Cisco ICM Software Supplement for VRU Peripheral Gateway

October 2006

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 (64387)
Fax: 408 526-4100

Contents

Figures

Preface

Purpose

This document provides configuration information specific to the VRU Peripheral Gateway (PG). The VRU PG implements the ICM/VRU Interface Protocol (hereinafter called VRU Interface). The VRU PG allows Cisco Systems, end users, VRU vendors, and other parties to integrate various kinds of a telephony device (hereinafter called VRU) into the ICM system. It is not within the scope of this document to address the specifics of any particular VRU that has been integrated. This document provides information that may be generally applied to any VRU connected to the ICM through the VRU PG.

Audience

This document is intended for Intelligent Contact Manager system managers. The reader is assumed to understand system manager functions as described in the *ICM Configuration Guide for Cisco ICM Enterprise Edition* and the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.* The reader is also assumed to have specific knowledge of the VRU Interface, as well as specific knowledge about one or more VRU Interface implementations.

Organization

Chapter 1, “Overview”

Provides an overview of the VRU interface, software and hardware requirements.

Chapter 2, “VRU Service Control Interface”

Describes the Service Control Interface that is used to control a VRU.

Chapter 3, “Time Synchronization Interface”

Describes how the VRU can use the TSI to synchronize its internal clock with the VRU PG.

Chapter 4, “Old Interfaces of VRU”

Describes some of the older interfaces of the VRU.

Chapter 5, “VRU PG Installation Options”

Describes the installation options of the VRU PG.

Chapter 6, “ICM VRU Configuration”

Describes the configuration details of the ICM and the VRU PG.

Chapter 7, “VRU Programming Considerations”

Describes the programming considerations for the VRU PG.

Typographic Conventions

This manual uses the following conventions:

- Boldface type is used for emphasis; for example:
- Real-time information **is not** stored in the central database.
- Italic type indicates one of the following:
  - A newly introduced term; for example:
  - A *skill group* is a collection of agents who share similar skills.
  - A generic syntax item that you must replace with a specific value; for example:
  - IF (*condition, true-value, false-value*)
  - A title of a publication; for example:
  - For more information see the *Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions.*
- Sans serif type with small caps is used to represent keys on your keyboard; for example:
- Press the SHIFT key to select a range of items.
- An arrow (→) indicates an item from a pull-down menu. For example, the Save command from the File menu is referenced as File→Save.

Other Publications

For more information on Cisco ICM software, see the following documents:

- *ICM Administration Guide for Cisco ICM Enterprise Edition*
- *ICM Installation Guide for Cisco ICM Enterprise Edition*
- *ICM Configuration Guide for Cisco ICM Enterprise Edition*
- *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*

For information on Cisco Network Applications Manager (NAM), see the following documents:

- *Product Description Guide for Cisco ICM Hosted Edition*
- *Setup and Configuration Guide for Cisco ICM Hosted Edition*
- *Multiple-NAM Setup and Configuration Guide for Cisco ICM Hosted Edition*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems

Attn: Customer Document Ordering

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Product Alert and Cisco Field Notice mechanisms. You can register to receive Product Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid

service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click **the Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by

inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *The Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet magazine* is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and

business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

1. Overview

The VRU PG connects to each VRU via a TCP/IP connection. The VRU PG can run in simplex or duplex configurations.

In a duplex configuration, only the active side of the PG connects to the VRU. If the active side of a duplexed PG fails, the inactive side is activated, and a new connection to the VRU is opened.

1.1. VRU Configuration

The typical configuration consists of a VRU system and a PG (or two PG's if duplexed) on an Ethernet hub. Each VRU PG is capable of connecting to up to 32 VRUs simultaneously.

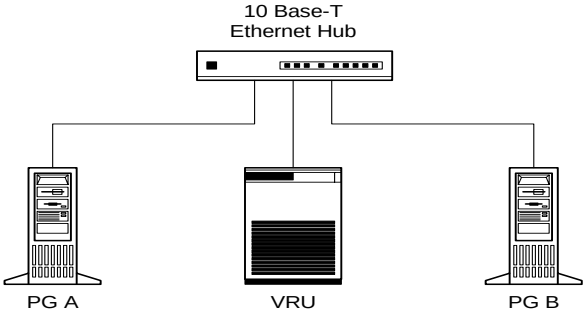

Figure 1: Configuration

Note: Bandwidth to the Central Controller must be sufficient to support the number of VRUs connected. Contact your Cisco representative for a network analysis.

