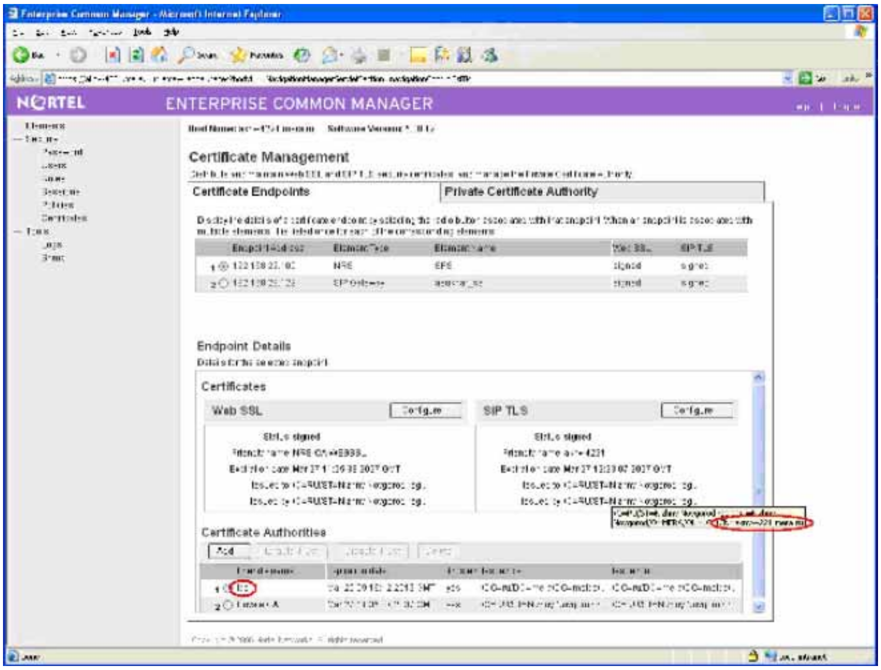
Friendly Name : lcs

```
T0+i8SkrAKDg
PUWPmu+c21IcAuICDOD4KgFenIN58jpzOnzfUUo9KLQ1GM1c+m2M
eUqhB1JDCgQe
k6hAf811AueiGAv+BA8rAdTYwinpN1WvpOh3YaO+MoQZiOvPtNjm
nkpi4MeaiU3L
FAnZ2TZIQnUDufOw7quD1N7Srf9aoJsBMr+/ggoGgvJRkYVpHTBR
zndiyYr3OA==
-----END CERTIFICATE-----
```

To install the above CA into your server, click Submit.

Figure 119 "Certificate Endpoints" (page 201) shows the newly added Certificate Authority:

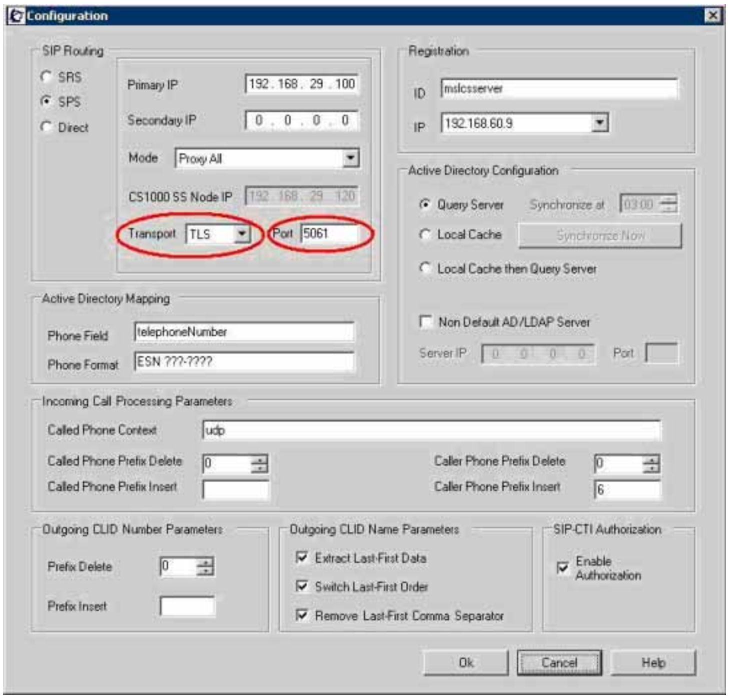
Figure 119
Certificate Endpoints



Note: The Certificate used by SPS is issued to its FQDN. If SPS is used by MCM in a Redirect mode (Redirect All, Proxy SIP and Redirect SIP-CTI) then the same actions have to be done for each SIP GW/SIP CTI FE.

