Setup and Configuration Guide for Cisco Unified Intelligent Contact Management Hosted Release 9.0(1)

First Published: June 15, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Preface

Purpose

This manual describes how to set up, run, and administer the Cisco Unified Intelligent Contact Management Hosted (Unified ICMH) product. It supplements the installation and configuration instructions in the general Cisco Unified Intelligent Contact Management (Unified ICM) software documentation set with Unified ICMH-specific instructions for installing, configuring, and upgrading software components.

Caution You must have a copy of the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available in addition to this manual in order to successfully complete Unified ICMH installation and configuration. Many of the details required for installation are found only in the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

Audience

This document is intended for managers and administrators working in a network service provider environment. Readers of this manual must already have a general understanding of the Unified ICMH product, as discussed in the *Product Description Guide for Cisco Unified ICM Hosted*. Readers must be familiar with general Unified ICM installation and setup procedures.

Organization

The manual is divided into the following chapters.

Chapter	Description
Overview, on page 7	Provides an overview of Unified ICMH architecture.
NAM installation and configuration, on page 17	Provides instructions for installing and configuring software on the NAM machine.
CICM installation and configuration, on page 29	Describes how to add and configure instances on Customer ICM (CICM) machines.
Customer Concept, on page 41	Discusses the Unified ICMH Customer Concept data sorting option and provides instructions for configuring it on NAM and CICM systems.
Advanced Services, on page 53	Describes how to setup and administer an Advanced Services instance.
Administrative Tools, on page 61	Describes how to run Unified ICMH administrative tools.
Security considerations, on page 63	Discusses some Unified ICMH security concerns and how to address them.
Special considerations, on page 69	Describes Unified ICM features of special interest to Unified ICMH users.
Network VRU, on page 83	Describes the concepts, architecture, configuration and operations of Network Voice Response Units (VRUs) in an Unified ICMH environment
Administration and Data Server features, on page 103	Summarizes the Network Administration & Data Server features that are not installed on a Limited (single instance) Administration & Data Server, and features that are not to be provided to Standard Administration& Data Servers with Feature Control.

Related documentation

Documentation for Cisco Unified ICM/Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at: http://www.cisco.com/cisco/web/psa/default.html.

Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management

Portal, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools. The following list provides more information.

-
- For documentation for these Cisco Unified Contact Center products mentioned above, go to http://www.cisco.com/cisco/web/psa/default.html, click **Voice and Unified Communications**, then click **Customer Collaboration**, then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product or option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center products mentioned above, go to http://docwiki.cisco.com/wiki/Category:Troubleshooting, then click the product or option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: http://www.cisco.com/cisco/web/psa/default.html.
- Technical Support documentation and tools are accessible from: http://www.cisco.com/en/US/support/index.html.
- The Product Alert tool is accessible from (login required): http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.
- For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC* available at (login required): http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.
- For a detailed list of language localizations, refer to the *Cisco Unified ICM/Contact Center Product and System Localization Matrix* available at the bottom of the following page: http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html.

Product naming conventions

In this release, the product names listed in the table below have changed. The New Name (long version) is reserved for the first instance of that product name and in all headings. The New Name (short version) is used for subsequent instances of the product name.

Note This document uses the naming conventions provided in each GUI, which means that in some cases the old product name is in use.

Old Product Name	New Name (long version)	New Name (short version)
Cisco IPCC Enterprise Edition	Cisco Unified Contact Center Enterprise	Unified CCE
Cisco System IPCC Enterprise Edition	Cisco Unified System Contact Center Enterprise	Unified SCCE
Cisco IPCC Hosted Edition	Cisco Unified Contact Center Hosted	Unified CCH

Old Product Name	New Name (long version)	New Name (short version)
Cisco Intelligent Contact Management (ICM) Enterprise Edition	Cisco Unified Intelligent Contact Management Enterprise	Unified ICME
Cisco Intelligent Contact Management (ICM) Hosted Edition	Cisco Unified Intelligent Contact Management Hosted	Unified ICMH
Cisco CallManager/Cisco Unified CallManager	Cisco Unified Communications Manager	Unified CM

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term; for example: A *skill group* is a collection of agents who share similar skills. • For emphasis; for example: *Do not* use the numerical naming convention. • A syntax value that the user must replace; for example: IF (*condition, true-value, false-value*) • A book title; for example: Refer to the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays; for example: `<html><title>Cisco Systems,Inc. </title></html>` • Navigational text when selecting menu options; for example: `ICM Configuration Manager > Tools > Explorer Tools > Agent Explorer`

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Documentation and support

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

CHAPTER 2

Overview

This chapter provides an overview of the Cisco Unified Intelligent Contact Management Hosted (Unified ICMH) architecture. It discusses the following aspects of the Unified ICMH system:

- Its two-tiered architecture, in which an initial Unified ICM system processes service provider network route requests and forwards those requests to other Unified ICM systems for further processing.
- The major components that comprise the product.
- The support architecture, a facility that gathers system event and message information at a central point and that provides network service provider personnel with details of system activity and problems.

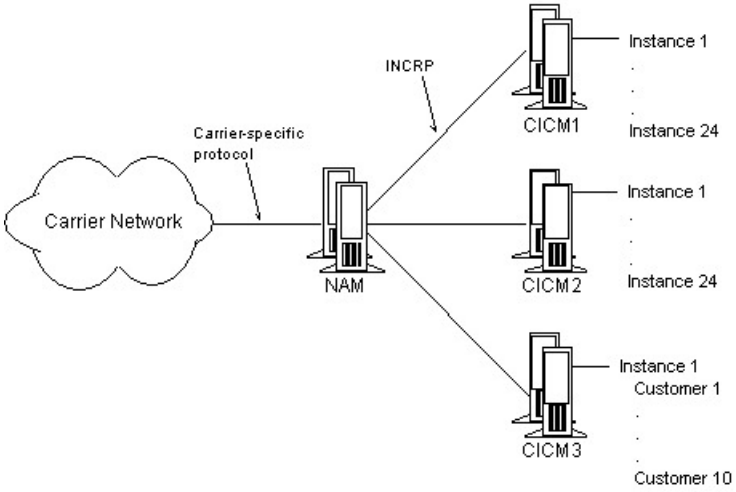
Two-tiered architecture

Unified ICMH is the carrier-class version of the Cisco Unified Intelligent Contact Management Enterprise software. It allows a network service provider to offer *virtual call center services* to its customers. Unified ICMH Network Applications Manager (NAM) can function like a Service Control Point (SCP) by distributing incoming calls to individual network service customers based on the number dialed, the call's point of origin, and caller-entered digits.

Unified ICMH uses a two-tiered architecture in which one Unified ICM passes route requests to a second Unified ICM. The first Unified ICM, called the *Network Applications Manager or NAM*, typically receives routing requests from a carrier network. The NAM can either return a label itself or pass the route request to

a second Unified ICM, called the *Customer ICM or CICM*. The NAM uses the proprietary INCRP protocol to pass a route request to a CICM.

Figure 1: Two-Tiered Architecture



Each CICM typically processes all calls for one specific ICM instance. Each ICM instance is typically used to support a single customer, although in some cases multiple customers can share an ICM instance (seeAdvanced Services ICM instance, on page 54). The CICM must have an INCRP Network Interface Controller (NIC) configured. The CICM receives the request, runs its own routing scripts to determine the destination for the call, and returns a routing label to the NAM. The NAM then returns the label to the original carrier network.

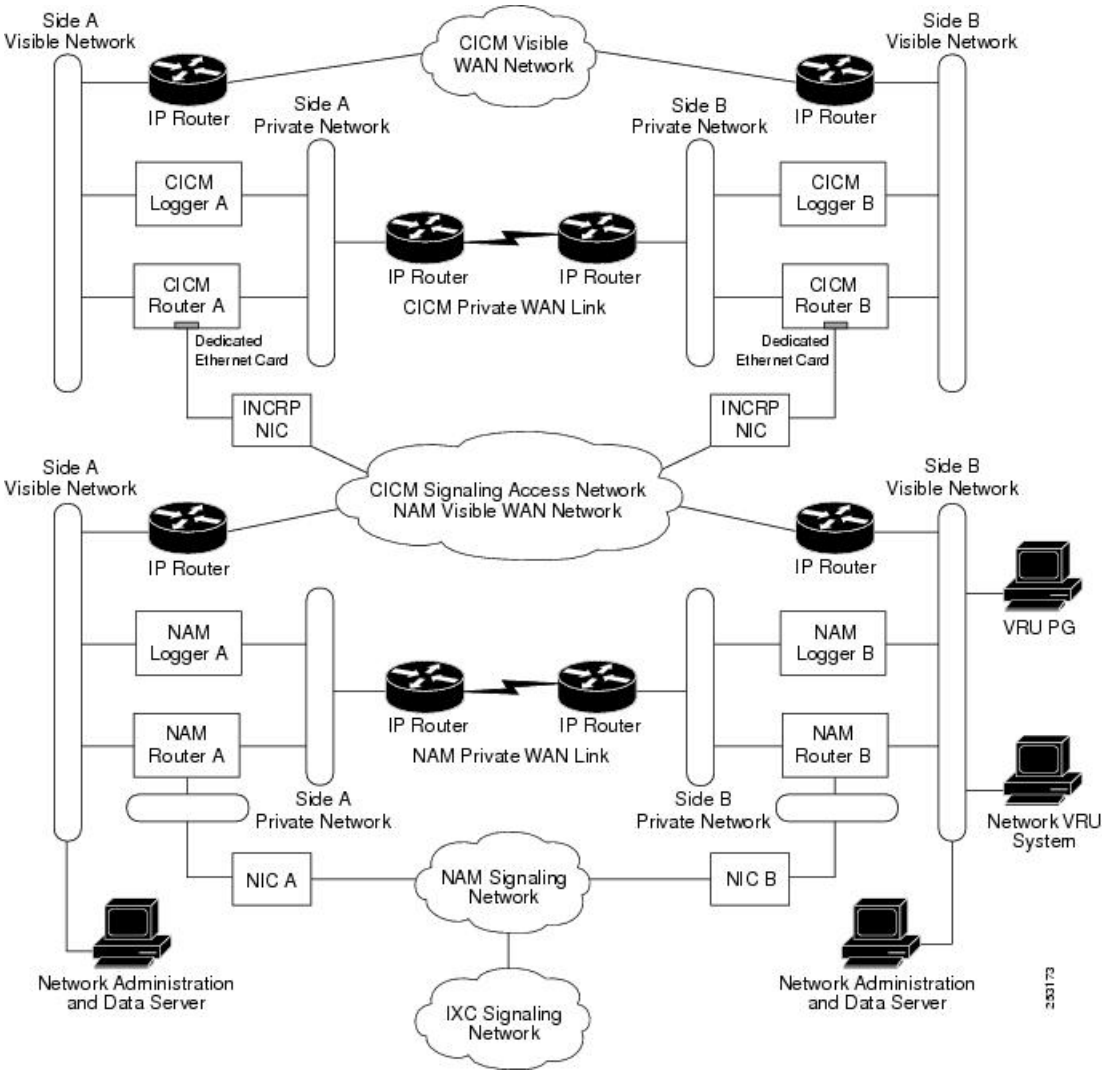
This architecture lets a service provider perform simple routing (within the NAM) for some customers while providing full Unified ICM functionality (in a CICM) for other customers.

Typically a single NAM can pass route requests to any of several CICMs, as shown in the figure above. Based on the information it has for the call (dialed number, caller-entered digits, and calling line ID), the NAM can run a routing script that chooses the appropriate CICM and sends it a route request.

Example network design

The following figure shows a sample design for a Network Applications Manager system.

Figure 2: Network Applications Manager Example Design



Note For clarity, the NIC processes are shown as though residing on standalone PCs in the figure above; however, the NICs are actually implemented as processes on the respective CallRouter machines.

In this example, the NAMs connect to the IXC signaling network via the NAM signaling access network and two separate Network Interface Controllers (NICs). Some Unified ICMH systems connect to the IXC signaling network via TCP/IP. For these systems, the NIC resides on the CallRouter. A dedicated network interface card in the CallRouter is used to connect the Unified ICM system to the signaling access network. The CICM signaling access network uses a dedicated network interface card in the CICM CallRouter machine.

Other types of dedicated communications cards may also be used in the CallRouter platform depending on the interexchange carrier.

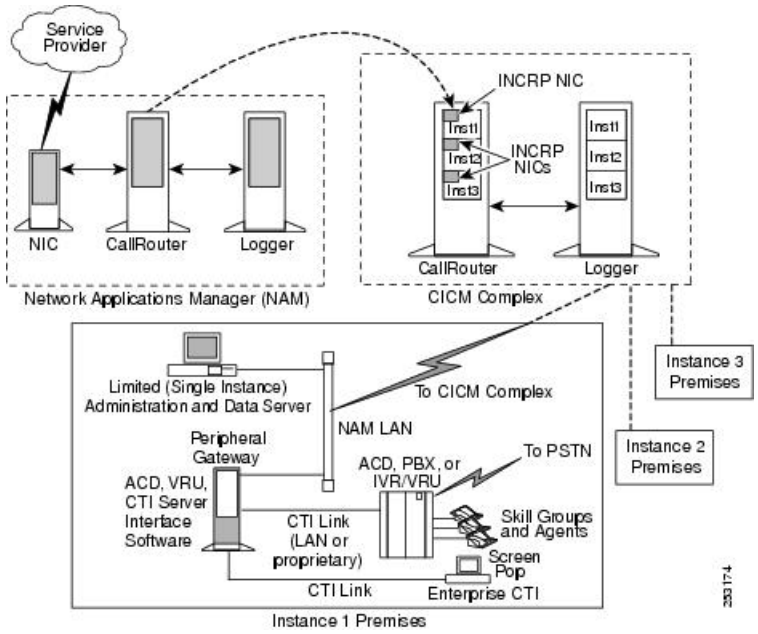
Note that in this configuration, the NAM visible WAN is shared by the CICM signaling access network. Data traffic for CICM signaling access network travels over the NAM visible WAN. The NAM visible WAN is an inter-site link that is independent of the private network.

Network VRU PGs and Network Administration & Data Servers connect to the NAM visible network. The VRU systems themselves reside on the NAM visible network. However, if this is not possible, the VRUs may be placed on a dedicated third LAN. This requires a third Ethernet card in the Network VRU PG machine.

Components

The following figure shows a typical Unified ICMH configuration and illustrates the components that reside on the network service provider site and the instance premises. (Note: For clarity, the NAM's NIC process is shown as though residing on a standalone PC in the figure below. However, the NAM's NIC is actually implemented as a process on the NAM's CallRouter machine.)

Figure 3: Cisco Unified Intelligent Contact Management Hosted Components



Network service provider site components

The NAM and CICM systems reside on the network service provider site.

The NAM is a Unified ICM system that is configured to handle initial route requests from the service provider network. Each NAM consists of a CallRouter and a Logger (simplexed or duplexed). The CallRouter and Logger may be on the same physical computer or on separate computers.

Each CICM consists of one or more CallRouter and Logger combinations (each of which is simplexed or duplexed). The CallRouter and Logger may be on the same computer or on two separate computers.

Furthermore, a single CICM computer may run multiple instances of each component, each of which can support one or more customers. That is, a single CICM may be running several instances of Unified ICM.

As shown in the figure above, several CICMs can share the same hardware platform. The shared hardware platform is called a CICM complex. A single NAM can distribute calls among multiple CICMs on multiple CICM complexes.

ICM instances

An instance is a single logical ICM. An instance typically consists of several software components (CallRouter, Logger, Peripheral Gateways, Administration & Data Servers)—some of which might be duplexed—typically installed on several different computers. A single computer can run components of multiple instances; for example, a single computer can run up to 25 CICM Routers.

An ICM instance is used to support a single customer. All customer PGs and Administration & Data Servers are connected to a single ICM instance. To support multiple customers, you need to install multiple ICM instances, possibly on computers that are shared by multiple instances.

There is a special ICM instance that is used for Advanced Services. Advanced Services are routing services for customers who do not have an ACD connected to Unified ICM. Therefore, Advanced Services customers do not have PGs connected. They also do not have dedicated Administration & Data Servers, but they do have web-based tools like WebView and Cisco Unified Intelligence Center (Unified IC) for reporting and Internet Script Editor to control their call routing.

The Advanced Services ICM is a multi-customer instance. A single Advanced Services ICM can support large numbers of customers.

An Advanced Services ICM is an ICM instance just like any other; it is just configured differently (see below). This means that a CICM complex can run a single Advanced Services ICM and a maximum of 24 “normal” customer ICMs. So one of the ICM instances on the CICM complex in the figure displayed in Components, on page 10 could be an Advanced Services ICM. However, for performance reasons it is desirable to run an Advanced Services ICM on dedicated hardware.

To support multiple customers on the same Advanced Services ICM, there is the concept of a customer. A customer is an organization that uses Unified ICM to manage its call center. Each customer has its own configuration elements, such as dialed numbers, labels, call types, Unified ICM scripts, IVR scripts, and scheduled targets. All these configuration elements are stored in the same Advanced Services ICM database, but the reporting and scripting tools will make sure that a specific customer only has access to their own data. Since Advanced Services customers *do not* have ACD and Peripheral Gateways, there are no configuration elements like peripherals, services, skill groups, and so forth.

Note No special security is applied at the customer level. Any Administration & Data Server user with access to the Advanced Services ICM instance can choose to view data for any or all customers in that instance. So the Service Provider can use the Administration & Data Server to administer the Advanced Services ICM as any other ICM instance. Advanced Services customers have access only to their own data using WebView, Unified IC, and Internet Script Editor. These tools will prevent a customer from accessing other customers' data.

Peripheral Gateways

Peripheral Gateways are typically located on instance sites and are associated with a CICM rather than the NAM. The NAM usually contains no trunk groups, skill targets, routes, or peripheral targets. Those entities are typically configured only on the CICMs; a CICM has a normal Unified ICM configuration for each instance.

Note If the NAM is duplexed, it must have a single Peripheral Gateway associated with it. In a duplexed environment, a CallRouter does not route calls unless it has active connections to the majority of the Peripheral Gateways. (This prevents both sides of a duplexed CallRouter from operating simultaneously.) If no Peripheral Gateways are defined, neither side of the CallRouter becomes active.

For guidelines on defining a Peripheral Gateway for the NAM, see NAM installation and configuration, on page 17.

Administration and Data Servers

Administration & Data Servers reside both at the service provider site and the customer sites.

Both of the following types of Administration & Data Servers reside at the service provider site:

- **Network Administration & Data Server for Network Application Manager**. A network Administration & Data Server associated with the NAM system.
- **Network Administration & Data Server for Customer ICM**. A network Administration & Data Server associated with the CICM systems.

Both of these Network Administration & Data Servers can reside on the same machine.

A customer site contains one of the following types of Administration & Data Servers:

- **Limited (Single Instance) Administration & Data Server**. Accesses one instance's data from a CICM.
- **Standard**. A standard Administration & Data Server. Optionally, the service provider can use the Configuration Manager Feature Control facility to define the customer's available tools.

You must specify the type of Administration & Data Server you are installing in the Web Setup tool. (Refer to the Web Setup tool's online help for more information.)

For guidelines on installing a NAM Administration& Data Server, seeNAM installation and configuration, on page 17.

For guidelines on installing a CICM Administration & Data Server, seeCICM installation and configuration, on page 29.

Standard Administration and Data Server with Feature Control

The Standard Administration & Data Server is a standard Administration & Data Server in a Unified ICM environment. A network service provider can provide such an Administration & Data Server for one of its customers and then use the Configuration Manager Feature Control facility to determine which Unified ICM tools that customer can use.

Refer to *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted* and the Configuration Manager tool's online help for information about Feature Control. Also, see Standard Administration and Data Server with feature control, on page 105.

Limited (Single Instance) Administration and Data Server

The Limited (Single Instance) Administration & Data Server type is for use by the customer of a network service provider. A Limited (Single Instance) Administration & Data Server can access data only for its associated instance; it cannot access data from other instances in the same CICM complex or other CICM complexes.

For more information on data access in the NAM architecture, see Chapter 7, Security considerations, on page 63.

The program group for a Limited (Single Instance) Administration & Data Server is a subset of the Network Administration & Data Server program group. The following tools are not available on a Limited (Single Instance) Administration & Data Server:

- Select Administration Instance
- Check Routes
- Router Log Viewer
- Schema Help

For a list of other features not installed on Limited (Single Instance) Administration & Data Servers, see Appendix A,Administration and Data Server features, on page 103.

Network Administration and Data Server for Network Application Manager

The Network Administration & Data Server for Network Application Manager types are for use by network service provider personnel. A Network Administration & Data Server has multiple Administration & Data Servers: one for the NAM instance, and one for each associated CICM instance.

The installation process installs the Unified CCE Tools folder on the desktop, and provides the **Cisco Unified CCE Tools** menu option on the Start menu (**Start** > **All Programs** > **Cisco Unified CCE Tools**).

Note The Administration Tools are only included in this folder if an Administration & Data Server is set up on the machine.

After you add an Administration & Data Server, the following happens:

- The Unified CCE Administration Tools folder displays on the desktop, along with the **Administration Tools** menu option on the Start menu (**Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools**).
- The **Administration Tools** icon displays in the Unified CCE Tools folder, which is a shortcut to the Administration Tools folder.

The following tools are available on Network Administration & Data Servers:

- **Select Administration Instance**. Allows you to switch between administration instances.

- **Call Tracer**. Lets you send test calls to the system software and see how they are processed and the target chosen.
- **Check Routes**. Lets you validate the configuration of routes referenced by a script.
- **CMS Control**. The Configuration Management Service (CMS) Control console is the control panel for CMS Node. CMS allows the Agent Re-skilling Web Tool and the CMS Node options access to the configuration.

Note This tool only displays if the Configuration Management Service (CMS) Node is enabled in the Administration & Data Server.

- **Configuration Manager**. Lets you set up and maintain your environment. The configuration includes the hardware within the system, the services provided by the system, and the agents who provide them.
- **Glossary**. Defines terms related to Unified ICMH.
- **Initialize Local Database**. Lets you copy current information from the NAM or CICM central database to the local database (awdb) on the Administration & Data Server. (Normally, this is done automatically.)
- **Lock Admin**. Lets you check or change the status of locks in a NAM or CICM central database. Only the holder of the Configuration lock can update configuration data; only the holder of a script lock can update a script.
- **Peripheral Gateway Setup** (PG Setup). A Unified ICM/CCE/CCH tool with which administrators and system administrators can set up Peripheral Gateways (PGs) and their associated Peripheral Interface Managers (PIMs), CTI Server, Outbound Option Dialer, and CompuCALL Server Gateway.
- **Router Log Viewer**. Displays information about calls processed by the system software and any errors encountered in processing them.
- **Scheduled Target Manager**. Lets you configure and manage scheduled targets, which indicate a special type of destination for a call.
- **Schema Help**. Describes the structure of the Unified ICM databases.
- **Script Editor**. Lets you create, modify, and schedule routing scripts. The system software executes these scripts to determine where to route each call.
- **Service Control**. Lets you stop and start Unified ICMH-related services.
- **SSL Encryption Utility**. Enables changing the default SSL settings (implemented by the Cisco Unified ICM/Contact Center Enterprise & Hosted Installer) and further configure WebView and Unified IC to enable encryption for the entire session, as opposed to only user authentication. The SSL Encryption Utility contains the functionality to re-generate the self-signed certificate and replace the IIS installed certificate, as needed.
- **Web Setup**. A browser-based application with which Unified ICM/CCE/CCH administrators and system administrators can manage instances, add and modify Unified ICM/CCE/CCH components, and manage Unified ICM/CCE/CCH-related system services.

