Genesys

Technical Support Troubleshooting Guide

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, is 100% focused on software for call centers. Genesys recognizes that better interactions drive better business and build company reputations. Customer service solutions from Genesys deliver on this promise for Global 2000 enterprises, government organizations, and telecommunications service providers across 80 countries, directing more than 100 million customer interactions every day. Sophisticated routing and reporting across voice, e-mail, and Web channels ensure that customers are quickly connected to the best available resource—the first time. Genesys offers solutions for customer service, help desks, order desks, collections, outbound telesales and service, and workforce management. Visit 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 CD, 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

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

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 at the following regional numbers:

Region	Telephone	E-Mail
North and Latin America	+888-369-5555 or +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-127-645-7002	support@genesyslab.co.uk
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
India	+91-(0)-22-3918-0537	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp

Prior to contacting technical support, please refer to the *Genesys Technical Support 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 7 Licensing Guide***.

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 70TechSupp_Trouble_05-2008_v7.0.003.00

Table of Contents

Chapter

1 Common Genesys Logging

This chapter covers the following topics:

Explanation of Logging

Genesys applications can report log events at five levels of detail: Alarm, Standard, Interaction, Trace, and Debug. Only the first four are intended for on-site analysis by a user. Log events of the Alarm, Standard, Interaction, and Trace levels feature the same unified log record format and can be stored in the Central Log Database.

If you experience a problem with Genesys software, logging is extremely important and can be necessary to the discovery of the root cause. Without sufficient logging showing the issue, Technical Support may not be able to resolve the issue.

Note: For the most recent information about log events, see the *Framework 7.2 Combined Log Events Help* on the Technical Support website. This file is updated periodically as new products are released: http://genesyslab.com/support/dl/retrieve/default.asp?item=B3BFC6DABE22B62AAE32A6D12150A4D1&view=item.

Logging and Application Performance

Follow these recommendations when running applications in production mode during normal use:

- Always enable buffering of the log output when sending logs to a log file. (Refer to "Common Log Options" on page 13.)
- On Windows host computers, avoid directing the log output to a console window or configure the application to send only log events of the Standard level to the console.

Follow these recommendations to increase an application's performance while enabling the application's logging:

- Store log files on the local disk of the computer running the application rather than using network file systems for log file storage. Network file systems may have low performance; in addition, heavy network traffic can affect the application's performance.
- Configure only log events of the Standard level to be sent to the Log Database.

Logging from Startup

Genesys Technical Support will occasionally ask for logs from startup of a particular component. During start up, extra information is printed to the log. For example: software version number, initial configuration items, registering with License Server, connections to other clients or servers, etc. Depending on the problem being investigated, this information can be extremely important.

Logging During Normal Operation

For complete specifications of log events reported at the Alarm, Standard, Interaction, and Trace levels, see *Genesys 7.2 Combined Log Events Help.*

Alarm Log Level

The Alarm-level logs contain only log records of the Alarm level. SCS generates Alarm log events on behalf of other applications when receiving from them log events that are configured as Detection events in Alarm Conditions. Using this level, Solution Control Server reports the occurrence and removal of all alarms to the Centralized Log Database. This level contains the Management Layer translations of log events of other levels into Alarms.

Standard Log Level

The Standard level of logging is the only one that should be permanently enabled during solution operation in regular production mode. It contains high-level events that report both major problems and normal operations of in service solutions.

An event is reported at the Standard level if it satisfies one of these criteria:

- Indicates that an attempt to perform any external operation has failed
- Indicates that the latest attempt to perform an external operation that previously failed has succeeded
- Indicates detection of a condition that has a negative impact on operations, actual or projected
- Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
- Indicates a security violation of any kind
- Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
- Indicates inability to process an external request
- Indicates successful completion of a logical step in an initialization process
- Indicates a transition of an Application from one operational mode to another
- Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
- Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range

Interaction Log Level

The Interaction-level logs report the details of an interaction process by Solution components that handle interactions. The log contains information about the processing steps for each interaction by each Solution component. An event is reported at the Interaction level if it:

- Is a recognizable high-level data exchange with another Application about an interaction.
- Indicates a change in real-time state of an interaction handled by the Application (unless such a change is visible from the high-level data exchange).

