



Cisco Network Applications Manager (NAM) Setup and Configuration

NAM Software Version 5.0

Corporate 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: 408 526-4100

Customer Order Number: DOC-7811592=
Text Part Number: 78-11592-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Cisco Network Applications Manager (NAM) Setup and Configuration

Copyright © 2000–2003, Cisco Systems, Inc.

All rights reserved.



About This Guide ix

Purpose ix

Audience ix

Organization x

Conventions xi

Other Publications xi

Obtaining Documentation xii

World Wide Web xii

Documentation CD-ROM xii

Ordering Documentation xii

Documentation Feedback xiii

Obtaining Technical Assistance xiii

Cisco.com xiii

Technical Assistance Center xiv

Cisco TAC Web Site xiv

Cisco TAC Escalation Center xv

CHAPTER 1

Network Applications Manager Overview 1-1

NAM Architecture 1-1

Example Network Design 1-3

NAM Components 1-5

Network Service Provider Site Components 1-6

Advanced Services ICM, Instances and Customers 1-7

Peripheral Gateways 1-8

- Admin Workstations **1-9**
 - Standard AW with Feature Control **1-10**
 - Network AW **1-11**
 - Limited AW **1-12**
- Real-Time Distributor **1-13**
- NAM Support Architecture **1-14**

CHAPTER 2

NAM Installation and Configuration 2-1

- Installing NAM Logger Software **2-2**
 - Post-Installation Setup and Installing Multiple Components **2-7**
- Installing NAM CallRouter Software **2-7**
- Installing a NAM Admin Workstation **2-10**
- NAM Configuration Data **2-11**
 - Defining CICM Instances and Customers on the NAM **2-13**
 - Configuring CICM Instances on the NAM **2-14**
 - Configuring CICM Associated Distributors on the NAM **2-16**
 - Defining CICM Customers **2-17**
- Installing and Configuring NAM NICs and PGs **2-18**
 - Network Interface Controllers **2-18**
 - Peripheral Gateways **2-18**
 - Creating an ICM Gateway to Access CICM Instances **2-21**
- Installing the Remote Monitoring Suite **2-26**
- Upgrading the NAM **2-27**

CHAPTER 3

CICM Setup 3-1

- Introduction to Instances **3-2**
 - Naming Conventions for Instances **3-2**
 - Selecting the CICM Complex **3-3**
 - Assigning an Instance Number to a CICM **3-3**

- Installing and Configuring CICM Loggers **3-5**
- Installing and Configuring CICM CallRouters **3-9**
- Installing and Configuring CICM Distributors on Network AWs **3-11**
- Configuring the CICM's INCRP NIC **3-12**
 - Update the Listener Configuration **3-19**
- Adding and Updating Components for Instances **3-19**
 - Deleting an Instance **3-19**

CHAPTER 4**Customer Concept 4-1**

- Overview of Customer Concept **4-1**
 - Business Units as Customers **4-3**
- Configuring Customer Concept **4-3**
- Customer Concept on Advanced Services Instances **4-5**
 - CICM Level **4-5**
 - NAM Level **4-6**
- NAM to CICM DN and Label Replication **4-6**
 - Configuring CICM Replication at NAM Level **4-7**
 - Configuring CICM Replication at CICM Level **4-11**
- Hosted IPCC and Hosted ICM with Network VRU **4-11**
 - NAM Level **4-11**
 - CICM Level **4-15**

CHAPTER 5**Advanced Services 5-1**

- Introduction **5-1**
- Setup and Configuration of an Advanced Services ICM Instance **5-3**
- Configuration of a new Advanced Services Customer **5-7**
 - Feature Control Set **5-7**
 - Customer **5-9**

User **5-11**
Call Type **5-12**
Dialed Number **5-13**
Scheduled Target **5-14**
Label **5-14**
Network VRU Script **5-15**
Routing Script **5-15**

CHAPTER 6

Administrative Tools 6-1

Service Control **6-1**
AW Select **6-3**
Customer ICM Monitor **6-5**
 What is CICM Monitor? **6-5**
 Defining CICM Profiles **6-6**
 Updating a Profile **6-7**
 Deleting a CICM Profile **6-8**
 Connecting to CICM Profiles **6-8**
 Launching Reports **6-9**
 Saving Report Data **6-14**
 Printing CICM Reports **6-14**

CHAPTER 7

Security Considerations 7-1

Windows 2000 Domains **7-1**
Running Node Manager on an Admin Workstation **7-3**
Validating Real-Time Clients **7-3**
Historical Data Server **7-5**

CHAPTER 8

Special Considerations 8-1

Calling Line ID (CLID) Masking **8-1**

Configuring CLID Masking	8-1
Dynamic Labels in NAM/CICM Configurations	8-4
Defining Dynamic Labels in the Script Editor	8-4
Dynamic Label Flow	8-5
NAM Network Event Reporting	8-6
Description	8-6
Table Overview	8-7
Events Reported	8-8
System Impacts	8-9
Limitations	8-9
Network Transfer	8-10
Detailed Call Flow	8-11
Call Flow Generalizations	8-13
Detailed Requirements	8-13
Supported Configurations	8-15
Routing Clients	8-15
Multiple Subsequent Network Transfers	8-16
Call Context	8-16
Route Call Detail Records and Termination Call Detail Records	8-16
Network Transfer Configuration on Existing Systems	8-18

CHAPTER 9

Network VRU 9-1

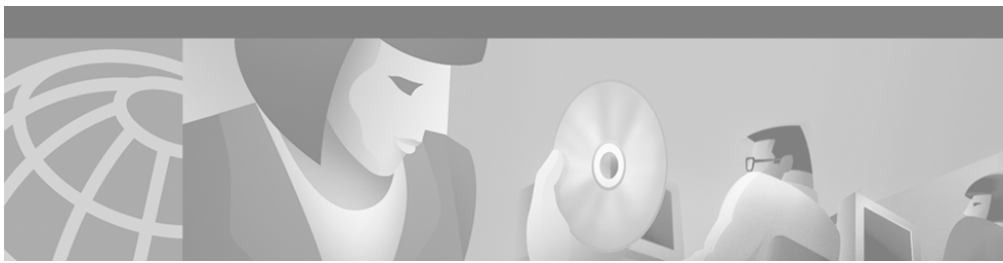
Network VRU Concept	9-1
Network VRU Architecture	9-2
Call Flows	9-7
Type 3 and 7 VRU call flows	9-8
Type 2 and Type 8 Call Flows	9-12
Type 5 and Type 6 Call Flows	9-16
Configuration	9-19

Configuration Manager	9-19
Type 3 and Type 7	9-19
Type 6	9-21
Type 5	9-21
Type 2 and Type 8	9-23
Network VRU Scripts (for all Network VRU types)	9-24
Configuring a VRU PG as Routing Client that is not also a Network VRU	9-25
Script Editor	9-26
Network VRU Control nodes	9-26
Connecting the Call to the Network VRU	9-27
Sending the VRU Instructions	9-28
Wait Node	9-28
Queue Nodes	9-28
Network VRU Operations	9-28
SendToVRU Node	9-29
TranslationRouteToVRU Node	9-29
RunVRUScript Node	9-30
Queue Node	9-30

APPENDIX A**Admin Workstation Features A-1**

Limited AW	A-1
Installed Tools	A-1
Configure ICM	A-2
Script Editor	A-2
Standard AW with Feature Control	A-3

INDEX



About This Guide

Purpose

This manual describes how to set up, run, and administer the Cisco Network Applications Manager (NAM) product. It supplements the installation and configuration instructions in the general Cisco ICM software documentation set with NAM-specific instructions for installing, configuring, and upgrading software components.



Warning

You must have a copy of the *Cisco ICM Software Installation Guide* available in *addition* to this manual in order to successfully complete NAM installation and configuration.

Audience

This document is intended for managers and administrators working in a network service provider environment. Readers of this manual should already have a general understanding of the NAM product, as discussed in the *Cisco Network Applications Manager (NAM) Product Description*. Readers should be familiar with general ICM installation and setup procedures.

Organization

The manual is divided into the following chapters.

Chapter	Description
Chapter 1, “Network Applications Manager Overview”	Provides an overview of Network Applications Manager (NAM) architecture.
Chapter 2, “NAM Installation and Configuration”	Provides instructions for installing and setting up software on the NAM machine.
Chapter 3, “CICM Setup”	Describes how to add and configure instances on Customer ICM (CICM) machines.
Chapter 4, “Customer Concept”	Discusses the NAM Customer Concept data sorting option and provides instructions for configuring it on NAM and CICM systems.
Chapter 5, “Advanced Services”	Describes how to setup and administer an Advanced Services instance.
Chapter 6, “Administrative Tools”	Describes how to run NAM administrative tools.
Chapter 7, “Security Considerations”	Discusses some NAM security concerns and how to address them.
Chapter 8, “Special Considerations”	Describes ICM features of special interest to NAM users.
Chapter 9, “Network VRU”	Describes the concepts, architecture, configuration and operations of Network Voice Response Units (VRUs) in a NAM/ICM environment
Appendix A, “Admin Workstation Features”	Summarizes the Network AW features that are not installed on a Limited AW.

Conventions

This manual uses the following conventions:

Format	Example
Boldface type is used for user entries, keys, buttons, and folder and submenu names.	Choose Script > Call Type Manager .
Italic type indicates one of the following: <ul style="list-style-type: none">• A newly introduced term• For emphasis• A generic syntax item that you must replace with a specific value• A title of a publication	<ul style="list-style-type: none">• <i>A skill group</i> is a collection of agents who share similar skills.• <i>Do not</i> use the numerical naming convention that is used in the predefined templates (for example, persvc01).• IF (<i>condition, true-value, false-value</i>)• For more information, see the <i>Cisco ICM Software Database Schema Handbook</i>.
An arrow (>) indicates an item from a pull-down menu.	The Save command from the File menu is referenced as File > Save .

Other Publications

For additional information about Cisco Intelligent Contact Management (ICM) software, see the [Cisco web site](#) listing ICM documentation.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.



Network Applications Manager Overview

This chapter provides an overview of the Cisco Network Applications Manager (NAM) software. It discusses the following aspects of NAM:

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

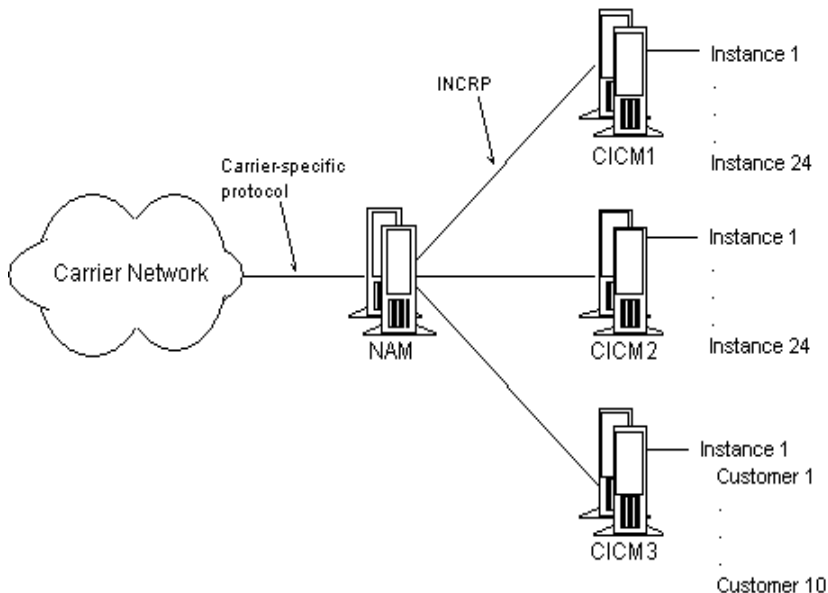
NAM Architecture

Cisco NAM is the carrier-class version of the Cisco Intelligent Contact Management (ICM) software. It allows a network service provider to offer *virtual call center services* to its customers. The NAM product functions much 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.

The NAM product uses a two-tiered architecture in which one ICM passes route requests to a second ICM. The first 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 ICM, called the *Customer ICM* or *CICM*. The NAM uses the proprietary INCRP protocol to pass a route request to a CICM.

Figure 1-1 NAM Two-Tiered Architecture



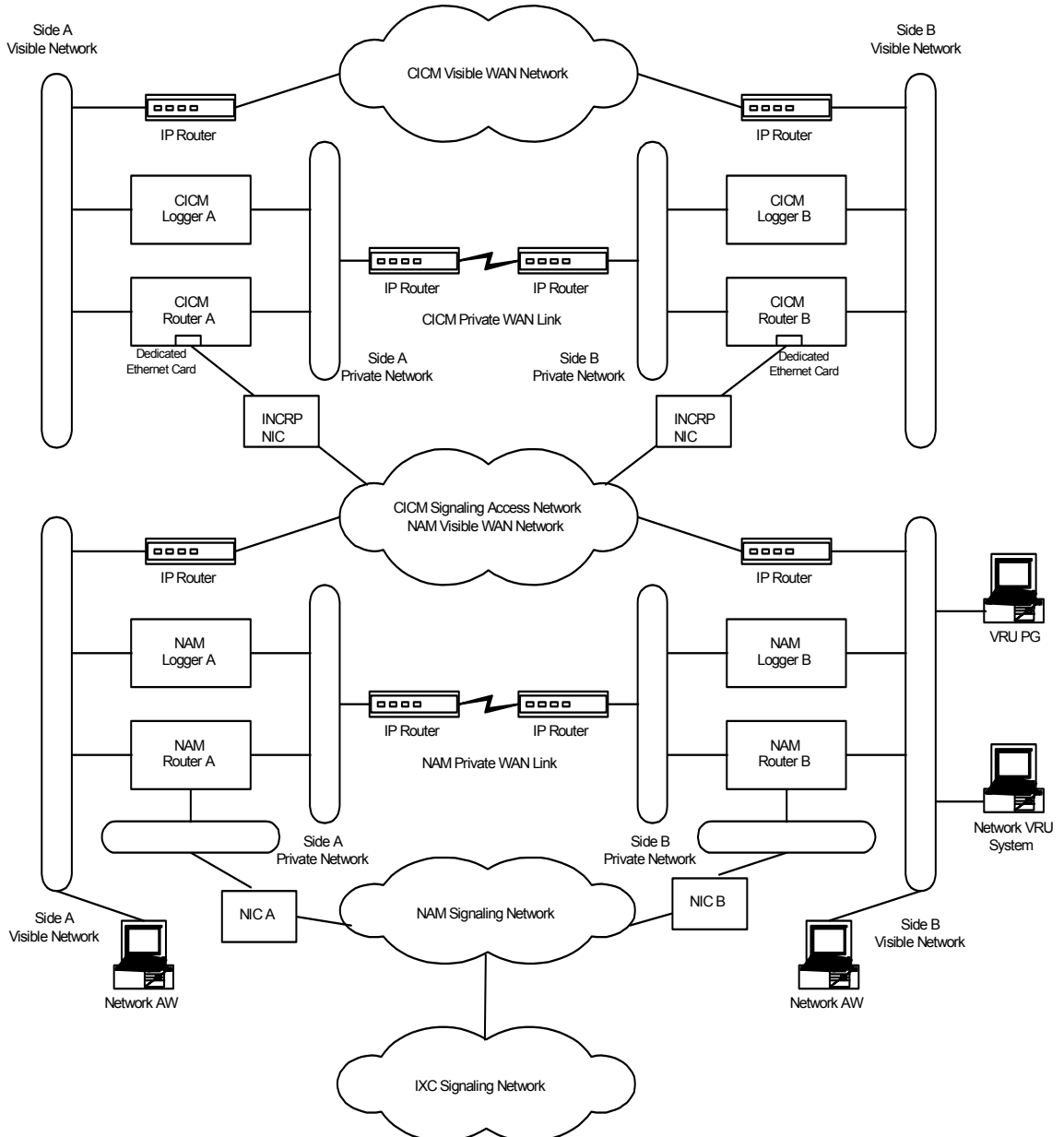
Each CICM typically processes all calls for one specific ICM instance; multiple customers may share an ICM instance (see the section [“Advanced Services ICM, Instances and Customers”](#)). The CICM must have an INCRP Network Interface Controller (NIC) configured. The CICM receives the request, runs its 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 ICM functionality (in a CICM) for other customers.

Typically a single NAM can pass route requests to any of several CICMs, as shown in [Figure 1-1](#). 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

Figure 1-2 shows a sample design for a Network Applications Manager system.

Figure 1-2 Network Applications Manager Example Design

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 Network Applications Manager 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 ICM system to the signaling access network. The CICM signaling access network uses a dedicated network interface card in the CICM CallRouter machine.

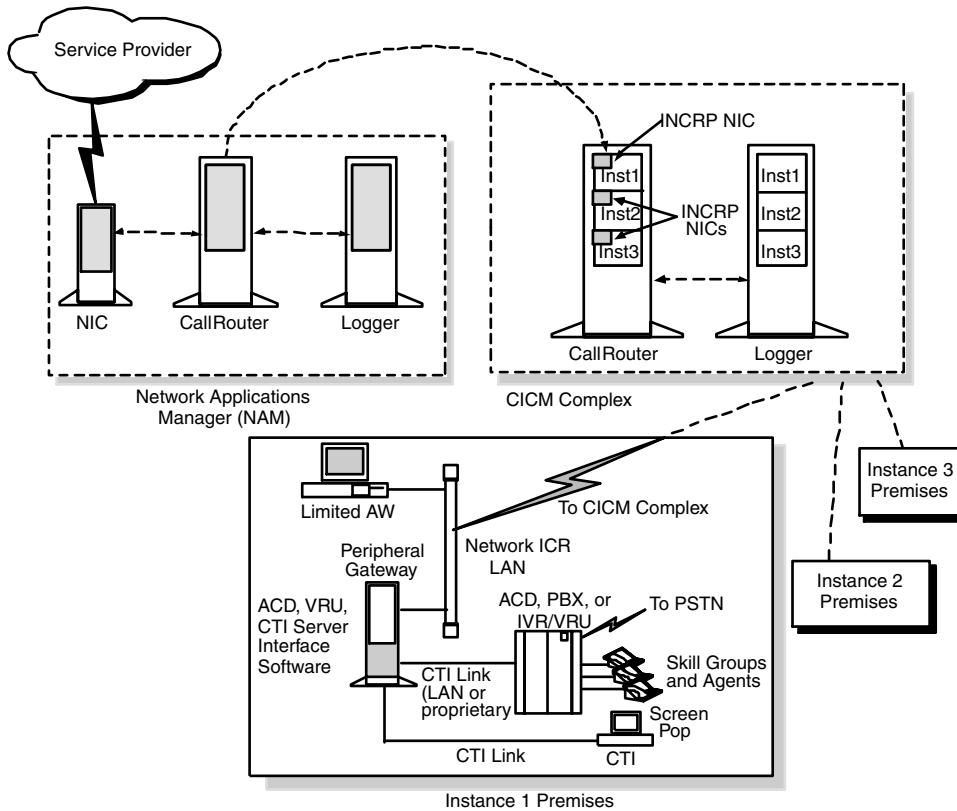
Other types of dedicated communications cards may be also used in the CallRouter platform depending on the interexchange carrier. For example, X.25 cards are installed in the CallRouter, along with the appropriate access links, to connect the ICM system to the Sprint signaling network.

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 AWs connect to the NAM visible network. The VRU systems themselves reside on the NAM visible network. However, if this is not possible the IVRs can be placed on a dedicated third LAN. This requires a third Ethernet card in the Network IVR PG machine.

NAM Components

[Figure 1-3](#) shows a typical NAM configuration and illustrates the components that reside on the network service provider site and the instance premises.

Figure 1-3 NAM Components

Network Service Provider Site Components

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

The NAM is an ICM system that is configured to handle initial route requests from the service provider network. Each NAM consists of a CallRouter and a Logger (simplex 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 simplex 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 the ICM.

As shown in [Figure 1-3](#), several CICMs may 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.

Advanced Services ICM, Instances and Customers

An *instance* is a single logical ICM. An instance typically consists of several software components (CallRouter, Logger, Peripheral Gateways, Admin Workstations)—some of which may be duplexed—typically installed on several different computers. A single computer may 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 AW 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 the ICM. Therefore Advanced Services customers do not have PGs connected. They also do not have dedicated Admin Workstations, but they do have web-based tools like WebView 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's 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 [Figure 1-3](#) could be an Advanced Service ICM. However, for performance reasons it might be desirable to run an Advanced Services ICM on its 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 the ICM to manage its call center. Each customer has its own configuration elements, such as dialed numbers, labels, call types, scripts, IVR scripts and scheduled targets. All these configuration elements are stored in the same Advanced Service ICM database, but the reporting and scripting tools will make sure that a specific customer only has access to his own data. Since Advanced Service customers do not have ACD and Peripheral Gateways there are no configuration elements like peripherals, services, skill groups, etc.

**Note**

No special security is applied at the customer level. Any Admin Workstation 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 Admin Workstation to administer the Advanced Services ICM as any other ICM instance. Advanced Services customers should only have access to their data using WebView and Internet Script Editor. These tools will prevent a customer from accessing other customer's data.

Peripheral Gateways

Peripheral Gateways are typically located on instance sites and are associated with a CICM rather than the NAM. Note that the NAM contains no peripherals, trunk groups, skill targets, routes, or peripheral targets. Those entities are configured only on the CICMs; a CICM has a normal 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 [Chapter 2, “NAM Installation and Configuration.”](#)

Admin Workstations

Admin Workstations reside both at the service provider site and the customer sites. Both of the following types of Admin Workstations reside at the service provider site:

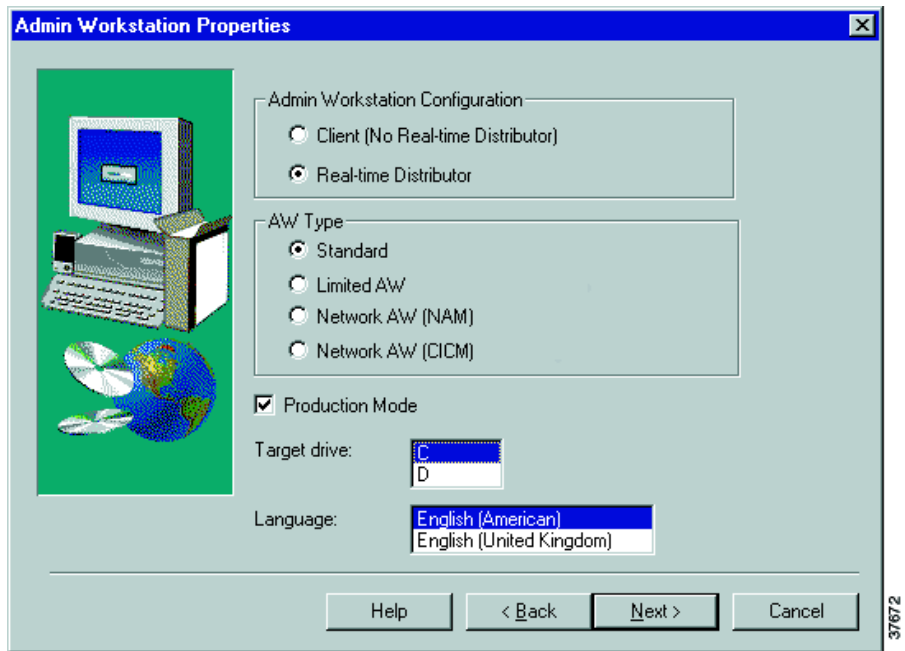
- **Network AW (NAM).** A network Admin Workstation associated with the NAM system.
- **Network AW (CICM).** A network Admin Workstation associated with the CICM systems.

Both of these Network AWs may reside on the same machine.

A customer site contains one of the following three types of Admin Workstations:

- **Limited AW.** Accesses one instance's data from a CICM.
- **Standard.** A standard ICM AW. Optionally, the service provider can use the ICM Configuration Manager Feature Control facility to define the customer's available tools.

You must specify the type of Admin Workstation you are installing on ICM Setup tool's Admin Workstation Properties dialog box, shown in [Figure 1-4](#).

Figure 1-4 Admin Workstation Properties Dialog Box

For guidelines on installing a NAM Admin Workstation, see [Chapter 2, “NAM Installation and Configuration.”](#) For guidelines on installing a CICM Admin Workstation, see [Chapter 3, “CICM Setup.”](#)

Standard AW with Feature Control

The Standard AW is a standard Admin Workstation in an ICM environment. A network service provider may provide such a workstation for one of its customers and then use the ICM Configuration Manager Feature Control facility to determine which ICM tools that customer can use.

See the *Cisco ICM Software Configuration Guide* and the ICM Configuration Manager on-line help for information on Feature Control.

Network AW

The Network AW types are for use by network service provider personnel. A Network AW has multiple distributors: one for the NAM instance, and one for each associated CICM instance.

When you install the ICM Admin Workstation software on a computer, the Admin Workstation program group is created in the Windows Program Manager. This group contains icons for the programs to be run by Admin Workstation users.