1.2. VRU Interface Requirements

The VRU PG requires a TCP/IP connection to the VRU. The VRU must provide an IP address and a TCP port number for the PG to connect to.

The VRU must implement the required interface defined in the document *ICM/VRU Interface Specification.*

1.3. Hardware and Software Requirements

The VRU PG requires a 10-Megabit Ethernet or equivalent physical connection to the VRU. The VRU PG can communicate remotely with VRUs via a TCP/IP network. However, you must ensure that the network link between the PG and VRU system provides enough bandwidth to support the call load for the VRU.

1.4. Supported ICM Software Features

The VRU PG supports the following ICM software features:

- Pre-Routing
- Post-Routing
- Translation Routing
- Peripheral, Trunk Group and Service real time reporting
- Duplexed PG implementation

1.5. Unsupported ICM Features

The VRU PG does not support features relating to Agents or Call Queuing. An SCI VRU allows the ICM Router to implement call queues but does not, implement queues.

2. VRU Service Control Interface

An ICM Router uses the Service Control Interface to control a VRU. The ICM Router can have the VRU play announcements and prompts, gather data from the caller, and route calls to destinations. This interface is required for in-network VRUs and for global call queues implemented in the ICM Router.

Because SCI allows the ICM Router to control the VRU, the ICM Router needs to know about the capabilities and configuration of the VRU. This is encoded in a number called the VRU Type configured in the Router settings. See the "Network VRUs" chapter of the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for details on choosing and configuring the VRU Type for different applications.

3. VRU Time Synchronization Interface

The VRU can use the TSI to synchronize its internal clock with the VRU PG clock, which is synchronized to the ICM clock. As certain messages arrive from the VRU the VRU PG compares the VRU time stamp with the ICM time. Significant differences are periodically reported to the VRU via the TSI.

The messages that contain the current VRU time:

SCI: INIT_SERVICE_CONTROL_VRU, VRU_STATUS

EDF: INIT_DATA_END_EVENT, VRU_STATUS_EVENT

Warning: The Time Synchronization Interface should not be use on any VRU connected to a PG that is being used as the ICM Time Source (Router registry key "Router \ CurrentVersion \ Configuration \ Time \ Source"). This can cause a time feedback loop that can cause the system time to fluctuate wildly.

4. Older VRU Interface Features

The Service Control Interface feature replaces several older interface features that are still supported for backward compatibility with the following older VRUs:

- Event Data Feed (EDF)
- Call Routing Interface (CRI)

4.1. Event Data Feed

The VRU uses the EDF feature to provide real-time events to the ICM. The ICM will accumulate call time statistics and write Termination Call Detail records for each call.

4.2. Call Routing Interface

The VRU uses the CRI feature to send route requests to the ICM Router. Each route request triggers a routing script and the routing script returns a route response. Typically the route response is used to direct the call to a new destination but in practice the script triggered by the route request can perform any decision-making or data-gathering task (such as a database lookup) and return the result in a route response. You can use this interface as a standalone but is generally used in conjunction with the EDF .

4.3. Mixing SCI and EDF

A VRU can support both the SCI and the EDF. This capability is provided as a migration path from legacy EDF applications to SCI. The VRU can deliver some calls under EDF (send a "delivered" event) and the others under SCI (send a "New Call" or "Request Instruction" message). If the VRU is not able to determine which mode to use based on data available when the call is delivered, it must start the call under EDF (send a "delivered" event) and later use the SCI "New Dialogue" message to convert the EDF call to an SCI dialogue.

5. VRU PG Installation Options

There are various options available during the installation of a VRU PG. This chapter describes the options available during the installation of a VRU PG.