The specific criteria depend on a particular component and its role in interaction processing.

Use the Interaction-level log records to analyze and troubleshoot new interaction-processing scenarios, especially when you introduce new Solutions

or enable new functions within existing Solutions. Note that Interaction-level records contain the interaction attributes, such as Interaction ID, that helps to search for log events generated by various applications but related to the same interaction.

Warning! Using the Interaction level generates a higher number of logging events on the network and that may adversely affect the performance of the DBMS, Message Servers, and interaction processing components.

Trace Log Level

The Trace-level logs report the details of communications between the various Solution components. The log contains information about the processing steps for each interaction by each Solution component. An event is reported at the Trace level if it satisfies one of these criteria:

- It is a recognizable high-level data exchange with another Application.
- It is a recognizable high-level data exchange with an external system.
- It indicates a change in real-time state of user-level objects handled by the Application (unless such a change can be seen from the high-level data exchange).

Use the Trace-level log records to analyze and troubleshoot new interaction processing scenarios, especially when you introduce new Solutions or enable new functions within existing Solutions.

Warning! Using the Trace level generates a higher number of logging events on the network that may adversely affect performance of the DBMS, Message Servers, and interaction-processing components.

Logging During Irregular Operation

Standard-level and Trace-level log events do not contain all the details needed to analyze and troubleshoot solutions malfunctions. Therefore, if you need to report an issue to Genesys Technical Support, Technical Support might request that you provide relevant Debug-level logs. The Debug level of logging contains information intended for analysis by Genesys Technical Support only. Log events of the Debug level do not have a unified format, are not specified, and can only be stored in a local text file. Logging at this level is likely to adversely affect application performance. Enable this log output level only when a Genesys representative requests it. Keep in mind that running Genesys servers with the Debug level of logging is highly resource-intensive and, as such, is not recommended for production mode. Carefully consider whether a situation (such as the initial deployment or first signs of technical problems) calls for setting a logging level more detailed than the Standard level, and

preferably test the network loads generated with detailed logging in a lab or controlled environment. Note that changing the log output level of a running application does not interrupt solution operations.

Technical Support might also request that you reproduce a problem because:

1. During their regular operations, many contact-center systems, such as DBMSs, IVRs, and switches, do not employ logging at the level of detail required to diagnose serious technical issues.
2. Other reasons than an application failure can contribute to interaction handling errors. For example, a call can be misrouted, that is, delivered to a wrong DN, despite the fact that applications are functioning properly.

Centralized Logging

The centralized logging function provides a number of advantages over the more traditional logging to a local text file:

- Keeping log records of all applications in one place and presenting them in the unified log record format provides for a comprehensive view of the solutions' operations history.
- Use of a relational database management system such as the central log storage enables quick access to the required records and allows for advanced record selections, which can be based on a variety of search criteria.
- Viewing, via Solution Control Interface, the logs stored in a Central Log Database gives an integrated view of the solutions' maintenance history and thus complements the solution control and alarming capabilities.
- Deleting, via a wizard in Solution Control Interface, the obsolete logs or logs of a particular solution, a host, or an application makes database management more convenient.

Given these advantages, Genesys recommends using the centralized logging as the primary method for storing Standard log events of all applications. When enabling the log output of the Interaction and Trace level (as directed in the section "Logging During Normal Operation" page 8), store log events of both levels in the Central Log Database in addition to log events of the Standard level. Simultaneous use of both local and centralized logging options, while technically possible, is not recommended except for some special temporary purposes.

The centralized logging system consists of:

- One or more Message Servers that collect log events from applications.
- One or more Log Databases.
- One or more DB Servers, which interface Message Server with the DBMS where the Log Database is set up.

Provided that the Standard level of log output is routinely used under normal production conditions, always limit the centralized logging system to one

Message Server and one Log Database for all but large and geographically distributed interaction management networks.

If any part of the centralized logging system becomes unavailable, the log outputs of the affected applications are temporarily redirected to local binary files. Upon restoration of normal functioning, the applications automatically resume logging to the Central Log Database. The log records accumulated in the local binary files are automatically transferred to the Log Database.

