Cisco Unified ICM ACD Supplement for Avaya Communication Manager, Release 12.5(1) and 12.5(2)

First Published: 2020-02-05

Last Modified: 2022-07-26

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

CONTENTS

PREFACE

Preface vii

Change History vii

About this Guide vii

Audience viii

Related Documents viii

Field Notice viii

Communications, Services, and Additional Information ix

Conventions ix

CHAPTER 1

Overview 1

Cisco Unified ICM PG and Avaya ACD 1

Avaya ACD Interface Requirements 1

Avaya ACD with CVLAN/TSAPI Service running on Avaya AES 2

Call Management System (CMS) 3

Avaya “CMS-less” Interface 4

Busy Hour Call Rates for Ethernet CTI Link 5

Hardware and Software Requirements 6

Supported Unified ICM Software Features 7

CHAPTER 2

ACD Configuration 9

Monitored VDNs and Inbound ACD Calls 9

Monitored Splits on CMS 10

Terminal Endpoint Identifier (TEI) Values 10

Configuring AES 10

Setting up the CVLAN and TSAPI Links on AES Server 10

Setting up Hunt Groups/Skill Groups 14

Defining a Hunt Group/Skill Group for Agents 14
Modifying the Agent Login ID 15
Setting up Call Routing 16
Create a Vector Directory Number 18
Configuring Return Destination VDN on Avaya Switch 18
Ethernet Busy Hour Call Rates 19
Post-Routing, Station Monitoring, Third-Party Call Control 20
Active Association Limit 20
Maximum Agent and BHCA 20
Call Handling Methods to Avoid 21
Universal Call ID 21
CVLAN Link Configuration 21
CMS Cisco Real-Time Report 22
CMS Minimum Refresh Rate 23
Configuring the CMS Report 23
Avaya Configuration for "CMS-less" PGs 23
ACD Notes and Restrictions 24
Multiple PGs 25
Dual PG Setup 26
Maintaining Your Configuration 27
Configuring High Availability CMS 27

CHAPTER 3 **Unified ICM Software Configuration** 29
Peripheral Configuration 30
Peripheral Skill Group Mask 30
Peripheral Call Control Variable Map 30
Peripheral Configuration Parameters 31
Peripheral Targets 34
Configuring VDN and Hunt Group Extensions as Peripheral Targets 34
Peripheral Monitor Table 35
Monitoring Stations 35
VDN Timed ACW Settings 35
Configuring the Return Destination VDN on Unified ICM 36
PIM Configuration 36

Connection management with AES using TSAPI Interface 39
Installing TSAPI Client 40
Service Observer 40
Trunk Groups 40
Trunks 41
Services 41
Skill Groups 42
Skill Group Subgroups 42
Using Skill Group Priorities without Configuring Sub-Skill Groups 44
Available Hold Off Delay 45
Service-to-Skill Group Mappings 45
Agents 45
Agent States 46
Skill Group Members 48
Translation Routes 48
Routes 48
Routing Client 48
Unified ICM Configuration for “CMS-less” PGs 48
Maintaining Your Configuration 49
Registry Keys 49

CHAPTER 4 **CVLAN to TSAPI Migration** 51
Migration Overview 51
Important Considerations for Migration 51
Migrating CVLAN Interface to TSAPI Interface 52
Trace Bits to Troubleshoot TSAPI PG Issues 53

CHAPTER 5 **Post-Routing** 55
Post Route Dial Number Registration for TSAPI Interface 55
Route Request 55
Route Request Elements 55
Route Request Peripheral Variable Usage 56
Call Control Variable Map 56
Route Select 57

Route Select Message 58
Restrictions on Digit Collection 58
Route Select Peripheral Variable Usage 59
Digit Collection/Dial Ahead 59
Trunk Access Code 60
User-user Information 60
Label Syntax 60
Network Take-Back and Transfer Support 62

Preface

- Change History, on page vii
- About this Guide, on page vii
- Audience, on page viii
- Related Documents, on page viii
- Field Notice, on page viii
- Communications, Services, and Additional Information, on page ix
- Conventions, on page ix

Change History

This table lists and links to changes made to this guide and gives the dates those changes were made. Earliest changes appear in the bottom rows.

Change	See	Date
Document updated for MR Release 12.5(2)		July 2022
Added the Release number-12.5(2) to the title		
Added a new section for Network Take-Back and Transfer Support	Network Take-Back and Transfer Support	
Added a new chapter that has details about migrating your existing Avaya PGs from the CVLAN interface to the TSAPI interface.	CVLAN to TSAPI Migration	
Initial Release of Document for Release 12.5(1)		February 2020

About this Guide

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

While the other Unified ICM documents cover general topics such as configuring an overall Unified ICM system and writing scripts to route contact center requests, this document provides specific information on configuring an Avaya PG and making any necessary adjustments to the Avaya ACD configuration.

Audience

This document is intended for Unified ICM system managers. The reader understands the Unified ICM functions as described in the following documents:

- *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*
- *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*

The reader should also have specific knowledge about the Avaya and CMS systems.

Related Documents

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

- *Administration Guide for Cisco Unified Contact Center Enterprise*
- *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*
- *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise*
- *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*

For information on Cisco Network Applications Manager (NAM), see the *Product Description Guide* for Cisco Unified ICM Hosted.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

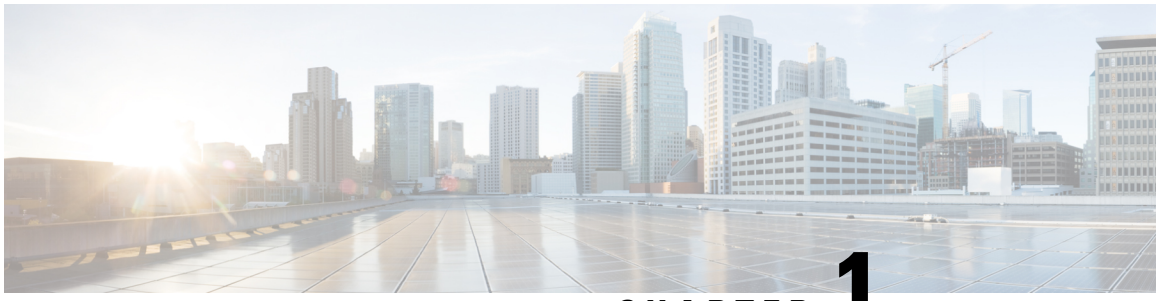
Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find** • Click **Finish**
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A skill group is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (condition,true-value, false-value) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
window font	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **<html><title>Cisco Systems, Inc. </title></html>**

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



CHAPTER 1

Overview

- Cisco Unified ICM PG and Avaya ACD, on page 1
- Avaya ACD Interface Requirements, on page 1
- Hardware and Software Requirements, on page 6

Cisco Unified ICM PG and Avaya ACD

The Cisco Unified Intelligent Contact Management (Unified ICM) Peripheral Gateway (PG) supports Avaya ACD using CVLAN or TSAPI Service, running on Avaya Application Enablement Services (AES).

CVLAN and TSAPI are Avaya software options that allow the Unified ICM PG to communicate with the Avaya ACD. Both CVLAN and TSAPI provide the PG with real time call events and allow the PG to query the ECS/MultiVantage/Avaya about splits, trunk groups, and agents.

CVLAN and TSAPI allow the PG to perform post-routing, station monitoring, and third-party call control.

The CVLAN and TSAPI software can be purchased from Avaya.

The *Call Management System (CMS)* is the Avaya ACD Management Information System (MIS). It provides the PG with real-time agent state data for non-station-monitored agents.

This chapter describes the options for connecting the Avaya ACD to the Unified ICM PG. To work with the system software, the Avaya ACD must meet several hardware and software requirements. This chapter lists the requirements for both CMS and non-CMS environments.

Note Avaya ACD is used across this document to represent the different names used by Avaya for their platform. Some of these names are Avaya Aura Communication Manager, Avaya Communication Manager, MultiVantage, Definity, and so on.

Avaya ACD Interface Requirements

A basic, simplexed Unified ICM PG has the following interface requirements:

- You must have at least one CVLAN / TSAPI link on the Avaya ACD. Up to eight CVLAN links can be supported for higher call loads.

- If CMS is used, the PG requires one Ethernet connection to the CMS system that is connected to the Avaya ACD.
- If CMS is used, the PG requires a Unified ICM Real-Time Adherence (RTA) custom report. This report is developed and provided by Avaya for the Unified ICM system.

Note A configuration without the CMS may be possible, subject to the restrictions listed in Avaya "CMS-less" Interface later in this chapter. If a "CMS-less" solution is possible, all references to CMS requirements in this document do not apply.

Related Topics

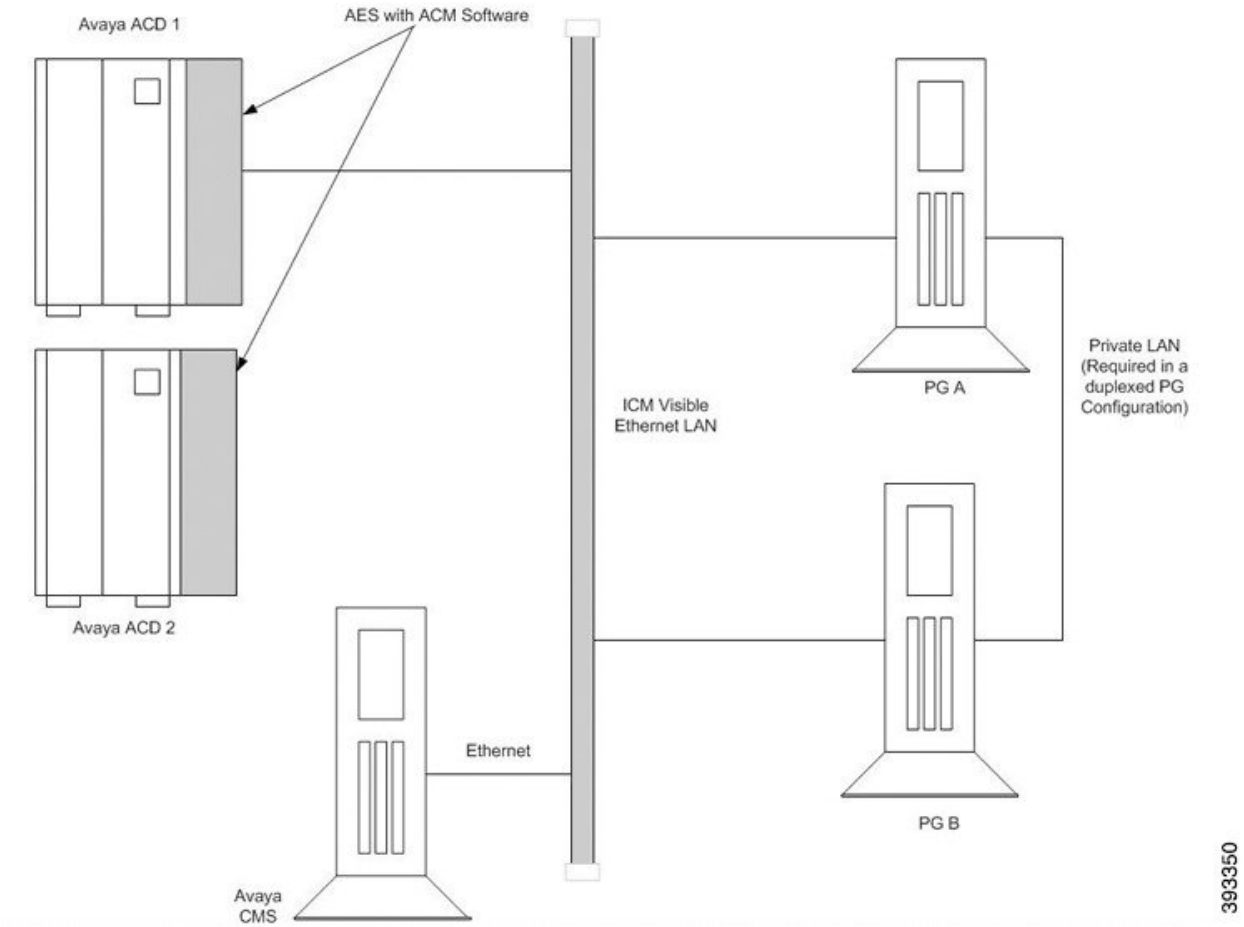
Avaya “CMS-less” Interface, on page 4

Avaya ACD with CVLAN/TSAPI Service running on Avaya AES

The AES interface allows the PG and Avaya ACD to communicate directly. In this configuration, CVLAN / TSAPI Service runs on Avaya AES software. The PG connects directly to the Avaya ACD through an Ethernet LAN. The PG acts as a client while the Avaya ACD acts as the server. An adjunct processor platform is not required in this configuration.

The following figure shows an example of AES interface with Avaya ACD.

Figure 1: Avaya ACD Interface



The CMS, if used, connects to Unified ICM visible LAN through a single Ethernet connection. A Cisco CMS custom report is installed on the CMS platform (one for each Peripheral Interface Manager).

The Avaya ACD Interface figure shows a two-ACD site. Some sites may have a single ACD only.

Install the PG and Avaya ACD on the same LAN.

For specifics on AES Server installation and SCO UNIX patch requirements, see the Configuring AES section.

Related Topics

Configuring AES, on page 10

Call Management System (CMS)

The Avaya CMS provides snapshots of the real-time agent login/logout and non-ACD-related agent state data to the PG through the CMS Ethernet connection. In configurations that use CMS, a custom report is required to ensure that real-time call and agent data is available to the system software.

CMS Report Versions

Avaya has Unified ICM RTA custom reports in Expert Agent Selection (EAS) and non-EAS versions. The Avaya CMS Professional Services Group installs the proper Unified ICM custom report (EAS or non-EAS) on the CMS. To support EAS, the custom report must have a major revision of at least 3 (for example: 3.x.x).

Single- and Multiple-PIM Configurations

One custom report must be installed on the CMS for each Peripheral Interface Manager (PIM) on the PG. A PIM is a system software module that allows communication between a peripheral and the PG. For example, if you have one Avaya ACD and a duplexed PG, each PG has one PIM. Therefore, the CMS requires two custom reports. If you have two ACDs and a duplexed PG, each PG has two PIMs. The CMS would therefore require four custom reports (two for each PG).

On a single Avaya ACD duplexed PG environment two CMS reports are installed. However, only one of the reports provide agent state data to the PG at any given time.

In other words, only one CMS report is running at any given time per Avaya ACD. From a resource utilization perspective on CMS, a single CMS report (when running) is equivalent to one more Supervisor running a real-time report.

For more information on CMS report requirements, see the CMS Cisco Real-Time Report section.

Note Customers who are using CMS with Unified ICM, over 1,000 agents/high call loads, may want to change certain ICM ACD PIM default settings. Changing settings may improve agent station visibility. But it can also cause a possible increase in message traffic to the Avaya ACD, switch CPU load, and network traffic between the PG and Central Controller (CC). Customers are supposed to work with the Cisco Content Security and Control (CSC) to evaluate and mitigate any possible issues. Cisco CSC must refer to internal documents on PIM registry configuration.

Related Topics

CMS Cisco Real-Time Report, on page 22

Avaya "CMS-less" Interface

ICM software support Avaya ACD configurations that do not use the Avaya CMS. Typically, this configuration is available only when agent count is less than 1,000 agents. However, the suitability of a CMS-less installation for a site may depend on several factors. This includes agent counts, **Busy Hour Call Rate** (BHCR), third-party activity, post-routing, and other **Avaya CTI** applications (if any).

Note If a CMS-less solution is used, all references to CMS requirements in this document do not apply.

In a CMS-less environment, both Unified ICM and Avaya ACD systems must meet more configuration requirements:

Additional Unified ICM Software Configuration

The following changes are possible using the Configure ICM tools.

- It is necessary for you to set all agents in the Unified ICM database.
- Map agents to skill groups in the Unified ICM database. The agent to-skill-group mapping must match the Avaya ACD configuration. In addition, the subgroup must correctly map to the agent's priority.
- It is essential for you to set monitored instruments in the Peripheral Monitor table of the Unified ICM database. Agent stations are to be monitored.
- Set up Peripheral Targets in the Unified ICM database for all Vector Directory Numbers (VDNs) through which monitored calls flow.

Additional Avaya Requirements

In a PG configuration that does not use CMS, additional configuration is necessary on Avaya.

- PG requires skill groups to be monitored to track agent login and logout events. No agents can log in to that skill group. if a skill group is not monitored. PG uses **3PDC** or **Monitor request API's** to monitor a skill group, based on the interface (CVLAN/TSAPI).

Avaya currently restricts one application to third-party domain control of a skill group.

- Enable **Event Minimization for the CVLAN CTI** links used by the **Peripheral Gateway.** This is not applicable when PG uses **TSAPI Interface** to connect to **AES**.
- Use the **EnterpriseCTI Interface** for optimal performance, external applications that alter agent state on the **Avaya ECS**.