10 Configure TLS transport on MCM as shown in Figure 120 "Configure TLS transport" (page 202).

Figure 120
Configure TLS transport



Configuration

SIP Routing
○ SRS
● SPS
○ Direct

Primary IP 192 . 168 . 29 . 100
Secondary IP 0 . 0 . 0 . 0
Mode Proxy All
CS1000 SS Node IP 192 . 168 . 29 . 120
Transport TLS
Port 5061

Registration
ID mslcsserver
IP 192.168.60.9

Active Directory Configuration
● Query Server Synchronize at 03:00
○ Local Cache Synchronize Now
○ Local Cache then Query Server
□ Non Default AD/LDAP Server
Server IP 0 . 0 . 0 . 0 Port

Active Directory Mapping
Phone Field telephoneNumber
Phone Format ESN ???-????

Incoming Call Processing Parameters
Called Phone Context udp
Called Phone Prefix Delete 0
Called Phone Prefix Insert
Caller Phone Prefix Delete 0
Caller Phone Prefix Insert 6

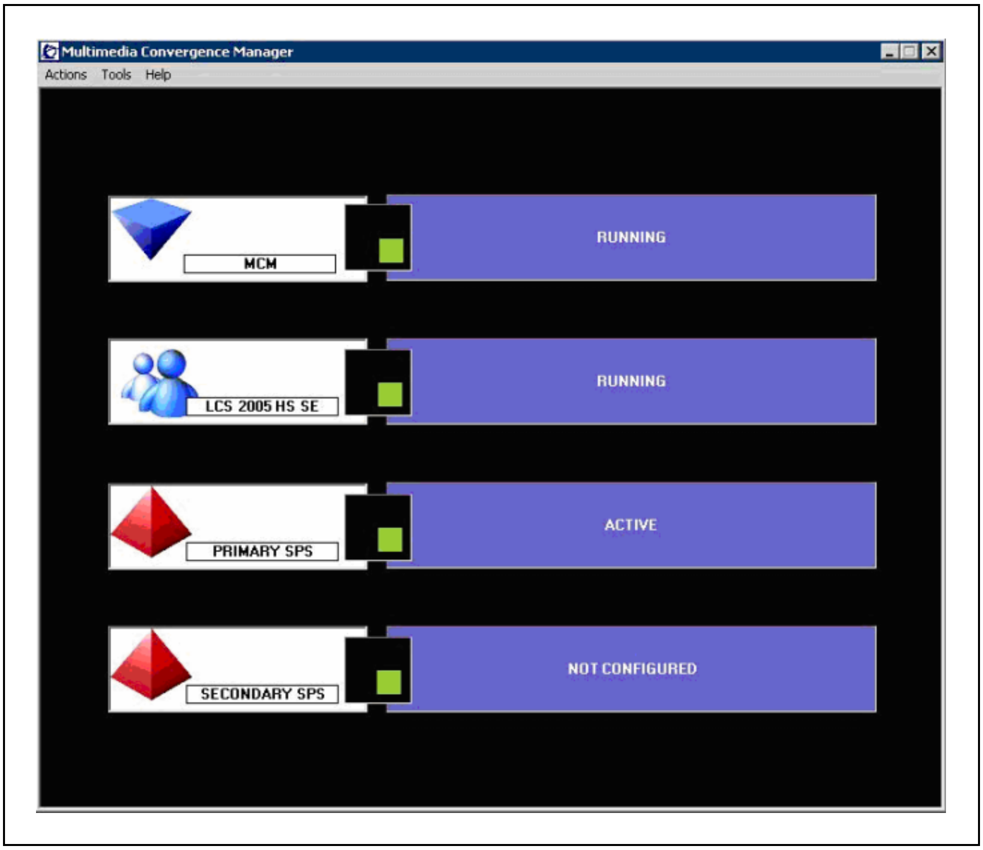
Outgoing CLID Number Parameters
Prefix Delete 0
Prefix Insert

Outgoing CLID Name Parameters
☑ Extract Last-First Data
☑ Switch Last-First Order
☑ Remove Last-First Comma Separator

SIP-CTI Authorization
☑ Enable Authorization

11 Check that MCM is registered with SPS (see Figure 121 "MCM Status" (page 203)).

Figure 121
MCM Status



If the SPS status is NOT RESPONDING, it may take up to five minutes until all the Live Communication Server changes are applied.

—End—

For more information on TLS, refer to:

- *Security Management* (NN43001-604) NTP
- Microsoft's Live Communications Server 2005 Configuring Certificates: office.microsoft.com/en-us/FX011450741033.aspx

Maintenance

Contents

This section contains information about the following topics:

Introduction

The following are maintenance and troubleshooting tips for the Telephony Gateway and Services and Remote Call Control components.

Telephony Gateway and Services

CS 1000

No new SIP tracing capabilities are available on the CS 1000. Existing SIP Trunk and Gateway tracing capabilities are used.

MCM

MCM 2.0 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 (set) which information is logged in the MCM log file. For more information about logging, refer to "Logging" (page 206).
- Get Active Calls Count: Show how many calls are connected through Live Communications Server.

