Genesys

Genesys Voice Platform 8.1

Troubleshooting Guide

About Genesys

Genesys is the world's leading provider of customer service and contact center software - with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support. Before contacting technical support, please refer to the ***Genesys Care Program Guide*** for complete contact information and procedures.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide.***

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 81gvp_tg_12-2012_v8.1.601.00

Table of Contents

Preface

Welcome to the *Genesys Voice Platform 8.1 Troubleshooting Guide*. This document provides information about Simple Network Management Protocol (SNMP) traps, as well as basic troubleshooting information for the Genesys Voice Platform (GVP).

This document is valid only for the 8.1 release(s) of this product.

Note: For versions of this document created for other releases of this product, visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

This preface contains the following sections:

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 59.

About GVP

GVP is a group of software components that constitute a robust, carrier-grade voice processing platform. GVP unifies voice and web technologies to provide a complete solution for customer self-service or assisted service.

In the Voice Platform Solution (VPS), GVP 8.1 is fully integrated with the Genesys Management Framework. GVP uses the Genesys Administrator, the standard Genesys configuration and management graphical user interface (GUI), to configure, tune, activate, and manage GVP processes and GVP voice and call control applications. GVP interacts with other Genesys components, and it can be deployed in conjunction with other solutions, such as Enterprise

Routing Solution (ERS), Network Routing Solution (NRS), and Network-based Contact Solution (NbCS).

Intended Audience

This document is primarily intended for system administrators, technical support, partners, and customers who are deploying and troubleshooting small, medium, or large single-tenant Genesys Voice Platform (GVP) environments. This document assumes that you have moderate experience with GVP, either by having attended a Genesys University course, or having worked with Genesys Professional Services on the GVP system.

This document also assumes that you have a basic understanding of these topics:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications.
- Network design and operation.
- Your own network configurations.
- GVP basic operations.
- SNMP traps.

You should also be familiar with Genesys Framework architecture and functions.

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to Techpubs.webadmin@genesyslab.com.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, please contact Genesys Technical Support.

Before contacting technical support, please refer to the *Genesys Care Program Support Guide* for complete contact information and procedures.

Document Change History

This section lists topics that are new or that have changed significantly since the first release of this document.

Release 8.1.6

- Chapter 2, "Basic Troubleshooting," on page 15:
  - Added the section "Configuring Windows Server 2008 to Generate Core Dump Files" on page 23.
- Appendix A, "Troubleshooting Tools," on page 43:
  - Added the section "Improving Conference Performance" on page 44, which describes the option `[conference] gain_control_enabled`.
  - Added the section "Licenses" on page 45.
- Appendix B, "Frequently Asked Questions," on page 47:
  - Added the section "Calls Are Not Being Accepted" on page 49.
  - Added the section "CPU Usage Higher than Expected When Using Video" on page 50.
  - Added the section "Cluster Mode Connection Failure" on page 53.
  - Added the section "480 SIP Response Code (Event Pool Throttling)" on page 53.

Release 8.1.5

- The "Collecting Log Files" on page 15, "Collecting Dump Files" on page 21, and "Locating Installation Package Versions" on page 23 sections have been updated with information about the new component in this release; T-Server-CUCM to Media Server Connector.
- Additional FAQs were added to Appendix B on page 47.
- A new FAQ section was added to Appendix B: "T-Server-CUCM to Media Server Connector" on page 56.
- This release does not contain the PSTN Connector component. Only GVP 8.1.2, 8.1.3, and 8.1.4 releases contain the PSTN Connector component. See the *Genesys Migration Guide* for information about using PSTN Connector 8.1.4 with the GVP 8.1.5 release.

Release 8.1.4

- The "Collecting Log Files" on page 15, "Collecting Dump Files" on page 21, and "Locating Installation Package Versions" on page 23 sections have been updated with information about the new components in this release; Policy Server (PS) and MRCP Proxy (MRCPP).
- A new section, "Debugging CTI Connector and ICM Client" on page 26, has been added to Chapter 2 to describe how to debug the CTI Connector and the new Cisco ICM Client.
- A new FAQ was added to Appendix B, in the section, "Media Control Platform" on page 47.

- New FAQs were added to Appendix B, in the section, "Resource Manager" on page 52.
- Chapter 4, "How to View SNMP MIBs" on page 41 was added.

Release 8.1.2

- PSTN Connector information has been added in this release.
- Debugging Dialogic has been added to this release.
- The details of the SNMP traps and the SNMP MIB tables have been moved from this guide to the *Genesys Voice Platform 8.1 SNMP and MIB Reference* file.

Chapter

1 Troubleshooting Methodology

When troubleshooting an issue with your Genesys Voice Platform (GVP) solution, it is important to take a methodical approach in order to quickly identify and resolve the cause of the issue. Drawing conclusions too quickly and making undocumented changes to the system(s) can result in making the issue worse.

This chapter outlines a brief methodology that you can follow in order to troubleshoot issues that you might encounter with your GVP solution. This chapter contains the following sections:

Describing the Problem

The first and most important step in troubleshooting any issue is to clearly define the problem. Your problem description should be as detailed as possible and include the following information:

- A clear indication of your system's symptoms.
- How you discovered the issue. For example, did you receive an alarm from the system? Did a caller identify the issue(s)?
- When did the symptom first start to occur?
- Was GVP previously running without issues, and the problem recently started to occur? If yes, what changes did you make to the system? For example, did you deploy a new VoiceXML application or make some configuration changes?

- How often does the symptom occur? For example, does it occur on every call or intermittently?
- Can you isolate the symptom to a particular site, system, voice application, or other component?

Gathering Relevant Information

Once you have a clear description of the issue, you can start to gather relevant information to isolate and identify the cause of the issue. This might include the following information:

- Recent changes that you have made to the system or environment. These can include operating system updates or patches, system or network configuration changes, or voice application changes.
- A more detailed description of the symptom. If callers are experiencing the symptom, can more specific information be gathered? For example, callers might report that their calls were dropped. In this case, it would be useful to know which voice application they were calling, where in the voice application they were dropped, and where they were calling from.
- Steps to reproduce the issue. If the symptom is reproducible, what are the detailed steps you can follow to make it occur?
- Whether the symptom can be isolated to a particular site, system, or voice application. If it can, you should review the particulars of that site, system, or voice application and compare them to that of ones that are not experiencing the issue.
- You may need to capture various log files for later analysis.
- Network traffic capture (via Wireshark or some other tool).
- You may need to export the configuration of the system.

Note: See Chapter 2, “Basic Troubleshooting,” on page 15 for information on how to collect log files, capture network traffic, and export the system configuration.

Creating an Action Plan

You can now create an action plan to further isolate the issue based on the information you have gathered.

Document the steps you are going to follow, and then check them off as you complete them.

Keep a record of any changes you make to the system as you go, as well as any observations you make. It is very difficult to remember what you did after the fact, and this information might be critical in preventing future issues.

Implement any changes one at a time, because you may not know which change corrected the issue if more than one change is implemented at a time.

Verifying the Resolution

Once you have taken measures to correct the problem, you must properly test the system to ensure that the symptoms are no longer occurring.

Document what you expect to happen, and then compare your expectations with your written observations of the system during your tests.

If the symptoms continue to occur, restart this process from the initial problem description. Describe what is occurring now as it may not be the same as the initial problem, especially if you have made changes.

Chapter

2 Basic Troubleshooting

This chapter provides basic troubleshooting information for Genesys Voice Platform (GVP). It contains the following sections:

Collecting Log Files

Genesys recommends that you check and collect the logs when you are troubleshooting an issue.

Note: When a GVP process shuts down unexpectedly, check the snapshot file instead of the log file for the reason for the crash. The snapshot file contains the last/latest log information, so it might have logs that are more recent than the regular log file. The snapshot file is circular; you should check it for the latest time stamp.

Table 1 on page 16 provides the default location and name of log files for the GVP components.