The following programs are available on network AWs:

- **AW Select.** Lets you switch among multiple instances on an Admin Workstation and optionally start and stop the distributor.
- **Call Tracer.** Lets you send test calls to the ICM and see how they are processed and the target chosen.
- **Check Routes.** Lets you validate the configuration of routes referenced by a script.
- **CICM Monitor.** Lets you connect to a CICM server and view real-time call routing performance for all instances installed on that CICM.
- **CMS Control.** Lets you access the CMS Control Console and perform CMS Server functions.
- **Configuration Manager.** Lets you set up and maintain your Cisco 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 NAM.
- **Initialize Local Database.** (Distributor workstations only). Lets you copy current information from the NAM or CICM central database to the local database on the Admin Workstation.
- **Job Scheduler.** Lets you schedule reports to be generated and printed at a later time.
- **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.
- **Print Server.** Works with the Job Scheduler to let you automatically print reports at specific times.

- **Router Log Viewer.** Displays information about calls processed by the ICM and any errors encountered in processing them.
- **Scheduled Target Manager.** Lets you create, update, and assign schedules to scheduled targets (routing targets that ICM does not monitor directly).
- **Script Editor.** Lets you create, modify, and schedule routing scripts. The ICM executes these scripts to determine where to route each call.
- **Service Control.** Lets you stop and start NAM-related services.
- **Setup.** Lets you modify NAM setup parameters.

[Table 1-1](#) lists the ICM documentation that describes each tool.

Table 1-1 ICM Tools Documentation

Tools	Where to find more information
AW Select, CICM Monitor, Service Control	Chapter 6, “Administrative Tools” in this manual.
Job Scheduler, Print Server, Send Home	<i>Cisco ICM Software Administrator Guide</i>
Setup	<i>Cisco ICM Software Installation Guide</i>
CMS Control, Configuration Manager and its associated tools, Lock Admin	<i>Cisco ICM Software Configuration Guide</i>
Call Tracer, Check Routes, Router Log Viewer, Script Editor	<i>Cisco ICM Software Script Editor Guide</i>
Glossary, Scheduled Target Manager,	<i>ICM On-Line Help</i>

Limited AW

The Limited AW type is for use by the customer of a network service provider. A Limited AW workstation 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.”](#)

The program group for Limited AW workstations is a subset of the Network AW program group. The following tools are *not* available on a Limited AW:

- AW Select
- Check Routes
- CICM Monitor
- Router Log Viewer
- Schema Help

For a list of other features not installed on Limited AW workstations, see [Appendix A, “Admin Workstation Features.”](#)

Real-Time Distributor

You have two options when installing the Admin Workstation software:

- **Real-time Distributor.** This configuration includes the real-time distributor and real-time client processes, and all processes that directly manage the local database. A single distributor Admin Workstation machine can run the distributor processes for multiple instances simultaneously. However, it can run client applications (such as Script Editor and Configure ICM) for only one instance at a time. Use AW Select to change the instance.
- **Client (No Real-time Distributor).** This configuration includes standard Admin Workstation applications, such as Script Editor and Configure ICM. It does not include the processes that directly manage a database.

[Table 1-2](#) summarizes the difference between Real-time Distributor and client-only Admin Workstations.

Table 1-2 Distributor vs. Client Admin Workstation

	Distributor Admin Workstation	Client Admin Workstation
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 2000 Service	Cisco ICM Distributor	N/A

Table 1-2 Distributor vs. Client Admin Workstation (continued)

	Distributor Admin Workstation	Client Admin Workstation
Background Processes	logger, rtclient, rtdist, updateaw	N/A
Optional Processes	schman, replication	N/A

- If you have more than one Admin Workstation on a single LAN, then only one of those machines needs to receive the real-time feed from the Central Controller. That machine acts as the real-time distributor and passes the real-time data to other Admin Workstations at the site. If possible, configure two machines at the site as real-time distributors: one as the primary and the other as the secondary (backup) distributor.

Optionally, you can configure a real-time distributor to also act as a Historical Data Server (HDS). The Logger then forwards historical data to a special database on the distributor. Admin Workstations at the local site can then access historical data from the distributor rather than from the central database.

For more information on real-time distributor and client workstations and for instructions on how to configure a Historical Data Server, see the *Cisco ICM Software Installation Guide*.

NAM Support Architecture

You can install and configure a set of processes and tools that transfer event and message information from the NAM and CICM systems to a single machine and then forward the information to network service provider administrative personnel. Collectively, these processes and tools are referred to as the *NAM support architecture*.

In the NAM support architecture, each ICM Logger collects event and message information from all NAM system components. The Logger sends this information through a facility called the Distributed Diagnostics and Services Network (DDSN) to a process called the Listener. The Listener, in turn, can distribute this information to a specified email distribution list, an automated paging system, or to the AlarmTracker management program. This provides a means of notifying network service provider personnel about NAM events that require immediate attention. It also provides an event history for each customer that lets you examine less urgent events later.

**Note**

For more information on the tools listed above, see the *Cisco Remote Monitoring Administration Guide*.



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 2000 and SQL Server are already installed.



Tip

You should have a copy of the following Cisco ICM documentation available in *addition* to this manual in order to successfully complete NAM installation and configuration: *Cisco ICM Software Installation Guide* and *Cisco Remote Monitoring Administration Guide*.

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 Admin Workstation.
- Setting up NAM configuration data.
- Defining CICM instances on the NAM.
- Configuring Network Interface Controllers.
- Installing and configuring a Peripheral Gateway for the NAM.
- Creating an ICM Gateway to access CICM instances.
- Installing and configuring the Remote Monitoring Suite.

**Note**

If you are installing and configuring NAM systems that will be part of a Multiple NAM configuration, see also the installation and configuration instructions in the *Cisco Network Applications Manager (NAM) Multiple-NAM Setup and Configuration* manual.

Installing NAM Logger Software

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

During NAM Logger configuration you enable the *Phone Home* option. This option enables the Logger to send the Listener customer event and message information through the NAM Support Architecture.

**Note**

For more information about the NAM support architecture, see the *Cisco Remote Monitoring Administration Guide*.

How to install and configure NAM Logger software

-
- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to install the Logger software on the NAM and create the central database. Continue to follow the instructions until the Logger Properties dialog box appears.
 - Step 2** In the Logger Type section of the dialog box, select the **NAM** option and click **Next**. The NAM Properties dialog box appears.

Step 3 Specify a NAM Type:

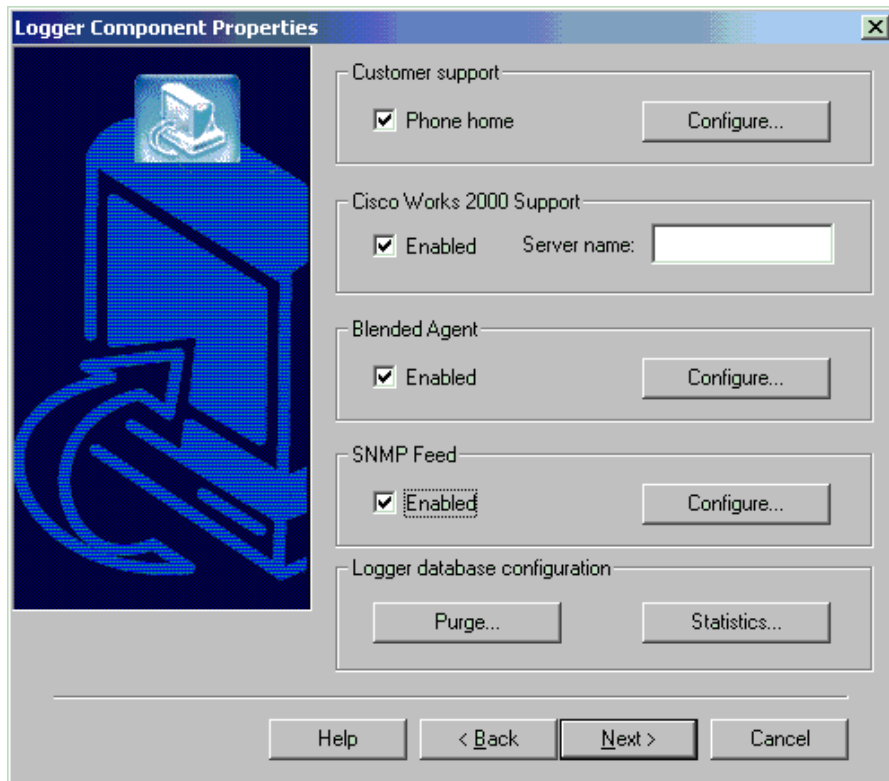
- **Provisioning/Standalone NAM.** Select if the Logger will provide Slave NAMs with configuration information.
- **Slave NAM.** Select to establish a slave relationship with a provisioning NAM Logger.
- **Site Name.** Machine name of the Slave Logger.



Note

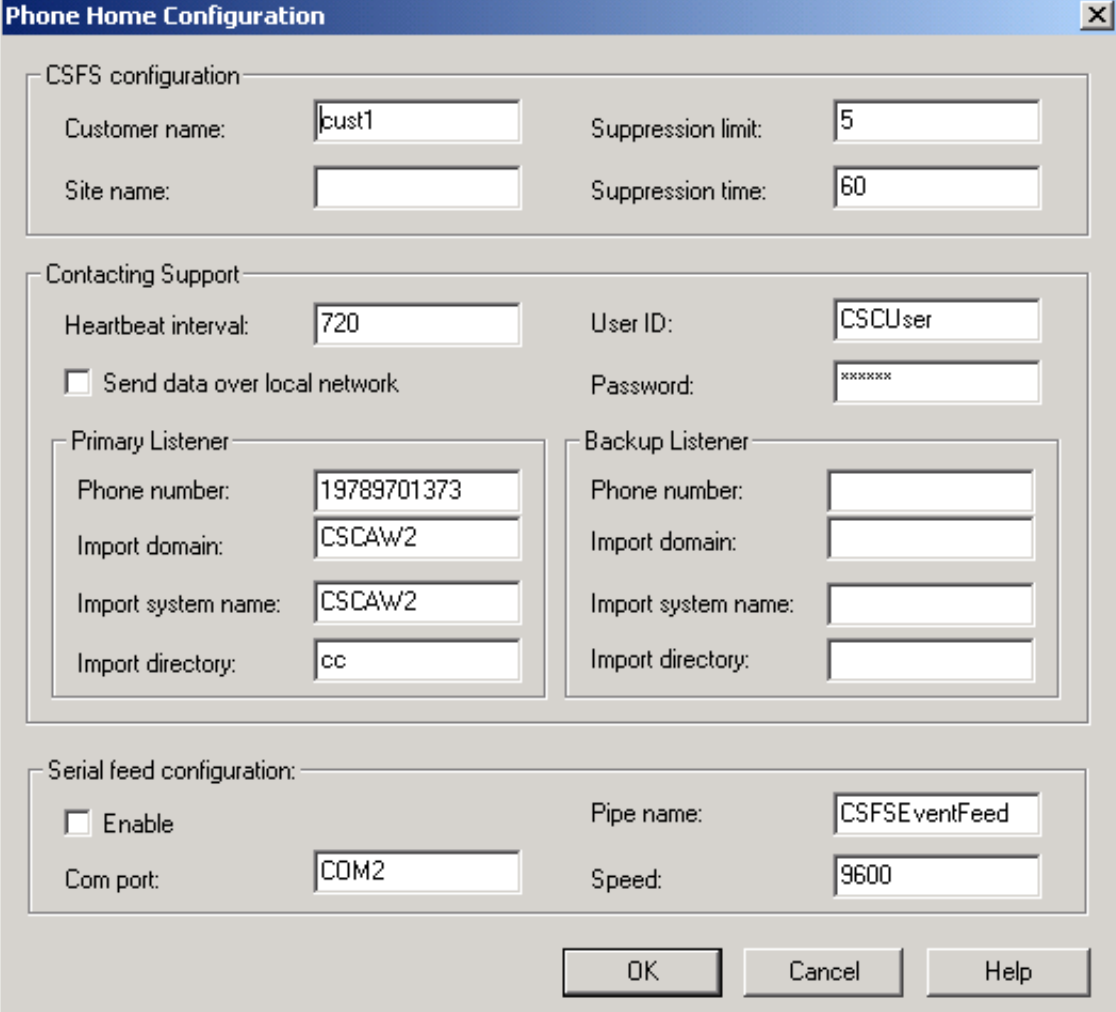
For an explanation of provisioning, Network Provisioning Platform (NPP) systems, and Slave NAMs, see the *Cisco Network Applications Manager (NAM) Multiple-NAM Setup and Configuration* manual.

- Step 4** Specify Provisioning NAM Information. (If the NAM type you selected was Provisioning NAM, you provide only the names of the Side A and Side B Provisioning Router machines. For Slave NAMs, enter information for all of the fields in this section.)
- **Instance Name.** Enter the Instance Name of the Provisioning NAM.
 - **Instance Number.** Enter the Instance Number of the Provisioning NAM.
 - **Side A Prov. Logger.** Enter the Side A machine name or IP address of the provisioning logger.
 - **Side B Prov. Logger.** Enter the Side B machine name or IP address of the provisioning logger.
 - **Side A Prov. Router.** Enter the Side A machine name or IP address of the provisioning CallRouter.
 - **Side B Prov. Router.** Enter the Side A machine name or IP address of the provisioning CallRouter.
- Step 5** Click **Next**. The Logger Component Properties dialog box appears.



Step 6 In the Logger Component Properties dialog box, check the **Phone Home** option.

Step 7 Click the **Configure** button. The Phone Home Configuration dialog box appears.



Phone Home Configuration

CSFS configuration

Customer name: Suppression limit:

Site name: Suppression time:

Contacting Support

Heartbeat interval: User ID:

☐ Send data over local network Password:

Primary Listener

Phone number:

Import domain:

Import system name:

Import directory:

Backup Listener

Phone number:

Import domain:

Import system name:

Import directory:

Serial feed configuration:

☐ Enable Pipe name:

Com port: Speed:

OK Cancel Help

Step 8 Identify the Listener the Logger will forward information to:

- **CSFS Configuration.** Specify a **Customer name** and a **Site name**.
- **Contacting Support.** Contact information for the network service provider primary and backup Listeners. Specify the following:

- A check in the **Send Data Over Local Network** box for a direct network connection.
- A customer name as the Import Directory value.
- Import System Name and Import Domain values pointing to the machine running the Listener.

Step 9 Click the **OK** button to make the changes and close the dialog box.

Step 10 Continue with the remaining Logger setup steps as described in the *Cisco ICM Software Installation Guide*, including creating the Central Database with the ICMDDBA tool.

Post-Installation Setup and Installing Multiple Components

A version of the ICM Setup program is installed as part of each ICM component. (On an Admin Workstation, the Cisco Admin Workstation group contains an icon for this program.) This version allows you to change the configuration settings of the software after it is installed. It does not allow you to install new software. To install—or reinstall—the software, you must run **SETUP.EXE** from the CD-ROM.

In cases where you want to install more than one ICM component on a single computer—for example, to install the CallRouter and Logger software on a single node—you must run **SETUP.EXE** from the CD-ROM for each component. Similarly, to install a specific component for more than one customer, you must run Setup from the CD-ROM for each instance.

Installing NAM CallRouter Software

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

During NAM CallRouter configuration you set up the following:

- **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.

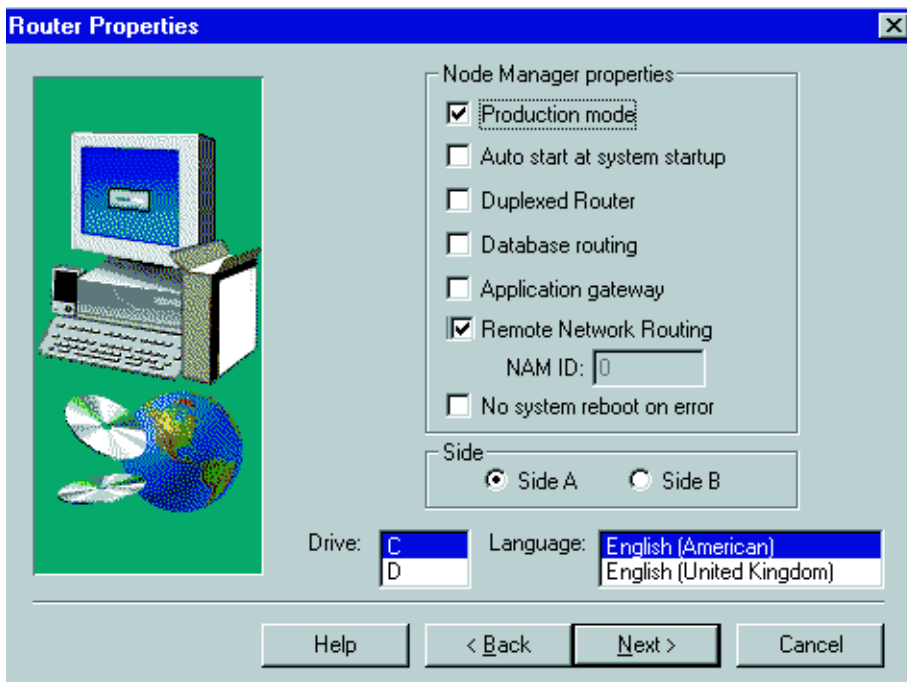
How to install and configure CallRouter software on the NAM

- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to install the CallRouter software.



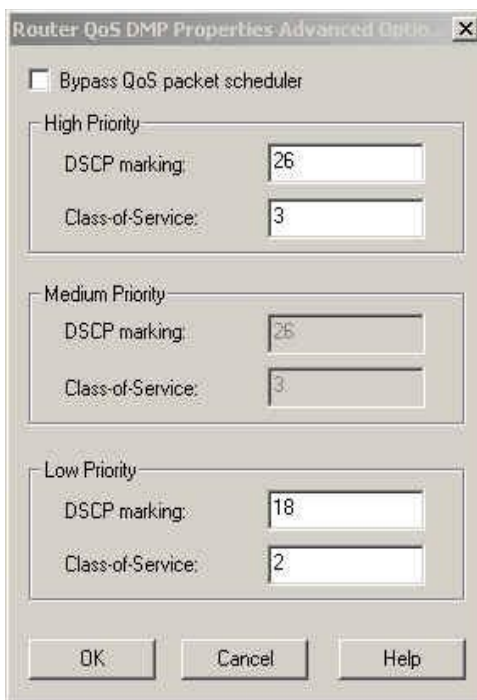
Note If you are installing more than one ICM component on a single computer, you must run **SETUP.EXE** from the CD-ROM. For more information, see page 2-7.

- Step 2** Continue to follow the instructions until the Router Properties dialog box appears.



- Step 3** In the Router Properties dialog box, check the **Remote Network Routing** option.

- Step 4** In the **NAM ID** field, do the following:
- If your NAM configuration contains only a single NAM, accept the default value of 0.
 - If your NAM configuration contains multiple NAMs that may communicate with a single CICM, specify a unique nonzero value.
- Step 5** Click the **Next** button. The Router Component Properties screen appears.
- Step 6** Ensure that the **Disable ICM Time Synchronization** box is checked. When checked, ICM software releases control of the system clock so other applications can use it.
- Step 7** Click the **Next** button. The Device Management Protocol Properties screen appears.
- Step 8** If you wish to configure QoS for the Central Controller selected on the Device Management Properties screen, click the **Advanced** button. The Router DMP Properties Advanced Options window displays.



The image shows a dialog box titled "Router QoS DMP Properties Advanced Options". It contains a checkbox labeled "Bypass QoS packet scheduler" which is unchecked. Below this, there are three sections for configuring QoS: "High Priority", "Medium Priority", and "Low Priority". Each section has two input fields: "DSCP marking" and "Class-of-Service". For High Priority, DSCP marking is 26 and Class-of-Service is 3. For Medium Priority, DSCP marking is 26 and Class-of-Service is 3. For Low Priority, DSCP marking is 18 and Class-of-Service is 2. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Priority	DSCP marking	Class-of-Service
High Priority	26	3
Medium Priority	26	3
Low Priority	18	2

Specify the DSCP (DiffServ Codepoint) marking and the Class-of-Service (802.1p) marking for each priority of the ICM traffic going to the PG. Click the **OK** button.

**Note**

For more information about ICM QoS, refer to the *Cisco ICM Software Network and Site Requirements Pre-Installation Planning Guide*.

Step 9 Click the **Next** button.

Step 10 Continue with the remaining CallRouter setup steps.

Installing a NAM Admin Workstation

The Admin Workstation (AW) provides the user interface to the NAM and ICM software. During NAM Admin Workstation configuration you set the AW Type option to *Network AW*.

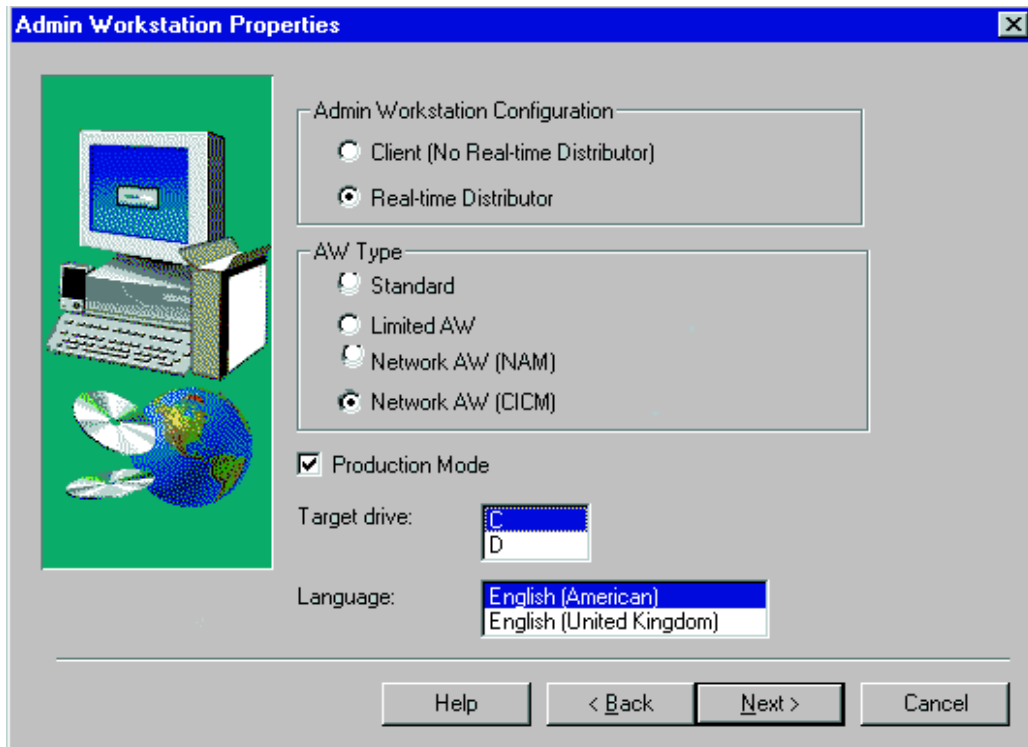
How to install and configure Admin Workstation software for the NAM

Step 1 Follow the steps described in the *Cisco ICM Software Installation Guide* to install an Admin Workstation.

**Note**

If you are installing more than one ICM component on a single computer, you must run **SETUP.EXE** from the CD-ROM. For more information, see page 2-7.

Step 2 Continue to follow the instructions until the Admin Workstation Properties dialog box appears.



- Step 3** In the Admin Workstation Properties dialog box, select **Network AW (NAM)** as the AW Type.
- Step 4** Click the **OK** button to make the changes and close dialog box.
- Step 5** Continue with the remaining Admin Workstation setup steps.

NAM Configuration Data

At this point, you can start the NAM Logger, CallRouter, and Admin Workstation, and set up the NAM configuration data.

In a two-tier architecture, the NAM system requires only a subset of the normal ICM configuration data. [Table 2-1](#) summarizes the configuration data for a NAM.

Table 2-1 Configuration Data on 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.
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.

The NAM needs only a limited configuration (dialed numbers, labels, basic routing scripts, etc.) while the instance-specific scripts, configuration, real-time, and historical data are stored on the CICM.

To set up your NAM configuration, run Configuration Manager on a NAM Admin Workstation.

For instructions on using Configuration Manager, see the *Cisco ICM Software Configuration Guide*.

Defining CICM Instances and Customers on the NAM

A process called the Network Applications Manager Replication Process (NIRP) runs on the NAM Logger system. The NIRP 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 NIRP determines which CICM is affected. The NIRP then forwards and automatically applies the change to the appropriate CICM.

**Note**

Because the NIRP 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 NIRP to function properly, you must do the following:

- Configure all associated CICMs as ICM instances and customers on the NAM so that the NIRP can forward changes to the appropriate CICM databases. (For instructions, see the [“Configuring CICM Instances on the NAM”](#) section on page 2-14.)
- Configure the distributors for each CICM and the customers, to allow the NIRP to locate the CICM databases to be updated (For instructions, see the [“Configuring CICM Associated Distributors on the NAM”](#) section on page 2-16.)
- 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 the [“How to associate a CICM routing client with a NAM routing client”](#) section on page 2-17.)