Busy Hour Call Rates for Ethernet CTI Link

Each Avaya Ethernet CTI link can support a BHCR. This BHCR is of approximately 32,000 in normal use by the PG and excludes Post-Routing or third-party call control. This is an approximate value. This value are affected by following factors:

- The number of agents
- Anticipated peak busy hour call rate
- Average number of CTI events/calls
- Number of splits
- Trunk groups
- VDNs

Establish a dedicated Ethernet CTI link for Unified ICM application.

For more information on Ethernet BHCRs, see the Ethernet Busy Hour Call Rates section.

Related Topics

Ethernet Busy Hour Call Rates, on page 19

Hardware and Software Requirements

In order to work with Unified ICM software, the Avaya ACD must meet the hardware and software requirements listed in these tables.

Table 1: Avaya Requirements-With CMS

Releases Supported	Avaya ACD CVLAN and TSAPI. For specific release information on Avaya ACD, CVLAN and TSAPI see the *Cisco ICM Software Supported Switches (ACD)* document.
Features Required	Call Management System (CMS) For specific release information for CMS, see the *Cisco ICM Software Supported Switches (ACD)* document.
	Call Vectoring
	CTI Monitoring
	CTI Host-Based Routing (only for systems using Unified ICM Post-Routing)
	Cisco Unified ICM real-time adherence custom report (developed and provided by Avaya for Cisco). The CMS requires one report for each PIM in service on the PG.
Performance	CMS minimum refresh rate: 3 seconds

Table 2: Avaya ACD Requirements—"CMS-less"

Releases Supported	Avaya ACD CVLAN and TSAPI For more information on Avaya ACD, CVLAN and TSAPI support, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Features Required	Call Vectoring
	CTI Monitoring
	CTI Host-Based Routing (only for systems using Unified ICM Post-Routing)

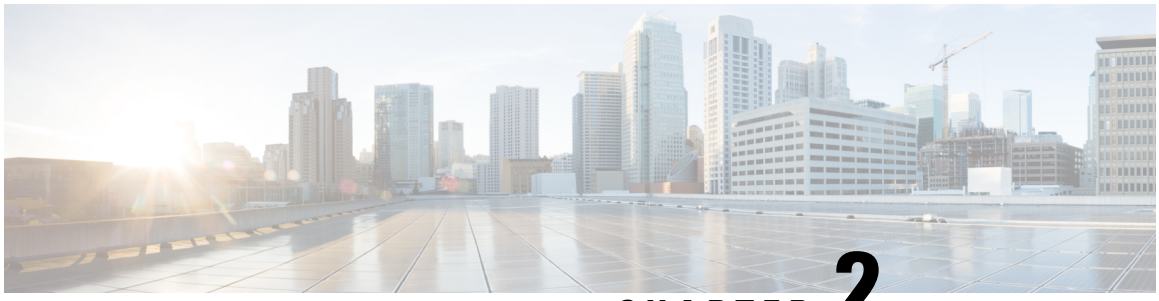
Supported Unified ICM Software Features

The Avaya PG supports the following Unified ICM software features:

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

Note

- The Avaya PG does not support Unified ICM integration with the Avaya ProLogix System.
- PIM supports a maximum of eight CTI links per CVLAN and a maximum of two CVLANs.



CHAPTER 2

ACD Configuration

No changes are required to the actual Avaya ACD configuration beyond the changes mentioned in the Chapter 1:**Avaya ACD Interface Requirements**. However, some ACD-specific settings must be confirmed. This chapter describes these settings and provides guidelines that help you maintain your Avaya ACD and Unified ICM configurations.

- Monitored VDNs and Inbound ACD Calls, on page 9
- Monitored Splits on CMS, on page 10
- Terminal Endpoint Identifier (TEI) Values, on page 10
- Configuring AES, on page 10
- Configuring Return Destination VDN on Avaya Switch, on page 18
- Ethernet Busy Hour Call Rates, on page 19
- Call Handling Methods to Avoid, on page 21
- Universal Call ID, on page 21
- CVLAN Link Configuration, on page 21
- CMS Cisco Real-Time Report, on page 22
- Avaya Configuration for “CMS-less” PGs, on page 23
- ACD Notes and Restrictions, on page 24
- Multiple PGs, on page 25
- Maintaining Your Configuration, on page 27
- Configuring High Availability CMS, on page 27

Monitored VDNs and Inbound ACD Calls

A monitored VDN handles all inbound ACD calls initially. It is important that all VDNS involved in ICM call flow are monitored to ensure that there are no stale calls. A monitored VDN is equivalent to a configured Unified ICM Peripheral Target. For example, **do not** specify a Hunt Group Extension as the destination for inbound ACD calls. Hunt Groups that are vector-controlled (which is true for all skill groups in an EAS environment) cannot be monitored for calls.

The inability to monitor vector-controlled hunt groups is a restriction imposed by Avaya. An unmonitored call that reaches a Hunt Group or Agent cannot be tracked and accounted properly in Unified ICM contact or agent statistics.

Important It is important that all VDNs to be monitored are properly configured as Peripheral Targets in the Unified ICM database.

Monitored Splits on CMS

The Avaya Hunt Group configuration screen for each monitored split on CMS must have its Measured field set to either "both" or "external." The field values are set in order for the CMS to receive Hunt Group (split) data.

Terminal Endpoint Identifier (TEI) Values

When you set up the Avaya ACD, the TEI value for an Avaya LAN or Avaya ACD is set to 1.

Configuring AES

Application Enablement Services (AES) software runs on an external server that communicates to Avaya Aura Communication Manager(or Avaya ACD) by using TCP/IP. It exposes a set of APIs that allow external applications like Cisco ICM to perform third-party call control and receive event notifications. The ICM PG uses either CVLAN or TSAPI link, which is a client/service software.

To best understand the configuration of the AES switch, begin with the Avaya documentation that shipped with your switch. The information provided here is meant to supplement but not replace the Avaya documentation.

We provide a limited amount of information to help you configure the switch to work with Cisco Avaya PG.

The following tasks are described:

- Setting Up the CV/LAN and TSAPI Links
- Setting Up Agents and Hunt Group
- Setting Up Call Routing

Related Topics

Setting up the CVLAN and TSAPI Links on AES Server, on page 10
Setting up Hunt Groups/Skill Groups, on page 14
Setting up Call Routing, on page 16

Setting up the CVLAN and TSAPI Links on AES Server

This section describes how to set up the **CVLAN** and **TSAPI** links on an **AES** server.

Perform the following procedure to establish the **CVLAN** link:

Procedure

Step 1 Open the **AES OAM** home page.

Step 2 Choose **AE Services** > **CVLAN** >**CVLAN**links.

Step 3 On the **CVLAN** Link administration screen, click **Add Link** and perform the following:

- Select the Signal
- Uncheck the **Proprietary** check box
- Select the **Switch** Connection
- Select the Switch **CTI** Link Number
- Select the **CTI** link version
- Check the **Heartbeat** check box

Step 4 Click **Apply Changes**.

Figure 2: CVLAN Link Setup Screen

Adding CTI Client IP for a CVLAN Link:

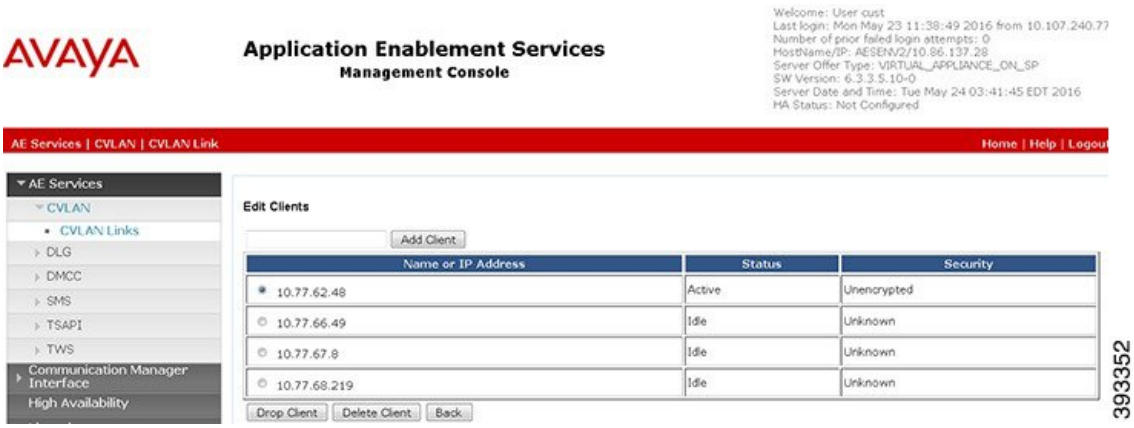
a. Open the **AES OAM** home page.

b. Choose **Administration** > **CTI Link Admin** > **CVLAN Links**.

c. Select the **CVLAN** link for which the client IP requires to be added and click **Edit Client**.

d. Enter the IP address and click **Add Client**.

Figure 3: Add CTI Client IP Screen



Follow the procedure to establish the TSAPI link:

a. Open the **AES OAM** home page.

b. Choose **AE Services** > **TSAPI** > **TSAPI** Links.

c. On the TSAPI Link administration screen, click **Add Link** and perform the following:

- Select the Link.
- Select the **ACM** (Avaya Communication Manager) to which you want to establish connection.
- Select the Switch **CTI Link** Number.
- Select the **ASAI** link version.

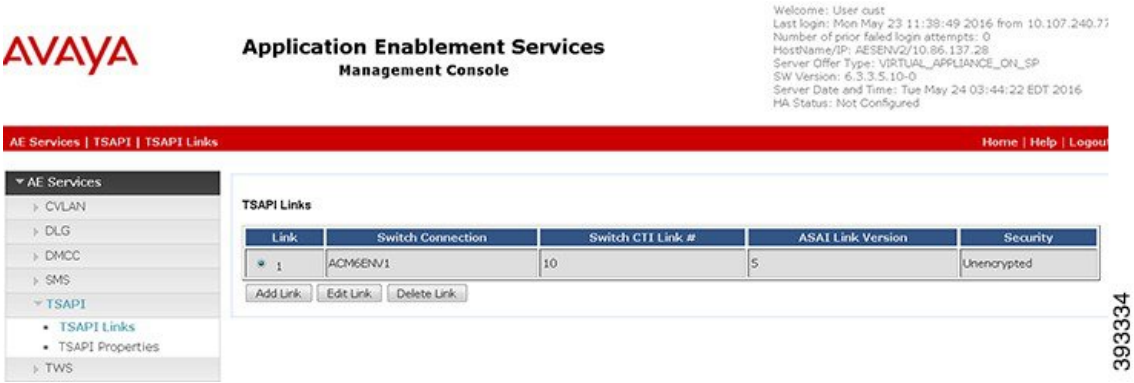
  Note The minimum link version for ASAI is 5.

- Select the security as **Unencrypted**.

  Note Currently security enabled TSAPI Link is not supported.

d. Click **Apply Changes**.

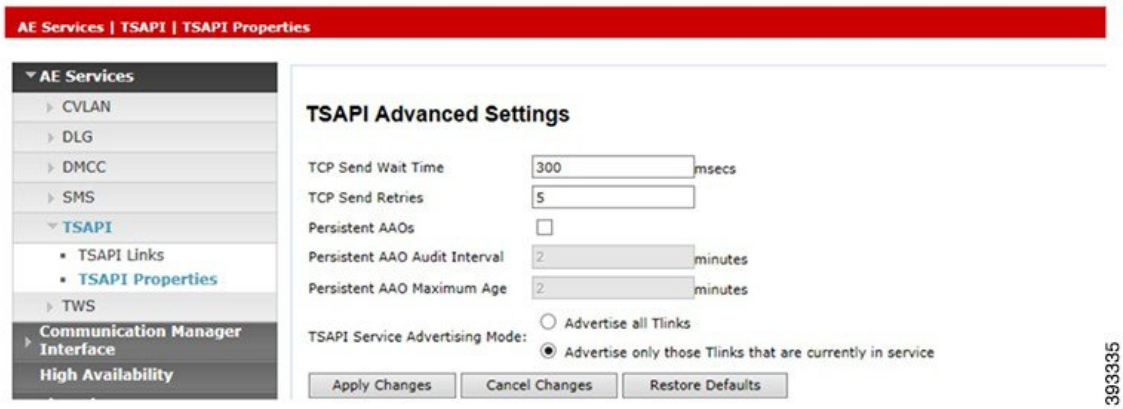
Figure 4: TSAPI Link Setup Screen



e. Select **AE Services** > **TSAPI** > **TSAPI** Links.

f. Go to the **TSAPI** Link Properties section. Click **Advanced Settings**.

Figure 5: TSAPI Advanced Settings



g. Select Advertise only those **Tlinks** that are currently in service option as TSAPI Service Advertising Mode.

Once the **Tlink** is created, navigate to the following path and note down the **Tlink** name. This is the name we use in **PIM configuration**.

1. Open the **AES OAM** home page.
2. Go to **Security**-> **Security Database**-> **Tlink** -> **Tlink Name**

Tlink Name for example:`AVAYA#CMSIM#CSTA#AESSIM`

This is applicable where,

- **AVAYA** is a fixed constant.
- Switch_Connection is a unique name, assigned to identify a switch (Communication Manager). In general, hostname of the switch is assigned as the name of Switch Connection in the **AE** Services server.
- Service Type: refers to the **CSTA** service type. It can be either of the following:
  - **CSTA** - For using unencrypted **TSAPI** Link (non-secure connection).
    - **CSTA-S** - For using encrypted **TSAPI** Link (secure connection).

      The **CSTA** versus **CSTA-S** service types specify whether encryption is used between the application and the **AE Services** server.

- **AE_Services_Server_Name** represents the hostname of the AE Services server which is assigned during the AE Services installation.

Adding CTI User in AES:

a. Open the**AES OAM** home page.
b. Go To **UserManagement** -> **User Admin** -> **Add User** Set the **CT** User option as "yes" and provide the remaining details as per Avaya documentation.

Note A **CTI** user is unique for each **PIM**, which gets connected to an **ACD**

Setting up Hunt Groups/Skill Groups

On the **Avaya** switch, a hunt group is a group of extensions to which similar calls are routed. A hunt group may include all agents who have a particular skill (for example, the ability to speak Spanish). It also includes all the agents who cover a geographical territory (for example, Boston sales). A hunt group is sometimes referred to as a skill group.

Note The Avaya PG (ECSPIM) supports extensions of up to ten digits – the agent can log in to a Softphone that has an extension up to ten digits. This ten-digit support applies to Agent Login IDs too. The Hunt Groups and VDNs support up to seven digits only.