- — The Multimedia Convergence Manager 1.0 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 Live Communications Server 2005 Application Proxy to provide call traces. MCM also provides full SIP-tracing capability. MCM SIP tracing is important particularly when MTLS is enabled -in future CS1000 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.
- — You can remotely access the Live Communications Server application using the Windows 2003 server remote access capability.
- — Task Manager is supported in Windows 2003 Server for MCM.

Logging

MCM 2.0 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 2.0.
- **Debug**: Debug information is logged to the MCM log file.
- **SIP and Debug**

The MCM 2.0 creates 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 MCM 2.0 application. Alarms are logged to an MCM log file in addition to the Windows 2003 Event Viewer.

Generally, when a problem is encountered, it is recommended that you check the logs as follows:

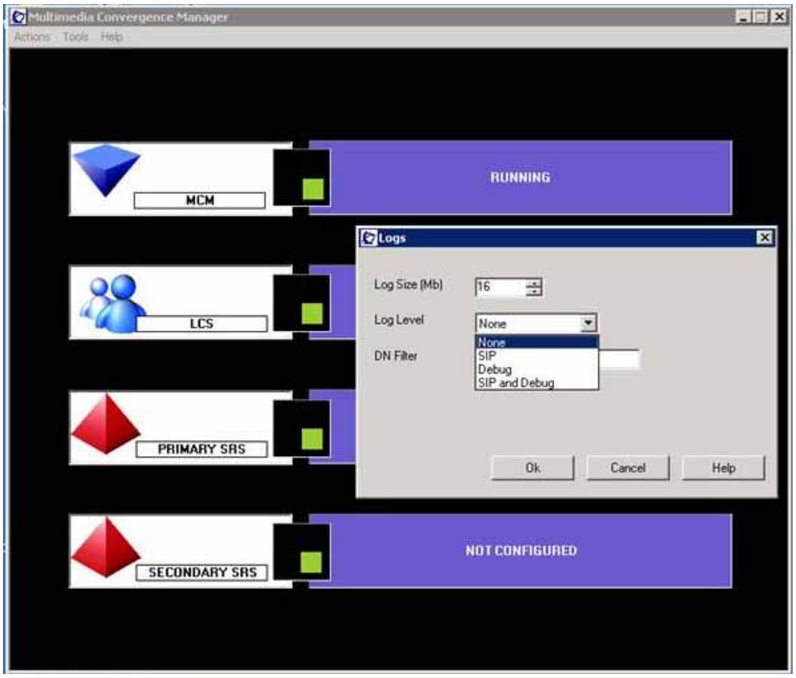
1. CS 1000 Signaling Server logs
2. MCM logs
3. Live Communications Server logs.

The following section details how to turn on MCM logging and what to expect.

MCM.log file The MCM log is captured through the MCM utility OAM.

Select **Tools > Set Log Level**. Set the Log Level to Debug (see Figure 122 "MCM Logs" (page 207)). This is the highest level of debug. The MCM.log file is located in the following directory: Program Files/Nortel Networks/MCM/MCM.log.

Figure 122
MCM Logs



Log Size (Mb) 16

Log Level None

DN Filter

The following is an example of an MCM log:

```
-----------------------------------------------------------------------------------------
05.04.2006 12:44:07: 1.0.19.14: Debug: ServerEventHandler: got Event #0
05.04.2006 12:44:07: 1.0.19.14: Debug: ServerEventHandler: got Event #0
05.04.2006 12:44:08: 1.0.19.14: Debug: ServerEventHandler: got Event #0
05.04.2006 12:44:08: 1.0.19.14: SIP:
-----------------------------------------------------------------------------------------

Request: INVITE sip:svg-cs1000@domain.local
contact:<sip:werner@domain.local:1668;maddr=192.168.77.100;transport=tcp;ms-received-cid=B00>
via: SIP/2.0/TCP192.168.77.100:13224;ms-received-port=
1668;ms-received-cid=b00
max-forwards: 70
from: "Werner Myrvang"<sip:werner@domain.local>;tag=a8d52f94b8;epid=a64eccfac2
```

```
to:<sip:sip:svg-cs1000@domain.local>
call-id: 3b55793fa6da4109bbb73f580d7002ae
cseq: 1 INVITE
user-agent: LCC/1.3
supported: timer
Session-Expires: 1800;refresher=uac
Min-SE: 1800
content-disposition: signal;handling=required
content-type: application/csta+xml
content-length: 350

<?xml version="1.0"?>
<RequestSystemStatus xmlns="http://www.ecma-international.org/ stan-
dards/ecma-323/csta/ed3"><extensions><privateData><private><lcs:line
xmlns:lcs="http://schemas.microsoft.com/Lcs/2005/04/
RCCExtension"><tel:67381:phones-context=cdpsvg-cs1000.livecomm-
lab.co
m</lcs:line></private></privateData></extensions></
RequestSystemStatus
```

Patches and upgrades

Patching is not supported in MCM 2.0. Fixes are provided in up-issues and maintenance releases.