Configuring CICM Instances on the NAM

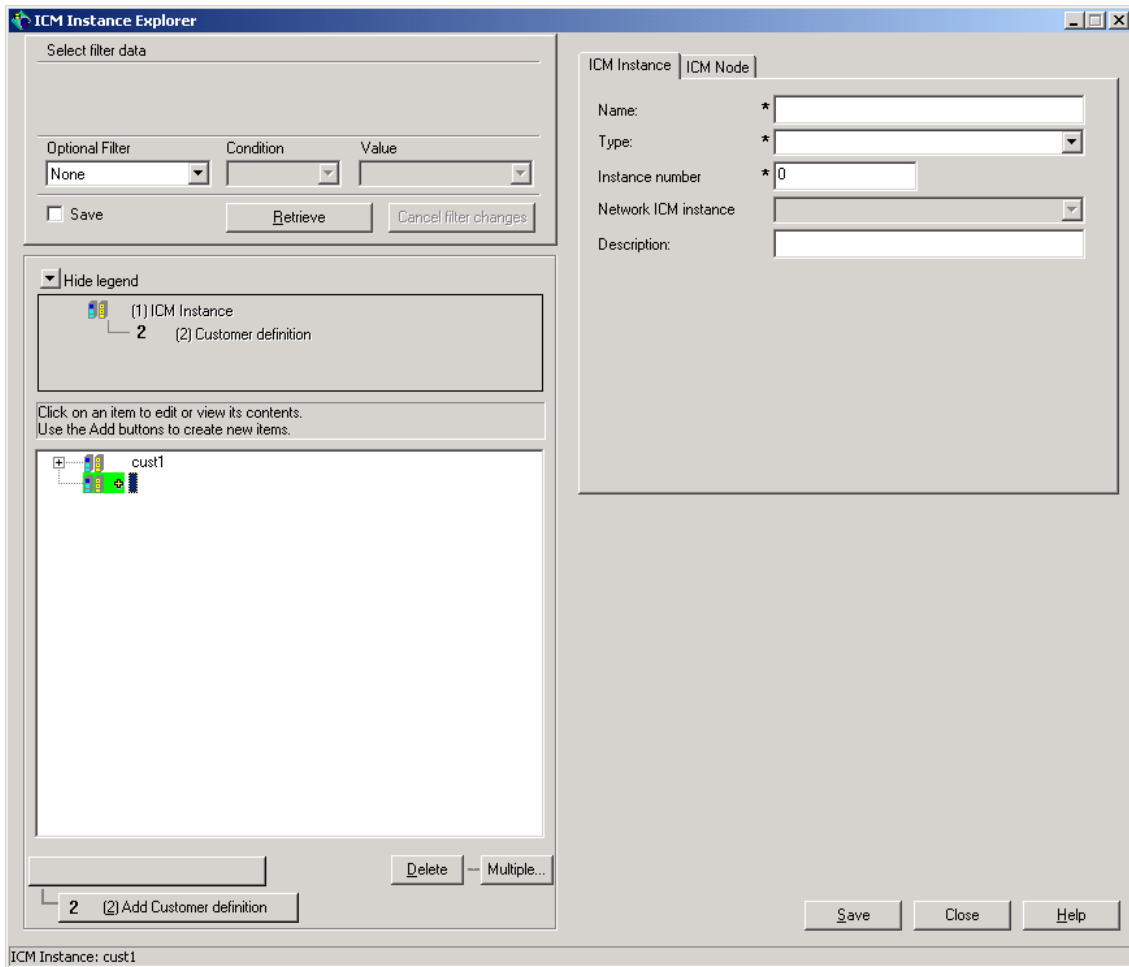
You must perform the following steps to configure an instance for each associated CICM.

**Note**

CICM instance names and numbers are defined on the CICMs. For information, see [Chapter 3, “CICM Setup.”](#)

How to configure a CICM instance on the NAM

-
- Step 1** On the NAM, start **Configuration Manager** from the **ICM Admin Workstation** group. The Configuration Manager window opens.
 - Step 2** Open the ICM Instance List tool (**Enterprise > ICM Instance > ICM Instance Explorer**). The ICM Instance List window appears.
 - Step 3** Click the **Retrieve** button.
 - Step 4** Click the **Add ICM Instance** button.



Step 5 Specify the following on the ICM Instance tab:

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



Note For information about defining a name and number for a CICM instance, see [Chapter 3, “CICM Setup.”](#)

- **Network ICM Instance.** (Drop-down list.) The associated NAM instance.
- **Description.** (Optional.) Additional information about the ICM Instance.

Step 6 Click **Save**.

Configuring CICM Associated Distributors on the NAM

You must perform the following steps to configure the primary and secondary distributors associated with the CICM instances you just defined.

How to configure the distributors associated with the instance:

- Step 1** On the NAM, in **Configuration Manager**, choose **Enterprise > ICM Node > ICM Instance Explorer**. The ICM Node List window appears.
- Step 2** Click the **Retrieve** button.
- Step 3** Click the **Add ICM Instance** button.
- Step 4** Specify the following on the ICM Node tab:
 - **ICM Instance.** (Drop-down list.) The name for the instance that contains the node.
 - **System Domain.** The name of the Windows 2000 security domain that contains the NAM machine.
 - **System Name.** The name of the computer that runs both instances.
 - **Node Type.** (Drop-down list.) The node type: Primary Distributor or Backup Distributor.



Note For more information on this option, see [“Real-Time Distributor”](#) in [Chapter 1, “Network Applications Manager Overview.”](#)

- **Name.** The enterprise name for the node. (The default enterprise name is formed by combining the ICM instance, system name, and node type.)
- **Configuration Parameter.** (Optional.) A string of configuration parameters to be passed to the node at initialization.
- **Description.** (Optional.) Additional information about the node.

Step 5 Click **Apply** and **Done**.

Defining CICM Customers

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

How to define a customer

-
- 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**.
-

How to associate a CICM routing client with a NAM routing client

-
- 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.
-

Installing and Configuring NAM NICs and PGs

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

Network Interface Controllers

Depending on your network interface, you may need to perform the following tasks to configure your NICs:

- Set up the NICs in Setup's Device Management Protocol Properties dialog box.
- Enable a DMP device on the NAM for each physical controller (A through H).

See the *Cisco ICM Software Installation Guide* and the System Manager Guide Supplement for your particular NICs for guidelines and procedures.

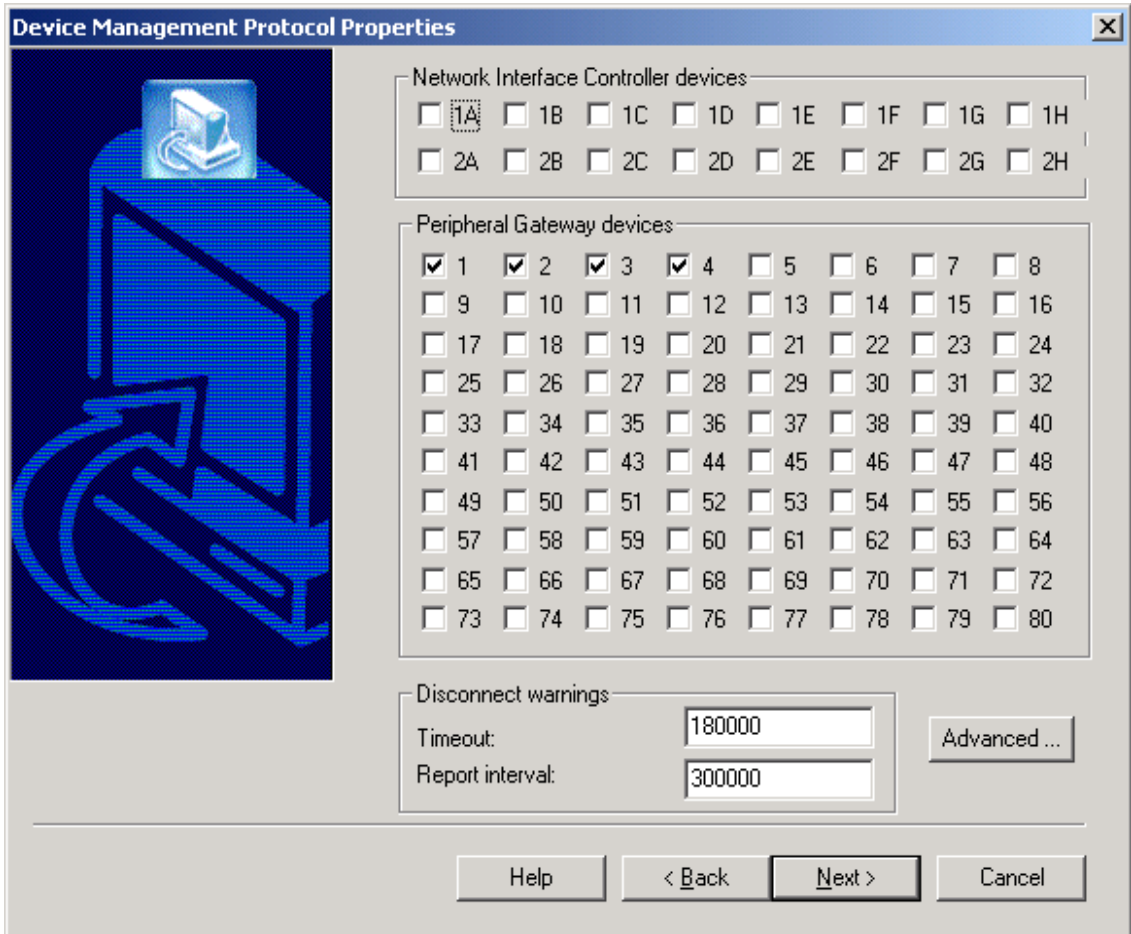
Peripheral Gateways

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 Admin Workstation machines associated with the NAM. The Peripheral Interface Manager (PIM) on the PG need not be enabled.

How to configure Device Management Protocols for NAM PGs

-
- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to set up a Peripheral Gateway. Continue to follow the instructions Device Management Protocol Properties dialog box appears.



- Step 2** In the Peripheral Gateway devices section of the Device Management Protocol Properties dialog box, check one box for each Peripheral Gateway. (The Network Interface Controller Types section is applicable only for AT&T NICs; see the *Cisco ICM Software ICM Installation Guide* for details.)
- Step 3** Continue with the remaining Peripheral Gateway setup steps.

Creating an ICM Gateway to Access CICM Instances

After adding the instance components to the CICM, you must configure an ICM gateway in Configuration Manager on an Admin Workstation associated with the NAM. (The ICM gateway is the path a NAM takes to access a CICM.) In the configuration, an ICM gateway is a variant of an application gateway.

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

**Note**

Instructions for creating the ICM on the NAM are described below. For information about using the ICM Gateway within a routing script, see [Chapter 8, “Special Considerations.”](#)

How to create the ICM Gateway

-
- Step 1** Within Configuration Manager on an Admin Workstation 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.

The screenshot shows the 'Application Gateway List' window. On the left, there is a filter section with 'Optional Filter' set to 'None', and buttons for 'Save', 'Retrieve', and 'Cancel filter changes'. Below this is a table with one header 'Name' and one empty row. At the bottom left are 'Add', 'Delete', and 'Revert' buttons. The main area on the right is titled 'Attributes' and has tabs for 'Connection Side A' and 'Connection Side B'. The 'Attributes' tab is active, showing fields for 'Name', 'Application gateway ID' (set to 0), 'Type' (set to 'Custom Gateway'), 'Preferred side' (set to 'Side A'), 'Encryption' (set to '<None>'), 'Fault tolerance' (set to '<None>'), 'Connection' (set to 'Duplex'), and 'Description'.

ICM Instance: cust1

Step 4 Specify the following values on the Attributes tab:

- **Name.** Enter a name for the ICM Gateway.
- **Type.** Choose **Remote ICM**.
- **Preferred Side.** Indicates the preferred side of the Gateway to use when both are available. If only one side is available, ICM 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 Application Gateway are encrypted. Choose **None**.
- **Fault Tolerance.** If the Application Gateway is duplexed, specifies the fault-tolerance strategy it uses.
- **Connection.** Choose whether the Gateway is Duplex (has both a Side 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 gateway.

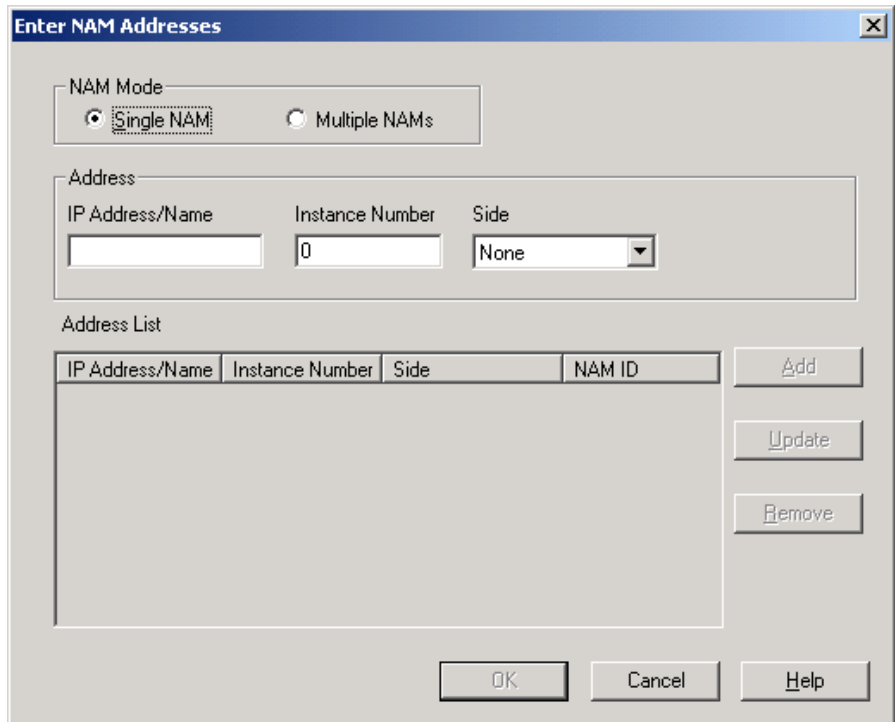
Step 5 Click the **Save** button to create the gateway.



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

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

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



The dialog box titled "Enter NAM Addresses" contains the following elements:

- NAM Mode:** Two radio buttons, "Single NAM" (selected) and "Multiple NAMs".
- Address:** A section with three input fields: "IP Address/Name" (empty), "Instance Number" (containing "0"), and "Side" (a dropdown menu showing "None").
- Address List:** A table with four columns: "IP Address/Name", "Instance Number", "Side", and "NAM ID". The table is currently empty.
- Buttons:** To the right of the table are three buttons: "Add", "Update", and "Remove". At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

Step 8 Specify the following information:

- **NAM Mode.** Select Single NAM or Multiple NAMs, depending on the number of NAMs connected to the selected application gateway.
- **IP Address/Name.** Enter the high priority IP address of the CICM. (Normally this is the public IP address, but if no public address is available, use the high priority private IP address.) This address *must* be the same address specified for the INCRP NIC on the targeted system. (You may 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 ICM software.

Step 10 When finished, click **Save** to save the changes.

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 should be less than the timeout value for the NAM's NIC.

How to set default values for the ICM Gateway

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

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

The screenshot shows the 'Application Gateway' dialog box. On the left, there are two radio buttons: 'Custom gateway' (unselected) and 'Remote ICM' (selected). To the right, there is a tabbed interface with four tabs: 'Timeout', 'Sessions', 'Heartbeats', and 'Errors'. The 'Timeout' tab is active, displaying three configuration items: 'Request' with a value of 500, 'Abandon' with a value of 5000, and 'Late' with a value of 400. Each value is in a text box with up and down arrows, followed by the unit 'milliseconds'.

Step 3 Use the Timeouts, Sessions, Heartbeats, and Error tabs to set the default values for the application gateway connections.

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

Installing the Remote Monitoring Suite

The last step in configuring the NAM machine is to install and configure the following Remote Monitoring Suite components:

- Listener
- LGMapper
- LGArchiver
- AlarmTracker Client

To install these components, follow the steps described in the *Cisco Remote Monitoring Administration Guide*.

Upgrading the NAM

For instructions on how to upgrade a NAM system, see the *4.6.2 to 5.0 ICM Software Upgrade Migration Guide*.



CICM Setup

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 Distributors (service provider distributor on NAM, customer distributors on CICM).
- Configure the CICM's INCRP NIC.
- Add or update components for a CICM instance.
- Delete instances on a CICM complex.



Tip

You should have a copy of the following Cisco ICM documentation available in *addition* to this manual in order to successfully complete CICM configuration: *Cisco ICM Software Installation Guide* and *Cisco Remote Monitoring Administration Guide*.



Note

If you are installing and configuring CICM systems that will be part of a Multiple NAM configuration, see also the installation and configuration instructions in the *Cisco Network Applications Manager (NAM) Multiple-NAM Setup and Configuration* manual.

Introduction to Instances

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

A single CICM complex may include multiple instances of the ICM—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 ICM components (Loggers, CallRouters, and Admin Workstations) 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.
- Creating the ICM gateway on the NAM.
- Setting up the CICM instance distributor on the NAM.
- Configuring the INCRP NIC.
- Updating the Listener configuration.

The following subsections explain these steps in detail. After completing these steps you can proceed to set up Peripheral Gateways and Admin Workstations at the customer premises.

Naming Conventions for Instances

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 ICM software converts the instance name to all lowercase.

The instance name is used in naming a registry subtree, a subdirectory of the \licm 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 Admin Workstation is named cust1_awdb.

Selecting the CICM Complex

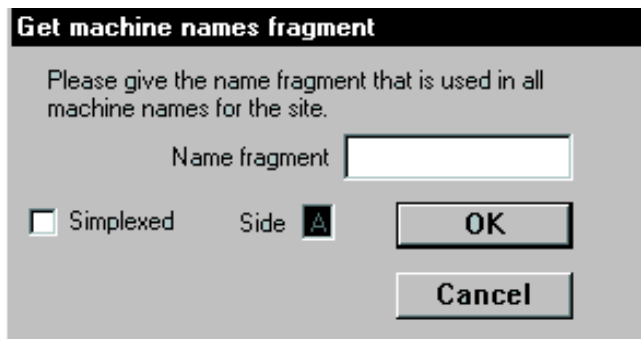
Choose which CICM complex will service this instance. Consider the current load on each CICM complex and the expected load for the new instance. Usually it is best to roughly balance the overall load among available CICM complexes. If all CICM complexes are nearing capacity, consider adding a new CICM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

Assigning an Instance Number to a CICM

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.

How to see instance numbers currently in use

- Step 1** On any Admin Workstation 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 \licm\bin directory on every Admin Workstation.) The Name Fragment dialog box appears.



- Step 3** Specify the machine name fragment that is used in all machines on your site. (For example, if Logger A is named geoxyzlgra, 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:

Instance number values

Instance Name	Router A	Router B	Logger A	Logger B
ins01	1	1	1	1
ins02	2	2	2	2
ins03	3	3	3	3
ins04	4	4	4	4
ins05	5	5	5	5
ins06	6	6	6	6
ins07	7	7	7	7
ins08	8	8	8	8
ins09	9	9	9	9
ins10	10	10	10	10
ins11	11	-1	11	11
ins12	12	-1	12	12
ins13	13	-1	13	13
ins14	14	-1	14	14
ins15	15	-1	15	15
ins16	16	-1	16	16
ins17	17	-1	17	17
ins18	18	-1	18	18
ins19	19	-1	19	19
ins20	20	-1	20	20
ins21	21	-1	21	21
ins22	22	-1	22	22
ins23	23	-1	23	23
ins24	24	-1	24	24
servb	-1	-1	-1	-1

Available Instance Numbers:

0

1.1

Close

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**.
-

How to add an instance to a CICM

- Step 1** On a CICM, start **Setup** from the Cisco ICM Admin Workstation group. The Cisco ICM Setup dialog box appears
- Step 2** Click **Add** in the ICM Instance section of the main Setup window. The Add Instance dialog box appears.
- Step 3** Enter the instance name and instance's domain. Specify the instance number you chose previously.
- Step 4** Click **OK** to submit the instance and return to the main Setup window.
-

Installing and Configuring 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.

How to install and configure a CICM Logger (Side A or Side B)

- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to install the Logger software.

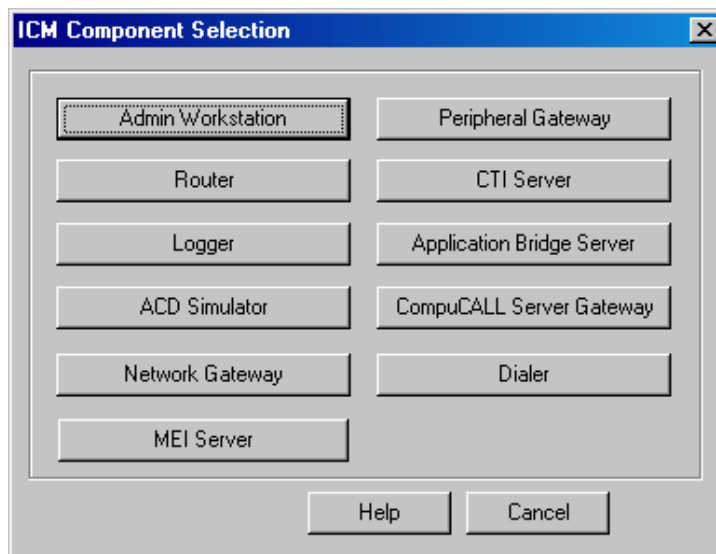
**Note**

If you are installing more than one ICM component on a single computer, you must run **SETUP.EXE** from the CD-ROM. For more information, see “[Post-Installation Setup and Installing Multiple Components](#)” in [Chapter 2, “NAM Installation and Configuration.”](#)”

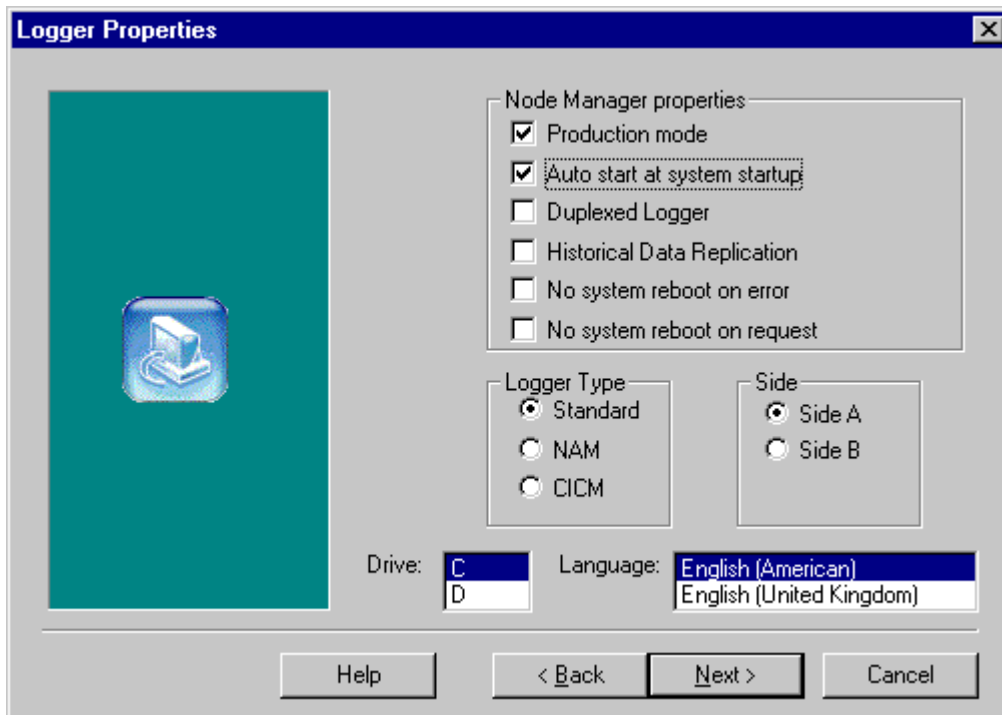
Step 2 In the Cisco ICM Setup dialog box, do the following:

- Select an **ICM Instances** value.
- Click the **Add** button in the *Instance Components* section.

The ICM Component Selection dialog box appears.



Step 3 Click **Logger**. The Logger Properties Window appears.



Step 4 Do the following:

- In the Node Manager Properties sections, select the following checkboxes:
 - **Production mode.** If this box is not checked, the ICM Node Manager runs in debug node.
 - **Auto start at system startup.** Always set this option.
 - **Duplexed Logger.** Check this box if the Logger is duplexed.
 - **Historical Data.** Check this box if the Logger passes historical data to an Admin Workstation configured as a Historical Data Server.
- In the Logger Type section, select **CICM**.

Step 5 Click **Next**. The Logger Component Properties window appears.

- Step 6** Select the **Phone Home** checkbox to enable the Logger to send the Listener customer event and message information via the NAM Support Architecture.
- Step 7** Click the Phone Home section's **Configure** button. The Phone Home Configuration window appears.

The **Phone Home Configuration** window is divided into three main sections:

- CSFS configuration:**
 - Customer name:
 - Site name:
 - Suppression limit:
 - Suppression time:
- Contacting Support:**
 - Heartbeat interval:
 - ☐ Send data over local network
 - User ID:
 - Password:
 - Primary Listener:**
 - Phone number:
 - Import domain:
 - Import system name:
 - Import directory:
 - Backup Listener:**
 - Phone number:
 - Import domain:
 - Import system name:
 - Import directory:
- Serial feed configuration:**
 - ☐ Enable
 - Com port:
 - Pipe name:
 - Speed:

At the bottom are buttons for **OK**, **Cancel**, and **Help**.