The following table lists the Unified ICM documentation that describes each tool.

Tools	Where to find more information
Select Administration Instance, Service Control	Chapter 6, Administrative Tools, on page 61.

Tools	Where to find more information
PG Setup and Web Setup	*Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*
CMS Control, Configuration Manager and its associated tools, Lock Admin	*Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted*
Call Tracer, Check Routes, Router Log Viewer, Script Editor	*Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*
Glossary, Scheduled Target Manager, Schema Help	Glossary, Scheduled Target Manager, Schema Help online help systems
SSL Encryption Utility	*Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)*

Real-Time Administration and Data Servers

You have two options when installing the system software:

- **Real-time Administration & Data Server**. This configuration includes the real-time Administration & Data Server and real-time client processes, and all processes that directly manage the local database. A single Administration & Data Server machine can run the Administration & Data Server processes for multiple instances simultaneously. However, it can run client applications (such as Script Editor and Configuration Manager) for only one instance at a time. (Use Select Administration Instance to change the instance.)
- **Administration Client (No Real-time Administration & Data Server)**. This configuration includes standard Administration & Data Server applications, such as Script Editor and Configuration Manager. It does not include the processes that directly manage a database.

The following table summarizes the difference between Real-time Administration & Data Server and Administration Client.

	Administration & Data Server	Administration Client
Types	Standard with Feature Control, NAM, CICM, or Limited	Standard with Feature Control, NAM, CICM, or Limited
Applications	Full complement, depending on type	Full complement, depending on type
Local Database	Yes	No
Windows Service	Administration & Data Server	N/A
Background Processes	logger, rtclient, rtdist, updateaw	N/A

	Administration & Data Server	Administration Client
Optional Processes	schman, replication	N/A

The CallRouter is responsible for providing real-time data to an Administration & Data Server at each admin site. Each site has at least one, and usually two, Administration & Data Servers that serve as real-time data Administration & Data Servers for the site. The primary Administration & Data Server maintains an active connection to the real-time server through which it receives real-time data.

Administration Clients at the site receive their real-time data through a connection to an Administration & Data Server. Administration Clients do not have the local database and Administration & Data Server processes required to receive real-time data directly from the Central Controller real-time server.

If the site has two Administration & Data Servers, Administration Clients are configured to automatically switch to a secondary Administration & Data Server if the first Administration & Data Server becomes non-functional for any reason. The secondary Administration & Data Server also maintains connections to the real-time server; however, these connections remain idle until needed.

You deploy an Administration & Data Server by installing the software using the Cisco Unified ICM/Contact Center Enterprise & Hosted Installer, and then set up the Administration & Data Server using the Web Setup tool.

You deploy an Administration Client by installing the software using the Administration Client Installer, and then set it up using the Administration Client Setup tool.

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for details about installing and setting up the Administration & Data Servers.

CHAPTER 3

NAM installation and configuration

This chapter discusses the procedures you need to perform to install and configure a NAM system. These instructions assume that Windows—including SNMP and SQL Server are already installed, and that Windows Active Directory services for the system software, including at least one ICM instance, have been set up.

Note You must have a copy of the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available in addition to this manual in order to successfully complete NAM installation and configuration.

The NAM installation and configuration process involves the following tasks:

- Installing Logger software and creating a central database.
- Installing CallRouter software and enabling Remote Network Routing.
- Installing a Network Administration & Data Server for Network Application Manager.
- Defining NAM configuration data.
- Configuring Network Interface Controllers.
- Installing and configuring a Peripheral Gateway for the NAM.
- Creating a Unified ICM Application Gateway to access CICM instances.

Note If you are installing and configuring NAM systems that will be part of a Multiple-NAM configuration, refer to the installation and configuration instructions in the *Multiple-NAM Setup and Configuration Guide for Cisco Unified ICM Hosted*.

• NAM upgrade, page 28

Install NAM Logger software

The Logger is the process that manages the central database. A Logger process runs on each NAM and CICM in the Unified ICMH system.

Procedure

Step 1 Create the central database on the Logger machine using the ICMDBA utility.

Step 2 Open the Web Setup tool.

Step 3 Select **Component Management** > **Loggers** in the left frame, then click **Add** in the right frame. The Add Logger Deployments page appears.

Step 4 On this page, be sure to select **Hosted** > **Network Application Manager (NAM)** for Logger Type.

Step 5 Provide values for the other fields on this page, then click **Next**.

Step 6 Provide values for the applicable fields on the Central Controller Connectivity and Additional Options page. Clicking **Next** from the Additional Options page takes you to a NAM page.

Step 7 On the NAM page, select one of the following values for NAM Type:

a) **Provisioning/Standalone NAM**: NAM Logger is either a Standalone NAM or a NAM that provides Slave NAMs with configuration information

b) **Slave NAM**: NAM Logger that obtains configuration information from a Provisioning NAM

Note This option is only used in a *Multiple-NAM* setup.

Step 8 Provide the following values in the NAM Configuration section:

a) **Provisioning/Standalone Router Side A**: Enter the Side A machine name or IP address of the provisioning Router

b) **Provisioning/Standalone Router Side B**: If a Side B machine exists, enter the Side B machine name or IP address of the provisioning Router

Step 9 If you specified a NAM Type of Provisioning/Standalone NAM, skip the Slave NAM Configuration section. If you specified a NAM Type of Slave NAM, specify the following information:

a) **Provisioning NAM Instance Name**: The instance name of the Provisioning NAM

b) **Provisioning NAM Instance Number**: The instance number of the Provisioning NAM

c) **Provisioning Logger Side A**: The Side A machine name or IP address of the Provisioning Logger

d) **Provisioning Logger Side B**: If present, the Side B machine name or IP address of the Provisioning Logger

e) **Slave Router Side A**: The Side A machine name or IP address of the Slave Router

f) **Slave Router Side B**: If present, the Side B machine name or IP address of the Slave Router

Step 10 Click **Next**.

Step 11 Complete the rest of the Logger setup.

Multiple installations

In cases where you want to install more than one Unified ICM component on a single computer (for example, to install the CallRouter and Logger software on a single node) you must run the Web Setup tool for each component. Similarly, to install a specific component for more than one customer, you must run the Web Setup tool for each instance.

NAM CallRouter software installation

The CallRouter process contains the call routing logic of the system. The CallRouter runs on each NAM and CICM in the Unified ICMH system.

During NAM CallRouter installation you set up the following:

- **Enable Remote Network Routing**. This option sets up the NAM to send routing requests to the CICM systems.
- **NAM ID**. This value is passed with messages sent to a CICM so that the CICM can identify which NAM in the configuration sent the message.

Install CallRouter software on NAM

Procedure

Step 1 Open the Web Setup tool.

Step 2 Select **Component Management** > **Routers** in the left frame, then click **Add** in the right frame.

Step 3 In the first Add Router window, be sure to check the **Enable Remote Network Routing** box.

Step 4 In the NAM ID field, do the following:

a) If your NAM configuration contains only a single NAM, accept the default value of **0**.

b) If your NAM configuration contains multiple NAMs that might communicate with a single CICM, specify a unique nonzero value. (The same NAM ID is used for Side A and Side B of a given NAM. However, the NAM ID must be different for different instances in a multiple NAM environment.)

Step 5 Click **Next**.

Step 6 Complete the rest of the CallRouter setup.

Network Administration and Data Server

The Administration & Data Server provides the user interface to the NAM and Unified ICM software.

Install Network Administration and Data Server software for NAM

Procedure

Step 1 Open the Web Setup tool.

Step 2 Select **Component Management** > **Administration & Data Servers** in the left frame, then click **Add** in the right frame.

Step 3 In the first Add Administration & Data Server page, select **Hosted** for the Deployment Type, and also select **Network Administration & Data Server for Customer ICM (CICM)**.

Step 4 Supply values for the other fields in this window, then click **Next**.

Step 5 Complete the rest of the Administration & Data Server setup.

NAM configuration data

At this point, you can start the NAM Logger, CallRouter, and Administration & Data Server, and set up the NAM configuration data.

In a two-tier architecture, the NAM system requires only a subset of the normal Unified ICM configuration data. The following table summarizes the configuration data for a NAM.

Table	Contents
Announcement	Any announcements used in NAM scripts.
Application Gateway	A remote ICM gateway for each instance on each associated CICM.
Business Entity	The default business entity only.
Call Type	Typically, one for each instance.
Call Type Map	Associate each NAM call type with a NAM script.
Dialed Number	All dialed numbers used on associated CICMs, plus those used for direct translation. (No default routes are defined for NAM dialed numbers.)
Dialed Number Map	Associates dialed numbers and calling line IDs with NAM call types.
Label	All labels that can be returned by associated CICMs, plus those used for direct translation.
Network Interface Controller	One required for the Network Interface Controller to the carrier network.

Table	Contents
Peripheral Gateway (PG)	One or more for the Peripheral Gateway to the carrier network.
Prefix	Any prefixes used in NAM regions.
Region	Any regions used in NAM dialed number map.
Routing Client	One or more for the carrier network.
Script	One or more for each call type.

NAM Replication Process on NAM

A process called the NAM Replication Process (NRP) runs on the NAM Logger system. The NRP monitors configuration changes made on the NAM for items such as the dialed number and label for a customer. Whenever you add a dialed number or label on the NAM, the NRP determines which CICM is affected. The NRP then forwards and automatically applies the change to the appropriate CICM.

Note Because the NRP cannot apply updates to records, modifications to dialed number and label strings are disallowed.

Database records do not necessarily share the same ID values between NAM and CICM. For example, when you add a dialed number for a customer into the NAM, the record created in the CICM has the same values for DialedNumberString and EnterpriseName, but not necessarily the same value for DialedNumberID. The Dialed_Number.LabelID on the CICM is set to point to a label that is equivalent to the label on the NAM, although the ID values might not be the same.

In order for the NRP to function properly, you must do the following:

- Configure all associated CICMs as ICM instances and customers on the NAM, so that the NRP can forward changes to the appropriate CICM databases. (For instructions, see Configure CICM instances on NAM, on page 21.
- Configure the Administration & Data Servers for each CICM and the customers to allow the NRP to locate the CICM databases to be updated. (For instructions, see Administration and Data Server configuration on NAM, on page 23.
- Define each customer associated with each CICM instance.
- Associate the routing client on a CICM with a routing client on the NAM, so that customer data on the NAM and CICM can match up. (For instructions, see Associate CICM routing client with NAM routing client, on page 24.

Configure CICM instances on NAM

You must perform the following steps to configure an instance for each associated CICM.

Note CICM instance names and numbers are defined on the CICMs. For information, see the CICM Installation and Configuration chapter.

Procedure

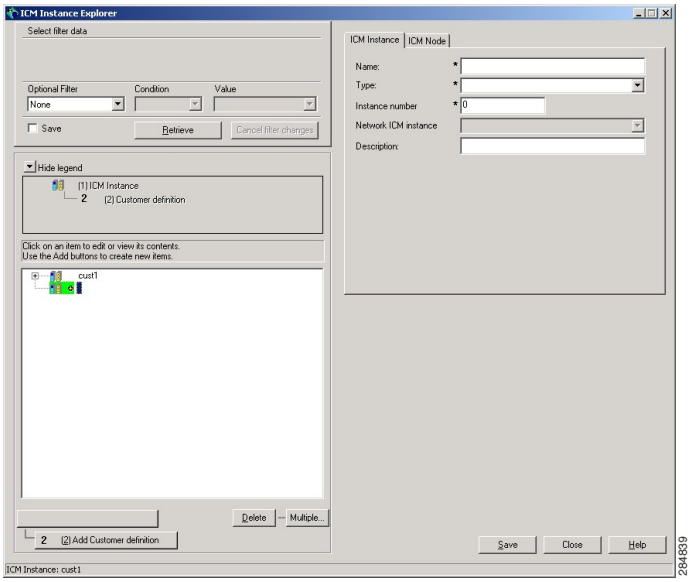
Step 1 On the NAM, start the **Configuration Manager** from the Administration Tools folder. The Configuration Manager window opens.

Step 2 Open the Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 3 Click **Retrieve**.

Step 4 Click **Add ICM Instance**.

Figure 4: ICM Instance Dialog



Step 5 Specify the following on the ICM Instance tab:

- **Name**. The enterprise name for the CICM instance, as used in the Web Setup tool.
- **Type** (drop-down list). Select **Customer ICM**.
- **Instance Number**. The instance number as defined in the Web Setup tool.

  Note For information about defining a name and number for a CICM instance, see the CICM Installation and Configuration chapter.
- **Network ICM Instance** (drop-down list). The associated NAM instance.
- **Description** (optional). Additional information about the ICM Instance.

Step 6 Click **Save**.

Administration and Data Server configuration on NAM

You must perform the following steps to configure the primary and secondary Administration & Data Servers associated with the CICM instances you just defined.

Configure Administration and Data Servers associated with ICM instance

Procedure

Step 1 On the NAM, start **Configuration Manager** from the Administration Tools folder. The Configuration Manager window opens.

Step 2 Open the Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 3 Click **Retrieve**.

Step 4 Click **Add ICM Instance**. (this button does not display)

Step 5 Specify the following on the ICM Node tab:

a) **ICM Instance** (drop-down list). The name for the instance that contains the node.
b) **System Domain**. The name of the Windows security domain that contains the NAM machine.
c) **System Name**. The name of the computer that runs both instances.
d) **Node Type** (drop-down list). The node type: Primary Administration & Data Server or Backup Administration & Data Server.
e) **Name**. The enterprise name for the node. (The default enterprise name is formed by combining the ICM instance, system name, and node type.)
f) **Configuration Parameter** (optional). A string of configuration parameters to be passed to the node at initialization.
g) **Description** (optional). Additional information about the node.

Step 6 Click **Apply** and **Done**.

CICM customer definition

You must perform the following steps to define each customer associated with each CICM instance.

Define a customer

You must perform the following steps to define a customer:

Procedure

Step 1 On the NAM, in **Configuration Manager**, choose **Enterprise** > **Customer** > **Customer List**. The Customer Definition List window appears.

Step 2 Click the **Add** button.

Step 3 Specify the following in the Attributes tab:

- **Name**. The enterprise name for the customer.
- **ICM Instance** (drop-down list). The name of the instance associated with the customer.
- **Network VRU** (drop-down list). The name of the network VRU (if any) associated with the customer.
- **Description** (optional). Additional information about the customer.

Step 4 Click **Save**.

Associate CICM routing client with NAM routing client

Procedure

Step 1 *On the NAM*, double-click the **NIC Explorer** tool. The NIC Explorer window appears.

Step 2 In the Select filter data box, click **Retrieve**. The NIC tree window appears.

Step 3 Select a NIC. The Explorer tab fields appear.

Step 4 Click the **Routing client** tab.

Step 5 Set the **Network routing client** field on the NAM to the same value to appear on the CICM. (For example, you can set it to the enterprise name of the NAM routing client.)

Step 6 Click **Done** to apply the changes and close the dialog box.

NAM NIC and PG installation and configuration

This section provides guidelines for configuring network interface controllers (NICs) and peripheral gateways (PGs) for the NAM.

Network Interface Controllers

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*, and the System Manager Guide Supplement for your particular NICs for guidelines and procedures.

Peripheral Gateways

To support duplexed operation, the NAM must also communicate with at least one Peripheral Gateway device. (In a duplexed environment, a CallRouter does not route calls when the duplexed partner has nodal or network failure unless it has active connections to a majority of the PGs and it cannot see the other CallRouter. This prevents both CallRouters from trying to route simultaneously.) Therefore, you must define at least one Peripheral Gateway for the NAM. You can run the Peripheral Gateway on one of the Administration & Data Server machines associated with the NAM. The Peripheral Interface Manager (PIM) on the PG need not be enabled.

Device Management Protocols for NAM PGs

Follow the steps described in the Peripheral Gateway Setup online help to set up a Peripheral Gateway. This includes instructions for the Device Management Protocol Properties dialog.

Cisco Unified Intelligent Contact Management Application Gateway access to CICM instances

After adding the instance components to the CICM, you must configure a Unified ICM Application Gateway in Configuration Manager on an Administration & Data Server associated with the NAM. (The Unified ICM Application Gateway is the path a NAM takes to access a CICM.)

After the Unified ICM Application Gateway is configured, you can reference it using a Unified ICM Application Gateway node within a routing script on the NAM.

Create Cisco Unified Intelligent Contact Management Application Gateway

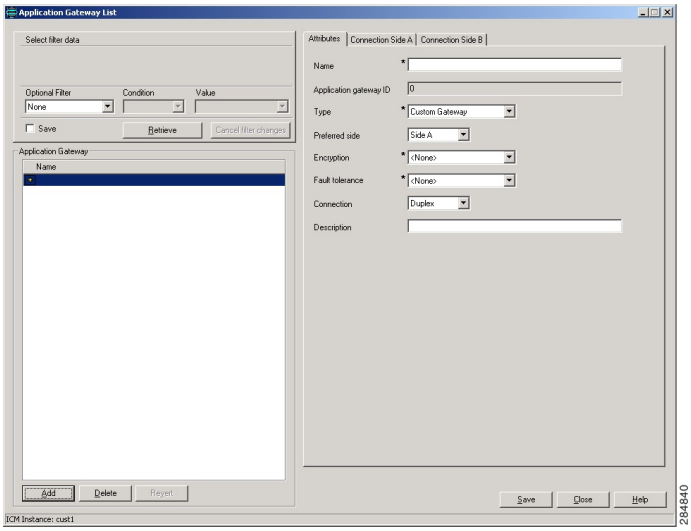
Procedure

Step 1 Within Configuration Manager on an Administration & Data Server associated with the NAM, select **Calls** > **Application Gateway** > **Application Gateway List**. The Application Gateway List window appears.

Step 2 Click **Retrieve**.

Step 3 Click **Add**. The Attributes tab appears.

Figure 5: Application Gateway List Window



Step 4 Specify the following values on the Attributes tab:

- **Name**. Enter a name for the Unified ICM Application Gateway.
- **Type**. Select **Remote ICM**.
- **Preferred Side**. Indicates the preferred side of the Unified ICM Application Gateway to use when both are available. If only one side is available, the system software uses that side regardless of preference. This option applies only for Custom Gateways. For Remote ICM systems, the preference is indicated by a suffix on the connection address.
- **Encryption**. Indicates whether requests to the Unified ICM Application Gateway are encrypted. Select **None.**
- **Fault Tolerance**. If the Unified ICM Application Gateway is duplexed, specifies the fault-tolerance strategy it uses.
- **Connection**. Select whether the Unified ICM Application Gateway is Duplex (has both a Side A and Side B connection), Simplex A (only has a Side A), or Simplex B (only has a Side B).
- **Description** (optional). Additional information about the Unified ICM Application Gateway.

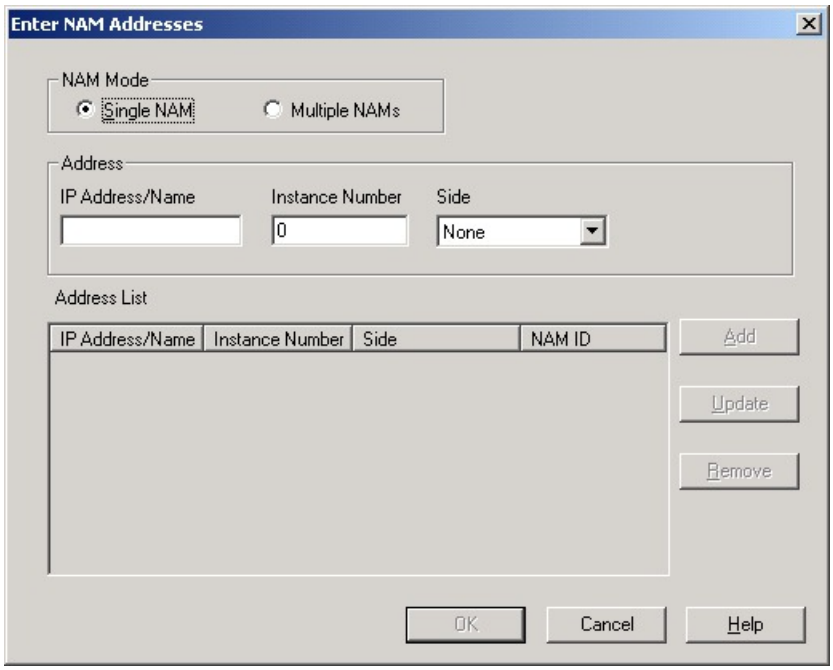
Step 5 Click **Save** to create the Unified ICM Application Gateway.

Note Make a note of the Unified ICM Application Gateway ID value, as you will need it when you run the Web Setup tool to configure the INCRP NIC on the CICM.

Step 6 To set the connection information, click the **Connection Side A** tab or the **Connection Side B** tab.

Step 7 To specify an address, click the **Enter Address** button. The Enter NAM Addresses dialog box appears.

Figure 6: Enter NAM Addresses Dialog



Step 8 Specify the following information:

- **NAM Mode**. Select **Single NAM** or **Multiple NAMs**, depending on the number of NAMs connected to the selected Unified ICM Application Gateway.
- **IP Address/Name**. Enter the Public (high priority) IP address of the CICM. Alternatively, the SAN can be used (consult your Cisco certified partner or TAC for assistance). This address *must* be the same address specified for the INCRP NIC on the CICM. (You can use the hostname in place of the address.)
- **Instance Number**. Enter the number of the customer ICM on the CICM (0 through 24).
- **Side**. Indicate which side of the NAM prefers this connection:
  - **Side A**. NAM Side A prefers to use this connection.
  - **Side B**. NAM Side B prefers to use this connection.
  - **None**. Neither side of the NAM prefers to use this connection.
  - **Both Side A and B**. Both sides of the NAM prefer to use this connection.

Note Consider network traffic in choosing this value. For example, if one side of the NAM is collocated with only one side of the CICM, you can make that the preferred connection in order to avoid unnecessary WAN traffic to the other side.

- **NAM ID**. This field appears only if you select a NAM Mode of Multiple NAM. Enter the NAM ID.

Step 9 Set the **In Service** field to indicate whether this connection is currently available for use by the system software.

Step 10 When finished, click **Save**.

The bottom half of the connection tab displays a number of timeout and limit values. The defaults for these values as shipped may not be appropriate for a NAM system; these values are highly configuration-dependent. A rough guideline is that the CICMs timeout value be less than the timeout value for the NAMs NIC.

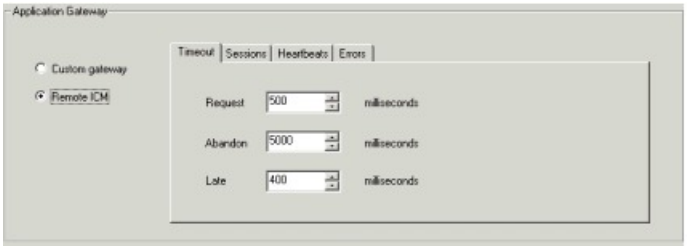
Set default values for Cisco Unified Intelligent Contact Management Application Gateway

Procedure

Step 1 Within Configuration Manager, select **Enterprise** > **System Information** > **System Information**. The System Information dialog box appears.

Step 2 In the Application Gateway section, select the **Remote ICM** radio button.

Figure 7: System Information Dialog



Step 3 Use the Timeouts, Sessions, Heartbeats, and Error tabs to set the default values for the Unified ICM Application Gateway connections. (The Unified ICM Application Gateway timeout settings for a CICM must be set keeping in mind the NAM NIC settings for timeout, late, and so on.)

Step 4 When finished, click **OK** to make the changes and close the dialog box.