In order to use a seven-digit, or ten digits, the config **PIM** registry **EnableTenDigitExtension** must be set to 1 in following path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\ICM\<cus01>\<PGXX>\PG\CurrentVersion\PIMS\pim1\ATTData\Config\
```

If the registry **EnableTenDigitExtension** is set to 0, then it limits support up to five digits for extension, Agent Login IDs, Hunt Groups, and VDNs.

Note By default, Avaya PG (TAESPIM) supports extensions of up to ten digits and this does not require registry configuration. The Agent Login IDs support up to ten digits.

Some **ACD** systems provide a feature called **EAS**. For various reasons, you want certain agents to handle specific types of calls. For example, you require only your most experienced agents to handle your most important customers. You have multilingual agents who can serve callers in various languages. **EAS** allows you to classify agents according to their specific skills and then to rank them by ability or experience within each skill. Avaya uses these classifications to match each call with the best available agent.

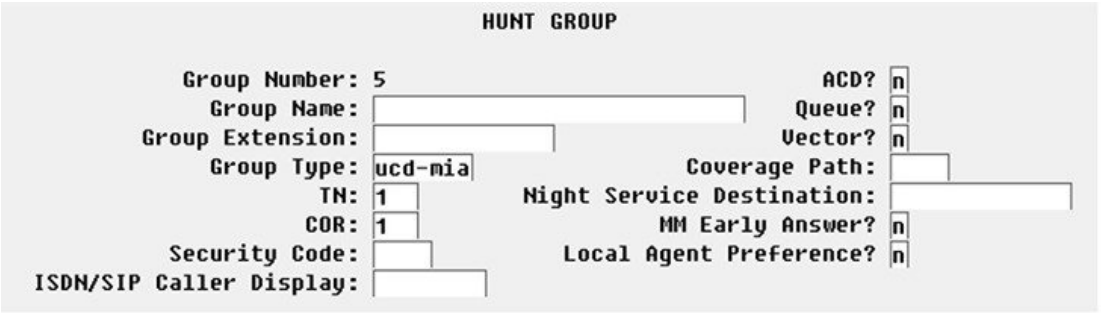
Defining a Hunt Group/Skill Group for Agents

To set up agents, you must define a hunt group by completing the following steps:

Procedure

Step 1 Enter the command **add hunt-group next** and press **Return**. (You can also enter **add hunt-group.xxx**, where .xxx is the hunt group number.) The first Hunt Group screen appears.

Figure 6: Defining Agent Hunt Groups



Step 2 Complete screens 1 through 2 of the hunt group record as described in the Avaya documentation.

Step 3 Press **Enter**. The hunt group is successfully created.

Modifying the Agent Login ID

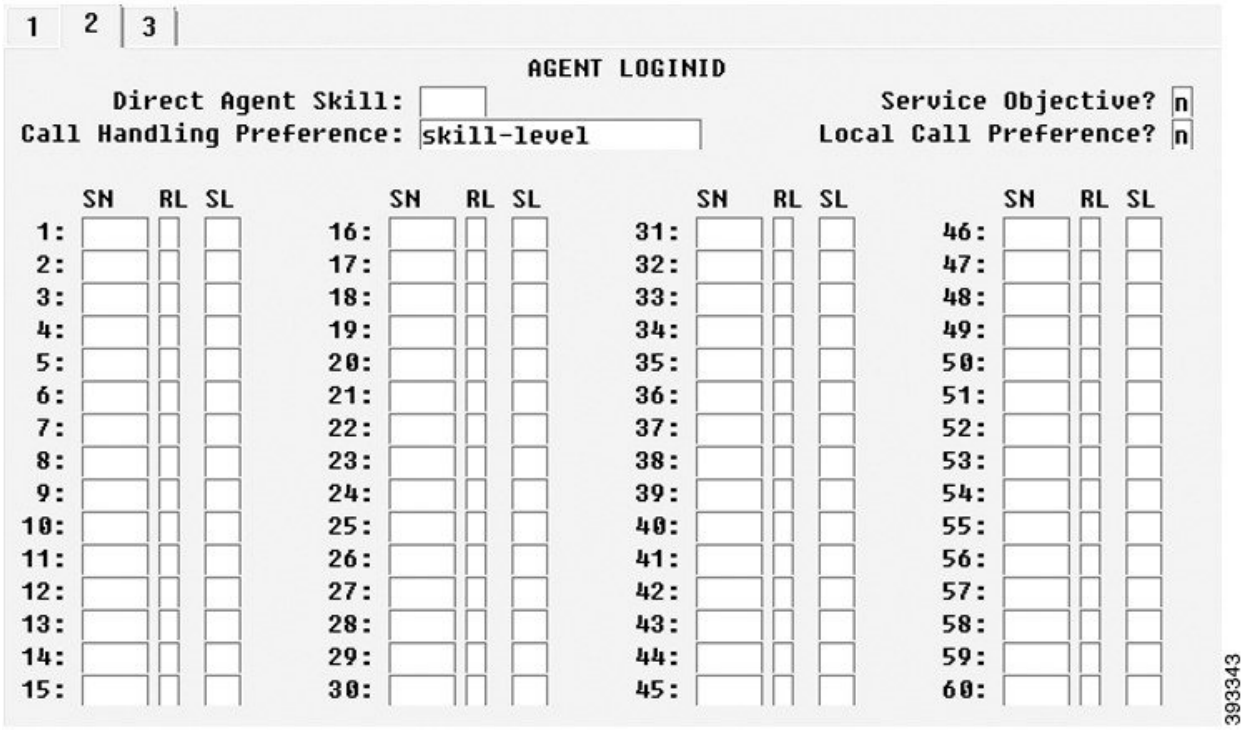
For each agent usingEnterprise Chat and Email, add the hunt group to the **Agent login ID** form.

To modify the **Agent login ID**, perform the following steps:

Procedure

Step 1 Enter the command change <**agent login ID number**>. The **Agent Login ID** screen appears.

Figure 7: Modifying Agent Login ID



Step 2 Add the **hunt group** that indicates **Unified CCE agents** in the **SN** (Skill Number) field in the table at the bottom of the screen.

Step 3 Complete the remaining fields as described in the **Avaya** documentation.

Setting up Call Routing

After you have set up your Enterprise Chat and Email agents and the phantom lines, ensure that the Avaya switch routes calls to them appropriately by:

- Writing a vector to route calls
- Creating a **VDN** to access the vector

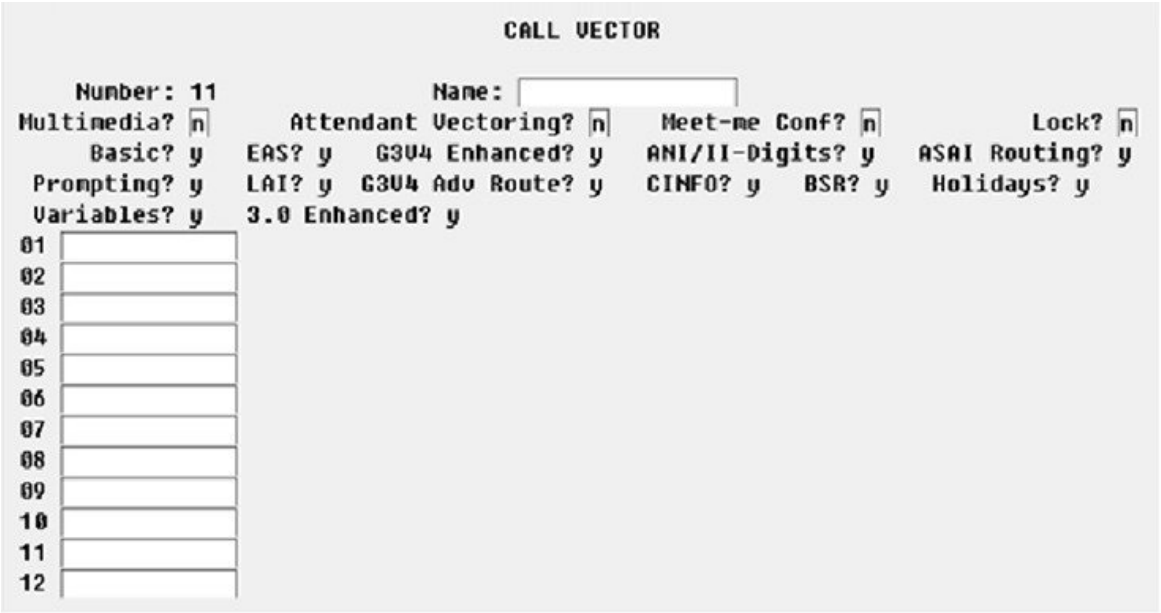
Write a Vector to Route Call

A vector is a set of instructions the switch follows to ensure that the right call gets to the right agent. Whether you use predictive or phantom **CTI** strategies, write a vector that routes appropriate incoming calls to an Enterprise Chat and Email agent hunt group. Write a vector for each group to which you want to route calls, and you require the hunt group number established for Enterprise Chat and Email agents when setting up a vector to route calls to those agents.

To create a vector:

1. Enter the command change vector xx (where xx is the vector number) and press Return. The Call Vector form appears.

Figure 8: Vector

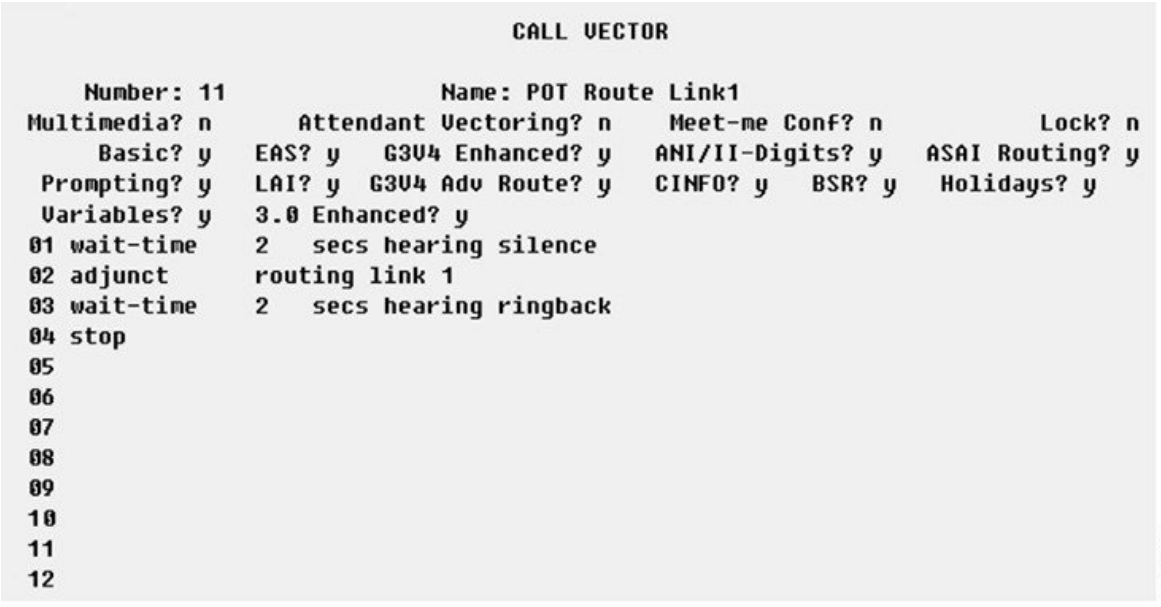


2. Complete the Call Vector screens 1 through 6. Instructions for completing these screens are provided in the Avaya documentation.

Example of a Post route Vector for a Call

Following is an example of a Post route call vector. This sends adjunct route request to the Unified CCE Avaya PG which is connected on routing link 1.

Figure 9: Call Vector



Create a Vector Directory Number

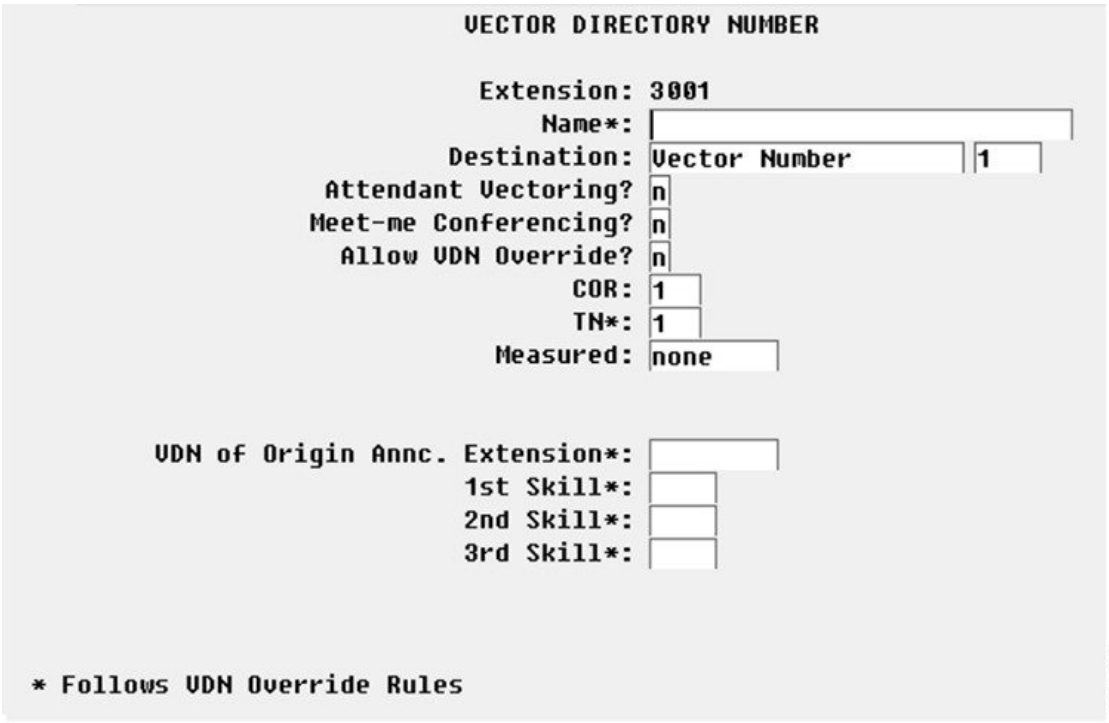
After setting up a vector for Enterprise Chat and Email calls, set up Vector Directory Numbers (VDNs) to direct incoming calls to that vector. You can create several VDNs that refer to the same vector, ensuring that calls from a variety of sources can be routed to the same skill group.

To create a VDN, complete the following steps:

Procedure

Step 1 Enter the command **add VDN.xxxx** (where *xxxx* indicates the VDN). The Vector Directory Number screen appears.

Figure 10: GUI for Vector Directory Number



Step 2 Complete the screens 1 through 3 based on the instructions in the Avaya documentation.

Configuring Return Destination VDN on Avaya Switch

The Return Destination automatically redirects a call from one monitored **VDN** to another **VDN** for continuous call processing, after an agent disconnects the call.

If the call flow involves two post-route **VDN**s, the call variables are preserved from the first route request to the second route request when call gets automatically redirected from a post-route **VDN** to another post-route

VDN for continued call processing (after an agent disconnects from the call). (This is according to the return destination feature enabled on Avaya ACD.)

If the call flow involves a first post-route **VDN** and then a non post-route VDN after return destination, the call variables are still preserved from the first call (post-route request) to the second call after return destination.

After return destination, the last agent also has the call variables which were set in the first call prior to return destination.

The Avaya PIM detects whether the return destination is configured on a VDN, by verifying the parameter string of that VDN in the Peripheral Monitor tab of the PG Explorer. The PIM then sends a **NEW_TRASACTION_IND** to **OPC**, allowing the OPC to preserve the call variables in the second route select.

For example:

1. VDN 32222 is the first post route VDN. VDN 32223 is the label returned for 32222. It is the **Return Destination** VDN as well.
2. After **Return Destination** occurs on VDN 32223, the call variables are preserved in the second post route. VDN 32224 is the **Post Route** VDN. It is configured as **Return Destination** VDN for VDN 32223 on Avaya Switch.

   When Agent on VDN 32223 drops the call, **Return Destination** occurs and call is redirected to VDN 32224. A NEW_TRANSACTION Indication is sent to OPC.

The **Return Destination** can be configured on the Avaya Switch. The following example explains the configuration of this feature:

Procedure

Step 1 Click Tab **1** on the VECTOR DIRECTORY NUMBER screen and set the following field:

a) Allow **VDN** Override: Set this field as **y**.

Step 2 Click **Tab 2** on the VECTOR DIRECTORY NUMBER screen to set the return destination VDN for 3606. Set the Return Destination field as 3001. This value is configured as return destination VDN for 3606. When an agent on VDN 3606 drops the call, it is automatically redirected to VDN 3001.

To set up **Return Destination VDN** on **Unified ICM**, see the section Configuring the Return Destination on Unified ICM

See the section ACD Notes and Restrictions for known caveats for Return Destination VDN.

Related Topics

Configuring the Return Destination VDN on Unified ICM, on page 36

Ethernet Busy Hour Call Rates

Each **Avaya Ethernet CTI** link can support a **BHCR** of approximately 32,000 in normal use by the **PG** (that is, without Post-*Routing* or third-party call control). This value is an approximation and may be affected by the number of agents, anticipated peak busy hour call rate, average number of **CTI** events/calls, and the number of splits, trunk groups, and **VDN**s. Provision a dedicated Ethernet **CTI** link for Unified **ICM** application.

Post-Routing, Station Monitoring, Third-Party Call Control

If Post-*Routing*, station monitoring, or third-party call control is performed on the same Ethernet CTI link, the link supports up to 20,000 BHCR due to additional message traffic. Depending on your configuration, you might need an additional Ethernet CTI link to be used exclusively for Post-*Routing*, station monitoring, or third-party call control.

An Ethernet CTI link dedicated exclusively to Post-*Routing* (that is, no event monitoring) can handle approximately 64,000 BHCR. Calculating throughputs for third-party use is dependent upon the number of stations involved and anticipated usage. In general, third-party usage on the CTI link uses some of the CTI bandwidth.

Active Association Limit

Active associations are used for all requests made of the switch. Some of the requests made of the switch remain open for an indefinite period of time (for example, event notification requests, monitoring VDNs). Other requests end when the switch returns the response (e.g., value query for time-of-day). The indefinite requests include VDN event monitoring, station monitoring, and skill group monitoring.

ASAI_TEST utility

ASAI_TEST is a utility that allows you to check the connectivity between Unified ICM PG and the Avaya ACD (Avaya ACD can include either Avaya ACD card or AES Server).

Before running the ASAI_TEST, ensure the IP connectivity between the PG and the Avaya ACD card. To do so, initiate a ping test from the PG to the Avaya ACD card. If the ping test passes, you can proceed with the ASAI_TEST.

To run ASAI_TEST, use this command syntax:

