

**Cisco ICM Software
ACD Supplement for
Nortel Meridian**
(MEI Version)

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

Customer Order Number:
Text Part Number: OL-0770-06

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 NON-INFRINGEMENT 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, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CDDP, 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, iQ Expertise, iQ logo, the iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0304R)

Cisco ICM Software ACD Supplement for Nortel Meridian (MEI Version)
Copyright © 2000-2003 Cisco Systems, Inc.
All rights reserved.

Contents

Preface	ix
Purpose	ix
Audience	ix
Organization	ix
Typographic Conventions	x
Other Publications	xi
1. Overview	13
1.1. ACD Interface Requirements	14
1.1.1. Meridian Link External Processor	15
1.1.2. Meridian Link Services 4.0	15
1.2. Remote PG Configuration	16
1.3. Modes Of Operation	17
1.3.1. MEI with No Meridian Link	17
1.3.2. MEI with Meridian Link for Post-Routing Only	17
1.3.3. Enhanced CTI Using MEI and Meridian Link	17
1.3.4. High-Speed Link	17
1.4. Cisco MEI Server Software	17
1.5. Hardware and Software Requirements	18
1.5.1. Post-Routing Requirements	19
1.5.2. Enhanced CTI Requirements	20
1.5.3. Supported ICM Features	21
1.5.4. Multiple Application Support	21
1.5.5. Restrictions	21
2. ACD Configuration	23

2.1. Meridian MAX MEI.....	24
2.2. Meridian 1.....	24
2.3. Additional Requirements for Enhanced CTI Mode and Cradle-to-Grave Reporting	24
2.3.1. Meridian Mail Considerations	26
2.4. Meridian Link Capacity Considerations.....	26
2.5. ACD Restrictions	26
2.5.1. Network ACD and ICM Reporting	26
2.5.2. NCFW and CTI Data.....	26
2.6. Maintaining Your Configuration	27
3. ICM Software Setup.....	29
3.1. PG-MEI Configuration (without MEI Server).....	30
3.2. PG-MEI Configuration (with MEI Server)	31
3.3. Meridian Link Configuration	31
3.4. Additional Considerations for Enhanced CTI Mode	33
3.4.1. Monitoring of Call Event Messages	33
3.4.2. Termination_Call_Detail Options	33
3.5. Cisco MEI Server Software	34
3.5.1. When Is MEI Server Required?	35
3.5.2. Simplex PG Configurations	35
3.5.3. Duplexed PG Configurations	36
3.5.4. Limitations in a Duplexed MEI Server Environment	37
3.5.5. Adding MEI Server to an Existing PG.....	37
3.5.6. MEI Server Setup	37
4. ICM Software Configuration	39
4.1. Peripheral Configuration.....	40
4.1.1. Peripheral Configuration Parameters	40
4.1.2. Peripheral Call Control Variable Map	42
4.1.3. Overwriting of Peripheral Call Variables 1 and 2	42
4.2. Peripheral Target Configuration	44
4.2.1. Attributing Calls to ICM Routes.....	44
4.2.2. Not Configuring Peripheral Targets for Each Trunk Group	45
4.2.3. Using DNIS Values Longer Than Four Digits	45
4.2.4. Setting the Delay Before Queue Value	46
4.3. Trunk Group Configuration.....	47
4.4. Trunk Configuration.....	48

4.5. Service Configuration	48
4.5.1. Configuring Services for ACD DN's	48
4.5.2. Configuring Services for CDNs	49
4.5.3. Attributing Calls To Services	49
4.5.4. Overriding DN with Route-to-Service Mapping.....	49
4.6. Skill Group Configuration	50
4.6.1. Skill Group Priorities	51
4.7. Service Member Mapping	51
4.8. Agent Configuration	51
4.8.1. Skill Group Members	52
4.8.2. Agent States	52
4.8.3. Agent ID	52
4.9. Route Configuration	53
4.10. Routing Client Configuration	53
4.11. Dialed Number Configuration	53
4.12. Label Configuration	54
4.13. Peripheral Monitor Configuration of ACD Positions	54
4.14. Maintaining Your Configuration	55
5. Post-Routing.....	57
5.1. Calling Line ID	58
5.2. Caller Entered Digits (CED).....	59
5.3. Routing Client State.....	60
5.3.1. Non-Enhanced Mode PIM	60
5.3.2. Enhanced CTI Mode PIM	60
5.4. Special Label Characters.....	60
5.4.1. Variable Substitution	60
5.4.2. Comment Character: @	61
5.4.3. Internal Translation Route Character: ^.....	61
5.5. Translation Routing	62
5.5.1. Configuring Translation Routes	62
5.5.2. Review of Translation Routing	62
5.5.3. Meridian Considerations	63
6. Meridian-Specific Interpretation of ICM Data	65
6.1. Termination Call Detail Records.....	66
6.2. Method of Attributing Calls to Services.....	66

6.3. Method of Attributing Calls to Skill Groups	66
6.4. Calculation of Handle Time.....	67
6.5. Handling of CCR Route To Treatment.....	67
6.6. Handling of CCR Force Busy Treatment	67
6.7. Handling of CCR Force Disconnect Treatment	67
6.8. Handling of CCR Give IVR/Transfer	68
6.9. Subset of Trunk Data Supported	68
6.10. Calls Arriving at a Meridian Trunk and then Post- Routed.....	69
6.11. Monitoring of Outbound Calls on Agent’s DN Key.....	70
7. Media Blender Configuration for Nortel Meridian.....	71
7.1. Media Blender Integration with the ICM system software	72
7.2. Key Property Files	72
7.2.1. Blender.Properties	73
7.2.2. ACD.ciscocti.properties	73
7.2.3. Collaboration.properties	75
7.2.4. Phantoms.properties	75
7.2.5. <Connection_CMB>.properties	75
7.2.6. Service.FWGW.properties	76
7.2.7. FirewallGateway.properties	76
7.2.8. Resource.Properties	79
7.3. Voice and Chat CTI Call Strategies.....	79
7.3.1. Voice Call Strategies	79
7.3.2. Chat Session Strategies	80
7.3.3. CTI Strategies for Nortel Meridian.....	80
7.3.4. Routing Address and Routing Numbers	80
7.4. Configuring the Meridian Switch.....	81
7.5. Testing the Meridian Switch.....	82
7.5.1. Create a CCS Agent for the Nortel Meridian Switch	82
7.5.2. Log in a Blended Collaboration Agent on a Meridian Phone ..	83
7.5.3. Make a Blended Collaboration Caller Request to a Meridian Agent/Phone	83
7.5.4. Log In an Agent on a Nortel Meridian Phone	84
7.5.5. Place a Call on a Nortel Meridian Phone	84
7.5.6. Transfer a Call on a Nortel Meridian Phone.....	84
7.5.7. Place a Conference Call on a Nortel Meridian Phone	85
7.6. Glossary	85
Index.....	91

Tables

Table 1: Meridian 1 ACD Requirements	18
Table 2: Meridian MAX Requirements.....	18
Table 3: Additional Requirements for Post- <i>Routing</i>	19
Table 4: Additional Requirements for Running in Enhanced CTI Mode.....	20
Table 5: ICM Software–Meridian Agent State Derivation	52
Table 6: Peripheral Monitor Param String Field	55
Table 7: Origination Address Types	58
Table 8: Trunk Group Real-Time Data Elements	68
Table 9: Trunk Group Half Hour Data Elements.....	69

Figures

Figure 1: Meridian 1 MEI (Duplexed PGs)	14
Figure 2: Meridian Link Services 4.0 Configuration (Duplexed PGs).....	16
Figure 3: MEI Configuration	30
Figure 4: Meridian Link Configuration.....	32
Figure 5: Termination Call Detail Options	34
Figure 6: Sample MEI Server Configuration	35
Figure 7: Simplex PG Configuration	36
Figure 8: Duplexed PG Configurations	36
Figure 9: MEI Server Properties	38
Figure 10: Peripheral Configuration (ICM 4.1 and earlier)	40
Figure 11: PG Explorer (ICM 4.5 and beyond).....	41
Figure 12: Call Control Variable Map Field	42
Figure 13: Peripheral Target Configuration Window.....	44
Figure 14: Peripheral Target Configuration.....	46
Figure 15: Trunk Group Configuration	47
Figure 16: Service Configuration	48
Figure 17: Skill Group Configuration	50
Figure 18: Peripheral Monitor Configuration	54

Preface

Purpose

This document contains the specific information you need to maintain a Meridian Peripheral Gateway (PG) in a Cisco Intelligent Contact Management (ICM) environment. It is intended to be used as the Meridian-specific companion to the Cisco ICM software documentation set.

While other ICM documents (for example, the *ICM Configuration Guide*, and the *ICM Script Editor Guide*) cover general topics such as configuring an overall ICM system and writing scripts to route contact center requests, the *ACD Supplement for Meridian* provides specific information on configuring a Meridian PG and making any necessary adjustments to the Meridian ACD configuration.

Audience

This document is intended for the ICM system managers. The reader should understand ICM functions as described in the *ICM Installation Guide*, *ICM Configuration Guide*, and *ICM Script Editor Guide*. The reader should also have specific knowledge of the Nortel Meridian ACD.

Organization

Chapter 1, “Overview”

Provides an overview of ACD interface and hardware and software requirements.

Chapter 2, “ACD Configuration”

Describes items in the Meridian configuration that must be checked to ensure compatibility with the ICM software.

Chapter 3, “ICM Software Setup”

Provides information specific to setting up a Meridian PG and, optionally, the Cisco MEI Server software, by using the ICM Setup tool.

Chapter 4, “ICM Software Configuration”

Describes the relationships between the Meridian ACD objects and the ICM database objects. This chapter also describes Meridian-specific settings that must be confirmed in the ICM configuration.

Chapter 5, “Post-Routing”

Describes the features of ICM Post-Routing available with the Meridian PG.

Chapter 6, “Meridian-Specific Interpretation of ICM Data”

Describes the issues involved when you attempt to compare Meridian data to ICM data.

Chapter 7, “Meridian Blender Configuration for the Nortel Meridian”

Describes what you need to know and do to configure the Cisco Media Blender for use with the Nortel Meridian ACD.

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 *Cisco ICM Software Installation Guide*.
- 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:

- *Cisco ICM Software Administrator Guide*
- *Cisco ICM Software Installation Guide*
- *Cisco ICM Software Product Description*
- *Cisco ICM Software Supervisor Guide*
- *Cisco ICM Software Configuration Guide*
- *Cisco ICM Software Script Editor Guide*

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

- *Cisco Network Applications Manager (NAM) Product Description*
- *Cisco Network Applications Manager (NAM) Setup and Configuration*

1. Overview

The Cisco Meridian Peripheral Gateway (PG) monitors agent and call activity on the Meridian 1 ACD through the MAX Event Interface (MEI). The PG interacts with two Nortel Meridian 1 components: the Meridian 1 ACD and the MAX system. In systems that use Post-Routing or Enterprise CTI, the PG interacts with a third Nortel system called the Meridian Link External Processor.

This chapter provides an overview of Meridian ACD interface and hardware and software requirements.

1.1. ACD Interface Requirements

In order to work with the Meridian PG, the Meridian 1 ACD must be equipped with Meridian MAX 8 and have the MEI Network Routing Option enabled. The MAX system must also be equipped with an Ethernet interface. Consult the Meridian MAX documentation before provisioning the MEI to ensure that loading factors such as total call rates, simultaneous supervisor sessions, reports, etc., are within supported limits for the given MAX platform.

The MEI runs over TCP/IP. The typical configuration consists of a Meridian MAX system and a PG (or two PGs if duplexed) on an Ethernet hub. The MAX system is connected to the Meridian 1 ACD via the High-Speed Link. Figure 1 provides an example.

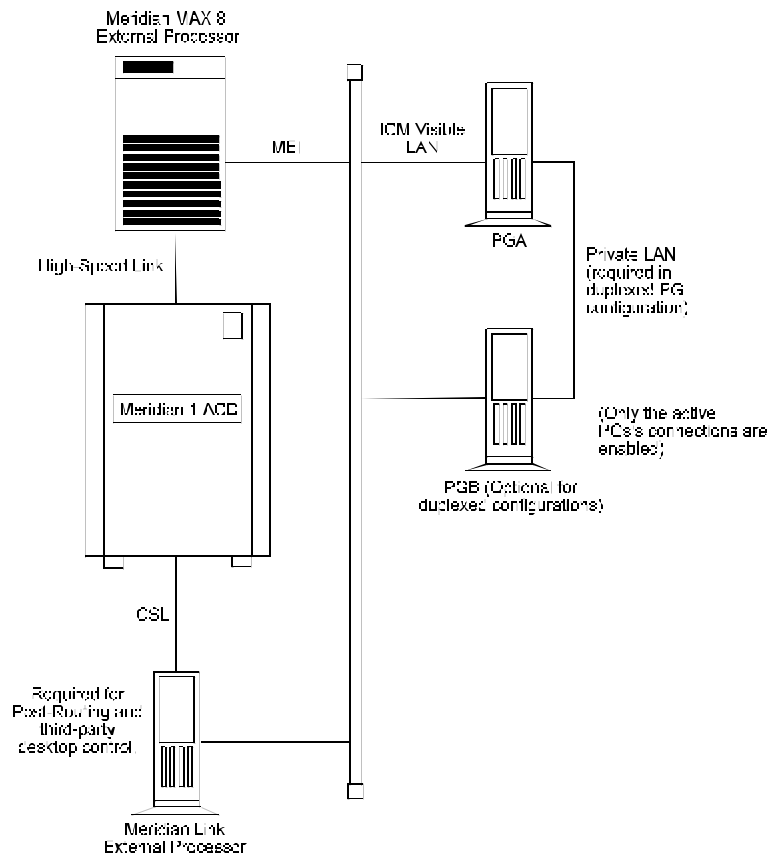


Figure 1: Meridian 1 MEI (Duplexed PGs)

As shown in Figure 1, the Meridian MAX system is connected to the ICM visible LAN and configured with an IP address. The MEI option must be enabled on the MAX system. The MEI also needs an IP port assignment.

The MEI does not define a default IP port number for MEI. Any valid port can be used. For consistency, a value of 44444 is suggested for the MEI port. The MAX IP address and MEI port are entered into the PG's configuration during PG software installation via the ICM Setup tool.

The High-Speed Link connects the Meridian 1 ACD to the MAX system. This physical connection consists of two RS-232 cables joined by DB-25 connectors. This is the standard Meridian MAX HSL connection.

The Meridian PG can run in simplex or duplex configurations. In a duplex configuration, one side of the PG maintains MEI and/or Meridian Link connections at any given time.

1.1.1. Meridian Link External Processor

For ICM Release 2.0 and later, the PG interfaces with the Meridian Link External Processor. The Meridian Link External Processor is an external computer system that provides host applications, such as the ICM PG, with an interface to the Meridian 1 ACD.

In ICM Release 2.0, the Meridian Link is only used to provide *Post-Routing* functionality. In ICM Releases 2.5 and beyond, the Meridian Link is also used to provide enhanced CTI functionality. If your Meridian installation is not using *Post-Routing* or Enhanced CTI, then the PG does not have to interface with the Meridian Link External Processor.

1.1.2. Meridian Link Services 4.0

An additional configuration is supported that uses Nortel's Meridian Link Services 4.0 on a Symposium Call Center Server (SCCS). This configuration is necessary due to the fact that Nortel is discontinuing support for some components of the Meridian Link External Processor.

Important: This configuration is certified only for the two versions of the Meridian PIM (that is, the Meridian Enhanced CTI PIM (merpimct) and the Meridian non-CTI PIM (merpimme)). This configuration **is not** supported for the Symposium PIM.

Figure 2 shows a sample of the supported Meridian configuration.

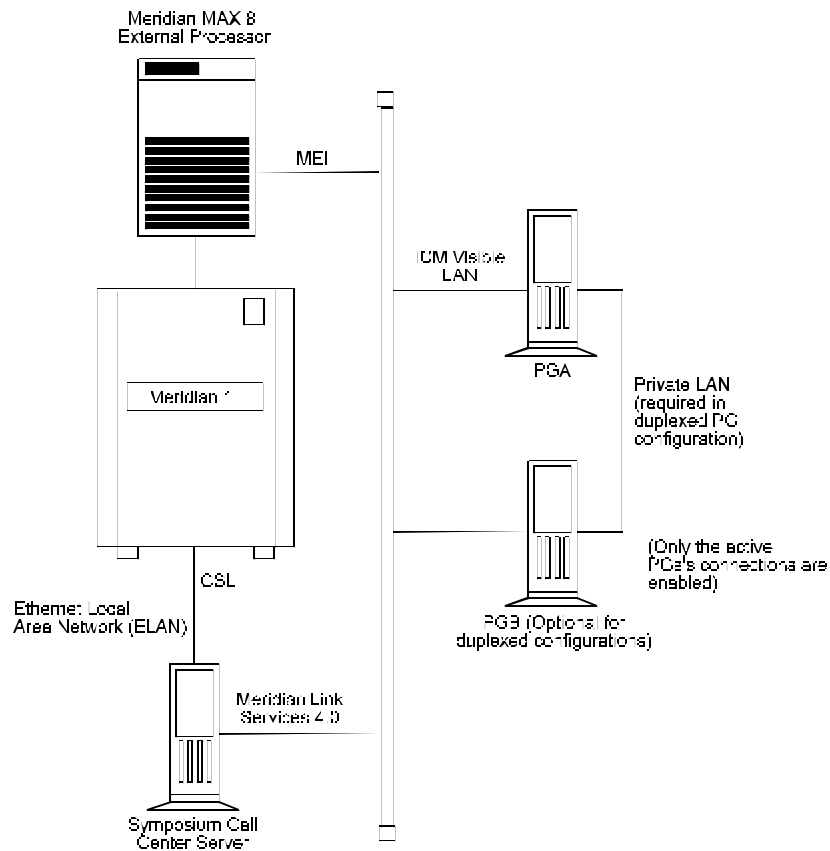


Figure 2: Meridian Link Services 4.0 Configuration (Duplexed PGs)

The Meridian Link Services (MLS) 4.0 software runs on a standard Windows NT 4.0 server. It is based on Symposium Call Center Server 4.0.