NAM upgrade

For instructions on how to upgrade a NAM system, refer to the *Upgrade Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

CHAPTER 4

CICM installation and configuration

This chapter discusses the procedures you need to perform to:

- Define CICM instance names and numbers.
- Add instances on a CICM complex.
- Install and configure CICM Loggers.
- Install and configure CICM CallRouters.
- Install and configure CICM Administration & Data Servers (service provider Administration & Data Server on NAM, customer Administration & Data Servers on CICM).
- Configure the CICM INCRP NIC.
- Add or update components for a CICM instance.
- Delete instances on a CICM complex.

Note You must have a copy of the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available in addition to this manual in order to successfully complete CICM configuration.

Note If you are installing and configuring CICM systems that will be part of a Multiple-NAM configuration, also refer to the installation and configuration instructions in the *Multiple-NAM Setup and Configuration Guide for Cisco Unified ICM Hosted*.

- CICM INCRP NIC, page 35
- Quality of Service (QoS), page 39
- Add or Upgrade components for instances, page 39

Instances

In a NAM environment, each duplexed CICM system serves up to 25 instances. Each instance is associated with one duplexed CICM system.

As mentioned earlier, a CICM complex is a single hardware platform on which multiple CICM instances may reside. Each instance, in turn, can be shared by several customers with limited functionality. As new instances are added to the system, you must install additional Unified ICM components (Loggers, CallRouters, and Administration & Data Servers) on the CICM machines.

Adding a new instance to a CICM complex consists of several tasks.

- Deciding on the instance name
- Selecting the CICM complex to service the instance
- Assigning an instance number
- Setting up the CICM Loggers
- Setting up the CICM CallRouters
- Setting up the CICM instance Administration & Data Server on the NAM
- Configuring the INCRP NIC

The following subsections explain these steps. After completing these steps you can proceed to set up Peripheral Gateways and Administration & Data Servers at the customer premises.

Instance naming conventions

Select a unique instance name of up to five characters. The first character of the name must be a letter (a–z or A–Z). Subsequent characters can be letters, digits, or the symbols # or $. The name must not contain spaces.

You cannot use case to differentiate instances. For example, you cannot name two instances cus01 and Cus01. When forming database names, the system software converts the instance name to all lowercase.

The instance name is used in naming a registry subtree, a subdirectory of the \icm directory, and as a prefix on database names. For an instance named cust1, the CICM databases are named cust1_sideA and cust1_sideB. The local database on an Administration & Data Server is named cust1_awdb.

CICM complex

Select which CICM complex will service this instance. Consider the current load on each CICM complex and the expected load for the new instance. Usually it is best to roughly balance the overall load among available CICM complexes. If all CICM complexes are nearing capacity, consider adding a new CICM complex.

Instance number

Each instance within a CICM complex must have a unique instance number. The same number must be used to identify the instance on each machine in the CICM complex.

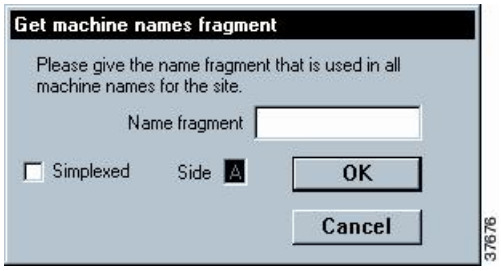
View instance numbers currently in use

Procedure

Step 1 On any Administration & Data Server in the CICM complex, select **Start** > **Run**. The Run dialog box appears.

Step 2 Type **instanceno.exe** in the Open field and click **OK**. (This executable is installed in the \icm\bin directory on every Administration & Data Server.) The Name Fragment dialog box appears.

Figure 8: Name Fragment Dialog

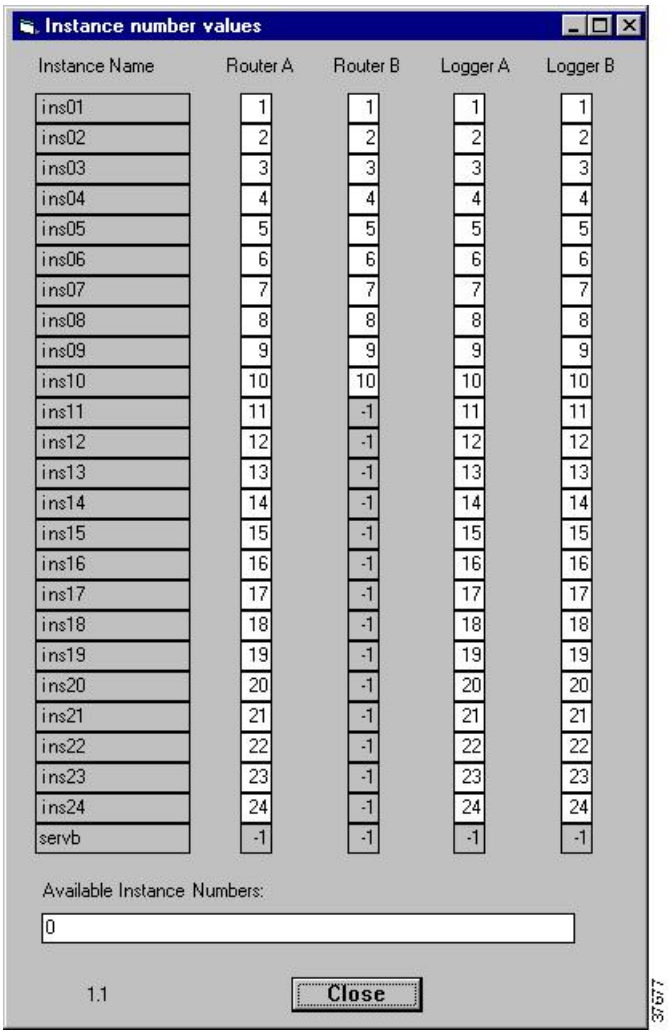


Step 3 Specify the machine name fragment that is used in all machines on your site. (For example, if Logger A is named CSOXYZLGRA, enter XYZ.)

Step 4 If the system is simplexed, check the Simplexed option and choose side A or B.

Step 5 Click **OK**. The system checks each CallRouter and Logger to find which instance numbers are in use. It then displays a screen similar to the following:

Figure 9: Instance Number Values Dialog



A value of –1 indicates that the instance is not defined on that machine. The field at the bottom of the window specifies which instance numbers are available for use.

Step 6 Take note of the available numbers so you can use one of them for the new instance. You must use this same number when adding the instance to each machine.

Step 7 Click **Close**

Add instance to CICM

Procedure

Step 1 On a CICM, open the Web Setup tool.

Step 2 Click **Instance Management** in the left frame, then click **Add** in the right frame. An Add Instance page appears.

Step 3 From the drop-down lists, select a facility and an instance.

Step 4 Enter the instance number you chose previously.

Step 5 Click **Save** to add the instance.

CICM Loggers

You must perform the following steps to install and configure a Logger in a CICM domain.

Note If a Logger is duplexed, perform these steps on each side. Be careful to use the same instance name and instance number on both sides.

Install and configure CICM Logger (Side A or Side B)

Procedure

Step 1 Create the central database on the Logger machine using the ICMDBA utility.

Step 2 Open the Web Setup tool.

Step 3 Select **Component Management** > **Loggers** in the left frame, then click **Add** in the right frame. The Add Logger Deployments page appears.

Step 4 On this page, be sure to select **Hosted** > **Customer ICM (CICM)** for Logger Type.

Step 5 Provide values for the other fields on this page. Click **Next**.

Step 6 Provide values for the applicable fields on the Central Controller Connectivity and Additional Options page. Clicking **Next** from the Additional Options page takes you to a NAM page.

Step 7 On the NAM page, select one of the following values for NAM Type:

a) **Provisioning/Standalone NAM**: NAM Logger is either a Standalone NAM or a NAM that provides Slave NAMs with configuration information

b) **Slave NAM**: NAM Logger that obtains configuration information from a Provisioning NAM

Step 8 Provide the following values in the NAM Configuration section:

a) **Provisioning/Standalone Router Side A**: Enter the Side A machine name or IP address of the provisioning Router

b) **Provisioning/Standalone Router Side B**: If a Side B machine exists, enter the Side B machine name or IP address of the provisioning Router

Step 9 If you specified a NAM Type of Provisioning/Standalone NAM, skip the Slave NAM Configuration section. If you specified a NAM Type of Slave NAM, specify the following information:

a) **Provisioning NAM Instance Name**: The instance name of the Provisioning NAM
b) **Provisioning NAM Instance Number**: The instance number of the Provisioning NAM
c) **Provisioning Logger Side A**: The Side A machine name or IP address of the Provisioning Logger
d) **Provisioning Logger Side B**: If present, the Side B machine name or IP address of the Provisioning Logger
e) **Slave Router Side A**: The Side A machine name or IP address of the Slave Router
f) **Slave Router Side B**: If present, the Side B machine name or IP address of the Slave Router

Step 10 Click **Next**.

Step 11 Complete the rest of the Logger setup.

CICM CallRouters

You must perform the following steps to install and configure a CallRouter in a CICM domain.

Note You must set up the instance on the Logger machines before the CallRouter machines.

Note If a CallRouter is duplexed, perform these steps on each side. Be careful to use the same instance name and instance number on both sides.

Install CICM CallRouter software

Procedure

Step 1 Open the Web Setup tool.

Step 2 Select **Component Management** > **Routers** in the left frame, then click **Add** in the right frame.

Step 3 Click **Next**.

Step 4 Complete the CallRouter setup.

Note If a CallRouter is duplexed, perform these steps on each side. Be careful to use the same instance name and instance number on both sides.

CICM Network Administration and Data Server installation

To create configuration data for an instance, you must add the instance to a CICM Network Administration & Data Server.

Install CICM Network Administration and Data Server

Procedure

Step 1 Open the Web Setup tool.

Step 2 Select **Component Management** > **Administration & Data Servers** in the left frame, then click **Add** in the right frame.

Step 3 In the first Add Administration & Data Server page, select **Hosted** for the Deployment Type, and also select **Network Administration & Data Server for Customer ICM (CICM)**.

Step 4 Supply values for the other fields in this window, then click **Next**.

Step 5 Complete the rest of the Administration & Data Server setup.

CICM INCRP NIC

The NAM communicates with the CICM by means of an INCRP NIC. To set up the INCRP NIC for each instance on the CICM, you must perform the following tasks:

- Define INCRP NIC, on page 35
- Complete INCRP NIC setup, on page 38

Define INCRP NIC

Note The preferred network for this connection is the Public/Visible or SAN network. When using the SAN network, it must have a WAN link between Side A and B (SAN was originally intended for the CallRouter to Network Gateway connection, which does not cross the A/B boundary).

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window displays.

Step 2 Select the instance you will be configuring.

Step 3 From the Configuration Manager, open the NIC Explorer tool by selecting **Tools** > **Explorer Tools** > **NIC Explorer**. The NIC Explorer window displays.

Step 4 In the Select filter data box, click **Retrieve**. This enables the **Add NIC** button.

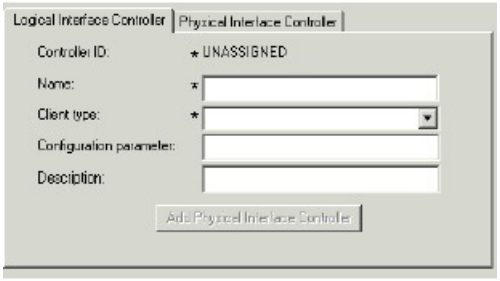
Step 5 Click **Add NIC**. A new NIC and its routing client display in the tree window. Next to each is a **To Be Inserted** icon.
On the right of the tree window, tabbed fields also display for the new NIC's and routing client's configuration information.

Step 6 Enter the following in the Logical Interface Controller tab fields:

- **Name**. An enterprise name that will serve as the NIC name. The name can be up to 32 characters. The valid characters are upper-case and lower-case letters, digits, periods (.) and underlines (_). The first character of the name must be a letter or digit.
- **Client Type** (drop-down list). The type of routing client serviced by the NIC. Select **INCRP**.

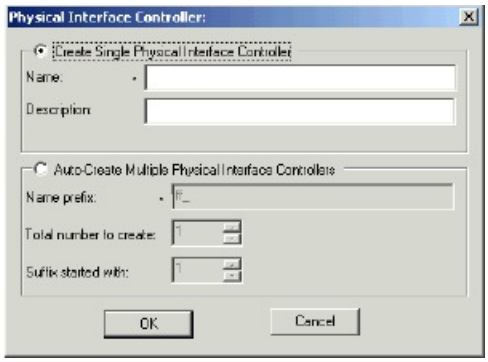
  Note Selecting a type of routing client automatically places that type's default values in the Routing Client's Timeout Threshold, Late Threshold, Timeout Limit, Use DN/Label Map, and Client Type fields.

Figure 10: Logical Interface Controller Tab



Step 7 Click the **Add Physical Interface Controller** button. The Physical Interface Controller dialog displays.

Figure 11: Physical Interface Controller Dialog



Step 8 In the Create Single Physical Interface Controller section, specify an **Enterprise Name** and, optionally, a **Description**.

Step 9 Click **OK**. The Physical Interface Controller tab displays, displaying the information you specified, and an ID value of UNASSIGNED.

Step 10 Click the **Add Routing Client** button, and enter the following on the Routing Client tab fields:

- **Name**. An enterprise name that will serve as the NIC Routing Client name. The name can be up to 32 characters. The valid characters are upper-case and lower-case letters, digits, periods (.) and underlines (_). The first character of the name must be a letter or digit.
- **Client Type** (drop-down list). The type of routing client that ultimately routes the call on the requesting NAM.

  Note This field is enabled only for the routing client associated with an INCRP NIC.

If your NAM has multiple routing clients, ensure that each client is defined and that the ClientType field in the Routing Client record matches the client type of the NAM's NIC. In addition, the Configuration Parameter field for each record must contain the parameter:

```
/CustomerID <RCID>
```

where <*RCID*> is the Routing Client ID of the matching routing client on the NAM, as defined in the SQL table.

Note For instructions on how to update a record in the Configuration Manager, refer to the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted*.

Step 11 If desired, define security settings on the records.

Step 12 Click **Save**. The newly defined NIC is saved in the database, a Physical Controller ID is assigned, and the **To Be Inserted** icon is removed from the tree window.

Note Make a note of the Physical Controller ID value. You need this value to set up the INCRP NIC on the CallRouter. If the NIC is duplexed, you need both Physical Controller ID values.

Step 13 Click **Close** to exit the NIC Explorer tool.

Complete INCRP NIC setup

To provide detailed set-up information for the NIC, do the following:

Procedure

Step 1 Open the Web Setup tool.

Step 2 Select **Component Management** > **Routers** > **Network Interface Controllers** in the left frame, then click **Add** in the right frame. The Add Network Interface Controllers Deployments page displays.

Step 3 Select a value for the Instance.

Step 4 On the Network Interface Controller pull-down menu, select **INCRP**.

Step 5 Click **Next**. The Properties page displays.

Step 6 Specify the following values:

a) **Physical Interface Controller ID**: Enter one of the physical controller IDs (from the Configuration Manager) for the INCRP NIC on the CICM. If the NIC is duplexed, be sure to enter a different physical controller ID on each side.

b) **Local Hostname or IP Address**: Enter the IP Name (IP Address or hostname) of the local address for incoming NAM connections. (Note that this address/host must be on the same network as the NAM Addresses.)

c) **Handshake Timeout (ms)**: Enter the milliseconds to wait for a handshake response from the routing client (the supplied default of 5000 milliseconds is usually appropriate).

Step 7 Click **Next**. The Client ICM/CCE/CCH page displays.

Step 8 Enter the following information:

a) **Enabled**: Check the box to enable the Client ICM.

b) **Description**: Enter a description of the Client ICM.

c) **Client ID**: Enter the ID of the Client ICM machine. In this case, that is the same as the NAM ID.

d) **AppGateway ID**: Specify the ApplicationGatewayID for the INCRP NIC as configured in the Client ICM database.

e) **SCP Side A IP Address/Hostname**: Enter the Public Network (or SAN) addresses/hostnames of the NAM on Side A.

f) **SCP Side B IP Address/Hostname**: Enter the Public Network (or SAN) addresses/hostnames of the NAM on Side B.

Step 9 Click **Next**, then click **Finish** to complete INCRP NIC installation.

Note You need not set up DMP devices for the INCRP NIC, because it is a process on the CallRouter rather than a separate device.

Multiple NAM/CICM routing clients

For multiple NAM/CICM routing client configurations that will use CICM Replication, you must associate a routing client on the CICM for each routing client on the NAM for that customer. You cannot use the same name for two different routing clients on the CICM or NAM.

For example:

- A NAM system has two routing clients with enterprise names XYZ_NIC_1 and INAP_NIC_1. The XYZ_NIC_1 routing client has a network routing client of XYZ_NIC, and the INAP_NIC_1 routing client has a network routing client of INAP_NIC.
- The associated CICM system has two routing clients with enterprise names INCRP_NIC_1 and INCRP_NIC_2.
- For these routing clients on the CICM, you must define network routing clients of XYZ_NIC and INAP_NIC, respectively.

Note Because routes are not normally defined on the NAM, a default route for a dialed number cannot be set on the NAM. However, labels are defined on both the NAM and the CICM. Therefore, dialed numbers have default labels rather than default routes.

Quality of Service (QoS)

If you wish to use the optional Unified ICM Quality of Service feature, the appropriate steps are provided in the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*, with discussion of QoS to be found in the *Pre-installation Planning Guide for Cisco Unified ICM Enterprise and Hosted*. However, note the following if you are using the Microsoft Packet Scheduler.

As all ICM instances of a CICM share, by design, public and private network interfaces, and the Microsoft Packet Scheduler is mapped to an address / interface, it follows that ICM instances hosted in a common physical CICM complex must be uniformly configured when deploying QoS.

Note The configuration settings of the last customer configured via the Web Setup tool will be those in effect.

Add or Upgrade components for instances

To add or upgrade components for instances, do one of the following:

- To add a new component for an instance, run the Web Setup tool. From the initial Web Setup page, click **Component Management** in the left column. Under Component Management, click the type of component you want to add; a List page for the component appears. Click **Add** on this List page to start the Add wizard for the component.

- To upgrade all installed components for all instances, rerun the main installation program (setup.exe) from the Release 8.0(1) ICM/CCE/CCH DVD. Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for instructions.

Remove an instance

The following steps describe the process for removing an instance.

Procedure

Step 1 Use the Service Control utility to stop the services for that instance on all CICM machines and Administration & Data Servers.

Step 2 Run the Web Setup tool.

Step 3 Click **Instance Management** in the left column. An Instance List page appears.

Step 4 Check the check box to the left of the instances you want to remove.

Step 5 Click **Remove** to remove the instances.

CHAPTER 5

Customer Concept

This chapter discusses the Unified ICMH Customer Concept data sorting option and provides instructions for configuring it on NAM and CICM systems.

Customer Concept overview

Customer Concept is a data sorting option whereby an ICM Instance is divided into multiple Customers for the sake of uniquely associating certain data objects with a particular Organization within an Instance.

An *instance* is a single logical ICM. An instance typically consists of several software components (CallRouter, Logger, Peripheral Gateways, Administration & Data Servers)—some of which might be duplexed—typically installed on several different computers. A single computer might run multiple components of a single instance or components of multiple instances.

A customer is an organization that uses Unified ICM to manage its call center enterprise. Each customer has its own dialed numbers, labels, call types, scripts, and scheduled targets. A customer can also be assigned its own network VRU with customer-specific scripts for special call treatment. However, all Peripheral Gateways, peripherals, services, skill groups, and so forth are associated with the instance rather than a specific customer. Therefore, customers who share an instance cannot have uniquely associated Peripheral Gateways.

The following table summarizes what data can be associated with a specific customer and what data are shared by an entire instance.

Customer	Instance
Dialed numbers (DNs), labels, call types, scripts, scheduled targets, and network VRU scripts	NICs and PGs; peripherals, trunk groups, peripheral targets, skill targets; regions; announcements; Unified ICM Application Gateways

Note No special security is applied at the customer level. Any Administration & Data Server user with access to an instance can choose to view data for any or all customers in that instance. However, you can set up WebView, Unified IC, and Internet Script Editor users who have access to only the data for a specific customer. (These users do not have direct access to an Administration & Data Server. They work only through a web browser.)

You can use Customer Concept to support multiple independent organizations with a single ICM instance rather than assigning a separate instance to each organization. However, customers that share an instance have more limited capabilities than a customer using a full instance. The following table summarizes the abilities of these two customer types.

Full Instance Customer	Shared Instance Customer
Monitored targets (skill groups, agents, and services) and scheduled targets	Scheduled targets only
Full routing capabilities based on Longest Available Agent, Minimum Expected Delay	Percent allocation routing and scheduled targets routing only
Dedicated Peripheral Gateways	No dedicated Peripheral Gateways
Administration & Data Server, Internet Script Editor, WebView, and Unified IC access	Internet Script Editor, WebView, and Unified IC access only
Full configuration, scripting, and administration capabilities	Script modifications according to Feature Control Set via Internet Script Editor

Note that all configuration and scripting for a shared instance customer must be performed by the service provider that manages the instance. The customer themselves can only perform script modifications according to their assigned Feature Control Set via Internet Script Editor.

Business units as customers

Alternately, an organization with a full ICM instance can use Customer Concept to more conveniently manage a large enterprise. You can divide the organization into several logical customers and assign each a set of dialed numbers, call types, routing scripts, and so forth. In the Configuration Manager or the Script Editor, you can choose to see data for all customers or for only a specific customer. All customers share the same Peripheral Gateways, skill targets, and so forth.

Note Again, Customer Concept does not provide security between business units. It only provides a way of organizing certain data and the convenience of allowing you to selectively view those data.

Configure Customer Concept

Perform the following steps to configure Customer Concept.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

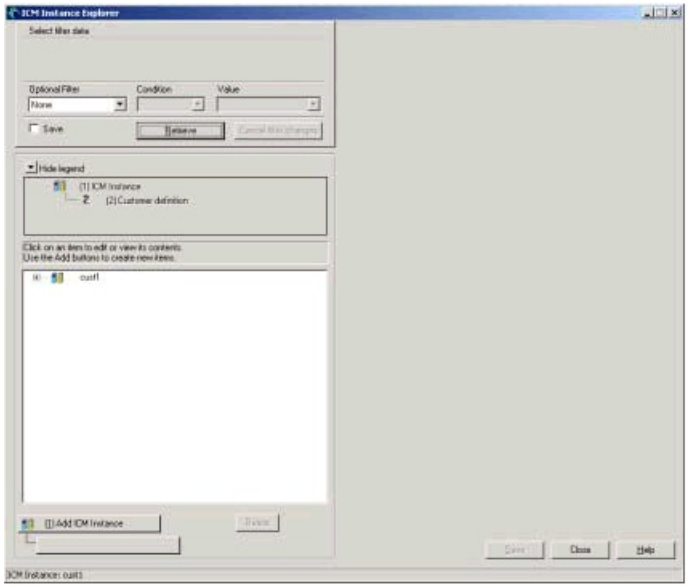
Step 2 Select the instance you will be configuring.

Step 3 From within the Administration Tools folder, double-click the **Configuration Manager**.

Step 4 Open the ICM Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 5 Click **Retrieve**.

Figure 12: ICM Instance Explorer Window



By default, the instance that you are configuring within will already appear, as will a default customer under that instance. The default customer will have the same name as the instance.

The ICM Instance Explorer is used to:

- Create customers within an instance.
- Create additional instances and their associated customers (for NAM to CICM DN and Label Replication and for Network VRU reporting).
- Associate a network Administration & Data Server (ICM Node) with an instance (for NAM to CICM DN and Label Replication).
- Assign a Network VRU to a customer.