Note: The format of records kept in the Log Database is specified in the "Log Formats" chapter of the *Framework 7.1 Management Layer User's Guide.*

Viewing Log Database Entries

Any general-purpose DBMS client can be used to make advanced selections from the Log Database. However, before considering use of such applications, review the log-viewing capabilities provided by Solution Control Interface (SCI). SCI allows the user to view an entire log. It also provides a number of predefined selections from the Log Database; the selections are based on the most typical maintenance selection criteria such as:

- Records generated by components of a selected solution.
- Records generated by applications located on a selected host.
- Records of a specified output level.
- Records containing a specified combination of symbols in text.

The selection criteria supported by Solution Control Interface can be used in combinations.

Additionally, SCI allows users to save selected log records in a regular text file or an XML file. Finally, SCI features a log maintenance tool to delete obsolete log records. For detailed information on the SCI log-managing capabilities, see the *Framework 7.1 Solution Control Interface Help* and *Framework 7.1 Management Layer User's Guide.*

Interaction Trace

You can configure Framework components to send Interaction-level log events to the Centralized Log Database.

Note: Storing Interaction-level log events in the Log Database might affect application performance and, therefore, is not recommended for production environments.

A set of extended attributes might be attached to each Interaction log event; in particular, each Interaction log event contains a unique identifier of the contact center interaction in the IID extended attribute.

Note: The set of extended attributes for Interaction-level log events may vary depending on a particular interaction properties and the component that generates the log event.

For complete specifications of Interaction-level log events reported by Framework components and for information about extended attributes for each log event, see *Framework 7.2 Combined Log Events Help*. Solution Control Interface displays all Interaction-level records from the Centralized Log Database, with a capability to search for all records with a particular Interaction ID, thus providing Interaction-Trace capability.

For detailed information on viewing Interaction-level log records with SCI, see the *Framework 7.1 Management Layer User's Guide* and *Framework 7.1 Solution Control Interface Help.*

Common Log Options

verbose

Default Value: `all`

Valid Values:

`all`	All log events (that is, log events of Standard, Trace, Interaction, and Debug levels) are generated.
`debug`	The same as `all`.
`trace`	Log events of the Trace and higher levels (that is, log events of Standard, Interaction, and Trace levels) are generated while log events of the Debug level are not generated.
`interaction`	Log events of the Interaction and higher levels (that is, log events of Standard and Interaction levels) are generated while log events of the Debug level are not generated.
`standard`	Log events of the Standard level are generated while log events of the Interaction, Trace, and Debug levels are not generated.
`none`	Produces no output.

Changes Take Effect: Immediately

Determines if a log output is created. If so, specifies the minimum level of log events generated. The log events levels, starting with the highest priority level, are Standard, Interaction, Trace, and Debug. See also “Log Output Options” on page 15.

Note: For definitions of Standard, Trace, Interaction, and Debug log levels, refer to the *Framework 7.2 Deployment Guide* or to the *Framework 7.1 Solution Control Interface Help*.

buffering

Default Value: `true`
Valid Values:

`true`	Enables buffering
`false`	Disables buffering

Changes Take Effect: Immediately

Turns on/off operating system file buffering. The option is only applicable to the `stderr` and `stdout` output (see page 15). Setting this option to true increases the output performance.

Note: When buffering is enabled, log messages may appear in the log with a delay.

segment

Default Value: `false`
Valid Values:

`false`	No segmentation allowed.
`<number> KB` or `<number>`	Sets maximum segment size in kilobytes. The minimum segment size is 100 KB.
`<number> MB`	Sets maximum segment size in megabytes.
`<number> hr`	Sets maximum segment size in hours. The minimum segment size is 1 hour.

Changes Take Effect: Immediately

Specifies if there is a segmentation limit for a log file. If there is, sets the mode of measurement along with the maximum size. If the current log segment exceeds the size set by this option, the current file is closed and a new one is created.

expire

Default Value: `false`
Valid Values:

`false`	No expiration; all generated segments are stored.
`<number> file` or `<number>`	Sets maximum number of log files to store. Specify a number from 1-100.
`<number> day`	Sets maximum segment size in megabytes.

Changes Take Effect: Immediately

Determines if log files expire. If they do, sets the measurement for determining when they expire along with the maximum number of files (segments) or days before the files are removed.