Software upgrades install the new application and use or upgrade the existing configuration file. MCM 2.0 is delivered on a CD and available for download from the Nortel web site.

All customer configured MCM application data is retained in case of the MCM application upgrade.

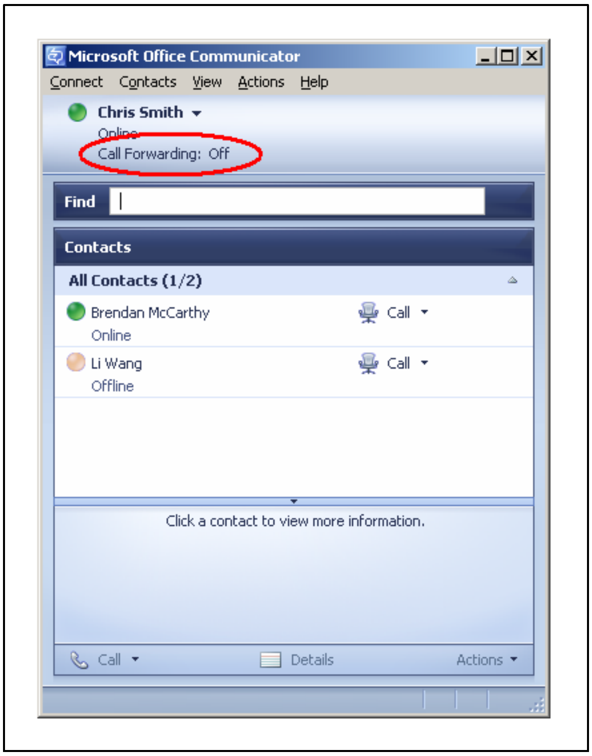
Remote Call Control

One of the first questions raised when Office Communicator 2005 is not working correctly is "Is Phone Integration enabled and active?"

If Phone Integration is enabled in Office Communicator and a SIP dialog for TR/87 was established successfully, the Call Forward menu item is visible in the Office Communicator user interface (see Figure 123 "Phone Integration enabled" (page 209)).

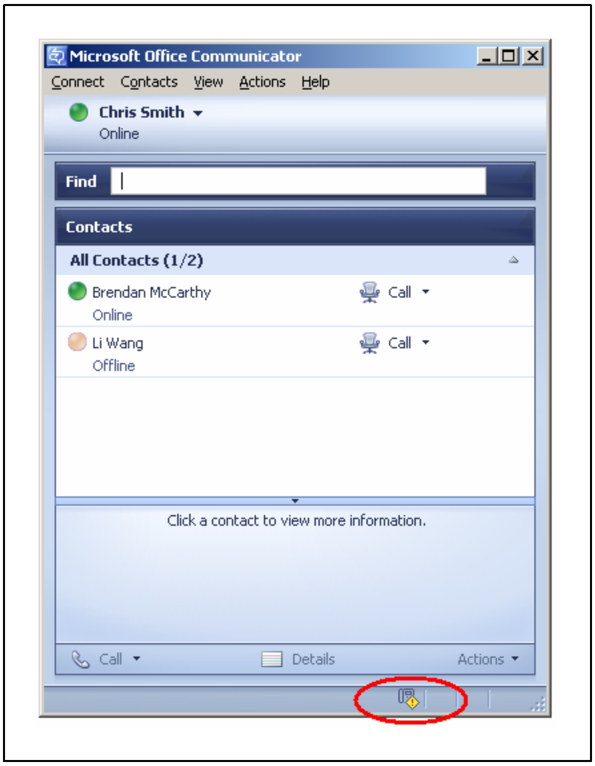
If Phone Integration is enabled in Office Communicator and a SIP dialog for TR/87 was attempted and not established successfully, a small icon is visible in the lower right corner of the Office Communicator user interface (see Figure 124 "SIP dialog not established" (page 210)).

Figure 123
Phone Integration enabled



Click a contact to view more information.

Figure 124
SIP dialog not established



Click a contact to view more information.

Signaling Server OAM Level CLI Commands

The Signaling Server OAM Level CLI commands are used to query activeTR/87 sessions to turn on tracing at the SIP level. 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 7
Signaling Server OAM Level CLI commands

Command	Description
SIPCTISessionShow	Show the total number of TR87 SIP sessions.
SIPCTITraceShow	Display the trace settings for SIP CTI application, including the trace filter setting and output setting.
SIPCTIShow	Show SIP CTI application status and configuration.
SIPCTIClientShow	Show information about the all the soft clients associated.

Command	Description
SIPCTITraceLevel <level>	Set 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: 1. TTY 2. RPTLOG 3. File 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.