Table 1: GVP Log Files

GVP Component	Location	Default Log File

Media Control Platform (MCP)	Windows:
	`<MCP Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<MCP>/logs`
		`mcp.<timestamp>.log`

Media Resource Control Protocol Proxy (MRCPP)	Windows:
	`<MRCPP Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<MRCPP>/logs`
		`MRCPProxy.<timestamp>.log`

Call Control Platform (CCP)	Windows:
	`<CCP Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<CCP>/logs`
		`ccp.<timestamp>.log`

Resource Manager (RM)	Windows:
	`<RM Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<RM>/logs`
		`ResourceMgr.<timestamp>.log`

Policy Server (PS)	Windows
	`<PS Installation Dir>\logs\`
	Linux
	`/opt/genesys/gvp/<PS>/logs/`
		`ps.log`

Fetching Module (FM)
Note: The FM functionality is part of MCP as of GVP version 8.1.2.
	Windows:
	`<FM Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<FM>/logs`
		`fm.<timestamp>.log`

CTI Connector (CTIC)	Windows: `<CTIC Installation Dir>\Logs\` **Note:** In 8.1.4 and later, the CTIC is supported on Windows and Linux.	`CTIConnector.<timestamp>.log`

Third-Party Squid (Optional)
Note: Squid is an open source product.
	Windows:
	`C:\squid\var\logs\`
	Linux:
	`/var/log/squid/`
		`access.log`

Table 1: GVP Log Files (Continued)

GVP Component	Location	Default Log File

Reporting Server (RS)	Windows:
	`<RS Installation Dir>\logs`
	Linux:
	`/opt/genesys/gvp/<RS>/logs`
		`rs.log`

Supplementary Services Gateway (SSG)	Windows:
	`<SSG Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<SSG>/logs`
		`SSG.<timestamp>.log`

PSTN Connector	Windows:
	`<PSTNC Installation Dir>\logs\`
	Linux:
	`/opt/genesys/gvp/<PSTNC>/logs`
		`PSTNConnector.<timestamp>.log`

T-Server-CUCM to Media Server Connector	Windows:
	`<UCMC Installation Dir>\Logs`
	Linux:
	`/opt/genesys/gvp/<UCMC>/Logs`
		`UCMConnector.<timestamp>.Log`

Note: The directory for logs can be changed from the default shown. A common practice is to create a folder named `Logs` and set it as the log location for each component (under `Options > Log` for that application). Name the log appropriately; for example, `RM_Debug.log`. This practice reduces the navigation through the OS when troubleshooting multiple components.

Exporting Configuration Options

Exporting configuration options and providing this information to Genesys Technical Support enables them to see how your platform is configured. You can export configuration options for any application from Genesys Administrator. For information on how to do so, see the *Framework 8.1 Genesys Administrator Help*.

You can also export IVR Profiles in the same manner, and you can export DN mapping data by exporting options of the `Tenant` object.

Another way to obtain configuration options is the local `.ini` file that GVP creates, which contains all of the configuration information read from Framework during startup. The `.ini` file is found in the

`<IP installation>\config` directory. The file name is `<application name>.ini` (for example, `MCP_jade_DITLoad.ini`), and the `<application name>` is the name of the application as configured in Framework.

Collecting Logs

Windows Event Viewer

You can access the Windows Event Viewer from `Control Panel > Administrative Tools`.

Some GVP components use the Event Viewer to log application event messages, which can then be accessed by clicking on the application file in the left pane of the Event Viewer GUI. The source of each Event Viewer message is the name of the executable program that is associated with the process that logs the event message. Processes such as the `pwcallmgr.exe`, `pwproxy.exe`, `resourcemanager.exe`, `ccpccxml.exe`, `CTIConnector.exe`, and `ssg.exe` use the Event Viewer to indicate problems that might occur during startup, before normal logging is available. In addition, the logging infrastructure used by `pwcallmgr`, `resourcemanager`, and `ccpccxml` might also use the Event Viewer to display special events that are related to GVP logging.

In the Event Viewer GUI, you can modify properties for the application file by clicking the application file > `Action` menu > `Properties`. The maximum log file size and filtering options are available through this `Properties` window. The location of the event file is also displayed.

For this release of GVP, only the Information event type is used by the GVP components.

RH Syslog

The default system log file on RHEL is `/var/log/messages`. You must have root privilege to read this file.

Collecting Data

Windows

This section describes the PerfMon counters, which enables you to check CPU and memory use. The PerfMon counters are detailed below:

- Process counters (`pwcallmgr.exe, ccpccxml.exe, ssg.exe, java.exe, resourcemgr.exe, CTIConnector.exe`):
  - % Processor Time
  - Working Set
  - Private Bytes
  - Handle Count
  - Thread Count
  - Virtual Bytes
- Memory counters:
  - Available Kilobytes
  - Committed Bytes
- Processor counters:
  - % Processor Time (choose `_Total from Select Instances From List`)
- LogicalDisk Counters (choose `_Total from Select Instances From list`)
  - Avg Disk Bytes/Read
  - Avg Disk Bytes/Write
  - Avg Disk Queue Length
- CPU time for the executable program. (This is a column in the Task Manager.)

Make sure the PerfMon data is written as a `.csv` file, not binary. The collection interval should be 15 seconds.

Linux

You can use the following commands to collect data:

- `top`—to monitor CPU and memory usage per process, and to monitor high level system CPU and memory usage (installed with Linux: `procps-3.2.3-8.9.i386.rpm` on RHEL)
- `sar`—to monitor detail system resource usage (installed with Linux: `sysstat-5.0.5-16.rhel4.i386.rpm` on RHEL)
- `gvpfd`—to monitor per process file descriptor usage

```
gvpfd source
$owner = "all";
$duration = shift;
$repeat = shift;
```

```
$logfile = shift;
$pattern = "/usr/local/phoneweb/logs/logProcess.txt";

sub trim($)
{
   my $string = shift;
   $string =~ s/^\s+//;
   $string =~ s/\s+$//;
   return $string;
}
sub tabify($)
{
   my $string = shift;
   $string =~ s/\s+//g;
   return $string;
}
print "Starting vgfd\n";
   print "Process Owner: $owner \n";
   print "Interval: $duration seconds \n";
   print "Repeat by: $repeat times \n";
   print "Log file: $logfile \n";
   open (LOGFILE, ">$logfile");
print LOGFILE
"TIME\tNumFD\tPID\tUSER\tPR\tNI\tCPU\tTIME+\tMEM\tVIRT\tRES\tSHR\tS\tCOMMAND
   for ($i=0; $i<$repeat; $i++){
   $ts = 'date +"%D %T"'; chop($ts);
   my @list;
   if ($owner eq "all"){
      @list='ps -A | grep -v PID | grep -f $pattern';
   }else{
      @list='ps -u$owner | grep -v PID | grep -f $pattern';
   }
   $index=0;
   while ($list[$index]){
      $list[$index]=trim($list[$index]);
      @token = split(/\s+/,$list[$index]);
      $pid = $token[0];
      $pname = $token[3];
      $numFD = 'find /proc/$pid/fd -not -type d | wc -l'; $numFD=trim($numFD);
      $top = 'top n 1 b | grep $pid | grep $pname'; $top=tabify(trim($top));
      print LOGFILE "$ts\t$numFD\t$top\n";
      $index++;
   }
   sleep $duration;
}
close (LOGFILE);
exit 0;
```

To initiate all three process, you can use the following script:

gvpmon source

```
echo "Starting gvpmon script"
```

```
N=$1
(( D=1+$2/$N))
rm -f ~pw/logs/sar.dat
nohup /usr/lib/sa/sadc $N $D /var/log/sar.dat >/dev/null &
nohup /usr/bin/top -d $N -n $D -b > /var/log/top.log &
nohup ./vgfd $N $D /var/log/fd.log >/dev/null &
```

It takes two arguments:

- `arg 1`—interval between each snapshot captured in seconds
- `arg 2`—number of snapshot to capture

The preceding scripts/programs require a super user privilege to execute. After creating the two preceding scripts, make sure that you add executable permission on them prior to running, by issuing:
`chmod a+x {script's filename}`

Checking Disk Space

Windows

Go to `My Computer` and take note of the free space under the `C` drive.

Linux

Use the `df -k` command or the `du .` command to check for disk space usage and availability.

Collecting Dump Files

This section describes looking for and collecting dump files for analysis.

Procedure:
Collecting dump files

Purpose: To collect dump files in Windows in the event of an unexpected exit of any of the components without any `.dmp` files generated.

Start of procedure

1. Log into the console of the machine.

You should see an error dialog box from Microsoft that states an error has occurred and asks whether you want to report it to Microsoft for the pwcallmgr.exe.

2. Click the option to view additional information, and click what will be sent to Microsoft.

   The location of an mdmp file and an hdmp file should be listed.

3. Back up these two files and send them to Genesys Technical Support.

End of procedure

Location of Core and Dump Files

Table 2 lists the location of core/dump files for each component.

Table 2: Core/Dump Files Per Component

Component	Operating system	File path
Media Control Platform	Windows	<MCP Installation Dir>\logs\pwcallmgr*.dmp file
	Linux	<MCP Installation Dir>\bin\core.* file
MRCP Proxy	Windows	<MRCPP Installation Dir>\logs\srmproxy*.dmp file
	Linux	<MRCPP Installation Dir>\bin\core.* file
Call Control Platform	Windows	<CCP Installation Dir>\bin\ccpccxml*.dmp file
	Linux	<CCP Installation Dir>\bin\core.* file
Resource Manager	Windows	<RM Installation Dir>\logs\resourcemgr*.dmp file
	Linux	<RM Installation Dir>\bin\core.* file
Fetching Module	Windows	<FM Installation Dir>\logs\pwproxy*.dmp file
	Linux	<FM Installation Dir>\bin\core.* file
CTI Connector	Windows	<CTIC Installation Dir>\logs\cticonnector*.dmp file
	Linux	<CTIC Installation Dir>\bin\core.* file
Supplementary Services Gateway	Windows	<SSG Installation Dir>\logs\ssg*.dmp file
	Linux	<SSG Installation Dir>\bin\core.* file
PSTN Connector	Windows	<PSTNC Installation Dir>\logs\pstnconnector*.dmp file

Table 2: Core/Dump Files Per Component (Continued)

Component	Operating system	File path
T-Server-CUCM to Media Server Connector	Windows	`<UCMC Installation Dir>\logs\ucmconnector*.dmp` file
	Linux	`<UCMC Installation Dir>\bin\core.*` file
Reporting Server	N/A	The Reporting Server (RS) is a Java-based product that does not produce dump files. Any errors produced by the RS are written to the log files under `<install dir>\logs`.
Policy Server	N/A	The Policy Server (PS) is a Java-based product that does not produce dump files. Any errors produced by the PS are written to the log files under `<install dir>\logs`.
Note: The Fetching Module functionality is part of MCP as of version 8.1.2.		