Log Output Options

To configure log outputs, set log level options (`all`, `standard`, `interaction`, `trace`, `memory`, and/or `debug`) to the desired types of log output (`stdout`, `stderr`, `network`, `memory`, and/or [`filename`], for log file output). You can use:

- One log level option to specify different log outputs.
- One log output type for different log levels.
- Several log output types simultaneously for logging the events of the same or different log level.

You must separate the log output types by a comma when you are configuring more than one output for the same log level. See “Examples” on page 18.

Note: The log output options are activated according to the setting of the verbose configuration option.

Warning! When you direct log output to a file on the network drive, an application does not create a snapshot log file (with the extension `*.snapshot.log`) in case it terminates abnormally.

all

Default Values: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (stdout).
`stderr`	Log events are sent to the Standard error output (stderr).
`network`	Log events are sent to Message Server, which can reside anywhere on the network; Message Server stores the log events in the Log Database. **Note:** Setting the `all` log level option to the `network` output enables an application to send log events of Standard, Interaction, and Trace levels to Message Server. Debug-level log events are neither sent to Message Server nor stored in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application’s working directory.

Changes Take Effect: Immediately

Specifies to which outputs an application sends all log events. The log output types must be separated by a comma when more than one output is configured. For example:

```
all = stdout, logfile
```

Note: To ease the troubleshooting process, consider using unique names for log files that different applications generate.

standard

Default Values: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (stdout).
`stderr`	Log events are sent to the Standard error output (stderr).
`network`	Log events are sent to Message Server, which can reside anywhere on the network; Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies to which outputs an application sends the log events of the Standard level. The log output types must be separated by a comma when more than one output is configured. For example:

```
standard = stderr, network
```

interaction

Default Values: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (stdout).
`stderr`	Log events are sent to the Standard error output (stderr).
`network`	Log events are sent to Message Server, which can reside anywhere on the network; Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies to which outputs an application sends the log events of the Interaction and higher levels (that is, log events of Standard and Interaction levels). The log outputs must be separated by a comma when more than one output is configured. For example:

```
interaction = stderr, network
```

trace

Default Values: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (stdout).
`stderr`	Log events are sent to the Standard error output (stderr).
`network`	Log events are sent to Message Server, which can reside anywhere on the network; Message Server stores the log events in the Log Database.
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies to which outputs an application sends the log events of the Trace and higher levels (that is, log events of Standard, Interaction, and Trace levels). The log outputs must be separated by a comma when more than one output is configured. For example:

```
trace = stderr, network
```

debug

Default Values: No default value
Valid Values (log output types):

`stdout`	Log events are sent to the Standard output (stdout).
`stderr`	Log events are sent to the Standard error output (stderr).
`memory`	Log events are sent to the memory output on the local disk. This is the safest output in terms of the application performance.
`[filename]`	Log events are stored in a file with the specified name. If a path is not specified, the file is created in the application's working directory.

Changes Take Effect: Immediately

Specifies to which outputs an application sends the log events of the Debug and higher levels (that is, log events of Standard, Trace, Interaction, and Debug levels). The log output types must be separated by a comma when more than one output is configured. For example:

```
debug = stderr, /usr/local/genesys/logfile
```

Note: Debug-level log events are never sent to Message Server or stored in the Log Database.

Log File Extensions

You can identify log files that an application creates for various types of output by file extensions:

- `*.log`—assigned to log files when you configure output to a log file. For example, if you set `standard = confservlog` for Configuration Server, it prints log messages into a text file called `<time_stamp>.confservlog.log`.
- `*.qsp`—assigned to temporary (spool) files when you configure output to the network, but the network is temporarily unavailable. For example, if you set `standard = network` for Configuration Server, it prints log messages into a file called `<time_stamp>.confserv.qsp` during the time the network is not available.
- `*.snapshot.log`—assigned to files that contain the output snapshot when you configure output to a log file. The file contains the last log messages that an application generates before it terminates abnormally. For example, if you set `standard = confservlog` for Configuration Server, Configuration Server prints the last log message into a file called `<time_stamp>.confserv.snapshot.log` in case of failure.

  Note: Provide `*.snapshot.log` files to Genesys Technical Support when reporting a problem.