Operational Measurements

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 on how to access these OM’s through Element Manager, refer to *Element Manager: System Administration* (NN43001-632).

Signaling Server Expert Level CLI Commands

Using Signaling Server Expert Level CLI commands (see Table 8 "Signaling Server Expert Level CLI commands" (page 213)), 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 8
Signaling Server Expert Level CLI commands

Command	Description
SIPCTIAmlTrace level	Set 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. ***Note:*** 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.

Appendix A
Call Flow and Protocol Details

Contents

This section contains information about the following topics:

Overview

The Converged Office feature provides interworking between Nortel and Microsoft® products to address the market in which customers require that their user community use Microsoft® client software for their multimedia needs, but want to use the Business Grade Telephony of 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 Microsoft® Office Communicator 2005 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 Microsoft® Office Communicator 2005, a TR/87 session initiated by the Contact Center Manager Server (CCMS), or some other SIP UA.

Within the scope of CS 1000 TR/87 supported services and events noted in this document, all operations performed on the set 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 Microsoft® Live Communications Server 2005 interworking and those components necessary to support the next generation SIP Contact Center requirements.

Figure 125 "Message sequence diagram - CSTA Session Establishment and Monitor Start" (page 216) shows the expected message flow for establishing and monitoring a CSTA session as defined by TR/87.

Figure 125
Message sequence diagram - CSTA Session Establishment and Monitor Start

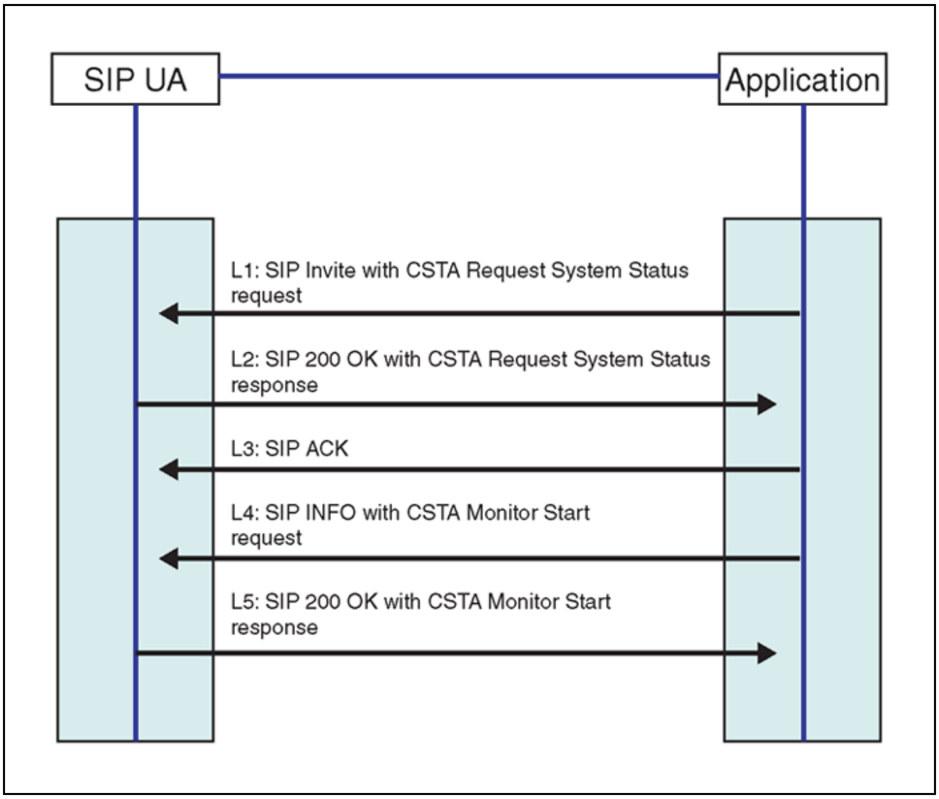
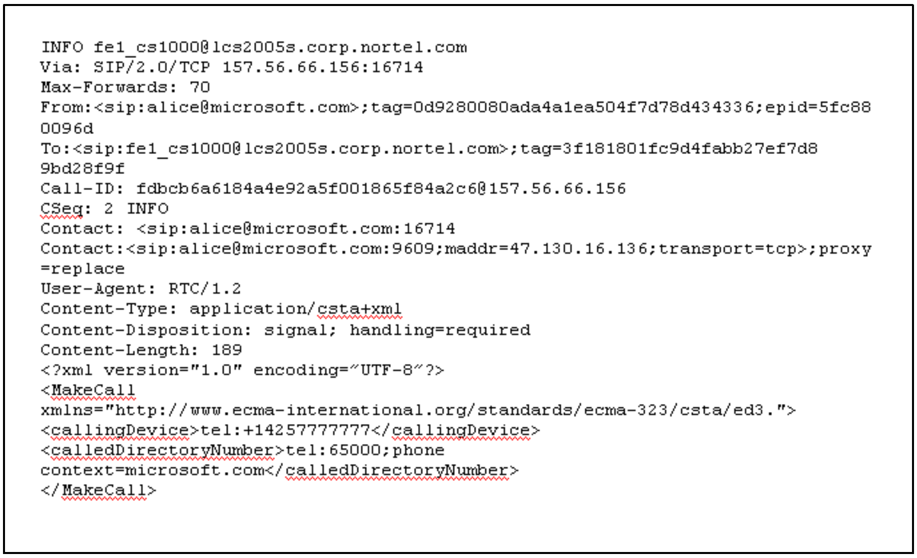