Configuring Windows Server 2008 to Generate Core Dump Files

A Windows Server 2008 R2 computer can generate core dump files when an application terminates because of both assertion failures and segmentation faults.

To enable this functionality, you must configure the Windows Server 2008 R2 computer to create core dump files using the registry.

To do so, see the following link:
http://msdn.microsoft.com/en-us/library/bb787181.aspx

In particular, the key `LocalDumps` does not initially exist; you must create it in the Registry.

Without that registry setting set, core dumps are *not* generated for both assertion failures and segmentation faults.

Locating Installation Package Versions

The GVP application log file will print the installation package version during process startup, or you can locate the version using the following procedures.

Windows

1. To locate the installation package (IP) version of your GVP system, right-click the GVP executable program:
   - Media Control Platform—`pwcallmgr.exe`
   - MRCP Proxy—`srmproxy.exe`

- Fetching Module (If installing GVP 8.1.0 or 8.1.1)—`pwproxy.exe`
- Resource Manager—`resourcemgr.exe`
- Call Control Platform—`ccpccxml.exe`
- CTI Connector—`cticonnector.exe`
- Supplementary Services Gateway—`SSG.exe`
- PSTN Connector—`PSTNConnector.exe`
- T-Server-CUCM to Media Server Connector—`UCMConnector.exe`

2. Go to the `Properties > Version` tab.
3. In the `Other Version Information` block, check the `File Version` value and report.

Linux

- Use the following command:

```
strings <GVP executable or .so> | grep '\$Id:' | grep 'Build:'
```

Example:

```
[pw@marsanne bin]$ strings pwcallmgr | grep '\$Id:' | grep 'Build:'
$Id: Media Control Platform: GVP 8.0 (Build: 8.1.001.10) $
@(#)$Id: GVP Common Lib: GVP Common Lib (Build: 8.1.001.01) $
[pw@marsanne bin]$ strings libCMSIP2.so | grep '\$Id:' | grep
'Build:'
$Id: Media Control Platform: GVP 8.0 (Build: 8.1.001.10) $
```

- You can also use the `ident` command:

```
ident <GVP executable or .so>
```

Collecting Packet Traces

Windows

Wireshark is a network protocol analyzer that you can use for analyzing network problems. You can download it from `Wireshark.org`.

After installing wireshark on your Microsoft Windows machine, you can perform the following actions.

Capturing Network Traffic

1. Open Wireshark.
2. To start capturing network traffic, go to `Capture` on the menu bar, and then click `Interfaces`. A window will open.

3. Click `Start` on the desired network interface. Wireshark will start capturing network traffic.
4. To stop capturing, go to `Capture` on the menu bar, and click `Stop`.
5. To save the captured packets, go to `File` on the menu bar, and click `Save As`. A window will open.
6. Enter a file name, and then click `Save` to save the file.

Note: The `Packet Range` option enables you to select a specific set of packets to save.

Creating a Packet Filter

Wireshark supports packet filters, which enables you to filter out unwanted packets. For example, the `sip || rtp` filter will display only SIP and RTP packets. You can click `Expression` to see more filter options.

Displaying VoIP Calls

Wireshark can look for VoIP calls from the captured packets. Go to `Statistics` on the menu bar and click `VoIP Calls`. A window will open with the list of VoIP calls.

Linux

1. Use the following command:

   ```
   dumpcap -i <interface-name> -w <output_file>.pcap
   ```

   If using RHEL5, use the following command:

   ```
   tcpdump -s 1500 -i eth0 -w /root/filename.pcap
   ```

2. Press `Ctrl + C` to stop and exit the capture.
3. You can then transfer the capture file to a Windows machine to view and filter it by using Wireshark software.

   For example—If `eth0` is the active interface on the machine with which the GVP component (such as MCP, CCP, or RM) is associated, the command in Linux would be the following:

   ```
   dumpcap -i eth0 -w gvpcapture.pcap
   ```

Running Test VoiceXML Applications

The MCP component of GVP includes sample VoiceXML applications, which are located in the following directory (for both Windows and Linux):
`<MCP_Installation_Dir>\samples\`

By using these sample VoiceXML applications, you can make a test call directly to the MCP by using the `NETANN` prompt and collect service (http://www.ietf.org/rfc/rfc4240.txt section 4) to troubleshoot the status of the MCP.

For example, in Windows or in Linux, if the MCP is running at the default 5070 SIP port and the installation directory is C:\Program Files\GCTI\gvp\MCP\, you can dial the following to the helloworld sample VoiceXML application from your softphone:

```
sip:dialog@<mcp_host_name>:5070;voicexml=file://C:\Program
Files\GCTI\gvp\MCP\samples\helloworld.vxml
```

Debugging VoiceXML Applications

Make use of the interaction level logs that are generated by the MCP. These logs provide details of the call execution.

Note: This only applies to GVP Next Generation Interpreter (NGI).

You can also use Composer for debugging applications.

Debugging CTI Connector and ICM Client

To debug issues with CTI Connector (CTIC) and Cisco's Intelligent Contact Management (ICM) Client, you might not require full logs but specific logs, such as, SIP messages and GED-125 messages.

To obtain these logs, use the following log configuration option and value:

```
[ems]logconfig.MFSINK option value in the format *|*|*
```

Where:

- The first * (asterisk) represents the log level and the valid values are 0-5.
- The second * (asterisk) represents the module ID.
- The third * (asterisk) represents the Universal Logon ID (ULID).

CTI Connector Modules

Three modules exist within the CTI Connector:

- CTIC Adaptor
- IVR Server Client
- Cisco ICM Client

To print logs that are associated with the CTIC Adaptor module; use a value of 171; For the ICM Client module, use a value of 173.

Examples

1. To obtain GED-125 message flows only, use the following value:

   *|173|1626,1637

2. To obtain SIP message flows only:

   ||1280

3. To obtain both GED-125 and SIP message flows, use the following values, appending them with the | (bar) symbol:

   |171,173|1626,1637||*|1280

Reserved ULIDs

Table 3 contains the ULIDs that are reserved for the CTIC Adapter and ICM Client.

Table 3: Reserved ULIDs

ULID	Configuration Option	Description
	CTIC Adapter	
1554	`CTICA_CALLFLOW_SIP`	
	ICM Client	
1626	`ICMC_MESSAGE_EXCHANGE_INFO`	All messages exchanged between CTIC & ICM.
1634	`ICMC_CALL_INFO`	Session-specific logs. For example, `OPEN/CLOSE`.
1637	`ICMC_SESSION_INFO`	Call-specific logs.

Printing a Call Statistics Summary to a Log File

Print a Call Statistics Summary to a log file by using the following configuration:

```
[CTIC]
LogMIBStatsInterval=180
```

Set this configuration option to `-1` to disable this feature. The default value is `180`. The minimum and maximum values for this option are `30` and `1800`, respectively.

See the following sample Call Statistics Summary:

Sample

```
Call Statistics Summary:
====================================================
              Total Calls = 28
              Total Calls Completed = 32
              Total Calls Failed AtCTI = 4
              Total Calls Failed AtGVPPlatform =
              Total Active Calls = 0
              Total Queued Calls =
              Total Bridged Calls =
```

```
              Total RouteResponses Received =
              Total Default Agent Number Received =
              Total NewCall Failed = 3
              Total RouteRequest Failed =
              Total SIP Calls/Legs = 52
              Total SIP Calls/Legs Answered = 48
              Total SIP Calls/Legs Rejected = 4
              Total SIP Calls/Legs Completed = 48
=====================================================
```

Debugging T-Server-CUCM to Media Server Connector

To debug issues with T-Server-CUCM to Media Server Connector, you might require specific logs, such as the call tracing and the media operations related to call leg.

To obtain these logs, use the following log configuration option and value:

`[ems]logconfig.MFSINK option value in the format *|*|*`

Where:

- The first * (asterisk) represents the log level, and the valid values are 0–5.
- The second * (asterisk) represents the module ID.
- The third * (asterisk) represents the Universal Logon ID (ULID).