5.1. Installation Options

The installation options available in the VRU PG are as follows:

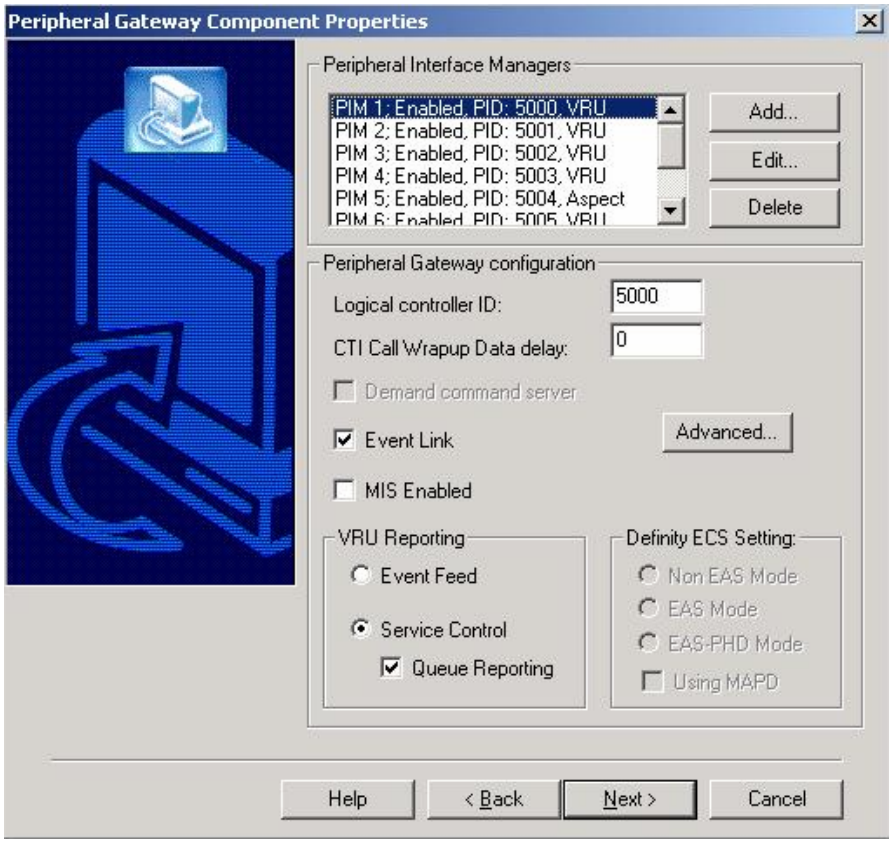

Figure 2: Installation Options

5.2. MIS Enabled checkbox

MIS is used to transfer call variables between an ACD and associated EDF/CRI VRU. Check the box if you want to use MIS.

5.3. VRU Reporting controls

Select one of the two options:

- Event Feed
- Service Control

Note: The names of these two options do not have a direct correspondence with the VRU Interface features of similar name. The features that the VRU can support are restricted somewhat by the choice, but within those restrictions the combination of features that the VRU chooses to support are left up to the VRU and are received from the VRU when the VRU PG connects to it.

5.3.1. Event Feed choice

Selecting this option makes the VRU PG not generate real-time trunk and service data update, and not write Termination Call Detail records for each SCI dialogue. VRU PG still generates real-time peripheral data update. If the Service Control Interface is used as a standalone, VRU peripheral data is initialized based on the Init_Service_Ctrl_VRU message during the SCI initialization. If Service Control Interface is used along with EDF interface, VRU peripheral data is initialized by messages in EDF interface.

5.3.2. Service Control choice

Selecting this option allows the VRU PG to generate real-time peripheral, trunk and service data update, and write one or more Termination Call Detail records for each SCI dialogue. For Service Control Interface, VRU peripheral data is always initialized based on Init_Service_Ctrl_VRU message during the SCI initialization, no matter if Service Control Interface is used alone, or combined with other interface.

Selecting this option also enables the Queue Reporting checkbox.

Queue Reporting checkbox

If this box is left unchecked the only events generated for SCI dialogues are **Delivered** and **Cleared** and the only call statistic calculated is total call time.

If this box is checked the PG will also generate Queue events. Calculated call statistics will then include queue times and abandons in queue, as well as total call time.