For the Meridian Link Services configuration shown in Figure 2, there is a special security procedure that you need to follow concerning the setup of the Ethernet Local Area Network (ELAN) that connects the Meridian ACD to the Symposium Call Center Server. (See “Additional Requirements for Enhanced CTI Mode,” in Chapter 2, “ACD Configuration” for instructions on properly setting up ELAN security in a Meridian Link Services 4.0 configuration.)

See also: For more information on Meridian Link Services features and requirements, see the Nortel Networks sales and marketing bulletin titled, *North America Introducing Meridian Link Services (MLS) 4.0*.

1.2. Remote PG Configuration

The PG may also be separated from the MAX system by a wide area network (WAN). A remote (i.e., WAN) Meridian PG configuration requires IP connectivity between the MAX system and the PG and at least 19.2 baud of dedicated bandwidth for communications between the two systems.

1.3. Modes Of Operation

The Meridian PG may be run in one of the following modes of operation:

- MEI with no Meridian Link
- MEI with Meridian Link for *Post-Routing* only
- Enhanced CTI using MEI and Meridian Link
- High-Speed Link

See also: For information on setup and configuration for these modes, see Chapter 4, “ICM Software Configuration.”

1.3.1. MEI with No Meridian Link

In this mode of operation, the PG interfaces only with the Meridian Event Interface (MEI). This mode is appropriate for sites that are not using Post-Routing or Enterprise CTI.

1.3.2. MEI with Meridian Link for Post-Routing Only

In this mode of operation, the PG uses MEI for monitoring calls and agents, and uses the Meridian Link for *Post-Routing*.

1.3.3. Enhanced CTI Using MEI and Meridian Link

This mode of operation makes greater use of Meridian Link to provide more CTI functionality. This mode is referred to as *Enhanced CTI mode*. In this mode, the PG uses a combination of MEI and Meridian Link to monitor calls. It also uses Meridian Link for Post-Routing and third-party call control through Enterprise CTI.

When running in enhanced CTI mode, the PG (specifically, the Peripheral Interface Manager (PIM) software) treats both the Meridian Link and MEI as essential interfaces. The PIM will always attempt to activate both interfaces. If either interface is down, the PIM will not be activated.

1.3.4. High-Speed Link

This mode uses a serial connection to the Meridian High-Speed Link to monitor calls and agents. The use of this mode is highly discouraged. Support for this mode is limited to existing customers and is capped at Meridian X11 Release 22 and ICM Release 2.5.

1.4. Cisco MEI Server Software

The Meridian MEI option supports two different styles of interface: MEI-Network and MEI-Observe. The ICM software requires the MEI Network interface. The MEI option, however, supports only a single MEI-Network interface. Therefore, in configurations where multiple connections to the MEI are required, a Cisco ICM software product called the *MEI Server* is installed on the PG to provide additional connections. The MEI Server software is available in ICM Release 4.1 and beyond.

See *also*: For information on setup and configuration for the Cisco MEI Server software, see Chapter 4, “ICM Software Configuration.”

1.5. Hardware and Software Requirements

In order to work with the Intelligent Contact Management (ICM) software, the Meridian 1 ACD requires the hardware and software listed in Table 1.

Table 1: Meridian 1 ACD Requirements

Hardware	Meridian 1, Option 11c, Option 21 through 81
Software	X11 software For specific release information for X11, see the <i>Cisco ICM Software Supported Switches (ACD)</i> document. This document can be found on Cisco Connection Online (CCO).

The Meridian MAX system requirements are listed in Table 2.

Table 2: Meridian MAX Requirements

Hardware	Meridian MAX system
Software	Meridian MAX For specific release information for Meridian MAX, see the <i>Cisco ICM Software Supported Switches (ACD)</i> document. This document can be found on Cisco Connection Online (CCO).
	MAX Event Interface (MEI) Network must be enabled. The MEI Network option is currently packaged as part of the “Virtual” MAX system offered by Nortel. Consult your Nortel representative to ensure that the MAX system has the MEI Network option enabled.
	The MAX system must be accessible via Ethernet.

1.5.1. Post-Routing Requirements

Systems that use *Post-Routing* have additional requirements, both on the Meridian switch itself and on the Meridian Link Module (see Table 3).

Table 3: Additional Requirements for Post-Routing

Meridian Switch Options	Package 214, Enhanced ACD Routing Package 215, Customer Controlled Routing ¹
Meridian Link Hardware	Meridian Link Module
	The Meridian Link machine must be configured to run TCP/IP (X.25 is not supported).
Meridian Link Software	Meridian Link For specific release information for Meridian Link, see the <i>Cisco ICM Software Supported Switches (ACD)</i> document. This document can be found on Cisco Connection Online (CCO).
	The Meridian Link Module must be equipped with the Nortel Host Enhanced Routing option.

¹ The requirement to have Package 215 installed on the switch in no way requires that the customer have the Nortel CCR product, which runs on a processor external to the switch.

1.5.2. Enhanced CTI Requirements

Several specific requirements apply to Meridian systems that use the *CTI Server* option. (A Meridian PG that uses the CTI Server option is referred to as running in Enhanced CTI mode.) In Enhanced CTI mode, the Meridian ACD must meet several additional requirements (Table 4).

Note: The Meridian configuration must also meet all of the requirements from Table 1, Table 2, and Table 3.

Table 4: Additional Requirements for Running in Enhanced CTI Mode

Hardware	Meridian Link Module
	The Meridian Link machine must be configured to run TCP/IP (X.25 is not supported).
Software	X11 switch software, Release 22.62. Alternatively, X11 Release 23 can be used provided that it is supplemented with a patch for Nortel: PRS # BV 67266. Consult your Nortel representative to ensure that you have the appropriate patch installed.
	Meridian Link software (for specific release information, see the <i>Cisco ICM Software Supported Switches (ACD)</i> document. This document can be found on Cisco Connection Online (CCO)). Note: If your system contains more than 1000 monitored directory numbers, you may require a patch from Nortel to support more than 1000 registrations. Each ACD position, ACD DN, CDN, and individual DN counts as one monitored directory number.
	The Meridian Link Module must be equipped with the Nortel Host Enhanced Routing option.
	The Meridian Link module requires one or both of the following Nortel options: - In Bound Call Management: At a minimum, the Meridian Link module must be equipped with the In Bound Call Management option. - Outbound Call Management: If CTI clients need to be able to initiate calls using MakeCall then the Meridian Link module must also be equipped with the Out Bound Call Management Option.

(continued)

Software (cont.)	<p>Associate Telephone (AST) licenses:</p> <p>The Meridian 1 must be equipped with enough Associate Telephone (AST) licenses so that all ACD positions can be configured as AST. AST software licenses are required for each agent that will access Enterprise CTI. Consult your Nortel representative to ensure that you have an appropriate level of AST support installed through Incremental Software Management (ISM).</p>
-------------------------	---

1.5.3. Supported ICM Features

The Meridian 1 PG supports the following ICM features:

- Pre-Routing
- Post-Routing
- Enterprise CTI (includes third-party call control)
- Agent Reporting
- Duplexed PG implementation

1.5.4. Multiple Application Support

The Nortel MEI option supports two styles of interface: MEI-Network and MEI-Observe. The Peripheral Gateway uses the MEI-Network interface. If you have third-party applications that also must use the MEI-Network interface, you need to install the Cisco MEI Server software. The *MEI Server software* allows multiple applications to share a single MEI-Network interface.

See also: For more information the Cisco MEI Server software, see Chapter 4, “ICM Software Configuration.”

1.5.5. Restrictions

- The Meridian PG does not support peripheral service level reporting.
- The Meridian PG supports a subset of trunk group real-time and half-hour data in the ICM database schema.
- The Meridian PG Post-Routing interface does not support Customer Entered Digits (CED).
- On systems that use the High-Speed Link, the Meridian Multiple Queue Assignment (MQA) feature is not supported.

2. ACD Configuration

Some configuration settings on the Meridian ACD must be changed to ensure proper operation with the ICM software. For example, in order for the PG to properly attribute calls to ICM routes and services, the Meridian Routes (ICM trunk groups) on which the calls arrive must have DNIS enabled.

This section describes the ACD configuration adjustments necessary for the Meridian to work with the ICM software. It also provides guidelines that will help you maintain your Meridian and ICM configurations.

2.1. Meridian MAX MEI

To interface with the ICM software, the Meridian MAX must meet the following requirements:

- The Meridian MAX system must be connected to the ICM visible LAN and configured with an IP address.
- The MEI option must be enabled and an IP port must be assigned to MEI. MEI does not define a default IP port number for MEI. Any valid port can be used. For consistency a value of 44444 is suggested for the MEI port.
- The MAX IP address and MEI port must be entered in the PG's configuration when the PG software is installed using ICM Setup.

2.2. Meridian 1

In order for the MEI to inform the PG of call and agent activity, the Meridian 1 must be configured to send this information to Meridian MAX. This includes the following switch configuration:

- The ACD DN and CDNs on the switch must be configured to send messages over the MEI. This is done in LD 23 by setting RPRT=YES for each ACD DN and CDN on the switch.
- If *Post-Routing* is used, then all CDNs that are to be post-routed must be configured to be in controlled mode. In addition, their VAS IDs must be set to the ID for the Meridian Link processor (**not** the VAS ID for CCR).
- In order for the PG to properly attribute calls to ICM routes and services, the Meridian routes (ICM trunk groups) on which the calls arrive must have DNIS enabled.

2.3. Additional Requirements for Enhanced CTI Mode and Cradle-to-Grave Reporting

Enhanced CTI mode requires additional changes to the ACD configuration:

- **ACD DNs.** ACD DNs must be configured with ISAP=YES and the VAS ID set to the ID for the Meridian Link processor (LD 23). Also the VAS ID in LD 15 must also be set to the Meridian Link processor.
- **ACD Positions.** All ACD positions need to be configured such that they send the required unsolicited status messages to Meridian Link. This is done by configuring the positions to be in an IAPG group that enables the required messages. The required messages are:

1,2,3,4,6,7,10,11,13,14,15

You can either configure all positions to be in Status Group 1 (all messages) or you can define a status group in LD 15 to contain just the

required messages and configure all positions to be in that Status Group.

- **AST.** All ACD positions need to be configured as AST. This is done in LD 10 and LD 11. For BCS sets that contain both an ACD position and an IDN, you should configure both keys as AST in LD 11.
- **Security.** The Meridian switch must have SECU=YES configured on the VAS ID for the Meridian Link. This prompt is set in LD 17. The current setting can be printed from LD 22. If SECU is not set to YES, the PG will still activate but third-party call control features will not work.
- **Security for ELAN.** If you are using the Meridian Link Services 4.0 configuration described in Chapter 1, you need to set security for the Ethernet Local Area Network (ELAN) to YES. If you are not using the Meridian Link Services 4.0 configuration, you **do not** need to perform this procedure.

➤ **To set security for ELAN to YES:**

1. Obtain the VAS ID of the ELAN and AML. To do this, type the following commands at the switch prompt:

Prompt:	Command to Enter:
>	LD 22
REQ	PRT
TYPE	VAS
TYPE	****

2. Next, set the Security of the ELAN:

Prompt:	Command to Enter:
>	LD 17
REQ	CHG
TYPE	VAS
VAS	CHG
VSID	<i>(Enter the VASID of ELAN)</i>
ELAN	<i>(Enter the VASID of ELAN)</i>
SECU	YES
VAS	****

3. Check to be sure that the switch is still enabled:

Prompt:	Command to Enter:
>	LD 48
.	STAT AML
.	STAT ELAN

4. If the switch is not enabled, enter the following commands at the switch prompt:

Prompt:	Command to Enter:
.	ENL AML <i>(Enter the VASID of AML)</i>
.	ENL ELAN
.	****

2.3.1. Meridian Mail Considerations

If Meridian Mail is integrated into the system, and there is any possibility that calls will be transferred from Meridian Mail to ACD agents, then the Meridian must be equipped with support for “Dual VAS ID.” Support for Dual VAS ID is included in Release 24 and up of Meridian X11 software. It is also available as a patch for Release 23.

The Dual VAS ID support is required so that the switch can send messages for the Meridian Mail ports to both Meridian Mail and Meridian Link.

There are two VAS IDs in LD 23 to configure for the Meridian Mail ACD DN: one points to the Meridian Link; the other points to Meridian Mail.

➤ **To set the VAS IDs:**

1. After setting Integrated Messaging Service (IMS) (that is, Meridian Mail) from LD 23 to YES, twelve or so new prompts are presented to be configured. Once the EES value is set, the next prompt is for a VAS ID. Enter the ID for Meridian Mail here.
2. Next, ISAP must be set to YES.
3. Immediately after setting ISAP, another prompt for a VAS ID is presented. Set this VAS ID to the ID for the Meridian Link processor.

Note: You must also configure the ACD positions for Meridian Mail in the ICM Peripheral Monitor table.

2.4. Meridian Link Capacity Considerations

Before installing the Enhanced CTI mode PIM, you must review the engineering of your Nortel Meridian Link to ensure that it can handle the expected message and CPU loads. In particular, review the values configured on the switch for INTL and MCNT. (Refer to Northern Telecom Publication 553-3211-520, “Meridian Link / Customer Controlled Routing Engineering Guide.”)

2.5. ACD Restrictions

Be aware of the following restrictions related to call tracking and reporting.

2.5.1. Network ACD and ICM Reporting

The use of network ACD to divert calls from one Meridian 1 to another can cause the ICM software to report inaccurate data because the progress of these calls is not reported through the MEI.

2.5.2. NCFW and CTI Data

If a call is translation routed to an ACD DN in night mode and that DN forwards the call to another ACD DN (the NCFW DN), the CTI data will not follow the call. This is due to the messages on the MEI link which treat the call as two separate calls.

This can be worked around in an ICM call routing script by checking the target DN for agents logged in. If no agents are logged in, then the DN is

in night mode. In this case, the script should translation route the calls directly to the eventual target DN.

2.6. Maintaining Your Configuration

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

3. ICM Software Setup

The ICM Setup tool is used to install ICM software components such as the Meridian PG and the Cisco MEI Server software. This chapter provides information specific to setting up a Meridian PG and, optionally, the Cisco MEI Server software, by using the ICM Setup tool.

See also: For specific information on using ICM Setup, see the *ICM Software Installation Guide*.

3.1. PG-MEI Configuration (without MEI Server)

This section describes the Meridian MEI-specific settings within ICM Setup that enable communication between the PG and MEI on the Meridian MAX.

Important: ICM Setup for PGs that use the MEI Server software is slightly different. (See “PG MEI Configuration (with MEI Server),” later in this chapter, for information.) Also, there are additional considerations for Meridian PGs running in Enhanced CTI mode. (See “Additional Considerations for Enhanced CTI Mode,” later in this chapter, for more information.)

Use the Meridian Configuration (PIM) window of ICM Setup to specify the MEI settings (see Figure 3).

Figure 3: MEI Configuration

The following Meridian MEI-specific settings must be made in ICM Setup:

- Set the “MEI Server A” field to be the IP name or address of the Meridian MAX system that is running MEI. Note that if the IP name is used then this name must be in the “hosts” file used by the PG.
- Set the “MEI Server A Port” field to be the port used when MEI was configured on Meridian MAX. A value of 44444 is suggested.

- Ignore the MEI Server B and MEI Server B port fields.
- Leave the “MEI Client ID” field at the default value (Cisco_ICM).

3.2. PG-MEI Configuration (with MEI Server)

This section describes the additional MEI settings required for PGs in which simplex or duplexed MEI Servers are used.