To print logs associated with the T-Server-CUCM to Media Server Connector module, use `244` for the module ID. For example, to obtain the call establishment/teardown messages along with SIP message exchange, use the following:

`*|244|2441`

To get media operations related information, use:

`*|244|2442`

To troubleshoot specific calls, enable both of them as follows:

`*|244|2441,2442`

Debugging Dialogic

This section describes the basic steps for troubleshooting Dialogic, TDM and PSTN Connector issues.

TDM Troubleshooting

This section describes how to troubleshoot a telephony TDM issue.

1. Check the back of the Dialogic board for any red or yellow LED lights which might point to a Dialogic or Trunk issue.
2. Use the MIB Browser to:
   a. Check the PSTN Connector MIB table (`pSTNCBoardTable`) for any alarms. .

   Note: The D-Channel status will always show an error if you are not using ISDN.

   b. Check the PSTN Connector MIB table (`pSTNCPortTable`) for out-of-service ports.
   c. Check the PSTN Connector MIB table (`pSTNCCallSummaryTable`) for any abnormalities in the call counters.

For more information on the MIB tables, see the *Genesys Voice Platform 8.1 SNMP and MIB Reference* file.

You can also use the PSTN Connector Dashboard in Genesys Administrator to see the current status of Dialog board. For more information, see the *Genesys Voice Platform 8.1 User's Guide*.

Call Failure Troubleshooting

This section describes how to troubleshoot failed calls.

Busy Signal

There are two types of busy signal:

- Slow busy
- Fast busy

Slow Busy

A slow busy signal indicates a failure to connect to the PSTN Connector. When this occurs:

1. Determine which PSTN Connector is receiving the call and check the voice circuits on that server.
2. Check the voice circuits on the server. If you do not see all of the D and B channels, restart the Dialogic services. If the channels do not start, work with the carrier to determine if the problem is a circuit issue.
3. Refer the problem to the engineer in charge of provisioning phone numbers.

Fast Busy

A fast busy signal indicates a carrier failure; that is, the call is dropped somewhere in the Network Service Provider (NSP) network. To solve this problem:

1. Duplicate the error.
2. Contact the NSP, and ask them to help troubleshoot the issue by tracing the call using the time of call, the ANI, the number dialed, and the trunk which the call should be routed.

Dead Air

Dead air is the lack of dial tone or busy signal. It suggests that a call was delivered successfully to the platform, but the call failed before connecting to the voice application.

If dead air is occurring, or a call returns dead air, make a test call and check for `All Ports Busy` trap.

PSTN Connector-Specific Issues

An inbound call to PSTN Connector can fail in the following scenarios:

- The inbound port is down, and the call cannot be delivered to the platform.
- The PSTN Connector process is stopped, and it cannot accept calls.
- A port is in a disconnect state, so calls fail to be accepted on the port.

When one of these failures occurs, it can result in dead air or a busy signal. To determine the source of this problem, make a test call and note whether or not the call is delivered to the PSTN Connector.

To solve these call failures:

1. Determine the PSTN Connector on which the calls should be landing.
2. If the failures are intermittent, isolate the servers on which the calls are failing. Make multiple calls, and make note of the servers on which the calls are serviced correctly, and the servers on which they are not received.
3. After you have isolated the server or servers that are not operating correctly, determine whether all the ports on the server have the `In Service` status.
4. If a port displays the `Out Of Service` status, reset the port. If the port does not come back into service, stop and restart PSTN Connector gracefully; that is, so that it waits for all the active calls to complete. If the ports are still marked as `Out Of Service`, restart the server.
5. If a port is in a `Disconnect` state:
   a. Stop the PSTN Connector gracefully. This will not enable the PSTN Connector to exit.

b. When all of the active calls have been completed, stop the `PSTNConnector.exe` process, and restart it.

6. If the port is `In Service,` make a test call to the maintenance number of the port in question, and determine whether the maintenance number is working.
7. If the maintenance number is working correctly, there may be a routing problem with the carrier for this number. Contact the carrier for assistance.
8. If the maintenance number is not working, reset the port and test the maintenance number.
9. If the maintenance number is routing correctly, and the maintenance call is still not working, contact the carrier for assistance.

Note: A slow busy signal indicates a problem with the server. A fast busy signal indicates a routing problem with the carrier.

PSTN Connector Restart

On the PSTN Connector, in certain scenarios, if there is an unexpected shutdown, it is possible that the Dialogic firmware end up in an inconsistent state, which would affect subsequent calls.

To recover from this situation:

1. Use Genesys Administrator to shut down the PSTN Connector.
2. Use DCM to shut down the Dialogic services.
3. Use DCM to restart the Dialogic services.
4. Use Genesys Administrator to start the PSTN Connector.

Dialogic Diagnostic Tools

Dialogic SR 6.0 includes several useful diagnostic tools. Most of the tools run only on the DM3 series boards. All Dialogic tools are located in the `\Dialogic\bin` directory.

- `PSTNDiag`—A GUI tool used for checking board, trunk, and channel status.
- `CASTrace`—A command line tool used to trace CAS signaling bits.
- `ISDNTrace`—A command line tool used to trace the ISDN D-Channel.

For more information on the tools, see the following documents provided by Intel:

- *Intel Dialogic System Software for DM3 Architecture Products on Windows*
- *Dialogic Universal Hardware Diagnostics Guide*

Genesys

Chapter

3 Troubleshooting with Composer

You can troubleshoot voice application errors by using Composer. The errors that are described in this chapter will appear in the call-trace view of Composer. When you start a call through Composer, a window automatically appears that contains the call traces. You can then check the call traces to obtain information about the Genesys Voice Platform (GVP) configuration and other issues.

Note: All of the example logs that are shown in this chapter are interaction level logs.

Select `Windows->Show View->Call Trace` to open the call trace window manually if required.

This chapter contains the following sections:

HTTP 503 Error

Check the traces for an error that is similar to the following:

For DTMF Grammar:

```
event error.badfetch.http.503:1|HTTP error response 503 [Target:
   http://10.10.30.80/vggrammarbase/inlinetmp/3-181105937.grxml]
event_handler_enter:error.badfetch|http://10.10.30.235:8080/Test05042008/src-gen/Main.v
   xml
log com.genesyslab.quality.failure:error.badfetch event terminated session
prompt
prompt_play audio|builtin:default_audio/the_requested_page_cannot_be_found.vox
fetch_end Fail (HTTP error response
   503):http://10.10.30.80/vggrammarbase/inlinetmp/1-181105937.grxml
fetch_end Fail (HTTP error response
   503):http://10.10.30.80/vggrammarbase/inlinetmp/5-181105953.grxml
prompt_play audio|builtin:default_audio/goodbye.vox
prompt_end done
event_handler_exit:error.badfetch
```

For Speech Grammar:

```
input_end ERROR|||||
event error.badfetch:1|
event_handler_enter:error.badfetch|file:///c:/VoiceGenie/mp/samples/helloasr.vxml
log com.voicegenie.quality.failure:error.badfetch event terminated session
prompt
prompt_play audio|builtin:default_audio/the_requested_page_cannot_be_found.vox
```

The preceding errors indicate that something is incorrect with the IIS settings on the Media Control Platform (MCP). Verify the following items:

1. Verify that IIS is running.
2. Verify that the `vggrammarbase` virtual directory is present and pointing to the `<MCP_INSTALL_PATH>\grammar\inlinetmp` folder.
3. Verify that the MIME type for `vggrammarbase` is configured properly.

No TTS Resource

The following example indicates that one of these scenarios might be occurring:

1. The TTS server is down.
2. The TTS server is not configured for the MCP.

3. The license has expired for the TTS server.
4. The TTS server is overloaded.

Example:

```
prompt_play tts|<?xml version="1.0" encoding="UTF-8"?><speak version="1.0"
   xmlns="http://www.w3.org/2001/10/synthesis" xml:lang="en-US">Welcome to the Composer
   Voice User Input Demo Press one for input I D, two for message, three for input
   grammar</speak>
exec_error Could not play audio <?xml version="1.0" encoding="UTF-8"?><speak
   version="1.0" xmlns="http://www.w3.org/2001/10/synthesis" xml:lang="en-US">Welcome
   to the Composer Voice User Input Demo Press one for input I D, two for message, three
   for input grammar</speak>
prompt_end error
input_end ERROR||||
```

No ASR Resource

The following example indicates that one of these scenarios might be occurring:

1. The ASR server is down.
2. The ASR server is not configured for the MCP.
3. The license has expired for the ASR server.
4. The ASR server is overloaded.