```
<Directory>:\icr\bin>asai_test
usage: asai_test [-m hostname/IP address] node_id
```

Note The node_id is also referred to as the CTI link number. The maximum number of CTI links can be 8.

Note The **Active Association Limit** is not applicable to **TAESPIM**.

Maximum Agent and BHCA

Unified ICM software (CC, PG, CTI server) currently supports 3000 Agents and 60000 BHCA.

Table 3: Unified ICM Compatibility for Maximum Agent and BHCA

Hardware, Software, and Tools	Software Component and Version
Unified ICM software	11.0
ACD Switch	Avaya 6.3 with CMS RTA 5.0.5 Std

Hardware, Software, and Tools	Software Component and Version
PG, CTI Server Configuration	For complete and current information on the PG Server Configuration, see the *Virtualization for Unified CCE*.

Call Handling Methods to Avoid

Following are the call handling methods you need to avoid:

1. Avoid setting up station coverage paths where all internal calls are marked to go to coverage.
2. Avoid having agents transfer calls directly to other agent stations or to other agent IDs. Instead, the calls can be transferred to a hunt group (or split). The calls can also be transferred to a VDN to ensure proper call monitoring.

Universal Call ID

If the **Avaya Universal Call ID** (UCID) is preferred. The field **Send UCID to ASAI** is set to **Yes**. You can do this through **Feature-Related System Parameters** form on the Avaya.

Starting with ICM 7.5(9), the Avaya PIM is enhanced to use **UCID** information from the Avaya Switch to clean up old calls in the **Avaya PIM**.

To enable the **UCID** feature on the **Avaya** Switch, change the following system-parameters features:

- Create Universal Call ID(UCID) ? **y**
- What is the value for UCID Network Node ID? **<any value_unique to a switch>**
- Is it necessary to send UCID to ASAI ? **y**

The UCID value is stored in the Unified CCE central database, in the Termination Call Detail table, in the CallReferenceID field. For more information, see the Database Schema Handbook for Cisco Unified Contact Center Enterprise.

CVLAN Link Configuration

CVLAN link configuration is set to have **Event Minimization** set to **Yes**. This is especially important if you are using third-party functionality.

To set Event Minimization to **Yes**:

1. Stop the PG.
2. Busy-out and release the CVLAN link. This activates this CVLAN link attribute.
3. Restart the PG.

When Event Minimization is enabled, the Unified ICM PG CVLAN links are dedicated to the PG (that is, no other applications are using those CVLAN links). In a duplexed environment, both PG sides can use the same CVLAN links.

CMS Cisco Real-Time Report

The guidelines in this chapter are intended for Avaya installers of the CMS Cisco RTA report:

- **Skillnums argument**: The **CMS** report uses the skillnums argument. The Unified **ICM PG** started supporting skillnums in Unified **ICM** software. Therefore, any installation of Unified **ICM** software uses **skillnums**. This applies to all the new installations and upgrades to **ICM** software.
- **Agent login**: For **CMS** report version 3.5 or later, the **PIM** does not log agents into a skill group unless the skill group is monitored by CMS. This is a requirement because **CMS** does not pass agent state data or logout events for non-monitored skill groups. The lack of this CMS data can cause agent count and agent state mismatches. Conversely, if the **CMS** report is a pre-3.5 version, the PIM still logs agents into all groups provided in the agent login event, but CMS does not provide logout events for the non-monitored skill groups.

Because no logout record (or any agent state record, for that matter) is provided by CMS for these non-monitored skills, and because the version of the **CMS** report is pre-3.5, the PIM may leave agents in their last state. For this reason, use a CMS report that is version 3.5 or later.

Note The **Avaya PG** currently supports 20 skills per agent. The enhanced RTA 5.0.5, which supports 60 skills per agent, is not supported by Unified **ICM**.

- **Noskillnum flag** Make sure that the noskillnum flag is set to skillnums (that is, CMS provides the list of monitored skills) in the following list of files. Split/Skill numbers need to be in the CMS startup header provided to the **PG**.

  The following files are impacted:

  - Startrta
  - testrta
  - skills1
  - skills2, and so on

These are files on the CMS machine.

- **Multiple CMS reports on one PIM** If multiple **CMS** reports are configured for a single **PIM** on a **PG**, the CMS report must use the timestamp argument. The timestamp argument causes the CMS report to include a UNIX timestamp in each of the records sent to the PG. The **PG** requires the timestamp to properly order the incoming **CMS** records from the multiple reports.
- **Agent-skill pairs** Upgrade to the newest **CMS** report if you find you need increased agent-skill pairs. The newer **CMS** reports can be configured to support up to 10,000 agent-skill pairs (default 2,400). Using this single (increased) agent-skill pair capability eliminates any need for using multiple CMS reports (and therefore not require timestamps in the CMS reports).

Note In later **CMS** reports, the arguments (for example, noskillnums) described above may have changed. Therefore, Avaya installers check for the correct arguments to achieve the desired functionality as described above.

CMS Minimum Refresh Rate

The CMS report is installed to run as an administrator in order to allow a minimum refresh rate of three seconds. It is necessary for you to ensure that the refresh rate used for the custom CMS report is allowed for an administrator CMS login. In addition, administer the CMS report via the appropriate login (for example, CMS). Using another login to administer the report does not work. The Avaya Professional Services group can provide the details on which login are used to administer the report.

If agents are being dynamically re-skilled (logged into and out of skill groups with some frequency), it is possible that the CMS report does not see an agent logout/login sequence for a skill group. For example, if the agent is logged into skill 1 and is logged out of and back into skill 1 within the CMS refresh rate period (that is, in between CMS snapshots of data), then CMS does not see this logout/login transition.

Dynamic re-skilling is supported only when the agent is in "Available" or "AUX" state. If the re-skilling is attempted for an agent who is in a state other than these states, then the reskill record is held by CMS until the agent state changes back to “Available” or “AUX” state.

Configuring the CMS Report

While configuring the CMS report the following data items are required:

- **ACD Number**: The ACD number is the Avaya ACD number as known to the CMS system.
- **Refresh Rate**: The refresh rate is the rate at which the report captures the agent data and pass it on to the PG. The minimum refresh rate is 3 seconds. A typical refresh rate is 10 seconds.
- **Splits to Monitor**: The splits to monitor are the ACD skill groups, that are required to be monitored by the PG. It is mandatory to update the list of CMS monitored splits periodically.
- **Avaya type**

  For example, Non-EAS or EAS.
- **PG LAN Information** This includes IP address, netmask, and hostname. The CMS and PG are usually on the same LAN. The PG LAN information is required by the Avaya Professional Services engineer to set up the CMS report, so that it is connected to the PG. After the initial installation, this is never changed.

Important If any of the above CMS information is changed (for example: Monitored splits or the refresh rate), the CMS report and PG **must** be stopped and restarted in order for the changes to take place.

Avaya Configuration for “CMS-less” PGs

In a PG configuration that does not use CMS, additional configuration is necessary on Avaya.

- PG requires skill groups to be monitored to track agent login and logout events. No agents can log in to that skill group. if a skill group is not monitored. PG uses **3PDC** or **Monitor request API**'s to monitor a skill group, based on the interface (CVLAN/TSAPI).

Avaya currently restricts one application to third-party domain control of a skill group.

- Enable **Event Minimization** for the **CVLAN CTI** links used by the **Peripheral Gateway**. This is not applicable when PG uses **TSAPI Interface** to connect to **AES**.
- For optimal performance, external applications that alter agent state on the **Avaya ECS**, use the Enterprise CTI interface. Contact your Cisco Unified ICM software representative for comprehensive and up-to-date information on configurations.

ACD Notes and Restrictions

Following are the notes and restrictions applicable to Avaya:

- **Monitoring VDN**s - It is important that all **VDN**s to be monitored are properly configured as Peripheral Targets in the Unified ICM database.
- **CTI links and BHCC**- Each CTI link can support the following link specification (approximate):
  - 8,000 BHCC using a BRI CTI link
  - 32,000 BHCC on a G3r using an Ethernet CTI link
  - 20,000 BHCC on a G3i or G3s using an Ethernet CTI link

  These link specifications are derived from Avaya-provided data and are subject to change.
- The Avaya PG **supports** Agent IDs, Agent Extensions, Hunt Group Extensions, and VDNs that start with a zero. This is supported for both CMS and CMS-less environments.
- The Avaya PG **does not support** Hunt Group Numbers that start with a leading zero.
- **Intermittent Failure of Network Transfer**: There is occasionally a timing issue in the set of events involved in a **Network Transfer**. Due to this issueIntermittent Failure of Network Transfer, the NIC Call ID is not populated in the transfer call. This results in call failure. To avoid this problem, introduce a delay of 1 second in the Vector for the post-route number (VDN); that is,

Due to this issueIntermittent Failure of	01 wait-time 1-secs hearing silence
02 adjunct routing link 1	

- **Avaya ECS PIM Failure** - The **ECS PIM** stops functioning when the AES link on the Avaya switch sends a "Busyout" command.
- **VDN Return Destination**
  - The Return Destination **VDN** feature does not support the **call conference** before agent drops the call (expecting return destination to set in). That is, the PG loses its track of the **VDN** to which the call was originally delivered and call variables are not retained post Return Destination. However, this feature supports **call transfer** before the agent drops the call (expecting return destination to set in). That is, the PG tracks the **VDN** to which the call was originally delivered and call variables are retained post return destination.

- Return Destination cannot be executed multiple times. That is, Return Destination can occur only once for a call in Avaya.

  See sections Configuring Return Destination VDN on Avaya Switch for Configuring the Return Destination VDN on Unified ICM respectively.

- **Processing Invalid CMS Records** - Whenever the CMS receives an invalid record, the Avaya PG service goes out of service. Create the following registry value and set its registry value data as 1 so that Avaya PG Service ignores the invalid CMS record and continue its normal operation.
  - **Registry Value:** IgnoreInvalidCMSRecord
  - **Registry Value Type:** DWORD
  - **Registry Value Path:** HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<cust_inst>\<pg_inst>\PG\CurrentVersion\PIMS\<pim_inst>\ATTData\Dynamic\
  - **Registry Value Data:**
    - 0 – Avaya PG Service will go out of service and log out all the Agents, if an invalid CMS record is received.
    - 1 – Avaya PG Service will ignore the invalid CMS record and continue its normal operation.

Related Topics

Configuring Return Destination VDN on Avaya Switch, on page 18
Configuring the Return Destination VDN on Unified ICM, on page 36

Multiple PGs

The Avaya ACD allows connections from multiple PGs. However, while using such a configuration, the resources (like Stations, Agents, VDNs, Splits, and any other resources) used by each PG, are maintained as separate configurations.

Multiple PG deployments on a single ACD are used to split the load on the PG. These can also have a dedicated PG to service a business line in the contact center.

To deploy multiple PGs on a single ACD, it is required for you to have distinct configuration between the PGs. Section Dual PG Setup describes the configuration of two PGs on a single ACD. You can follow the same steps to configure multiple PGs to the same ACD.

Note Contact the ACD vendor for ACD-related issues or limitations on connecting multiple PGs to a single ACD.

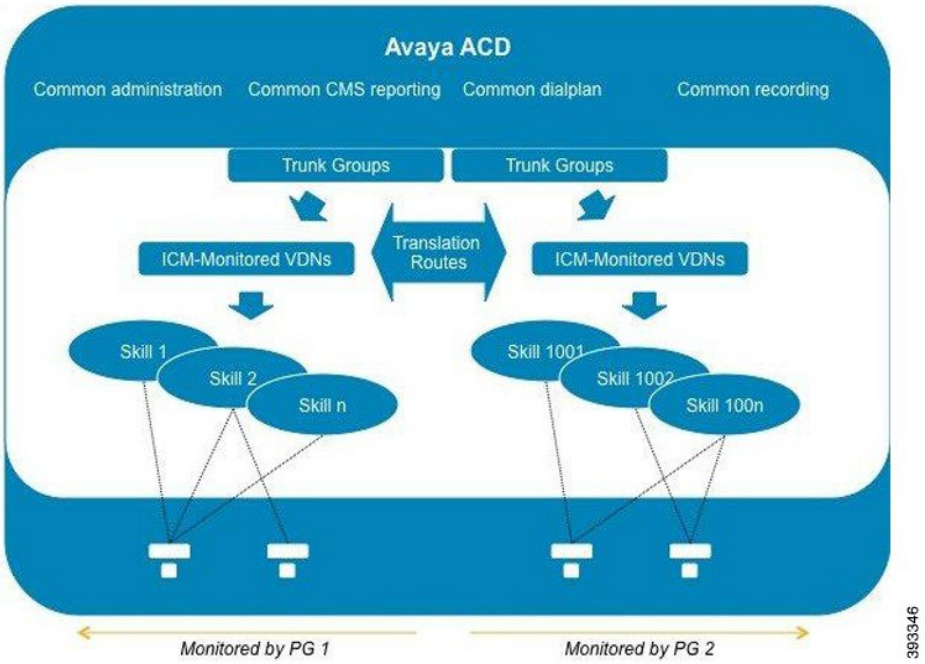
Related Topics

Dual PG Setup, on page 26

Dual PG Setup

Note Ensure that you adhere to the requirements provided in this section while deploying multiple PGs. The performance and functionality of the PG is impacted if you do not follow the requirements listed in this section. When two **PG**s are deployed, **ICM** routing effectively sees the **Avaya** system as two independent peripherals. As such, there are some specific configuration and operational requirements that are required to be put in place. The following figure describes the overview of **Dual PG setup**.

Figure 11: Dual PG Overview



For the same Avaya **ACD** to behave as an independent peripheral to **Unified ICM**, avoid having one skill group monitored by the two **PG**s. To achieve this, you have to determine which Avaya skill numbers are associated with PG1 and PG2, respectively. For example, skill groups 1-1000 and 1001-2000 would be two separate sets monitored by each instance.

When two **PG**s share the load of a single **PG**, have a logical correlation between the skill numbers associated with the different PGs. For example, the "pre-paid sales" skill associated with **PG1** might be 500, and the one associated with **PG2**, 1500 (just added the digit 1 in front). It is essential for the supervisor to look at a report that combines the information from the two corresponding skills to understand the overall skill performance. After the correlation is defined, each agents are assigned only the skill numbers. These numbers belong to the same PG (considering the example stated before, an agent must not have skills 500 and 1502 at the same time).

Because the **PG**s also monitor Avaya stations, the agents associated with that PG must log in to the stations monitored by that **PG** only. All stations and agent-IDs at a given physical site is required to be defined at only one **PG**. You can avoid having one site with entities from two PGs. Assign stations sequentially for every **PG**.

The **VDN**s (that are monitored by Unified ICM) are independent, regardless of whether they are used by calls when they first enter the environment or for translation routes. The **CTI** links used by these VDNs (through the vectors they point to), are separated; the CTI links established with PG1 A and B, and with PG2 A and B. You can also define dial-plan ranges for VDNs in each PG to make the configuration simpler (but it is not required).

The calls within the **PG** can be dialed directly using normal dial plan numbers such as **VDN**s, **Agent ID**s, extensions, and hunt groups. Ideally, the calls are not disconnected across two **PG**s. However, in such scenarios, the call has to be translation routed to the target PG over trunk, which is equivalent to routing to a **PG** connected to a different switch. To achieve this kind of a routing, loop back trunks is required to be provisioned on the switch and used for routing calls to dial plan numbers of another PG.

When the call is routed from **PG1** to **PG2**, the target **PG2** understands the call as an inbound call and the **ICM** reporting reflects the same. To prevent inappropriate agent behavior, the Avaya system can be programmed to block incorrect call flows (COR or tenant settings). Design the system to avoid or minimize the call between the two **PG** groups.

Cisco mandates that trunk groups monitored by each PG be separate. If two PGs are used to monitor the same trunk group, Unified ICM software do not understand that the feeds, it gets are duplicated.

Other Avaya resources such as announcements, classes of restriction, **CMS** reporting, recording, and so on, are not affected with dual PG implementation.

Note Although two **PG**s can provide scalability from a Cisco Unified ICM perspective, it is also necessary for you to consult Avaya about how ACDs handle the increased **CTI traffic**. It also considers all other applications that currently used, such as recording and virtual hold. These thresholds are associated with a large number of CTI-enabled agents in the **Avaya ACD**s, although, two PGs are being used.

Maintaining Your Configuration

It is preferred that changes made to your configuration are accomplished on the **Avaya/CMS** and in the **Unified ICM** database consecutively. This ensures that the PG gets the configuration updates on the Avaya/CMS systems.

It is imperative that the **Avaya**, **CMS**, and the **Unified ICM** database configurations are kept synchronized (that is, up-to-date with each other). Inaccurate or incomplete data results in inaccurate agent or call data.

Configuring High Availability CMS

The high availability **CMS** configuration minimizes the down time in the event of **Avaya CMS** failure. If you want to have such configuration in your call center environment, set up the **PG**s as follows:

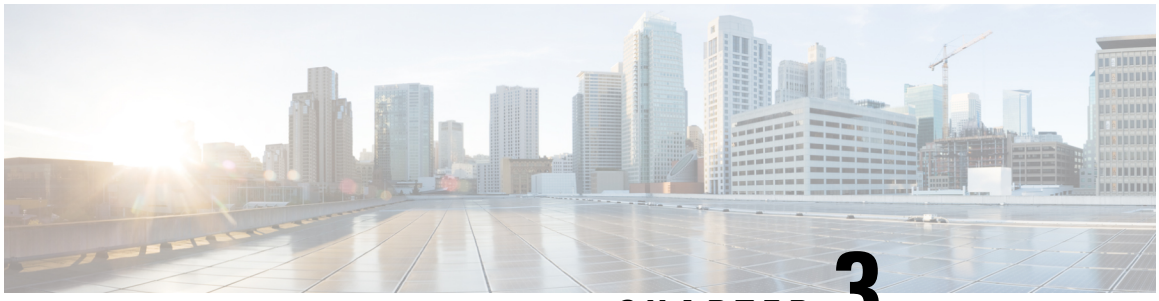
- **Duplex PG configuration**: Both **CMS**s (CMS no.1 and CMS no.2) require to use both PG's IP addresses (that is, IP addresses of PG-A and PG-B) for connections. It is the same as they do in a single CMS configuration. However, at any given time, only one CMS can connect to the active PG. The other PG is always in standby mode. So if PG-B is currently active, PG-A is in standby mode (and conversely).

When running the Peripheral Gateway Setup tool, ensure that the **CMS** Hostname field in the AvayaPIM Configuration pop-up menu is blank. This allows the PIM to accept a connection from either **HA CM**S server. If one HA CMS server goes down, the other initiates a connection to the PIM on the active PG.

Note Irrespective of this being a **High Availability CMS** configuration or not, a **CMS** Data Feed failure results in a failover from one side of a duplexed PG to the other.

- Simplex PG configuration: Both CMSs use the PG's IP address for connection. But only one CMS can connect to the PG at any given time. Also, be sure when running Peripheral Gateway Setup tool that the CMS Hostname field in the **Avaya PIM Configuration** pop-up menu is blank. This allows the PIM to accept a connection from any one CMS server. If one CMS server goes down, the other initiates a connection to the PIM.

Note The **HA CMS** server going down, leads to **CMS** Data Feed failure; this results in a brief outage on a simplex PG.



CHAPTER 3

Unified ICM Software Configuration

In order to properly set up and maintain the Unified ICM database, you need to understand the relationships between the Avaya database objects and the Unified ICM database objects. Some Unified ICM objects (for example, Unified ICM Services) do not correspond directly to a specific object on the Avaya. Other Unified ICM objects, such as trunks, correspond directly to objects on the ECS/MultiVantage/Avaya. By understanding the relationships between the database objects of the Avaya and Unified ICM systems, it will be easier to keep the Avaya ECS/MultiVantage, CMS, and the Unified ICM databases synchronized (that is, up-to-date with each other). This chapter describes how objects map between the Avaya and Unified ICM software. It also provides Avaya-specific information that may assist you in configuring the PG through the Configuration Manager tools. For detailed information on the Configuration Manager tool user interface, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* available at:

http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligent-contact-management-enterprise/products-installation-and-configuration-guides-list.html

- Peripheral Configuration, on page 30
- Peripheral Targets, on page 34
- Peripheral Monitor Table, on page 35
- PIM Configuration, on page 36
- Connection management with AES using TSAPI Interface, on page 39
- **Installing TSAPI Client** , on page 40
- Service Observer , on page 40
- Trunk Groups, on page 40
- Trunks, on page 41
- Services, on page 41
- Skill Groups, on page 42
- Service-to-Skill Group Mappings, on page 45
- Agents, on page 45
- Skill Group Members, on page 48
- Translation Routes, on page 48
- Routes, on page 48
- Routing Client, on page 48
- Unified ICM Configuration for “CMS-less” PGs, on page 48
- Maintaining Your Configuration, on page 49
- Registry Keys, on page 49

Peripheral Configuration

In **Unified ICM** terms, the **Avaya** corresponds to a peripheral. Unified **ICM** software treats all contact center devices (for example, **ACD**s, **PBX**s, **VRU** systems) as peripherals.

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

Peripheral Skill Group Mask

The Peripheral (default) **Skill Group Mask**, which is available from the **PG Explorer** tool, are checked and set appropriately. The **Skill Group Mask** is used when configuring all skill groups for the peripheral.

If your peripheral is an **EAS** type, ensure that all check boxes are appropriately checked/unchecked. These check boxes identify the sub-groups or skill levels created for each skill group.

The default setting is that **Skill Level 1**(primary) and **Skill Level 2** (secondary) are checked, all other boxes (by default) are unchecked. The existence of the sub-skill groups can affect agent counts and call reporting. The **Peripheral Skill Group Mask** are overridden on a skill group by skill group basis as required.

Peripheral Call Control Variable Map

The **Call Control Variable Map** field, which is available on the **PG Explorer** tool, controls the mapping of route request elements to **Peripheral Variables**.

The **Call Control Variable Map** field can be used to set up the specific peripheral variables. Although these variables are reserved for a **CTI** application, the **PG** can use them as well.

Following are the ways to control variable usage by the **CallControlVariableMap**:

- Direct the **PM**: The **PIM** is 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 (that is, the **PIM** does not set call variables 2 through 4).

Note This argument is from the perspective of the **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** to set call variable 1 and call variables 5 through 10. These call variables are set, while preserving the peripheral-determined values of call variables 2 through 4.