- Set the “MEI Server A” field to be the IP name or address of the MEI Server A system that is running MEI Server A. Note that if the IP name is used, then this name must be in the “hosts” file used by the PG.
- For a duplexed MEI Server system, set the “MEI Server B” field to be the IP name or address of the MEI Server B system that is running MEI Server B. Note that if the name is used, then this name must be in the “hosts” file used by the PG. Ignore this field for simplex MEI Server configurations.
- Set the “MEI Server A Port” field to be the port used when MEI was configured on MEI Server A. A value of 44444 is suggested for the first instance installed on the system. For multiple MEI Servers on one system, each MEI Server should have its own unique port number.
- For a duplexed MEI Server system, set the “MEI Server B Port” field to be the port used when MEI was configured on MEI Server B. A value of 44444 is suggested for the first instance installed on the system. For multiple MEI Servers on one system, each MEI Server should have its own unique port number.
- Leave the “MEI Client ID” field at the default value (Cisco_ICM).

3.3. Meridian Link Configuration

For the “Enhanced CTI Using MEI and Meridian Link” and “MEI with Meridian Link for Post-Routing Only” options, you must make settings in the Meridian Link Configuration portion of the Meridian Configuration (PIM) window (Figure 4).

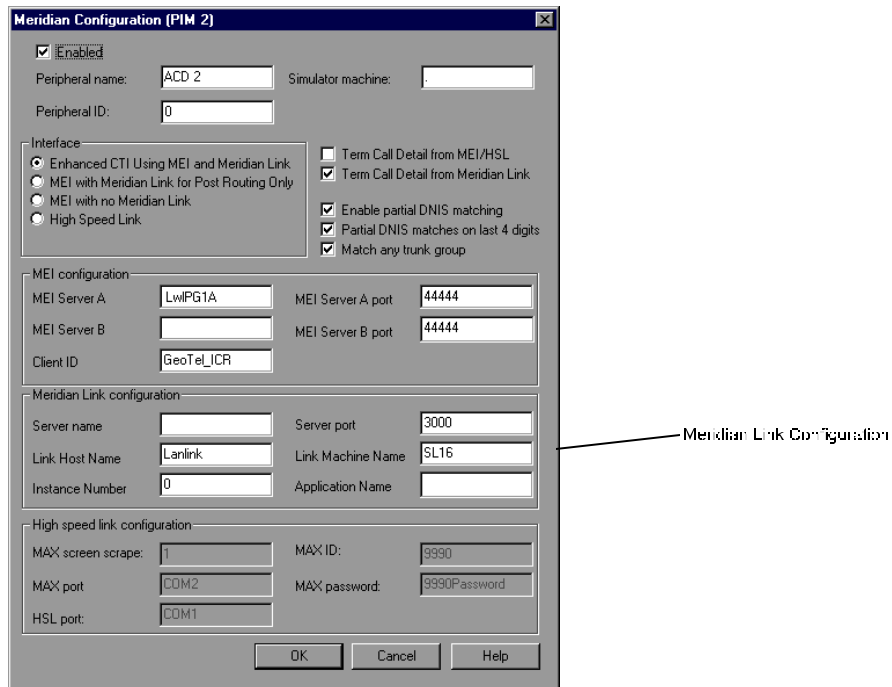


Figure 4: Meridian Link Configuration

The following Meridian Link settings must be made in ICM Setup (if you are using Meridian Link):

- Check the “MEI with Meridian Link for Post-Routing Only” checkbox if the PG is to act as a routing client (i.e., use *Post-Routing*).
- Set the Meridian Link “Server Name” field must to be the IP name or address of the Meridian Link system. Note that if the IP name is used, then this name must be in the “hosts” file used by the PG.
- Set the Meridian Link “Server Port” field to be the well known port used by Meridian Link. The Meridian Link and ICM Setup both use a default value of 3000.
- Set the “Link Host Name” to be the host name configured in the link 1 configuration file on the Meridian Link system. This defaults to “Lanlink” and normally should not be changed.
- Set the “Link Machine Name” to be the Meridian 1 Machine name in the link 0 configuration file on the Meridian Link system. This defaults to “SL16” and normally should not be changed.
- Set the “Customer Number” to be the customer number on the Meridian 1 that the PG wishes to route calls for. This defaults to 0.
- The “Application Name” is a string that uniquely identifies this ICM peripheral to the Meridian Link. It is recommended that you specify the NT machine name of the PG as the application name. If multiple PGs will access this particular Meridian Link, you must ensure that the Application Name used by each gateway is unique.

3.4. Additional Considerations for Enhanced CTI Mode

In order to run in Enhanced CTI mode, you must make some changes to the ICM Setup and the ICM configuration:

- In the Meridian Configuration (PIM) window in ICM Setup (see Figure 3), select “Enhanced CTI Using MEI and Meridian Link.”
- You must configure the positions on the Meridian 1 itself to have the AST attribute and to enable certain unsolicited messages. (See Chapter 2, “ACD Configuration,” for information on enabling the AST attribute).
- Configure all of your Meridian positions in the Peripheral Monitor table by using the Configure ICM tool. (See Chapter 4, “ICM Software Configuration,” for information on the ICM Peripheral Monitor table).

3.4.1. Monitoring of Call Event Messages

When running in Enhanced CTI mode, all call event messages that are sent to the Enterprise CTI Server are based on Meridian Link messages. As a result, CTI clients are informed earlier of call arrival (that is, CALL_DELIVERED/ALERTING). This is because the notification comes from the Meridian Link at the time the switch identifies the agent for the call.

Enhanced CTI mode also provides more detailed reporting of call events, including call initiation, transfer, and conference. (In the non-enhanced mode, clients are notified of call arrival only when the call is actually answered by the agent and notified over MEI.)

In Enhanced CTI mode, the PIM monitors calls through events on MEI and Meridian Link. For post-routed calls, the PIM tracks each call as a single call object, resulting in a single ICM Termination_Call_Detail record (assuming there were no consultation calls, which would result in more call detail records).

For calls that are not post-routed, the PIM actually tracks two call objects for each call. This is necessary because when post-routing is not used, there is no way to correlate the MEI events for a given call with the Meridian Link events. One call object is based on the MEI events. This is the call object that is used to attribute the call to ICM routes, services, and skill groups. The other call object is based on the Meridian Link events. This is the call object that is made visible to CTI clients through Enterprise CTI.

3.4.2. Termination_Call_Detail Options

When configuring the PIM to run in Enhanced CTI mode, you can choose whether you want the ICM software to write Termination_Call_Detail records for the MEI-based call objects, the Meridian Link-based call objects, or both. In either case, you will always get a single Termination_Call_Detail record for post-routed calls.

Figure 5 points out where you can make these selections within the ICM Setup Meridian Configuration (PIM) window.

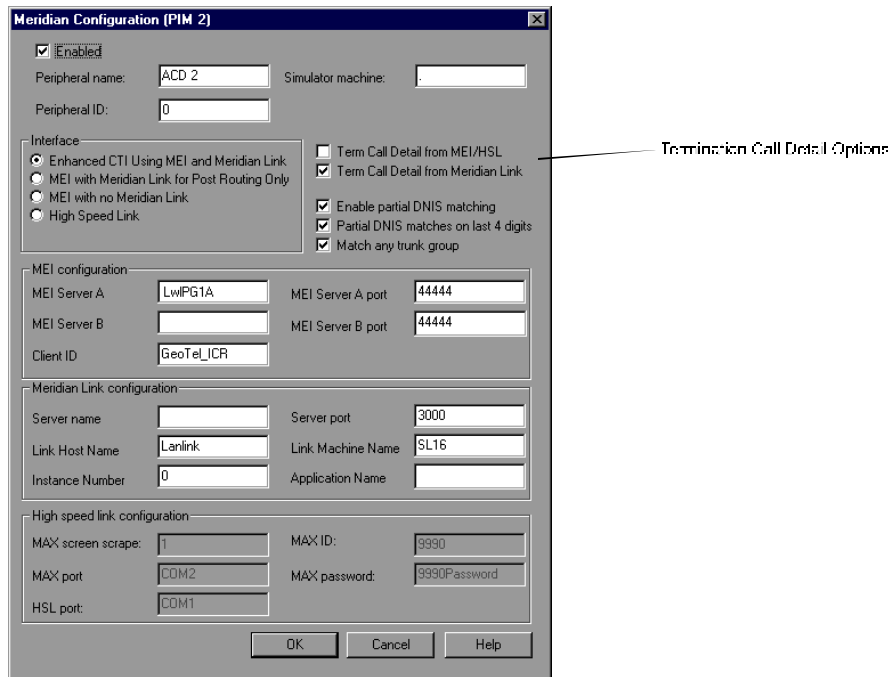


Figure 5: Termination Call Detail Options

MEI-based Termination_Call_Detail records for non-post-routed calls **will** include any queue time the call waited before being answered or abandoned, but they **will not** contain any updated call variable values that CTI clients may have set for the call.

Meridian Link-based Termination_Call_Detail records for non-post-routed calls **will** include any updated call variable values that CTI clients may have set for the call. They **will not** contain queue time since Meridian Link only notifies the host about non-post-routed calls when they reach an agent.

Note: When not running in Enhanced CTI mode, these checkboxes are disabled and you will receive termination records based on MEI only.

3.5. Cisco MEI Server Software

In configurations where multiple connections to the MEI are required, a Cisco ICM software product called the *MEI Server* is installed on the PG to provide additional connections. The MEI Server software is available in ICM Release 4.1 and beyond.

The Cisco MEI Server connects to a single MEI Network interface and provides multiple MEI network client connections. The MEI Server acts as a client to the MEI, which runs on the MAX system. The PG and any third-party applications act as clients to the MEI Server.

As shown in Figure 6, the MEI Server can be configured as simplex or duplexed.

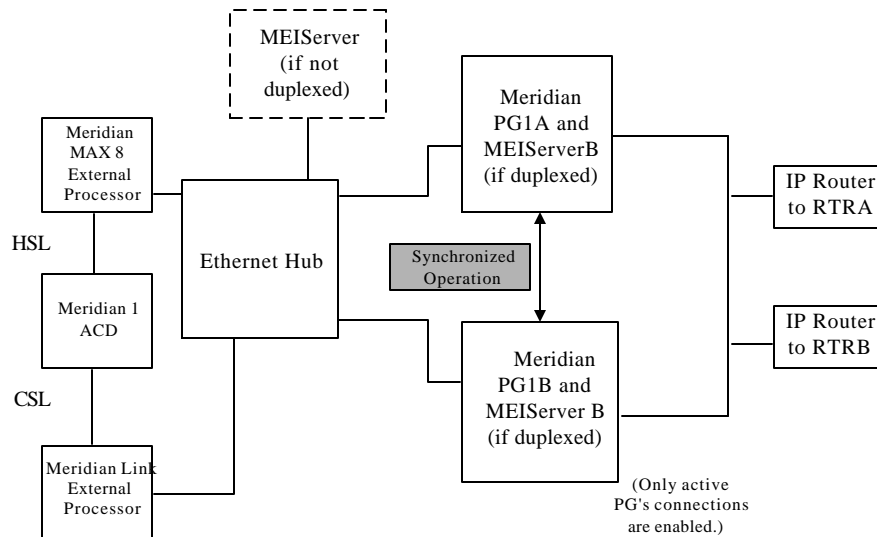


Figure 6: Sample MEI Server Configuration

3.5.1. When Is MEI Server Required?

If you have a standard duplexed PG configuration and no other applications need to use the MEI-Network interface, you **do not need** the MEI Server software. In a duplexed PG setup, only one side of the PG has an active connection to the MEI-Network interface at any one time.

If more than one logical PG needs to interface with the Meridian ACD, then you need to install the MEI Server software. An example of this would be two different customers, each with its own ICM software, and each sharing a single Meridian ACD. In this case, each PG will receive the full set of MEI messages from the MEI Server (that is, there is no partitioning capability in the MEI Server).

Note: Third-party applications that use the MEI-Observe interface do not interfere with the PG (which uses the MEI-Network interface) and can be used without the MEI Server.

3.5.2. Simplex PG Configurations

The MEI Server can be configured as simplex or duplexed. In either case, the PG(s) connects to a single MEI Network interface. In a simplex Meridian PG configuration, a single MEI Server can be installed on the PG machine. Figure 7 shows a system architecture that employs a single MEI Server with a two simplex PGs.

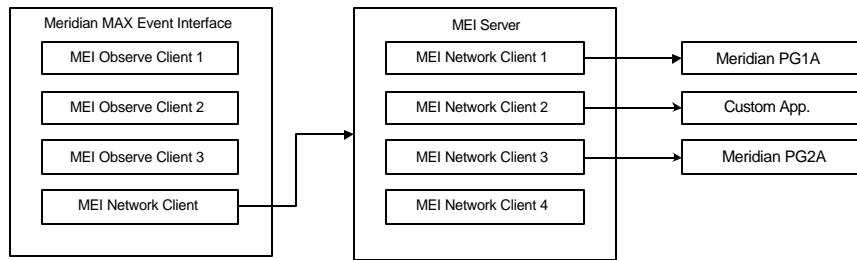


Figure 7: Simplex PG Configuration

The MEI Server can be installed on a PG or on its own machine. It is configured using the Meridian Max system hostname and the Meridian MAX MEI-Network port.

3.5.3. Duplexed PG Configurations

In a duplexed PG configuration, two MEI Servers are installed to provide redundancy. An MEI Server can be installed on each PG (for example, one on PG1A, one of PG1B), or the MEI Servers can be installed on their own platforms. Figure 8 shows a system architecture that employs duplexed MEI Servers and a duplexed PG.

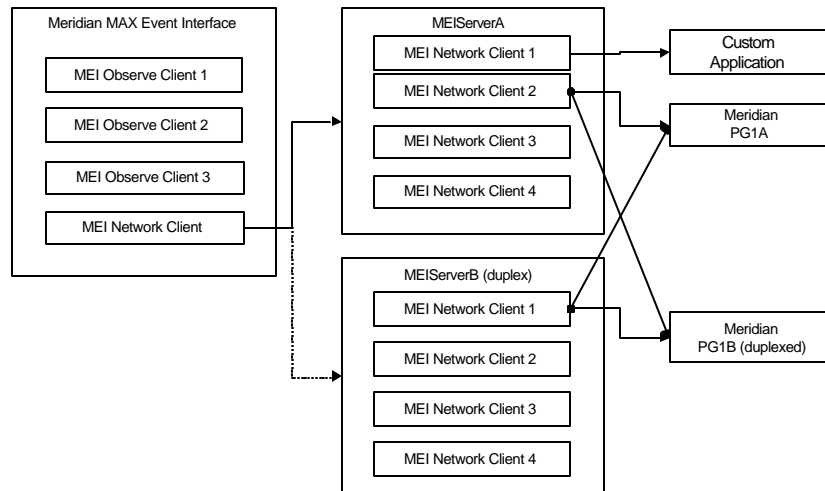


Figure 8: Duplexed PG Configurations

Each side of the duplexed PG is configured to locate the two sides of the MEI Server and their respective ports. When the PG starts up, it attempts to connect to one MEI Server. If this is not successful, it attempts to connect to the other MEI Server.

The MEI Servers are configured to locate the same Meridian MAX system host-name and to use the same Meridian MAX MEI-Network port. Although the two MEI Servers share the same MEI-Network interface, only one of the MEI Servers has an active connection to the MEI-Network interface at any given time. One MEI Server remains idle. If the active

MEI Server releases its connection with MEI Network interface, the idle MEI Server establishes a connection.

See also: See Chapter 4, “ICM Software Configuration,” for instructions on configuring PGs with and without MEI Server.

3.5.4. Limitations in a Duplexed MEI Server Environment

Mission-critical third-party applications **should not** be run through a duplexed MEI Server unless the application are able to perform automatic switchover between the two sides of the duplexed MEI Server.

Third-party applications likely do not have the capability to attempt connections to duplexed MEI Servers in sequence since the Meridian MAX is not redundant. Typically, such applications are coded to directly support a single MEI. This may mean that these applications have to be configured to access a “primary” MEI Server (i.e., the side A MEI Server).

However, this is not an ideal configuration because the application still has no mechanism to automatically switch over to a backup MEI Server. For example, if the primary MEI Server fails and the active MEI connection is taken over by the backup MEI Server, the third-party application would lose its access to the MEI. Manual intervention would be required to reestablish MEI Server access to the third-party application. First the problem with the primary MEI Server would have to be fixed. Then the backup MEI Server would have to be shut down to allow the third-party application to reestablish its connection with the primary MEI Server.

3.5.5. Adding MEI Server to an Existing PG

If required, the MEI Server can be added to a currently installed PG. However, since currently installed PGs are configured to directly access MEI, you must change the ICM PG Setup. Specifically, you must configure the PG to locate the MEI Server host-name and MEI Server port (44444 by convention). You must also configure any custom applications to locate the MEI Server hostname and server port.

See also: See the “PG-MEI Configuration” sections, earlier in this chapter, for instructions on configuring PGs with and without MEI Server.

3.5.6. MEI Server Setup

To install the MEI Server, use the ICM Setup tool. The MEI Server properties window of ICM Setup is shown in (Figure 9).