- Assign a Feature Control Set to a customer.
- Set a flag to indicate that the customer is to be billed for VRU time.

Once the customer has been created via the Instance Explorer, the DNs, labels, call types, scheduled targets and network VRU scripts can be associated with a customer from within their individual configuration tools. Scripts can be associated with a customer from within the Script Explorer.

Implementation of Customer Concept is required in certain Hosted offerings such as:

- Advanced Services – at the CICM level – multiple customers reside within the Advanced Services CICM instance.
- Advanced Services – at the NAM level – multiple Network VRUs at the NAM level service multiple customers within an instance at the CICM level.
- NAM to CICM DN and Label Replication – at the NAM level – configured DNs and labels automatically replicated to the associated CICM level.
- Unified ICMH (and Cisco Unified Contact Center Hosted) – at the NAM level – multiple Network VRUs at the NAM level service multiple CICM instances.

Customer Concept on Advanced Services instances

This section lists guidelines for implementing Customer Concept on Advanced Services instances. See Chapter 5, Advanced Services, on page 53 for more information on Advanced Services instances.

CICM level

Implementation of Customer Concept is required for Advanced Services CICM Instances.

Implementation of Customer Concept is required in a standard CICM when multiple logical network VRUs are available at the NAM and a single CICM is using more than one network VRU. In that case, Customer Concept can be used to assign specific Network VRUs to each dialed number.

Implementation of Customer Concept is required in a standard CICM when NAM to CICM replication of Dialed Numbers and Labels is configured on the CICM (see NAM level, on page 44 for details).

NAM level

As just stated, implementation of Customer Concept is required in a standard CICM when NAM to CICM replication of Dialed Numbers and Labels is configured on the CICM (seeNAM to CICM DN and label replication, on page 45 for details). An additional benefit of implementing Customer Concept at the NAM level is that it allows detailed Network VRU usage reporting down to the customer level.

NAM to CICM DN and label replication

A process called CICM Replication runs automatically on the NAM Logger system. Once configured properly at the NAM level, dialed numbers and labels configured at the NAM level are automatically replicated at the CICM level.

CICM Replication does not write directly to the CICM instance database. It writes to a CICM Administration & Data Server on Network Administration & Data Server (CICM). This CICM Administration & Data Server may be on a separate Network Administration & Data Server machine or may co-reside with the NAM instance Network Administration & Data Server (NAM) and other CICM instance Network Administration & Data Servers. The CICM Administration & Data Server receives the change from the NAM logger and, in turn, writes the change to the CICM logger database.

The advantage of implementing NAM to CICM DN and Label Replication is an administrative one since DNs and labels only need to be added at the NAM level. However, the process depends on the availability of at least one Network Administration & Data Server at all times.

Because the NAM Replication Process (NRP) cannot apply updates to records, modifications to dialed number and label strings are disallowed.

Database records do not necessarily share the same ID values between NAM and CICM. For example, when you add a dialed number for a customer into the NAM, the record created in the CICM has the same values for DialedNumberString and EnterpriseName, but not necessarily the same value for DialedNumberID. The Dialed_Number.LabelID on the CICM is set to point to the equivalent label as on the NAM, although the ID values might not be the same.

In order for the replication process to function properly, you must do the following within the **NAM instance configuration**:

- Configure all associated CICMs as ICM instances on the NAM so that CICM Replication can forward changes to the appropriate CICM Administration & Data Server.
- Configure the associated CICM customer(s) within each CICM instance on the NAM. If Customer Concept is implemented at the CICM level (Advanced Services) each customer is added under the Advanced Services instance at the NAM level. If Customer Concept is not implemented at the CICM level, the default first customer (same name as CICM instance) is added under the CICM instance.
- Associate all DNs and labels configured at the NAM level with the appropriate CICM customer.
- Configure the Network Administration & Data Server(s) (ICM Node) for each CICM which will receive DN and labels from the NAM CICM Replication process.
- Associate the network routing client for each CICM routing client with its associated NAM routing client.

Configure CICM replication at NAM level

Perform the following steps to configure CICM Replication at the NAM level.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

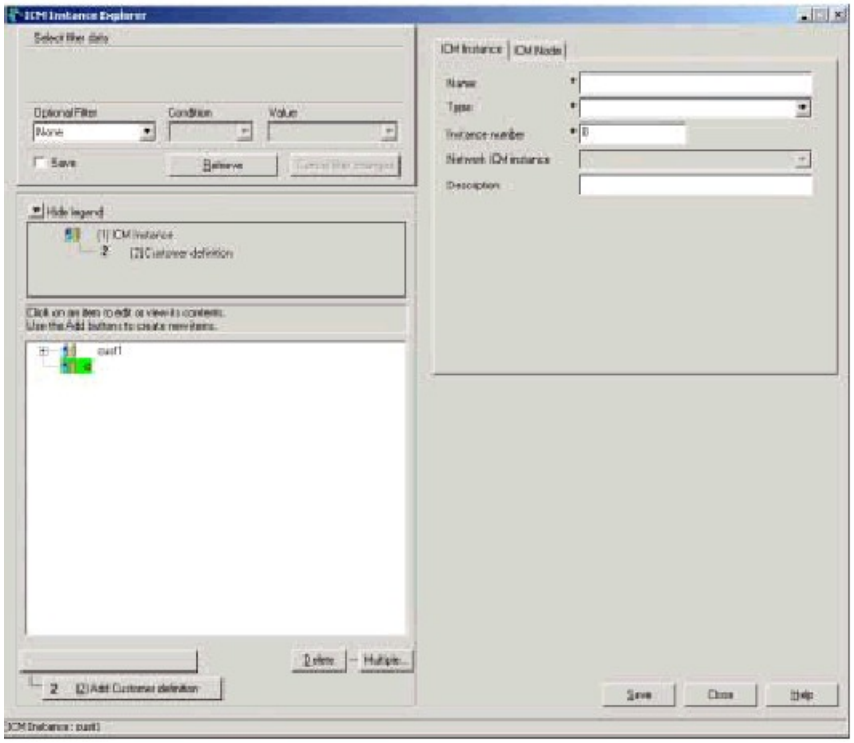
Step 2 Select the NAM instance you will be configuring.

Step 3 From within the Administration Tools folder, double-click the **Configuration Manager**.

Step 4 Open the ICM Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 5 Click **Retrieve**.

Figure 13: ICM Instance List Window



By default, the NAM instance that you are configuring within will already appear, as will a default customer under that instance. The default customer will have the same name as the NAM instance.

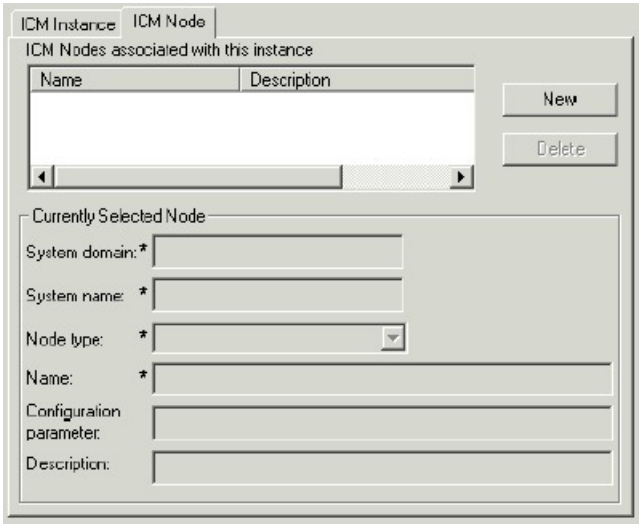
Step 6 Click **Add ICM Instance**.

Step 7 Under ICM Instance tab:

- Enter CICM instance name.
- For Type, select **Customer ICM** from the pull-down menu.
- Enter CICM instance number.
- For Network ICM Instance, select the name of the NAM instance.

Step 8 Under ICM Node tab:

Figure 14: ICM Node Tab

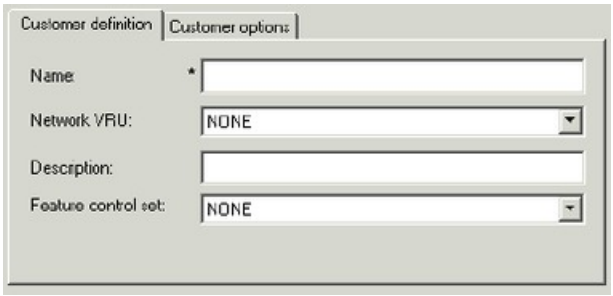


- Click **New**.
- Under Currently Selected Node:
  - Enter Domain Name of machine on which the CICM Network Administration & Data Server resides
  - Enter System Name (hostname) of machine on which the CICM Network Administration & Data Server resides
  - From pull-down menu, select primary or secondary Administration & Data Server (secondary is the backup CICM Network Administration & Data Server in case the primary is not available)
  - Save

Step 9 Click **Add Customer Definition**.

Step 10 Under Customer Definition tab:

Figure 15: Customer Definition Tab



- Enter the customer name within the CICM instance. If this is an Advanced Services CICM instance, repeat this Add process until you have entered the names of each individual customer within the instance. If this is not an Advanced Services CICM instance, the name to be added is the same name as the instance.
- Select the Network VRU assigned to each customer under the Network VRU pull-down menu.
- If a Feature Control Set has been defined for a user or group of users within a customer, associate the Feature Control Set with the customer from within the Feature Control Set pull-down menu.

Step 11 Under Customer Options tab, check **Bill for VRU Time**. This is a flag that can be set and used by service providers to indicate how Network VRU usage is to be billed.

Step 12 Click **Save**.

Step 13 Open NIC Explorer. Click **Retrieve** and define the network routing client.

Since DNs and labels have different routing clients at the NAM level than at the CICM level, it is necessary to associate each NAM routing client to its associated CICM routing client for the purpose of CICM Replication. When the DNs and labels are replicated to the CICM level, the routing client associated with them will automatically change from the NAM routing client to the CICM routing client. In order to achieve this change, a network routing client name is assigned to each of the corresponding NAM and CICM routing clients.

At the NAM level, enter a unique name for the network routing client in each routing client tab.

DNs and labels must be associated with a customer when configured at the NAM level.

Configure CICM replication at CICM level

Perform the following steps to configure CICM Replication for CICM instances.

Procedure

Step 1 Open NIC Explorer for each CICM Instance.

Step 2 Retrieve and define associated network routing client.

You must go into Configuration Manager *for each CICM instance* and enter the same network routing client name in the routing client tab that was entered at the NAM level for the associated NAM routing client.

Customer concept implementation with Network VRUs

This section discusses how to implement Customer Concept on Unified ICMH with Network VRU instances.

Note See Configuration, on page 94 for details on how to configure network VRUs.

Implement Customer Concept for NAM level

Implementation of Customer Concept is required for management and reporting purposes within the NAM instance that provides Network VRU services to CICM instances.

NAM to CICM DN and Label Replication is optional. (see NAM to CICM DN and label replication, on page 45).

To implement Customer Concept for this type of instance, perform the following steps.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

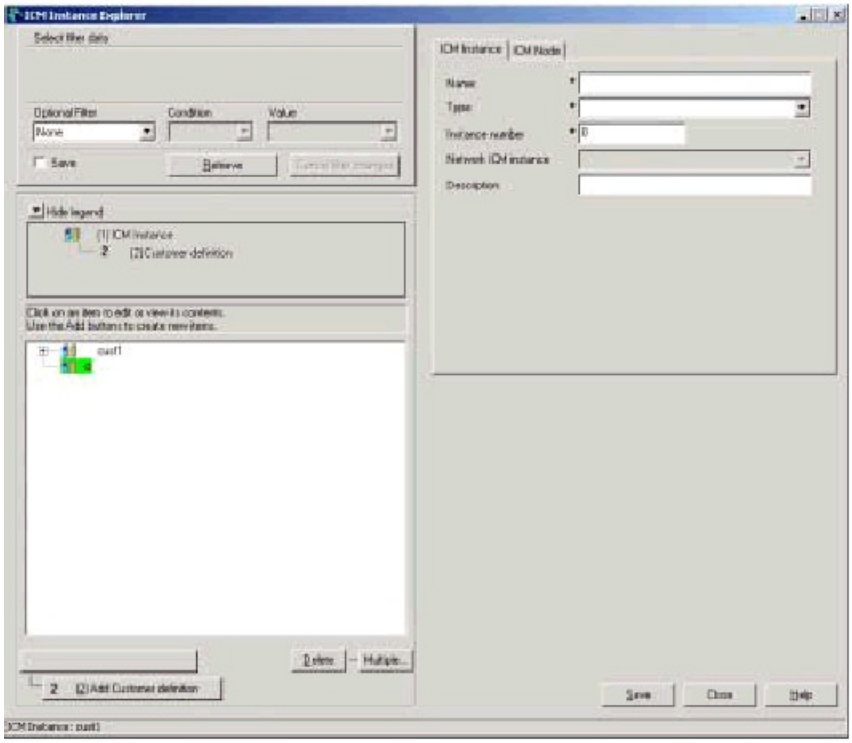
Step 2 Select the NAM instance you will be configuring.

Step 3 From within the Administration Tools folder, double-click the **Configuration Manager**.

Step 4 Open the ICM Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 5 Click **Retrieve**.

Figure 16: ICM Instance Explorer Window



Step 6 By default, the NAM instance that you are configuring within will already appear, as will a default customer under that instance. The default customer will have the same name as the NAM instance.

Step 7 Click **Add ICM Instance**.

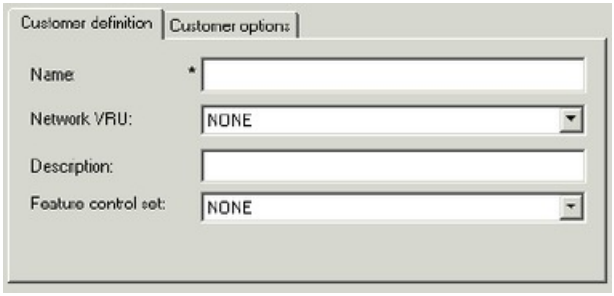
Step 8 Under ICM Instance tab:

- Enter CICM instance name
- For Type, select **Customer ICM** from the pull-down menu
- Enter CICM instance number
- For Network ICM Instance, select the name of the NAM instance

Step 9 Click **Add Customer Definition**.

Step 10 Under Customer Definition tab:

Figure 17: Customer Definition Tab



- Enter the customer name within the CICM instance. Since this is **not** an Advanced Services CICM instance, the name to be added is the *same name* as the instance.
- Select the Network VRU assigned to each customer under the Network VRU pull-down menu.
- If a Feature Control Set has been defined for a user or group of users within a customer, associate the Feature Control Set with the customer from within the Feature Control Set pull-down menu.

Step 11 Under Customer Options tab, check **Bill for VRU Time**. This is a flag that can be set and used by service providers to indicate how Network VRU usage is to be billed.

Step 12 Click **Save.**

Implement Customer Concept for CICM level

To implement Customer Concept on a CICM instance, perform the following steps.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

Step 2 Select the CICM instance you will be configuring.

Step 3 From within the Administration Tools folder, double-click the **Configuration Manager**.

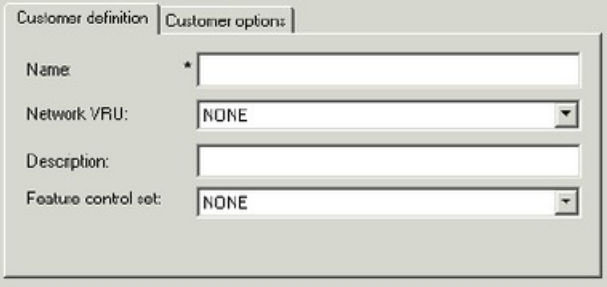
Step 4 Open the ICM Instance Explorer tool by selecting **Configure ICM** > **Enterprise** > **ICM Instance** > **ICM Instance Explorer**. The ICM Instance Explorer window appears.

Step 5 Click **Retrieve**.

Step 6 By default, the CICM instance that you are configuring within will already appear, as will a default customer under that instance. The default customer will have the same name as the CICM instance.

Step 7 Under Customer Definition tab:

Figure 18: Customer Definition Tab



- Select the Network VRU assigned to each customer under the Network VRU pull-down menu.
- If a Feature Control Set has been defined for a user or group of users within a customer, associate the Feature Control Set with the customer from within the Feature Control Set pull-down menu.

Step 8 Click **Save**.

CHAPTER 6

Advanced Services

Advanced Services allows service providers to offer call center routing services to end-customers independent of any end-customer equipment, such as ACDs, PBXs, key systems or even simple analogue phone lines. This section describes how to setup and administer an Advanced Services instance. For the relation between Customer Concept and Advanced Services, see Chapter 4,Customer Concept, on page 41.

Introduction

There is a special ICM instance that is used for Advanced Services. The Advanced Services ICM is a multi-customer instance. A single Advanced Services ICM can support large numbers of customers. Advanced Services customers have web-based tools to control and manage their call routing, specifically WebView and Unified IC for reporting and Internet Script Editor for call routing.

An Advanced Services ICM is an ICM instance just like any other, but it is configured differently. This means that a CICM complex can run a single Advanced Services ICM and a maximum of 24 CICMs. However, for performance reasons it is desirable to run an Advanced Services ICM on its own dedicated hardware.

To support multiple subscribers on the same Advanced Services ICM, Advanced Services has a particular concept of a customer. A customer is an organization that uses Unified ICM to manage its call center. Each customer has its own configuration elements, such as dialed numbers, labels, call types, scripts, VRU scripts and scheduled targets. All these configuration elements are stored in the same Advanced Services ICM database, but the reporting and scripting tools will make sure that a specific customer only has access to his own data. Since Advanced Services customers do not have ACD and Peripheral Gateways there are no configuration elements like peripherals, services, skill groups, and so forth.

No special security is applied at the customer level. Any Administration & Data Server user with access to the Advanced Services ICM instance can choose to view data for any or all customers in that instance. So the Service Provider can use the Administration & Data Server to administer the Advanced Services ICM as any other ICM instance. Advanced Services customers must only have access to their data using WebView, Unified IC, and Internet Script Editor. These tools will prevent a customer from accessing other customer data. This is achieved by having a user login with a personal userid and password. The user ID is tied to a specific

customer and WebView, Unified IC, and Internet Script Editor will only expose this customer's data. Each individual user also has a profile, called a Feature Set, that determines his or her access rights in detail.

The following table provides an overview of the tools used by the Service Provider and the end-customer for day-to-day management tasks.

Task	Service Provider (Tool)	End-user (Tool)
Configuration	Configuration Manager	N/A
Scripting		
New scripts	Administration & Data Server Script Editor	Internet Script Editor in full edit mode
Structural script changes	Administration & Data Server Script Editor	Internet Script Editor in full edit mode
Changing script parameters	Administration & Data Server Script Editor	Internet Script Editor in quick edit mode
Reporting		
Defining and running report based on existing template	WebView and Unified IC, using Call Type reporting and scheduling, exporting and e-mail options	WebView and Unified IC, using Call Type reporting
Defining custom reporting template	Using Sybase InfoMaker to define new Call Type templates	N/A

Advanced Services ICM instance

The following steps are required to setup and configure an Advance Services ICM instance. These steps assume that a NAM has been setup with at least one Network VRU connected to it.

- Install a new ICM instance.

  This includes installing a Logger, Router with INCRP NIC and one or more Administration & Data Servers (Administration & Data Server instances) for the Service Provider to manage the service. Do not configure or install any Peripheral Gateways (PGs), since they are not used by Advanced Services.

- Install one or more WebView, Unified IC, and Internet Script Editor Servers that will act as web servers for end-customer use.

  A WebView or Unified IC server will fetch real-time data for reporting purposes from its local Administration & Data Server (if installed on an Administration & Data Server) or from another Administration & Data Server's real-time Administration & Data Server. Historical data will be fetched from an Administration & Data Server with the Historical Data Server (HDS) option installed. This could be the same or a different Administration & Data Server as the WebView or Unified IC server.

The remainder of the setup is identical to setting up a regular Administration & Data Server.

- Configure the Network VRU. Only Network VRUs of Type 3, 5, 6 or 7 are supported with Advanced Services.
- Enter customer specific configuration data using Configuration Manager. For each customer this consists of the elements listed in the following table.

Data elements	Required/optional	Tool used to configure
Customer	Required	ICM Instance Explorer
Feature Control Set	Required (although generic, non-customer specific feature control sets can be used)	Feature Control Set List
User	Required (see Configure user, on page 57)	User List
Call Type	Required	Call Type List
Dialed Number	Required	Dialed Number List
Label	Required unless dynamic labels are used; which they must not be because of security reasons	Label List
Label List	Optional	Network VRU Script List
Scheduled Target	Optional	Scheduled Target Explorer
Routing Script	Required unless performed by the customer using Internet Script Editor	Script Editor

The next section describes these steps in detail.

Enter customer specific configuration data in the NAM. This is identical to normal ICM instances and is only summarized here. The main customer specific configuration elements in the NAM are:

- Labels
- Dialed Numbers
- Routing Script to forward route requests to the Advanced Services ICM
- Customer (required only for CICM replication)

New Advanced Services customer configuration

For each new Advanced Services customer, the following configuration elements need to be defined by the Service Provider.

For more information, refer to the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted*, the Configuration Manager online help, and the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

Configure Feature Control Set

Perform the following steps to configure Feature Control Set.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

Step 2 Select the instance you will be configuring.

Step 3 From within the Administration Tools folder, double-click the **Configuration Manager**.

Step 4 Open the Feature Control Set List tool (**Tools** > **List Tools** > **Feature Control Set List**). The Feature Control Set List window appears.
Configure a Feature Control Set that contains the maximum number of elements that this customer can get access to. Since an Advanced Services customer will never use the Configuration Manager, uncheck all check boxes.

Under the Script Editor application, click **Advanced**. Under Edit Options, select either **Full Editor**, or **Quick Edit**. This determines what edit mode this user is allowed to use.

Under Node Control uncheck each Script Node that this profile must not provide access to. For Advanced Services, the following nodes must always be unchecked, since they are not permissible with Advanced Services:

- Agent
- Agent to Agent
- DB Lookup
- Enterprise Service
- Enterprise Skill Group
- Gateway
- ICM Gateway
- Queue to Agent
- Route Select
- Select
- Service

- Skill Group
- Translation Route to VRU

In particular, the DB Lookup and Gateway nodes must not be allowed end-customer access since they might expose other customer data. It is possible for Advance Services Scripts to use these nodes for database lookups. The DB Lookup and Application Gateway configuration must be controlled entirely by the Service Provider and not by the end-customer. An end-customer must not get access to these nodes since it will expose other customers' databases and external applications. This implies that end-customers do not have full edit access to routing scripts containing these nodes, since they will not be able to full edit scripts that include these nodes.

Multiple Feature Control Sets can be defined for a single customer. Feature Control Sets are assigned to a user (not a customer), so that different users can have different levels of access.

Customer

Using ICM Instance Explorer, configure a new Customer under the Advanced Services ICM Instance. Select a Network VRU to be used by this customer and the customer level Feature Set. This Feature Set is used for users associated with this Customer, unless the user is associated with a different Feature Set in the User List tool.

Configure user

Note You only need to use the User List tool if the user will have restrictions (such as Feature Control or Read-only); otherwise, the user can be given access using Domain Manager.

Using the User List tool, configure one or more users for this customer.