SIP UA
Application
L1: SIP Invite with CSTA Request System Status request
L2: SIP 200 OK with CSTA Request System Status response
L3: SIP ACK
L4: SIP INFO with CSTA Monitor Start request
L5: SIP 200 OK with CSTA Monitor Start response

Figure 126 "SIP INFO message with ECMA-323 content" (page 217) is an example of a SIP INFO message with ECMA-323 content.

Figure 126
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>
```

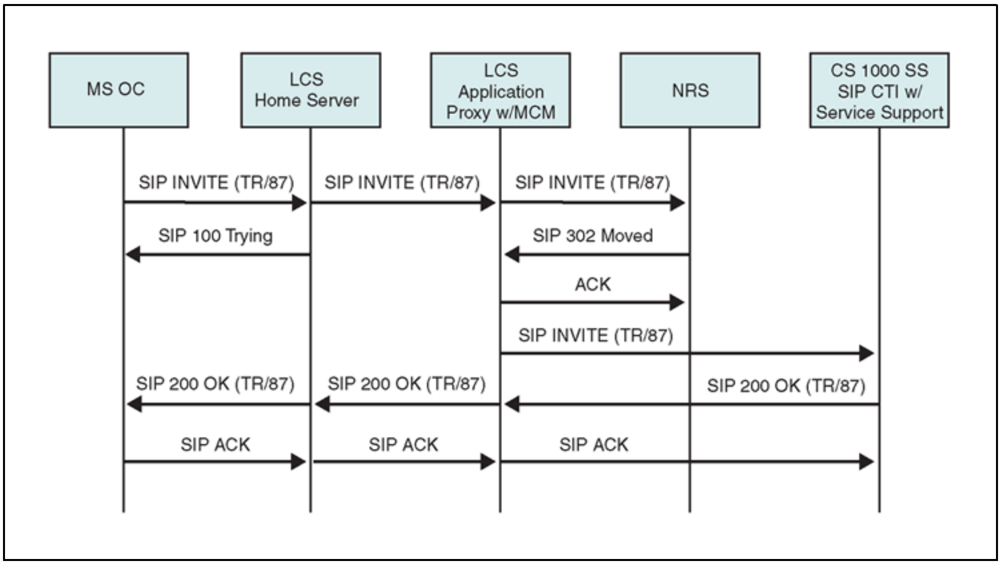
Call flow

This section illustrates the call flow sequence for both Remote Call Control and Telephony Gateway and Services.

Remote Call Control Call Flow

Figure 127 "Remote Call Control Session Establishment through NRS" (page 217) illustrates the Remote Call Control Session Establishment through SRS.

Figure 127
Remote Call Control Session Establishment through SRS



Telephony Gateway and Services Call Flow

Microsoft® Office Communicator Incoming Call Flow

Incoming calls to Office Communicator can originate directly from a phone behind CS1000 where the Request URI represents the destination.

Incoming calls can also come from a PCA, where the Request URI is a service DN used to route the call to the Live Communications Server, 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.

Personal Call Assistant (PCA) configuration provides additional Office Communicator features such as forwarding to voice mail, and so on. Configuration of PCA is performed through station administration tools. Refer to the CS 1000 Release 4.5 NTP for a complete description of operation and configuration.