- Step 8** Specify the following:
- **CSFS Configuration.** Specify a **Customer name** and a **Site name**.
 - **Contacting Support.** Contact information for the network service provider primary and backup Listeners. Specify the following:
 - Either a Phone Number for a Remote Access Service (RAS) connection or a check in the Send Data Over Local Network option for a direct network connection.
 - A customer name as the Import Directory value.
 - Import System Name and Import Domain values pointing to the machine running the Listener.
- Step 9** Click the **OK** button to make the changes and close the dialog box.
- Step 10** Continue with the remaining Logger setup steps as described in the *Cisco ICM Software Installation Guide*, including creating the Central Database for the appropriate side (A or B).
-

Installing and Configuring 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.

How to install and configure CICM CallRouter software

- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to install the CallRouter software.

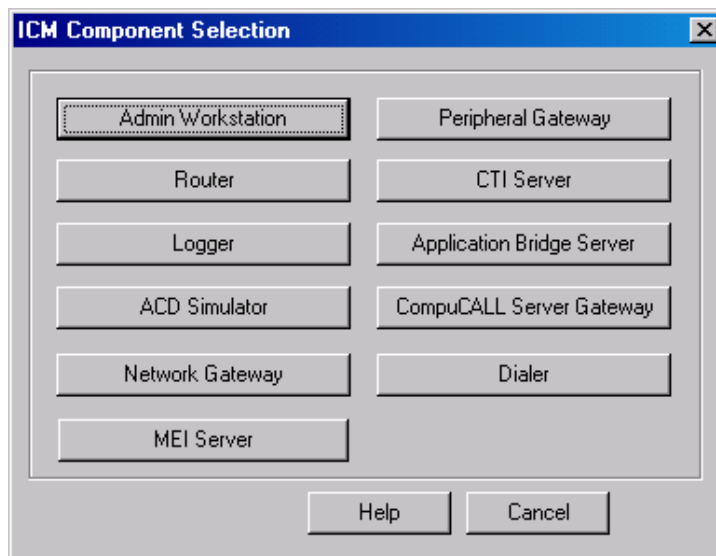
**Note**

If you are installing more than one ICM component on a single computer, you must run **SETUP.EXE** from the CD-ROM. For more information, see “[Post-Installation Setup and Installing Multiple Components](#)” in [Chapter 2, “NAM Installation and Configuration.”](#)”

Step 2 In the Cisco ICM Setup dialog box, do the following:

- Select the same **ICM Instances** value as you did for the CICM Logger.
- Click the **Add** button in the *Instance Components* section.

The ICM Component Selection dialog box appears.



Step 3 Click **Router**. The Router Properties Window appears.

Step 4 Make your selections and click **Next**. The Router Component Properties window appears.

Step 5 On the Router Component Properties window, select **INCRP NIC**.

Step 6 Continue with the remaining CallRouter setup steps.

**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.

Installing and Configuring CICM Distributors on Network AWs

To create configuration data for an instance, you must add the instance to a CICM Network Admin Workstation.

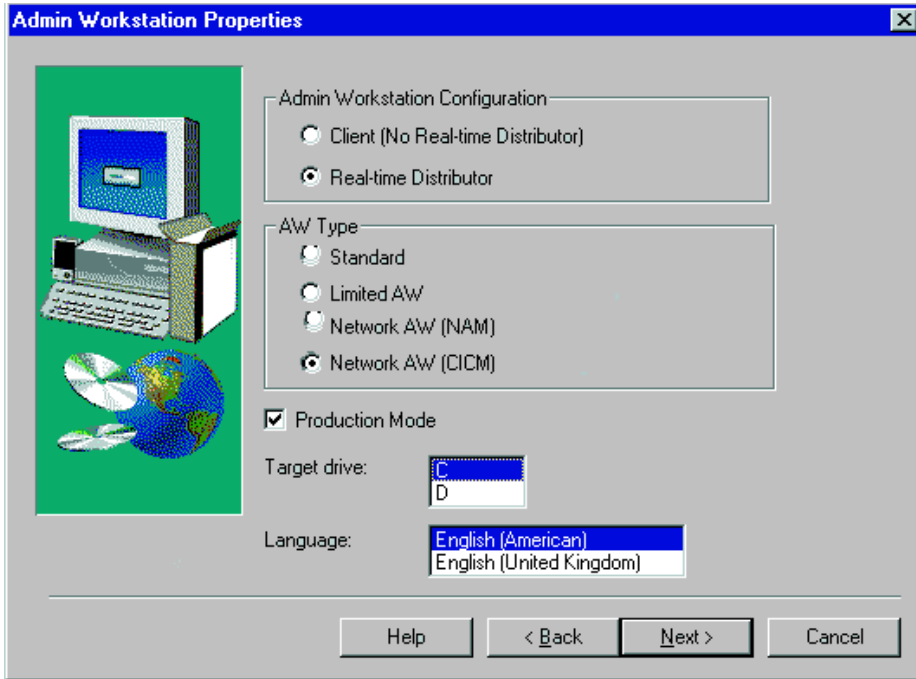
How to install and configure CICM Network Admin Workstation software

- Step 1** Follow the steps described in the *Cisco ICM Software Installation Guide* to install an Admin Workstation.

**Note**

If you are installing more than one ICM component on a single computer, you must run **SETUP.EXE** from the CD-ROM. For more information, see “[Post-Installation Setup and Installing Multiple Components](#)” in [Chapter 2, “NAM Installation and Configuration.”](#)

- Step 2** In the Cisco ICM Setup dialog box, do the following:
- Select the same **ICM Instances** value as you did for the CICM Logger and CallRouter. If the AW is on a different domain, enter the Central Controller domain name.
 - Click the **Add** button in the *Instance Components* section.
- The ICM Component Selection dialog box appears.
- Step 3** Click **Admin Workstation**. The Admin Workstation Properties Window appears.




- Step 4** In the Admin Workstation Properties dialog box, select **Network AW (C1CM)** as the AW Type.
- Step 5** Click the **OK** button to make the changes and close dialog box.
- Step 6** Continue with the remaining Admin Workstation setup steps.
-

Configuring the C1CM's INCRP NIC

The NAM communicates with the C1CM by means of an INCRP NIC. To set up the INCRP NIC for each instance on the C1CM, you must perform the following tasks:

- Define the INCRP NIC using the NIC Explorer tool.
- Add CallRouter configuration information using ICM Setup.

How to define the INCRP NIC

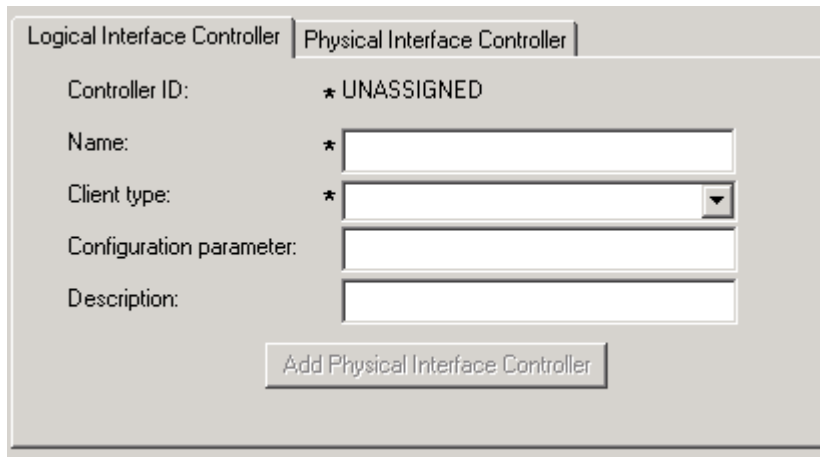
-
- Step 1** Within the ICM Admin Workstation group, double-click **AW Select**. The Select ICM AW Service window appears.
- Step 2** Select the instance you will be configuring.
- Step 3** From the ICM Configuration Manager, open the **NIC Explorer** tool. The NIC Explorer window appears.
- Step 4** 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:
- **Enterprise Name.** A 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** if this system will be part of a Multiple NAM configuration.

**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.

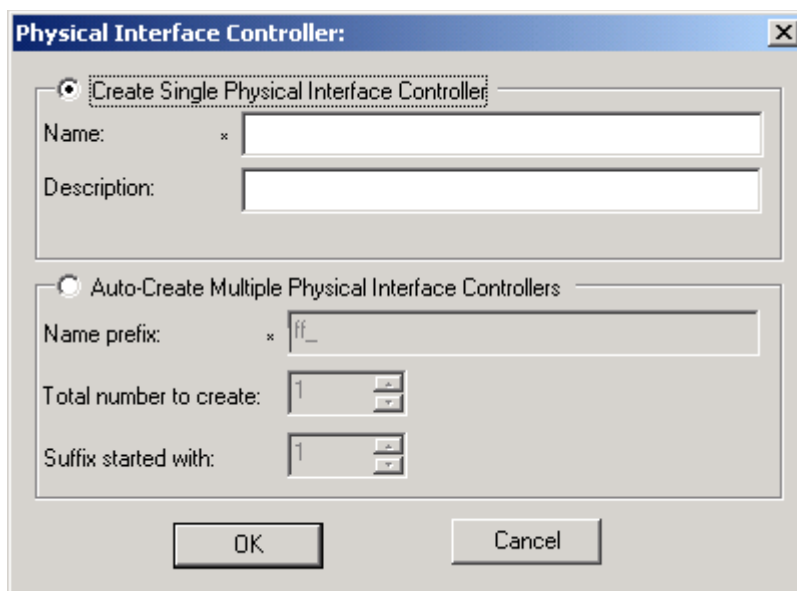


The dialog box has two tabs: "Logical Interface Controller" and "Physical Interface Controller". The "Physical Interface Controller" tab is active. It contains the following fields:

- Controller ID: ★ UNASSIGNED
- Name: ★ [Text Field]
- Client type: ★ [Dropdown Menu]
- Configuration parameter: [Text Field]
- Description: [Text Field]

At the bottom, there is a button labeled "Add Physical Interface Controller".

- Step 7** Click the **Add Physical Interface Controller** button. The Physical Interface Controller dialog box appears.



The dialog box is titled "Physical Interface Controller:". It has two radio buttons for selection:

- ☒ Create Single Physical Interface Controller:
 - Name: * [Text Field]
 - Description: [Text Field]
- ☐ Auto-Create Multiple Physical Interface Controllers:
 - Name prefix: * ff_ [Text Field]
 - Total number to create: [Spin Box with value 1]
 - Suffix started with: [Spin Box with value 1]

At the bottom, there are "OK" and "Cancel" buttons.

- 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 appears, displaying the information you specified, and an ID value of UNASSIGNED.
- Step 10** Enter the following on the Routing Client tab fields:
- **Enterprise Name.** A 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, see the *Cisco ICM Software Installation Guide*.

- 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.

How to complete the INCRP NIC setup

To provide detailed set-up information for the NIC, you need to rerun ICM Setup on each CICM CallRouter for the instance.

- Step 1** In the Cisco ICM Setup dialog box, do the following:
- Select an **ICM Instances** value
 - Select **Router** from the Instance Components list and click **Edit**.

The Router Component Properties window appears.

- Step 2** Click **Next**. The Router Components Properties dialog box appears.

- Step 3** Select the **INCRP** checkbox and click the **Configure** button to its right. The INCRP NIC Properties dialog box appears.

INCRP NIC Properties

Network Interface Controller properties

Physical controller: IP name: Handshake timeout:

Client ICM

Enable	Description	Client Id	AppGatewayId	Side A address:	Side B address:
<input checked="" type="checkbox"/>	First NAM Pair	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>		<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>

OK Cancel Help

Step 4 Enter the following values:

- **Physical Controller ID.** Enter one of the physical controller IDs for the INCRP NIC on the CICM. If the NIC is duplexed, be sure to enter a different physical controller ID on each side.
- **IP Name.** Enter the hostname of the CICM machine.
- **Handshake Timeout.** Enter the milliseconds to wait for a handshake response from the routing client.
- **Client ICM.** In this section, enter the following information for each Client ICM that acts as a Service Control Point (SCP) for the INCRP NIC
 - **Enable.** Check the box to enable the Client ICM
 - **Description.** Enter a description of the Client ICM.

- **Client ID.** Enter the name of the Client ICM machine. If you are setting up the NIC for a NAM system, enter the NAM ID.
- **AppGateway ID.** Specify the ApplicationGatewayID for the INCRP NIC as configured in the Client ID database.
- **Side A address.** Enter the high priority visible address of the NAM for the Side A SCP.
- **Side B address.** Enter the high priority visible address of the NAM for the Side B SCP.

**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.

Consideration for multiple NAM/CICM routing clients

For multiple NAM/CICM routing client configurations that will use CICM Replication (see the section [“NAM to CICM DN and Label Replication”](#) in [Chapter 4, “Customer Concept”](#)), 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 at 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.

Update the Listener Configuration

As a final step, you must add the CICM instance to the Listener configuration. Follow the steps described for updating the Listener configuration in the *Cisco Remote Monitoring Administration Guide*.

Adding and Updating Components for Instances

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

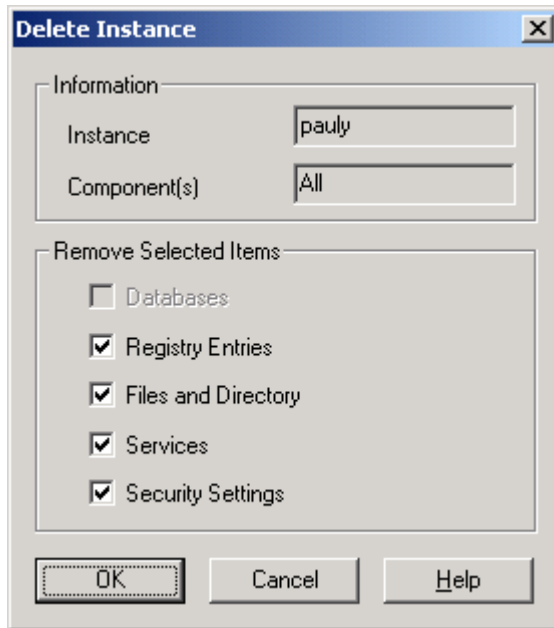
- To add a new component for an instance, run Setup. From the ICM Setup main screen, select the instance in the ICM Instances box and then click the Add button in the Instance Components box.
- To upgrade an existing component to the latest release, select the instance and the component and then click the Edit button in the Instance Components box.
- To upgrade all installed components for all instances, click the Upgrade All button. This option does *not* give you the opportunity to change configuration settings; it only copies the latest files and applies the current configuration settings.

Deleting an Instance

The following steps describe the process for deleting an instance.

How to delete an instance

-
- | | |
|---------------|--|
| Step 1 | Use the Service Control utility to stop the services for that instance on all CICM machines and Admin Workstations. |
| Step 2 | Run ICM Setup on each machine where components for the instance are installed. Select the instance in the ICM Customers list and click the adjacent Delete button. The Delete Instance dialog box appears. |



- Step 3** Choose which items you want Setup to delete for the instance. (The best practice is to let Setup remove all items it can.) Click the **OK** button. Setup displays status messages as it deletes the items.
- Step 4** When the process completes, click the **Close** button and exit Setup.
- Step 5** Using ICMDBA, delete all databases for the instance on Loggers and Admin Workstations. This also deletes any dedicated data devices that were created for the instance and the file system file associated with each of the data devices.
- Step 6** From the NAM associated with the instance, delete or modify any scripts that reference the instance's system. Also delete the Application Gateway for the instance; this forces deletion of the related Application Gateway Connections.
-



Customer Concept

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

Overview of Customer Concept

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, Admin Workstations)—some of which may be duplexed—typically installed on several different computers. A single computer may run multiple components of a single instance or components of multiple instances.

A *customer* is an organization that uses the 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, etc. are associated with the instance rather than a specific customer. Therefore, customers who share an instance cannot have uniquely associated Peripheral Gateways.

[Table 4-1](#) summarizes what data can be associated with a specific customer and what data are shared by an entire instance.

Table 4-1 Customer and Instance Data

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; application gateways

**Note**

No special security is applied at the customer level. Any Admin Workstation 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/Internet Script Editor users who have access to only the data for a specific customer. (These users do not have direct access to an Admin Workstation. 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. [Table 4-2](#) summarizes the abilities of these two customer types.

Table 4-2 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, etc.	Percent allocation routing and scheduled targets routing only
Dedicated Peripheral Gateways	No dedicated Peripheral Gateways
Admin Workstation, Internet Script Editor, and WebView access	Internet Script Editor and WebView 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, etc. In Configure ICM 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, etc.



Note

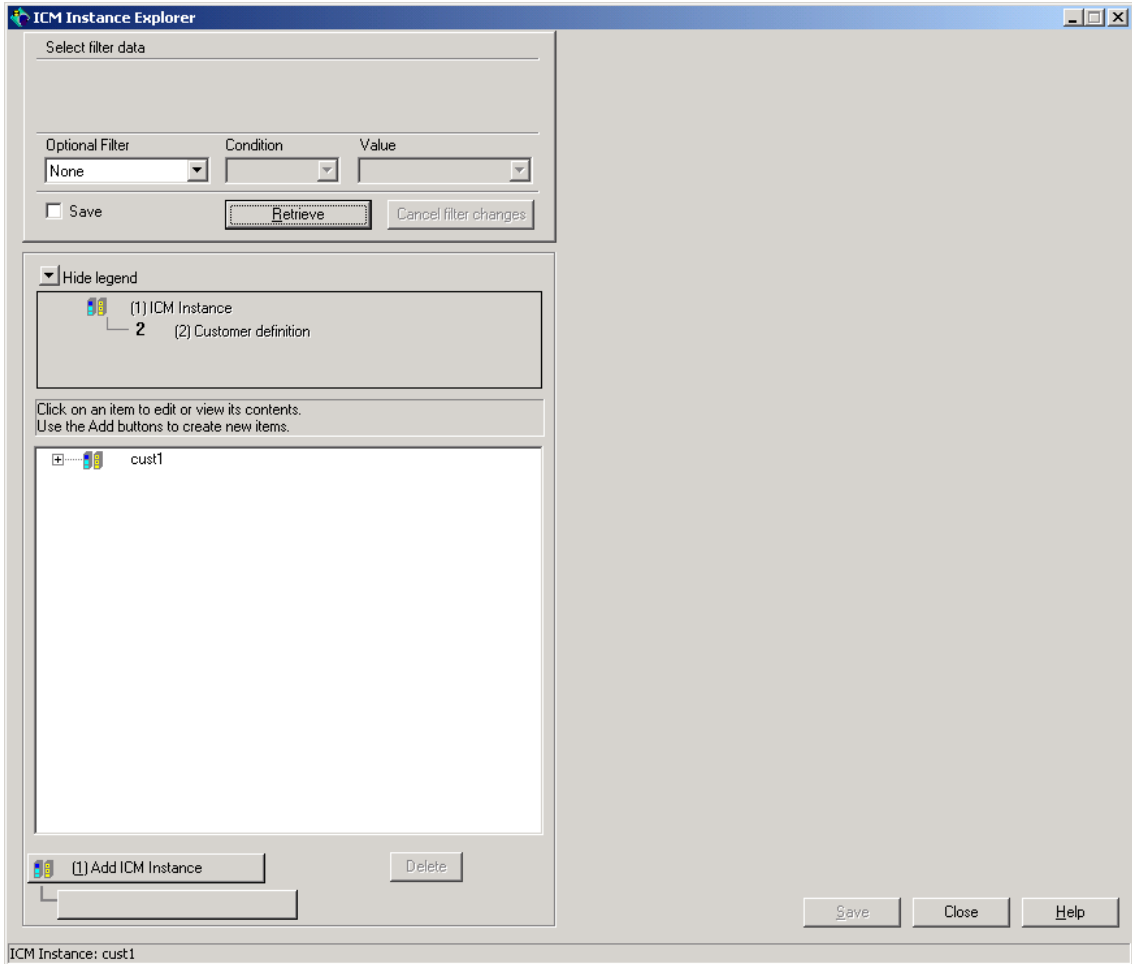
Again, Customer Concept does not provide security between business units. It only provides a way of organizing certain data and the convenience of allowing you to selectively view those data.

Configuring Customer Concept

Perform the following steps to configure Customer Concept.

- Step 1** From within the ICM Admin Workstation Group open AW Select and double click on the Instance.
- Step 2** From within the ICM Admin Workstation Group, open the Configuration Manager.
- Step 3** Open **Configure ICM > Enterprise > ICM Instance > ICM Instance Explorer**.
- Step 4** Click on **Retrieve**.

Configuring Customer Concept



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 AW (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.
- Hosted IPCC (HIPCC) and Hosted ICM – 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,”](#) 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 the next section for details).

NAM Level

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 the next section 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 the 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 Distributor on Network AW (CICM). This CICM Distributor may be on a separate Network AW machine or may co-reside with the NAM instance Network AW (NAM) and other CICM instance Network AWs. The CICM Distributor 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 AW at all times.

Because the Network Applications Manager Replication Process (NIRP) 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**:

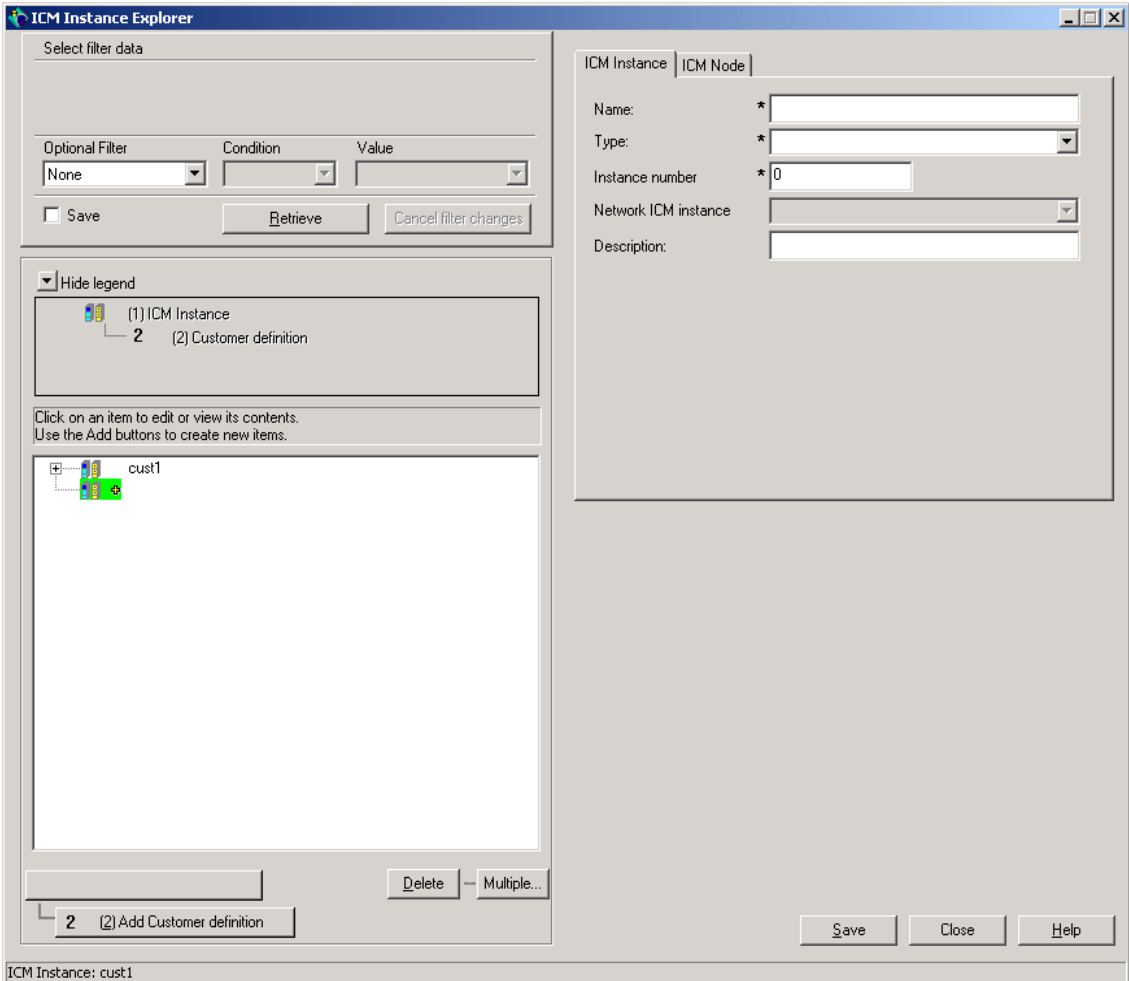
- Configure all associated CICMs as ICM instances on the NAM so that CICM Replication can forward changes to the appropriate CICM Distributor.
- Configure the associated CICM customer(s) within each CICM instance on the NAM. If Customer Concept is implemented at the CICM level (Advanced Services) each 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 AW Distributor(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.