```
/CTI = ynnnyyyyyy
```

See also: For details on **Route Request** Elements, see Chapter 4, Post Routing. For more details on Unified ICM CTI capabilities and interaction with the PG, see the *ICM Software Enterprise CTI Interface Specification*.

Related Topics

Post-routing

Peripheral Configuration Parameters

Several default settings are entered in the **Configuration Parameters** field of the **PG Explorer tool**. This includes default work-mode, default login skill level, reserved agent preference levels, and station monitoring of logged-in agents.

1. **Default Work-Mode** The default work-mode used by the **PIM**, while setting an agent to the **READY** state through a **CTI** application. This is configured by the **Configuration Parameters** field. The keyword/defworkmode, followed by manual or auto, sets the default work-mode to the **Avaya** which is equivalent of **Manual-In** and **AUTO-IN** respectively. The following example sets the default work-mode to **AUTO-IN**:

   ```
   /defworkmode auto
   ```

   This default work-mode is used by the **PIM**. This happens, in case where a **CTI** application does not provide a proper work-mode while setting the agent to the READY state. If unspecified, the **PIM** default is **MANUAL-IN**.
2. **Default Login Skill Level**: The default login skill level (that is, priority or skill level) used by the **PIM**. This is configured by the **Configuration Parameters** field. The default login skill is used when an agent logs in and no agent skill group member are found for that agent in **Unified ICM Configuration**. The keyword/ Default Work-Modedefskilllevel followed by a numeric skill level sets the default skill level. The following example sets the default login skill level to 3:

   ```
   /defskilllevel 3
   ```

   If unspecified, the **PIM** default is 16.
3. **Reserved Agent Preference Levels** (in ICM software, Release 4.0 and greater) are configured by the **Configuration Parameters** field. The reserved agent 1 and agent 2 preference levels (represented as preference level 51 and 52, respectively, in CMS) are mapped again to a valid preference level. The PIM defaults the values to the highest valid preference level. The keywords / r1pref and / r2pref are used to re-map reserve preference level 1 and 2 respectively. The following example causes the PG to re-map reserve agent 1 and reserve agent 2 preference levels to preference level 15 and 16, respectively

   ```
   /r1pref 15 /r2pref 16
   ```

   Setting a preference value of zero (0) causes the **PIM** to ignore that reserve agent skill login and preference level. This means that the agents are not going to be considered to have logged in to that reserved skill. No metrics are collected for that agent for that skill.
4. **Station Monitoring of Logged-In Agents**

   Station monitoring of logged-in agents are automatically configured by the **Configuration Parameters** field. The **keyword / monitoragent** followed by a **y** or **n** causes the PG to automatically monitor or not monitor a logged-in agent. The following example causes the **PG** to automatically monitor a logged-in agent:

   ```
   /monitoragent y
   ```

At the time, of an agent login, with a setting of **y**, the **PG** automatically monitors that agent's station. This happens, even if that station is not in the **Peripheral Monitor** list. If station monitoring is enabled, the PG defaults to automatically monitoring logged-in agents. If station monitoring is disabled, the PG does not monitor any agent stations.

Note

- **/monitoragent** is set to y in **PIM** by default. If you do not want to monitor specific extensions, then it is necessary for you monitor all the logged agents, set /monitoragent to y (use /monitoragent y). Configuring the extensions in the Peripheral Monitor Table of the PG Explorer is not needed. In such configurations, **PIM** monitors only those extensions, where agents are logged in.
- If you are using **CMS** with Unified **ICM** and have over 1000 agents, disable the station monitoring of logged-in agents. Monitoring agent stations (That is providing visibility to all station activity) results in increased message traffic to the A, increased switch CPU load, and increased network traffic between the PG and Central Controller.

5. **Use Encoded Trunk Information over ANI in Calling Field** with a setting of y, the PIM reports events in the calling field populated with encoded trunk information rather than **ANI**. The default mode is to populate the calling field with **ANI**. This argument defaults to n. If the argument is not specified or is specified as /**UseTrunkOverANIInCallingField**.

   An example of one event may be:

```
19:31:20 pg1A-pim1 Trace: CSTA DELIVERED,
 PrivData=[UU=None Consult[CID 603 Dev 6505 DevType 0] II 0
 Alert[Handle -1 Type LT_UNKNOWN] ANI 6505
 dnis_chars [] UCID 0x0
 TG 7 Tk 5 Mult 1]
 LoginDigits [] CallPrompt []
 CallID      = 604  DeviceID = 6505  DeviceType = Static
 Alerting    = 3501
 Calling     = 6505
 Called      = 3501
 Redirection = 6505
 LocalState  = INITIATE
 Cause       = EC_NEW_CALL
```

   If the argument is specified as /**UseTrunkOverANIInCallingField y** that same event may appear as:

```
19:31:20 pg1A-pim1 Trace: CSTA DELIVERED,
 PrivData=[UU=None Consult[CID 603 Dev 6505 DevType 0] II 0
 Alert[Handle -1 Type LT_UNKNOWN] ANI 6505
 dnis_chars [] UCID 0x0
 TG 7 Tk 5 Mult 1]
 LoginDigits [] CallPrompt []
 CallID      = 604  DeviceID = 6505  DeviceType = Static
 Alerting    = 3501
 Calling    = 229381  <= decimal equivalent of encoded trunk Called      = 3501
 Redirection = 6505
 LocalState = INITIATE
Cause       = EC_NEW_CALL
```

Note The scheme for trunk information encoding is such that the upper 17 bits represent the Trunk Group and the lower 15 bits represent the Trunk. From the above example: For a Trunk Group value of 7 and a trunk value of 5, the binary representation for the encoded value is 00000000000000111 000000000000101. The decimal equivalent is 229381.

```
/UseTrunkOverANIInCallingField y
```

6. **Use Encoded Trunk Information over ANI in Calling Field for Outbound Calls**

   To support the selecting of trunk data or ANI in calling device field for outbound calls, use the configuration parameter: **/UseTrunkOverANIInCallingFieldForOutboundCalls**

   The flag-usage is as follows:

   a. Set the configuration parameter to **y**, if the trunk information is required in the calling device field for outbound calls.

   ```
   /UseTrunkOverANIInCallingFieldForOutboundCalls y
   ```

   b. Set the configuration parameter to **n**, if the trunk information is not required in the calling device field for outbound calls.

   ```
   /UseTrunkOverANIInCallingFieldForOutboundCalls n
   ```

Note
a. When the value of this flag is n, **ANI** appears in the calling device field. Also, the default value of this flag is n.
b. This flag controls the value of calling device field in **CSTA DELIVERED** and **CSTA ESTABLISHED** messages for outbound calls.
c. This flag is available from Releases ICM 6.0(0) SR9, and ICM 7.1(3) onwards.

Note The **UseTrunkOverANIInCallingField** and **UseTrunkOverANIInCallingFieldForOutboundCalls** are not applicable to **TAESPIM**.

7. **Display the Caller Entered Digits (CEDs) on the Agent Desktop**

   To ensure that the **CED**s are populated on the agent desktop, set the following parameters in the PG Explorer. In the **Advanced tab**, ensure that the **Agent auto-configuration** check box is checked.

8. In the **Agent Distribution** tab, ensure that the **Enable agent reporting** check box is checked.

Note If you do not select them together, the **CED**s is not going to get populated on the agent desktop.

These settings are applied only to the **Avaya PG** with the **CMS** mode enabled.

Peripheral Targets

A Unified ICM Peripheral Target is equivalent to the combination of **DNIS** (**VDN** extension or Hunt Group Extension) and the trunk groups through which incoming calls arrive. **VDN**s are equivalent to the DNIS (for example, **VDN** 1100 would be **DNIS** 1100).

A Peripheral Target can be either of the following:

- A Network Target, identified by a Trunk Group and **DNIS** (VDN) that terminates on the **Avaya**. A Network Target is a target that Unified ICM software identifies as a termination for calls routed through the network. These trunk group-DNIS pairs are typically associated with labels provisioned by a long-distance carrier.
- An Internal Target, identified by the **DNIS** (VDN) alone. An Internal Target is a VDN or Hunt Group extension used as a destination for internal call transfers, tie lines, and so on.

  All Peripheral Targets, both internal (that is transfer points) and network, requires to be configured as Peripheral Targets in the Unified **ICM** database. This is done by using the Configure ICM tool. It is not necessary to enter every **TrunkGroup/VDN** in combination in the Unified ICM database unless you require them for call routing. In other words, a **VDN** requires to be entered only once in the Unified ICM database as a Peripheral Target. This is done for the **PG** to monitor the calls on that **VDN**.

  You can configure Peripheral Targets by using the Peripheral Target Configuration window within the Configure ICM tool.

Configuring VDN and Hunt Group Extensions as Peripheral Targets

All **VDN** and **Hunt Group** extensions that are in any way connected with the handling of an incoming call must be configured in the Unified **ICM** database as **Peripheral Targets**. This ensures complete call monitoring. The **PG** monitors only those **VDN**s and, optionally, Hunt Groups that are configured as **Peripheral Targets**.

The **Trunk Group** (which are used internally), does not access **VDN**s or **Hunt Group Extensions** directly. This requires to use the default **Trunk Group** 9999. (See Trunk Groups later in this chapter.)

Note The Avaya PG (ESCPIM) supports extensions up to ten digits. The agent can log in to a Softphone that has an extension up to ten digits. This ten-digit support applies to Agent Login IDs too.

The Hunt Groups and VDNs support up to seven digits only. In order to use a seven digits, or a ten-digit, the config PIM registry, **EnableTenDigitExtension** is set to 1 in following path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\ICM\<cus01>\<PGXX>\PG\CurrentVersion\PIMS\pim1\ATTData\Config\
```

If the registry **EnableTenDigitExtension** is set to 0, then it limits support up to five digits for extension, Agent Login IDs, Hunt Groups, and VDNs.

Note By default, Avaya PG (TAESPIM) supports extensions of up to ten digits and this does not require registry configuration. The Agent Login IDs support up to ten digits.

Related Topics

Trunk Groups, on page 40

Peripheral Monitor Table

Unified ICM Peripheral Monitor table is used to set up stations for station monitoring and VDNs that have Timed ACW values. A Peripheral Monitor table **VDN** entry is used only to indicate any **Timed ACW** value as configured on the switch. This Peripheral Monitor VDN entry **does not** replace a Peripheral Target for **VDN** monitoring.

Note VDNs must also be configured as Peripheral Targets in order to be monitored for reporting.

You can set up the Peripheral Monitor Table by choosing **Peripherals** > **Peripheral Monitor** within Configure ICM to display the Peripheral Monitor table.

Click the **Insert** button to add records using the Peripheral Monitor Configuration window.

Monitoring Stations

The **Peripheral Monitor** table is used to specify which station, or range of stations, should be monitored by the PG. Multiple peripheral monitor entries are allowed. Set the **Peripheral Monitor Type** to Station. When specifying a single station (e.g., 1100), use the Extension field. When specifying a range of stations (e.g., 1100-1200), use the Param String field.

VDN Timed ACW Settings

VDNs that have a Timed **ACW** value on the **Avaya** is added as a **Peripheral Monitor** table entry with a Type of **VDN**. The **Peripheral Monitor Param** field indicates the **Timed ACW** value.

For **VDN**s that **do not** have the **VDN** override set, specify the Timed ACW value in the Peripheral Monitor table parameter string using the following format:

```
acw=N
```

Note

1. The acw keyword must be in lower-case. Replace the **N** with the number of Timed ACW seconds. For example, a **VDN** with a Timed **ACW** of **30** seconds that does not have **VDN** override set would specify a Timed **ACW** value in the Peripheral Monitor table as:

   ```
   acw=30
   ```

   For VDNs that do have **VDN** override set, specify the Timed **ACW** value in the Peripheral Monitor table parameter string using the following format:

   ```
   ACW=NNNN
   ```

2. The ACW keyword must be in upper-case. Replace **N** with the number of Timed **ACW** seconds. For example, a **VDN** with a Timed **ACW** of **180** seconds which does not have VDN override set specifies a **Timed ACW** value in the **Peripheral Monitor** table.

3. Only those **VDN**s that are monitored and for which the **Avaya** generates call events on their behalf, are considered as being in the **call path** by the PG when determining the correct **Timed ACW** value. In other words, if the **PG** is not notified by the switch that the call has passed through a **VDN**, the PG cannot consider that **VDN** when determining the **Timed ACW** value. The **PG** endeavors to use the same rule set as documented for the switch in determining the Timed **ACW** value to use (including **VDN** override).

Configuring the Return Destination VDN on Unified ICM

The **Return Destination** feature is configured in the **PG Explorer** Tool for a particular VDN for which the Return Destination is enabled on Avaya Switch.

In **PG Explorer > Peripheral Monitor** tab, set the Parameter string for the return destination **VDN** as **returndestination**.

To set up Return Destination VDN on Avaya Switch, see the section Configuring the Return Destination on Unified ICM

See the section ACD Notes and Restrictions for known caveats for Return Destination VDN.