Figure 128
Microsoft® Office Communicator Outgoing Call Flow

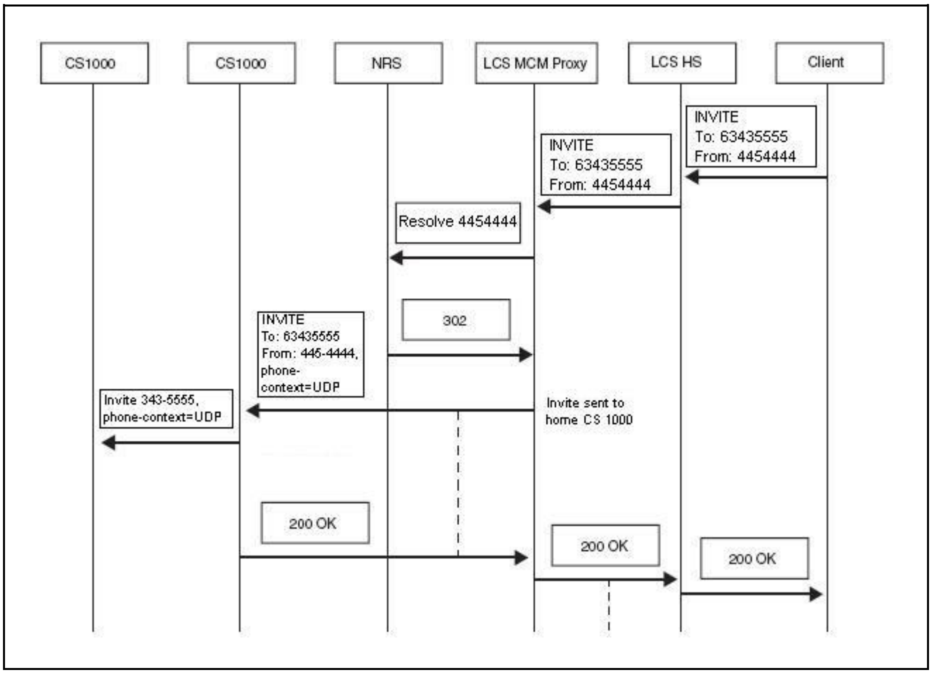


Figure 129
Microsoft Office Communicator Outgoing Call Flow with SPS

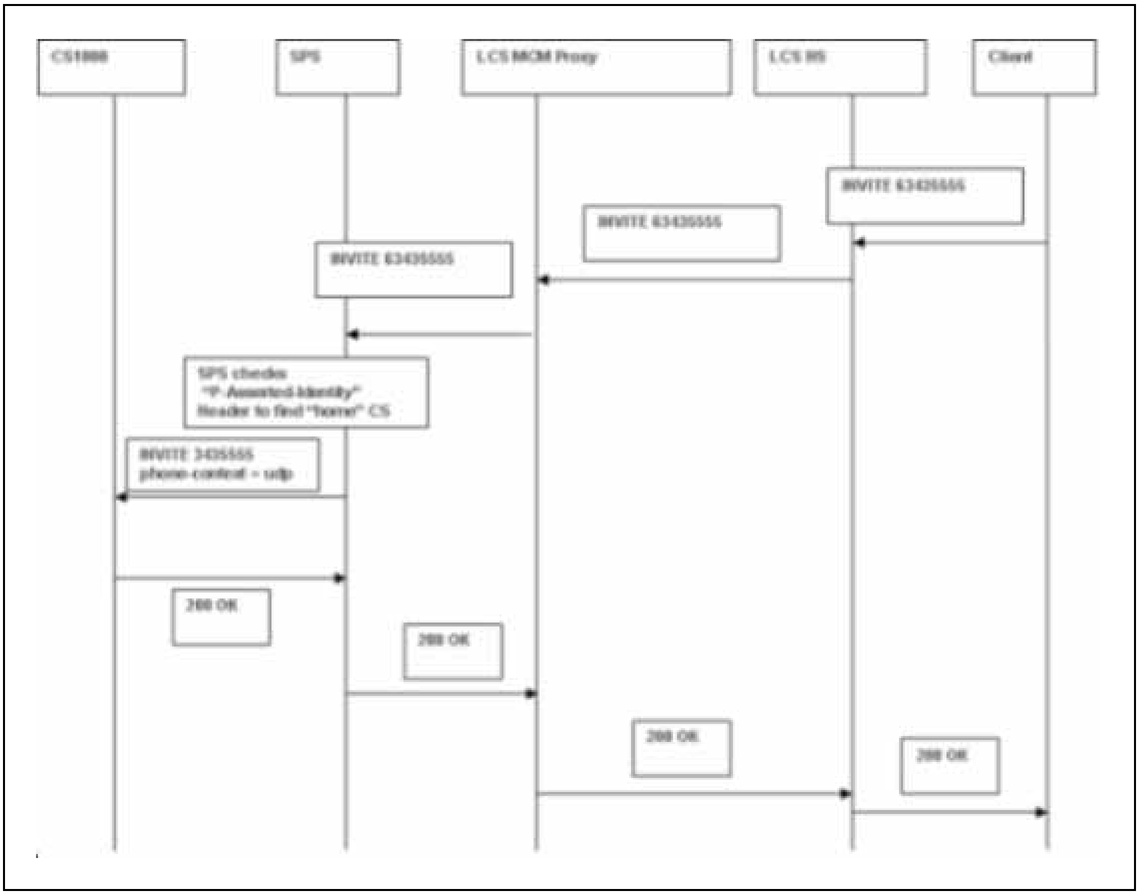
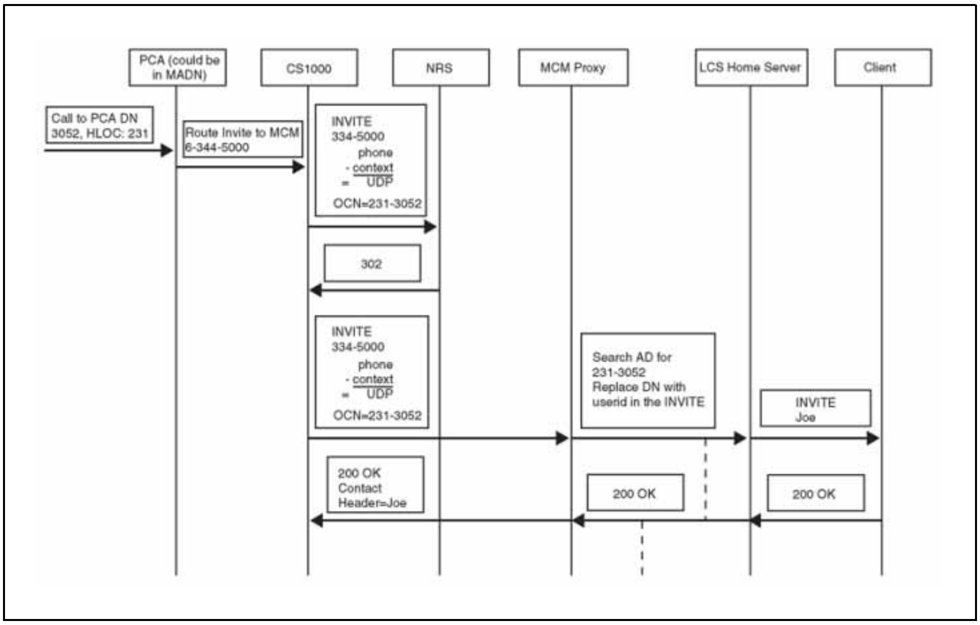


Figure 130
Microsoft® Office Communicator Incoming Call Flow using PCA



Supported features

Table 9
SIP CTI supported features

Feature	Supported by CS 1000 TR/87 FE	Supported by Microsoft® Office Communicator 2005
Call Control Events		
17.2.3 - Conferenced	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		

Feature	Supported by CS 1000 TR/87 FE	Supported by Microsoft® Office Communicator 2005
18.1.4 - Generate Digits	**X**	**X**
Call Associated Events		
18.2.5 - Service Completion Failure	**X**	**X**
Logical Device Features		
22.1.9 - Get Do Not Disturb	**X (Release 5.0)**	**X**
22.1.10 - Get Forwarding	**X**	**X**
22.1.17 - Set Do Not Disturb		**X**
22.1.18 - Set Forwarding	**X**	**X**
Logical Device Feature Event		
22.2.12 - Do Not Disturb	**X (Release 5.0)**	**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**	**X**

Feature	Supported by CS 1000 TR/87 FE	Supported by Microsoft® Office Communicator 2005
17.1.10 - Consultation Call	**X**	**X**
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 B Abbreviations

ACD
Automatic Call Distribution

AML
Applications Module Link

ATS
Activity Tracking System

AUX
Auxiliary

BRSC
Basic Rate Signaling Concentrator

CAST
Customer Assurance and Serviceability Test

CCMS
Contact Center Manager Server