Example:

```
prompt_end asrbargein
prompt_play tts|<?xml version="1.0" encoding="UTF-8"?><speak version="1.0"
   xmlns="http://www.w3.org/2001/10/synthesis" xml:lang="en-US">Welcome to the Composer
   Voice User Input Demo Press one for input I D, two for message, three for input
   grammar</speak>
input_end ERROR||||
asr_trace ASR_NORESOURCE:results:<Error>
event error.noresource.asr:1|
event_handler_enter:error.noresource.asr|http://10.10.30.235:8080/Test05042008/src-gen/
   Main.vxml
log com.genesyslab.quality.failure:error.noresource.asr event terminated session
prompt
prompt_play audio|builtin:default_audio/sorry_there_is_no_asr_resource_available.vox
prompt_play audio|builtin:default_audio/goodbye.vox
prompt_end done
event_handler_exit:error.noresource.asr
```

Debug Call Failed

If the error that is shown in Figure 1 appears, one of following scenarios might be occurring:

- The GVP MCP/Resource Manager (RM) is stopped.
- The wrong IP address and/or port is specified for the MCP/RM.
- Debugging is not enabled on the MCP.

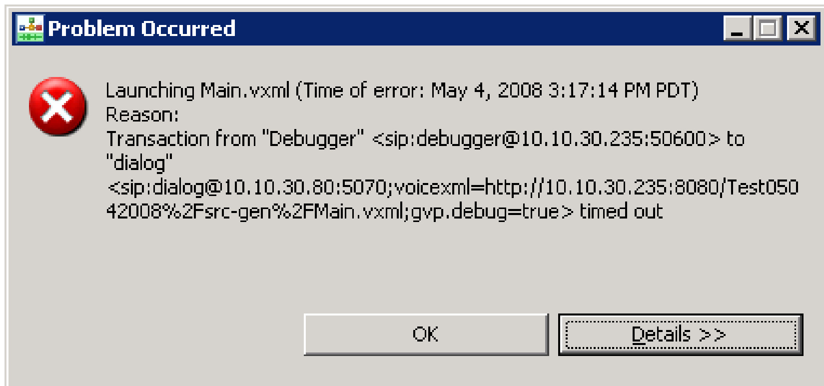

Figure 1: Problem Occurred Dialog Box

The error that is shown in Figure 2 indicates an incorrect port. For example, instead of a request being sent to the MCP/RM, it is being sent to the SIP Server.

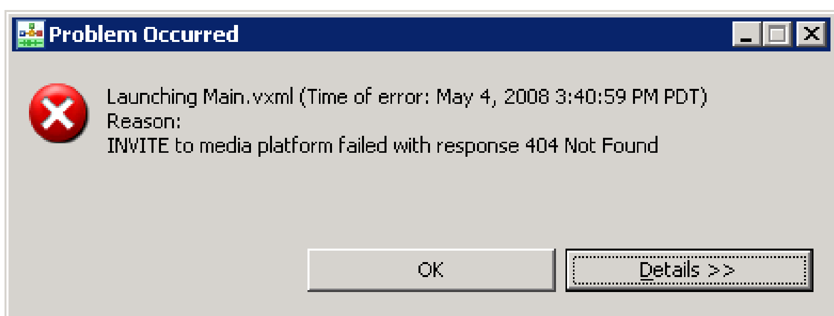

Figure 2: Problem Occurred Dialog Box

The error that is shown in Figure 3 on page 37 indicates an incorrect IP address and/or port number of the SIP phone.

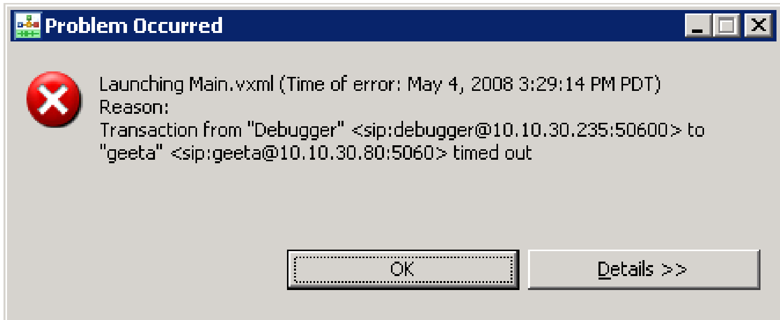

Figure 3: Problem Occurred Dialog Box

The error that is shown in Figure 4, along with traces that look similar to those shown in the example, indicates that you should check the Tomcat configuration on your desktop:

1. Make sure that the Tomcat preferences in Composer are configured correctly: Tomcat port number and administrator user/password.
2. Make sure that the `CV801Tomcat` Tomcat service is running.
3. If you are using some other server for a handcoded application, verify that the web application URL is valid and that the server is running.
4. Make sure the SquidNT service is up and running in the GVP installed machine.

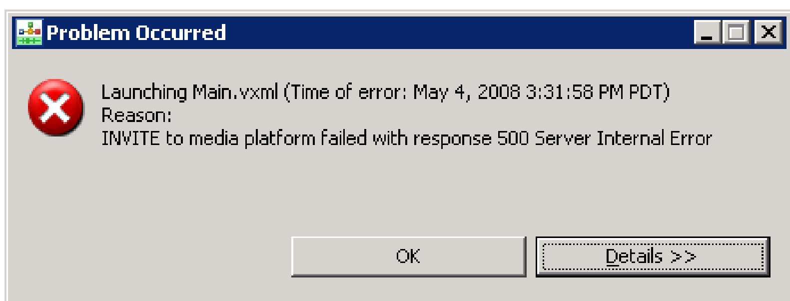

Figure 4: Problem Occurred Dialog Box

Example:

```
appl_begin
   INIT_URL=http://10.10.30.235:8001/Test05042008/src-gen/Main.vxml|DEFAULTS=file://C:\
   Program Files\GCTI\gvp\VP Media Control Platform
   8.0\MCP_dev-vm-geeta_8.0.004.01\config\defaults-ng.vxml|ANI=|DNIS=|PROTOCOLNAME=unde
   fined|PROTOCOLVERSION=undefined|CALLIDREF=08441b4de6dda90f05c220cfcd3d85d1@10.10.30.
   235|VXMLI_TYPE=NGI
wf_lookup http://10.10.30.235:8001/Test05042008/src-gen/Main.vxml
fetch_start document:http://10.10.30.235:8001/Test05042008/src-gen/Main.vxml
wf_lookup file://C:/Program Files/GCTI/gvp/VP Media Control Platform
   8.0/MCP_dev-vm-geeta_8.0.004.01/config/defaults-ng.vxml
```

```
fetch_start document:file://C:/Program Files/GCTI/gvp/VP Media Control Platform
   8.0/MCP_dev-vm-geeta_8.0.004.01/config/defaults-ng.vxml
fetch_end Fail (HTTP error response
   503):http://10.10.30.235:8001/Test05042008/src-gen/Main.vxml
wf_arrived s (memory):file://C:/Program Files/GCTI/gvp/VP Media Control Platform
   8.0/MCP_dev-vm-geeta_8.0.004.01/config/defaults-ng.vxml
appl_end
```

Stale Application Pages

The following example indicates that stale application pages are being picked. During the development mode, change the settings as shown:

1. For dynamic applications with jsp/aspx pages, set the `expires` immediately so that the latest copy of the pages is picked.
2. In production, upon redeploying the application, flush the Squid cache.
3. In the VoiceXML properties explicitly, set `documentmaxage=1s`.

Example:

```
appl_begin
   INIT_URL=http://10.10.30.235:8080/Test05042008/src-gen/Main.vxml|DEFAULTS=file://C:\
   Program Files\GCTI\gvp\VP Media Control Platform
   8.0\MCP_dev-vm-geeta_8.0.004.01\config\defaults-ng.vxml|ANI=|DNIS=|PROTOCOLNAME=unde
   fined|PROTOCOLVERSION=undefined|CALLIDREF=bc668983caef34cc5e4707d52c730b23@10.10.30.
   235|VXMLI_TYPE=NGI
wf_lookup http://10.10.30.235:8080/Test05042008/src-gen/Main.vxml
fetch_start document:http://10.10.30.235:8080/Test05042008/src-gen/Main.vxml
wf_lookup file://C:/Program Files/GCTI/gvp/VP Media Control Platform
   8.0/MCP_dev-vm-geeta_8.0.004.01/config/defaults-ng.vxml
fetch_start document:file://C:/Program Files/GCTI/gvp/VP Media Control Platform
   8.0/MCP_dev-vm-geeta_8.0.004.01/config/defaults-ng.vxml
wf_arrived s (memory):http://10.10.30.235:8080/Test05042008/src-gen/Main.vxml
```

CTIC Application Errors

The following example uses a CTIC operation, which throws an error event to indicate that the operation is not supported in the case of CTI using SIP Server.

Example:

```
eval_cond:{AppState.g_CTICCall == 'false'}=true
event error.com.genesyslab.composer.unsupported:1|AccessNumGet is not supported in case
   of CTI using SIPServer
event_handler_enter:error.|http://10.10.10.97:8080/JavaVoiceProj_CTIC/src-gen/AccessNum
   GetApp.vxml
log com.genesyslab.quality.failure:error event terminated session
```

Scenarios:

- Through `InteractionData`, you want to perform a `userdata delete` in CTI using SIPS scenario.
- Through `InteractionData`, you want to perform a `userdata deleteAll` in CTI using SIPS scenario.
- Through `InteractionData`, you want to perform a `userdata replace` in CTI using SIPS scenario.
- You want to perform a `Statistics PeekStatReq` or `GetStatReq` in the CTI using SIPS scenario.
- You want to perform an `AccessNumGet` in the CTI using SIPS scenario.
- Through `RouteRequest`, you set a transfer type to `consultation` in the case of CTI using SIPS scenario.