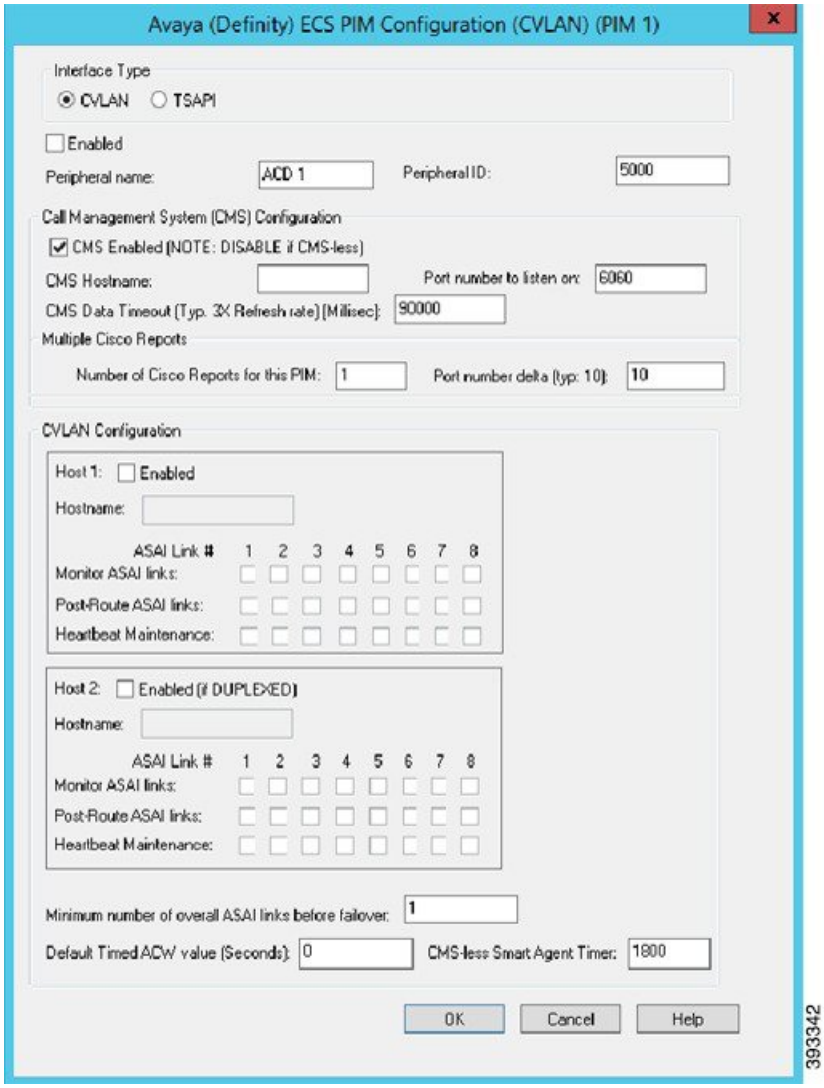
Related Topics

ACD Notes and Restrictions, on page 24
Configuring Return Destination VDN on Avaya Switch, on page 18

PIM Configuration

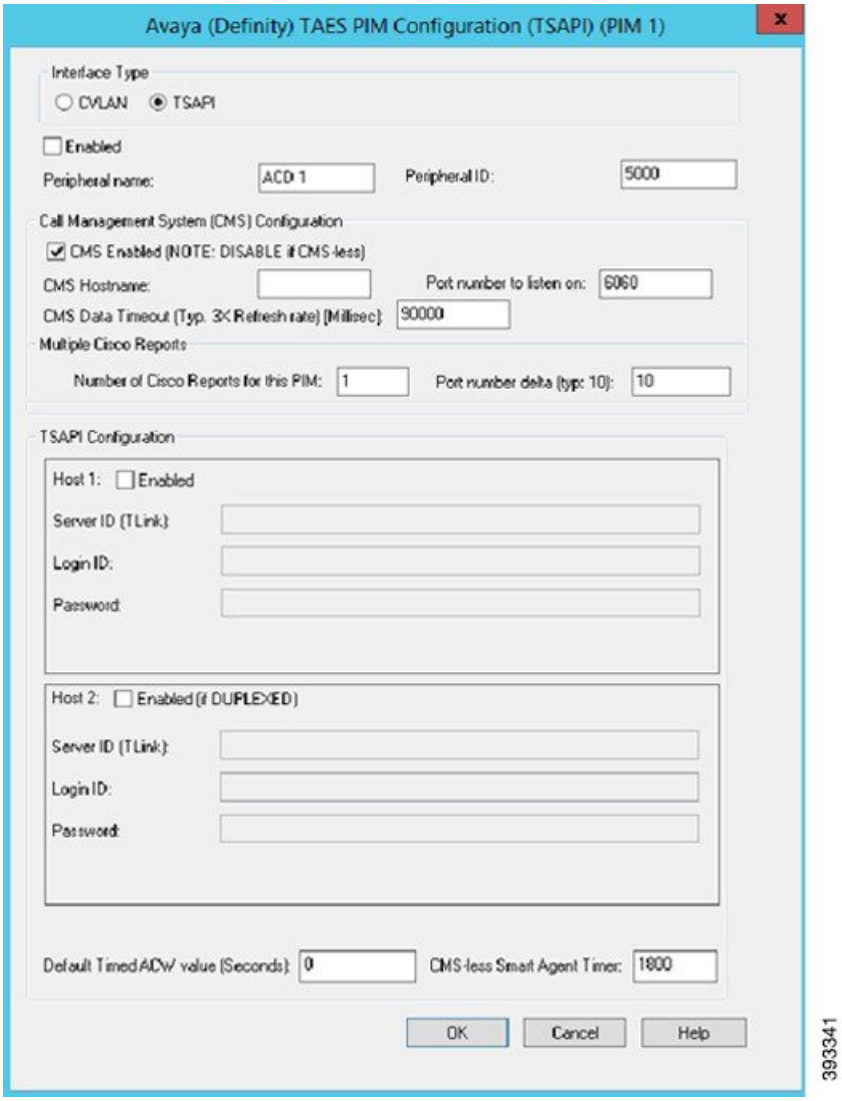
The following figure shows **PIM Configuration** UI for **CVLAN Interface.**

Figure 12: PIM Configuration UI for CVLAN interface



Similarly, the following figure shows **PIM Configuration** UI for **TSAPI Interface**. The following points describe the **Avaya ECS PIM Configuration** Setup window:

Figure 13: PIM Configuration UI for TSAPI interface



Note Before starting the PG service with TSAPI interface, **TSAPI Client 7.0** is required. Please refer Installing TSAPI Client section for the client installation procedure.

1. Select the **Interface Type**. This selection of the interface type, determines the interface that the **PIM** uses to communicate with the **Application Enablement Services** (AES).
2. Check the **Enabled** option to put the **PIM** into service. This option allows the **PIM** to communicate with the peripheral when the Peripheral Gateway is running.
3. Check the **Enabled** option to put the **PIM** into service. This option allows the **PIM** to communicate with the peripheral when the Peripheral Gateway is running.
4. In **Configuration Manager** (use the **PG Explorer** tool to view the **Peripheral ID**), each **Configuration dialog box** contains an **Enabled** option, a **Peripheral name**, and a**Peripheral ID** field. From the

Peripheral record, enter the name of the peripheral in the **Peripheral name** field. Similarly, in the **Peripheral ID** field, enter the appropriate value.

5. If you want to use **CMS**, check the **CMS Enabled** checkbox. Fill in the information about the **CMS** connection in the Call Management System (CMS) Configuration section. The **CMS** Data Timeout is in milliseconds. For the **Interface Type**, select either **CVLAN** or **TSAPI**.
   - If you select interface type as **CVLAN** and complete the steps that are listed in the following:
     a. Use the **CVLAN Configuration** fields to describe the **AES** connections for **PG** and its duplexed pair (if any)
     b. In the Monitor **ASAI** links field, specify which **ASAI** Links in the AES system the **PG** uses for monitoring calls, stations, and so on.
        1. In the Post-Route **ASAI** links field, indicate which **ASAI** lnks in the **AES** system the **PG** uses for **ICM Post-Routingpostroute_def**.
        2. In the Heartbeat Maintenance field, specify which **ASAI** Links in the **AES** system the Unified **ICM** uses for heartbeat maintenance.
     c. In the Minimum number of overall **ASAI** links before **Failover** field, enter the minimum number of **ASAI** links. This is required for the expected call load. If the PG is duplexed and the number of links available to the **PG** reduces lower than this value, the **Unified ICM** attempts to switch over to the other PG.
   - Similarly, if you select interface type as **TSAPI**, you can follow the steps that are listed in the following:
     a. Use the **TSAPI Configuration** fields to describe the **AES** connections for the **PG** and its duplexed pair (if any).
     b. In the **ServerID** field, specify the **TLink** that is configured in the **AES** Server.
     c. In the **LoginID** field, specify the **CTI** username that is configured in the AES Server.
     d. In the Password field, specify the **CTI** password that is configured in the **AES** Server.
6. In the Default Timed **ACW** value (Seconds) field specify the default time that the agents are allocated for after-call-work (ACW). A zero in this field indicates that the **Unified ICM** obtains this value from the Peripheral Monitor table. The values you have entered in this field are applicable to the monitored agents.

Related Topics

Installing TSAPI Client , on page 40

Connection management with AES using TSAPI Interface

At any point, AVAYA **TAESPIM** connects to one of the **AES server**. This **AES server** is configured in **PIM** configuration window.

In case if any failure occurs in the connection **PIM** tries to connect to another host. All the monitoring sessions are started from the beginning against the new **AES server**.

Installing TSAPI Client

Before you install the TSAPI client on your Avaya PG machine, you must download it from the Avaya Support website or from the Avaya DevConnect website.

Note Download the 32 Bit version of TSAPI client for Windows that must be installed on the Avaya PG machine.

The following steps help you with the installation of **TSAPI Client**:

1. Run **setup.exe** from the Installation folder and launch the **TSAPI Client** installer wizard.
2. Click **Next**. On **License Agreement** screen, select the appropriate radio button to accept the terms and license agreement.
3. Click **Next**.
4. To install the **TSAPI Client**, choose the default destination folder and click **Next**. In case if you want to select another folder, browse to the applicable folder.
5. Enter the **Hostname** or **IP Address** of the **AES** server. Click **Add to List**. This stores all AES server details in **TSLIB.ini** file of the client installation folder.
6. Click **Next**.
7. A warning message appears. This prompts you to replace the existing DLL files with aes-libeay32.dll and aes-ssleay32.dll, which is recommended. Select **No** to continue without replacing the files in icm\bin folder.
8. Click **Finish** to complete the installation process.

Note You can change the **AES** server details in the **TSLIB.ini** file, which is located in the client installation folder. This enables you to change the server details without running the setup again.

Service Observer

The Service Observer feature allows a supervisor to silently monitor the conversation between an agent and a customer by using various monitor options available from the ACD. The supervisor uses the configured features' codes on the switch to perform service observing.

The Termination Call Detail (TCD) record for an observed call has a call disposition of Conferenced (30).

Trunk Groups

An Avaya Trunk Group is equivalent to a Unified ICM Trunk Group. The Avaya Trunk Group Number (For example, trunk group 5) is Unified ICM Trunk Group Peripheral Number. The Trunk Group Access Code

(TAC) is Unified ICM Trunk Group Extension (For example, 500). TrunkGroupTimer is the value in the Registry that specifies the interval (in seconds) in which the PIM generates trunk group value requests. In other words, the TrunkGroupTimer specifies the timer period at which the PIM issues a Trunk Group query for each configured ICR trunk group. The default value for TrunkGroupTimer in the Registry is set to 10 seconds.

The PG uses the Trunk Group Extension to value query the Avaya and monitor Trunk Group trunk utilization. The PG also uses the Trunk Group Extension to properly identify an incoming call on translation route applications. The Trunk Group Extension is set in the Trunk Group Configuration window of Configure ICM.

For example, Trunk Group 11 with Trunk Access Code 111 would be entered in the Unified ICM database as Trunk Group 11 with Trunk Group Extension 111.

Create a default trunk group 9999 for use in those instances where a physical Trunk Group does not exist. For example, Hunt Groups or VDNs that are internal transfer points for agents, and therefore not accessible via an external trunk group, uses the default trunk group 9999 to allow the creation of the Peripheral Target. The default Trunk Group extension (that is, TAC) can either be left blank or specify 9999.

The NT Registry is be configured to allow the PG to "Map Peripheral Targets without Trunk Group."

Note During a translation route, you need not set up the Network Trunk Group (NTG) if Unified ICM trunk reports are not required. A dummy NTG configuration, with a dummy peripheral number, can be configured and associated with the configured translation routes.

Trunks

Individual trunks may or may not be monitored on the Avaya.

No special configuration information is required on an individual trunk basis. However, you must specify the number of trunks in the **Trunk Group** in the **Trunk Group** configuration Trunk Count field. Because the switch provides only the number of trunks-in-use and the trunks-idle, this count allows the **Avaya PIM** to determine the number of out-of-service trunks.

Services

A Unified **ICM Service** is the combination of call type (known by the VDN) and call treatment (that is, vector). There is no direct correlation of **Unified ICM** Service to a specific **Avaya** object. However, a service does appropriate with what users typically identify **Call treatment** on the **Avaya**.

The **Service Peripheral Number** is equivalent to the **VDN** extension number. The **Peripheral Service Level** is equivalent to the **VDN** service level.

Note The Avaya **PIM** does not support the updating of **Peripheral Service Level**.

Using the **Service Explorer** tool, set the **Peripheral Service Level** to C**omputed By Call Center**. The **Unified ICM Peripheral** Service **Peripheral Service Level** corresponds to the **VDN** Service Level.

Skill Groups

The **Avaya**-to-**Unified ICM Skill Group** mapping is as follows:

Table 4: Avaya-to-Unified ICM Skill Group Mapping

Unified ICM Software	Avaya
Skill Group	Skill Group
Skill Group Peripheral Number	Skill Group Number
Skill Group Extension	Skill Group Extension
Subgroups	Skill Group and Skill LevelsTPF FPT

Note Unified **ICM Skill Group Peripheral Number** is the **Avaya Skill Group Number**. The Unified ICM Skill Group Extension is the **Avaya Skill Group Extension**. For example, if the **Spanish skill group** has a group number of 11 and an extension of 1100, then the **Unified ICM Skill Group Peripheral Number** is 11 and the **Skill Group Extension** is 1100.

Important The Unified ICM Skill Group **Peripheral Number** and **Skill Group Extension** are important and must be kept synchronized (that is, up-to-date) with the Avaya skill group configuration. Failure to keep the skill group information synchronized between the Avaya and the Unified **ICM** database may result in incomplete (or worst case, inaccurate) call and agent statistics.

Skill Group Subgroups

Sometimes, while created, a single Unified ICM skill group causes more than one skill group to be created in the **Unified ICM** database. These other skill groups are sub-skill groups, or subgroups, for the created **base** (priority 0) skill group. A subgroup has a unique priority and is associated with the base skill group.

Note For every **base** skill group created, at least one sub-group must be created under it.

Important subgroups are created.

The **PG**s require to be cycled every time new subgroup are created.

The creation of these subgroups is determined on which subgroup mask is used at the time of the base skill group creation. The subgroup mask can have one of two settings: Peripheral Default or Specified. These settings are specified in the Skill Group Explorer tool.

If the subgroup mask is **Peripheral Default**, then the **Peripheral's Skill Group Mask** is used to determine which subgroups are created; otherwise, the Sub Group Mask for the Skill Group is used.

A subgroup is created for each checked box in the Sub Group Mask. The subgroups are used by the PG to properly log in the agent to the appropriate subgroup based on the agent's skill group skill level. For example, in an EAS type switch configuration, agents may be logged into a skill group with a PRIMARY or SECONDARY skill level. In order to properly account for agent counts and roll up call statistics properly, the subgroup for the agent's skill group requires to be configured in the Unified **ICM** database.

Note In order for AutoLoginBase to work correctly and provide consistent LAA stats for agents in all priorities, at least one agent must be logged in to the base skill group.

For CMS Configurations:

The Avaya **Hunt Group** configuration screen for each split **must** have the Measured Field set to either **both** or "external" in order for the CMS to receive Hunt Group (split) data. Agent configurations on an Avaya **EAS** switch can use any of the valid skill-types (1-16) if the Cisco CMS report that is installed and running is an **EAS** report. Likewise, the agent configurations on an Avaya EAS are limited to 1-2 skill-types. If you configure agents with a skill type greater than 2 for a Non-EAS or EAS CMS report, the PG is not properly activated.

Note When working with ICM Version 4.5(x) and later, while activating the **ACD PIM** if you get an error message that contains the term **C_NOENT**, do the following:

- Add the name and IP address of the ACD **PIM** to the host file.
- Restart the PG ICM Services.

For CMS-less Configurations:

The subgroups are used to associate an agent with the correct skill group **and** skill level. For example, if an agent is configured on the ACD switch to be logged into skill 1 priority 3, then you would configure that agent in the Unified ICM database to be a skill group member of skill group 1 subgroup 3.