6. ICM Configuration

In ICM terms, the VRU itself corresponds to a peripheral. The ICM software treats all contact center devices (e.g., ACDs, PBXs, IVR systems) as peripherals.

In order to properly configure and maintain the ICM database, you need to understand the relationship between the objects configured in the VRU, and the ICM database, the relationship of the field in the VRU message, and the attribute of objects in the ICM database.

Some of the mappings are described in this chapter, for example, an ICM Trunk Group Peripheral Number corresponds to the Trunk Group ID value in the VRU messages.

Note: Different VRU vendors may use different object names; refer to the document from the VRU vendor for detailed object mapping. This chapter also provides information specific to configuring a VRU PG by using the ICM Configuration Manager's PG Explorer tool.

6.1. Peripheral

The ICM Peripheral corresponds to the VRU. The following values can be used in any combination in the Peripheral Configuration Parameter for the Peripherals configured with the VRU PG:

- **"/BTTELSIS"**: Send a single-byte pad message, after any message with odd length is sent to the VRU, and read a single-byte message, after any message with odd length is received from the VRU. The default action is to not send or read pad messages.
- **"/ZEROTRUNKS"**: Tell the ICM to set the available trunk count to zero if the VRU PG goes out of service.
- **"/FILTERVARS"**: Send to the VRU only those call variables that have been changed by the ICM since the last time the call variables were sent to or received from the VRU. The default action is to send all non-null call variables to the VRU.
- **"/ASSUME_ANSWERED"**: Count calls as successfully connected as soon as the Connect message is sent to the VRU. This will prevent calls from being counted as abandoned when a VRU fails to send an Event Report / Answered message in response to a Connect message.
- **"/TYPE_3_TALK_TIME "**: This value is used to support customers who might be relying on the old behavior that when Service Control Queue Reporting is enabled, VRUPIM treat the call arrived at Type3 or Type 7 VRU for self-service as in Talking state and the TalkTime in TCD is the time the call spent at VRU. The new behavior is to treat calls arriving at Type 3 and Type 7 VRUs the same as Type 2 and Type 8 VRUs and the TalkTime in TCD is not incremented for self-service call at VRU when Service Control Queue Reporting is enabled.

6.2. Peripheral Targets

An ICM Peripheral Target is a network target identified by a Trunk Group and DNIS that terminates on the VRU. For EDF, a Peripheral Target must be configured for all DNIS and Trunk Group(s) through which an incoming call arrives. Peripheral Targets used for Translation Routes can be most easily built with the Translation Route Wizard.

6.2.1. Event Feed VRUs

All Trunk Group/DNIS combinations that are in any way connected with the handling of any incoming VRU call should be configured in the ICM as a Peripheral Target to ensure complete call monitoring.

Those calls that do not map to a valid Peripheral Target are associated with the Service defined in the Delivered or Originated call event. If neither mapping fits, the call is associated with the Peripheral's default route as defined by in the ICM Peripheral Configuration Table. If a Default Route is not defined, the PG will log an event.

The OPC Registry variable “MapPeripheralTargetsWithoutTrunkGroup” must be set to the default value of zero for Event Data Feed VRUs.

6.2.2. Call Routing VRUs

Configuration of all Trunk Group/DNIS combinations as Peripheral Targets is not essential. However, Peripheral Targets necessary for Post Routing / Translation Routing must still be configured.

The OPC Registry variable “MapPeripheralTargetsWithoutTrunkGroup” must be changed to 1 for Call Routing-only VRUs.

6.3. Trunk Groups

The ICM Trunk Group Peripheral Number corresponds to the Trunk Group ID value in VRU messages. No special configuration information is required for Trunk Groups for the VRU PG. The trunk count is obtained dynamically from the VRU and should not be configured. The VRU PG does not use the ICM Trunk Group Extension.

6.4. Trunks

Incoming calls are identified according to the individual trunk or port that the call occupies. However, there is no need to configure individual trunks in the ICM; the identification of trunks is handled automatically by the VRU and the VRU PG.

6.5. Services

The ICM Service Peripheral Number corresponds to the Service ID value in VRU messages.

6.6. Translation Routes

No special configuration considerations apply.