Configuring CICM Replication at NAM Level

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

-
- | | |
|---------------|--|
| Step 1 | From within the ICM Admin Workstation Group open AW Select and double click on the NAM instance. |
| Step 2 | From within the ICM Admin Workstation Group, open the Configuration Manager. |
| Step 3 | Open Configure ICM > Enterprise > ICM Instance > ICM Instance Explorer . |
| Step 4 | Click on Retrieve . |

NAM to CICM DN and Label Replication



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 5 Click on **Add ICM Instance**.

Step 6 Under ICM Instance Tab:

- Enter CICM instance name.

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

Step 7 Under ICM Node Tab:

The screenshot shows a software window titled "ICM Instance" and "ICM Node". It contains a table for "ICM Nodes associated with this instance" with columns "Name" and "Description". To the right of the table are "New" and "Delete" buttons. Below the table is a section titled "Currently Selected Node" with several input fields: "System domain: *", "System name: *", "Node type: *" (with a dropdown arrow), "Name: *", "Configuration parameter:", and "Description:". The "System domain" and "System name" fields are empty, while the others contain placeholder text.

- Click on **New**
- Under Currently Selected Node:
 - Enter Domain Name of machine on which the CICM Network AW resides
 - Enter System Name (hostname) of machine on which the CICM Network AW resides
 - From pulldown menu select primary or secondary distributor (secondary is the backup CICM Network AW in case the primary is not available)
 - Save

Step 8 Click on **Add Customer Definition**.

Step 9 Under Customer Definition Tab:

The screenshot shows a dialog box titled 'Customer definition' with two tabs: 'Customer definition' and 'Customer options'. The 'Customer definition' tab is active. It contains the following fields:

- Name:** A text input field with a required field indicator (star) to its left.
- Network VRU:** A dropdown menu currently showing 'NONE'.
- Description:** A text input field.
- Feature control set:** A dropdown menu currently showing 'NONE'.

- Enter the customer name within the CICM instance. If this is an Advanced Service CICM instance, repeat this Add process until you have entered the names of each individual customer within the instance. If this is a Hosted IPCC/ICM 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 pulldown 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 pulldown menu

Step 10 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 11 Click **Save**.

Step 12 Open NIC Explorer. Click **Retrieve** and define the network routing client.

Since DNs and labels have a 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.

Configuring CICM Replication at CICM Level

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

-
- | | |
|---------------|--|
| 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.

Hosted IPCC and Hosted ICM with Network VRU

This section discusses how to implement Customer Concept on Hosted IPCC and Hosted ICM with Network VRU instances.

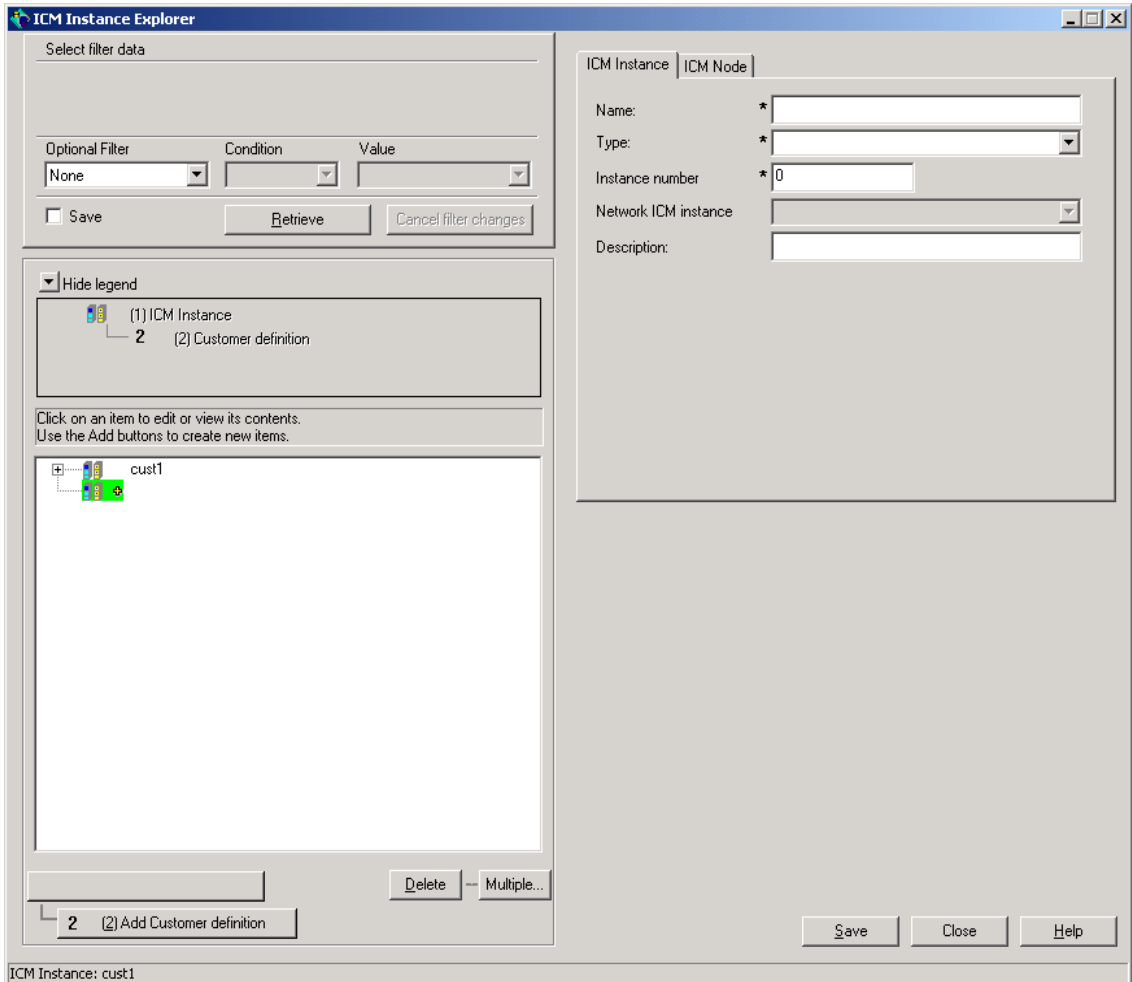
NAM Level

Implementation of Customer Concept is optional but highly recommended for management and reporting purposes within the NAM Instance which provides Network VRU services to Hosted IPCC (CICM) and Hosted ICM (CICM) Instances.

NAM to CICM DN and Label Replication is optional. (see [“NAM to CICM DN and Label Replication”](#)).

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

-
- Step 1** From within the ICM Admin Workstation Group open AW Select and double click on the NAM instance.
 - Step 2** From within the ICM Admin Workstation Group, open the Configuration Manager.
 - Step 3** Open **Configure ICM > Enterprise > ICM Instance > ICM Instance Explorer**.
 - Step 4** Click on **Retrieve**.



- Step 5** 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 on **Add ICM Instance**.
- Step 7** Under ICM Instance Tab:
- Enter CICM instance name

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

Step 8 Click on Add Customer Definition

Step 9 Under Customer Definition Tab:

The screenshot shows a configuration window with two tabs: 'Customer definition' (selected) and 'Customer options'. Under the 'Customer definition' tab, there are four input fields:

- Name:** A text input field with a required field indicator (star).
- Network VRU:** A dropdown menu currently showing 'NONE'.
- Description:** A text input field.
- Feature control set:** A dropdown menu currently showing 'NONE'.

- Enter the customer name within the CICM instance. Since this is a Hosted IPCC/ICM 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 pulldown 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 pulldown menu.

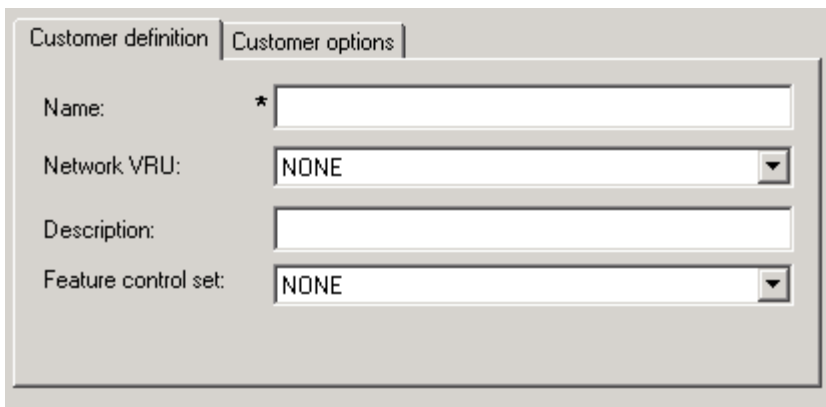
Step 10 Under Customer Options Tab, check **Bill for VRU Time**. This is a flag that can be set and used by service providers to indicate how Network VRU usage is to be billed.

Step 11 Click **Save**.

CICM Level

To implement Customer Concept on a Hosted IPCC or Hosted ICM CICM instance, perform the following steps.

- Step 1** From within the ICM Admin Workstation Group open AW Select and double click on the CICM instance for Hosted IPCC or Hosted ICM.
- Step 2** From within the ICM Admin Workstation Group, open the Configuration Manager.
- Step 3** Open **Configure ICM > Enterprise > ICM Instance > ICM Instance Explorer**.
- Step 4** Click on **Retrieve**.
- Step 5** 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 6** Under Customer Definition Tab:



Customer definition | Customer options

Name: *

Network VRU:

Description:

Feature control set:

- Select the Network VRU assigned to this customer under the Network VRU pulldown 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 pulldown menu.

Step 7 Click **Save**.



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.

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 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 might be desirable to run an Advanced Services ICM on its 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 the 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, etc.

No special security is applied at the customer level. Any Admin Workstation 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 Admin Workstation to administer the Advanced Services ICM as any other ICM instance. Advanced Services customers should only have access to their data using WebView and Internet Script Editor. These tools will prevent a customer from accessing other customer's data. This is achieved by having a user login with a personal userid and password. The userid is tied to a specific customer and WebView and Internet Script Editor will only exposes this customer's data. Each individual user also has a profile, called a Feature Set that determines his or her access rights in detail.

[Table 5-1](#) provides an overview of the tools used by the Service Provider and the end-customer for day-to-day management tasks.

Table 5-1 Service Provider Tools

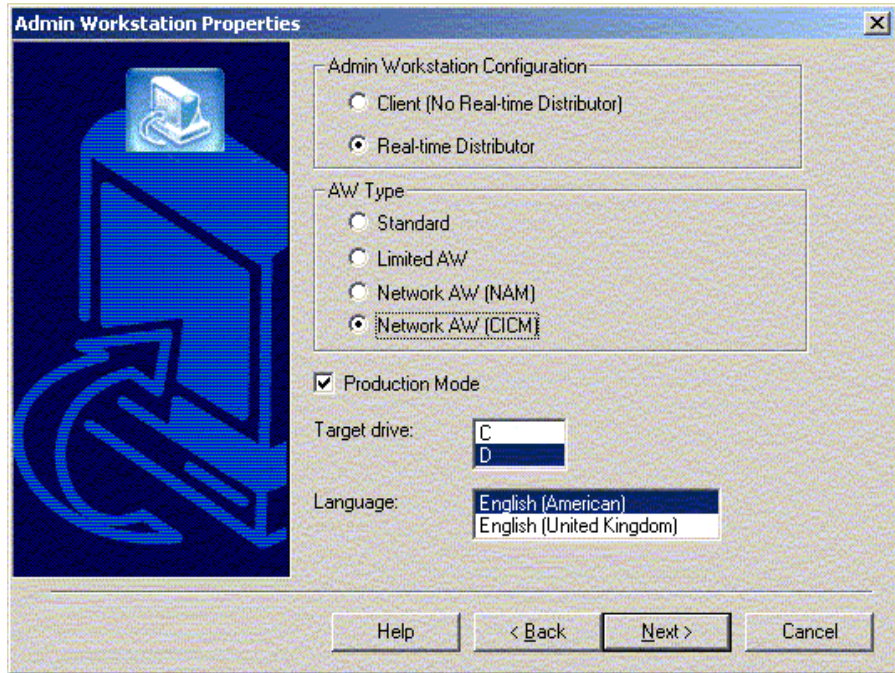
Task	Service Provider (Tool)	End-user (Tool)
Configuration	Configuration Manager	N/A
Scripting		
New scripts	Administrative Workstation Script Editor	Internet Script Editor in full edit mode
Structural script changes	Administrative Workstation Script Editor	Internet Script Editor in full edit mode
Changing script parameters	Administrative Workstation Script Editor	Internet Script Editor in quick edit mode
Reporting		
Defining and running report based on existing template	WebView, using Call Type reporting and scheduling, exporting and email options	WebView, using Call Type reporting
Defining custom reporting template	Using Infomaker to define new Call Type templates or modify existing ones	N/A

Setup and Configuration of an Advanced Services ICM Instance

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

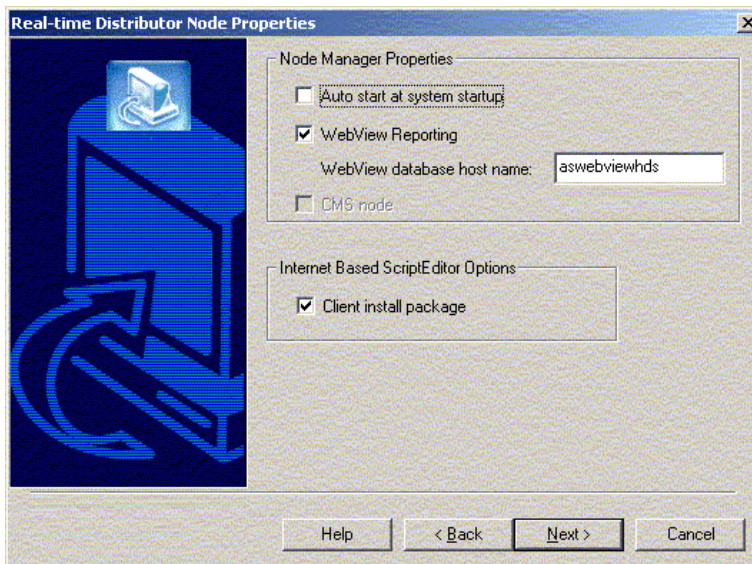
- Install a new ICM instance This includes installing a Logger, Router with INCRP NIC and one or more Administrative Workstations (Distributor instances) for the Service Provider to manage the service. Do not configure or install any Peripheral Gateways (PG), since they are not used by Advanced Services.
- Install one or more WebView and Internet Script Editor Servers that will act as web servers for end-customer use. WebView and Internet Script Editor servers are setup as installation options of an Administrative workstation turning the Administrative workstation into a WebView and or Internet Script Editor server. The server can at the same time function as a normal Administrative Workstation as well. A WebView server will fetch real-time data for reporting purposes from its local distributor or from another Administrative Workstation's real-time distributor. Historical data will be fetched from either the Advanced Services ICM logger or an Administrative workstation with the Historical Data Server (HDS) option installed. This could be the same or a different Administrative Workstation as the WebView server. For performance reasons it is not recommended to have the WebView server use Logger data for historical reporting purposes. Better scalability is achieved by having the WebView server use another Administrative Workstation with HDS option for historical reporting.

When running setup to install an Administrative Workstation, in the Administrative Workstation Properties screen select Real-time Distributor and Network AW (CICM).



In the Real-time Distributor Node Properties box check the WebView Reporting check box if you want to make the AW a WebView server. In the box labeled WebView database hostname fill in the machine name of the Administrative workstation with HDS option that the WebView server will use to fetch real-time and historical data from.

Check the Client Install package box if you want to make the Administrative Workstation an Internet Script Editor server. This will also install the software required for end-users to download the Internet Script Editor client software.



The remainder of the setup is identical to setting up an Admin Workstation.

Note that WebView contains many standard reporting templates that are not applicable to Advanced Services, such as Services templates. There are also reporting templates that a Service Provider probable does not want to expose to an end-customer, such as Routing Client templates. After installing the WebView server, these templates can be removed using Infomaker. It is recommended to remove all standard reporting templates, except Call Type templates. Detailed instructions on how to use Infomaker are provided in the *Cisco ICM Customer Screen Builder Tutorial*.

- Configure the Network VRU according to the instructions in [Chapter 9, “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 [Table 5-2](#).

Table 5-2 Customer Configuration Data

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	User List
Call Type	Required	Call Type List
Dialed Number	Required ¹	Dialed Number List
Label	Required unless dynamic labels are used, which is not recommended for security reasons.	Label List
Network VRU Script	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

1. Population of Dialed Numbers and Labels in the Advanced Services ICM can be automated when CICM replication is used. See [Chapter 4, “Customer Concept.”](#)

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)

Configuration of a new Advanced Services Customer

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

Feature Control Set

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.

Feature Control Set List

Select filter data

Optional Filter: None Condition: Value:

☐ Save

Feature Control Set

Name: MomsandDads

Attributes

Name: *MomsandDads

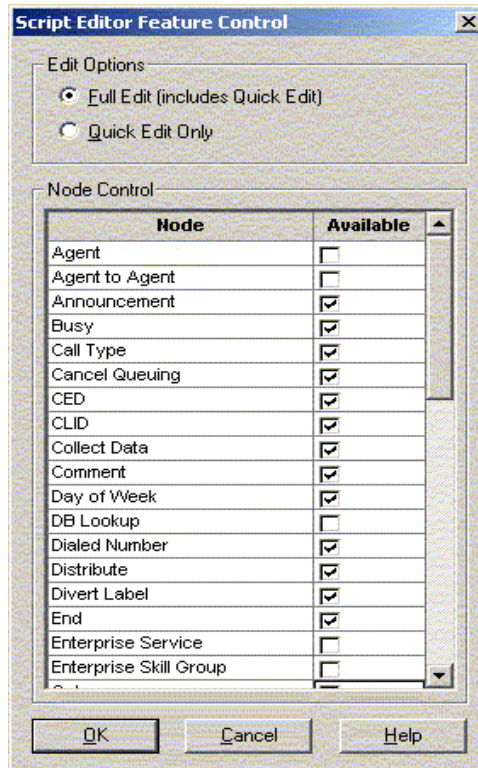
Description: Mom's and Dad's Hardware Store

Application Name	Enabled	Advanced
Script Editor	<input checked="" type="checkbox"/>	...
Call Type Bulk Edit	<input type="checkbox"/>	
Dialed Number Bulk Edit	<input type="checkbox"/>	
Dialed Number Plan Bulk Edit	<input type="checkbox"/>	
Label Bulk Edit	<input type="checkbox"/>	
Network VRU Script Bulk Edit	<input type="checkbox"/>	
Scheduled Target Bulk Edit	<input type="checkbox"/>	
VRU Port Map Bulk Edit	<input type="checkbox"/>	
Device Target Bulk Edit	<input type="checkbox"/>	
Trunk Group Bulk Edit	<input type="checkbox"/>	
Trunk Bulk Edit	<input type="checkbox"/>	
Agent Bulk Edit	<input type="checkbox"/>	

ICM Instance: icm01

Configuration of a new Advanced Services Customer

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 should not provide access to. For Advanced Services, the following nodes should 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 are not recommended for end-customer access since they might expose other customers' data. It is possible for Advance Services Scripts to use these nodes for database lookups. The DB Lookup and Application Gateway configuration should be controlled entirely by the Service Provider and not by the end-customer. An end-customer should 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 when a user associated with this customer does not have a user specific feature set associated.

Configuration of a new Advanced Services Customer

ICM Instance Explorer

Select filter data

Optional Filter	Condition	Value
None		

☐ Save

☒ Hide legend

- (1) ICM Instance
 - 2 (2) Customer definition

Click on an item to edit or view its contents.
Use the Add buttons to create new items.

- icm01
 - 2 icm01
 - 2 MomsandDads

2 (2) Add Customer definition

ICM Instance: icm01

ICM Instance | ICM Node

Name: * icm01

Type: * Standard

Instance number: * 1

Network ICM instance:

Description:

Customer definition | Customer options

Name: * MomsandDads

Network VRU: ISN

Description:

Feature control set: MomsandDads

User

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

- In the Domain field, type 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 and Internet Script Editor servers.
- The Username 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. If the AD account already exists, the password for the account needs to be entered.
- Leave the 'User can create other users' check box unchecked. If this is an existing AD account the AD account settings will be left unchanged.
- By checking the Read-only box this user will not be able to create or change any routing scripts. His feature set will determine which scripts he can view. By unchecking this box, the users feature set will determine what routing scripts the user can get access to and change or create.
- Check the WebView and Internet Script Editor only box and select the customer that this user is associated with.
- Select the feature set that needs to be associated with this user. If this setting is left to None, the Customer level feature set will be used.

Configuration of a new Advanced Services Customer

User List

Select filter data

Feature control set: <All>

Customer: <All>

Optional Filter: None Condition: Value

☐ Save

User

Name
S1_webuser01
S1_winijenh

Attributes

Domain name: * S1

User name: * webuser01

Description:

Password:

Confirm password:

☐ Can create other user accounts

☐ Read only

☐ WebView and Internet Script Editor only

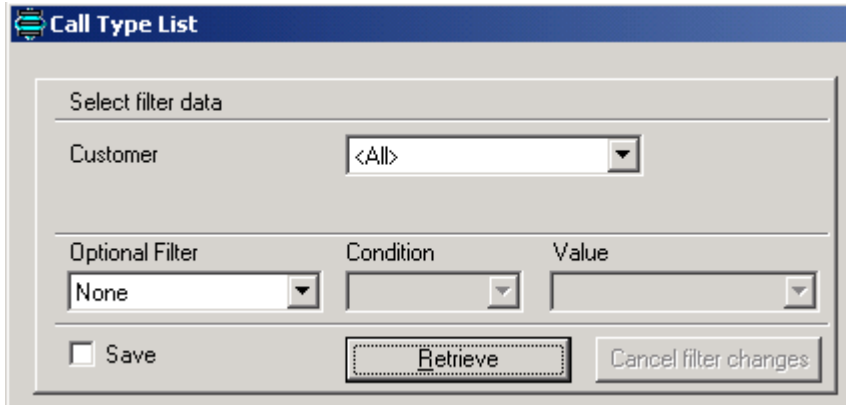
Customer: All Customers

Feature control set: <None>

ICM Instance: icm01

Call Type

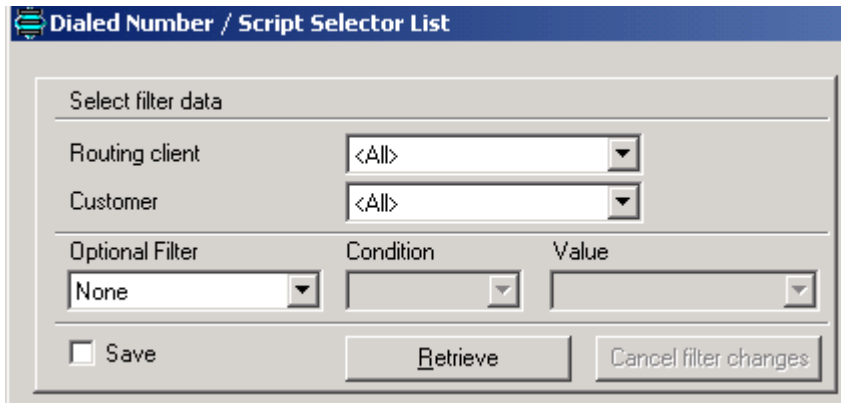
Configure one or more call types for this customer using the Call Type List tool. Select the associated customer from the Customer dropdown menu.



The **Call Type List** dialog box is used to filter call types. It features a 'Select filter data' section with a 'Customer' dropdown menu set to '<All>'. Below this is an 'Optional Filter' section with three dropdowns: 'Optional Filter' set to 'None', 'Condition', and 'Value'. At the bottom, there is a 'Save' checkbox, a 'Retrieve' button, and a 'Cancel filter changes' button.

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 dropdown menu.

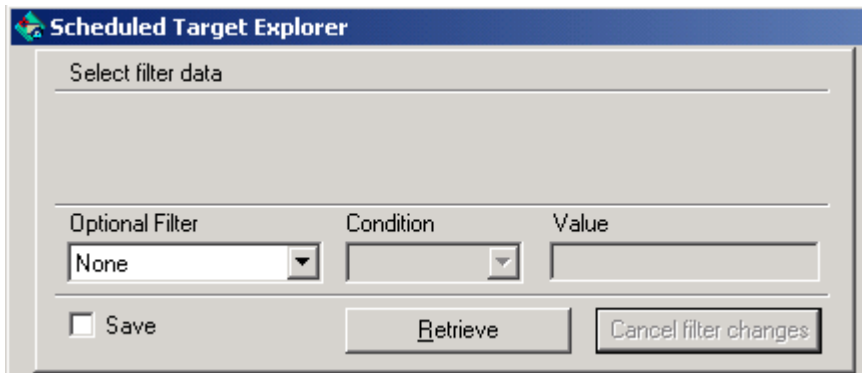


The **Dialed Number / Script Selector List** dialog box is used to filter dialed numbers. It features a 'Select filter data' section with two dropdown menus: 'Routing client' and 'Customer', both set to '<All>'. Below this is an 'Optional Filter' section with three dropdowns: 'Optional Filter' set to 'None', 'Condition', and 'Value'. At the bottom, there is a 'Save' checkbox, a 'Retrieve' button, and a 'Cancel filter changes' button.