A receive error event is thrown to indicate when a `<receive>` operation fails and an error is reported by CTIC.

```
<genesys:receive maxtime="10s"/>
<if cond="isCTICResult(application.lastmessage$) == 'false'">
<throw event="error.com.genesyslab.composer.receiveerror" messageexpr="'The received
   message has invalid content-type.'" />
</if>
```

An operation timeout error event is thrown to indicate when a `<receive>` operation, which is executed in the context of a CTIC specific operation, times out.

```
<if cond="AccessNumGet1ResultReason == 'Timeout'">
<throw event="error.com.genesyslab.studio.operationtimeout"
   messageexpr="AccessNumGet1ResultReason" />
...
```

Chapter

4 How to View SNMP MIBs

This chapter describes how to view the SNMP MIBs by using a MIB browser. Genesys Voice Platform (GVP) components maintain status information and statistics in SNMP MIB tables. You can view and query these MIBs with an SNMP Management Console.

For a list of the GVP SNMP traps and SNMP MIB tables, see the *Genesys Voice Platform 8.1 SNMP and MIB Reference.*

Note: GVP Policy Server does not support SNMP MIBs or traps.

This chapter contains the following sections:

Viewing the MIBs

This section describes how to enable SNMP MIB browsing.

Prerequisites

- You must have already installed and configured the Genesys SNMP Master Agent. See the *Framework 8.1 Deployment Guide*.
- You must have already installed the GVP installation package VP MIB. See the *Genesys Voice Platform 8.1 Deployment Guide*.

Requesting Values

1. Install any MIB browser.
2. Import the GVP MIBs from the MIB installation directory, and have them compiled in the MIB browser that you have installed.

The GVP MIB component has two files: `GVP.mib` and `GVP-TRAPS.mib`. It is important that you compile the mibs in the following order:

a. Compile `GVP.mib` first.

b. When you are done compiling `GVP.mib`, compile `GVP-TRAPS.mib`. The `GVP-TRAPS.mib` has dependencies from the `GVP.mib` file and will create compilation errors if you compile it first.

Note: You cannot query and extract MIB data from any of the agents in which GVP is running unless GVP MIBs are compiled and imported into the MIB browser.

3. Configure the browser to connect to the Master Agent's `ip:port`.
4. Load the MIB from the VP MIB IP: Expand the tree, and select a leaf node—for example, `GVP-MIB > gvpApps > mcp > mcpScalarTable > mcpScalarEntry-mcpStartTime`.
5. Issue a `GETNEXT`. When correctly set up, the Master Agent will return a name/value/type—for example, `mcpStartTime.<MFDBID>, <some date+time>, OCTET STRING`.
6. To use `GET`, you will need to know the index variables (such as the MF DBID for scalar values) and append it to a node's OID. For example, select `mcpStartTime` and you will get `OID .1.3.6.1.4.1.1729.200.145.1.1.2`.

   To issue a `GET` with `MFDBID=100`, add `.100`, such that the OID is `.1.3.6.1.4.1.1729.200.145.1.1.2.100`.

   For a non-scalar table, you must append more values after the `MFDBID`.

Debugging

1. If you get a timeout, verify that the Master Agent is running and the `ip:port` of the MIB browser is the same as the `ip:port` of the `ServerInfo` in the Master Agent's Management Framework configuration.
2. If you receive a random value for `GETNEXT`, verify that the component being queried is running and has a connection to the Master Agent in the component's Management Framework configuration.

   You can also check if there is a port conflict by stopping the Master Agent and running it directly from Window's `Start` menu. The console will display that the ports were opened for listening.

Appendix

A Troubleshooting Tools

This appendix provides information about third-party tools that might be useful in assisting you with troubleshooting Genesys Voice Platform issues.

This appendix contains the following sections:

Wireshark

Windows

Wireshark is a network protocol analyzer that captures packets from a number of different devices. Although Wireshark supports over 700 protocols, for call flow analysis only, SIP and RTP are typically investigated. Wireshark is freeware and you can obtain it from the Wireshark website at `www.wireshark.org`.

See "Collecting Packet Traces" on page 24 for more information.

Linux

To collect network capture, log in as root user, and enter the following command:

```
tcpdump -s 0 > filename.cap
```

See `man tcpdump` for more information.

System Tools

Windows

The two Windows built-in tools available to monitor the system performance are PerfMon and Task Manager. You can use these tools for GVP troubleshooting by monitoring CPU usage, memory usage, and network traffic.

See "Collecting Data" on page 19 for more information.

Linux

Two Linux tools are available to monitor system performance. To see process related system information, you can use the `top` command. To see system level information, you can use the `sar` system tool to investigate system information.

Note: By default, Linux systems typically store seven days of system data taken in 10-minute intervals in the `/var/log/sa/` directory. The Linux System Administrator can modify the default or add their own system monitor settings.

Improving Conference Performance

Large conferences can achieve higher performance by disabling Conference Gain Control. But Genesys does not recommend doing so in the default configuration Conference Gain Control.

To enable Conference Gain Control, use the MCP option `[conference] gain_control_enabled`.

gain_control_enabled

Optional
Valid values: `true`, `false`
Default: `true`
Takes effect at: start or restart.

Set to `true` to enable conference gain control; various configurations used to set gain levels will be respected fully. Set to `false` to disable gain control; streams are muted for gains of `0`. Streams are unaffected for gains greater than `0`.

Nuance

You can test the SpeechWorks Media Server install by using the included `mrcpClient`, and you can test the Nuance Speech Server install by using the included `client`. Install the client on a Windows server and run the sample application from the command line. This generates an MRCP log output file, which you can compare to the log in the appendix of the Nuance installation manual. See the Nuance documentation for additional information about the clients.

Licenses

When Nuance Speech Servers are overloaded and are running out of licenses, they return the message `500 Server Internal Error` for any subsequent requests from MRCP Proxy or MCP—and the request fails.

Workaround: Provision your Nuance licenses based on the expected capacity of the deployment—the number of peak concurrent GVP ports that use ASR and TTS—so that the Nuance Speech Servers do not run out of concurrent licenses.

Softphone

Approximately 50 different softphones are available on the internet. You must have a sound card, microphone, and speakers to use in conjunction with a softphone. You can use a softphone to generate calls to the GVP IP environment to ensure correct call flow.

A commonly used variation is X-Lite, which is available from Counter Path, at `www.counterpath.com`. Another variation is SJphone, which is available from SJ Labs website; `www.sjlabs.com`. SJphone supports SIP and H.323 messaging.

The Kapanga Softphone variation is also used. It enables users to make phone and video calls, and send and receive faxes using any Voice over IP (VoIP) telephone provider. It is available from the vendor web site at www.kapanga.net.

Curl

Curl is a command line tool for transferring files with URL syntax. It supports FTP, FTPS, HTTP, HTTPS, GOPHER, and TELNET. It is useful for checking HTTP cache headers. Curl is available by default on the RedHat Linux system, or you can find this tool on the Curl website; `http://curl.haxx.se/`.

Example for returning only the HTTP Header:

```
C:\ Curl -I http://localhost/SampleApp/TestGrammar.grxml
```

Note: The `-I` is an upper case letter `i`.

Appendix

B Frequently Asked Questions

This appendix describes common issues with Genesys Voice Platform (GVP) components, and how to resolve them.

This appendix contains the following sections:

Media Control Platform

This section describes issues with the Media Control Platform (MCP).

RTP Not Played: Announcement Application on Linux

Problem

On Linux, a call flow in which an announcement is played prior to being transferred to an agent, does not play the announcement and the RTP stream does not show up in a Wireshark test.

Resolution

This issue might be due to an incorrect configuration in the `/etc/hosts` file, which can cause the MCP to send an incorrect IP address in the Session

Description Protocol (SDP). Some SIP phones filter RTP packets, based on the source IP address.

There are two parts to this resolution:

1. Avoid this issue by ensuring that the first line of the original `/etc/hosts` file is not changed.

   For example, you will see the following instructions in the file:

   ```
   # Do not remove the following line, or various programs
   # that require network functionality will fail.
   127.0.0.1 localhost.localdomain localhost
   ```

   This means that the line that begins with `127.0.0.1` must not be changed.

2. It is possible that the MCP server cannot resolve the hostname of other servers in the network. In this case, there are a few options:
   - If DNS is used, ensure that the MCP server is configured to use the correct DNS server, and that it can resolve the hostname correctly (recommended).
   - Configure the other network components to use the IP address instead of the hostname.
   - Edit the `/etc/hosts` file for Linux, at `C:\WINDOWS\system32\drivers\etc for Linux` to specify the mapping between the hostname and IP address.