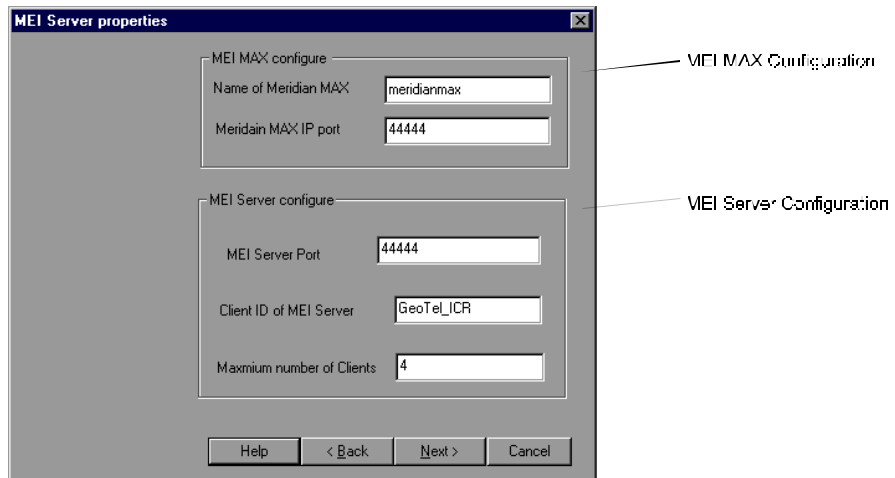


Figure 9: MEI Server Properties

MEI MAX Configuration

MEI Server must be configured through the ICM Setup program to communicate with the MEI on the Meridian Max:

- Set the “Name of Meridian Max” field to be the hostname or IP address of the Meridian MAX system that is running MEI. Note that if the IP name is used, the name must be in the “hosts” file used by the MEI Server (for example, meridianmax).
- Set the “Meridian MAX IP port” field to be the port used when MEI was configured on Meridian MAX (44444 is the suggested value).

MEI Server Configuration

MEI Server must be configured through the ICM Setup program to listen to the connections from the PG:

- Set the “MEI Server Port” field to be the port used by the Meridian PG. If multiple MEI Servers are installed on one system, the port numbers should be unique for each MEI Server.
- Leave the “Client ID of MEI Server” set at the default value (Cisco_ICM).
- Leave the “Maximum number of Clients” at the default value (4), which is the maximum number of client applications (including the ICM software) which can be connected to the MEI Server.

4. ICM Software Configuration

In order to properly configure and maintain the ICM database, you need to understand the relationships between the Nortel Meridian database objects and the ICM database objects. For example, ICM skill groups correspond to the Meridian ACD DN into which the agent logs on. ICM services do not necessarily map to anything configured on the Meridian.

By understanding the relationships between the database objects of the Meridian and ICM software, it will be easier to keep the Meridian and ICM databases synchronized (that is, up-to-date with each other).

This section describes how objects map between the Meridian ACD and the ICM software. It also provides information specific to configuring a Meridian PG by using the Configure ICM tool.

See also: For detailed information on the Configure ICM user interface, see the *ICM Software Configuration Guide*.

4.1. Peripheral Configuration

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

No special peripheral configuration parameters are required. However, there are certain items within the ICM configuration that you may want to check.

4.1.1. Peripheral Configuration Parameters

The “Requesters→Configure PG” option in Configure ICM automatically creates a peripheral object with the appropriate defaults for a Meridian peripheral (see Figure 10).

The screenshot shows a 'Peripheral Configuration' window with the following fields and values:

- Peripheral ID: 5000
- Logical Controller: Lowell_PG
- Type: Meridian
- Enterprise Name: Lowell_PG_1
- Peripheral Name: Lowell_PG_1
- Location: (empty)
- Aband Call Wait Time: 5 seconds
- Configuration Parameters: (empty)
- Call Control Variable Map: (empty)
- Description: (empty)
- Default Desk Settings: (empty)
- Peripheral Service Level Type: (empty)
- Service Level Type: Abandoned Calls Ignored
- Service Level Threshold: 30 seconds
- Available Holdoff Delay: 0 seconds
- Default Route: (empty)
- Answered Short Calls Threshold: 0 seconds
- Network VRU: <None>
- Agent Reporting:
- Agent Auto-Configuration:
- SkillGroup Mask: Absent

Buttons at the bottom: Skill Group Mask, Apply, Revert, Help, Done.

Figure 10: Peripheral Configuration (ICM 4.1 and earlier)

In ICM Software, Release 4.5 and beyond, a new tool called the PG Explorer tool can be used to configure PGs (see Figure 11).

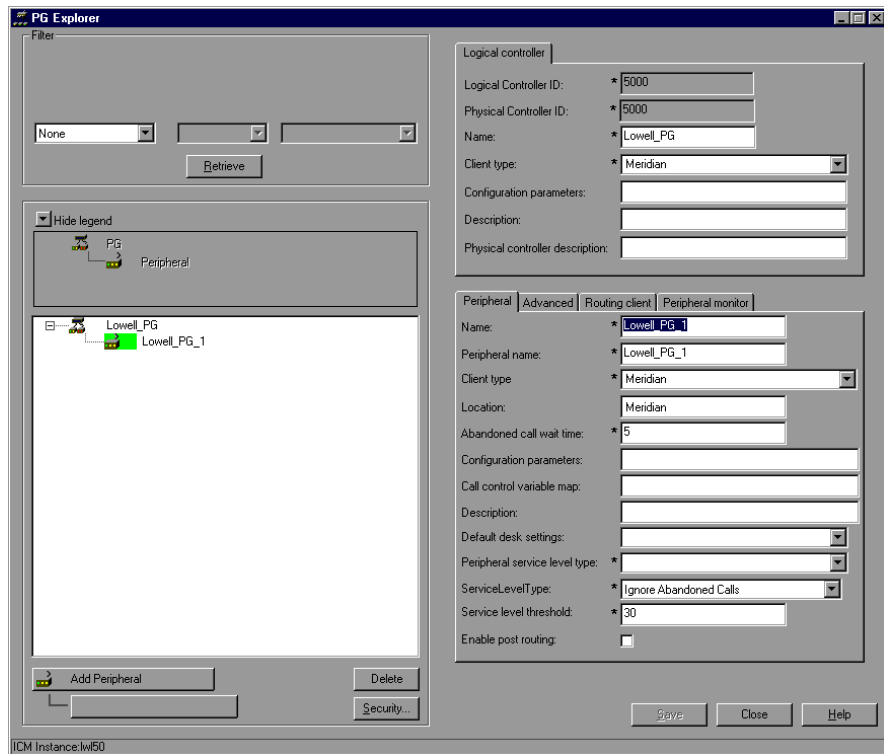


Figure 11: PG Explorer (ICM 4.5 and beyond)

Note that the “Peripheral Service Level Type” setting has no effect since the Meridian PG does not report a peripheral service level (it does report an ICM service level).

In addition, the “Available Holdoff Delay” setting is used by all skill groups for this peripheral that do not explicitly specify a value for “Available Holdoff Delay” at the skill group level. (See “Skill Groups,” later in this chapter for a discussion of the meaning of this value.)

4.1.2. Peripheral Call Control Variable Map

The mapping of route request elements to Peripheral Variables is controlled by the Call Control Variable Map field, which is found on the Peripheral Configuration window within Configure ICM (Figure 12).

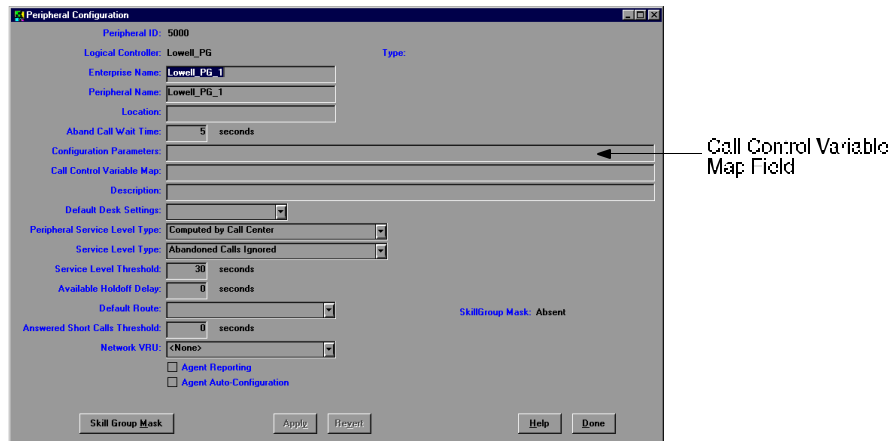


Figure 12: Call Control Variable Map Field

The Call Control Variable Map field can be used to configure which peripheral variables should be reserved for a CTI application, and which ones the PG can use. There are two ways to control variable usage via the CallControlVariableMap:

- Direct the PIM.** The PIM can be directed on which call variables can be accessed. For example, the following setting allows the PIM to set call variable 1 and call variables 5 through 10 while preserving the existing values of call variables 2 through 4 (i.e., the PIM will not set call variables 2 through 4). Note, this argument is from the perspective of the Peripheral Interface Manager (PIM).

```
/PIM=ynnnyyyyyy
```

- Direct the CTI portion of the PG.** The CTI portion of the PG can be directed to allow the CTI Client to override any PIM Call Variable setting. For example, the following setting allows a CTI Client (that is, a third-party application) to set call variable 1 and call variables 5 through 10, while preserving the peripheral-determined values of call variables 2 through 4.

```
/CTI = ynnnyyyyyy
```

See also: For more information on route request elements, see Chapter 5, “Post-Routing.” For more details on ICM CTI capabilities and interaction with the PG, refer to the *ICM Software Enterprise CTI Interface Specification*.

4.1.3. Overwriting of Peripheral Call Variables 1 and 2

By default, the Meridian PIM allows the call variable information in PeripheralVariables 1 and 2 to be overwritten. For example, when Post-

Routing and Translation Routing are used, the PIM sets PeripheralVariable1 with the OriginationAddressDN (DNIS, device, etc.). The PIM sets PeripheralVariable2 with the OriginationAddressDNType, which may have one of the following values:

- 08 Internal
- 09 Trunk Access Code/Member
- 0A Route only
- 0B Attendent/Member
- 0C ACD DN/ACD position
- 0F In-Band ANI
- 16 CDN
- 17 DCN/DNIS
- 1E ACD POS ID
- 27 TrunkRoute and Member

For RouteRequest messages, the OriginationAddressDNType is limited to 16 and 17.

In some cases, you may want to disable automatic overwriting by the PIM. The following registry key controls whether or not the Meridian PIM automatically overwrites PeripheralVariables 1 and 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\ICR\CustomerName\PG1\PG\
CurrentVersion\PIMs1\MeridianData\Dynamic\MeridianLinkPeriphVarUse
```

The default configuration setting of this key is 0, which means that automatic overwriting by the PIM is enabled. To disable automatic overwriting of call variables 1 and 2 by the Meridian PIM, set this registry key to 1.

4.2. Peripheral Target Configuration

An ICM *peripheral target* is a network target identified by a Network Trunk Group and DNIS that terminates on the Meridian ACD. A peripheral target **must be configured** for all DNIS and Network Trunk Group combinations through which incoming ACD calls arrive.

You can configure Peripheral Targets by using the Peripheral Target Configuration window within Configure ICM (Figure 13).

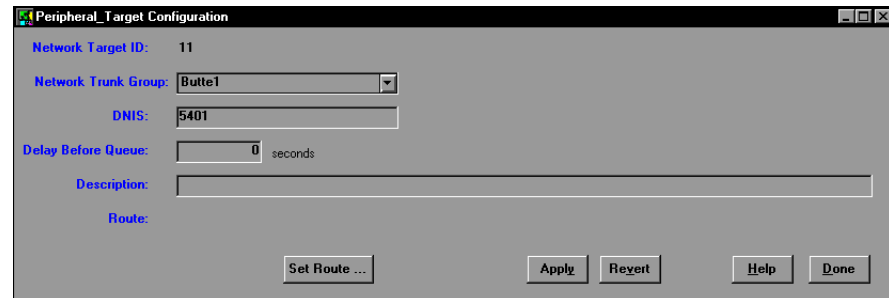


Figure 13: Peripheral Target Configuration Window

Note that the Meridian ACD supports configurations where multiple Incoming Digit Conversion (IDC) tables can be used to map a single DNIS value to different destination DNs on different Meridian routes (that is, ICM trunk groups). If this feature is used, then care must be taken when configuring network trunk groups and peripheral targets in the ICM software.

Specifically, all the trunk groups in a network trunk group should map DNIS values the same way. If multiple IDC tables are in use, network trunk groups should be created to correspond to each IDC table. Peripheral targets should then be created to correspond to each network trunk group in use.

Peripheral targets **must also be configured** for Translation Routing. In addition, Translation Routing requires that the translation route DNIS values map to the same CDN on all trunk groups. So, if multiple IDC tables are used, care should be taken to ensure that the translation route DNIS values map to the same CDN in each IDC table.

See also: For more information on Translation Routing, see Chapter 5, “Post-Routing.”

4.2.1. Attributing Calls to ICM Routes

For ICM route statistics, the PG attributes calls to ICM routes by looking for a peripheral target that matches the trunk group and DNIS for the call and using the route associated with that peripheral target. If no matching peripheral target is found then the call is attributed to the default route for the peripheral (if one is configured).

4.2.2. Not Configuring Peripheral Targets for Each Trunk Group

If the design of the routing application does not require that separate peripheral targets be configured for every trunk group on which a given DNIS can arrive, then the PG can be configured to match incoming calls against any peripheral target that matches the DNIS, regardless of trunk group.

In order to configure the PG to act in this way, you must check the “Match Any Trunk Group” checkbox on the “Meridian Configuration” window in ICM Setup for the PG.

See also: Chapter 3, “ICM Software Setup,” provides an example of the Meridian Configuration window in ICM Setup.

You must also set the following OPC registry variable to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\ICM\PGxx\PG\CurrentVersion\OPC\
MapPeripheralTargetsWithoutTrunkGroup
```

Note that even if these fields are set to search for peripheral targets without trunk group, if the trunk group is available and a peripheral target is configured that does match the trunk group then that peripheral target will be used.

As of ICM Release 2.0, both of these fields are set to “TRUE” by default. Note that the use of translation routing requires that both of these fields be set to “TRUE.”

4.2.3. Using DNIS Values Longer Than Four Digits

The Meridian supports DNIS values up to seven digits in length. However, when using Meridian X11 software prior to Release 23, the MEI interface only provides a maximum of four DNIS digits to the PG. The Meridian can be configured to send either the first four or last four DNIS digits for DNIS lengths greater than four.

By default the Meridian PG will match DNIS values received from MEI against the last four digits of DNIS values configured in peripheral targets. This allows the ICM peripheral targets to be configured with the full DNIS values and still match.

In cases where two DNIS values are not unique in the last four digits (e.g. 11234 and 21234), the PG attempts to determine the correct match by looking at the ICM service associated with the route associated with each matching peripheral target. If only one of these services match the DN to which the call was presented on the Meridian, then the peripheral target that corresponds to this service is used. If there is more than one match, then the matching peripheral target with the lowest numerical DNIS value is used. In either case, the PG substitutes the full configured ICM DNIS value for the four-digit value and stores the full value in the termination call detail record.

Note: In cases where there is no unique match, this DNIS value may not be the actual DNIS value associated with the call (though at least the last four digits will be correct).

If the Meridian is configured to send the first four digits of DNIS instead of the last four, then you must clear the “Partial DNIS Matches On Last Four Digits” checkbox on the “Meridian Configuration” window within ICM Setup for the PG. This will cause the PG to match on the first four digits of DNIS.

To disable the partial DNIS matching feature and require that DNIS values exactly match the values configured in ICM peripheral targets, clear the “Enable Partial DNIS Matching” checkbox on the “Meridian Configuration” window within ICM Setup for the PG.

4.2.4. Setting the Delay Before Queue Value

The ICM distinguishes between calls that truly waited in queue before being handled and calls that were answered as soon as possible after some mandatory delay not related to agent availability. For example, if a caller is required to first hear an announcement in its entirety before being connected to an agent and the caller is connected to an agent directly after having heard the announcement, then the call is not considered to have been queued.

In order to support this distinction, the ICM software administrator must set the “Delay Before Queue” value for peripheral targets that enforce a mandatory delay. This is done through the Peripheral Target Configuration window of Configure ICM (see Figure 14). To display this window, choose Targets→Peripheral Target from the Configure ICM main menu. Then select a peripheral target from the list to update.

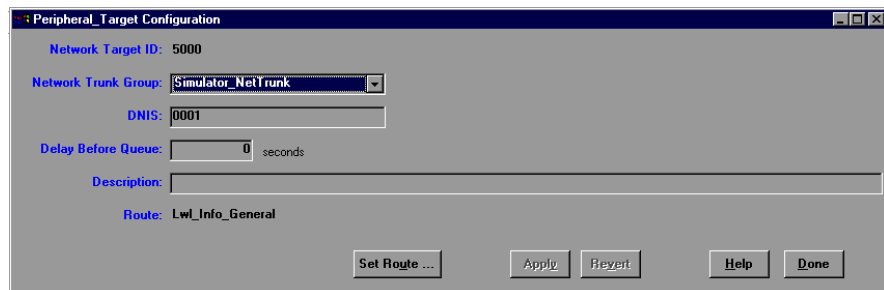


Figure 14: Peripheral Target Configuration

For example, if the trunk group/DNIS combination 1/1001 maps to a DN in night service that plays a “first RAN on arrival” and then forwards the call to a night destination, then the “Delay Before Queue” value should be set to the number of seconds that the announcement takes. Note that flexible call force times can also prevent a call from being answered immediately even if agents are available when the call arrives. These timers should be accounted for in the “Available Holdoff Delay” field of the skill group configuration (see “Skill Groups,” later in this chapter for more details).