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.

Scheduled Target

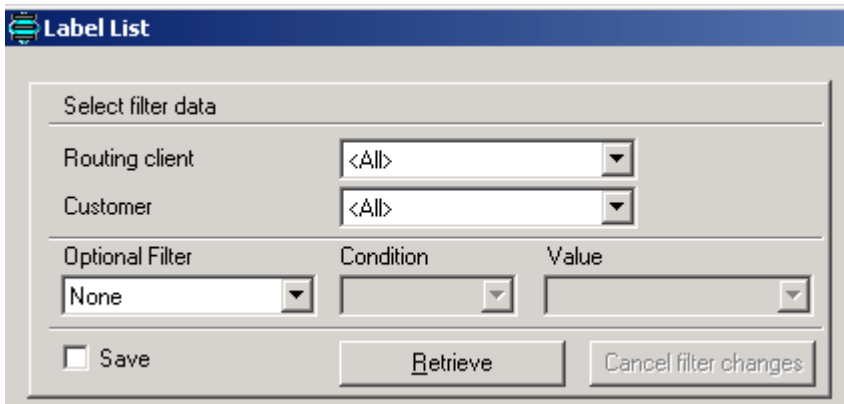
Configure one or more Scheduled Targets for this customer using Scheduled Target Explorer. Select the associated customer from the Customer dropdown menu.



The **Scheduled Target Explorer** dialog box features a title bar with a small icon and the text "Scheduled Target Explorer". Below the title bar is a section labeled "Select filter data" with a horizontal line underneath. Further down, there are three columns: "Optional Filter" with a dropdown menu showing "None", "Condition" with a dropdown menu, and "Value" with a text input field. At the bottom, there is a checkbox labeled "Save", a button labeled "Retrieve", and a button labeled "Cancel filter changes".

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 dropdown menu.



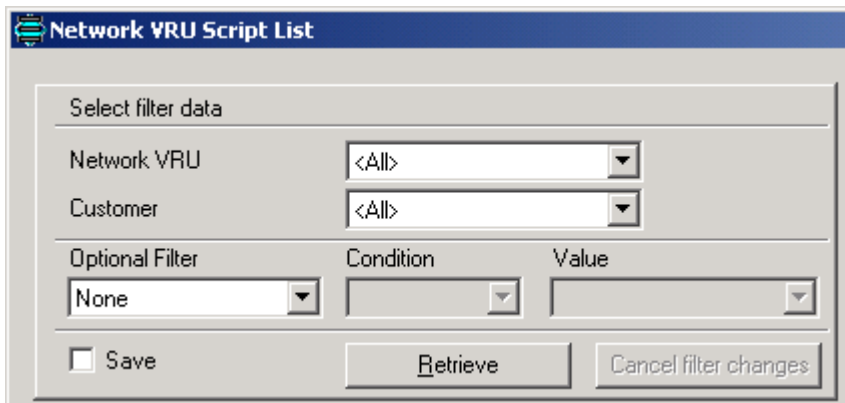
The **Label List** dialog box has a title bar with a small icon and the text "Label List". Below the title bar is a section labeled "Select filter data" with a horizontal line underneath. Below this line are two rows of dropdown menus: "Routing client" with "<All>" and "Customer" with "<All>". Below these are three columns: "Optional Filter" with a dropdown menu showing "None", "Condition" with a dropdown menu, and "Value" with a dropdown menu. At the bottom, there is a checkbox labeled "Save", a button labeled "Retrieve", and a button labeled "Cancel filter changes".

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 dropdown menu.

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 dropdown menu.



The screenshot shows the 'Network VRU Script List' dialog box. It has a title bar with a Cisco logo and the text 'Network VRU Script List'. Inside the dialog, there is a section titled 'Select filter data'. Below this, there are two dropdown menus: 'Network VRU' and 'Customer', both currently set to '<All>'. Below these, there is a section with three dropdown menus: 'Optional Filter' (set to 'None'), 'Condition', and 'Value'. At the bottom of the dialog, there are three buttons: 'Save' (with an unchecked checkbox next to it), 'Retrieve', and 'Cancel filter changes'.

Routing Script

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 Customer, 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 to the customer and holding it there briefly will show the default business unit.



Administrative Tools

The Network Applications Manager (NAM) product includes tools that help you administer your NAM configuration. This chapter discusses three of these tools:

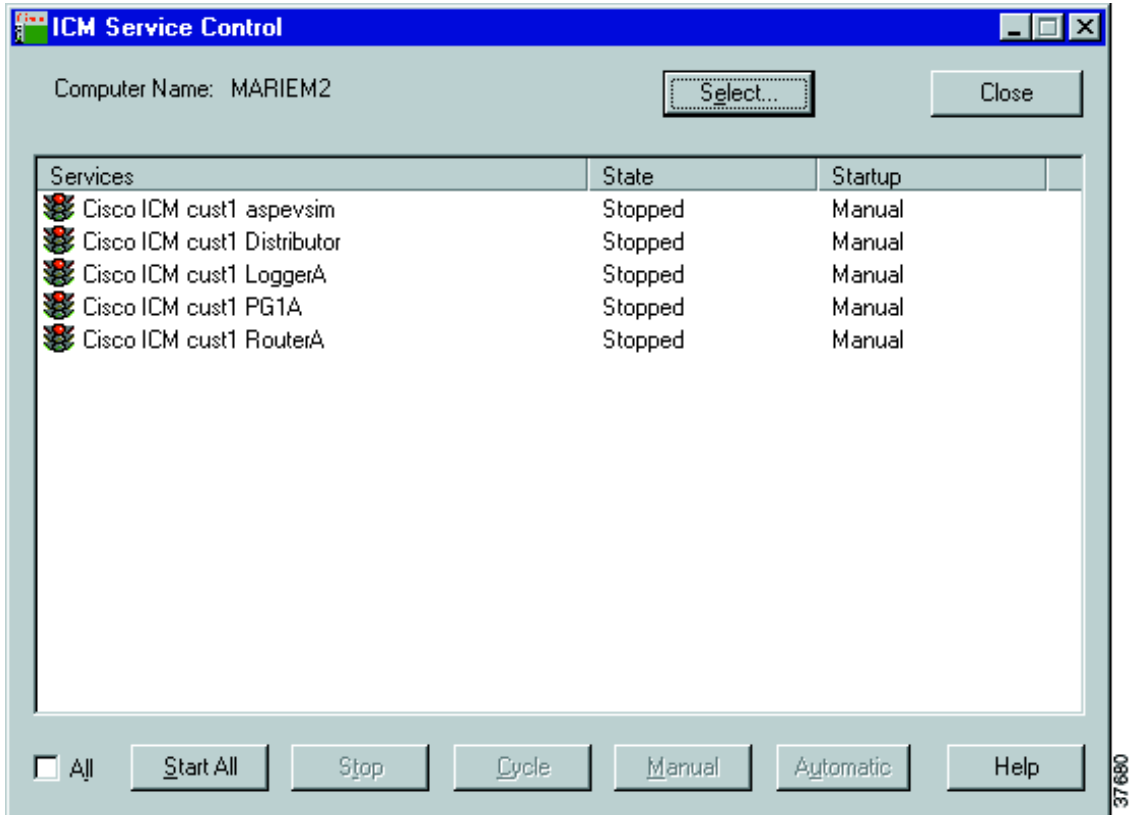
- Service Control
- AW Select
- CICM Monitor

Service Control

The Service Control tool lets you view, stop, and start Windows 2000 services related to the ICM software. This tool is installed on each Admin Workstation, CallRouter, Logger, and Peripheral Gateway.

How to start Service Control

-
- Step 1** Start **Service Control** from the **ICM Admin Workstation** group. The Service Control window opens.



Step 2 Specify the following:

- **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.

- **Select.** (Button) Click to choose another computer. You can then view and control services on that machine remotely.
 - **Cycle.** (Button) Stops and then restarts an active service in a single action.
 - **Manual** and **Automatic.** (Buttons) Let you switch the startup mode for a service between manual (user initiated) and automatic (starts when the computer is turned on).
-

AW Select

The AW Select tool lets you choose which instance to use at a network Admin Workstation.

You can have up to 25 AW services running on an Admin Workstation at once. Although you can only generate reports or view real-time data on one instance at a time, you *can* switch to another instance at any time. This makes it possible to generate reports and view real-time data for multiple instances from a single Admin Workstation.

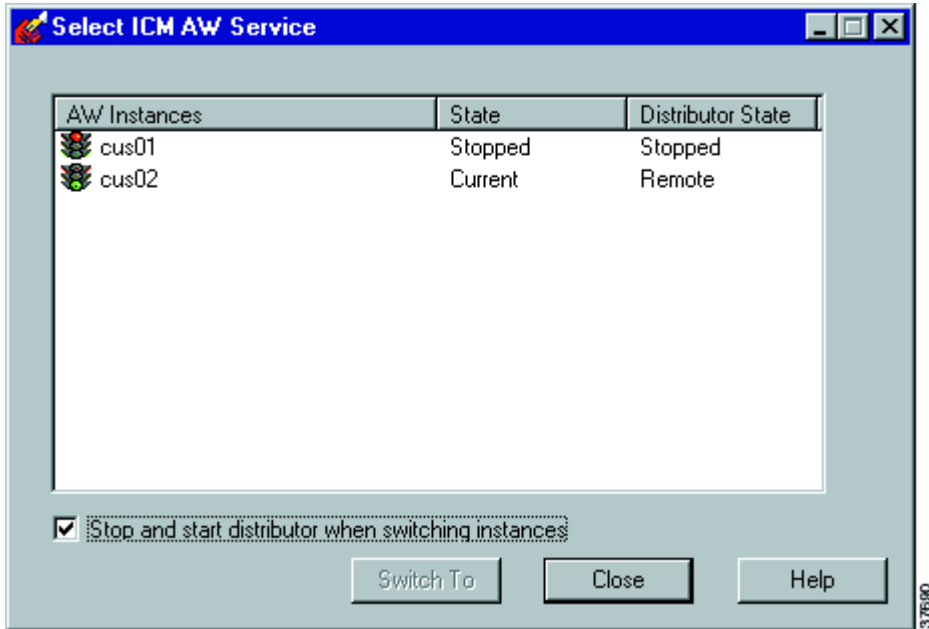


Note

To receive an overview of routing performance data from multiple instances simultaneously, use CICM Monitor as described in the [“Customer ICM Monitor”](#) section on page 6-5.

How to use AW Select

-
- Step 1** Start **AW Select** from the **ICM Admin Workstation** group. The Select ICM AW Service dialog box appears.



Step 2 Choose the service for the instance you want and click the **Switch To** button. The AW does the following:

- Stops any other AW services that are running on the current machine.
- Starts the AW service that you selected.



Note

If the Stop and Start Distributor when Switching Instances box is checked when you click **Switch To**, the distributors for all instances except the selected instance are stopped and the distributor for the selected instance is started.

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

Customer ICM Monitor

The Customer ICM software (CICM) Monitor is a diagnostic tool that lets you connect to a CICM complex and view near real-time call routing performance for all the instances on that CICM complex. CICM Monitor gathers and displays information that you can use to diagnose potential problems with CICM performance.

This section describes the CICM Monitor tool and the tasks you can perform with the CICM Monitor, including

- Adding and deleting CICM profiles.
- Connecting and disconnecting from CICM profiles.
- Launching CICM Monitor reports.
- Saving report data.
- Printing reports.
- Updating an instance profile.

What is CICM Monitor?

In the NAM architecture, multiple configurations can be installed on a single Customer ICM (CICM) machine. For example, you might have ten instances of the ICM software running on a single CICM complex; each instance, in turn, serves one or more customers. The CICM complex can route calls for each of the instances configured on the machine.

Rather than focus on an individual instance's call routing data, you might want to view call routing information for all the instances on a CICM. The CICM Monitor tool lets you define a profile that describes the database configuration on each CICM complex. Once you define a CICM profile, you can view call routing information for all the instances on the CICM complex.

**Note**

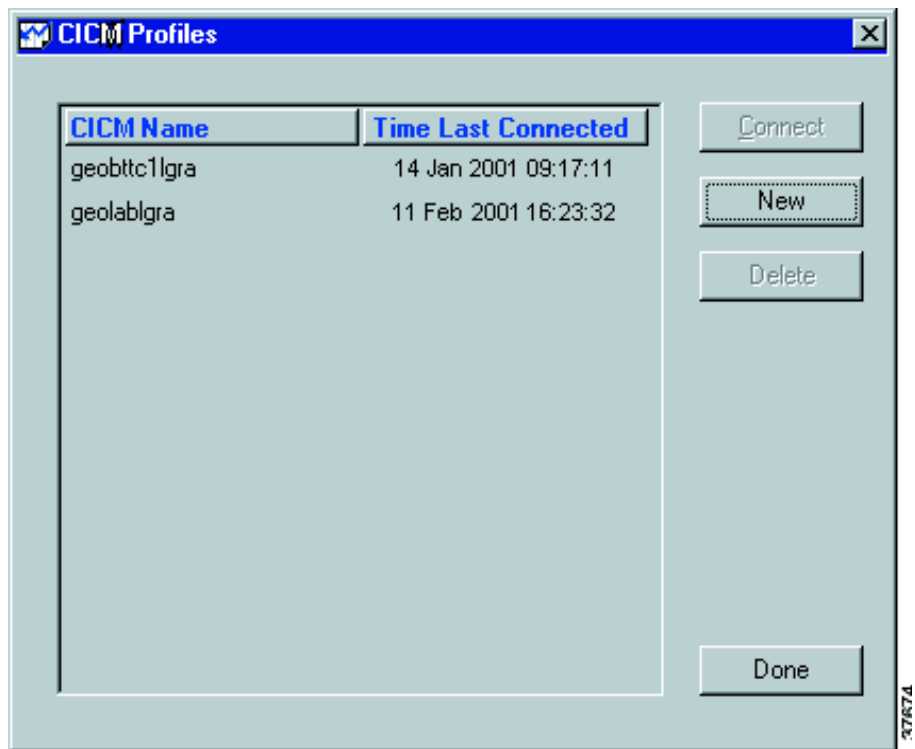
The CICM Monitor tool is installed on NAM and CICM AWs. It is not installed on Limited Admin Workstations. Users on Limited Admin Workstations can view data for only one instance.

Defining CICM Profiles

In order to view data for the instances on a CICM complex, you need to define a CICM profile and install a monitoring utility on the CICM complex. The CICM profile defines the individual instance databases that are installed on a CICM complex. This lets you access data for each instance.

To define and connect to a CICM profile:

- Step 1** Start **CICM Monitor** from the **ICM Admin Workstation** group. The CICM Monitor window box appears.
- Step 2** Choose **Tools > Connection Profiles** or click the Profiles button on the toolbar. The CICM Profiles dialog box appears.



The C1CM Profiles dialog box displays a list of names of C1CM machines with Loggers. (This list includes the current machine, plus any other machines for which you have defined profiles.) This list also provides the date and time that you last connected to the C1CM complex via the C1CM Monitor.

- Step 3** Click the **New** button. An empty text field appears at the bottom of the list of available C1CM profiles.
- Step 4** Enter the name of a valid C1CM complex Logger and click the **Connect** button. (If you enter an invalid name, C1CM Monitor returns a SQL Server error when you attempt to connect to that C1CM.)

**Note**

The first time you connect to a new C1CM profile, a dialog box appears to confirm that you wish to install the Monitoring utility on the selected C1CM. Click Yes to continue. Once the Monitoring utility is installed, C1CM Monitor connects to the C1CM's central database.

- Step 5** Click the **Done** button to make the changes and close the window.

**Note**

Repeat this procedure to add other C1CMs in your NAM system.

Updating a Profile

When you add a new instance or remove an instance from a C1CM, you must update the C1CM Monitor instance profile.

To update the C1CM Monitor instance profile:

- Step 1** Connect to the C1CM profile where the instance has been added or removed.
- Step 2** Choose **Tools > Install Utilities**. A dialog box appears, prompting you for confirmation.
- Step 3** Click **Yes** to continue. C1CM Monitor then deletes the old utility, scans for existing C1CM instance information, and installs the new monitoring utility.

Every time you update the profile, the entire CICM complex is scanned for instance information. This procedure may be time-consuming and should be performed only when instances are added to or removed from a CICM.

Deleting a CICM Profile

If you need to delete a CICM profile, you can do so at any time.

To delete a CICM profile:

-
- Step 1** Choose **Tools > Connection Profiles** or click the Profiles button on the toolbar.
 - Step 2** In the CICM Profiles window, highlight the CICM profile you want to remove and click the Delete button.
 - Step 3** Click the Done button to close the CICM Profiles window.
-

Connecting to CICM Profiles

When you want to view call routing information for the instances on a CICM, you need to connect to the appropriate CICM profile.

To connect to a CICM profile

-
- Step 1** Choose **Tools > Connection Profiles** or click the Profiles button on the toolbar.
 - Step 2** In the CICM profiles window, choose the CICM for which you want to view information and click the Connect button. The status bar at the bottom of the CICM Monitor main window displays a “Connecting to” message. Once connected, a Disconnect button replaces the Connect button.



Note You can connect to only one CICM profile at a time.

- Step 3** Click the Done button to close the CICM Profiles window and return to the CICM Monitor main window.

Once connected to a CICM profile, you can launch reports that contain data for the instances on the CICM.

To disconnect from a CICM profile

-
- Step 1** Choose **Tools > Connection Profiles** or click the Profiles button on the toolbar.
- Step 2** The CICM Profiles window highlights the profile to which you are currently connected. Click the Disconnect button.
- Step 3** Click the Done button to close the CICM Profiles window.
-

Launching Reports

You can launch two types of reports to monitor call routing information for the instances on a CICM:

- **Summary report.** The summary report offers routing-client data and call routing information for all instances on a selected CICM complex. The summary data report is updated every 30 seconds with data from the Routing_Client_Five_Minute table.
- **Detail report.** For all physical controllers on a selected CICM complex, the detail report provides the same information found in the summary report plus data on discarded and timed out calls. The detail data report is also updated every 30 seconds with data from the Routing_Client_Five_Minute table.

The specific fields in each report are described later in this section.

See the *Cisco ICM Software Database Schema Handbook* for information on the Routing_Client_Five_Minute table.

To launch a Summary report

- Step 1

Connect to a CICM profile as described on page 6-8.
- Step 2

Choose **File > Open Summary Report**. CICM Monitor displays a Summary Report window:

CICM Monitor for geobttc1lgra Summary

8/4/91 11:54:25

Customer Status Summary

Company Name	Routing Client	Current Interval						Previous Interval					
		Time	Resp	Mean	Lates	Delay	Errors	Time	Resp	Mean	Lates	Delay	Errors
cus01	INCRP_NIC_1	11:50	6598	7	0	94	0	11:45	6602	7	0	93	0
cus02	INCRP2_NIC_1	11:50	4800	6	0	125	0	11:45	4800	7	0	94	0
cus02	cus02_PG4	11:50	0	0	0	0	0	11:45	0	0	0	0	0
cus02	cus02_PG80	11:50	0	0	0	0	0	11:45	0	0	0	0	0
cus03	INCRP_NIC_1	11:50	0	0	0	0	0	11:45	0	0	0	0	0
cus04	INCRP_NIC_1	11:50	600	6	0	31	0	11:45	600	6	0	47	0
cus05	INCRP_NIC_1	11:50	600	5	0	31	0	11:45	599	6	0	31	0
cus06	INCRP_NIC_1	11:50	600	8	0	32	0	11:45	600	7	0	94	0
cus07	INCRP_NIC_1	11:50	600	5	0	125	0	11:45	600	5	0	125	0
cus08	INCRP_NIC_1	11:50	600	6	0	94	0	11:45	600	5	0	47	0
cus09	INCRP_NIC_1	11:50	600	5	0	16	0	11:45	600	5	0	31	0
cus10	INCRP_NIC_1	11:50	600	4	0	31	0	11:45	600	4	0	203	0
cus11	INCRP_NIC_1	11:50	600	4	0	16	0	11:45	600	5	0	94	0
cus12	INCRP_NIC_1	11:50	599	7	0	32	0	11:45	600	6	0	78	0
cus13	INCRP_NIC_1	11:50	600	7	1	438	0	11:45	600	6	1	438	0
cus14	INCRP_NIC_1	11:50	601	4	0	47	0	11:45	599	6	0	31	0
cus15	INCRP_NIC_1	11:50	600	5	0	250	0	11:45	600	6	1	297	0
cus16	INCRP_NIC_1	11:50	600	4	0	16	0	11:45	600	5	0	63	0
cus17	INCRP_NIC_1	11:50	600	5	0	32	0	11:45	600	5	0	110	0
cus18	INCRP_NIC_1	11:50	600	5	1	281	0	11:45	600	5	0	156	0
cus19	INCRP_NIC_1	11:50	600	5	0	31	0	11:45	600	5	0	31	0
cus20	INCRP_NIC_1	11:50	600	5	0	16	0	11:45	600	5	1	281	0
cus21	INCRP_NIC_1	11:50	600	4	0	47	0	11:45	599	5	0	47	0
cus22	INCRP_NIC_1	11:50	600	5	0	31	0	11:45	600	5	0	172	0
cus23	INCRP_NIC_1	11:50	600	4	0	31	0	11:45	600	5	0	78	0
cus24	INCRP_NIC_1	11:50	600	4	0	31	0	11:45	600	4	0	16	0
Total:			23998		2	438	0		23999		3	438	0

Once a Summary report is displayed, you can print or save the report, or export the report data in any of several file formats.

The Summary report retrieves the following data from the Routing_Client_Five_Minute table in the selected CICM database.

- **Date and Time.** The system date and time on the selected CICM complex appears in the upper left corner of the report.
 - **Company Name.** The name of the CICM instance configuration.
 - **Routing Client.** The name of the CICM device that receives the call routing request.
 - **Time.** Marks the end of the five-minute interval when data was retrieved. If the time displayed in the column is 10:15, for example, then the data shown represents the interval between 10:10 and 10:15.
 - **Resp (Routing client responses).** The number of route responses sent to the routing client during the five-minute interval.
 - **Mean (Mean routing client responses).** The mean time, in milliseconds, for the route responses to the routing client during the five-minute interval.
 - **Lates (Late calls).** The number of route responses to the routing client that exceeded the late threshold but did not time out.
 - **Delay (Maximum delay).** The maximum response time, in milliseconds, for any route response to the routing client during the five-minute interval.
 - **Errors (Receive in error).** The number of routing requests from the routing client that produced errors during the five-minute interval.
-

To Launch a Detail Report:

-
- Step 1** Connect to a CICM profile as described on page 6-8.
 - Step 2** Choose **File > Open Detail Report**. CICM Monitor displays a Detail Report window.

Customer Status Details									
Company Name	Physical Controller	Time	Responses	Mean	MaxDelay	Lates	Discarded	RcvInError	Timeout
cus02	ICRP2_NIC_1	09:10	1200	3	32	0	0	0	0
cus02	ICRP2_NIC_1	09:15	1199	3	31	0	0	0	0
cus02	ICRP2_NIC_2	09:10	0	0	0	0	0	0	0
cus02	ICRP2_NIC_2	09:15	0	0	0	0	0	0	0
cus03	ICRP_NIC_1	09:10	600	12	109	0	0	0	0
cus03	ICRP_NIC_1	09:15	599	12	172	0	0	0	0
cus03	ICRP_NIC_2	09:10	0	0	0	0	0	0	0
cus03	ICRP_NIC_2	09:15	0	0	0	0	0	0	0
cus04	ICRP_NIC_1	09:10	600	3	47	0	0	0	0
cus04	ICRP_NIC_1	09:15	600	3	16	0	0	0	0
cus04	ICRP_NIC_2	09:10	0	0	0	0	0	0	0
cus04	ICRP_NIC_2	09:15	0	0	0	0	0	0	0
cus05	ICRP_NIC_1	09:10	599	3	16	0	0	0	0
cus05	ICRP_NIC_1	09:15	600	4	31	0	0	0	0
cus05	ICRP_NIC_2	09:10	0	0	0	0	0	0	0

Step 3 Once a Detail report is displayed, you can print or save the report, or export the report data in any of several file formats.

The Detail report retrieves the following data from the Routing_Client_Five_Minute table in the selected CICM database:

- **Date and Time.** The system date and time on the selected CICM complex appears in the upper left corner of the report.
- **Company Name.** The name of the CICM instance configuration.
- **Physical Controller.** The name of the device that receives the call routing request.
- **Time.** Marks the end of the five-minute interval when data was retrieved. If the time displayed in the column is 10:15, for example, then the data shown represents the interval between 10:10 and 10:15.
- **Responses (Routing client responses).** The number of route responses to the routing client during the five-minute interval.

- **Mean (Mean routing client responses).** The mean time, in milliseconds, for the route responses to the routing client during the five-minute interval.
 - **MaxDelay (Maximum delay).** The maximum delay, in milliseconds, of route responses to the routing client during the five-minute interval.
 - **Lates (Late calls).** The number of route responses to the routing client that exceeded the late threshold but did not time out.
 - **Discarded (Discarded calls).** The number of routing requests from the routing client that were discarded because of an internal constraint such as buffering.
 - **RcvInError (Receive in error).** The number of routing requests from the routing client that produced errors during the five-minute interval.
 - **Timeout (Timeout calls).** The number of route responses to the routing client that timed out during the five-minute interval.
-

Saving Report Data

You can save CICM Monitor report data to a file for use in another application, such as a spreadsheet or a word processing program.