     For Linux, you must still ensure that the first line in the `/etc/hosts` file is not modified.

Network Connection Problem: SocketError

Problem

When the Media Control Platform is under load, some calls are terminated due to an error when the network connection is created. The Media Control Platform log contains error messages that refer to `SocketError`.

Resolution

If this problem is found on Windows, ensure that you change the registry settings, as described in the section “Modify Windows Registry Settings”, see Chapter 5 in the *Genesys Voice Platform 8.1 Deployment Guide*.

On Windows, after a TCP connection is closed, the operating system does not release the TCP port for 240 seconds. The registry change reduces the timeout to 30 seconds to release the TCP ports sooner for new calls.

If the problem is not resolved after the registry change, increase the port range that is allocated for the connection that runs out of ports. The following port range configuration options are available for the Media Control Platform.

- `[stack]connection.portrange`

- `[vrm]rtp.portrange`
- `[vrm]client.mrcpv2.portrange`
- `[mpc]rtp.portrange`
- `[mpc]rtsp.connection.portrange`
- `[mpc]rtsp.rtp.portrange`

Conference Video Mixing Does Not Work

Problem

When attempting conference video mixing, the calls end immediately upon joining the conference or the video is not mixed.

Resolution

Confirm that the video transcoders corresponding to the conference participant video codecs are enabled (H.263 and/or H.264) in the `[mpc]` transcoders configuration.

Video Text Overlay does Not Work

Problem

Video text overlay does not work, either by not displaying any text overlayed on the video, or by throwing an error in the application.

Resolution

Confirm that the video transcoders corresponding to the video file being played and the video codec negotiated are enabled (H.263 and/or H.264) in the `[mpc]` transcoders configuration.

If this does not resolve the issue, check that the font file you want to use is located in the directory specified by `[mpc] font_paths_linux` (for Linux) or [mpc] font_paths_win (for Windows).

Calls Are Not Being Accepted

Problem

SIP calls are not being accepted, and the `100 Trying` message is not being sent.

Resolution

Confirm that the firewall for your machine allows traffic on all SIP related and media related ports.

Media Files Are Slow to Start Playing

Problem

Media files (in particular large ones) are slow to start playing.

Resolution

If the files are large (as can be the case with video files), it is possible that the files are being fetched multiple times, and are not being cached. Try increasing the values on `[fm] cachemaxsize` and `[fm] cachemaxentrysize`, with `[fm] cachemaxentrysize` being larger than the file being played, and `[fm] cachemaxsize` being increased in similar magnitude to the increase done for `[fm] cachemaxentrysize`.

If this change does not resolve the issue, try separating the video file into smaller size files.

CPU Usage Higher than Expected When Using Video

Problem

MCP CPU usage is higher than expected when video calls occur, while all participants are using the same video codec.

Solution

If all users are using the same video codec and the same profiles and levels when relevant, disabling the video transcoders can improve performance, since the MCP may be performing bitrate or framerate adjustments as is requested by the negotiated codecs. Even though this adjustment is desired based on the negotiation, it does require additional CPU resources to perform, and may not be explicitly required by the clients. Removing the transcoders can be done by removing H263, H264 and VP8 from [mpc] transcoders and restarting the MCP, or, adding `gvp.config.mpc.disabledtranscoders=H264 H263 VP8` to the relevant IVR Profile.

Note: This will disable text overlay, mixed video conferencing capabilities, track cache abilities for the video, and video transcoding between codecs and different profiles and levels will not work.

Reporting Server

This section describes issues with the Reporting Server (RS).

Internet Explorer Error: Web Page Cannot Be Found

Problem

The RS returns HTTP errors in numerous situations, such as when the report URLs or parameters are malformed, or when data is not available to fulfill a given report request. In such cases, the HTTP response has error code `400`, and contains a human-readable error message.

By default, in Internet Explorer (IE), an HTTP response with error code `400`; however, results in IE displaying a page with the text `Web Page Cannot Be Found`. As a result, the error message returned by the RS is not displayed.

Resolution

1. In IE, go to the `Tools > Internet Options > Advanced` tab.
2. Clear the `Show Friendly HTTP Error Messages` option.
3. Click `OK`.

Only Loopback Connection is Supported

Problem

The RS can connect to an LCA only on the local host, and it relies on the DNS resolution of the host name `localhost` for this. If the local host file has been modified so that local host is resolved to anything other than 127.0.0.1, the RS will not be able to start up and would generate an error message like this:

```
17:19:59.082 gvp-linux-ngi RS_252 ERROR LCAManager -
com.genesyslab.platform.commons.protocol.ProtocolException: Only
loopback (localhost or::1) connection is supported
```

Resolution

On a Linux platform, open the `/etc/hosts` file and make sure the line `127.0.0.1 localhost` is in the file.

On a Windows Server 2003 platform, open the `c:\windows\system32\drivers\etc\hosts` file and make sure the line `127.0.0.1 localhost` is in the file.

GVP Dashboard

In the IVR Profile Utilization report, the value for `In-Progress Sessions` is current as of the CDRs in the Reporting Server's database. If this value does not appear to be accurate, generate a corresponding CDR report to validate that CDRs are available for calls.

Resource Manager

This section describes specific issues with the Resource Manager (RM) that might require troubleshooting.

Failover Does Not Work

Problem

The Resource Manager is configured for failover but it is not working.

Resolution

From the command line, issue the `$InstallationRoot$/bin/NLB.bat <enable|disable> <cluster node ID>` command to see if the traffic can be redirected manually.

- If traffic can be redirected manually, it is an RM issue. Check the configuration options in the RM `cluster` section to ensure that the IP address and port numbers that are specified for each cluster member (1 and 2) are reachable from the other RM host (1 is reachable by 2 and vice-versa).

  Specifically check the following configurations:

  a. Ensure that the TCP port that is configured in the `cluster` section for cluster members 1 and 2 is open and is in a *listening* state. Verify this by running the `netstat` command.

  b. Ensure that the you can ping the IP addresses that are specified in the `cluster` section for cluster members 1and 2 from each of the RM hosts.

  c. If the RMs are installed on Windows, ensure that the IP addresses that are specified in the `cluster` section for cluster members 1 and 2 do not belong to the NLB-dedicated NIC (where the virtual-IP is defined).

  d. Ensure that the firewall, if enabled, is not blocking the communication between the RMs in the cluster.

  e. Ensure that all cables are properly connected.

- If traffic cannot be redirected manually, the issue is outside of the RM and you must check the entire HA configuration.

Both RMs Are Active, When in Active/Standby Mode

Problem

The Resource Manager (RM) is deployed in active/standby High Availability (HA) mode and both RMs are active.

Resolution

This is an indication that the RM nodes cannot communicate properly with each other. See Steps a to e in “Failover Does Not Work” on page 52.

Neither RM is Active, When in Active/Standby Mode

Problem

The Resource Manager (RM) is deployed in active/standby High Availability (HA) mode and neither of the RMs are active.

Resolution

This is an indication that the RM nodes cannot communicate properly with each other. See Steps a to e in “Failover Does Not Work” on page 52.

Cluster Mode Connection Failure

Problem

In cluster mode, a message similar to the following is printed continuously in one of the Resource Manager (RM) logs:

```
RMCommTCPBonding.cxx:725 700351472 VGSocketError nSocket=605517456
```

This message indicates that the cluster connection between the two RMs has problems, and even after retries there is no further communication between the two RMs on the cluster port (which is used for exchanging messages).

Resolution

Restart the RM process that is printing the log(s) where you find the repeating message.

SIP Error Codes for Rejected Requests

This section describes specific SIP error codes that are returned by the Resource Manager (RM) when a request is rejected.

480 SIP Response Code (Event Pool Throttling)

The Media Server (MS) may reject incoming calls when the MS control event pools are running low on available events, in a behavior termed Event Pool Throttling.

When one of the event pools is above the high threshold configurable percentage of used events, it becomes a “saturated pool.” (Each control event pool's size is configurable.) When there is at least one saturated pool, the MS starts rejecting calls, using SIP response code 480.

When a saturated pool has dropped below a low threshold configurable percentage of used events, it is no longer a saturated pool. When there are no saturated pools, calls are accepted again.

503 Service Unavailable

This error occurs when the RM suspends the acceptance of new RM sessions before it gracefully shuts down. Requests for new RM session creation are rejected with this error code.

500 Server Internal Error

This error occurs if the RM tries to forward a message to a resource that does not have the TCP port open. The RM tries to use the TCP transport if the forwarded request exceeds the MTU size (estimation) or if the set route in the `ROUTE` header of the SIP message, or the `Request-URI` in the body of the message, dictates that it to go through TCP (transport=TCP).

Resolution

Three options exist to resolve this issue:

1. Enable TCP on the resource side.
2. Increase the MTU size by configuring the `proxy.sip.mtusize` configuration option to a value greater than the default value of `1500`.
3. Disable TCP on the RM.