4.3. Trunk Group Configuration

The ICM software and Meridian mapping for trunk groups is as follows:

ICM Software	Meridian
Trunk Group	Route
Trunk Group Peripheral Number	Route number (e.g., Route 5)
Number of ICM trunks in a trunk group	Count of Meridian Members within a Meridian Route
Trunk Group Extension	Meridian Route Access Code (ACOD) for the Route

Trunk groups are configured in the Trunk Group Configuration window of Configure ICM (Figure 15).

Figure 15: Trunk Group Configuration

To display this window, choose Peripherals→Trunk Group from the Configure ICM main menu. Select a trunk group from the list to update.

There are several trunk group settings for the Meridian PG.:

- Configure an ICM Trunk Group for each Meridian Route on which ACD calls arrive.
- Set the ICM Peripheral Number to be the Meridian ACD Route Number.
- Set the ICM Trunk Count to be the number of Meridian Members in the Meridian Route.
- Set the ICM Trunk Group Extension to be the Meridian route access code (ACOD) for this Meridian route. (This allows the Enhanced CTI mode PIM to associate post-routed calls that arrive on trunks that do not provide ANI with the correct trunk. If the extension is not

configured (or if enhanced CTI mode is not used) post-routed calls are not associated with trunks by the PIM.)

4.4. Trunk Configuration

Individual trunks are not monitored by the Meridian PG. As a result, trunks need not be entered in the ICM configuration.

4.5. Service Configuration

ICM services do not necessarily map directly to anything configured on the Meridian. An ICM service is a particular type of processing that a caller requires. ICM Services are configured in the Service Configuration window of Configure ICM (Figure 16).

The screenshot shows the 'Service Configuration' dialog box. It contains the following fields and controls:

- Skill Target ID: 5000
- Peripheral: Lowell_PG_1 (dropdown)
- Peripheral Number: 1 (text input)
- Peripheral Name: Information (text input)
- Enterprise Name: Lowell_PG_1.Information (text input)
- Extension: (empty text input)
- Peripheral Service Level: Use Peripheral Default (dropdown)
- Service Level Type: Use Peripheral Default (dropdown)
- Service Level Threshold: Default seconds (text input)
- ConfigParm: (empty text input)
- Description: (empty text input)
- Deleted: Yes No
- Buttons: Apply, Revert, Help, Done

Figure 16: Service Configuration

There are several items to note for Meridian service configuration:

- Set the ICM peripheral number to be the ACD DN or CDN number that corresponds to the service. For services that do not correspond to anything configured on the Meridian 1 (for example, the “default” service for a peripheral), the peripheral number should be chosen so as not to coincide with any real ACD DN or CDN.
- The “Extension” value is not currently used.
- The “Peripheral Service Level Type” setting has no effect since the Meridian PG does not report a peripheral service level (it does report an ICM service level).

4.5.1. Configuring Services for ACD DNs

In some cases, Meridian ACD DNs can be made to correspond to ICM services. To do this, use Configure ICM and set the ICM Peripheral Number of the service to the ACD DN number.

Some ACD DNs may be used simply as skill groups available to answer calls arriving at many other ACD DNs (ICM services). In this case, these

“skill group” ACD DNs would be configured in the ICM as skill groups and not as services.

4.5.2. Configuring Services for CDNs

If calls are directed to Meridian CDNs, then typically an ICM service would be configured with the ICM Peripheral Number set to the CDN number.

4.5.3. Attributing Calls To Services

When an ACD call arrives at a Meridian ACD, the Meridian PG attempts to attribute the call to an ICM service:

- If the directory number (ACD DN or CDN) to which the call is presented matches the peripheral number of a configured ICM service, then the PG attributes the call to that service.
- If no configured service matches the directory number, then the PG looks for a peripheral target whose trunk group and DNIS match the trunk group (Meridian Route) and DNIS for the call. If a matching peripheral target is found, and this peripheral target has an associated route, and the route, in turn, has an associated service, then the PG attributes the call to that service.
- If neither of the previous two methods yields a service, then the PG attributes the call to the service associated with the default route for the peripheral (if configured). Note that calls are attributed to the service corresponding to the directory number to which the call is originally presented.

If Meridian features such as “Night Call Forward,” “Basic Time Overflow,” “Enhanced Time Overflow,” or “Automatic Overflow” are used, they do not affect the ICM service to which the call is attributed. For example, if calls arrive at DN 1 and are overflowed to DN 2 through time overflow, the calls will be attributed to the ICM service corresponding to DN 1. If the calls are ultimately answered by agents in DN 2 they will be attributed to the ICM skill group corresponding to DN 2.

4.5.4. Overriding DN with Route-to-Service Mapping

The Enhanced CTI mode Meridian PG provides an additional option for attributing calls to services. This option allows the PG (specifically, the PIM) to always attribute the call according to the Peripheral Target-to-Route-to-Service mapping defined in the ICM configuration. This is slightly different from the method described in the previous section.

In this mode, even if the directory number to which the call is delivered matches the peripheral number of a configured ICM service, the PIM will ignore that service and attribute the call according to the Peripheral Target-to-Route-to-Service mapping defined in the ICM configuration.

To enable this mode, set the registry value “DNOverrideRouteToService” to zero in the PIM registry. This value can be found in the following registry key:

```
HKEY_LOCAL_MACHINE\Software\cisco\icr\custname\pg\currentversion\pimx
MeridianData\Dynamic
```

4.6. Skill Group Configuration

The ICM software and Meridian Skill Group mapping is as follows:

ICM Software	Meridian
Skill Group	Meridian ACD DN into which agents log in.
Skill Group Peripheral Number	ACD DN number
Skill Group Extension	(Not used by Aspect PG)

Note: If no agents log in to an ACD DN then an ICM skill group need not be configured for it.

ICM Skill Groups are configured in the Skill Group Configuration window of Configure ICM (Figure 17).

Figure 17: Skill Group Configuration

There are several items to note for Meridian skill group configuration:

- Set the ICM Skill Group Peripheral Number to be the ACD DN number.
- The “Extension” value is not currently used.
- The sum of "Available Holdoff Delay" and the value of dynamic PIM registry subkey "ExtraSecondsBeforeAvailable" should match the flexible call force timer (FCFT) for this ACD DN. If "Available Holdoff Delay" is left as “Use Peripheral Default,” then the default value configured for this peripheral will be used for "Available Holdoff Delay".

The “Available Holdoff Delay” field and dynamic PIM registry subkey "ExtraSecondsBeforeAvailable" are used by the PG to determine when the agents are truly available. For example, if the FCFT is set to 5 seconds, then the "Available Holdoff Delay" and "ExtraSecondsBeforeAvailable" should be configured such that their sum is 5. With this configuration, when an agent releases an ACD call, that agent is not truly available to answer another ACD call until five seconds have elapsed.

4.6.1. Skill Group Priorities

Agents in a Meridian ACD DN have a priority associated with them from 1 to 48. By default, the ICM software will consider all agents logged in to a given ACD DN to be in a single skill group for that DN regardless of priority. However, it is possible to configure some or all of the skill groups to contain sub groups for discrete priority levels (e.g., 1, 2, 3 or 1, 5, 10 etc.). If a skill group is configured with sub groups for priorities then the ICM will track skill group data for each sub group individually and for the overall group as a whole.

4.7. Service Member Mapping

The ICM Service Member mapping corresponds to the group of ACD DN's whose agents are eligible to answer a call to a given service. For example, if calls to CDN 1000 are queued to ACD DN's 2100 and 2200, then the ICM configuration would include service member relationships that would associate skill groups 2100 and 2200 with service 1000. Or, if calls to ACD DN 3000 are queued through an NACD day table to DN's 4100 and 4200, then the ICM configuration would include service member relationships that would associate skill groups 4100 and 4200 with service 3000.

No special ICM configuration consideration is required.

4.8. Agent Configuration

The ICM software and Meridian Agent mapping is as follows:

ICM Software	Meridian
Agent	ACD Agent
Peripheral Number	Meridian Agent ID (or Position ID)
Extension	Meridian Position ID

It is **not necessary** to pre-configure Meridian agents in the ICM software.

If agents are configured, then set the ICM Peripheral Number to be the Meridian Agent ID (or Position ID if the Meridian is running in Position ID mode). Set the ICM extension to be the Meridian Position ID.

4.8.1. Skill Group Members

If agents are configured in the ICM software, then the skill groups to which the agents log in can also be configured through the ICM Skill Group Member table. Note that this is only used optionally to generate events if agents log in to the wrong group(s).

For skill group monitoring purposes, the ICM software always counts an agent's time against the skill group(s) into which he is currently logged, not the skill groups configured as skill group members for the agent.

4.8.2. Agent States

Table 5 lists the ICM software agent states and the Meridian agent states from which they are derived.

Table 5: ICM Software–Meridian Agent State Derivation

ICM Software State	Derivation from Meridian Agent State
Not Ready	Walkaway
Ready	Logged in and not in Walkaway
Available	WAIT
WorkNotReady	Not used.
WorkReady	NOT READY
TalkingIn	Talking on an ACD call
TalkingOut	Not used.
TalkingOther	Talking on a DN call
Reserved	RESERVE
Logged Out	SPARE

4.8.3. Agent ID

If a Meridian peripheral needs to use Agent IDs with leading zeroes, all IDs for that peripheral are restricted to a 4-digit length due to limitations in the MAX interface. The Meridian PIM dynamic registry subkey `LeadingZeroFourDigitAgentID` must be enabled before this feature is activated.

ICM versions that support Meridian Agent IDs with leading zeroes are:

- **ICM version 4.6.1**
Install hotfix #112. If leading zeroes are used:
Agent level reporting is not available. Peripheral configuration Agent Reporting and Auto Agent reporting must be disabled. Agent configuration cannot be entered.
- **ICM version 4.6.2**
Install hotfix #16. If leading zeroes are used:
Agent level reporting is not available. Peripheral configuration Agent

Reporting and Auto Agent reporting must be disabled. Agent configuration cannot be entered.

4.9. Route Configuration

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

No special ICM configuration consideration is required.

4.10. Routing Client Configuration

The Meridian PG supports *Post-Routing* and can be configured as a Routing Client. Use the “Configure PG” window within the Configure ICM tool to configure the Meridian PG as a Routing Client and enable Post-Routing.

Note: In ICM software, Release 4.5 and beyond, use the PG Explorer tool to configure the PG as a Routing Client and enable Post-Routing.

If a routing client is enabled for a Meridian PG, you must select either “Enhanced CTI Using Meridian Link and MEI” or “MEI with Meridian Link for Post-Routing Only” when the peripheral is added via the ICM Setup tool.

See also: Chapter 3, “ICM Software Setup,” contains more information about these ICM Setup options.

4.11. Dialed Number Configuration

ICM dialed numbers for the peripheral’s routing client correspond to the CDNs on the Meridian 1 that are to be post-routed. ICM dialed numbers must also be configured for any CDNs to which calls are directed as part of a Translation Route.

If *Post-Routing* is used to route external DNIS calls arriving at the Meridian then, by default, the CDN is used as the dialed number when the PIM sends the route request to the CallRouter. If it is necessary for routing purposes to differentiate calls by DNIS, then you can configure special dialed numbers within the Configure ICM tool of the form CDN.DNIS.

For example, say DNIS values 1001 and 1002 both map to CDN 1000. If you want your routing script to treat these different DNIS values differently, you could configure dialed numbers 1000.1001 and 1000.1002. You would also need to configure a dialed number for the CDN itself “1000.”

When calls arrived at CDN 1000 with DNIS 1001, the PIM would send “1000.1001” as the dialed number instead of simply “1000.” The ICM *CallRouter* can be configured to treat these calls specially. This allows a single CDN to be used to post-route multiple external call types differentiated by DNIS.

See *also*: For more information on ICM Post-Routing capabilities, see Chapter 5, “Post-Routing.”

4.12. Label Configuration

ICM labels for the peripheral’s routing client correspond to destinations to which calls can be routed. Labels can be configured for any number that can be dialed on the switch. For example, this could be an ACD DN, CDN, or route access code followed by external number.

Each destination to which post-routed calls should be routed should have an ICM label configured with the label string set to the destination as it would be dialed from a phone set. For example, labels may be configured to route calls to an ACD DN, CDN, individual DN, or route access code and external number.

See *also*: See “Special Label Characters,” in Chapter 2, “ACD Configuration,” for more information.

4.13. Peripheral Monitor Configuration of ACD Positions

When running in Enhanced CTI mode, you must configure your Meridian Positions in the ICM Peripheral Monitor table. This is required so that the PIM can register with Meridian Link to receive events for these positions. It also allows the PIM to associate IDNs with their corresponding position ID values.

Note: If you do not configure all of your positions correctly, you may experience difficulty monitoring data and using Enterprise CTI.

To configure ACD positions in the Peripheral Monitor table, use the Peripheral Monitor Configuration window in Configure ICM (Figure 18).

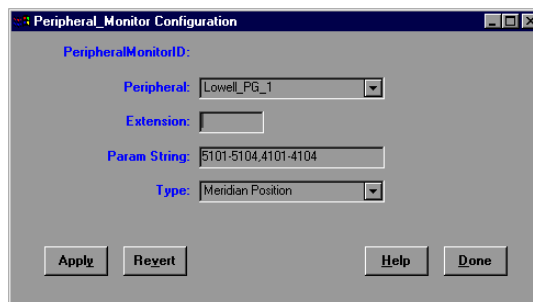


Figure 18: Peripheral Monitor Configuration

Note: In ICM Software, Release 4.5 and beyond, you can also configure ACD positions in the Peripheral Monitor Table by using the PG Explorer tool.

There are several things to note when you are configuring ACD positions in the Peripheral Monitor table:

- The extension field is not currently used.
- The “Param String” field allows several different types of input that can be used to specify individual positions or ranges of positions (see below). The Type field should be set to “Meridian Position.”

The “Param String” field can be used to specify a single ACD position, a range of positions, a single ACD position and IDN pair, or a range of positions and IDN pairs. A dash is used to indicate a range. A comma is used to indicate that what follows is an IDN specification.

Table 6: Peripheral Monitor Param String Field

Param String Format	Example	Meaning
ACD Position	5201	Indicates a single ACD position “5201” with no associated IDN
ACD Position, IDN	5201,4201	Indicates a single ACD position “5201” with associated IDN “4201”
ACD Position ID Range	5201-5299	Indicates a range of ACD positions from “5201” up to “5299.” None of these positions have associated IDN keys.
ACD Position ID Range, IDN Range	5201-5299, 4201-4299	Indicates a range of ACD positions from “5201” up to “5299.” Position 5201 is associated with IDN 4201. Position 5202 is associated with IDN 4202 etc.

If your position ID and IDN values are arranged in sequence, then you can reduce the amount of entries required in the peripheral monitor table by specifying ranges of positions. Note that the maximum range allowed by the PIM is 200 positions. If you have ranges that span more than 200 positions then you must enter them as multiple contiguous ranges in Configure ICM.

4.14. Maintaining Your Configuration

It is important to keep your ICM configuration up to date as you make configuration changes on your Meridian 1. It is preferred that changes made to your configuration be accomplished first on the Meridian ACD, then in the ICM configuration. This will ensure that the PG sees the configuration updates on the Meridian ACD systems.

The following types of Meridian 1 changes need to be reflected in the ICM configuration:

- Addition of new ACD-DNs. Also, if new priorities are put into use and the ICM software is configured with sub-skill groups with explicit priorities then this configuration must be kept up to date.
- Addition of new CDNs. May require creation of new services and of dialed numbers if the CDNs are to be post-routed.
- Changes to FCFT values for ACD-DNs.
- Changes to DNIS to DN mappings.
- Changes to NACD tables that queue calls to DNs.
- Changes to CCR scripts that queue calls to DNs.
- Changes to ACD positions and IDNs must be reflected in your ICM Peripheral Monitor table if running in Enhanced CTI mode.

5. Post-Routing

This chapter describes the features of ICM Post-Routing available with the Meridian PG. It also discusses any considerations you should be aware of when using Post-Routing or Translation Routing on the Meridian PG.

5.1. Calling Line ID

The ICM Script Editor allows the script writer to check the calling line ID (CLID) for calls. However, CLID is not available in all cases. The Meridian Link interface provides the PG with an origination address and an origination address type for route requests. If the origination address type indicates that the origination address is a calling line ID, then the origination address is passed as the calling line ID. Otherwise, the calling line ID is not set.

Examples of where the CLID would not be available include internal calls and calls on trunks that do not provide ANI or CLID.