6.7. Routes

An ICM Route is one or more ICM Peripheral Targets. An ICM Peripheral Target is a network target identified by a Trunk Group and DNIS that terminates on the VRU. A Peripheral Target is equivalent to the combination of DNIS and the Trunk Group(s) through which the incoming calls arrive.

6.8. Routing Client

The VRU PG supports post routing and can therefore be considered a Routing Client. To configure a Routing Client for the VRU, the ICM Routing Client Peripheral entry should be set to the ICM Peripheral defining the configured VRU. The PG can route to any valid dialed number.

6.9. Labels

The format of label strings sent to the VRU in a Route Select, Connect, Temporary Connect, or Connect-to-Resource message is not dictated by the ICM. The VRU is responsible for interpreting the label and acting upon it; this interpretation may vary from one VRU implementation to another.

For labels of type BUSY, RING, and DEFAULT the label type configured in the ICM is passed to the VRU in Route Select and Connect messages. Other ICM label types are marked as type NORMAL. The VRU may use the label type (where available), in addition to the label itself, to determine how to process the response.

6.10. Network Trunk Groups

The ICM supports a configuration in which several VRUs share a single Network Trunk Group. In this configuration, the physical VRUs combine to give the appearance of a single “virtual” VRU with increased capacity. Since the network can deliver a call on any trunk in the Network Trunk Group, the call may arrive on any of the VRUs sharing the Network Trunk Group. For this reason, all the VRUs sharing the Network Trunk Group should perform identical call processing.

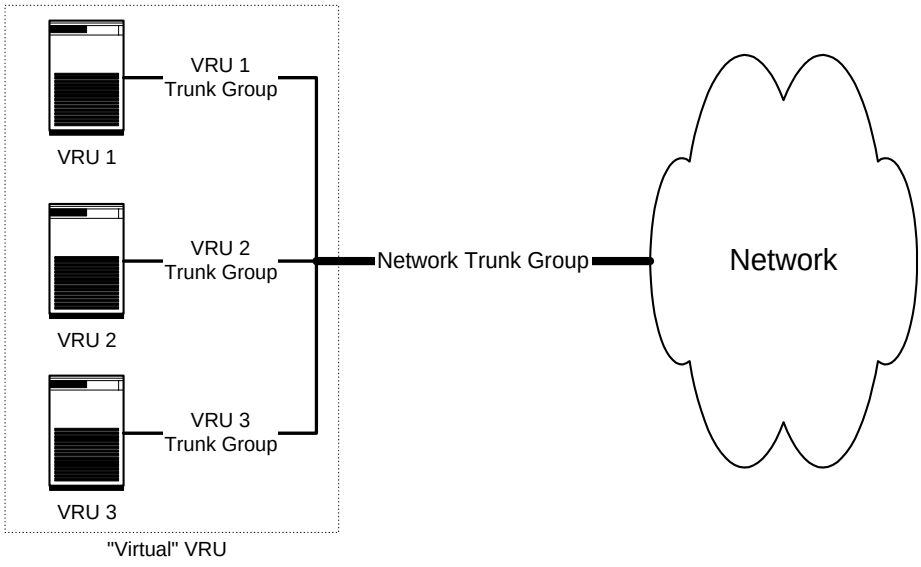

Figure 3: Network Trunk Groups

Configure one ICM Network Trunk Group for the “virtual” VRU. Then, for each physical VRU, configure the Trunk Group(s) on that peripheral. Set the Network Trunk Group for each peripheral Trunk Group to be the Network Trunk Group for the “virtual” VRU.

Note that all Peripheral Targets associated with any of the VRUs are defined in terms of the Network Trunk Group. It is therefore not possible

to route calls to an individual VRU in this configuration. Calls may be routed to the “virtual” VRU, but there is no way to predict which physical VRU will actually receive the call. Monitoring of call activity on either the “virtual” VRU or any of the physical VRUs can be done by examining the data for the Network Trunk Group or the peripheral Trunk Group, respectively.

All physical VRUs that comprise a “virtual” VRU must be connected to the same VRU PG.