- *See also:* See the section CMS Cisco Real-Time Report for more information on CMS-related skill group issues related to configuration and CMS report revision.

Related Topics

CMS Cisco Real-Time Report, on page 22

Using Skill Group Priorities without Configuring Sub-Skill Groups

In **Unified ICM**, sub-skill groups are created when configuring the skill group priority. Each sub-skill group creates a target ID in the Unified ICM database. This target ID is used by all **Unified ICM** processes during the real-time messaging. It is essential for PG to send constant real-time messages and reports to the Central Controller for each of the configured skill groups. The PG requires to save the reports on the disk so that they are available to the Central Controller at any time. These operations are demanding sometimes, when many Unified ICM skill groups are configured together.

If the number of ACD skill groups and skill group priorities is large, do not use sub-skill groups. This causes increased data flow between the PG and the **Central Controller**. When the sub-skill group is not configured, the PG reports the skill group peripheral number only. This is defined in the ACD to the **Central Controller** without the skill group priority. In this case, **Unified ICM** reports contain only the skill group defined by the ACD peripheral number.

Note This feature is applicable from ICM 6.0 SR7 and 7.1(2) with Avaya PG.

1. **Peripheral Configuration:**

   To avoid the base and sub-skill groups from being created, you must not have a skill group mask selected.

2. **Skill Group Configuration:** When configuring the skill group, do not select a skill group mask. The peripheral number is required to match the ACD skill group number without the skill group priority.

3. **Impact on Unified ICM Reports:**

   Table 5: Impact on Unified ICM Reports

Report Type	Impact
Agent Skill Group Half Hour	When you do not set up a skill group priority in **Unified ICM**, the **Agent Skill Group Half Hour** report adds all the statistics of the ACD priorities to a single skill group. If you set up the ACD priority in Unified ICM, the reports display the statistics for each priority.
Skill Group Half Hour	The reports display all the configured Unified ICM skill groups. This happens while using ACD priority, the **Unified ICM** reports display a skill group for each of the priorities configured (called **Unified ICM** sub-skill group) and one base skill group. When you use a skill group with no priority configured, the reports display one Unified ICM skill group configured for each ACD skill group.
Termination Call Detail	The **Termination Call Detail** for calls for the ACD skill groups with priority configured, contain the Unified ICM skill group. This is defined by the ACD peripheral number (base skill group).

4. **Migrating from Sub-skill Groups to Skill Groups with no ACD Priority Configured:**

   To migrate from sub-skill groups to skill groups with no ACD priority configured, remove Unified ICM sub-skill groups. To do this, complete the following steps:

   a. Remove all references to sub-skill groups in the router scripts and agent skill group membership.

   b. In the **Subgroup Mask** tab, in the **Skill Group Configuration** area, uncheck the Override peripheral default mask check box.

   c. In the Skill Group Mask tab, in the **Peripheral Explorer** configuration area, uncheck all the check boxes.

   d. Restart the **PG**s to reflect the change in the peripheral configuration.

5. **Impact on WebView Reporting:**

   After the sub-skill group migration, the base skill group reporting continues to work the same way and there is no impact on historical reporting.

   After the migration is complete, the sub-skill groups are not permanently deleted from the database and are available for historical reporting until they are permanently deleted. The sub-skill group records before the migration process was completed are available for historical reporting.

Available Hold Off Delay

The **Available Hold Off Delay** configuration parameter in the **Skill Group Explorer Tool** are set to the **Timed ACW** value on the **ACD** for this skill group.

Service-to-Skill Group Mappings

Since **VDN**s typically correspond to Unified **ICM** Services, the service-to-skill group mapping is equivalent to the skill groups used by the vector for the **VDN**. In order to ensure accurate call and agent reporting, be sure to include **all skill groups** used by the **VDN** in the service-to-skill group mapping for that **VDN**. Service-to-skill group mappings are made in the Service Member window of **Configure ICM**.

Agents

The **ACD**-to-**Unified ICM Agent** mapping is given as follows:

Table 6: ACD-to-Unified ICM Agent Mapping

Unified ICM Software	ACD
Agent	Agent
Agent Peripheral Number	Agent ID
Agent Extension	Agent's Physical Extension

Important The **PG** configures the agents dynamically. This is applicable for the **PG**s that are using **CMS**. The **Configure ICM** tool do not add them individually. For **CMS-less PG** installations, agents require to be configured by the **Configure ICM** tool. Further, agent skill group member assignments are required to be completed to match the switch configuration.

The **Agent Peripheral Number** is equivalent to the **ACD** Agent ID. The following considerations for CMS and non-CMS environments:

- For **CMS** configurations, agent configuration data is not required in the Unified ICM database.
- For CMS-less configurations, the agents must be configured in the **Unified ICM** database. This is done through the **Agent Configuration** window of **Configure ICM**.

Note In Unified ICM, issues with reporting and routing arises if the agent is not logged in a station before making and receiving calls.

Agent States

The Table 7: Agent State Definitions lists Avaya agent states and their definitions. Some agent states have an optional call direction, [IN/OUT], in case a call comes in or is initiated while in that state.

The Table 8: Unified ICM-Avaya Agent State Derivation shows how Unified ICM agent states are derived from the Avaya states.

Table 7: Agent State Definitions

Avaya Agent State	Definition
ACD IN/OUT	Agent is on an incoming/outgoing ACD call
DACD	Agent is on a direct agent ACD call.
ACW [IN/OUT]	Agent is bookkeeping, doing data entry, or is at any other work related to the previous call, and is not available to receive another ACD call. Includes times an agent is on incoming and outgoing calls during ACW. If on a call, IN/OUT specifies the call direction.
DACW	Agent is in the ACW state for a direct agent ACD call.

AUX [IN/OUT]	Agent is doing non-ACD work, on break, or in a meeting. Agents initially log in AUX mode until they AUTO-IN or MANUAL-IN. Includes times an agent is on incoming and outgoing calls during AUX. Agent is not available to receive an ACD call. If on a call, IN/OUT specifies the call direction.
AVAIL	Agent is available to receive calls.
RINGING	Call is ringing at the agent's extension.
OTHER	Agent is doing other work. For example, there can be many such scenarios where: • The call is on hold • The agent is dialing to call • Access a feature • The agent is handling a personal call • DACD is ringing with no answer
UNKNOWN	Agent is in an unknown state (for example, when CMS link to G3 switch is not operational).

Table 8: Unified ICM-Avaya Agent State Derivation

Unified ICM Agent State	Derivation from Avaya Agent States
Logged_On	Logged_In
Logged_Off	Logged_Out
Ready	All states other than AUX and UNKNOWN
Available	AVAIL
WrapUp	ACW, DACW
TalkingIn	ACD-IN, DACD
TalkingOut	ACD-OUT (not in AUX)
TalkingOther	AUX IN/OUT, ACW IN/OUT
Other	OTHER

Note: Support for **AUX** reason code change in Not Ready state is available from ICM 8.5(3) onwards.

Skill Group Members

For CMS-less configurations, the agent skill levels for their logged-in skill groups can only be determined via Unified ICM configuration. That is, Avaya does not yet provide skill level information over the CTI link for agent logins. Therefore, you must preconfigure and associate the agent with the correct subgroup in order to properly identify the agent's skill level.

Translation Routes

Translation routes are supported on the Avaya PG. Translation routes can be used to pass caller information to the Avaya (for example, ANI or Network CED

No special Unified ICM configuration is required for the Avaya.

Routes

A Unified ICM Route is one or more Unified **ICM Peripheral Targets**. A Unified **ICM Peripheral Targets** is a Network Target identified by a trunk group and **DNIS** that terminate on the Avaya. A Peripheral Target is equivalent to the combination of **DNIS** (**VDN** extension or **Hunt Group** extension) and the trunk groups through which the incoming calls arrive.

No special Unified ICM configuration is required for the Avaya.

Routing Client

The Routing Client Configuration Parameters field requires to be null-terminated. The field delimiter, -DEFROUTE, are specified.

Order and case are not significant. However, all fields are separated by spaces. The following example shows a default Post-Route (Avaya Extension) to be used if the PG does not get a route response from the Router, for a reason:

```
DEFROUTE 3214
```

If a default route is not configured, the PG gives a negative acknowledgement (NAK) to the Avaya causing vector processing to proceed. The NAK may be the desirable action, depending on how the Avaya vectors are written.

Unified ICM Configuration for “CMS-less” PGs

In a PG configuration that does not use **CMS**, some additional configuration is necessary in Unified ICM software. Each of the following changes can be made by using the Configuration Manager's **PG Explorer tool**.

- You must set up **all agents** in the Unified **ICM** database.

- You must map agents to skill groups in the Unified **ICM** database. The agent-to-skill group mapping must match the **Avaya** configuration. In addition, the subgroup must correctly map to the agent's priority.
- You must set up monitored instruments in the **Peripheral Monitor** table of the Unified **ICM** database. Agent stations are monitored.
- You must set up Peripheral Targets in the Unified ICM database for all VDNs through which monitored calls flow.

Maintaining Your Configuration

It is preferred that changes made to your configuration are accomplished on the **Avaya/CMS** and in the **Unified ICM** database consecutively. This ensures that the PG gets the configuration updates on the Avaya/CMS systems.

It is imperative that the **Avaya**, **CMS**, and the **Unified ICM** database configurations are kept synchronized (that is, up-to-date with each other). Inaccurate or incomplete data results in inaccurate agent or call data.

Registry Keys

This section provides the usual values for the **ESCPIM** dynamic registry keys and PIM config registry keys.

The usual values for the **ESCPIM** dynamic registry keys are:

- *BriCheckMeters* = 0 (for CMS), 1 (for CMS-less)

  This value indicates whether the PIM regulate the **ASAI/CTI** message rates or not. "1" indicates that it enables message metering (that is, throttle outgoing messages).

Note The dynamic registry field**BriMaxOutstandingMessages** is used along with **BriCheckMeters** registry field to indicate the number of outstanding ASAI/ CTI messages (that is, messages waiting for a response from the **CVLAN** Server). After the PIM has reached the maximum number of outstanding messages, it does not send messages until one pending **ASAI/CTI** message has been received.

Note During the startup of the PIM process, the PIM sends the **ASAI/ CTI** messages at a faster rate until the limit controlled by the **BriMaxOutstandingMessages** field. The high priority outgoing messages take precedence over the normal priority outgoing messages.

Note The PIM also uses message metering to ensure that it does not exceed the maximum number of active associations per CTI link (see the config registry field, MaxActiveAssocPerASAILink).

- *BriMaxOutstandingMsgs* = 100
- *SmartAgentStateTimer = 1800 (for CMS), 10 (for CMS-less)*
- *BriCheckMessageRates* = 0 (for CMS), 1 (for CMS-less)

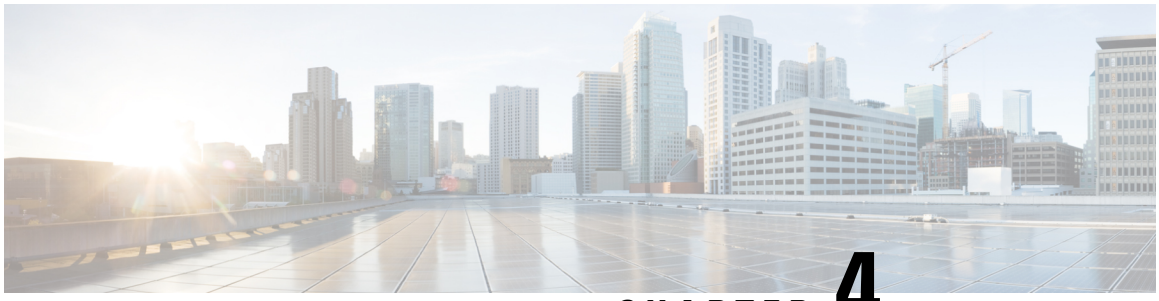
  This value indicated whether the PIM measures the ASAI/ CTI message rates or not. "1" indicates that the ASAI/ CTI message rates are measured.

  The usual values for the PIM config registry keys are:

- *MaxActiveAssocPerASAILink* key are set, depending on the version of *CVLAN server.* (The *MaxActiveAssocPerASAILink* refers to the maximum active association per CTI link)

CVLAN server	MaxActiveAssocPerASAILink
6.1.0	2048
8.2.1	4096
9.1	8192
AES Server	12000

Note It is not required to cycle (restart) the PG, for the changed dynamic registry values to be effective; however, for the changed config registries to be effective, you need to cycle the PG.



CHAPTER 4

CVLAN to TSAPI Migration

•
• Migration Overview, on page 51
• Important Considerations for Migration, on page 51
• Migrating CVLAN Interface to TSAPI Interface, on page 52
• Trace Bits to Troubleshoot TSAPI PG Issues, on page 53

Migration Overview

12.5(1) is the last supported release in the 12.5 release train for the Unified ICM peripheral gateway integration with Avaya Communications Manager using the ECS PIM / CVLAN interface peripheral gateway. Migrate your existing Avaya PGs from the CVLAN interface to the TSAPI interface. However, you are not required to reconfigure the skill groups, services, PGs, and agents for the Avaya PGs that you are planning to migrate.

Important Considerations for Migration

Consider the following before you migrate your Avaya PGs to the TSAPI interface:

- Ensure that you download the TSAPI client from the Avaya Support website or from the Avaya DevConnect website.
- Install the downloaded TSAPI client before you start the peripheral gateway service. For instructions about installing TSAPI client, see the Installing TSAPI Client , on page 40 section.
- Use the same interface type that is TSAPI for all the PIMs under the peripheral gateway.
- Secured TSAPI links are not supported.
- By default, TAESPIM supports up to a maximum of ten-digit agent extension.
- TAESPIM can process the Universal Call Identifier (UCID) that is received from the switch when certain events such as service initiated, delivered, and so on, are triggered. The UCID is stored in the CallReferenceID column of the Termination_Call_Details table and is also added as Peripheral Variable 7.

Note To avoid reporting the UCID in the Peripheral Variable, set the value of the `DisableUCIDinPV` attribute to 1. You must create the DWORD registry under the PIM dynamic registry hive.

Let us take a conference call scenario as an example to see how Avaya reports the UCID and also how the UCID numbering model and the Computer-Supported Telecommunications Applications (CSTA) event call ID are arrived.

Conference Call	CSTA Event Call ID	UCID
Customer A calls an agent B.	1000	1
Agent B initiates a conference call to consult with the supervisor C.	1001	2
Agent B completes the conference call with the supervisor C and continues the call with the customer A.	1001	1

In this scenario, the call model for the CSTA event call ID is 1-2-2 and the call model for UCID is 1-2-1.

As other parties are added to the conference call and new calls are created, the original UCID 1 continues to survive and appears in all the conference event. Therefore, the UCID 1 is included in all legs of a conference call to tie them all together.

Migrating CVLAN Interface to TSAPI Interface

To migrate your existing Avaya PGs to the TSAPI interface:

Procedure

Step 1 Create TSAPI links on the Application Enablement Services (AES) server. See the *Follow the procedure to establish the TSAPI link:* section in Setting up the CVLAN and TSAPI Links on AES Server, on page 10.

Step 2 Create a CTI user in AES. The TSAPI PG uses this CTI user to connect to the AES server over TSAPI. See the *Add CTI User in AES* section in Setting up the CVLAN and TSAPI Links on AES Server, on page 10.

Step 3 In the **PIM Configuration** UI, switch the **Interface Type** option from **CVLAN** to **TSAPI** and enter the required details to finish the setup. See PIM Configuration, on page 36.

Step 4 Ensure that you have set up the peer side of the PG to use the TSAPI interface.

Step 5 Configure all post-route VDNs as dialed numbers in the Unified ICM configuration. This is to register the TSAPI PIM as the routing server for these VDNs. The PIM sends the route registration request to AES server for these dialed numbers. It also sends the registration request for translation route Dialed Number Identification Service (DNIS) configured in Unified ICM.

Trace Bits to Troubleshoot TSAPI PG Issues

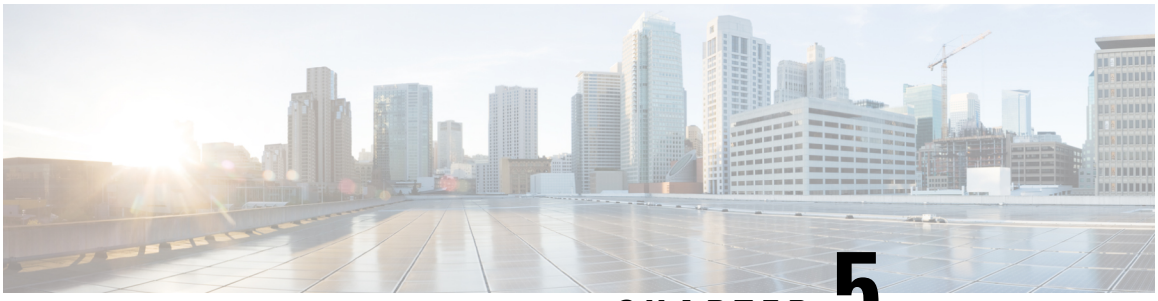
Use the trace bits in the TAESPIM procmon interface to troubleshoot TSAPI PG issues. To enable the trace bits, from the diagnostic framework, set the debug level to 3. The following is the list of trace bits:

Table 9: Trace Bits

Trace Bits	Description
monitor_unsolicited_msgs	Prints all the monitoring-related unsolicited events.
monitor_request_msgs	Prints all the monitor requests.
monitor_resp_msgs	Prints the successful confirmation or the universal failure of all the monitor requests from the switch.
value_query_request_msgs	Prints all the value query requests towards the switch.
value_query_resp_msgs	Prints the successful confirmation or the universal failure of all the value query requests.
tsapi_msgs	This is a high-level trace command that you must use along with the other trace commands at the TSAPILib-level.
tsapi_internal_msgs	Prints all the traces that are related to the interaction between the TSAPILib and the Avaya Client library.