- `*.memory.log`—assigned to log files that contain the memory output snapshot when you configure output to memory and redirect the most recent memory output to a file. For example, if you set `standard = memory` and `memory = confserv` for Configuration Server, it saves the latest memory output to a file called `<time_stamp>.confserv.memory.log`.
- output to a file called `<time_stamp>.confserv.memory.log`.

Examples

This section presents examples of a `log` section you might configure for an application when that application is operating in production mode and in two lab modes, debugging and troubleshooting.

Production Mode Log Section

```
[log]
verbose = standard
standard = stdout, network, logfile
```

With this configuration, an application only generates the log events of the Standard level and sends them to the standard output, to Message Server, and to a file named `logfile`, which the application creates in its working directory. Genesys recommends that you use this or a similar configuration in a production environment.

Lab Mode Log Section

```
[log]
verbose = all
all = stdout, /usr/local/genesys/logfile
trace = network
```

With this configuration, an application generates log events of the Standard, Interaction, Trace, and Debug levels and sends them to the standard output and to a file named `logfile`, which the application creates in the `/usr/local/genesys/` directory. In addition, the application sends log events of the Standard, Interaction, and Trace levels to Message Server. Use this configuration to test new interaction scenarios in a lab environment.

Failure-Troubleshooting Log Section

```
[log]
verbose = all
all = memory
memory = logfile
memory-storage-size = 32
```

With this configuration, an application generates log events of the Standard, Interaction, Trace, and Debug levels and sends them to the memory output. The most current log is stored to a file named `logfile`, which the application creates in its working directory. An increased memory storage allows an application to save more log information generated before a failure. Use this configuration when trying to reproduce an application's failure. The memory log file would contain the snapshot of the application's log at the moment of failure; this should help you and Genesys Technical Support identify the reason for the failure.

Note: If you are running an application on Unix and you do not specify any files to store the memory output snapshot, a core file that the application produces before terminating contains the most current application log. Provide the application's core file to Genesys Technical Support when reporting a problem.

Changes from 6.5 to 7.2

Table 1 documents changes in common log configuration options between release 6.5 and the initial release 7.2.

For a complete list of these log options and their descriptions, refer to the "Common Log Options" chapter of *Framework 7.2 Configuration Options Reference Manual* (CORM).

Table 1: Common Log Option Changes

Current Option Name	Option Values	Type of Change	Occurred in Release	Details
Log Section				
keep-startup-file	false, true, <number> KB, <number> MB	New	7.1	This option applies only to T-Servers.
verbose	all, standard, interaction, trace, debug, none	New values	7.0	New values: interaction, debug
buffering	true, false	See Details	7.0	The option now applies to stderr and stdout output instead of log-file output as in 6.x.
memory-storage-size	<number>	New	7.0	
message_format	short, full	New default value	7.0	New default value: short
time_format	time, iso8601, locale	New value; new default value	7.0	New value (which is the new default): time
print-attributes	true, false	New	7.0	
check-point	0–24	New	7.0	
memory	<string>	New	7.0	
spool	<path>	New	7.0	

Table 1: Common Log Option Changes (Continued)

Current Option Name	Option Values	Type of Change	Occurred in Release	Details
Log-Filter Section				
default-filter-type	copy, hide, skip	New	7.2	
Log-Filter-Data Section				
<key name>	copy, hide, skip	New	7.2	
Log Output Options				
all	stdout, stderr, network, memory, [filename]	New output level	7.0	New level: memory
standard	stdout, stderr, network, memory, [filename]	New output level	7.0	New level: memory
interaction	stdout, stderr, network, memory, [filename]	New	7.0	
trace	stdout, stderr, network, memory, [filename]	New output level	7.0	New level: memory
		See Details	7.0	Log events of higher levels are now also sent to the specified output.
dbprocess_number	`0` or any positive integer	Correction	7.1	The default value and valid values were incorrectly documented in the previous releases of the document.