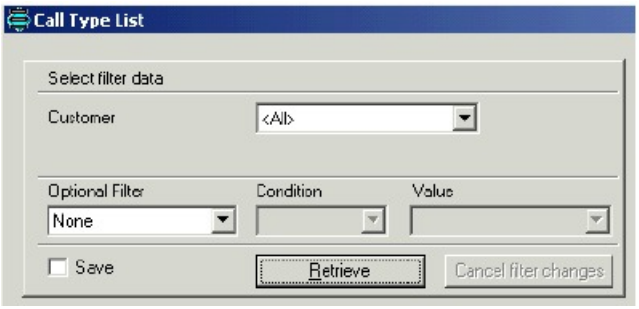
- In the **Domain name** field, select the Active Directory (AD) Domain that this user's AD domain account is going to be created in. This would typically not be the CICM domain, but a separate domain specific to the WebView, Unified IC, and Internet Script Editor servers.
- The **User name** for this user. This becomes the AD domain username as well.
- The user's **Password**. This becomes the AD domain user's password as well.
- The **Customer** created using the ICM Instance Explorer, or All Customers.
- Select the **Feature Control Set** that is to be associated with this user. If the setting chosen is **<None>**, the Customer level feature control set will be used.
- Checking **Configuration** gives the user access to Configuration Manager and Script Editor. If you also check **Read only**, the user cannot make any changes using Configuration Manager or Script Editor. In any case, the user's feature control set determines which routing scripts the user can access.
- Checking **Setup** gives the user access to Setup, Configuration Manager, Script Editor, and WebView.
- Checking **WebView** gives the user access to WebView.

Note This checkbox is not applicable when deploying Unified IC.

Configure call type

Configure one or more call types for this customer using the Call Type List tool. Select the associated customer from the Customer drop-down menu.

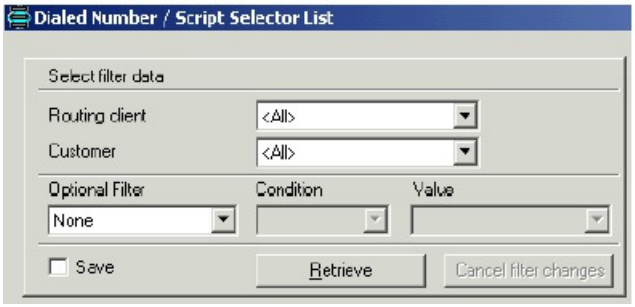
Figure 19: Call Type List Dialog



Configure dialed number

Configure one or more Dialed Numbers for this customer using the Dialed Number List tool. On the attributes tab, select the associated customer from the Customer drop-down menu.

Figure 20: Dialed Number List Tool

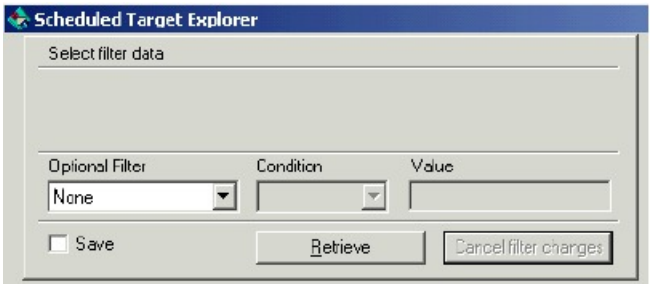


On the Dialed Number Mapping tab, select a Call Type mapping for this Dialed Number. The tool will only show Call Types defined for the customer selected on the attributes tab.

Configure Scheduled Target

Configure one or more Scheduled Targets for this customer using Scheduled Target Explorer. Select the associated customer from the Customer drop-down menu.

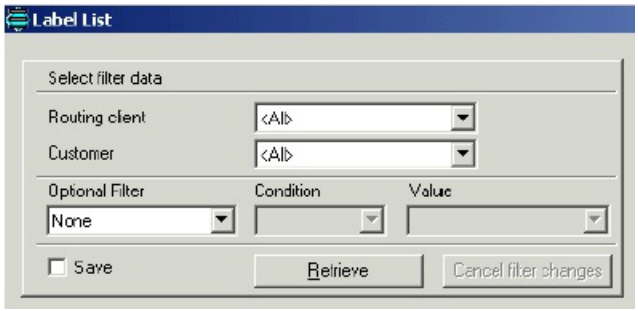
Figure 21: Scheduled Target Explorer Tool



Add label

You can add one or more Labels for each Scheduled Target using this tool or using the Label List tool. In either case, select the same customer for the Label as selected for the Scheduled Target. Select the associated customer from the Customer drop-down menu.

Figure 22: Label List Dialog



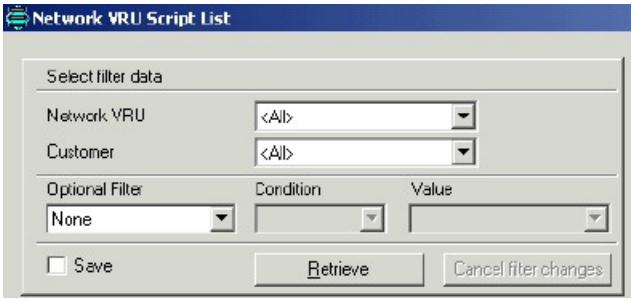
Observe the following guidelines for labels:

- If this is a standard Label to be used in a Label or Divert Label node, leave the Target Type and Network Target set to **None**.
- If this is a Label for a Scheduled Target Type, select the Scheduled Target from the Network Target drop-down menu.
- You can configure multiple labels for Scheduled Targets, but for a specific Routing Client only the first label will be used; therefore, when you configure multiple labels, configure each for a different Routing Client. Configuring more than one label for the *same* Routing Client will have no effect.

Configure Network VRU Script

Configure one or more Network VRU Scripts for this customer using the Network VRU Script List tool. Select the associated customer from the Customer drop-down menu.

Figure 23: Network VRU Script List Tool



Associate Script with specific customer

The Service Provider can either create routing scripts for the customer or the customer can use Internet Script Editor to create routing scripts himself.When the Service Provider is creating routing scripts for an end-customer, the scripts are not automatically associated with any specific customer. Use the following action to associate a script with a specific customer, so that the customer can get access to it:

- Make sure the script is saved.
- Using Script Editor, select Script Explorer from the File menu.
- Under All Customers, Default business unit, locate the script(s) to associate with a specific customer and drag them over to the customer's Default business unit. Dragging the mouse pointer to the customer and holding it there briefly will show the default business unit.

CHAPTER 7

Administrative Tools

The Unified ICMH product includes tools that help you administer your Unified ICMH configuration. This chapter discusses three of these tools:

- Service Control
- Select Administration Instance

Service Control

The Service Control tool lets you view, stop, and start Windows services related to the system software. This tool is installed on each Administration & Data Server, CallRouter, Logger, and Peripheral Gateway.

Start Service Control

Procedure

Step 1 Double-click the **Unified CCE Service Control** icon on the desktop to open this tool. The Service Control window opens.

Step 2 Specify the following:

- **Select** (button). Click to choose another computer. You can then view and control services on that machine remotely.
- **All** (checkbox). If checked, the dialog box displays all Windows services on the machine. You can then stop or start any service installed on the machine.
- **Start/Start All** (button). Starts the selected service(s). The button name is Start All if the Service Control window shows only ICM services (the All box is clear) and no services are selected; at other times, the button name is Start.

- **Stop/Stop All** (button). Starts the selected service(s). The button name is Stop All if the Service Control window shows only ICM services (the All box is clear) and no services are selected; at other times, the button name is Stop.
- **Cycle** (button). Stops and then restarts an active service in a single action.
- **Manual** and **Automatic** (buttons). Lets you switch the startup mode for a service between manual (user initiated) and automatic (starts when the computer is turned on).

Select Administration Instance tool

The Select Administration Instance tool lets you choose which instance to use at a network Administration & Data Server.

You can have up to 25 Administration & Data Server services running on an Administration & Data Server at once. Although you can only view real-time data on one instance at a time, you can switch to another instance at any time. This makes it possible to view real-time data for multiple instances from a single Administration & Data Server.

Use Select Administration Instance

The following instructions describe how to use Select Administration Instance.

Procedure

Step 1 Access the Select Administration Instance tool by selecting **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Select Administration Instance**. The Select Administration Instance window appears.

Step 2 Select the service for the instance you want and click the **Switch To** button. The Administration & Data Server does the following:

- Stops any other Administration & Data Server services that are running on the current machine.
- Starts the Administration & Data Server service that you selected.

Note If the Stop and Start Administration & Data Server when Switching Instances box is checked when you click **Switch To**, the Administration & Data Servers for all instances except the selected instance are stopped and the Administration & Data Server for the selected instance is started.

Step 3 When finished, click **Close**.

CHAPTER 8

Security considerations

The Unified ICMH product allows several customers to share the same Central Controller complex. This presents some possible security concerns in the following areas:

- Relationships between Windows domains
- Preventing unauthorized access to real-time data
- Access to historical data

This chapter discusses these concerns and the means by which the Unified ICMH product addresses them.

For a more general discussion of security, refer to the *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)*.

Windows domains

Components in this architecture are divided among several Windows domains. All NAMs and their associated Administration & Data Servers are in a single domain. Each CICM complex and its associated Administration & Data Servers is in a separate domain. Each instance's Administration & Data Servers can be in two different domains:

- CICM instance Administration & Data Server on the NAM
- CICM instance Administration & Data Server on the Customer Administration & Data Server

Each CICM domain must have a two-way trust relationship with the NAM domain and a two-way trust relationship with each customer domain that it serves.

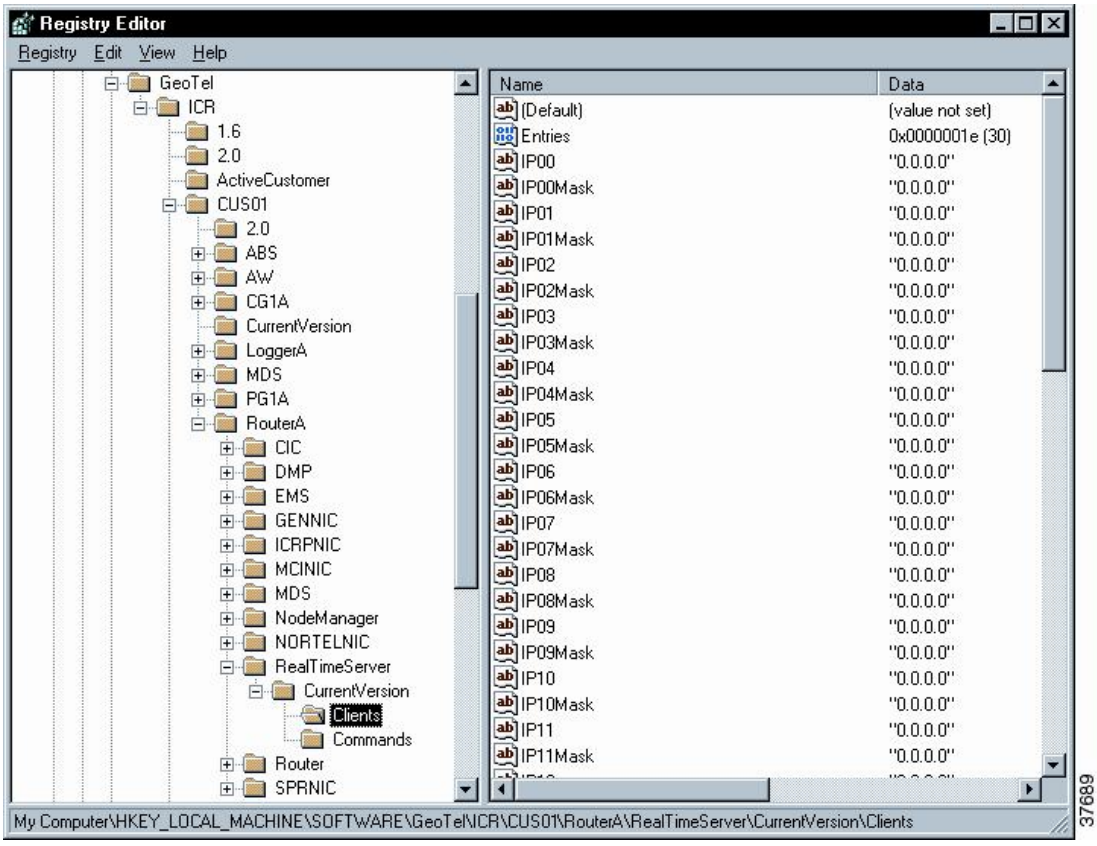
For more information, refer to the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)*.

Real-time clients validation

To prevent unauthorized access to real-time data, you can configure the Unified ICM's Real-Time Server process to validate each connection. This ensures that only expected clients receive the real-time data.

To set up this validation, you must edit the Windows Registry on the CallRouter machine. Locate the customer's subtree under the registry tree HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM. The customer's subtree contains either a RouterA or RouterB tree. Under that tree locate RealTimeServer\CurrentVersion\Clients.

Figure 24: Registry Editor Window



To allow access for a specific machine or subnet, you must specify an IP address (IP00, IP01, IP02, etc.) and a corresponding mask (IP00Mask, IP01Mask, IP02Mask, etc.). The IP address can be a complete or partial address. The mask indicates which part of the address must match. You can specify up to 30 addresses and associated masks.

For example, to allow access only to a machine with an address of 199.99.123.45, specify that value as IP00 and set IP00Mask to 255.255.255.255 (meaning to match all four octets of the address). To then allow access to any member of the 199.99.125 subnet, set IP01 to 199.99.125.0 and set IP01Mask to 255.255.255.0 (meaning to match only the first three octets of the address).

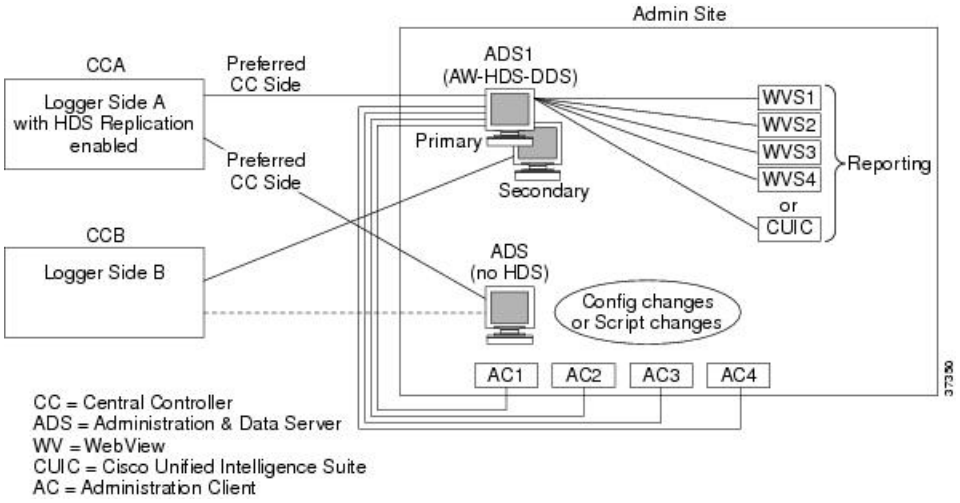
The IP mask 0.0.0.0 is a special value indicating that the associated IP address is to be ignored. By default, all the masks are set to this value. If Unified ICM does not find any valid values, it allows any machine to connect.

Historical Data Server

Administration & Data Servers need to access historical data (15-minute and half hour data, call detail, and so forth). The system software normally stores historical data in the central database on the Logger, as well as on the Administration & Data Server that acts as the Historical Data Server (HDS).

One Administration & Data Server at each admin site is an HDS machine. The Central Controller forwards historical records to the HDS machine for storage in a special local database (awdb). Other Administration && Data Servers at the local site can retrieve historical data from the HDS machine without having to access the central site (see the following figure).

Figure 25: Historical Data Server Architecture



To set up an Historical Data Server, you must configure the Logger to perform historical data replication. You must also configure an Administration & Data Server to be an Historical Data Server. You can use the ICMDBA tool to create an HDS database, then use the Web Setup tool to add an Administration & Data Server with an HDS role.

Small to medium Historical Data Server deployments

Note Before reviewing this section, review the *Cisco Unified Contact Center Enterprise 8.x Solution Reference Network Design (SRND)* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html for scalability details about small to medium deployments.

In this deployment, all agent-related historical data is replicated to an HDS.

This deployment type supports the following Logger setup:

- Maximum of 2 Loggers
- Maximum of 2 Historical Data Servers allowed per Logger side

There are three options available for an Administration & Data Server role in a small to medium deployment:

- **Administration Server, Real-time and Historical Data Server and Detail Data Server (AW-HDS-DDS)**: Stores real-time, historical, call detail, and call variable data, including agent historical data filtered by peripheral

  This role is similar to the "Distributor AW with HDS" role in previous ICM releases. It provides ability for configuration changes as well as both real-time and historical reporting. The real-time and historical reporting is supported using one of two reporting clients: WebView server or Cisco Unified Intelligence Center (CUIC). The call detail and call variable data are supported for custom reporting data extraction to meet the requirements for System Call Trace tool and feed historical data to the CUIS (Archiver).

- **Administration Server and Real-time Data Server (AW)**: Stores real-time data, including agent historical data filtered by peripheral, but no historical data

  This role is similar to the "Distributor AW" role in previous ICM releases. This role provides the ability for configuration changes as well as for real-time reporting. The real-time reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client). This role does not support historical reporting.

- **Configuration-Only Administration Server**: HDS is not enabled and real-time reporting is turned off. This deployment only allows configuration changes with no real-time and historical reporting.

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for details about how to use the Web Setup tool to add Administration & Data Servers

Large Historical Data Server deployments

Note Before reviewing this section, review the *Cisco Unified Contact Center Enterprise 8.x Solution Reference Network Design (SRND)* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html for scalability details about large deployments.

Note This deployment is *not* supported in Unified SCCE; however, Unified SCCE Release 7.5 is supported in the 8.0(1) solution.

In this deployment, historical data can be distributed for scalability purposes.

This deployment type supports a maximum of 4 Historical Data Servers per Logger side, which can be configured as 3 AW-HDS and 1 HDS-DDS deployments (see descriptions below).

There are four options available for an Administration & Data Server role in a large deployment:

- **Administration Server and Real-time and Historical Data Server (AW-HDS)**: Stores real-time and historical data, including agent historical data filtered by peripheral, but no call detail and call variable data

This role provides ability for configuration changes as well as for both real-time and historical reporting. The real-time and historical reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client).

- **Historical Data Server and Detail Data Server (HDS-DDS)**: Stores only historical data, including all agents and detail data (TCD, and so on) with additional indices (this option is limited to one per Logger side)

  This role provides support for historical reporting, Call Detail data extraction for System Call Trace tool and feed to CUIS Archiver. This deployment also includes configuration data available for historical reporting. Real-time data reporting and the ability to make configuration changes are not supported.

- **Administration Server and Real-time Data Server (AW)**: Stores real-time data, including agent historical data filtered by peripheral, but no historical data

  This role is similar to the "Distributor AW" role in previous ICM releases. This role provides the ability for configuration changes as well as for real-time reporting. The real-time reporting is supported using either WebView server or Cisco Unified Intelligent Center (Reporting client). This role does not support historical reporting.

- **Configuration-Only Administration Server**: HDS is not enabled and real-time reporting is turned off. This deployment only allows configuration changes with no real-time and historical reporting.

Refer to the *Installation Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for details about how to use the Web Setup tool to add Administration & Data Servers.

For specific information about setting up an HDS database, see CICM installation and configuration, on page 29

CHAPTER 9

Special considerations

This chapter describes some features of special interest to Unified ICMH users:

- Calling Line ID (CLID) masking.
- Dynamic Labels in NAM/CICM configurations.
- NAM Network Event Reporting
- Network Transfer

Calling line ID (CLID) masking

The Calling line ID (CLID) masking feature restricts the presentation—that is, masks the display—of a caller's phone number on a CICM application. This feature is specifically designed to be used in an Unified ICMH environment where the NAM receives a call from a Network Interface Controller (NIC) that supports presentation restriction. The NAM then uses a Script Editor ICM Gateway node to deliver the call to the CICM with a modified calling line ID.

Historical data for the call will differ between the NAM and the CICM. The NAM will record the complete CLID, while the CICM will record the masked CLID.

CLID masking configuration

CLID Masking rule configuration is defined through two applications on the NAM:

- Configuration Manager, where the masking rule is enabled in the configuration database.

- Script Editor, where the ICM Gateway node indicates whether the masking rule must be used before forwarding the call to the CICM.

Define a CLID masking rule

Use Configuration Manager's System Information tool to specify the masking rule.

Procedure

Step 1 Start the Configuration Manager on the Administration & Data Server. To start the Configuration Manager, double-click **Configuration Manager** from the Administration Tools folder. The Configuration Manager window opens.
For information about the Configuration Manager, refer to the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise and Hosted*.

Step 2 Run the System Information tool by selecting **Tools** > **Miscellaneous Tools** > **System Information**.

Step 3 In the CLID Masking section, specify the following:

- **Enabled** (checkbox). Select this option to enable CLID masking.
- **Number of characters**. The number of trailing digits at the end of the CLID that you want to remove or replace.
- **Remove Digits** (checkbox). Select this option to remove the specified Number of Characters from the customer's view. (If you select this option, then the Mask Characters option is not enabled.)
- **Mask Character**. A character with which to replace the specified Number of Characters for the customer's view. (If you specify this option, then the Remove Digits option is not enabled.)

Note For more information on the System Information tool, refer to the online help.

Use Script Editor ICM Gateway Node on NAM

Once the CLID Masking rule is set up through Configuration Manager, the rule can be applied through the Script Editor's ICM Gateway node.

Procedure

Step 1 Within Script Editor on the NAM, add an ICM Gateway node to the script workspace and right-click. The ICM Gateway Properties dialog box appears, listing all application gateways that have been configured with the **Remote ICM** option.

Step 2 Set the following:

- **ICM Gateways**. Select the gateway for the system you want to access.
- **Validate returned labels**. (Checkbox). Select if you want the NAM to validate returned labels.

- **Calling line ID masking**. (Radio buttons) Indicate whether Calling Line ID masking instructions must be applied before the call is passed to the CICM. The options are:
  - **Do not apply masking rule**. If selected, masking instructions are ignored.
  - **Apply masking rule if call is presentation restricted**. If selected, applies masking instructions if the call variable CLIDRestricted is set to 1.
  - **Always apply masking rule**. If selected, masking instructions are always applied.

Step 3 Click **OK** to apply the changes and close the dialog box.

Dynamic labels in NAM/CICM configurations

The Script Editor contains a Label node and a Divert Label node. Both of these nodes allow a user to select a configured label for a particular routing client, to be returned when the label node is reached during script processing.

Note When the system software executes a Label node, it chooses the *first* valid label for the current routing client. This differs from the Divert Label node, which returns *all* the values in the Selected Labels list to the routing client.

Configured labels are static, defined through the Configuration Manager. A second label type, *dynamic* labels, is also available. Dynamic labels are expressions the CallRouter processes "on the fly," converting an expression into a character string that is then returned to the routing client as a label.

Dynamic labels in Script Editor

Both the Label node and the Divert Label node dialog boxes contain a Label Type drop-down list. The default setting for this field is **Configured**, which results in the display of all labels configured in the system.

If you change the Label Type setting to **Dynamic**, the Label Expression field appears. You can either enter an expression or string using this field or open the Formula Editor to create one.

Note For information about using the Script Editor with these nodes, refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

Dynamic label flow

In NAM/CICM configurations, the dynamic label flow is as follows:

1. A call request comes through the NAM ICM Gateway node to the Customer ICM.
2. The Customer ICM generates a dynamic label and sends it back to the NAM.