Note All the TSAPI library-level traces are prefixed with [TSAPILIB] in the PIM logs. For example:

```
PG2B-pim1 Trace: [TSAPILIB] Succesfully connected to TSAPI Server
[AVAYA#ACM6ENV1#CSTA#AESENV2]
```



CHAPTER 5

Post-Routing

- Post Route Dial Number Registration for TSAPI Interface, on page 55
- Route Request, on page 55
- Route Select, on page 57

Post Route Dial Number Registration for TSAPI Interface

When **Avaya** PG uses **TSAPI** interface **PIM** gets registered as the routing server to post route the calls. Every time a new dial number is added to the **ICM** configuration, **PIM** sends a route registration request to the **AES** server. On confirmation, **PIM** acts as the routing server for that dial number.

Route Request

To initiate a post-route, the **Avaya** vector that is handling the incoming call must include an **adjunct route request** step with the correct **ASAI/CTI** extension specified.

A **wait time** is specified after the adjunct route request to allow for **Unified ICM** software to route the call. Although Unified ICM post-route destination decision is(virtually) instantaneous, a typical wait time of four to six seconds in the vector is appropriate. The wait time may require to be adjusted depending on anticipated call volumes.

Vector writers consider the state of the call, if **Avaya** cannot properly route the post-routed call, or if the CTI link is down. There can be a scenario, where the label (call destination) returned from the CallRouter is not valid. For example incorrect Trunk Access Code, extension destination is busied-out, Class of Restriction (COR) does not allow the call to complete. In this case, it is necessary for you to consider how you want the call to be handled.

Route Request Elements

The Avaya sends a route request to the PG containing the following Route Request Elements.

- Calling number (CLID)
- Called number (typically the VDN)
- User-user information (32 bytes maximum, where the data type is (a) user defined or (b) ASCII)
- Last set of Avaya collected digits (CED) (if any)

- Digit collection timeout (seconds)
- Call priority level (values: not_used, not_in_queue, low, medium, high, top)
- Interflow type (that is, cause of interflow; values: all, threshold, vector)
- Time (time the routed call is to spend in the queue before interflow)
- DNIS chars (optional)
- Call ID
- ·Trunk group number and trunk number (optional; mutually exclusive with calling number)
- UCID
- II - digits\Call Originator Information

Route Request Peripheral Variable Usage

If PIM is allowed Peripheral variable modification through **Call Control Variable Map**, the **Route Request** elements (such as **CLID** and Called Number) into **Peripheral Variables**. Unified **ICM** script writer can then use the information in the **Peripheral Variables** to create scripts that determine which destination best suits the caller's needs. All **Peripheral Variable** data types are ASCII.

The **Call Control Variable Map** field is available on the **Peripheral Configuration** window of the **Configure ICM** tool. This field controls the mapping of **Route Request Elements** to **Peripheral Variables**.

Call Control Variable Map

The **Call Control Variable Map** fields are used to configure the peripheral variables, which are reserved for a **CTI** application. These fields are used by the **PG**. There are (two) ways, by which you can control the variable usage through the **Call Control Variable Map** field:

- Direct the **PIM**. The **PIM** can be directed on which call variables are accessed. For example, the following setting (made in the Call Control Variable Map field) allows the PIM to set call variable 1 and call variables 5 through 10. The call variables are set, while preserving the existing values of call variables 2 through 4 (which means that the PIM does not set call variables 2 through 4). This argument is from the perspective of the **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 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 details on **Unified ICM CTI** capabilities and interaction with the PG, see the ICM Software Enterprise **CTI Interface** Specification. The Route Select Peripheral Variable Map displays the **Peripheral Variable** numbers and the **Route Request Elements** which these numbers represent. It also displays the possible values contained in the **Route Request Elements**.

Table 10: Route Request Peripheral Variable Map

Peripheral Variable	Route Request Element	Possible Values
1	CallPriorityLevel	CP_UNUSED, CP_NOT_IN_QUEUE, CP_LOW, CP_MEDIUM, CP_HIGH, CP_TOP
2	InterflowType	IT_UNUSED, IT_ALL, IT_THRESHOLD, IT_VECTOR
3	TimeInQBeforeInterflow	ASCII char string (empty string if unused), units = Seconds
4	DNIS	ASCII char string (empty string if unused)
5	User-User Information	See Note 1.
6	CED	Caller Entered Digits (empty string if unused)
7	II - digits \ UCID	II - digits (ASCII form) (empty string if unused) **Note** In ECS PIM, Peripheral Variable 7 is set with II - digits. The TSAPI PIM is set with UCID.
8	Trunk Information	Format (if provided by switch): TrunkGroup Number, Trunk Number, Trunk Direction
9	Calling Number	If provided by switch (for example if on ISDN trunks or on-switch call)
10	VDN	Vector Directory Number

Note The **UUI** is limited to **ASCII** characters (null-terminated ASCII character string). That is, any non-ASCII UUI data received are not stored in the Peripheral Variable.

UUI data (ASCII and non-ASCII) is stored in the **Termination call Detail** table Unified ICM database. ICM Schema guide can be referred for more details.

Related Topics

Route Select Peripheral Variable Usage, on page 59

Route Select

The PG receives the selected route information from the Call*Router* and converts it to a Route Select message for the **Avaya**. The **Route Select** message can be used to set call attributes, request digit collection from the switch, provide dial-ahead digits to the switch for collection, or specify user-user information to be included in the call.

You can specify the **Route Select** functionality through the **Peripheral Variables** or the syntax used in the **Label**. Unified ICM script can be used to set the Peripheral Variable contents. Where the setting of Route Select functionality overlaps, the **Peripheral Variable** setting takes precedence. Refer to the **Avaya** documentation to determine when any of the Route Select features can be used. For example, it may not make sense to have call priority **ON** if the destination is a **VDN** or **Split**. As another example, direct agent calling does not make sense if the destination is a **VDN**.

Route Select Message

The Avaya Route Selection Message has the following elements:

- Destination route select. On-switch or off-switch called number.
- User-user information.

  This consists of:

  - DataType: (a) UU_TYPE_USER (user defined); or (b) UU_TYPE_IA5 (ASCII)
  - Length: number of bytes (40 bytes maximum)
  - Data

- Call priority (**ON** or **OFF**). If **ON**, this parameter represents a special type of call. This call carries three burst distinctive ringing. The call does not go to the covering point for coverage or send all calls.
- Direct agent call. This consists of:
  - Agent extension.
  - ACD Split extension, specifies the queue, to place the waiting call. The agent must be logged in to this split.
- **User data**. Used for digit collection or to specify dial-ahead digits:
  - **User data type**:

    1. **COLLECT** that specifies digits are to be collected
    2. **COLLECTED**, which specifies dial-ahead digits

    The PIM default is **COLLECTED**.
  - **Digit collection timeout (0-63 seconds)**: Specifies the number of seconds tone detector will continue to collect digits after the first digit is received. The **PIM** default is no timeout.
  - **Data**: If the user data type is **COLLECT**, this field is interpreted as a binary integer specifying the number of digits to collect. If the user data type is **COLLECTED**, this field is an ASCII string specifying the dial-ahead digits.
  - Use external **trunk identified by Trunk Access Code (TAC)**. The TAC can be prefixed in the called_number field.

Restrictions on Digit Collection

The **Avaya** restrictions that apply to digit collection include:

- Only incoming trunks of any type, including **ISDN**, **MFC**, and **R2MFC**, are eligible for ASAI/CTI-requested digit collection.
- Incoming disconnect supervision must be administered on the incoming trunk to allow a call prompter/tone detector to connect.

Route Select Peripheral Variable Usage

The PG maps the Peripheral Variables received in the CallRouter's Route Select message as shown in Table 9: Route Request Peripheral Variable Map. All Peripheral Variable data types are ASCII. Peripheral Variables 1-4 and 6-10 are unassigned and can be used for the Route Select elements shown in Label Syntax table.

Table 11: Route Select Peripheral Variable Map

Peripheral Variable	Route Select element	Possible Values
1-4, 6-10	Call Priority	CP_ON, CP_OFF (default).
1-4, 6-10	Digit Collection/Dial Ahead	See the topic Digit Collection/Dial Ahead for more information.
1-4, 6-10	Trunk Access Code	See the topic Trunk Access Code for more information.
5	User-User Information	See the topic User-User Information for more information.

A Peripheral Variable can only be used for one Route Select element at a time. If a **Peripheral Variable** syntax is invalid or the **Peripheral Variable** is an empty string, the **Peripheral Variable** is ignored. The only fixed **Peripheral Variable** is PV 5, that is designated for UUI.

Digit Collection/Dial Ahead

The Digit Collection/Dial Ahead peripheral variable string has the following syntax:

```
COLLECT NUMBER_OF_DIGITS_TO_COLLECT TIMEOUT DIGIT_COLLECTION_TIMEOUT
```

or

```
DIAL DIAL_AHEAD_DIGITS
```

COLLECT, TIMEOUT, and DIAL are keyword delimiters and must be specified as shown (case is not important). The fields *NUMBER_OF_DIGITS_TO_COLLECT*, *DIGIT_COLLECTION_TIMEOUT*, and *DIAL_AHEAD_DIGITS* are supplied by the customer. Some points to remember are:

- The number of digits to collect must be between one (1) and 24, inclusively.
- All fields are separated by spaces.
- Every # and * count as one digit each.
- The digit collection timeout must be between one (1) and 31, inclusively.

The following example indicates that four digits are collected with a digit collection timeout of ten seconds:

```
COLLECT 4 TIMEOUT 10
```

The next example indicates that the digits 3, 2, 1 precedes the route selection:

```
DIAL 321
```

With proper configuration using translation routes, the DIAL syntax can allow you to provide the caller's ANI (or any set of digits) to the **Avaya**. Afterwards it is displayed on an agent's console.

Trunk Access Code

The **Trunk Access Code Peripheral Variable** has the syntax:

```
TAC TRUNK_ACCESS_CODE
```

TAC is a keyword delimiter and must be specified as shown (case is not important). The **TRUNK_ACCESS_CODE** field specifies a valid T**runk Access Code** extension for the **Peripheral**. The **TAC** can also be pre-pended in the Label. All fields must be space separated.

The following example indicates a **Trunk Access Code** of 111 for the route selection:

```
TAC 111
```

User-user Information

This is a null-terminated ASCII character string. The **UUI** data is stored in **Peripheral Variable** 5 for both the Route Request and Route Select messages only if the protocol format of the UUI data is C_UU_IA5. Therefore, unless modified, all UUI data received for a call are included when sent to the calls' destination. UUI data is limited to 40 bytes.

Avaya PIM was designed to support the User-to-User information (UUI) up to 32 bytes inline with the older switch version support, which was 32 bytes.

ASAI supports UUI up to 96 bytes for **Avaya CVLAN Server** Release 8, and link version 4 and beyond.

With this enhancement **Avaya PIM** supports 40 bytes for the UUI field.

Label Syntax

The **Unified ICM Label** can be used to specify additional Route Select[1] functionality. Incorrect or incomplete Route Select data may result in the **Avaya** denying the Route Selection and proceeding with vector processing.

A special label type to support the incorporation of dial-ahead digits into the label is supported. The string **DTMF** within the label indicates the presence of these dial-ahead digits.

The format of this label type is as follows:

```
XXXXXDTMFYYYYY
```

The XXXXX is required and is the destination where the post-routed call are directed. YYYYY, maximum 16 digits (can include * and #), are included as dial-ahead digits when the route response is sent to the switch for the post-routed call. This label type can be used for post-routed or translation-routed calls. A label using this special label type cannot use any of the other special label formatting capabilities listed in the following table Table 11: Label Identifiers and Capabilities. Peripheral Variables can still be used.

Table 12: Label Identifiers and Capabilities

Label Identifiers	Definition	Example
!	An exclamation point at the beginning of the label indicates that **Call Priority** are turned ON. The default is Call Priority OFF. See Note 1	!1234 indicates that the call directed to extension 1234 has call priority ON.

Label Identifiers	Definition	Example
@	The “at” sign (@) at the beginning of the label indicates that this is a **DACD** call. The call destination must be an agent’s extension. The default is No DACD call. (See Note 1.)	@2345 indicates that the call directed to the agent at extension 2345 is a DACD call. Because no agent group or agent group extension was specified in this example, the PIM attempts to select the first known agent group login for the agent. Both the agent and the destination agent group must have been previously known to the PIM for this to be successful.
&	The ampersand (&) used within the Label is used to specify the **Agent Group Peripheral Number**. The Agent Group Peripheral Number must immediately follow the ampersand and must be configured in Unified ICM software. The **PIM** determines the correct Agent Group extension.	@2345 &11 indicates that the call directed to the agent at extension 2345 is a **DACD** call and the agents group number is 11. Using the Agent Group Peripheral number may be convenient if the agent group extension is changed anytime.
#	The pound sign (#) used within the Label is used to specify the **Agent Group Extension** number. The **Agent Group Extension** must immediately follow the pound sign. The Agent must be a logged-in member of that agent group.	@2345 #1000 indicates that the call directed to the agent at extension 2345 is a DACD call and the agents’ agent group extension is 1000.
%1 %2 ..... %10	The percent sign ‘%’ at the beginning of the label indicates that the call destination is contained in the specified **Peripheral Variable** number. See Note 2	“%1” indicates that the call destination is contained in Peripheral Variable 1 (PV1). This is useful if you want to specify the destination in the PV’s or to place CEDs in a PV as a destination.

Note

1. All Label Identifiers can be used together unless otherwise noted. Label Identifiers designated to be at the beginning of the label cannot be preceded by any digits. For example, "!%1" indicates a Priority call to the agent specified in Peripheral Variable 1.
2. Peripheral Variable 5 is reserved for User-User Information (UUI) only

[1] ICM 5.0 SR13 supports star (*) as a valid routing label for translation routing and post-routing in Avaya PIM. For example, *173001 is a valid routing label where *17 can be the Trunk Access Code and 3001 indicates the extension/VDN to which the call would be directed. The post-route label containing the star (*) character is configured in Service explorer.

Network Take-Back and Transfer Support

The Adjunct Switch Application Interface (ASAI) provides messages to enable an application (for example, the PG) to take advantage of the Network Take-Back and Transfer feature. The message set enables a host to generate a transfer call request to the carrier. Unified ICM customers currently perform the following actions when transferring inter-switch calls using Unified ICM Enterprise Routing:

1. An agent receives an inbound call.
2. The agent begins a consultative call (#8XXX or speed dial #), which results in a new call in a VDN that performs a Post-Route Request.
3. The Unified ICM response to the Post-Route request is either of the following:
   a. A VDN that targets another Switch using tie lines between ACDs.
   b. A VDN that targets agent groups locally on the requesting ACD.
4. The agent then consults with the target agent and either conferences or transfers the call.

When inter-switch transfers are performed, the ACD requires trunk lines between all targeted ACDs.

The following steps are performed when transferring inter-switch calls using the Network Take-Back and Transfer feature:

1. An agent receives an inbound call.
2. The agent then starts a consultative call (#8XXX or speed dial #). A new call get initiated owing to the consult call, that executes a vector that performs a Post-Route Request.
3. Unified ICM response to the Post-Route request is a label of the form DTMF*8xxxxxxxx or DTMFD*8xxxxxxx. The DTMF and DTMFD prefix in the label informs the PIM that it must perform a Carrier Call Transfer.

PIM performs the following steps for Carrier Call Transfer:

1. The PG terminates or clears the consultative call that performed the post-route request by issuing a ClearCall Request.
2. When the PG receives a Clear Call confirmation response for the consult call disconnecting, the PG connects back the initial call that was placed on HOLD with the customer, by issuing a Retrieve Call Request. The feature requires that the call stays in the connected state to execute the Carrier Call Transfer.
3. When the PG receives the Retrieve Call Confirmation Response confirming that the call was retrieved and is in the connected state, the PIM issues the Send DTMF tone request with the digits received in the label from Unified ICM (the portion of the label string following the keyword DTMF / DTMFD).

   The DTMFD is similar to the DTMF prefix, except that DTMFD instructs the PG to disconnect the original call when the Send DTMF tone processing completes. This enables the PIM to clear the agent's association with the call if the DTMFD prefix is used (similar to a blind transfer case where the network clears the original call with the associated agent).

   The PIM currently uses the Clear Call Request and Retrieve Call Request for CTI Third-Party Call Control Interfaces. These enable hands-free transfer steps after initiating the consultative call.