CCR
Customer Controlled Routing

CDR
Call Detail Recording

CSTA
Computer Supported Telecommunications Applications

DRAM
Dynamic Random Access Memory

DN

Directory Number

DNIS

Dialed Number Identification Services

EMS

Enterprise Multimedia Systems

EPROM

Erasable Programmable Read-Only Memory

FS

Feature Specification

GNTS

Global Network Technical Support

MISP

Multipurpose ISDN Signaling Processor

MNM

Meridian Network Management

MSDL

Multi-purpose Serial Data Link

NCR

Number of Call Registers

NTP

Northern Telecom Publications

P

Pentium

PRD

Product Requirements Document

SA

StrongARM

SISP

Small System ISDN Signaling Processor

TN

Terminal Number

VGMC

Voice Gateway Media Card

XPEC

Expanded Peripheral Equipment Controller Pack

Appendix C Glossary

TR/87 Front End/ECMA Front End

The front end application (FE) is the application that resides on the Signaling Server to provide TR/87 session support. The FE interfaces with the SIP GW to manage TR/87 sessions. The FE also issues and receives AML messages from the CS to service the TR/87 sessions.

Nortel Communication Server 1000

Nortel Converged Office Fundamentals

Publication: NN43001-525
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

To provide feedback or report a problem in the document, go to www.nortel.com/documentfeedback

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, the Nortel Logo, the Globemark, SL-1, Meridian1, and Succession are trademarks of Nortel Networks. All other trademarks are the property of their respective owners.