3 The NAM can validate the label against the NAM label database (in which case, the NAM does not consider the label to be dynamic), or the NAM can accept the label, even if it is not in the NAM label database (in which case, the NAM does consider the label to be dynamic).

The NAM cannot distinguish between a CICM dynamic label and a CICM configured label. By default, the NAM rejects any label returned by an ICM Gateway node that is not known by the NAM.

In the event that the CICM returns multiple labels, such as with a Divert Label node—and only some of the labels are known by the NAM—the behavior of the NAM will depend on the Script Editor's ICM Gateway node's **Validate returned labels** property:

- If the NAM is instructed to validate all labels, it will discard any of the unknown labels. Only NAM-configured labels will be used.
- If the NAM is instructed to not validate labels, it will treat the entire set of labels as dynamic. This is only significant for the call termination record, which will indicate that the final label used is dynamic. This is indicated even if the final label used was one of the NAM known labels.

NAM network event reporting

The NAM can provide detailed records on call disposition information that the network may provide. The NAM populates the Network_Event_Detail table when this feature is enabled.

Note This feature requires a NIC that is designed to support populating this table. Contact your Cisco representative to obtain information on the capabilities of your NIC.

Description

The NAM database has a specific table for recording call disposition information, Network_Event_Detail. The table contains a record for each network event that is received for a call, such as answer, busy and disconnect events.

Network Event Reporting can be enabled or disabled at the NIC level. It cannot be enabled or disabled on a per call(-type) basis. Refer to the System Manager Guide Supplement for your NIC on how to enable or disable this feature.

The table will be written for events related to all call legs that happen under control of the NIC. This includes the incoming call leg (calling party, or leg 1) and the outgoing call leg (called party, or leg 2). In case of network transfer, there could be multiple subsequent outgoing call legs, and information is recorded for each of them separately. For example, for a simple call, there will be an ANSWER event record for leg 1 (this implies that leg 2 answered the call) and a DISCONNECT event record for leg 1 or leg 2, depending on whomever initiated the disconnect (that is, hung-up first). If leg 1 hangs up before leg 2 has answered, an ABANDON event record will be written for leg 1. If the called party executes a blind network transfer controlled by the NIC, Network Event Reporting will write a DISCONNECT event record for leg 2, followed by an ANSWER event for the new called party, followed by a DISCONNECT event upon call completion. The event records for the second called party will have leg id 2 as well, but can be distinguished from the first called party by the different RouterCallKeySequenceNumber.

Call legs originated by a PG and setup outside of the control of the NIC (for example, a local transfer executed by an ACD) are not included in the table.

Table overview

A record will be written for every network event sent to the NIC. The following table lists the fields in this record.

Field	Data Type	Explanation
RouterCall KeyDay	Int	Used with RouterCallKey and RouterCallKeySequenceNumber to identify the related Route_Call_Detail record. Refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for information on the corresponding field in the Route_Call_Detail table.
RouterCall Key	Int	Used with RouterCallKeyDay, RouterCallKeySequenceNumber to identify Route_Call_Detail record. Refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for information on the corresponding field in the Route_Call_Detail table.
RouterCall KeySequence Number	Int	Used with RouterCallKey, RouterCallKeyDay to identify related Route_Call_Detail record. Refer to the *Database Schema Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* for information on the corresponding field in the Route_Call_Detail table.
CallLegID	Smallint	Identifier of the call leg this event relates to. Possible values are1 for calling party, 2 for the called party. Notice that after a network transfer, the new called party would still have CallLegID 2.

Field	Data Type	Explanation
Event		Event from network that caused record to be written. Values: ROUTE_SELECT_FAILURE (1), CALLED_PARTY_BUSY (2), NO_REPLY (3), ANSWER (4), ABANDON (5), DISCONNECT (6), UNKNOWN (7).
DateTime	DateTime	Timestamp of receipt of event at the NIC (in NAM Central Controller time).
TimeZone	Int	The time zone of the NAM Central Controller used for DateTime.
Duration	Int	This field contains the call duration. It is only written for DISCONNECT events and for UNKNOWN events, when the call has been answered. Duration is measured in seconds as the delta between the NIC time stamps for DISCONNECT/UNKNOWN and ANSWER.
Value1	Int	Value dependent upon event and NIC that provides additional reporting information. This might contain a network provided releaseCause (for DISCONNECT), failureCause (ROUTE_SELECT_FAILURE), etc.
Value2	Varchar(128)	Reserved for future use.
RecoveryKey	float	A value used internally by the system software to track virtual time.
RecoveryDay	int	A value used internally by the system software to track virtual time.

Events reported

The events reported on depend on the NIC. The standard SS7 IN NIC will arm for the following events:

- Route Select Failure (DP4 – request or notification)
- O_CalledPartyBusy (DP5 – request or notification)
- O_No Answer (DP6 – request or notification)
- O_Answer (DP7 – notification)
- O_Disconnect (DP9 – notification)
- O_Abandon (DP10 - notification)

Determination of the type of arming (request or notification) is based upon the script and feature that sent the label to the NIC.

System impacts

Network Event Reporting will have an impact on the performance of the NAM, the switch and the signaling links, since the call transaction remains open for the life of the call, additional event arming takes place and additional records are written to the NAM database.

- The switching network will have the additional overhead of every call transaction (TCAP) being open until call disconnects. This may impact memory utilization on the Service Switching Points.
- The NAM will be impacted by the additional database records being written by the Logger. The database size will need to account for Network Event Reporting.
- PSTN to Unified ICM connection sizing (such as SS7 link sizing) needs to be reviewed to ensure that sufficient capacity is available for additional event messages.

Limitations

- The Network_Event_Detail table will be available in the NAM database only. The data will not be available in a CICM connected to the NAM.
- The NAM does not contain any standard reporting templates for providing reports based on the information stored in the Network_Event_Detail table. A custom reporting solution is required to provide reports based on this information; contact your Cisco representative.
- Not all NICs support Network Event Reporting. (Contact your Cisco Support representative for more information.)
- Network Event Reporting is not supported for ACD or VRU PG routing clients, such as a VRU acting as a service node (for example, Cisco Customer Voice Portal). In this case, the Termination_Call_Detail table will contain call duration and call disposition information.
- Network Event Reporting does not record data on temporary call legs to type 3 or type 7 Network VRUs. The Termination_Call_Detail table will contain the call duration and call disposition information for the VRU leg.

- Call legs originated by a PG and setup outside of the control of the NIC (for example, a local transfer executed by an ACD) will not be included in the table. Information on these call legs is recorded in the Termination_Call_Detail table.

Network transfer

NAM/ICM provides capabilities to transfer calls to another destination after they have been answered by an agent. The general call flow is as follows:

1. A call is pre-routed to an agent by Unified ICM and the agent has answered the call.
2. The agent indicates, through his softphone or hard phone, that he wants to transfer the call to another destination. Typically the agent would transfer the call to a number that indicates a skill group rather than to a specific agent or phone number.
3. A route request is sent to Unified ICM to determine the real destination for the call, that is, Unified ICM will run a routing script to determine the agent or call center location best suited to handle this call.
4. At this point there are two options: either a network transfer is executed or a local transfer. The difference lies in what device takes care of transferring the call to the new destination selected by Unified ICM.

In the case of a *local transfer* the transferring agent's ACD is responsible for transferring the call. If the new destination is not an agent on the same ACD, the ACD will typically do this by tromboning or hair pinning the call to the new destination through tie lines or the PSTN network.

In case of a *network transfer* the network that pre-routed the call to the transferring agent in the first place is responsible for taking the call away from the transferring agent and reconnecting the call to the new destination.

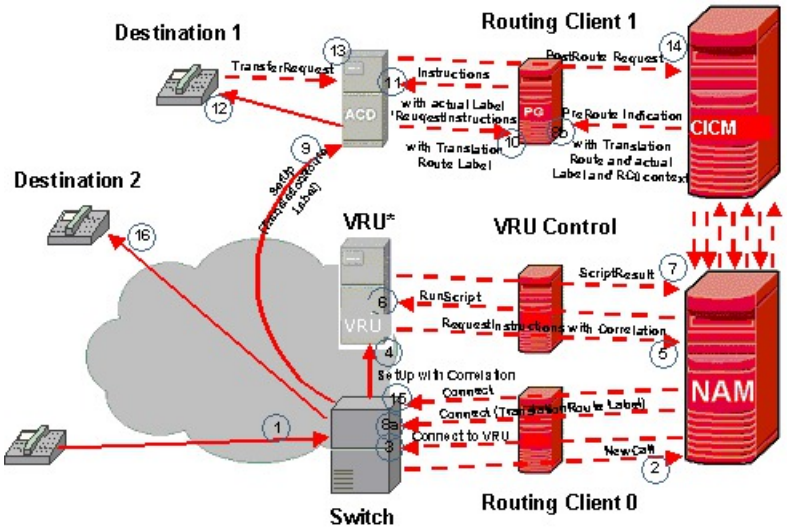
This section describes the detailed call flows, conditions and configuration required to implement network transfers. It does not cover local transfers.

Detailed call flow

A network transfer itself involves only a small number of steps. However, the steps preceding the network transfer are important as well, since they set the conditions for a network transfer to take place.

The call flow that is described in detail in the following figure is a specific example.

Figure 26: Network Transfer Call Flow



This call flow consists of the following steps:

1. A caller makes a call into a network that has the capability to trigger a NAM route request.
2. The switching network sends the NAM a route request through Routing Client 0. A routing script is executed in the NAM and the NAM forwards the route request to the CICM.
3. In this example the call is sent to a Network VRU for call treatment first. The NAM sends an instruction to the switching network through Routing Client 0 to connect the call to a Network VRU.
4. The switching network connects the call to a Network VRU.
5. The Network VRU asks the NAM for instructions. Unified ICM script execution continues at this point.
6. Unified ICM, through the NAM, instructs the Network VRU to execute a certain VRU script.
7. The Network VRU responds back to the NAM and CICM that VRU script execution is completed. Steps 6 and 7 can be repeated any number of times under control of the CICM script.
8. Once the CICM is done with VRU treatment and reaches a point in the script where a destination is selected. 8a) An instruction is sent to the switching network through Routing Client 0 to connect the call to the selected target (destination 1). If a translation route is used to reach the selected target, step 8b) is performed: Unified ICM sends a message to the target's PG with the call context information of the call.
9. The switching network tears down the connection to the Network VRU and connects the call to the selected destination 1.
10. If a translation route was used the ACD will recognize this and request the PG for the call context and the target for the call.
11. The PG responds with the requested information.
12. The ACD connects the call to the agent and the agent answers the call and speaks with the caller.

    At this point the actual network transfer starts.

13 The agent requests a call transfer, in this example through the ACD hard phone.

14 This request is sent to the CICM. The CICM executes a routing script and the script selects a destination for the call, destination 2.

15 An instruction is sent through the NAM and Routing Client 0 to the switching network to transfer the call.

16 The network will tear down the call to destination 1 and reconnect the caller to destination 2.

Call flow generalizations

The following generalizations can be made to this specific call flow example:

- It is not required to use a Network VRU in order to perform a network transfer. Steps 3 through 7 can be omitted.
- Any type of Network VRU can be used with this call flow, except Type 2 VRUs. Using different Network VRU types changes the specific call flow slightly, of course.
- If a device target is used for destination 1, steps 8b, 10 and 11 do not happen.
- If the agent is using a softphone or CTI desktop application to initiate the transfer, step 13 is slightly different.

Detailed requirements

The following are detailed requirements in order to make a network transfer happen. If these requirements are not met, either a local transfer will happen or no transfer will happen at all.

- A call is pre-routed by a routing client that supports the network transfer capabilities (see next section for details on which routing clients support network transfer).
- The call is pre-routed to either a device target or translation routed to a peripheral target (“the target”). A device target would typically be an IPCC agent. A peripheral target would be an agent on a TDM ACD or a customer premise VRU system that is connected to Unified ICM using the Call Routing interface. The latter means that a VRU system can request a network transfer in the same way that an agent can, for example, to network transfer the call from the VRU to an agent. Note that Network VRUs that are connected using the Service Control Interface do not support requesting network transfers in this way, but that these VRUs use other mechanisms to transfer a call from the VRU to an agent.
- The call is answered by the target. Network transfer only happens after the target has answered the call, and not before, for example, while the agent phone is still ringing.
- The target indicates that the call needs to be transferred to a specific dialed number. This can be done in two ways: either through the target's softphone or CTI desktop, or through the target's hard phone. In the former case the agent needs to indicate to what destination he wants to transfer the call (typically a number). This will trigger the softphone or CTI application to send a route request to the CICM. In the latter case the agent puts the caller on hold and dials an ACD extension, which needs to trigger the ACD to send a route request to the CICM, typically with the extension as the dialed number. Note that not all ACDs support the hard phone initiated transfer.

  In case the peripheral target is a VRU connected to the CICM using the Call Routing interface, the VRU would send a route request message to the CICM using the Call Routing interface.

- The CICM receives the route request and executes the routing script scheduled for the dialed number received with the route request. The script will select a target to transfer the call to.
- The CICM will send a label for the selected target to the routing client that pre-routed the call in step 2), if all of the following three conditions are true:
    - The selected target has a label for the routing client that pre-routed the call. Typically this would be the INCRP NIC on the CICM that is mapped to the routing client on the NAM. If the Label node is used, this condition is true if the Label node has a label for the routing client or if a dynamic label is used.
    - Both the CICM and NAM script that pre-routed this call in steps 1) and 2) have set the NetworkTransferEnabled flag to 1 (for blind transfer only) or 2 (for both consultative and blind transfer), using a Set node. This requirement allows the service provider controlling the NAM script to allow or disallow the CICM customer the use of the network transfer feature. It also allows the CICM customer controlling the CICM script to allow or disallow its agent to transfer calls.
    - If the selected target also has a label for the PG that requested this transfer ("local label") or, when using a label node, the label node also has a local label, the PG needs to have the "Network Transfer Preferred" flag set in the Routing Client tab of the Peripheral configuration using PG Explorer. If this flag is not set, the CICM will pick the local label and a local transfer will be executed.

The routing client that originally pre-routed the call will receive a connect message from the NAM/CICM and will pass it on to the switching device. The switching device will tear down the call to the initial target and re-connect the caller to the new destination.

Supported configurations

Routing clients

Only the following NAM routing clients support network transfer:

- CRSP NIC
- SS7 IN NIC
- VRU PG
- INCRP NIC (An INCRP NIC is the NIC between the NAM and a CICM. Even though the INCRP NIC supports network transfer, the capability of executing a network transfer ultimately depends on the NAM routing client.)

Multiple subsequent network transfers

It is possible to network transfer a call to another agent, who can subsequently network transfer the call again. This process can be repeated any number of times. In order for an agent who has received a call through network transfer to be able to network transfer the call again, all the conditions in the section Detailed Requirements need to be met, with the following amendments:

- The agent who first receives a call through network transfer can only network transfer the call again if the routing script that executes the transfer has a Set node that sets the NetworkTransferEnabled flag to 1 or 2 again. This allows the next agent who receives the call to network transfer the call again.
- The agent who first receives a call through network transfer needs to be a device target or a peripheral target reached using translation routing. In general only an agent or VRU can network transfer a call if it is a device target or a peripheral target reached using translation routing. Note that a call can be network transferred to any sort of destination supported by a CICM, such as Labels, Divert Labels, Scheduled Targets, etc., but that only device targets or peripheral targets reached using translation routing can subsequently transfer the call again.

Call context

When a call is network transferred from an agent or VRU to another destination, Unified ICM call context is transferred as well.

Route Call Detail and Termination Call Detail records

A normal pre-route to an agent will generate the following Route Call Detail (RCD) and Termination Call Detail (TCD) records:

- RCD in the NAM. The RouterCallKeySequenceNumber is 0.
- TCD in the NAM for the VRU treatment, in case the call is handled by a Network VRU connected to the NAM or in case the VRU is the routing client. If the VRU is not the routing client, this TCD record has a RouterCallKey that is equal to the NAM RCD RouterCallKey. If the VRU is the routing client, this TCD record has a RouterCallKey that is equal to the RouterCallKey of the NAM RCD for the transfer request (see below). If the call is transferred multiple times the TCD RouterCallKey is equal to the last NAM RCD RouterCallKey. The RouterCallKeySequenceNumber is 1 in all cases.
- RCD in Unified ICM. The RouterCallKey is identical to the other Unified ICM TCD and RCD records for this call. The RouterCallKeySequenceNumber is 0.
- TCD in Unified ICM for the agent connection. The RouterCallKeySequenceNumber is 1. The RouterCallKey is identical to the other Unified ICM TCD and RCD records for this call.

A network transfer will generate the following Route Call Detail and Termination Call Detail records:

- RCD in the NAM for the transfer request. Note that this RCD represents the routing decision generated by Unified ICM, passed back through the NAM to the routing client. This RCD has a new RouterCallKey (it is not related to the RCD records generated when the call was pre-routed) and the RouterCallKeySequenceNumber is 0.
- TCD in the NAM for the VRU treatment (if that happens before the transfer), in case the VRU is not the routing client (if the VRU is the routing client, there is only one TCD record; see above). This record has a RouterCallKey that is equal to the NAM RCD for the transfer request. The RouterCallKeySequenceNumber is 1.
- RCD in Unified ICM for the transfer request. The RouterCallKey is identical to the other Unified ICM TCD and RCD records for this call. For the first network transfer, the RouterCallKeySequenceNumber is 2. For each subsequent network transfer the RouterCallKeySequenceNumber is incremented by 2 (for example, 4, 6, and so on).

- TCD in Unified ICM for the call from the transferring agent to the other agent. When doing a Blind Network Transfer, this call leg never happens, but Unified ICM generates a TCD for it anyway. This TCD has the CallTypeID field set to –1. The RouterCallKey is identical to the other Unified ICM TCD and RCD records for this call. For the first Blind Network Transfer, the RouterCallKeySequenceNumber is 2. For subsequent Blind Network Transfers, the RouterCallKeySequenceNumber is incremented by 2 (for example, 4, 6 and so on). For the first Network Consultative Transfer, the RouterCallKeySequenceNumber is 3. For subsequent Network Consultative Transfers, the RouterCallKeySequenceNumber is incremented by 2 (for example, 5, 7, and so on).
- This TCD is present only if the call is transferred to a device target or peripheral target.
- TCD in Unified ICM for the new transferred call from the caller to the agent. For both Blind and Network Consultative Transfers, the RouterCallKey is identical to the other Unified ICM TCD and RCD records for this call. The RouterCallKeySequenceNumber is 3 (for the first network transfer; if this is for a subsequent network transfer, the RouterCallKeySequenceNumber is set to the next odd number, such as 5, 7, etc.). This TCD is present only if the call is transferred to a device target or peripheral target.

Note that the Unified ICM RouterCallKey is different from the NAM RouterCallKey. If records need to be correlated between the NAM and Unified ICM, the NAM can insert its RouterCallKey in one of the call variables (using a Set node in the NAM script). This value will then be populated in the call variable field for all NAM and Unified ICM RCD and TCD records. It can then be used to link all records together.

Network transfer configuration

The following is a high level check list as to what needs to be configured to support network transfer. The starting point is a configuration that supports pre-routing to device targets (IPCC agents) or translation routing to peripheral targets (TDM ACD agents or a VRU).

To configure the NAM/CICM for network transfer, perform the following steps:

- On the NAM and CICM add a Set node to the routing script that pre-routes the calls to the device target or peripheral target. The Set node must set the call context variable NetworkTransferEnabled to 1 or 2.
- On the CICM, configure Dialed Number, Call Type and routing script to handle the transfer request.
- On the CICM, configure Labels for the device targets and Translation Route Labels for peripheral targets that need to receive network transferred calls. In general these configurations would be identical to what would be needed to pre-route calls to these targets. Make sure these labels have as routing client the INCRP NIC that is mapped to the NAM routing client that pre-routes the calls.
- If the targets for network transferred calls also have “local” labels (labels with the CICM ACD PG as routing client), use PG Explorer on the CICM to set the “Network Transfer Preferred” check box on the Routing Client tab of the ACD PG.
- If required, configure the Labels on the NAM as well.

CHAPTER 10

Network VRU

This chapter describes the concepts, architecture, configuration and operations of Network Voice Response Units (VRUs) in a NAM/CICM environment. VRU types are discussed in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted.

Network VRU concept

A Network VRU is a Voice Response Unit that is controlled by the NAM or by the CICMs connected by the NAM for the purpose of diverting a call to the VRU for voice treatment, such as prompting and queuing, before connecting the call to a call center agent. The NAM or CICM routing script contains explicit instructions for the VRU to execute and the VRU will report the result back to the NAM/CICM. This mechanism is used for various applications, such as:

- Prompting the customer using multiple menus to determine the purpose of the call in order to route the call to the applicable agent group.
- Collecting customer data (for example, an account number), which can then be used by the CICM to lookup the customer in a database and take routing decisions, based on the customer's status and provide data to a CTI application, so that the agent can have a screen pop-up with the customer data when he answers the call.
- Providing complete “self-help” interactive voice response applications under control of the CICM, including database lookups and voice responses back to the customer, such as account balance lookups or complete business transactions. In this case, the caller might never leave the VRU to be connected to an agent, or they might indicate a desire to speak to an agent, in which case the data retrieved using the VRU system and the state of the transaction can be made available to the agent's desktop application using CTI.

- Providing recorded announcements during queuing. Information can be provided on the customer's status in the queue, expected delay times, alternative options, such as a self help VRU application, leaving a voice message, and so on.

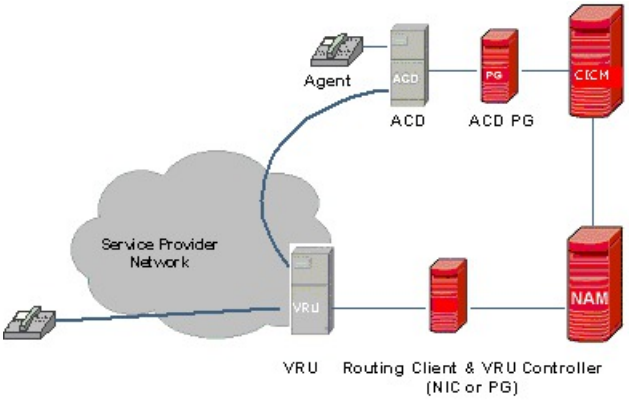
Network VRU architecture

There are several different architectures for NAM-based Network VRU solutions. The following questions determine which one is applicable:

1. Is the Network VRU acting as the routing client as well, or is there a separate routing client?

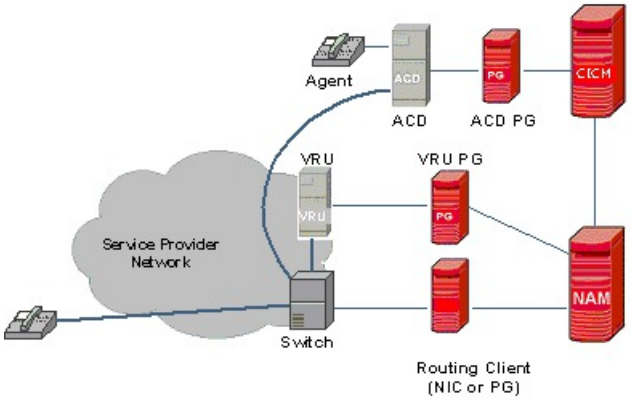
   The scenario where the VRU is acting as the routing client for the call, as well as the voice response function itself, is called a Service Node implementation. The following figure gives the basic architecture. The VRU is used for both prompting/queuing the call as well as for connecting the call to the call center agent.