For information on the formats in which you can export data, see the *Cisco ICM Software Supervisor Guide*.

To save CICM Monitor report data:

-
- Step 1** With a report displayed in the CICM Monitor main window, select **File > Save As**. The Save As dialog box appears.
 - Step 2** Specify a directory, file name, and a format for the report data.
 - Step 3** Click the **Save** button to save the report.
-

Printing CICM Reports

You can print reports that are displayed in the CICM Monitor window.

How to print a CICM report:

With a report displayed in the CICM Monitor main window, select **File > Print**. A dialog box provides printing options and prompts you for confirmation.



Security Considerations

The Cisco Network Applications Manager (NAM) product allows several customers to share the same Central Controller complex. This presents some possible security concerns in the following areas:

- Relationships between Windows 2000 domains
- Installing an Admin Workstation
- Preventing unauthorized access to real-time data
- Access to historical data

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

Windows 2000 Domains

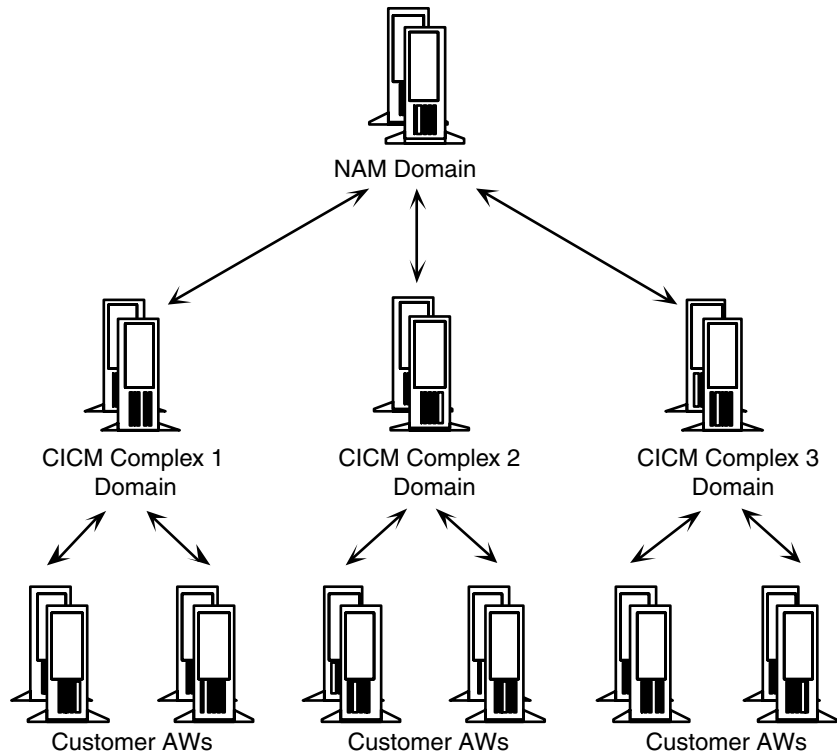
Components in this architecture are divided among several Windows 2000 domains. All NAMs and their associated Admin Workstations are in a single domain. Each CICM complex and its associated Admin Workstations is in a separate domain. Each instance's Admin Workstations can be in two different domains:

- CICM instance distributor on the NAM
- CICM instance distributor on the Customer AW

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.

Figure 7-1 illustrates the relationship between the Windows 2000 domains in the Network Applications Manager architecture.

Figure 7-1 Relationship Between Windows 2000 Domains



37686

A customer-owned ICM can be deployed with no trust relationship between the NAM domain and the ICM domain. In this case, the operation of the ICM differs from an ICM on a network-hosted NAM/CICM platform as follows:

- Network AWs from the NAM domain do not have ICM instance distributors.
- AWs for the customer ICM are standard AWs, so that the customer can perform all of the necessary ICM configuration.
- Automated provisioning from the NAM to the ICM does not work.

Typically in this situation, the Service Provider owning the NAM should not have direct access to the customer-owned ICM.

**Note**

Service providers who have a class of customer that only accesses the ICM through WebView should have their WebView Server in a separate Windows 2000 domain. A single ICM instance can be shared by many customers of this type.

Running Node Manager on an Admin Workstation

When you install an Admin Workstation, you have the choice of running the Node Manager under one of two accounts:

- Under the System account
- Under a specific user account

If Node Manager runs under the System account, then the associated Central Controller must provide unrestricted access to the System account. For security reasons, you might not want to grant full access to the system account.

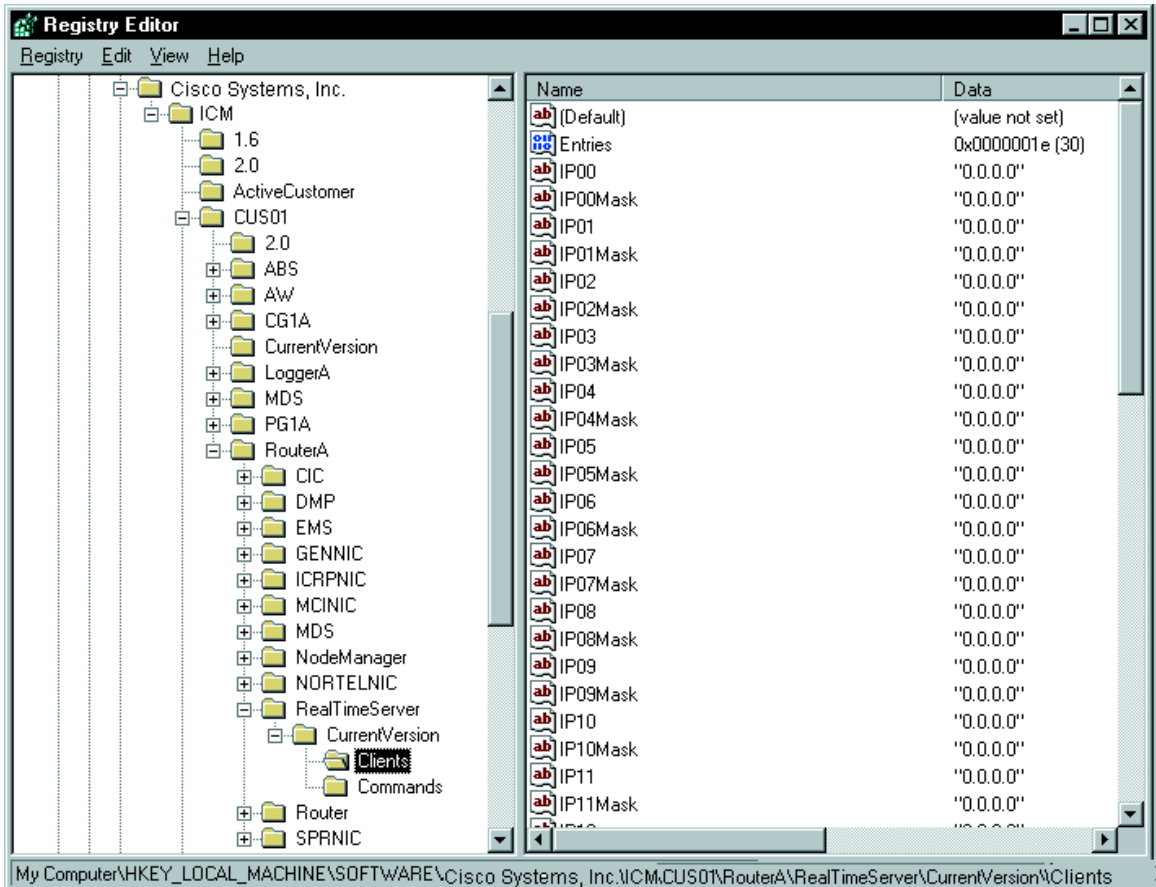
To minimize security risks, you should define a specific user account for the Node Manager in the Admin Workstation domain. You must grant that user account appropriate access to the Central Controller domain.

Validating Real-Time Clients

To prevent unauthorized access to real-time data, you can configure the 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 2000 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 7-2 Registry Editor on CallRouter



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).

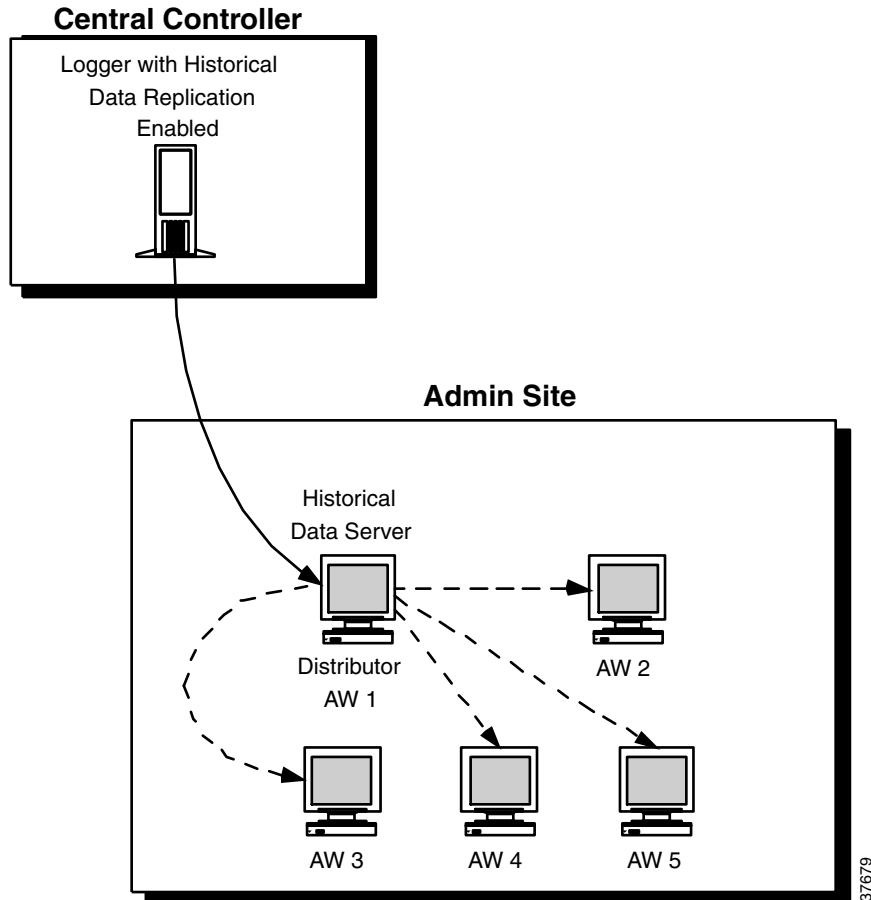
The IP mask 0.0.0.0 is a special value indicating that the associated IP address should be ignored. By default, all the masks are set to this value. If the ICM does not find any valid values, it allows any machine to connect.

Historical Data Server

In the standard ICM architecture, historical (half-hour) data is stored in the central database on the Logger. Users in this architecture access the Logger database directly for historical reports. However, this requires users to have access to the Logger's domain (the CICM domain in the Network Applications Manager environment). This is not recommended when multiple instances are running on a CICM.

As an alternative, you can set up the real-time distributor Admin Workstation at a site as a Historical Data Server (HDS). The ICM feeds historical records to the HDS machine through a secure mechanism. Other Admin Workstations at the site can read historical data from the HDS machine rather than from the Logger.

The Central Controller forwards historical records to the HDS for storage in a special local database. Other Admin Workstations at the local site can retrieve historical data from the HDS machine without having to access the central site.

Figure 7-3 Historical Data Server Architecture

To set up a Historical Data Server, you must configure the Logger to perform historical data replication. You must create an HDS database on the real-time distributor Admin Workstation and configure that Admin Workstation to be a Historical Data Server.

Information in the real-time feed tells each client Admin Workstation where to obtain historical data. If the real-time distributor is a Historical Data Server, then it instructs its clients to get historical data from it. Otherwise, it instructs its clients to get historical data from the Logger.

**Note**

For specific information on enabling historical data replication and setting up HDS machines, see the *Cisco ICM Software Installation Guide*.



Special Considerations

This chapter describes some ICM features of special interest to NAM 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 a NAM 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.

Configuring CLID Masking

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

- Configure ICM, where the masking rule is enabled in the configuration database.

■ Calling Line ID (CLID) Masking

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

How to use Configure ICM to define a CLID Masking rule

Use Configure ICM's System Information dialog box to specify the masking rule.

- Step 1** In Configure ICM, select **Enterprise > System Information**. The System Information dialog box appears.

System Information

General

Company name:

Controller domain name:

Retain script versions:

Default network VRU:

Minimum correlation number:

Maximum correlation number:

Minimum script schedule time: seconds

ICM type: Standard

☒ Enable expanded call context

☐ Partitioning enabled Maximum partitions: 0

Person Security

☐ Login name case sensitive

Minimum password length:

Call Type

Default call type:

Abandoned call wait time:

Service level threshold:

Service level type:

CLID Masking

☒ Enabled

Number of characters:

☒ Remove digits

Mask character:

Application Gateway

☒ Custom gateway

☐ Remote ICM

Timeout Sessions Heartbeats Errors

Request: milliseconds

Abandon: milliseconds

Late: milliseconds

Save Close Help

ICM Instance: cust1

- Step 2** 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 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 with 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 dialog box, see the *Cisco ICM Software Configuration Guide*.

- Step 3** When finished, click **OK** to submit the changes and close the dialog box.
-

How to use Script Editor's ICM Gateway Node on the NAM

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

- 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 should 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 ICM 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 ICM 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 Configure ICM. 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.

Defining Dynamic Labels in the 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 complete information about using the Script Editor with these nodes, see the *Cisco ICM Software Script Editor Guide*.

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 (which, in this 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.

**Note**

For more information on using the ICM Gateway node, see page 8-3.

NAM Network Event Reporting

The NAM can provide detailed records on call disposition information that the network may provide. The NAM populated 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 (i.e. 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 and subsequent DISCONNECT event record for the new called party. 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. [Table 8-1](#) lists the fields in this record.

Table 8-1 Network Event Record Fields

Field	Data Type	Explanation
RouterCall KeyDay	Int	Used with RouterCallKey and RouterCallKeySequenceNumber to identify the related Route_Call_Detail record. See the <i>Cisco ICM Software Database Schema Handbook</i> 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. See the <i>Cisco ICM Software Database Schema Handbook</i> 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. See the <i>Cisco ICM Software Database Schema Handbook</i> 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 are 1 for calling party, 2 for the called party. Notice that after a network transfer, the new called party would still have CallLegID 2.
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).

Table 8-1 Network Event Record Fields (continued)

Field	Data Type	Explanation
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 ICM software to track virtual time.
RecoveryDay	int	A value used internally by the ICM 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 life of the call, additional event arming takes place and additional records are written to the NAM database.

- The switching network will have 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.
- SS7 link sizing will need 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.
- In ICM Release 5.0, only the standard SS7 IN NIC supports Network Event Reporting. It may be possible to adapt other NICs to support this feature; contact your Cisco Representative.
- Network Event Reporting is not supported for ACD or VRU PG routing clients, such as an VRU (like Cisco ISN) acting as a service node. 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

The 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 an 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 the ICM to determine the real destination for the call, i.e. the 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 the 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.

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. ICM script execution continues at this point.
6. The ICM, through the NAM instructs the Network VRU to executes 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 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: the 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 agents 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 the 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 the 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 step 1) and 2) have set the NetworkTransferEnabled flag to 1, 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 it's 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

The following NAM routing clients support network transfer:

- CRSP NIC
- SS7 IN NIC
- Some Custom NICs
- 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).

The following routing clients *do not* support network transfer:

- GKTMP NIC
- AT&T NIC
- MCI NIC
- Sprint NIC
- ACD PGs

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 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 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, the ICM call context is transferred as well.

Route Call Detail Records 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 records 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 the ICM. The RouterCallKey is identical to the other ICM TCD and RCD records for this call. The RouterCallKeySequenceNumber is 1.
- TCD in the ICM for the agent connection. The RouterCallKeySequenceNumber is 1. The RouterCallKey is identical to the other 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 the 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 the ICM for the transfer request. The RouterCallKey is identical to the other ICM TCD and RCD records for this call. The RouterCallKeySequenceNumber is 2 (for the first network transfer; if this is for a subsequent network transfer the RouterCallKeySequenceNumber is set to the next number, like 3, 4, etc.).
- TCD in the ICM for the call from the transferring agent to the other agent. When doing a Blind Network Transfer (which is the only network transfer supported in ICM release 5.0), this call leg never happens, but the ICM generates a TCD for it anyway. This TCD has the CallTypeID field set to -1. The RouterCallKey is identical to the other ICM TCD and RCD records for this call. The RouterCallKeySequenceNumber is 2 (for the first network transfer; if this is for a subsequent network transfer the RouterCallKeySequenceNumber is set to the next even number, like 4, 6, etc.). This TCD is present only if the call is transferred to a device target or peripheral target.

- TCD in the ICM for the new transferred call from the caller to the agent. The RouterCallKey is identical to the other 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, like 5 , 7, etc.). This TCD is present only if the call is transferred to a device target or peripheral target.

Note that the ICM RouterCallKey is different from the NAM RouterCallKey. If records need to be correlated between the NAM and 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 all NAM and ICM RCD and TCD record's call variable field. It can then be used to link all records together.

Network Transfer Configuration on Existing Systems

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 should set the call context variable NetworkTransferEnabled to 1.
- 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 Transferred Preferred' check box on the Routing Client tab of the ACD PG.
- If required, configure the Labels on the NAM as well.



Network VRU

This chapter describes the concepts, architecture, configuration and operations of Network Voice Response Units (VRUs) in a NAM/CICM environment.

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 balances lookups or complete business transactions. In this case the caller might never leave the VRU to be connected to an agent, or he 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.

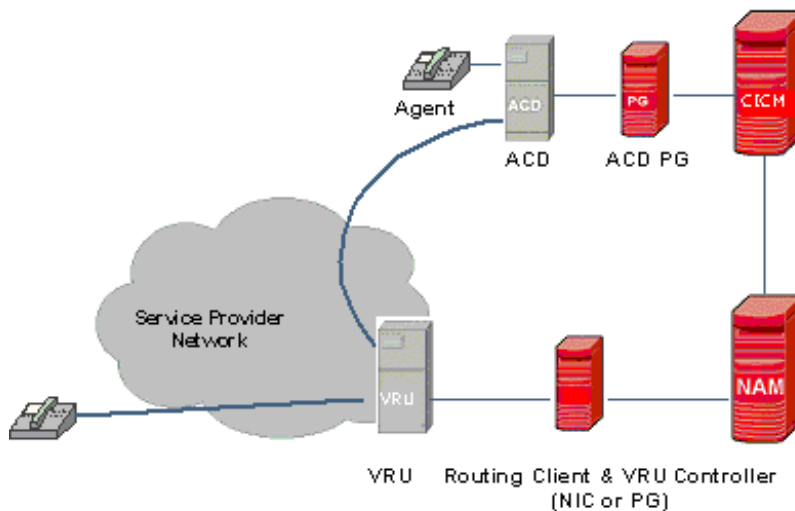
- Providing recorded announcements during queuing. Information can be provided on the customer's status in the queue, expected delay times, alternative options, such as a self help VRU application, leaving a voice message, and so on.

Network VRU Architecture

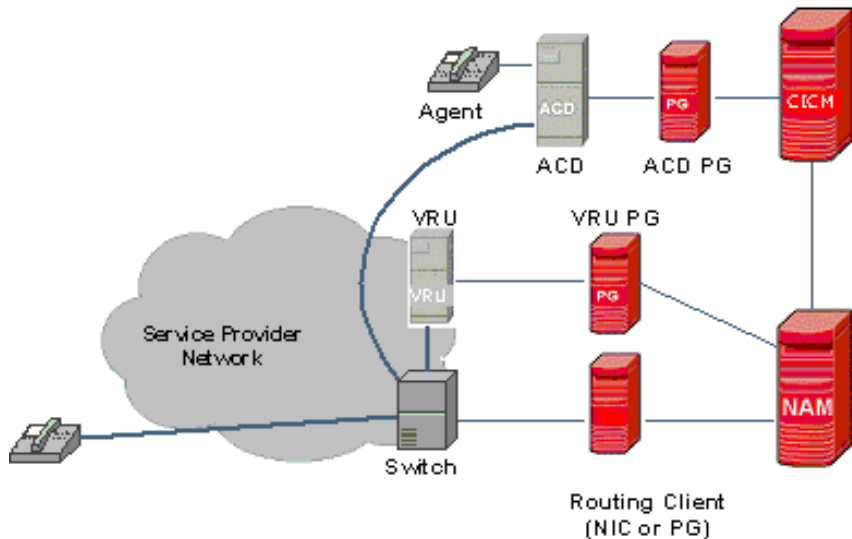
There are several different architectures for NAM-based Network VRU solutions. The following questions determine which one is applicable:

- **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 figure below 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 9-1 Service Node Implementation

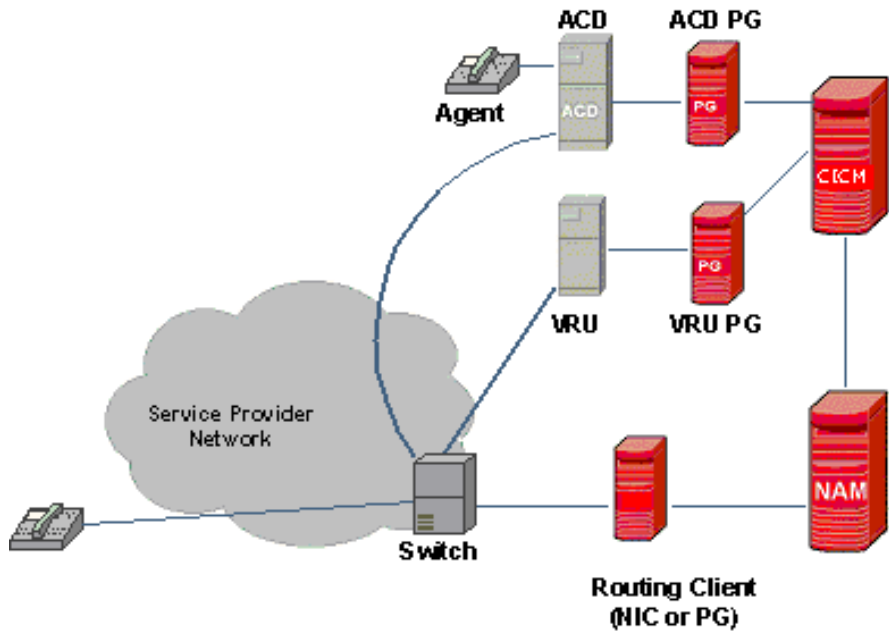
The alternative scenario where there is a separate routing client that switches the call to the VRU and later to an agent is shown in the figure below. In this case the routing client is connected to a switching device that switches the call to the VRU and the agent.

Figure 9-2 Network VRU Implementation with Separate Routing Client

- **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. [Figure 9-3](#) shows a basic architecture with a VRU connected at the ICM.

Figure 9-3 Network VRU at Customer Premises, Connected to ICM Instead of the NAM



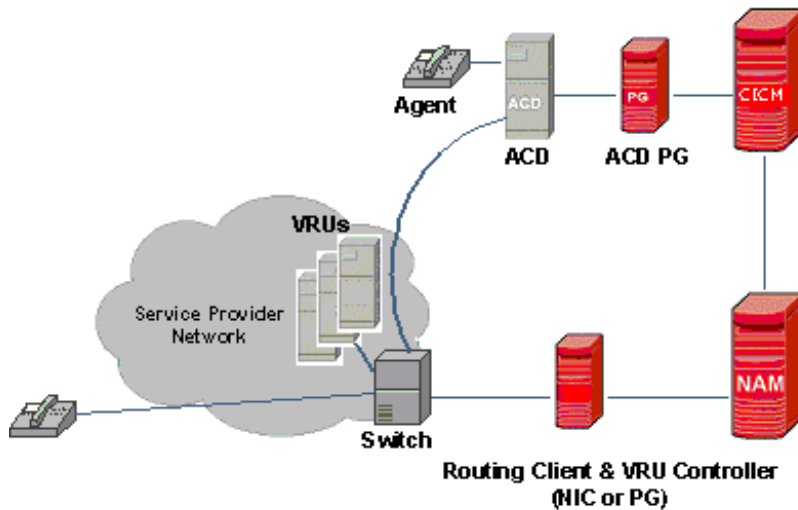
One of the most significant differences between a network-hosted VRU (connected to the NAM) and a customer premise-hosted VRU (connected to the CICM) is the correlation mechanism used. The correlation mechanism takes care of uniquely identifying the same call across the two dialogs that the NAM/CICM 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.