The first resolution is recommended. The third resolution is would be considered a *last resort* solution, since both the proxy should have TCP and UDP ports available.

485 Ambiguous

This error occurs if the RM session ID is specified in a request, and the RM does not recognize it. The RM tries to create the session, but if the RM session creation fails, the `485` response code is returned.

482 Loop Detected

This error occurs if the RM detects a request that will be forwarded to itself.

481 Call/Transaction Does Not Exist

This error occurs if the RM receives a `CANCEL request` that does not match any existing `INVITE` transactions.

Resolution

1. Check the route that is set, and ensure that the next hop is not the RM itself.
2. Check the configured resources to ensure that the Address of Record (AOR) does not point to RM itself.

If the User Agent Client (UAC)-to-UAC communication is SIPp when the error occurs in the call scenario, it generates a SIP `BYE` message with the RM's address in the `Request-URI` (instead of the address of the User Agent Server [UAS]). The RM receives the `BYE` message, determines that it points to itself, and rejects it with the `481` error. To workaround this issue, use SIPp with the `-nd` option.

480 Temporarily Unavailable

This error occurs in either one of two scenarios:

1. If all resources are down or unavailable.
2. If the port count, usage limit, or another limit is reached.

408 Request Timeout

This error occurs if the UAS does not respond within the timer-B or timer-F interval.

405 Method Not Allowed

This error occurs in either one of two scenarios:

1. If an out-of-dialog method, other than a SIP `INVITE` or `OPTIONS` message is sent to the RM.
2. If the SIP `OPTIONS` message contains a `user-info` parameter and does not have a `Max-Forwards` header configured with a value of `0`.

404 Not Found

This error occurs in either one of three scenarios:

1. The Logical Resource Group (LRG) that is servicing the requested service type cannot be found.

2. A default IVR Profile is not specified and a matching IVR Profile, based on the DNIS cannot be found.and no default.
3. A resource cannot be allocated for a request is to be forwarded to a specific gateway or CTI Connector.

403 Forbidden

This error (which is the default) occurs when either the `allow` or `disallow policy` parameter for a Tenant or IVR Profile is enforced.

400 Bad Request

This error occurs when the request contains values that are not acceptable to the RM. For example:

- If the conference ID is missing in the `sip:conf=@<host>:<port>` request
- If the `Min-SE` header in the SIP message has a refresher value other than `uac` or `uas`.

T-Server-CUCM to Media Server Connector

This section describes specific issues with the T-Server-CUCM to Media Server Connector that might require troubleshooting.

Call Related Errors

Rejecting or Aborting Calls

For rejected or aborted call errors, check the SNMP MIB table, `UCMCSummaryTable`. The contents of the `UCMCSummaryTable` are printed in the log file at regular intervals. You can also check the SNMP Statistics Summary.

4xx, 5xx, or 6xx Error Responses

The 4xx, 5xx, or 6xx error responses from SIP Server and Resource Manager will be logged in the `UCM-C` logs. The calls on SIP/MSML and CP4SM side can be related using the `Call LegID` received in the `CP4SM` message.

Tracing Calls and Media Operations

For tracing calls and media operations, separate ULIDs have been declared that can be leveraged during load tests for troubleshooting call related issues.

Troubleshooting Fetch Issues

1. Ensure that the resource can be fetched from a web browser on the same machine as the platform. If that fails, troubleshoot the web server.

   On Linux, you can do this by invoking the following command:

   ```
   wget ·output-document=<output_file> <Resource_URL>
   ```

   Where `<output_file>` is the location of the file the fetched content will be written to, and `<Resource_URL>` is the URL that you are trying to fetch.

2. Try the fetch again using the web browser and ensure that it is configured to use the Squid HTTP proxy (`127.0.0.1:3128`), and check the Squid access logs for errors. If that fails, ensure that the Squid service is running.

   On Linux, you can do this by invoking the following command:

   ```
   curl --output <output_file> --proxy 127.0.0.1:3128 <Resource_URL>
   ```

Note: On Linux, you can use either the `wget` command or the `curl` command for fetching. The preceding steps show each method.

Step 2 applies only when troubleshooting NGI and MCP (does not apply to GVPi).

Supplements

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

Management Framework

- *Framework 8.1 Deployment Guide,* which provides information about configuring, installing, starting, and stopping Framework components.
- *Framework 8.1 Genesys Administrator Deployment Guide*, which provides information about installing and configuring Genesys Administrator.
- *Framework 8.1 Genesys Administrator Help,* which provides information about configuring and provisioning contact center objects by using the Genesys Administrator.
- *Framework 8.1 Configuration Options Reference Manual,* which provides descriptions of the configuration options for Framework 8.1 components.

SIP Server

- *Framework 8.1 SIP Server Deployment Guide,* which provides information about configuring and installing SIP Server.

Genesys Voice Platform

- *Genesys Voice Platform 8.1 Deployment Guide,* which provides information about installing and configuring Genesys Voice Platform (GVP).
- *Genesys Voice Platform 8.1 User's Guide,* which provides information about configuring, provisioning, and monitoring GVP and its components.
- *Genesys Voice Platform 8.1 Troubleshooting Guide,* which provides troubleshooting methodology, basic troubleshooting information, and troubleshooting tools.

- *Genesys Voice Platform 8.1 SNMP and MIB Reference*, which provides information about all of the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) and traps for GVP, including descriptions and user actions.
- *Genesys Voice Platform 8.1 Genesys VoiceXML 2.1 Reference Help,* which provides information about developing Voice Extensible Markup Language (VoiceXML) applications. It presents VoiceXML concepts, and provides examples that focus on the GVP Next Generation Interpreter (NGI) implementation of VoiceXML.
- *Genesys Voice Platform 8.1 Legacy Genesys VoiceXML 2.1 Reference Manual*, which describes the VoiceXML 2.1 language as implemented by the Legacy GVP Interpreter (GVPi) in GVP 7.6 and earlier, and which is now supported in the GVP 8.1 release.
- *Genesys Voice Platform 8.1 Application Migration Guide*, which provides detailed information about the application modifications that are required to use legacy GVP 7.6 voice and call-control applications in GVP 8.1.
- *Genesys Voice Platform 8.1 CCXML Reference Manual,* which provides information about developing Call Control Extensible Markup Language (CCXML) applications for GVP.
- *Genesys Voice Platform 8.1 Configuration Options Reference,* which replicates the metadata available in the Genesys provisioning GUI, to provide information about all the GVP configuration options, including descriptions, syntax, valid values, and default values.
- *Genesys Voice Platform 8.1 Metrics Reference,* which provides information about all the GVP metrics (VoiceXML and CCXML application event logs), including descriptions, format, logging level, source component, and metric ID.
- *Genesys Voice Platform 8.1 Web Services API wiki,* which describes the Web Services API that the Reporting Server supports.

Voice Platform Solution

- *Voice Platform Solution 8.1 Integration Guide,* which provides information about integrating GVP, SIP Server, and, if applicable, IVR Server.

Composer Voice

- *Composer 8.1 Deployment Guide,* which provides information about installing and configuring Composer Voice.
- *Composer 8.1 Help,* which provides information about using Composer Voice, a GUI for developing applications based on VoiceXML and CCXML.

Open Standards

- *W3C Voice Extensible Markup Language (VoiceXML) 2.1, W3C Recommendation 19 June 2007,* which is the World Wide Web Consortium (W3C) VoiceXML specification that GVP NGI supports.
- *W3C Voice Extensible Markup Language (VoiceXML) 2.0, W3C Recommendation 16 March 2004,* which is the W3C VoiceXML specification that GVP supports.
- *W3C Speech Synthesis Markup Language (SSML) Version 1.0, Recommendation 7 September 2004,* which is the W3C SSML specification that GVP supports.
- *W3C Voice Browser Call Control: CCXML Version 1.0, W3C Working Draft 29 June 2005,* which is the W3C CCXML specification that GVP supports.
- *W3C Semantic Interpretation for Speech Recognition (SISR) Version 1.0, W3C Recommendation 5 April 2007,* which is the W3C SISR specification that GVP supports.
- *W3C Speech Recognition Grammar Specification (SRGS) Version 1.0, W3C Recommendation 16 March 2004,* which is the W3C SRGS specification that GVP supports.

Genesys

- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD and which provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, and which provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.
- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at `http://genesyslab.com/support`.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Manual*
- *Genesys Supported Media Interfaces Reference Manual*

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the `system level documents by release` tab in the Knowledge Base `Browse Documents` Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at http://genesyslab.com/support.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at orderman@genesyslab.com.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

80fr_ref_06-2008_v8.0.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

Table 4 describes and illustrates the type conventions that are used in this document.

Table 4: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 64).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for . . .

Table 4: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	All programming identifiers and GUI elements. This convention includes: • The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. • The values of options. • Logical arguments and command syntax. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages in `EventError` events. If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index

Symbols

A

B

C

D

F

G

H

I

L

M

N

P

S

T

U

V

W