Figure 27: Service Node Implementation



The alternative scenario where there is a separate routing client that switches the call to the VRU and later to an agent is shown in the figure below. In this case, the routing client is connected to a switching device that switches the call to the VRU and the agent.

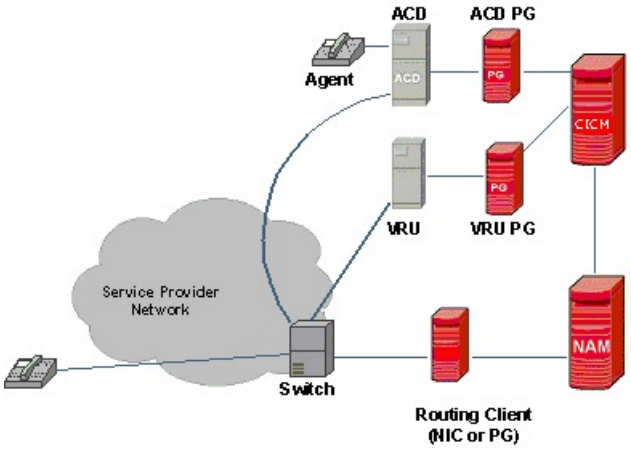
Figure 28: Network VRU Implementation with Separate Routing Client



2 If there is a separate routing client, is the VRU connected to the NAM or to a CICM instance?

Both scenarios shown above have the VRU connected to the NAM, but the VRU can also be connected to the CICM. Typically, “Network” VRUs connected to a CICM would be customer specific VRUs physically located on the customer premises rather than a shared network resource, but from a NAM/CICM point of view they are still called Network VRUs, due to the fact that the capabilities are virtually identical to a “real” network VRU connected to the NAM. The following figure shows a basic architecture with a VRU connected at Unified ICM.

Figure 29: Network VRU at Customer Premises, Connected to Cisco Unified Intelligent Contact Management Instead ofthe NAM



One of the most significant differences between a network-hosted VRU (connected to the NAM) and a customer premise-hosted VRU (connected to the CICM) is the correlation mechanism used. The correlation mechanism takes care of uniquely identifying the same call across the two dialogs that the NAM/CICM maintains for each call, one with the routing client and the other with the VRU Peripheral Gateway.

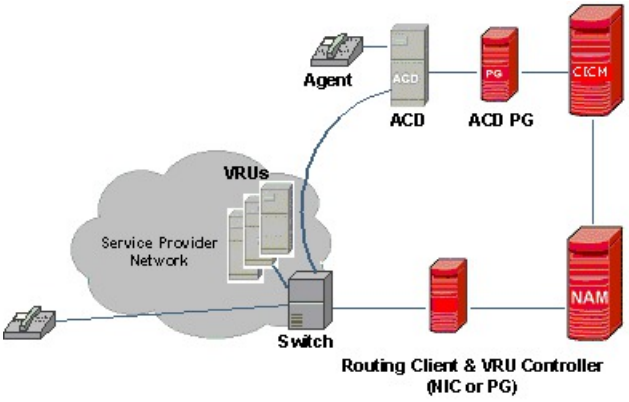
Network-hosted VRUs can generally use a simple correlation id that can be passed along with the call, whereas premise hosted VRUs are typically connected through the PSTN network that cannot transport a correlation ID directly. In that case a translation route mechanism is used to correlate the calls.

3 What capabilities does the routing client have to divert calls to a VRU and take them back later in order to connect the call to an agent?

The answer to this question does not influence the architecture so much, but it does impact the call flow. There are many variations in routing client capabilities and they will be explained in detail in the next section.

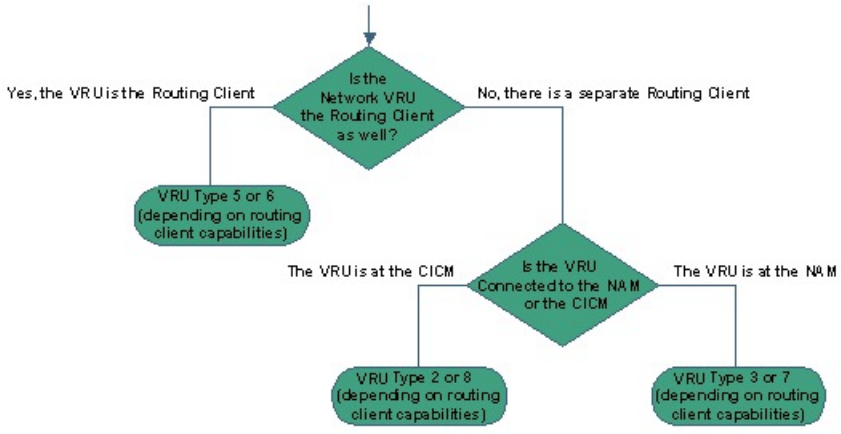
The following figure shows an example of a slight variation of the Service Node architecture shown in this section, where the routing client has the capability of switching the call to different VRUs that are all controlled through the same dialog with the NIC or PG.

Figure 30: Example of a Service Node Implementation with Additional Routing/Switching Capabilities



The first two questions lead to the following decision tree:

Figure 31: Decision flow for different Network VRU architectures



The resulting end points of the tree known as VRU Types 2, 3, 5, 6, 7 or 8, are internal NAM/CICM representations of different Network VRU architectures. Each end point has two Network VRU types listed (5/6, 2/8 and 3/7, respectively) and the choice between the two depends on the third question above:

the routing client capabilities. The next section describes the different call flows and the differences between the types in detail.

Call flows

The call flow diagrams in this section do not indicate details on the ACD connected to the CICM, since the VRU part of the call flow is independent of the actual final destination of the call. It might be an agent on an ACD connected to the CICM, but it could be any destination, for example a Scheduled Target or even just a destination phone number selected by the Label node. The call flows also abstract, where immaterial, from whether the VRU control is done by the NAM or the CICM.

Type 3 and 7 VRU call flows

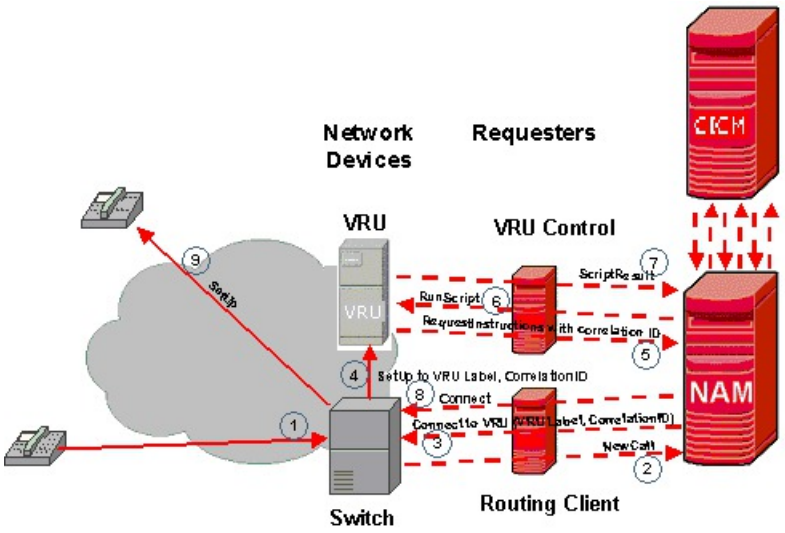
The type 3 and 7 VRU call flows are for Network VRUs connected at the NAM, where there is a separate (NIC or PG) routing client. The difference between types 3 and 7 is in how the routing client handles taking the call away from the VRU after the VRU treatment and connecting it to an agent.

The routing client in a type 3 or type 7 Network VRU architecture can be either a NIC or a VRU PG (VRU PG is supported as routing client from NAM Release 4.6.2 or later). An ACD PG routing client does not support the type 3 or 7 network VRU call flow.

Note that when the Routing Client is a VRU PG, the switching device connected to the routing client VRU PG is completely independent of the Network VRU itself; even though they could both be VRUs. The switching device is just performing a switching function. Some special configuration instructions are applicable for this case. It is of course possible that the switching device itself is a VRU that can perform VRU functions. In that case, there are two Network VRUs in the configuration. The switching device would be a type 5 or type 6 VRU.

Type 3 Call Flows

Figure 32: Type 3 Call Flow

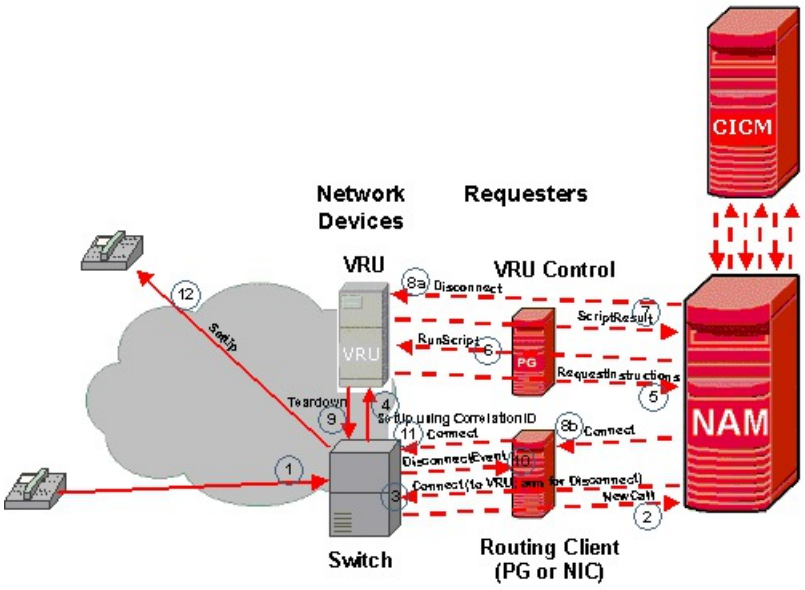


The type 3 call flow is as follows:

1. Caller dials a number that causes the switch to query the NAM.
2. Switch queries the NAM/CICM (VRU control can be scripted in either the NAM or the CICM, or both).
3. A NAM or CICM routing script executes and hits a *SendToVRU* node. NAM instructs the switch to connect the call to the VRU, using a Network VRU label and a correlation number.
4. The switch connects the call to the VRU using the label and passing along the correlation number.
5. When the call arrives, the VRU asks the NAM or CICM for instructions and it sends the correlation number along with the request. This allows the NAM or CICM to identify the call and continue script processing.
6. The NAM or CICM script hits a RunExternalScript node and sends an instruction to the VRU to run a certain Network VRU script.
7. When done, the VRU reports the result back to the NAM. The result might include digits collected from the caller. The NAM or CICM script continues and steps 6 and 7 might be repeated any number of times.
8. When the NAM or CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the NAM instructs the switch to take the call away from the VRU (that is, tear down the call leg setup in step 4) and connect the call to the selected destination. The dialog between the NAM and the Network VRU is now terminated.
9. The switch connects the call to the new destination.

Type 7 Call Flows

Figure 33: Type 7 Call Flow



The type 7 call flow is identical to the type 3 call flow up to step 8, where the call is taken away from the VRU and connected to a destination. The type 7 Network VRU is for routing clients who do not support the

capability to receive instructions from the NAM asynchronously (that is, without the switch asking for instructions) to take the call away from the VRU and connect it to a destination.

Instead, the NAM instructs the VRU to drop the call, upon which the switch will report this to the NAM and the NAM can send the instruction with the new destination.

The type 7 call flow is as follows:

1. Caller dials a number that causes the switch to query the NAM.
2. Switch queries the NAM/CICM (VRU control can be scripted in either the NAM or the CICM or both).
3. A NAM or CICM routing script executes and hits a SendToVRU node. NAM instructs the switch to connect the call to the VRU, using a Network VRU label and a correlation number. In order for step 10 to happen, the NAM will typically have to instruct the switch at this point in time that the switch must return control to the NAM in case the call leg to the VRU is disconnected.
4. The switch connects the call to the VRU using the label and passing along the correlation number.
5. When the call arrives, the VRU asks the NAM for instructions and it sends the correlation number along with the request. This allows the NAM or CICM to identify the call and continue script processing.
6. The NAM or CICM script hits a RunExternalScript node and sends an instruction to the VRU to run a certain Network VRU script.
7. When done, the VRU reports the result back to the NAM. The result might include digits collected from the caller. The NAM or CICM script continues and steps 6 and 7 might be repeated any number of times.
8. When the NAM or CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the NAM does two things:
   - it instructs the VRU to disconnect the call and
   - it instructs the routing client to connect the call to the selected destination. The routing client will not (can not) pass this instruction along to the switch asynchronously and holds onto the instruction until the switch reports back to the routing client.
9. The VRU drops the call.
10. The Switch reports this event to the routing client, keeping the originating leg of the call (that is, to the caller) open.
11. The routing client now sends the instruction to the switch to connect this call to its new destination.
12. The routing client now sends the instruction to the switch to connect this call to its new destination.

Type 2 and type 8 call flows

The type 2 and 8 VRU call flows are for Network VRUs connected at the CICM. The difference between types 2 and 8 lies in how the routing client handles taking the call away from the VRU and connecting it to an agent.

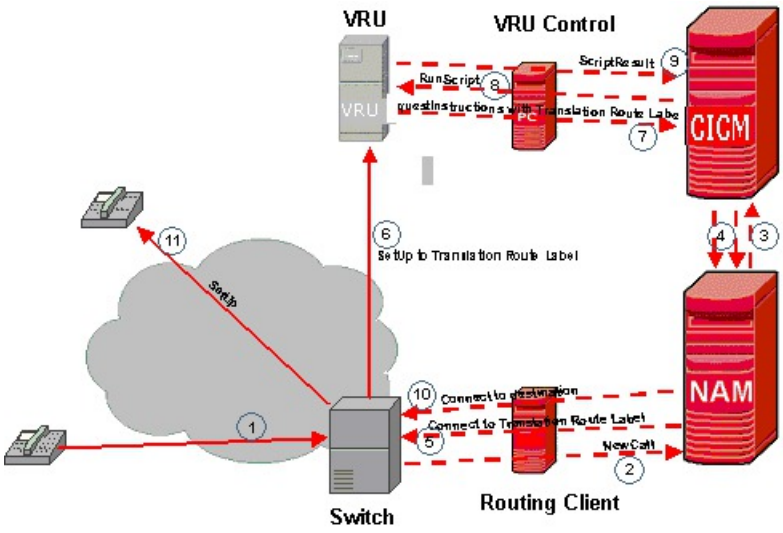
Note that when the Routing Client is a VRU PG, this switching device is completely independent of the Network VRU itself. The switching device is just performing a switching function. Some special configuration instructions are applicable for this case. It is of course possible that the switching device itself is a VRU that

can perform VRU functions. In that case, there are two Network VRUs in the configuration. The switching device would be a type 5 or type 6 VRU.

Type 8 Call Flows

The routing client in a type 8 Network VRU architecture can be either a NIC or a VRU PG. An ACD PG routing client does not support type 8.

Figure 34: Type 8 Call Flow



The type 8 call flow is as follows:

1. Caller dials a number that causes the switch to query the NAM.
2. The switch queries the NAM.
3. The NAM forwards the request to a CICM (VRU control needs to be scripted in the CICM with this Network VRU type).
4. A CICM routing script executes and hits a *TranslationRouteToVRU* node. The CICM instructs the NAM to connect the call to the VRU, using a translation route label.
5. The NAM instructs the switch to connect the call to the translation route label.
6. The switch connects the call to the VRU using the translation route label.
7. When the call arrives, the VRU asks the CICM for instructions. The VRU sends the translation route label along with the request. The translation route label functions as the correlation ID. It allows the CICM to uniquely identify the call and continue script processing.
8. The CICM script executes a RunExternalScript node and sends an instruction to the VRU to run a certain Network VRU script.
9. When done, the VRU reports the result back to the CICM. The result might include digits collected from the caller. The CICM script continues and steps 8 and 9 might be repeated any number of times.
10. When the CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the CICM instructs the NAM and the NAM in turn instructs the switch to tear down

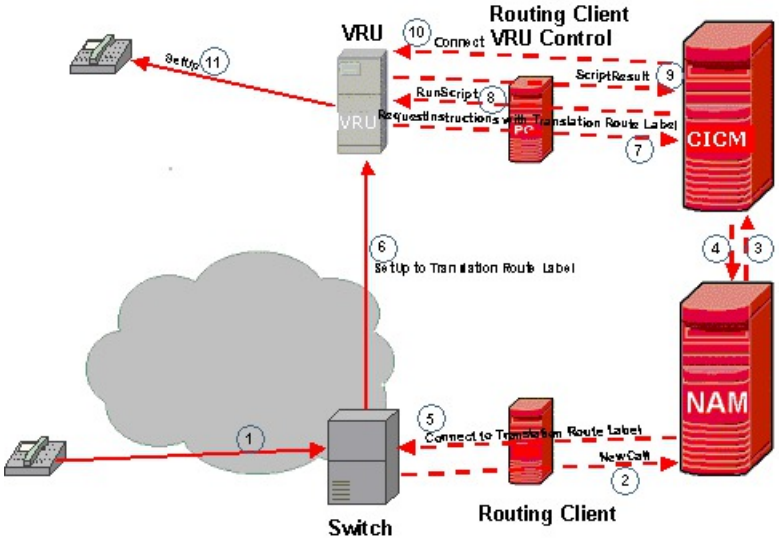
the connection to the VRU and to connect the call to the selected destination. The dialog between the CICM and the Network VRU is now terminated.

11 The VRU connects the call to the new destination.

Type 2 Call Flows

The routing client in a type 2 Network VRU architecture can be either a NIC, a VRU PG, or an ACD PG routing client.

Figure 35: Type 2 Call Flow



The type 2 call flow is identical to the type 8 call flow up to step 10, where the call is taken away from the VRU and connected to a destination. The type 2 Network VRU is for routing clients who do not support the capability to receive requests from the NAM without the switch asking for instructions to take the call away from the VRU and connect it to a destination. Instead, the CICM instructs the VRU to connect the call to the new destination. This call flow is typically used in situations where the call needs to be connected to an ACD that is in the same location as the VRU, if the VRU has good capabilities to switch the call to the ACD.

The type 2 call flow is as follows:

1 Caller dials a number that causes the switch to query the NAM.

2 The switch queries the NAM.

3 The NAM forwards the request to a CICM (VRU control needs to be scripted in the CICM with this Network VRU type).

4 A CICM routing script executes and hits a *TranslationRouteToVRU* node. The CICM instructs the NAM to connect the call to the VRU, using a translation route label.

5 The NAM instructs the switch to connect the call to the translation route label.

6 The switch connects the call to the VRU using the translation route label.

7 When the call arrives, the VRU asks the CICM for instructions and it sends the translation route label along with the request. The translation route label functions as the correlation ID. It allows the CICM to uniquely identify the call and continue script processing.

8 The CICM script executes a RunExternalScript node and sends an instruction to the VRU to run a certain Network VRU script.

9 When done, the VRU reports the result back to the CICM. The result might include digits collected from the caller. The CICM script continues and steps 8 and 9 might be repeated any number of times.

10 When the CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the CICM instructs the VRU to connect the call to the selected destination. The dialog between the CICM and the NAM/routing client is now terminated and the VRU becomes the new routing client for the call.

11 The VRU connects the call to the new destination.

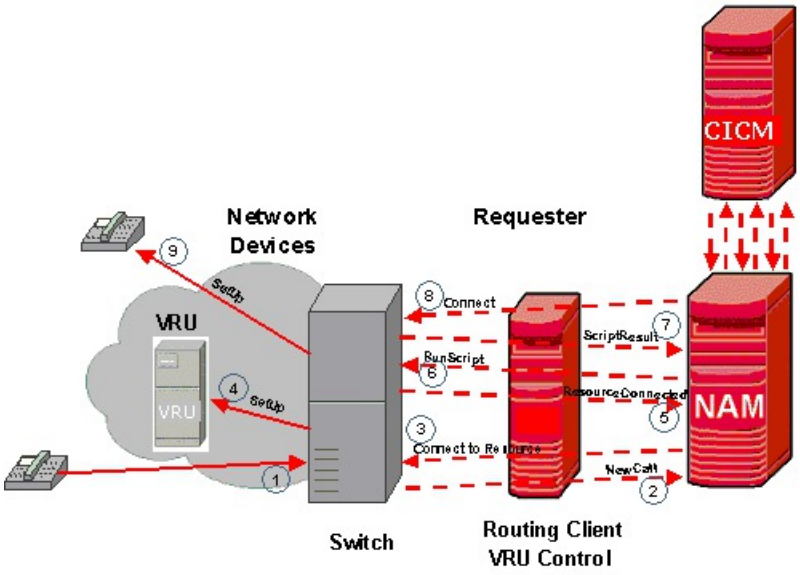
Type 5 and type 6 call flows

The type 5 and 6 VRU call flows are for Network VRUs connected at the NAM, where the VRU is also the switching device, so that there is a single “requester” acting as the routing client and the VRU controller at the same time. This requester in a type 5 or type 6 Network VRU architecture can be either a NIC or a VRU PG. An ACD PG is not supported in this case, since it does not support VRU control.

The difference between Network VRU call flows of type 5 and type 6 lies in whether the routing client needs explicit instructions to connect the call to the VRU (type 5) or not (type 6). The fact that explicit instructions are used with type 5 to connect the call to the VRU resource implies that the VRU might have different (types of) VRU resources available and that the NAM/CICM can control which ones are being used. With a type 6 Network VRU it is simply assumed that there is a single VRU available that can be used.

Type 5 Call Flows

Figure 36: Type 5 Call Flow

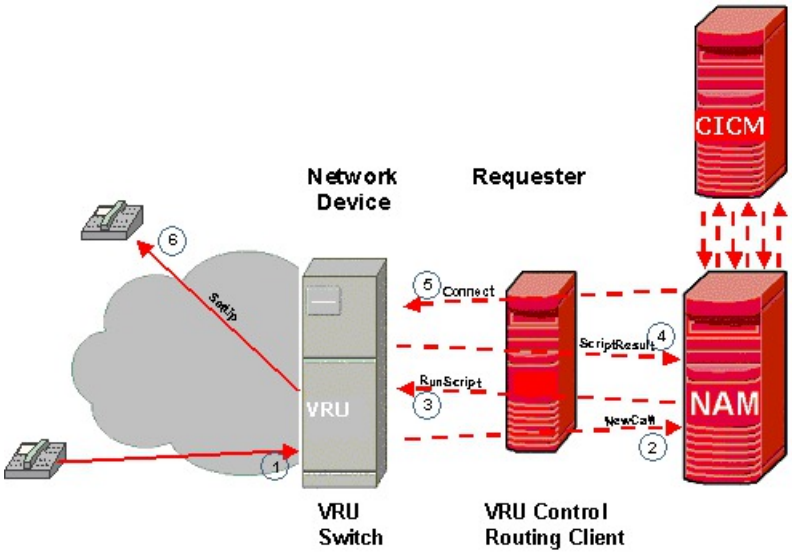


The type 5 call flow is as follows:

1. Caller dials a number that causes the switch/VRU to query the NAM.
2. The switch/VRU queries the NAM/CICM (VRU control can be scripted either in the NAM or the CICM or both).
3. A NAM or CICM routing script executes and hits a SendToVRU node. NAM instructs the switch/VRU to connect the call to the VRU resource, using a Network VRU label. No correlation mechanism is required, since the NAM will only have one dialog with the routing client/VRU controller for the call control as well as the VRU control.
4. The switch/VRU connects the call to the (internal) VRU resource using the label. Depending on whether the switch and the VRU are actually different devices, this step might contain real activity or not. In any case, the activity is invisible to the NAM.
5. When the call is connected to the VRU, the switch/VRU acknowledges this to the NAM and asks the NAM for instructions.
6. The NAM or CICM script hits a RunExternalScript node and sends an instruction to the VRU to run a certain Network VRU script.
7. When done, the VRU reports the result back to the NAM. The result might include digits collected from the caller. The NAM or CICM script continues and steps 6 and 7 might be repeated any number of times.
8. When the NAM or CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the NAM will instruct the switch/VRU to connect the call to the selected destination.
9. The switch/VRU will connect the call to the new destination.