Regardless of whether the PG fills in the CLID for post-routed calls, it always passes the origination address in call variable 1 and the origination address type in call variable 2. This allows script writers to reference this information if they can find a use for it.

Table 7 lists the possible values for the origination address type field (passed as call variable 2).

Table 7: Origination Address Types

Type	Value (Hex)	Description	Example	Used for CLID?
Unknown	00	This conforms to the ISDN Number Type Standards. This is also used as a default in all messages that contain a DN type field (applies to ISDN and non-ISDN)		No
International	01	This conforms to the ISDN Number Type Standards (ISDN only). This type is used for an international call.	01144...	Yes
National	02	This conforms to the ISDN Number Type Standards (ISDN only). This type is used for a national call.	4159422399	Yes
Special Number	03	This conforms to the SL-1 implementation of ISDN Number Type Standards (ISDN only). This type is used for special cases.		No
Subscriber Number	04	This conforms to the ISDN Number Type Standards (ISDN only). This type is used for calls within a particular area code.	9402399	No
Location Code Call	05	This conforms to the SL-1 implementation of ISDN Number Type Standards (ISDN only). This type is used for calls with a specific location expressed as 3 digits plus the remainder of the number.	6462399	No

(continued)

Type	Value (Hex)	Description	Example	Used for CLID?
Coordinated Dialing Plan	06	This conforms to the SL-1 implementation of ISDN Number Type Standards (ISDN only). This type is used when two or more switches coordinate to have the same dialing plan.	7771234	No
Internal	08	This type is used when a DN is internal to the SL-1.	2399	No
Route/Member	09	This type is only used for the Origination Address or Other Device DN IEs when a call is coming over a trunk that does not provide ANI or CLID to the SL-1. The trunk (route) and member numbers are stored in the address digits field.	720F01	No
Route only (NACD - Network ACD)	0A	Network ACD. This type is only used for the Origination Address. This is used when a network ties more than one SL-1 switch together. The trunk (route) of the originator is stored in the address digits field. This type is not used with an ISDN (ANI) trunk.	720	No
Attendant/Member.	0B	Attendant/Member. This type is only used for the Origination Address or Other Device DN IEs when an attendant originates a call. The attendant and member numbers are stored in the address digits field.	123F45	No
ACD DN/ ACD Position	0C	This type is only used for the Origination Address or Other Device DN IEs when an ACD agent initiates a transfer or conference. The ACD DN and position are stored in the address digits field.	8900F5001	No
In-Band ANI	0F	This type is only used for the origination address of an In-Band ANI call. The number of the calling party is stored in the address digits field.	4159402399	Yes
CDN	16	This message is used in the Origination Address of the RouteRequest message.	6800	No
CDN/DNIS	17	This message is used in the Origination Address of the RouteRequest message.	6800F1234	No

5.2. Caller Entered Digits (CED)

The Meridian Link Host Enhanced Routing interface does not provide any facility for Caller Entered Digits (CED). Therefore, calls post-routed through the Meridian PG will not provide CED to the *CallRouter*. The

ability to collect digits and play Meridian Mail voice files, which is supported by the Meridian Link Host Enhanced Voice Processing interface, **is not** supported by the Meridian PG.

5.3. Routing Client State

There are slight differences in the way the routing clients operate on the non-enhanced and Enhanced CTI mode PIMs:

5.3.1. Non-Enhanced Mode PIM

The routing client portion of the Meridian PG operates through a CTI link (that is, the Meridian Link), which is separate from the MEI link normally used for monitoring calls and agents (that is, MEI). As a result, it is possible for the PIM to be active and online, but for the routing client functionality to be unavailable (for example, if the Meridian Link processor is down).

In order to make it possible for a script writer to detect this condition, the routing client state is communicated to the *CallRouter* through the first peripheral real time variable. If the PG is online, and this variable is set to 1, then the routing client is online. If this variable is set to 0, then the PG is offline. A routing script could interrogate this variable and, for example, not translation route to a peripheral whose routing client is offline

5.3.2. Enhanced CTI Mode PIM

In enhanced CTI mode, both the MEI and the Meridian Link are required for the PIM to be active and online. If Meridian Link is down, then the peripheral is considered off-line. The routing client state is still communicated to the *CallRouter* through the first peripheral real time variable, just as it is for non-enhanced mode PIM. However, in most cases, if the routing client is offline, then the peripheral is offline as well.

An exception to this is the case where successive routing client timeouts cause the PIM to declare the routing client temporarily offline. In this case, the Meridian Link may still be up, and the PIM may be active and online, but the routing client is offline.

5.4. Special Label Characters

The Meridian PG provides special label characters that can be used in labels to indicate different call treatments to the routing client.

5.4.1. Variable Substitution

In some cases, it may be convenient **not** to configure individual labels for each distinct destination to which post-routed calls can be routed. In these cases, special labels can be configured that instruct the routing client to read the destination for the call from one of the call variables which can be set by a script.

The syntax for this is the percent character % followed by the number of the call variable that contains the destination. For example, a label string of

%3 indicates to the routing client that the destination to which the call should be routed can be found in call variable number 3.

5.4.2. Comment Character: @

In some cases, it may be necessary to configure multiple labels that are functionally equivalent (that is, they send calls to the same destination). However, the ICM configuration tools require that label strings for a given routing client be unique. In these cases, the special character @ can be used in a label to indicate to the routing client that it should drop all characters from the comment character to the end of the label before returning the destination to the switch. For example, 5100 and 5100@ could both be configured as labels. If the Meridian routing client received either of these labels from the *CallRouter* it would return a destination of 5100 to the Meridian Link.

5.4.3. Internal Translation Route Character: ^

When configuring a translation route for a Meridian peripheral, you must configure labels for each routing client that will send calls to that translation route. For network routing clients, these labels indicate to the network that the call should be delivered to the peripheral with a specific translation route DNIS.

When the call arrives with the special DNIS, the PG knows to match it up with the data for that call sent by the call router to the PG. However, if a Meridian peripheral routing client wants to send calls to the translation route on the **same** peripheral, the Meridian routing client cannot actually cause the call to “reappear” on the local switch with a translation route DNIS.

In order to make the translation route work, the translation route label must indicate to the PIM that the call is being translation routed. One way to accomplish this is with a pool of CDNs, as described “Meridian Considerations,” later in this chapter. Another way is to configure special labels that use the internal translation route character (that is, ^).

For example, say that you are configuring a translation route for a Meridian peripheral. You configure ten peripheral targets with translation route DNIS values 1001 through 1010. For each network routing client you would configure ten labels, one for each translation route peripheral target. If the Meridian peripheral routing client also needs to send calls to its local translation route, you would then configure 10 labels for the Meridian routing client. The labels would be of the form ^1001 ^1002 ...

When one of these labels is returned to the Meridian PIM, it will strip off the ^ character and use the rest of the label as a DNIS value. The PIM will then process the call as if it had just arrived with that DNIS value. This is much more efficient than using a pool of CDNs for calls translation routed to the local peripheral. However there will still be some cases where a pool of CDNs is required, such as when a local VRU translation routes a call to the Meridian peripheral through an internal transfer.

5.5. Translation Routing

Translation routing is described in the *ICM Software Script Editor Guide*. A quick review is presented here with emphasis on implementing translation routing with Meridian switches. Note that the Translation Route Wizard now automates much of the actual ICM configuration work for translation routes.

5.5.1. Configuring Translation Routes

A translation route is a mechanism for sending a call to a destination and passing information along with the call. The call information is passed from the ICM *CallRouter* to the PG where the call is targeted.

A translation route is associated with a logical controller (that is, a PG). In the case of a VRU PG, a single translation route can be used to target calls to any of the peripherals (VRUs) associated with the PG. In the case of an ACD PG, a translation route is required for each peripheral (ACD) to which calls are to be targeted. This discussion focuses on configuring translation routes to target calls to the ACDs.

In order to translation route calls to an ACD, you must create a translation route as described above. If a single PG talks to multiple ACDs, then you must create one translation route for each target ACD. In order to use a translation route, you must configure one or more routes whose target is the translation route. For each of these routes you must then configure one peripheral target that points to the route. The DNIS values for the peripheral targets should be chosen from a range of values dedicated to translation routing.

For each routing client that must be able to send calls to a given translation route, you must configure a label for each peripheral target that is associated with the routes that are associated with the translation route. The label string should be set to whatever string will tell that routing client to send the call to that peripheral with the trunk group and DNIS specified in the peripheral target. ICM dialed numbers **must** also be configured for any CDNs to which calls are directed as part of a translation route.

5.5.2. Review of Translation Routing

- To send calls to an ACD through a translation route, configure one translation route for that peripheral and associate it with the logical controller for the PG for that peripheral.
- Decide how many calls can be targeted to this translation route and can be “pending” at any given point in time. “Pending” here means that the initial route request has been received from the initial routing client, but the call has not yet arrived at the target and been matched up by OPC. Once the call arrives at the ACD and is matched up by OPC, it is no longer “pending.” A typical maximum number of expected pending calls would be ten. Allocate ten unique “DNIS” values to be used only by this translation route.

- For each of the DNIS values allocated to the translation route, create a route and set the target of the route to be the translation route. Set the service of the route to be the “Translation Routing” service for the peripheral.
- For each of the routes created above, create a single peripheral target whose DNIS is set to one of the allocated DNIS values. The network trunk group can be set to any valid trunk group for the peripheral. Each peripheral target should target its corresponding route.
- For each of the peripheral targets created above, create labels for each routing client that will target calls to this translation route.

5.5.3. Meridian Considerations

The “DNIS” values allocated to translation routing for Meridian PGs can be real DNIS values or they can be CDNs. If the translation route will only be targeted by routing clients other than the local PG, then the DNIS values can be real DNIS values. In this case, a single CDN can be allocated on the switch for all calls arriving to the translation route.

However, if a Meridian PG routing client needs the ability to target calls to the translation route on the **local** switch, then the translation route DNIS values must actually be CDNs’. That is, you must allocate ten (for example) CDNs on the switch to receive calls sent to the translation route. The peripheral targets would set their DNIS fields to the CDN numbers. These CDNs would also need to be configured as dialed numbers for the PG routing client. This type of setup requires the use of more CDNs. However, it allows more flexibility.

With this type of translation route configuration, any routing client can direct calls to the translation route. For a network routing client to use this type of translation route it would need to be able to provision DNIS values that match the CDN pool allocated on the switch. The labels for this routing client would then instruct the network to send the call to the trunk group and DNIS (CDN) specified in the peripheral target.

Another way to configure translation routing to the local peripheral is by using the internal translation route label character (see “Internal Translation Route Character,” earlier in this chapter, for more information.

6. Meridian-Specific Interpretation of ICM Data

This chapter discusses principles to keep in mind when attempting to compare ICM database reporting elements to the reporting elements of the Meridian ACD.

6.1. Termination Call Detail Records

The Enhanced CTI mode allows you to configure the PIM to generate Termination_Call_Detail records based on Meridian Event Interface (MEI) events, Meridian Link events, or both.

See also: See Chapter 2 and Chapter 5 for more information on Enhanced CTI mode.

6.2. Method of Attributing Calls to Services

When an ACD call arrives at a Meridian ACD, the Meridian PG attempts to attribute the call to an ICM service using one of the following methods:

- If the directory number (ACD DN or CDN) to which the call is presented matches the peripheral number of a configured ICM service, then the PG attributes the call to that service.
- If no configured service matches the directory number, then the PG looks for a peripheral target whose trunk group and DNIS match the trunk group (Meridian Route) and DNIS for the call. If a matching peripheral target is found, and this peripheral target has an associated route, and the route, in turn, has an associated service, then the PG attributes the call to that service.
- If neither of the previous two methods yields a service, then the PG attributes the call to the service associated with the default route for the peripheral (if configured). Note that calls are attributed to the service corresponding to the directory number to which the call is originally presented.

If Meridian features such as “Night Call Forward,” “Basic Time Overflow,” “Enhanced Time Overflow,” or “Automatic Overflow” are used, they do not affect the ICM service to which the call is attributed. For example, if calls arrive at DN 1 and are overflowed to DN 2 through time overflow, the calls will be attributed to the ICM service corresponding to DN 1. If the calls are ultimately answered by agents in DN 2 they will be attributed to the ICM skill group corresponding to DN 2.

An ACD call is **always** attributed to the original service to which it is presented. If a call is ultimately handled by another DN as the result of any of the Meridian overflow techniques, this does not affect the service to which the ICM attributes the call (though it does affect the skill group, see “Method of Attributing Calls to Skill Groups”).

If a call is answered and then transferred to an ACD DN or CDN, the Meridian PG tracks the second call as an independent call to the destination service.

6.3. Method of Attributing Calls to Skill Groups

The Meridian PG attributes answered calls to the ICM skill group that corresponds to the ACD DN in which the agent answered the call. Thus, if a call is originally presented to DN 1 but answered by an agent in DN 2

through some overflow feature, then the ICM service for DN 1 and the ICM skill group for DN 2 will reflect this call.

6.4. Calculation of Handle Time

The ICM defines handle time for a call as “the time an agent spends talking on a call and performing related after-call work.” The Meridian allows an agent to go into “Not Ready” state to perform after-call work but does not directly support the concept of attributing after-call work time to an individual call.

Since it is possible to activate the “Not Ready” key at any time, there is no guarantee that simply dividing the total “Not Ready” time by the number of calls answered will yield a useful number for per-call after-call work time.

The Meridian PG attributes “Not Ready” time to individual calls if the agent enters the “Not Ready” state directly after handling a call and before the “Available Holdoff Delay” period (set to the Flexible Call Force Timer for the ACD-DN) has elapsed. If the agent enters the “Not Ready” state during this time interval, then the Handle Time for the call (and for the service) will include the time spent in the “Not Ready” state.

Note that all time in the Meridian “Not Ready” state is also accounted for in the ICM skill group wrap-up time statistics.

6.5. Handling of CCR Route To Treatment

When a call to a CDN is given the “Route To” treatment by a CCR script, the call is removed from the CDN. When this occurs, the PG receives no more information about the call and stops monitoring it. The call is removed from real time calls in queue statistics. The disposition in the Termination_Call_Detail record is set to “Redirected.” The call is reflected in historical services records as an “Overflow Out” call.

If the call is routed to another CDN or ACD DN on the same switch then this will be tracked by the PG as a new call.

6.6. Handling of CCR Force Busy Treatment

When a call to a CDN is given the “Force Busy” treatment by a CCR script, the call is removed from the CDN. When this occurs, the PG receives no more information about the call and stops monitoring it. The call is removed from the real-time calls in queue statistics. The disposition in the Termination_Call_Detail record is set to “Forced Busy.” The call is reflected in the historical services records as a “Terminated Other” call.

6.7. Handling of CCR Force Disconnect Treatment

When a call to a CDN is given the “Force Disconnect” treatment by a CCR script, the call is removed from the CDN. When this occurs, the PG receives no more information about the call and stops monitoring it. The call is removed from the real-time calls in queue statistics. The disposition in the Termination_Call_Detail record is set to “Disconnect Drop No

Answer.” The call is reflected in the historical service records as a “Terminated Other” call.

6.8. Handling of CCR Give IVR/Transfer

When a call to a CDN is given the “Give IVR” treatment by a CCR script, and the call is transferred from the IVR, the call is removed from the CDN. When this occurs, the PG receives no more information about the call and stops monitoring it. The call is removed from the real-time calls in queue statistics. The disposition in the Termination_Call_Detail record is set to “Redirected.” The call is reflected in the historical service records as an “Overflow Out” call.

6.9. Subset of Trunk Data Supported

Only a subset of the trunk group data reported by the ICM is populated for Meridian trunk groups. Table 8 and Table 9 list the data elements that are supported.

Table 8: Trunk Group Real-Time Data Elements

Field Name	Supported on Meridian PG?
AllTrunksBusyHalf	YES
AllTrunksBusyToday	YES
CallsAbandonedHalf	YES
CallsAbandonedToday	YES
CallsInHalf	YES
CallsInNow	YES
CallsInToday	YES
CallsOutHalf	NO
CallsOutToday	NO
InServiceTimeHalf	NO
InServiceTimeToday	NO
InUseInboundTimeHalf	YES
InUseInboundTimeToday	YES
InUseOutboundTimeHalf	NO
InUseOutboundTimeToday	NO
TrunksIdle	NO
TrunksInService	NO

Table 9: Trunk Group Half Hour Data Elements

Field Name	Supported on Meridian PG?
CallsAbandonedToHalf	YES
CallsInToHalf	YES
TrunksInService	NO
CallsOutToHalf	NO
AllTrunksBusyToHalf	YES
InServiceTimeToHalf	NO
TrunksIdle	NO
InUseInboundTimeToHalf	YES
InUseOutboundTimeToday	NO

6.10. Calls Arriving at a Meridian Trunk and then Post-Routed

Calls that arrive at a Meridian on a trunk and are then post-routed are not associated with the trunk group on which they arrived. This means, for example, that the data element “CallsInToHalf” in the Trunk_Group_Half_Hour record would not reflect the calls that arrived on that trunk group that were post-routed. It also means that Termination_Call_Detail records for post-routed calls do not contain the trunk number on which the call arrived.