- **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?**

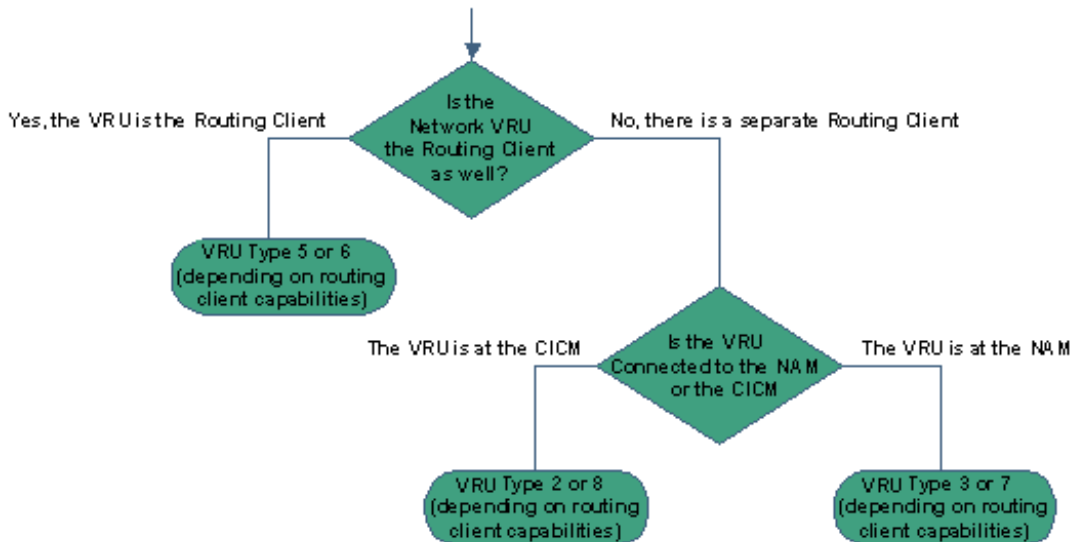
The answer to this question does not influence the architecture so much, but it does impact the call flow. There are many variations in routing client capabilities and they will be explained in detail in the next section.

Figure 9-4 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 9-4 Example of a Service Node Implementation with Additional Routing/Switching Capabilities



These two questions lead to the following decision tree:

Figure 9-5 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 3rd 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.

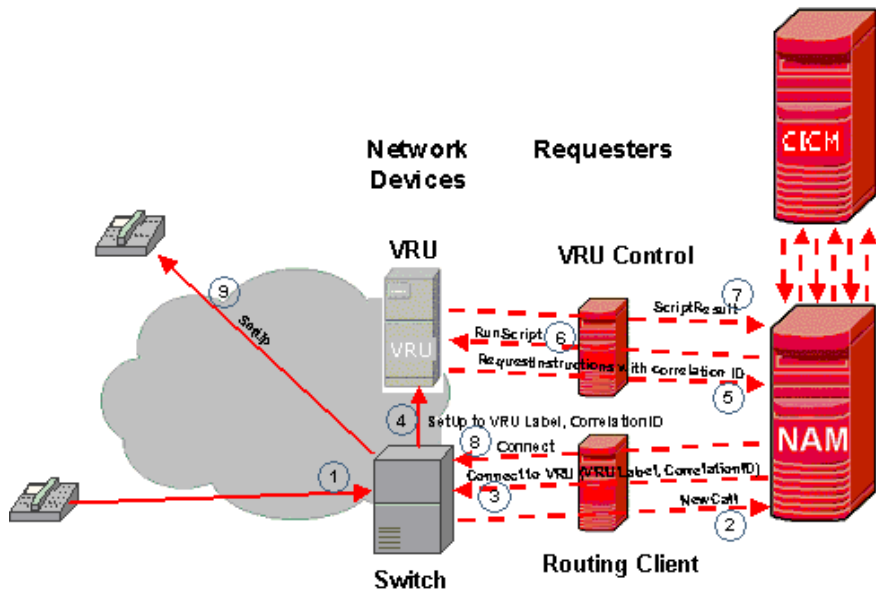
Type 3 and 7 VRU call flows

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.

Figure 9-6 Type 3 Call Flow

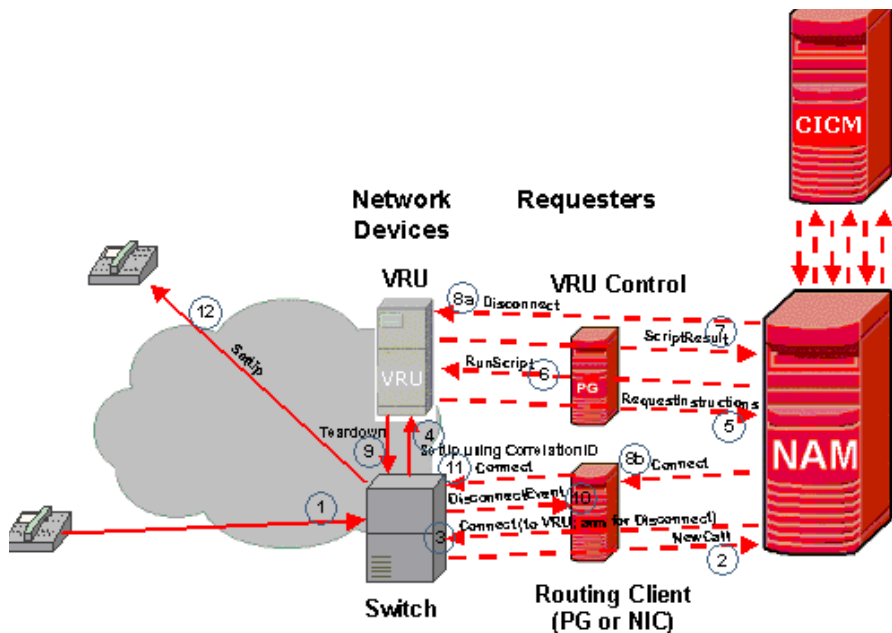


The Type 3 call flow is as follows:

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 ICM, 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 correlationID.
- The switch connects the call to the VRU using the label and passing along the correlationID.
4. When the call arrives, the VRU asks the NAM or CICM for instructions and it sends the correlationID along with the request. This allows the NAM or CICM to identify the call and continue script processing.
 5. The NAM or CICM script hits a *RunVRUScript* node and sends an instruction to the VRU to run a certain Network VRU script.

6. 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.
7. When the NAM or C ICM 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 ready queuing the call using a Queue node and an agent becomes available, the NAM will instruct the switch to take the call away from the VRU (i.e. tear down the call leg setup in step 4) and connect the call to the selected destination. The dialog between the the NAM and the Network VRU is now terminated.
8. The switch will connect the call to the new destination.

Figure 9-7 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 (i.e. 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 ICM 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 correlationID. In order for step 10 to happen, the NAM will typically have to instruct the switch at this point in time that the switch should 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 correlationID.
5. When the call arrives, the VRU asks the NAM for instructions and it sends the correlationID 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 *RunVRUScript* 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 ready queuing the call using a Queue node and an agent becomes available, the NAM will do two things:
 - a. it will instruct the VRU to disconnect the call and
 - b. it will instruct 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 will hold onto the instruction until the switch will report back to the routing client.
9. The VRU will drop the call.
10. The Switch will report this event to the routing client, keeping the originating leg of the call (i.e. to the caller) open.

11. The routing client will now send the instruction to the switch to connect this call to its new destination.
12. The switch will connect the call to the new destination.

Type 2 and Type 8 Call Flows

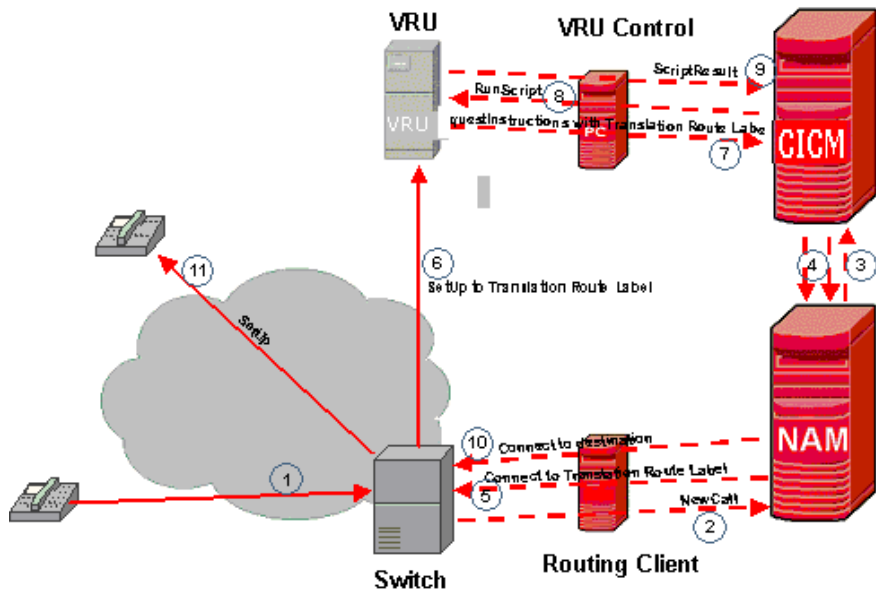
The Type 2 and 8 VRU call flows are for Network VRUs connected at the CICM. The difference between types 2 and 8 lies in how the routing client handles taking the call away from the VRU and connecting it to an agent.

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

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.

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.

Figure 9-8 Type 8 Call Flow

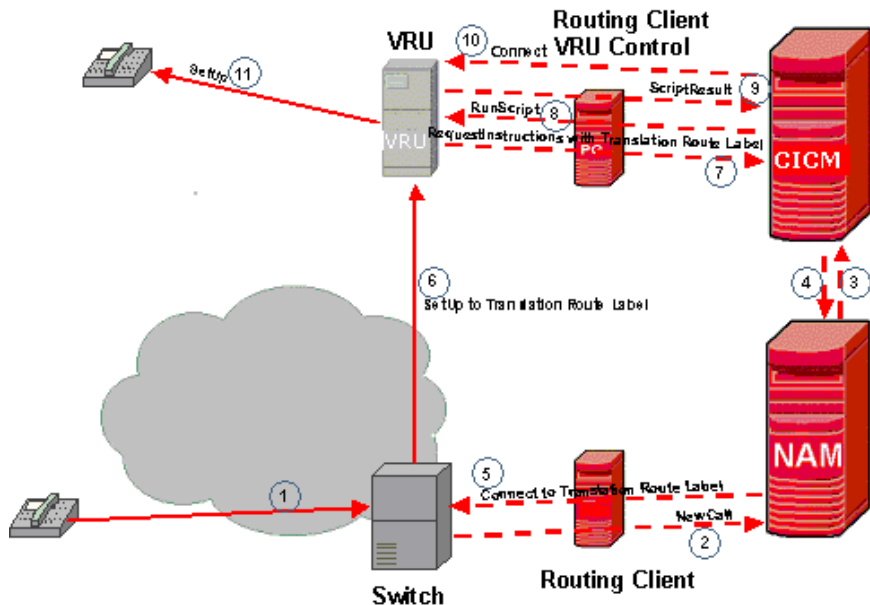


The Type 8 call flow is as follows:

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 an 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 RunVRUScript 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 ready queuing the call using a Queue node and an agent becomes available, the CICM will instruct the NAM and the NAM in turn will instruct 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 will connect the call to the new destination.

Figure 9-9 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:

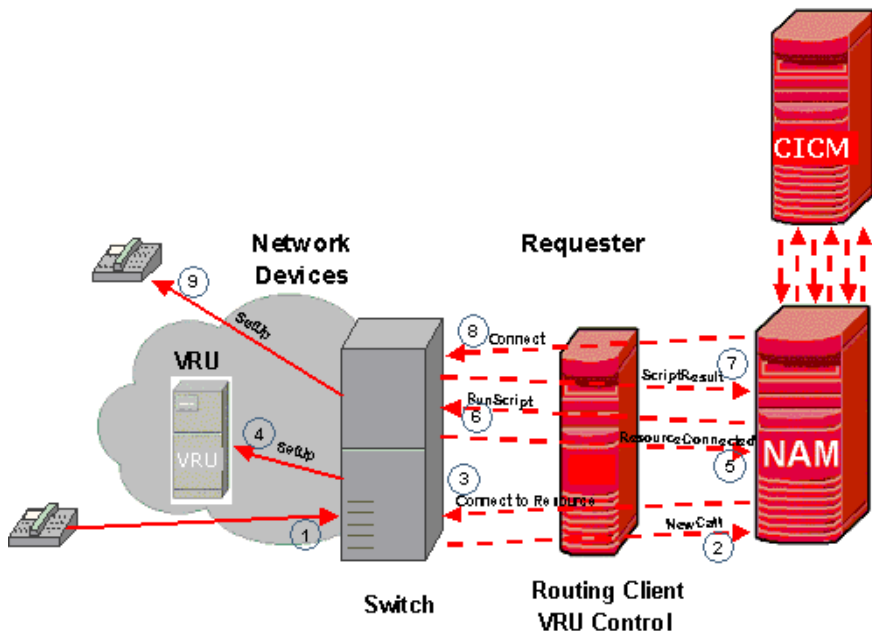
1. Caller dials a number that causes the switch to query the NAM.
2. The switch queries the NAM.
3. The NAM forwards the request to a CICM (VRU control needs to be scripted in the CICM with this Network VRU type).
4. A CICM routing script executes and hits a *TranslationRouteToVRU* node. The CICM instructs 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 *RunVRUScript* 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 ready queuing the call using a *Queue* node and an agent becomes available, the CICM will instruct 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 will connect 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 lays 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.

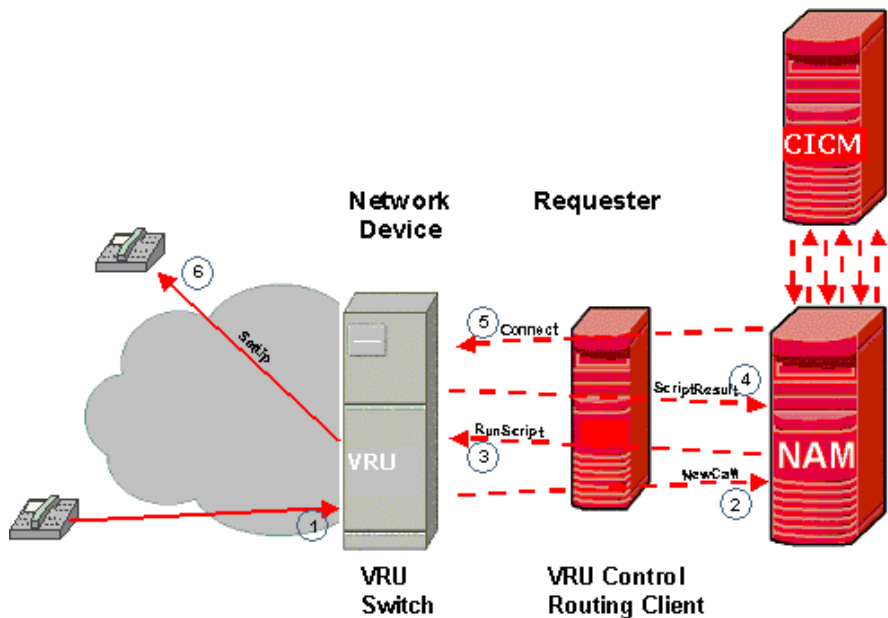
Figure 9-10 Type 5 Call Flow



The Type 5 call flow is as follows:

1. Caller dials a number that causes the switch 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 *RunVRUScript* 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 ready 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.

Figure 9-11 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 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 executes a *SendToVRU* node and a subsequent *RunVRUScript* 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 ready 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.
6. The switch/VRU will connect 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 the use of Setup to configure NICs and PGs, since this is completely independent of Network VRU types 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.

Type 3 and Type 7

-
- 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 should 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 label is identical in the NAM and CICM. It is recommended that the Network VRU Name is 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 check box. 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 CorrelationID to the required values. The NAM will go through the range of correlationIDs sequentially. For example, if the correlation ID 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 ICM 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.
-

Type 6

-
- Step 1** Using Network VRU Explorer, define a Network VRU of Type 6. Do this in both the NAM and the CICM. It is recommended that the Network VRU Name is 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 check box. 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 it's 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.
-

Type 5

-
- Step 1** Using Network VRU Explorer, define a Network VRU of Type 5. Do this in both the NAM and the CICM. It is recommended that the Network VRU Name is 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 check box. 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 need 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 need 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 ICM. If calls handled by this ICM 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.
-

Type 2 and Type 8

- 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 check box. 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. It is recommended to 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. Choose 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 the 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 field are sent to the VRU and should be entered in a way that is meaningful to the specific Network VRU.
- Check the Interruptible check box if the caller using DTMF tones can interrupt the Network VRU Script.
- Check the Overridable check box 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 to <none> the Network VRU Script is available to all users and routing scripts.

Configuring a VRU PG as Routing Client that is not also a Network VRU

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 2 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 should be configured as described under Type 5 VRU above. Note that there are now 2 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 should 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 as strictly speaking not Network VRU control nodes)
- RunExternalScript
- Wait

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

- **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.

Connecting the Call to the Network VRU

Before any RunVRUScript 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 RunVRUScript 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 the section [SendToVRU Node](#).

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.

Sending the VRU Instructions

The RunVRUScript 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 (e.g. 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 executing for the specified number of seconds. In the mean time 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 should continue with a RunVRUScript 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 (i.e. no SendToVRU or TranslationRouteToVRU node has been encountered yet), an implicit SendToVRU node will be executed before the first RunVRUScript 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 will continue script processing with the next node without taking further action.

If the flag is not set, the router will lookup 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 correlationID from the range configured. The router will wait until it receives a RequestInstruction message from one of the connected VRU PGs with the same correlationID 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 will use 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 will fail and script processing will continue through the failure exit.

If so, the router will send 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 will wait 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 will result in a connect instruction to be 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.

RunVRUScript Node

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

encountered and then continue processing the Queue node. If the flag is set, the router will continue script processing out of the success node. The script should contain further RunVRUScript nodes to determine call treatment while queuing.

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



Admin Workstation Features

This appendix summarizes the Network AW features that are not installed on a Limited AW. It also presents a recommended set of software features that the service provider should not provide to subscribers with Standard AWs with Feature Control.

Limited AW

The Limited Admin Workstation provides a network service provider customer with a subset of the tools and functionality of the Network AWs that reside at the network service provider site. This section discusses the following topics:

- Admin Workstation program group tools that are not installed on a Limited AW
- Configure ICM menu items that are not available
- Script Editor features that are not available

Installed Tools

The following Admin Workstation program group tools are *not* installed on a Limited AW.

- AW Select
- Check Routes
- CICM Monitor

- Router Log Viewer
- Schema Help

Configure ICM

The following Configure ICM menu items are *not* available on a Limited AW.

- Translation Route
- Dialed Number
- Dial Number Plan
- Script Table
- Script Table Column
- Application Gateway
- Requesters
- Label
- Network VRU
- Network VRU Script
- Scheduled Target
- Dialed Number Label
- VRU Service Arrays
- Customer
- Agent Distribution
- ICM Instance
- ICM Node

Script Editor

The following nodes are *not* available on the Script Editor palette on a Limited AW:

- Wait

- Gateway
- ICM Gateway
- DB Lookup
- Busy
- Ring
- Termination

Standard AW with Feature Control

Through the ICM Configuration Manager Feature Control facility, a service provider can define what ICM tools and features a subscriber with a Standard AW can access.

For such subscribers, it is recommended that the service provider *not* provide access to the following ICM tools.

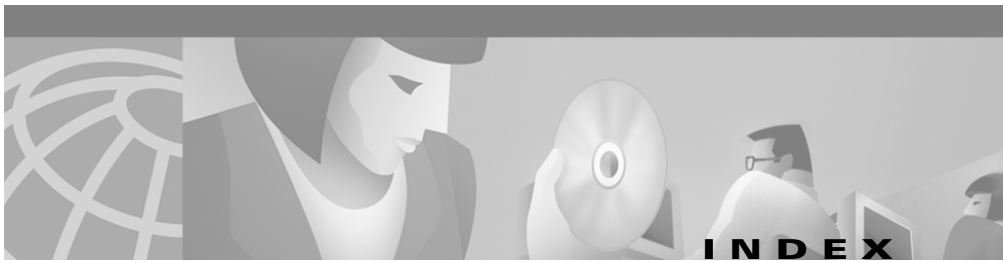
Script Editor Nodes

- ICM Gateway
- TranslationRouteToVRU

Configuration Tools:

- Dialed Number Bulk Edit
- Label Bulk Edit
- VRU Port Map Bulk Edit
- Trunk Group Bulk Edit
- Trunk Bulk Edit
- Network Trunk Group Bulk Edit
- Peripheral Target Bulk Edit
- Route Bulk Edit
- Dialed Number Bulk Insert
- Label Bulk Insert
- VRU Port Map Bulk Insert

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



A

Adding an instance [3-2](#)

Admin Workstations [1-9](#)

- definition [2-10](#)

- installing on NAM [2-10, 3-11](#)

- Limited [1-12, A-1](#)

- Network [1-11](#)

Advanced Services [5-1](#)

AlarmTracker [1-14](#)

Application Gateway

- remote ICM [2-21](#)

AW Select [6-3](#)

AW Select tool [1-11](#)

- connecting to profiles [6-8](#)

- defining CICM profiles [6-6](#)

- deleting profiles [6-8](#)

- reports [6-9](#)

- updating instance profile [6-7](#)

CICR Replication [4-6](#)

Component selection [3-6, 3-10](#)

Configured labels [8-4](#)

Configure ICM tool [1-11](#)

Customer Concept [4-1](#)

Customer ICM [1-2](#)

Customers for CICM instances

- configuring on NAM [2-17](#)

C

CallRouter

- installing [2-8](#)

- installing on NAM [2-8, 3-9](#)

- installing on the CICM [3-9](#)

- with no PGs [1-8](#)

Call tracer tool [1-11](#)

Check routes tool [1-11](#)

CICM Monitor [6-5](#)

D

Database

- Historical Database Server (HDS) [7-5](#)

- names [3-2](#)

DDSN

- Distributed Diagnostics and Services
Network [1-14](#)

defining

- NIC [3-13](#)

Deleting an instance [3-19](#)

Distributed Diagnostics and Services Network (DDSN) [1-14](#)

Distributors for CICM instances

configuring on NAM [2-16](#)

Documentation

ICM Tools [1-12](#)

Domain [7-1](#)

Duplexed

CallRouter [1-8](#)

Dynamic label

flow on NAM/CICM configurations [8-5](#)

Dynamic labels [8-4](#)

G

Glossary help [1-11](#)

H

Historical Data Server (HDS) [7-5](#)

I

ICMDBA

using in deleting an instance [3-20](#)

ICM gateway [2-21](#)

ICR Setup [2-7](#)

INCRP NIC [1-2, 3-12](#)

INCR Protocol [1-2](#)

Initialize local database tool [1-11](#)

Installing

Admin Workstation [2-19](#)

Admin Workstation on NAM [2-10, 3-11](#)

CallRouter on CICM [3-9](#)

CallRouter on NAM [2-8](#)

Listener on NAM [2-26](#)

Logger on CICM [3-5](#)

Logger on NAM [2-2](#)

instanceno.exe [3-3](#)

Instances

adding [3-2](#)

adding and upgrading components [3-19](#)

assigning to a CICM [3-3](#)

choosing the CICM [3-3](#)

deleting [3-19](#)

naming conventions [3-2](#)

procedure to add to CICM [3-5](#)

Instances for CICMs

configuring on NAM [2-14](#)

J

Job scheduler tool [1-11](#)

L

Labels

configured and dynamic [8-4](#)

Listener

adding CICM instance to NAM [3-19](#)

installing on NAM [2-26](#)

Lock Admin tool [1-11](#)

Logger

installing on CICM [3-5](#)

installing on NAM [2-2, 3-5](#)

M

Multi-customer systems [2-7](#)

Multiple components [2-7](#)

N

NAM

architecture [1-1](#)

configuration data [2-11](#)

NAMCallRouter

Remote Network Routing option [2-7](#)

Naming conventions

databases [3-2](#)

instances [3-2](#)

NAM Logger

Phone Home option [2-2](#)

NAM Replication Process (NIRP) [2-13](#)

Network Applications Manager [1-1](#)

Network Interface Controller

configuring on NAM [2-18](#)

INCRP [3-12](#)

Network Interface Controller (NIC)

defining [3-13](#)

Network Voice Response Units (VRUs) [9-1](#)

call flows [9-7](#)

configuring [9-19](#)

types [9-7](#)

NIC

defining [3-13](#)

Nodes

ICM Gateway [8-3](#)

P

Peripheral Gateway

configuring on NAM [2-18](#)

required [1-8](#)

Phone Home

NAM Logger option [2-2](#)

Physical controller ID

INCRP NIC [3-14](#)

Print server tool [1-11](#)

Program group [1-11](#)

R

Remote diagnostics [1-14](#)

Remote Network Routing

NAM CallRouter option [2-7](#)

Router log viewer tool [1-12](#)

S

Script editor tool [1-12](#)

Security considerations [7-1](#)

Service Control [6-1](#)

Service Control Point [1-1](#)

Service control tool [1-12](#)

Setup

 post-install [2-7](#)

Setup tool [1-12](#)

Support architecture [1-14](#)

T

Tools [1-11](#)