6.11. Service Arrays

A Service Array is similar to a Network Trunk Group but aggregates Services instead of Trunk Groups.

In a “virtual” VRU, each physical VRU must be configured and programmed to perform the same call processing. This implies that each physical VRU must have the same Service(s) configured. However, because of the shared Network Trunk Group, the ICM cannot target a call for a Service on a specific VRU within a “virtual” VRU. Instead, a Service Array is used for this purpose. A Service Array defines a “virtual” Service on a “virtual” VRU, and may be used as a Skill Target in an ICM routing script.

To configure a Service Array, first configure a Service for every physical VRU in the “virtual” VRU. Next, create a Service Array. Add the Services configured for the physical VRUs as members of the Service Array. There should be one Service from each VRU in the “virtual” VRU that is a member of the Service Array.

For example, suppose the 3 VRUs in the diagram above can service “Sales” callers and “TechSupport” callers. Six services would be configured; for example: VRU_1.Sales, VRU_2.Sales, VRU_3.Sales, VRU_1.TechSupport, VRU_2.TechSupport, and VRU_3.TechSupport. Then, two Service Arrays would be configured; for example: VRUSales and VRUTechSupport. VRUSales would include VRU_1.Sales, VRU_2.Sales, and VRU_3.Sales as members. VRUTechSupport would include VRU_1.TechSupport, VRU_2.TechSupport, and VRU_3.TechSupport as members.

6.12. Maintaining Your Configuration

It is preferred that changes made to your configuration be accomplished first on the VRU, then on the ICM Configuration. This will ensure that the PG sees the configuration updates on the VRU systems.

7. VRU Programming Considerations

This chapter describes the programming considerations for the VRU environment.

7.1. VRU Script Timeout

When the ICM Router encounters a Run VRU Script node in a routing script it sends a Run VRU Script request to a Service Control VRU and starts a timer. If the Script Result response does not arrive from the VRU before the timer expires, the ICM Router will take the failure path from the Run VRU Script node and continue processing. The VRU PG and the VRU are not notified of the timeout.

The default timeout value is 3 minutes but the value can be configured for each Network VRU Script. The timeout value should be set higher than the longest that the VRU script is expected to execute.

7.2. Translation Routing

When a VRU is the target of a translation route, the call arrives at the VRU with a DNIS reserved for translation routing. This DNIS must be presented to the ICM so that the arriving call can be associated with the existing call context information. How the DNIS is presented to the ICM depends on the interface feature being used.

7.2.1. SCI

When a translation-routed call arrives at the VRU, the VRU must recognize the call as being a translation route connection and send a Request Instruction message to the VRU PG. The Request Instruction message must include whatever Correlation ID, DNIS, and/or "Called Number" values arrived with the call. The identifying data allows the ICM Router to associate the message with a waiting ICM Router Script.

7.2.2. CRI with EDF

When a translation-routed call arrives at the VRU, the VRU must issue a Delivered Event as it would for any arriving EDF call. The Delivered Event associates the VRU-assigned call ID with the new call and specifies the DNIS that arrived with the call. After recognizing the DNIS as a translation-route DNIS, the VRU must issue a Route Request Event to obtain the data associated with the call. The Route Request Event must specify the call ID that was in the Delivered Event.

Warning: The Dialed Number in the Route Request Event must NOT match any configured Dialed Number. For clarity we recommend that the string "TRANSLATION_ROUTE" be used for the Dialed Number.

The ICM uses the call ID in the Route Request Event to find the DNIS that was in the Delivered Event message, and uses that DNIS to find the call context information associated with the call. The VRU PG delivers the associated call context information to the VRU in a Route Select message.

7.2.3. CRI without EDF

When a translation-routed call arrives at the VRU, the VRU must recognize the DNIS as a translation-route DNIS and issue a Route Request

Event to obtain the call context information associated with the call. The VRU must specify the call ID of the Route Request Event as a NULL ID value (FFFFFFFF hex) and must give the DNIS value in the "DialedNumber" field.

The ICM uses the DNIS supplied in the "DialedNumber" field of the Route Request Event to find the call context information associated with the call. The VRU PG delivers the associated call context information to the VRU in a Route Select message.

Index