Type 6 Call Flows

Figure 37: Type 6 Call Flow



The type 6 call flow is identical to the type 5 call flow, except that steps 3, 4 and 5 are omitted: the NAM does not send explicit instructions to the VRU to connect the call to a VRU resource, assuming that the VRU is ready to receive VRU control instructions.

The type 6 call flow is as follows:

1. Caller dials a number that causes the switch/VRU to query the NAM.
2. Switch/VRU queries the NAM/CICM (VRU control can be scripted in either the NAM or the CICM or both).
3. A NAM or CICM routing script executes and executes a *SendToVRU* node and a subsequent *RunExternalScript* node and sends an instruction to the VRU to run a certain Network VRU script.
4. When done, the VRU reports the result back to the NAM. The result might include digits collected from the caller. The NAM or CICM script continues and steps 3 and 4 might be repeated any number of times.
5. When the NAM or CICM script hits a script node that selects a destination for the call, such as a Select, Label, Scheduled Select node, or when the CICM is already queuing the call using a Queue node and an agent becomes available, the NAM instructs the switch/VRU to connect the call to the selected destination.
6. The switch/VRU connects the call to the new destination.

Configuration

This section deals with NAM/CICM configuration using the Configuration Manager and Script Editor only. It does not cover using the Web Setup tool to configure NICs and PGs, since this is completely independent of Network VRU type architectures.

The configuration guidelines in this section assume that the VRU scripting is done in the CICM. If the scripting is only done in the NAM, no configuration is required in the CICM. Note that this is not an option with type 2 and 8. If scripting is to be done on both the NAM and the CICM, it is noted when this requires additional NAM configuration.

Configuration Manager

The following sections provide procedures for configuring the various VRU types.

Configure type 3 and type 7

Procedure

Step 1 Using Network VRU Explorer, define a Network VRU of type 3 or type 7. Also define one Label of Type Normal. The label must be set to whatever the switch needs to connect the call to the VRU. Do this in both the NAM and the CICM. Make sure the Network VRU labels are identical in the NAM and CICM. Make the Network VRU Names identical as well, to avoid confusion. In the NAM configuration, choose whatever the applicable Routing Client is for the Label. In the CICM configuration choose the INCRP routing client that is mapped to the applicable NAM routing client.

Step 2 On the NAM, using PG Explorer, define a PG and one Peripheral for each VRU connected to this PG. For the Logical Controller, select Client Type “VRU”. For the Peripheral, select Client Type “VRU” and check the **Enable Post Routing** checkbox. On the Advanced tab, for Network VRU, select the type 3 or 7 Network VRU name as configured above. On the Routing Client tab, select Client Type “VRU”.

Step 3 On the NAM, using System Information, set the maximum and minimum correlation number to the required values. The NAM will go through the range of correlation numbers sequentially. For example, if the correlation number needs to be any 4 digits, not starting with 0, the applicable range would be from 1000 to 9999.

Step 4 On the CICM, using System Information, set Default Network VRU to the Network VRU defined in Step 1.

Step 5 The configuration under step 4 is sufficient if a single Network VRU is configured that is used for all calls handled by this CICM. If calls handled by this CICM need to be treated on different Network VRUs, dependent on the Dialed Number, configure the following on the CICM:

- Configure Customers, using Instance Explorer and associate each Customer with a Network VRU.
- Using Dialed Number List, associate each Dialed Number with a Customer as configured above. Calls for this Dialed Number will use the Network VRU associated with its Customer. If such association does not exist, the default Network VRU, as configured under step 4, is used.

This step is required for CICM instances that are shared by multiple customers, known as Advanced Services, even if there is only a single Network VRU for all customers.

Step 6 If NAM routing scripts need to control VRU interaction as well, set, using System Information, the Default Network VRU to the Network VRU defined in Step 1. If multiple Network VRUs are configured, define Customers associated with a Network VRU and associate Dialed Numbers with Customers, as described above for the CICM under step 5.

Configure type 6

Procedure

Step 1 Using Network VRU Explorer, define a Network VRU of type 6. Do this in both the NAM and the CICM. Make the Network VRU Names identical, to avoid confusion.

Step 2 On the NAM, using PG Explorer, define a PG and one Peripheral for each VRU connected to this PG. For the Logical Controller, select Client Type “VRU”. For the Peripheral, select Client Type “VRU” and check the **Enable Post Routing** checkbox. On the Advanced tab, for Network VRU, select the type 6 Network VRU name as configured above. On the Routing Client tab select Client Type “VRU” and, for Network Routing Client, fill in a unique name; for example, use the Routing Client name.

Step 3 On the CICM, using NIC Explorer, select the INCRP NIC and its Routing Client. In the Routing Client tab, make sure the Client Type is set to “VRU”. In the Network Routing Client field, fill in the unique name used for the VRU PG Routing Client on the NAM.

Step 4 On the CICM, go back to the Network VRU Explorer. Select the Network VRU with an ID less than 1 and configure a Label of type Normal for this Network VRU. The Routing Client for the Label needs to be the INCRP Routing Client mentioned under 3. The contents of the Label itself are irrelevant, but it needs to exist and it needs to be identical to the Network VRU Label configured on the NAM in step 5.

Step 5 On the NAM, go back to the Network VRU Explorer, select the Network VRU with an ID less than 1 and configure a Label of type Normal for this Network VRU. The Routing Client for the Label needs to be the Routing Client with an ID less than 2. The contents of the Label itself are irrelevant, but it needs to exist and it needs to be identical to the Network VRU Label configured on the CICM in step 4.

Configure type 5

Procedure

Step 1 Using Network VRU Explorer, define a Network VRU of type 5. Do this in both the NAM and the CICM. Make the Network VRU Names identical as well, to avoid confusion.

Step 2 On the NAM, using PG Explorer, define a PG and one Peripheral for each VRU connected to this PG. For the Logical Controller, select Client Type “VRU”. For the Peripheral, select Client Type “VRU” and check the **Enable Post Routing** checkbox. On the Advanced tab, for Network VRU, select the type 5 Network VRU name as configured above. On the Routing Client tab, select Client Type “VRU” and, for Network Routing Client, fill in a unique name, for example use the Routing Client name.

Step 3 On the CICM, using NIC Explorer, select the INCRP NIC and its Routing Client. In the Routing Client tab, make sure the Client Type is set to “VRU”. In the Network Routing Client field fill in the unique name used for the VRU PG Routing Client on the NAM.

Step 4 On the CICM, go back to the Network VRU Explorer, select the Network VRU with an ID less than 1 and configure a Label of type Normal for this Network VRU. The Routing Client for the Label needs to be the INCRP Routing Client mentioned under 3. The Label needs to be set to whatever the VRU needs to connect

to an internal VRU resource and it needs to be identical to the Network VRU Label configured on the NAM in step 5.

Step 5 On the NAM, go back to the Network VRU Explorer, select the Network VRU with an ID less than 1 and configure a Label of type Normal for this Network VRU. The Routing Client for the Label needs to be the Routing Client configured less than 2. The Label needs to be set to whatever the VRU needs to connect to an internal VRU resource and it needs to be identical to the Network VRU Label configured on the CICM in step 4.

Step 6 On the CICM, using System Information, set Default Network VRU to the Network VRU defined in Step 1.

Step 7 The configuration under step 4 is sufficient if a single Network VRU is configured that is used for all calls handled by this CICM. If calls handled by this CICM need to be treated on different Network VRUs, dependent on the Dialed Number, configure the following on the CICM:

- Configure Customers, using Instance Explorer and associate each Customer with a Network VRU.
- Using Dialed Number List, associate each Dialed Number with a Customer as configure above. Calls for this Dialed Number will use the Network VRU associated with its Customer. If such association does not exist, the default Network VRU, as configured under step 4, is used.

Note that the only effect of the configuration under steps 6 and 7 is the label sent by the NAM in the ConnectToResource message to the switch/VRU. It does not affect actual type 5 Network VRU selection, since the VRU is selected by the network that delivers the call to the VRU in the first place. However, it can affect the selection of using a type 3 or 7 network VRU if both are present.

This step is required for CICM instances that are shared by multiple customers, known as Advanced Services, even if there is only a single Network VRU for all customers.

Step 8 If NAM routing scripts need to control VRU interaction, set, using System Information, the Default Network VRU to the Network VRU defined in Step 1. If multiple Network VRUs are configured, define Customers associated with a Network VRU and associate Dialed Numbers with Customers, as described above for the CICM in step 7.

Configure type 2 and type 8

Procedure

Step 1 On the CICM, using Network VRU Explorer, define a Network VRU of type 2 or type 8.

Step 2 On the CICM, using PG Explorer, define a PG and one Peripheral for each VRU connected to this PG. For the Logical Controller, select Client Type “VRU”. For the Peripheral, select Client Type “VRU” and check the **Enable Post Routing** checkbox. On the Advanced tab, for Network VRU, select the type 2 or 8 Network VRU name as configured above. On the Routing Client tab, select Client Type “VRU”.

Step 3 On the CICM, define a Translation Route for the VRU Peripheral. This includes the following components.

- Using Service Explorer, configure a Service and a Route for each VRU Peripheral.
- Using Network Trunk Group Explorer, configure, for the VRU PG, a Network Trunk Group, one or more Trunk Groups for each Peripheral and one or more Trunks for each Trunk Group, depending on the VRU trunk configuration. Make sure that the Trunk Group Name and Number are identical to what is configured in the VRU system itself.

- Using Translation Route Explorer, configure, for the VRU PG, a Translation Route of Type DNIS. For the Translation Route, configure as many Routes as are required. Configure one route for each Translation Route Label needed. For each Route, select the Service configured above. For each Route, configure one or more Peripheral Targets. For DNIS use the Dialed Number that the VRU will return with the Request Instruction message. Typically this is equal to the Translation Route Label or is just the last 10 digits of the Translation Route Label, depending on the network setup. For Network Trunk Group, select one from the ones configured above. For each Peripheral Target, configure a Translation Route Label of Type Normal. The Routing Client for the Label is the INCRP Routing Client that is mapped to the applicable NAM Routing Client.

Step 4 On the NAM, using Network VRU Explorer, define a Network VRU of type 2 or type 8. Give it the same name as the type 2 or type 8 Network VRU configured with an ID less than 1. Also configure a number of Labels of Type Normal. Select whatever the applicable NAM Routing Client is for the Label. Configure a Label for each Translation Route Label configured in the CICM under step 3 above. Make sure the Network VRU labels in the NAM are identical to the Translation Route Labels in Unified ICM and that all Translation Route Labels in the CICM have a matching Network VRU Label in the NAM.

Network VRU Scripts (for all Network VRU types)

Configuring the appropriate Network VRU Script using Network VRU Script List on the CICM (or on the NAM if VRU control scripting) is done from the NAM.

- Network VRU Scripts are associated with a specific Network VRU.
- The VRU Script Name and Config Parameters fields are sent to the VRU and must be entered in a way that is meaningful to the specific Network VRU.
- Check the Interruptible checkbox if the caller using DTMF tones can interrupt the Network VRU Script.
- Check the Overridable checkbox if the Interruptible setting can be changed dynamically by the Network VRU Script itself.
- A Network VRU Script can be associated with a Customer. This limits its use to routing scripts that belong to a specific customer and users who belong to a specific customer. If this setting is left as <none> the Network VRU Script is available to all users and routing scripts.

VRU PG as routing client

With Network VRUs of type 2, 3, 7 and 8 the routing client can be a VRU PG. Note that when the Routing Client is a VRU PG, the switching device connected to it is completely independent of the Network VRU. The switching device is just performing a switching function.

It is of course possible that the switching device itself is a VRU that can perform VRU functions. In that case there are two Network VRUs in the configuration. The switching device would be a type 5 or type 6 VRU.

Some special configuration instructions are applicable in case the routing client is a VRU PG. There are three cases:

- The switching device has only a switching function and not a VRU function.

- Configure an additional “dummy” type 5 Network VRU in the NAM. No label is required. Note that there are now two Network VRUs configured in the NAM. This “dummy” type 5 and a type 2, 3, 7 or 8 Network VRU.
- Using PG Explorer, select the “routing client” VRU PG and its Peripheral. In the Advanced tab, select the type 5 Network VRU configured above as the Network VRU for this Peripheral.

This configuration will “trick” the system into thinking that the switching device is not a VRU, which is required to enable the flexibility of dynamically selecting a Network VRU, based on the System Default Network VRU setting or the Network VRU associated with the call's Dialed Number's Customer.

- The device not only has a switching function, but also acts as a type 5 Network VRU

  In this case the VRU PG must be configured as described under type 5 VRU above. Note that there are now two Network VRUs configured in the NAM. A type 5 and a type 2, 3, 7 or 8 Network VRU.

  The System Default Network VRU or the Network VRU associated with any Customer as described under the type 3/7 configuration could now be set to the type 5 VRU as well, which allows dynamic selection of a particular Network VRU.

- The device not only has a switching function, but also acts as a type 6 Network VRU

  In this case the VRU PG must be configured as described under type 6 VRU above, with the following additions:

  - Configure an additional “dummy” type 5 (not a typo) Network VRU in the NAM. No label is required. Note that there are now three Network VRUs configured in the NAM. The “dummy” type 5, the type 6 Network VRU as defined according to the type 6 instructions, and a type 2, 3, 7 or 8 Network VRU according to those instructions.
  - Contrary to what is stated under the type 6 configuration instructions, step 2: in the Advanced tab select the “dummy” type 5 Network VRU configured above as the Network VRU for this Peripheral, and not the type 6 Network VRU.

  This configuration will “trick” the system into thinking that the switching VRU is not a type 6 VRU, which is required to enable the flexibility of dynamically selecting a Network VRU, based on the System Default Network VRU setting or the Network VRU associated with the call's Dialed Number's Customer.

  The System Default Network VRU or the Network VRU associated with any Customer as described under the type 3/7 configuration could now be set to the type 6 VRU as well, which allows dynamic selection of a particular Network VRU.

Script Editor

This section assumes that Network VRU control is done at the CICM routing script. If Network VRU control is done at the NAM (not an option for Network VRU types 2 and 8), the identical scripting applies.

Network VRU control nodes

The routing script has several script nodes related to Network VRU control:

- SendToVRU
- TranslationRouteToVRU

- Queue (as well as CancelQueue and QueuePriority, which are strictly speaking not Network VRU control nodes)
- RunExternalScript
- Wait

ICM release 5.0 added the following nodes that are for the purposes of this document identical to RunExternalScript:

- **Play**. This node instructs a VRU to play a series of media files and/or data.
- **Menu**. This node prompts a caller to choose one of a list of options. The caller-entered data (digits) are used to redirect the call to the appropriate destination.
- **CollectData**. This node plays a prompt and instructs the caller to enter some information. The caller-entered data (digits) are used to redirect the call to the appropriate destination.

Call connection to Network VRU

Before any RunExternalScript or Queue node can be used, the routing script needs to have an explicit node to force the routing client to connect the call to the Network VRU. The node used to send the call to the Network VRU depends on the Network VRU type:

- For type 3, 5, 6 and 7 use SendToVRU
- For type 2 or 8 use TranslationRouteToVRU

These nodes make the NAM or CICM send the instruction to the routing client to connect the call to the Network VRU.

If any of the RunExternalScript or Queue nodes is used in a script before a SendToVRU or TranslationRouteToVRU node, an implicit SendToVRU node is assumed. From this it follows that for Network VRUs of types 3, 5, 6 or 7 the SendToVRU node does not have to be used at all and that for Network VRUs of types 2 or 8 a TranslationRouteToVRU node is mandatory.

The SendToVRU node (implicit or explicit) does not have any parameters that can be set. Selecting which Network VRU the call is sent to (if there are multiple) is determined by rules described in SendToVRU node, on page 101.

The TranslationRouteToVRU node has extensive capabilities to select from specific Services and Translation Routes. Since these are linked to specific Peripherals that are Network VRUs of type 2 or 8, this node offers extensive capabilities to select a specific Network VRU, routes to connect to it or distribute over multiple Network VRUs.

Instructions to Network VRU

The RunExternalScript node is used to send the Network VRU instructions as specified in the Network VRU Script selected in the node. The CICM or NAM will wait for the VRU to respond back with the result of the VRU transaction. The VRU can put retrieved data (for example, prompted information or a menu choice received) in one of the call context variables, for example, Caller Entered Digits (CED) or a peripheral variable or even an Expanded Call Context (ECC) variable.

Wait node

The wait node will simply stop script execution for the specified number of seconds. In the meantime the Network VRU is waiting for instructions. This implies that the protocol time-out variables in the VRU system need to be set to a value greater than the longest wait node used in the script.

Queue nodes

The Queue nodes will not actually result in instructions being sent to the VRU. When queuing occurs the Queue node will exit immediately through the success exit. The call is now assumed to be at the VRU and the script must continue with a RunExternalScript node to instruct the VRU what to do while the call is held at the VRU waiting for an agent to become available. Typically this would invoke a Network VRU Script that plays music-on-hold, possibly interrupted on a regular basis with an announcement. If queuing occurs in a Queue node and the call is not yet at a VRU (that is, no SendToVRU or TranslationRouteToVRU node has been encountered yet), an implicit SendToVRU node will be executed before the first RunExternalScript node is processed.

Network VRU operations

This section describes how the NAM or CICM actually handles Network VRU calls and the script execution of various Network VRU related nodes. Most of it is relatively straightforward from the call flows and the configuration descriptions above, but there are some tricky areas.

SendToVRU node

The router checks the CallAtVRU flag. If it is set, it continues script processing with the next node without taking further action.

If the flag is not set, the router looks up the call's Dialed Number, the Dialed Number's Customer and the Customer's Network VRU. If that fails to retrieve a Network VRU, the router will use the system default Network VRU.

- If the Network VRU is of type 5 the router will send an instruction to the routing client to connect the call to a VRU resource. The instruction will contain the label configured for this Network VRU. The router will wait for a response back from the routing client that the call is properly connected to the VRU resource.
- If the Network VRU is of type 6, the router will simply continue without further action, since type 6 VRUs do not need explicit instructions to connect the call to the VRU resource.
- If the Network VRU is of type 3 or 7, the router will send an instruction to the routing client to connect the call to the Network VRU. The instruction will contain the label configured for this Network VRU as well as a correlation number from the range configured. The router will wait until it receives a RequestInstruction message from one of the connected VRU PGs with the same correlation number as a sign that the call is now connected to the VRU.

The router will now set the CallAtVRU flag and continue with the next script node.

TranslationRouteToVRU node

The TranslationRouteToVRU node uses its select rules to select one of the Services and TranslationRoutes specified in the node. The selected translation route is associated with a Peripheral. The router checks if this Peripheral is associated with a Network VRU type 2 or 8 (step 2 in the type 2/8 configuration). If not, the node fails and script processing continues through the failure exit.

If so, the router sends instructions to the routing client to connect the call to the VRU using the selected translation route and one of the translation route labels.

The router waits until the Peripheral sends a RequestInstructions message with a DNIS that matches the selected Translation Route's Peripheral Target's DNIS.

When that message is received the CallAtVRU flag is set and script processing continues from the success exit.

Note that this node does not check the CallAtVRU flag before processing. This implies that multiple TranslationRouteToVRU nodes can be used in the same routing script to subsequently connect calls to multiple Network VRUs of type 2 or 8.

Also note that if a call is translation routed to a type 2 VRU, the next TranslationRouteToVRU, Select, or Label node results in a connect instruction being sent to the Network VRU and not to the original routing client. This implies that the type 2 Network VRU is going to connect the call to the next destination. So using a second TranslationRouteToVRU node after a call is connected to a type 2 Network VRU results in a call connected through the first (type 2) Network VRU to a second Network VRU.

RunExternalScript node

The Router checks the CallAtVRU flag. If it is not set, it will first act as if a SendToVRU node was encountered and then continue processing the RunExternalScript node.

If the flag is set, the router will send a RunScript instruction to the Network VRU where the call is currently connected. The router will wait until a ScriptResult is received from the VRU and continue processing from the success or failure exit depending on the result.

Queue Node

The router checks the queue and selects a destination (agent) if one is available. In that case the appropriate label is sent to the routing client and no VRU activity takes place. If no agent is available and the call needs to be queued, the router checks the CallAtVRU flag. If it is not set, it acts as if a SendToVRU node was encountered and then continues processing the Queue node. If the flag is set, the router continues script processing out of the success node. The script must contain further RunExternalScript nodes to determine call treatment while queuing.

If subsequently an agent becomes available, the router interrupts script processing and connects the call to its destination without further script execution.

APPENDIX A

Administration and Data Server features

This appendix summarizes the Network Administration & Data Server features that are not installed on a Limited (single instance) Administration & Data Server. It also presents a set of software features that the service provider must not provide to subscribers with Standard Administration & Data Servers with Feature Control.

Limited (single instance) Administration and Data Server

The Limited (single instance) Administration & Data Server provides a network service provider customer with a subset of the tools and functionality of the Network Administration & Data Servers that reside at the network service provider site. This section discusses the following topics:

- Administration& Data Server program group tools that are not installed on a Limited (single instance) Administration & Data Server
- Configuration Manager menu items that are not available
- Script Editor features that are not available

Installed tools

The following Administration & Data Server program group tools are not installed on a Limited (single instance) Administration & Data Server:

- Select Administration Instance
- Check Routes
- Router Log Viewer
- Schema Help

Configuration tools unavailable on Limited (single instance) Administration and Data Server

The following Configuration tools are *not* available on a Limited (single instance) Administration & Data Server.

- Application Gateway List
- Application Wizard
- Business Entity List
- DB Lookup Explorer
- Dial Number Plan Bulk
- Dialed Number Bulk
- Dialed Number List
- Feature Control Set List
- Label Bulk
- Label List
- Network VRU Explorer
- Network VRU Script Bulk
- Network VRU Script List
- NIC Explorer
- PG Explorer
- Scheduled Target Bulk
- Scheduled Target Explorer
- Service Array Explorer
- Translation Route Explorer
- Translation Route Wizard

Nodes not available on Script Editor palette

The following nodes are *not* available on the Script Editor palette on a Limited (single instance) Administration & Data Server:

- Busy
- DB Lookup
- Gateway
- ICM Gateway

- Ring
- Termination
- Wait

Standard Administration and Data Server with feature control

Through the Configuration Manager Feature Control facility, a service provider can define what Unified ICM tools and features a subscriber with a Standard Administration & Data Server can access. For such subscribers, the service provider must not provide access to the following Unified ICM tools.

Script Editor Nodes:

- ICM Gateway
- TranslationRouteToVRU

Configuration Tools:

- Application Gateway List
- Application Wizard
- Blended Agent Configuration Tools
- Business Entity List
- Class Security List
- Dialed Number Bulk
- Dialed Number List
- Feature Control Set List
- ICM Instance Explorer
- Label Bulk
- Label List
- Network Trunk Group Bulk
- Network Trunk Group Explorer
- Network VRU Explorer
- NIC Explorer
- Peripheral Target Bulk
- PG Explorer
- Route Bulk
- Translation Route Explorer
- Translation Route Wizard
- Trunk Bulk

- Trunk Group Bulk
- User Group List
- User List
- VRU Port Map Bulk

INDEX

I

L

M

N

P

Q

R

S

T

U

V