Note: If you run in Enhanced CTI mode, and configure the Meridian route access code (ACOD) as the ICM Trunk Group Extension, and calls arrive without ANI and are post-routed, then these calls will be associated with the trunk group on which they arrive.

6.11. Monitoring of Outbound Calls on Agent's DN Key

In ICM releases prior to 2.0 the Meridian PG pegs agents with an active DN call as "Talking Other" and accounts for their time as "TalkOtherTime." No distinction is made between inbound and outbound DN calls and no call counts are kept.

Starting with ICM 2.0, the Meridian PG provides more metrics for calls made and received on an agent's DN key. The skill group fields AgentOutCalls and AgentOutCallsTime provide the number of outbound DN calls and the time spent on outbound DN calls respectively. When an agent is active on an outbound DN call the agent is now pegged as "Talking Out" and his time is accounted for as "TalkOutTime." The skill group fields "InternalCalls" and "InternalCallsTime" provide the number of inbound DN calls answered and the time spent on inbound DN calls, respectively. When an agent is active on an inbound DN call the agent is now pegged as "Talking Other" and his time is accounted for as "TalkOtherTime."

7. Media Blender Configuration for Nortel Meridian

This chapter discusses what you need to know and do to configure the Cisco Media Blender for use with the Nortel Meridian ACD.

7.1. Media Blender Integration with the ICM system software

Media Blender software is integrated with ICM software and the ICM software routes calls through the Media Blender by means of the Cisco CTI Driver.

The Media Blender provides support for IPCC and legacy ACDs, including the Nortel Meridian, using the Cisco CTI driver. A new firewall gateway service allows CCS (Cisco Collaboration Server), which resides outside a firewall, to communicate with the ICM Peripheral Gateway(s) that reside inside the firewall. An example of a FirewallGatewayService.properties file is shown later in this document.

7.2. Key Property Files

You need to edit or check the following Media Blender property files:

Blender.Properties

ACD.ciscocti.properties

Collaboration.properties (copied from CCS)

Phantoms.properties

<Connection_CMB>.properties (copied from CCS)

Service.FWGW.properties

FirewallGateway.properties

Resource.properties

The following two of these files are connection property files that you need to copy from the collaboration **CCS** (Cisco Collaboration Server) system to the **CMB** (Cisco Media Blender) system:

Collaboration.properties

<Connection_CMB>.properties

The appropriate directory paths to copy from and to are listed below under the associated property file names.

Note: As a user, you name the <Connection_CMB>.properties file. By doing so, you can create a meaningful name for the site; for example, a name containing the names of the machines that are linked.

7.2.1. Blender.Properties

In the CiscoMB\Servlet\Properties\Blender**blender.properties** file, configure the following two properties as follows. This means that you uncomment the two lines setting these properties in the property file:

medium1=ACD.ciscocti.properties

Required. The Medium1 property identifies the property file for the ACD medium used with the Media Blender. **Note** that this property file must reside in the same directory as `blender.properties`. The file used for the Nortel Meridian is `ACD.ciscocti.properties`.

medium2=Collaboration.properties

Required. The **Medium2** property identifies the property file for the call queuing medium and should be listed after `medium1`. **Note** that this property file must reside in the same directory as `blender.properties`. The file gets created by the Cisco Collaboration Server and needs to be copied to the Cisco Media Blender directory. See the separate section on the `Collaboration.properties` file for further information.

Verbose=8

Optional. Add the `verbose=8` entry to the property file if you want to enable more test related information in the blender logs

Service1=Service.jwgw.properties

Required. Uncomment `Service1` to enable Firewall Gateway Service.

7.2.2. ACD.ciscocti.properties

In the CiscoMB\Servlet\Properties\Blender**ACD.ciscocti.properties** file, edit or add the following property settings:

peripheral.type=Meridian

Required. Uncomment the line with the Meridian peripheral type.

peripheral.id=<insert here the peripheral ID, as defined in the ICM PG Explorer>

Required.

Example: `peripheral.id=5007`

peripheral.hostname=<insert here the host name for CTI Server for this peripheral>

Required. This is the peripheral name or the Agent PG's IP address to the peripheral.

Example: `peripheral.hostname=m2pg10a`

peripheral.hostport=<insert here the host port of CTI Server for this peripheral>

Required. This can be obtained from the process window title bar of the CTI Server connected to the Agent PG.

Example: peripheral.hostport=42027

peripheral.hostname2=

This is the name of the backup peripheral that connections to the media blender

Optional.

Example: peripheral.hostname2=m2pg10b

peripheral.hostport2=

This is the backup port connection between the media blender and the peripheral.

Optional.

Example: peripheral.hostport2=43027

peripheral.username =<insert here the peripheral user name>

Required.

Example: peripheral.username=cmb-m2cmb3

peripheral.password= (if there is no password, you can leave this blank)

Optional.

Example: peripheral.password=

peripheral.comment= /*<Enter optional comments here>*/

Optional.

Example:

peripheral.comment=/* m2cmb3 is attached to a Meridian ACD via M2PG8a */

phantompool=phantoms.properties

Required if you are using any phantom strategies.

The name of the file that contains the list of phantoms. This file must be used if you are using phantom strategies.

autoanswer=true

Optional.

Set this to true so that the Media Blender answers Media Blender-controlled incoming calls for the agent. There is no need for the agent to answer the agent's phone.

readyaftersignon=true

Required.

Set this to true to place an agent in the ready state after auto-login.

Ignoreareacode=<insert here the area code that you want ignored. You can also include the exchange that you want to have ignored>

Optional. However, it must be set if you want the area code or part of the phone number ignored. This setting is used for internal testing with the next property so that calls can be routed by their last digits only.

Example: Ignoreareacode=978322

Permittedphonenumlength=<insert here the phone digits>

Optional. However, this setting must be used if you are using the Ignoreareacode property. This specifies the number of digits, beginning with the last one that is used to route a number. Do not use commas to separate number length options. Use spaces to separate the numbers. The following example says that the system will route calls by 10, 5, or 4 digits.

Example: Permittedphonenumlength=10 5 4

7.2.3. Collaboration.properties

This properties file is created by the Collaboration Server. You need to manually copy the **Collaboration.properties** file from the collaboration **CCS** (Cisco Collaboration Server) system to the **CMB** (Cisco Media Blender) system.

The directory paths to copy from and to are as follows:

From:

<CCS_dir>\servlet\properties\cmb\connection_name\blender\collaboration.properties

To:

<Cisco_MB_directory>\servlet\properties\blender\collaboration.properties

7.2.4. Phantoms.properties

In the CiscoMB\Servlet\Properties\Blender**phantoms.properties** file, add or edit the ID list of all your phantom agents and their types. You can use the agent's ID or the agent's extension number as an ID. D=DIGITAL is the only valid type. Use the format **ID_number=D**.

Required.

Example: 5584=D
5583=D

7.2.5. <Connection_CMB>.properties

This properties file is created by the Collaboration Server but named by you when configuring the Collaboration server for the media blender. For instance, the name you give to this properties file can include the two machines it connects.

You need to manually copy the <**Connection_CMB**>.properties file from the collaboration **CCS** Cisco Collaboration Server system to the Cisco Media Blender system.

The directory paths to copy from and to are:

From:
<CCS_dir>\servlet\properties\cmb\conn_name\<Connection_CMB>.properties
To:
<CMB_dir>\servlet\properties\<Connection_CMB>.properties

An Example <Connection_CMB>.properties File

```
## -----##  
  
## RMI Properties ##  
## -----##  
conn6_cmb.rmi.Name=conn6_cmb  
conn6_cmb.rmi.RemoteHost=m2ccs6  
conn6_cmb.rmi.RemoteRegistryPort=1099  
conn6_cmb.rmi.RemotePassword={enc:2}Zm9v  
conn6_cmb.rmi.LocalRegistryPort=1099  
conn6_cmb.rmi.LocalPassword={enc:2}Zm9v  
conn6_cmb.rmi.Description=  
conn6_cmb.rmi.DisableAutoConnect=false  
conn6_cmb.rmi.PollingHeartbeatCount=2  
conn6_cmb.rmi.ConnectionAttempts=1
```

Note: The **HOSTS** file in the system32/drivers/etc directory should contain the host and IP address mappings for all the machines involved with RMI Firewall Gateway connections.

Verify and/or add entries as necessary on the CCS and CMB machines.

7.2.6. Service.FWGW.properties

In the CiscoMB\Servlet\Properties\Blender**service.FWGW.properties** file, set autostart to **true** for the Firewall Gateway service.

Required.

Example: **autostart=true**

7.2.7. FirewallGateway.properties

The FirewallGateway.properties file is stored in the CiscoMB\Servlet\Properties directory. The following is an example FirewallGateway.properties file. The property values in bold are examples. You need to replace the bold text with the correct values for your system's configuration.

NOTE: If there is only a primary CTI Server host, either comment out the **backup** server or use the same information as the primary. If you do not do this, the cmb.log file will fill an 1800 K file, 3 files per minute!

```
#####
# FirewallGateway.properties #
#####

#-----
#- Agent Reporting and Management (ARM) section
#-----

# Set the value of this property to false if there is no ARM
#connection
FirewallGateway.ARM.active=true

# Edit <Connection_CMB> in the following properties
FirewallGateway.ARM.LocalService=conn6_cmb_CMB_ARM
FirewallGateway.ARM.RemoteService=conn6_cmb_CCS_ARM
FirewallGateway.ARM.RMIProps=conn6_cmb.properties

# Edit <PrimaryHostname> and <BackupHostname> in the following
#properties
FirewallGateway.ARM.plugin.param.primaryCtiServerHostname=m1pg4a
(or IP address)
FirewallGateway.ARM.plugin.param.backupCtiServerHostname=m1pg4b
(or IP address) * use the same info as for the primary
connection OR just comment the line out (#)

# Edit <PrimaryServerPort> and <BackupServerPort> in the
#following properties
FirewallGateway.ARM.plugin.param.primaryCtiServerPort=42027
FirewallGateway.ARM.plugin.param.backupCtiServerPort=43027

# Do not edit the following properties
FirewallGateway.ARM.ACKType=ACK_ALL
FirewallGateway.ARM.ACKMaxDelay=5000
FirewallGateway.ARM.flushOnDisconnect=false
FirewallGateway.ARM.plugin.messageSpecsFile=CCSGED188ARMDefs.xml
FirewallGateway.ARM.plugin.class=com.cisco.msg.plugin.socket.CTI
ServerPlugin
FirewallGateway.ARM.plugin.param.topicCreator=com.cisco.ics.ccs.
bus.ICMCcsTopicCreator
FirewallGateway.ARM.plugin.param.waitForApplication=10
```

```
#-----  
#- Media Routing (MR) section - Primary  
#-----  
  
# Set the value of this property to false if there is no MR  
connection  
FirewallGateway.MR_Primary.active=true  
# Edit <Connection_CMB> in the following properties  
FirewallGateway.MR_Primary.LocalService=conn6_cmb_CMB_MRI  
FirewallGateway.MR_Primary.RemoteService=conn6_cmb_CCS_MRI  
FirewallGateway.MR_Primary.RMIProps=conn6_cmb.properties  
  
# Edit <Port> in the following property  
FirewallGateway.MR_Primary.plugin.param.port=2000  
  
# Do not edit the following properties  
FirewallGateway.MR_Primary.ACKType=ACK_ALL  
FirewallGateway.MR_Primary.ACKMaxDelay=5000  
FirewallGateway.MR_Primary.flushOnDisconnect=false  
FirewallGateway.MR_Primary.plugin.messageSpecsFile=MR.xml  
FirewallGateway.MR_Primary.plugin.class=com.cisco.msg.plugin.sock  
et.MediaRoutingPIMPlugin  
FirewallGateway.MR_Primary.plugin.param.waitForApplication=10  
  
#-----  
#- Media Routing (MR) section - Backup  
#-----  
  
# Set the value of this property to false if there is no backup  
MR connection  
FirewallGateway.MR_Backup.active=true  
  
# If the preceding property line is false, you can disregard the  
following Edit lines  
# and comment out the next 3 lines.  
# Edit <Connection_CMB> in the following properties  
FirewallGateway.MR_Backup.LocalService=conn6_cmb_CMB_MRI  
FirewallGateway.MR_Backup.RemoteService=conn6_cmb_CCS_MRI  
FirewallGateway.MR_Backup.RMIProps=conn6_cmb.properties  
  
# Edit <Port> in the following property  
FirewallGateway.MR_Backup.plugin.param.port=2000
```

```
# Do not edit the following properties
FirewallGateway.MR_Backup.ACKType=ACK_ALL
FirewallGateway.MR_Backup.ACKMaxDelay=5000
FirewallGateway.MR_Backup.flushOnDisconnect=false
FirewallGateway.MR_Backup.plugin.messageSpecsFile=MR.xml
FirewallGateway.MR_Backup.plugin.class=com.cisco.msg.plugin.socket.MediaRoutingPIMPlugin
FirewallGateway.MR_Backup.plugin.param.waitForApplication=10
```

7.2.8. Resource.Properties

The Resource.properties file is located in the C:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec Data\default directory. This file allows you to add a user name by which you can log into Media Blender.

Example Resource.Properties File

Note: Before doing the following, you need to **create** the user “qaadmin” through Microsoft Windows (Go to Programs → Administrative Tools → Computer Management. When the Computer Management window displays, select System Tools, then Local Users and Groups. Right click on the Users directory to add a new user. Make the new user a member of “Administrator”.) Then **restart** the Blender IIS Admin and WWW services.

The following example adds the user **qaadmin** to login as Blender Administrator:

```
Blender.groups=
Blender.users=Administrator, qaadmin
BlenderNew.groups=
BlenderNew.users=Administrator, qaadmin
wlPageCompile.groups=
wlPageCompile.users=Administrator, qaadmin
```

7.3. Voice and Chat CTI Call Strategies

The available CTI strategies are designed to provide appropriate callback in different configurations and for different call strategies.

7.3.1. Voice Call Strategies

The following two CTI strategies can be used with voice calls.

PhantomWaitRelease

Media Blender dials into a queue using one of the phantom lines. Once the agent answers, the phantom line is placed on hold while Media Blender places an outbound call to the caller using the agent’s second line. Once the caller answers the phone, the phantom line is released.

PhantomWaitNoRelease

This strategy is similar to PhantomWaitRelease except the phantom line that stays connected to the agent for the length of the call. This approach provides a more detailed agent handle time reporting from the ACD, but it requires a larger pool of phantom lines. **One phantom** line is allowed for each caller.

7.3.2. Chat Session Strategies

The following three CTI strategies can be used for chat sessions. Note that when a chat session is active, the agent's phone is unavailable.

PhantomNoCallRelease

Use this strategy if you want to provide chat sessions and if your ACD is configured to place agents in a busy state as soon as their phones disconnect. This strategy connects to an agent but releases the phantom line immediately. The agent is placed in a busy state, allowing the agent and caller to engage in a text chat session uninterrupted.

PhantomNoCallNoRelease

Use this strategy if you want to provide chat sessions and if your ACD does not support the automatic busying out of agents. Media Blender uses the phantom line to select the agent; however, the phantom does not release the agent's phone until the session is complete. This provides more accurate reporting, but requires a larger pool of phantom lines.

PhantomNoCallNoHold

This strategy is similar to the PhantomNoCallNoRelease strategy except the call from the phantom line to the agent is not placed in the hold state. Rather it remains in the talking state. For reporting purposes, this strategy has the ACD report that the agent is talking while using chat.

7.3.3. CTI Strategies for Nortel Meridian

Nortel Meridian is supported with ICM CTI Server for ICM integration on Windows 2000. The following table lists the CTI strategies that can be used for the Nortel Meridian supported by the basic Media Blender configuration:

```
PhantomWaitRelease
PhantomWaitNoRelease
PhantomNoCallRelease
PhantomNoCallNoRelease
PhantomNoCallNoHold
```

7.3.4. Routing Address and Routing Numbers

When a callback request comes in, Media Blender retrieves the routing address from the callback form and matches it to the ACD routing number. The ACD then routes the request to the appropriate agent.

The **Routing Address** is a code embedded in the Blender Callback HTML form used by the caller. The Routing Address is set in a hidden field, RoutingAddr, on the Callback form. Cisco provides a sample callback form (`<CCS dir>/pub/html/forms/callFormACD.html`) that the CCS administrator can use to create the callback form for your site.

The **Routing number** is equal to a value unique to the CDN routing number logic on the Nortel Meridian.

See a switch administrator to obtain appropriate routing numbers. In most cases, it will be necessary to create a new routing number, such as CDN, on the switch for use with the Collaboration Server application. Refer to the *Cisco Media Blender Switch Administration Guide* and consult a switch administrator for more information

7.4. Configuring the Meridian Switch

Configure your agents, skill groups, services, and any phantom phones.

Skill group: Create the skill group in the ICM Configuration Manager. When doing so, you **must** also create the **Meridian Position** on the Peripheral Monitoring tab within the Configuration Manager’s PG Explorer by **adding** the agent ids and instrument numbers.

For example: 5571 – 5574;5581 – 5584

An Example Skill Group Configuration on a Nortel Meridian

TYPE	ACD	OBTN	NO	RAGT	4
CUST	0	RAO	NO	DURT	30
ACDN	5054	CWTH	1	RSND	4
MWC	NO	NCWL	NO	FCTH	20
DSAC	NO	BYTH	0	CROS	100
MAXP	20	OVTH	2047		
SDNB	NO	TOFT	NONE		
BSCW	NO	HPO	NO		
ISAP	YES	OCN	NO		
VSID	1	OVDN			
AACO	NO	IFDN			
RGAI	NO	OVBU	LNK LNK LNK LNK		
ACAA	NO	EMRT			
FRRT	MURT				
SRRT		RTPC	NO		
NRRT		HOML	YES		
FROA	NO	RDNA	NO		
FNCF	NO	ACNT			
FORC	NO	NRAC	NO		
RTQT	0	DAL	NO		
SPCP	YES	RPRT	YES		

Service: Configure the service when you configure the PG.

Phantom phones: Use any available phones. Do not just log in.

Example Configuration Settings on the Nortel Meridian ACD

```
Meridian link: merlink
Server port: 3000
Link Host Name: Lanlink
Link Machine Name: SL16
Blender Application name: m2cmb3
CCS Application name: m2ccs3
```

Example Configuration Settings on the MEI (MAX Event Interface) Server

```
PG: m2pg8a
MRPG: m2pg1a PIM 6
Peripheral ID: 5037
MeiServer: geolabntrgra
port: 44444
```

7.5. Testing the Meridian Switch

7.5.1. Create a CCS Agent for the Nortel Meridian Switch

1. Log into the **Cisco Collaboration Server Admin** workstation.
2. Click **Agents > Create**. Then click **Next**.
3. Enter the agent's **login name** (first and last name) and password. Then enter the voice agent's ID and press **Next**.
4. Leave **ICM Routing** as the default and click **Apply**.
5. If you select the **Terminal ID**, the physical phone extension for agent creation, then the agent will automatically be logged into the same terminal all the time and cannot switch terminals by using the "ACD Blended Login" form in the CCS.

NOTE:

- You have to use the instrument ID of the phones instead of the phone extension.
For example: Agent LoginID: 5571
 Terminal: 5571
- If you want the agents to be able to select the "allow agent to change terminals" option when they log in, then you cannot enter a specific terminal ID. If you do not select this option, it will restrict you to only that terminal; so you are required to enter a terminal ID.

See the *About Settings for Blended Collaboration Agents* sub section in the *Collaboration Agents* section in the *Cisco Collaboration Server Administrator Guide* for more information.

6. Enter the **Meridian ACD Password** if required. Otherwise, leave it blank for any Agent ID.
7. Enter the assigned **skill group number**. For example: #5560

NOTE: When you place a call, use the extension # (for example: 5582, 5581, 4501) and not the instrument #.

7.5.2. Log in a Blended Collaboration Agent on a Meridian Phone

1. Access the **//CCS-Host-Server/**
2. Click on the **'ACD Blended Login, Change Terminals'** link
3. Enter the agent's **login name** and **password**.
For example: meridian5571, weblines.
4. Enter the **Terminal ID** in the Terminal # field.
For example: 5571, 5572, 5573 or 5574.
5. Click **LOGIN**.

The Cisco Collaboration Server Single Session Chat user interface should show the Agent as logged into the Blended Collaboration user interface.

Note: You can make an agent not ready by pressing the **Not Ready** button.

7.5.3. Make a Blended Collaboration Caller Request to a Meridian Agent/Phone

1. **Agent:** Access the **//CCS-Host-Server/**
2. **Agent:** Access the **'Blended ACD caller.'** To do so, enter the Caller's First and Last name.
3. **Agent:** Enter the **Caller's Phone Number**. For example: 978 322-4501 or 978 322-4502. Always use the extension number of the Meridian phone for the caller's phone number.
4. **Agent:** Enter the **Script Number** for making a blended collaboration call: For example: Meridian_DN, where DN is the dialed number label name used in the ICM Configuration Manager.

The Agent's phone will light up at the instrument button (the bottom right button). This means the phantom phone is being used.

The Caller's phone will ring and light at the Extension button.

5. **Caller:** Presses the Caller's **Extension** button.

The Agent and Caller will now be connected through the phones AND in an active session through Collaboration.

7.5.4. Log In an Agent on a Nortel Meridian Phone

1. Press the **Skill Group/Instrument** button. This is the bottom right button.
2. Enter the agent's extension number.
3. Press the pound (#) button 3 times to login.

NOTE: The agent's extension is usually 10 or sometimes 1000 greater than the instrument number. So if the button shows '5000/5203', then the agent's extension number is 5213 or 6203. You can also login an agent using the skill group to which the agent is assigned.

To Logout: press the **Make Ready** button twice.

7.5.5. Place a Call on a Nortel Meridian Phone

1. **Calling Agent:** Presses **Extension** button.
2. **Calling Agent:** Enters the receiving agent's 4-digit extension number.
The receiving agent's phone rings.
3. **Receiving Agent:** Presses the **Extension** button on receiving agent's phone.

The agents are now talking.

NOTE: Press the **Release** button to hang up the call. (The Release button is the upper left, small red button.)

7.5.6. Transfer a Call on a Nortel Meridian Phone

1. Execute **LOGIN** and place a call (see the preceding "Place a call..." steps).
2. **Calling Agent:** Presses the **Transfer** button.
3. **Calling Agent:** Enters the agent's 4-digit extension to whom the call is to be transferred.
Receiving agent's phone rings.
4. **Receiving Agent:** Presses the receiving agent's **Extension** button.
5. **Calling Agent:** Presses the **Transfer** button again.

Receiving agent and caller are now talking.

NOTE: The Originating Agent is no longer connected with the call. The call is transferred either BLIND or by the receiving agent answering the call.

7.5.7. Place a Conference Call on a Nortel Meridian Phone

1. Execute **LOGIN** and place a call (see the preceding “Place a call...” steps).
2. **Calling Agent:** Presses the **Conference** button (It is the button just above the Extension button.).
3. **Calling Agent:** Enters the agent’s 4-digit extension to whom the call is to be conferenced.
The Receiving agent’s phone rings.
4. **Receiving Agent:** Presses the receiving agent’s **Extension** button.
5. **Calling Agent:** Presses the Conference button again.

Both agents and the caller are now talking.

NOTE: Both agents must press the red **RLS** (Release) button to hang up the conference call.

7.6. Glossary

ACD

Automatic Call Distributor. Also called a switch, an ACD is a specialized phone system designed for handling incoming and outgoing calls.

ACD Medium

The ACD medium on the Cisco Media Blender handles CTI messages coming from an ACD.

Agent

An individual who receives and handles customer calls and web-based requests within a call center.

BAPI (Blender Application Programming Interface)

The CCS BAPI interface connects to a Cisco Media Blender remote medium.

Blended Collaboration

In the basic Media Blender integration, a blended collaboration session is one that is blended with the ACD. Blended Collaboration sessions typically begin when a caller submits a Web-based request by clicking

a callback button on a web page. The caller completes a callback form and Collaboration Server retrieves caller information (name, phone number, skill group). Media Blender then blends the information over to the ACD, which provides a callback to the customer. The customer and agent talk on the phone and are linked in a collaborative Web session.

Blended collaboration in the ICM integration is provided when the agent is assigned by the ICM (when using IPCC) or by the ACD (when using a legacy ACD). When the ICM software selects an agent for the task, the Web collaboration interface appears on the agent desktop. At the same time, the agent's telephone places an outbound call to the customer.

Callback Button

A button placed on a web site used by the caller to initiate a blended Collaboration session.

Callback page

A form sent to the caller to retrieve caller information, such as name, telephone number, and skill group.

Caller

An individual submitting a phone call or web-based request to a call center.

Call Manager

The Cisco Call Manager (CCM) is a computer platform that provides traditional PBX telephony features and functions to packet telephony devices such as Cisco IP phones and Voice over IP (VoIP) gateways. The Call Manager also supports supplementary and enhanced services such as hold, transfer, forward, conference, automatic route selection, speed dial, and last number redial.

CCT

Call Control Table. A table located in a switch, such as the Aspect, that determines the call characteristics for routing purposes.

Central Controller

The computer or computers running the ICM CallRouter and the ICM Database Manager. In addition to routing calls, the Central Controller maintains a database of data collected by the Peripheral Gateways (PGs) and data that the Central Controller has accumulated about the calls it has routed.

Collaboration Medium

The Collaboration medium communicates with the Cisco Collaboration Server (CCS) and accepts and shares session and agent-related events with the other CMB media.

Collaboration Server

The Cisco Collaboration Server (CCS) is an application that provides contact centers with the ability to handle Web requests. CCS allows contact center agents to share information with customers over the Web—including Web pages, forms, and applications—while at the same time conducting a voice conversation or text chat using nothing more than a common Web browser.

CTI

Computer Telephony Integration. A term for connecting a computer to a telephone switch. The computer issues telephone switch commands to move the calls around.

CTI Driver

Software designed to accommodate the CTI package and middleware used in a Media Blender configuration. The CTI driver supports the legacy ACDs when Media Blender is a part of the ICM integration.

CTI strategy

Software that determines the call flow of the outbound call to the caller.

Driver

A module that controls data transferred to and received from peripheral devices.

Firewall Gateway Service

The Media Blender firewall gateway service allows Collaboration Server, which resides outside a firewall, to communicate with an ICM peripheral gateway that resides inside the firewall.

Intelligent Contact Management (ICM) software

The Cisco system that implements enterprise-wide call distribution across call centers. ICM software provides Pre-Routing®, Post-Routing®, and performance monitoring capabilities.

Interactive Voice Response (IVR)

A telecommunications computer, also called a Voice Response Unit (VRU), that responds to caller entered touch-tone digits. The IVR responds to caller entered digits in much the same way that a conventional computer responds to keystrokes or a click of the mouse. The IVR uses a digitized voice to read menu selections to the caller. The caller then enters the touch-tone digits that correspond to the desired menu selection. The caller entered digits can invoke options as varied as looking up account balances, moving the call within or to another ACD, or playing a pre-recorded announcement for the caller.

JRMP

Java Remote Message Protocol. The wire-level protocol to transport RMI calls and objects.

Legacy ACD

Any of the following ACDs supported in the ICM integration that uses the Cisco CTI driver:

- Avaya (Lucent) Definity ECS G3
- Aspect CallCenter
- Nortel Meridian 1
- Nortel Symposium
- NEC NEAX 2400
- Rockwell Spectrum
- Siemens Hicom 300E

Media Blender Administrator

An individual responsible for installing, configuring, and administering Media Blender.

Media Routing Domain

The Media Routing Domain (MRD) is a collection of skill groups and services that are associated with a common communication medium. ICM software uses a MRD to route a task to an agent who is associated with a skill group and a particular medium. MRDs are assigned in the ICM configuration and have unique IDs across the enterprise.

Media Routing Peripheral Gateway (MR PG)

An ICM PG that is capable of routing media requests of different kinds; for example, email and Web callback. An MR PG supports multiple media routing clients by placing multiple, independent Peripheral Interface Managers (PIMs) on a PG platform.

Medium

An electronic form of session-based information. Media Blender functions as an event bus and shares events between participating media. In a typical installation, Media Blender shares events between a Collaboration medium and an ACD medium.

Peripheral Gateway (PG)

The computer and process within the ICM system that communicates directly with the ACD, PBX, or IVR at the call center. The Peripheral Gateway reads status information from the peripheral and sends it to the Central Controller. In a private network configuration, the Peripheral Gateway sends routing requests to the Central Controller and receives routing information in return.

Peripheral Interface Manager (PIM)

The Cisco proprietary interface between a peripheral and the Peripheral Gateway (PG).

Phantom Line

Phone lines set aside for providing callback to customers. Used with Phantom line CTI strategies, phantom lines wait in queue on behalf of the caller, ensuring the caller receives callback only when an agent is available.

PhantomLoginThreshold (property)

The minimum percentage of phantom agents, configured in a phantom pool that should get logged in to the phones. Default is 100%.
phantomloginthreshold=<1-100>.

Only %1 out of %2 phantoms are logged in and is less than the phantom login threshold (%3 percent). Current configuration of Cisco Media Blender requires a minimum number of phantoms to login successfully. This is determined by the phantomloginthreshold property in ACD.ciscocti.properties file. Testing covered in the Dev. ACD Unit Test Plan.

Unavailability of phantom phones might affect the performance of the Cisco Media Blender. Make sure the phantoms are configured properly in the property files. Logout any agents already logged into the phantom phones. Restart Media Blender if problem happens during startup.

Phantom Strategy

A CTI strategy that places a call in the ACD queue and waits for call assignment (agent selection). Once the agent is selected, the outbound call is placed to the customer.

PBX

Private Branch eXchange, a smaller version of the phone company's larger central switching office.

RMI

Remote Method Invocation. A remote procedure mechanism for communicating between two Java programs within (potentially) separate Java Virtual Machines.

Routing Logic

Logic set up on the ACD to ensure calls are routed to agents who possess appropriate skills.

Routing Script

A script that ICM software executes to find the destination for a call. A routing script might examine information about several possible targets before choosing the best destination. You can schedule different scripts to execute for different types of calls and at different times and dates. Use the Script Editor to create, modify, and schedule routing scripts.

Switch

An Automatic Call Distributor (ACD) or PBX.

Switch Administrator

An individual responsible for ACD administration. The switch administrator must work with the Media Blender Administrator to ensure proper communication between Media Blender and the ACD.

Web Administrator

An individual responsible for creating and maintaining HTML pages and forms as they relate to Media Blender.

Web Callback

A feature of the Cisco Collaboration Server (CCS) that allows a customer to use a "call me" button on a company's Web site. The resulting callback request is handled by either an ACD (for Basic Media Blender) or the ICM software (for Media Blender in the ICM integration). Web callback, sometimes referred to as "callback only," is for simple callbacks that do not involve blended Web collaboration or blended text chat.

Index

- Symbol**
- @ common character, 61
 - ^ internal translation route character, 61
 - <Connection_CMB>.properties, 75
- A**
- ACD
 - configuration, 23
 - interface requirements, 14
 - restrictions, 21, 26
 - software requirements, 18
 - ACD.ciscocti.properties, 73
 - Agent
 - configuration, 51
 - ID, 52
 - mapping, 51
 - states, 52
 - Agent states, 52
 - Aspect
 - agent states, 52
 - Attributing calls to routes, 44
- B**
- Blender.Properties, 73
- C**
- Call Control Variable Map field, 42
 - Call event messages
 - monitoring of, 33
 - Caller Entered Digits (CED), 59
 - Calling Line ID (CLID), 58
 - Cisco Media Blender
 - configuring for Meridian, 71
 - Collaboration.properties, 75
- Common character (@), 61
 - Configure ICM tool, 39
 - CTI Client, 42
- D**
- Dialed number
 - configuration, 53
 - Duplexed MEI Servers, 36
 - Duplexed PGs, 14
- E**
- Enhanced CTI mode, 17
 - configuration, 33
 - Enhanced CTI Mode
 - ACD requirements, 24
 - Enhanced CTI requirements, 20
- F**
- FirewallGateway.properties, 76
- H**
- High-Speed Link, 17
- I**
- ICM feature support, 21
 - ICM Setup tool, 29
 - ICM software configuration, 39
 - Internal translation route
 - character (^), 61
- L**
- Label
 - configuration, 54
- M**
- MAX requirements, 18
 - MEI Server software, 17, 34

- adding to a PG, 37
- configurations, 35
- ICM Setup, 37
- limitations, 37
- sample configuration, 34
- MEI setting in ICM Setup, 30
- Meridian 1 requirements, 24
- Meridian Link
 - configuration in ICM Setup, 31
- Meridian Link capacity, 26
- Meridian Link External Processor, 15
- Meridian mail, 26
- Meridian MEI requirements, 24
- Meridian Switch
 - testing, 82
- Meridian-specific ICM Setup, 30
- Modes of operation, 17

O

- Origination address types, 58

P

- Peripheral configuration, 40
- Peripheral Interface Manager (PIM), 42
- Peripheral monitor
 - configuration, 54
- Peripheral target
 - configuration options, 45
- Peripheral target configuration, 44
- Phantoms.properties, 75
- Post-Routing, 57
- Post-Routing requirements, 19

- Property Files, 72

R

- Remote PG configuration, 16
- Resource.Properties, 79
- Route
 - configuration, 53
- Routing client
 - configuration, 53
 - operation of, 60

S

- Service
 - configuration, 48
 - member mapping, 51
- Service.FWGW.properties, 76
- Skill group, 47, 50
 - configuration, 50
 - members, 52
 - priorities, 51
- Special label characters, 60

T

- Termination call detail options, 33
- Translation routes
 - configuring, 62
- Translation routing, 62
 - considerations, 63
 - review of, 62
- Trunk groups
 - configuring, 47
- Trunks
 - configuring, 48