Table 1: Common Log Option Changes (Continued)

Current Option Name	Option Values	Type of Change	Occurred in Release	Details
debug	stdout, stderr, memory, [filename]	New output level	7.0	New level: memory
		See Details	7.0	Log events of higher levels are now also sent to the specified output.
eventloghost	Any host name	Obsolete	6.5	Removed from common log options as an option specific to Solution Control Server.
alarm	stdout, stderr, network, [filename], syslog	Obsolete	6.5	Removed from common log options as an option specific to Solution Control Server.
message_format	full, short	New	6.5	Introduced after the initial 6.5 release.
time_convert	local, utc	New	6.5	Introduced after the initial 6.5 release.
		See Details	6.5	The option name was misspelled in a prior release of the document. The correct name is *time_convert.*
time_format	locale, ISO8601	New	6.5	Introduced after the initial 6.5 release.

Chapter

2 Desktops and G*plus* Adapters

Products within this category include:

- Agent Scripting
- Genesys Contact Navigator (GCN)
- Genesys Desktop (for Agent)
- Genesys Desktop (for Supervisor)
- Gplus Adapter for Microsoft
- Gplus Adapter for mySAP CRM
- Gplus Adapter for mySAP ERP
- Gplus Adapter for PeopleSoft
- Gplus Adapter for Siebel 2000
- Gplus Adapter for Siebel 7

This chapter covers the following topics:

Architecture

This sections contains graphics for some of products mentioned in this chapter. Please refer to the Deployment Guide for the respective products for additional information.

Desktop Applications

Genesys Desktop 7.2

Figure 1 illustrates the topology of Genesys Desktop 7.2. Figure 2 illustrates its architecture.

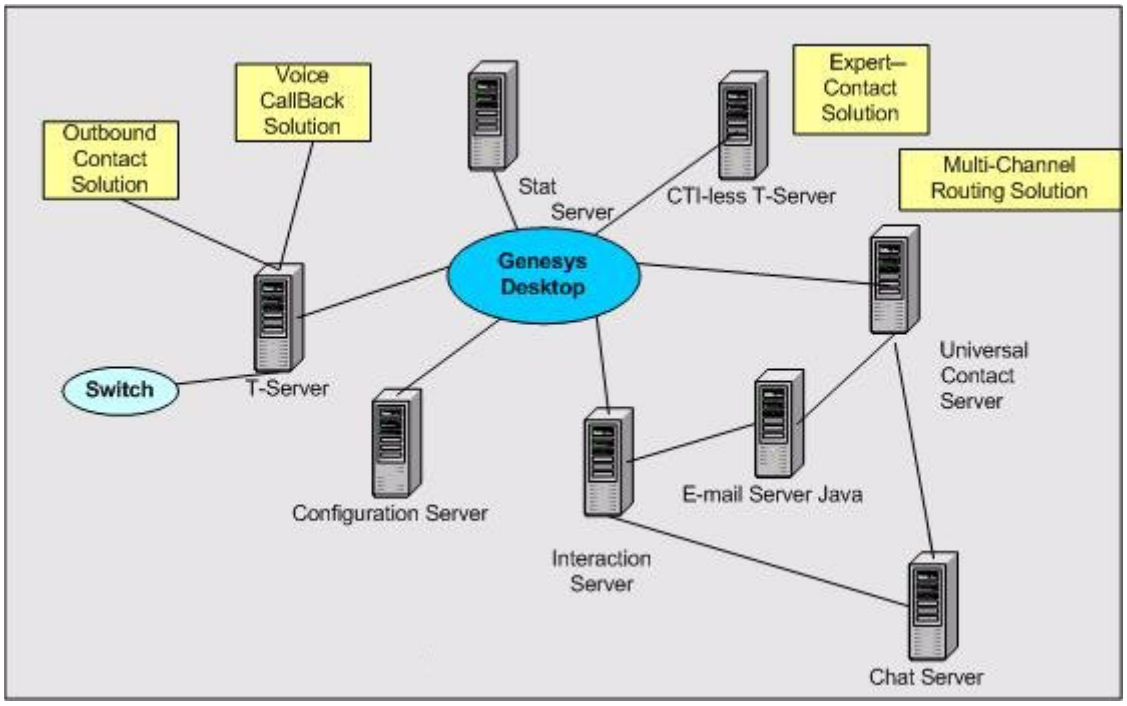


Figure 1: Genesys Desktop 7.2 Topology

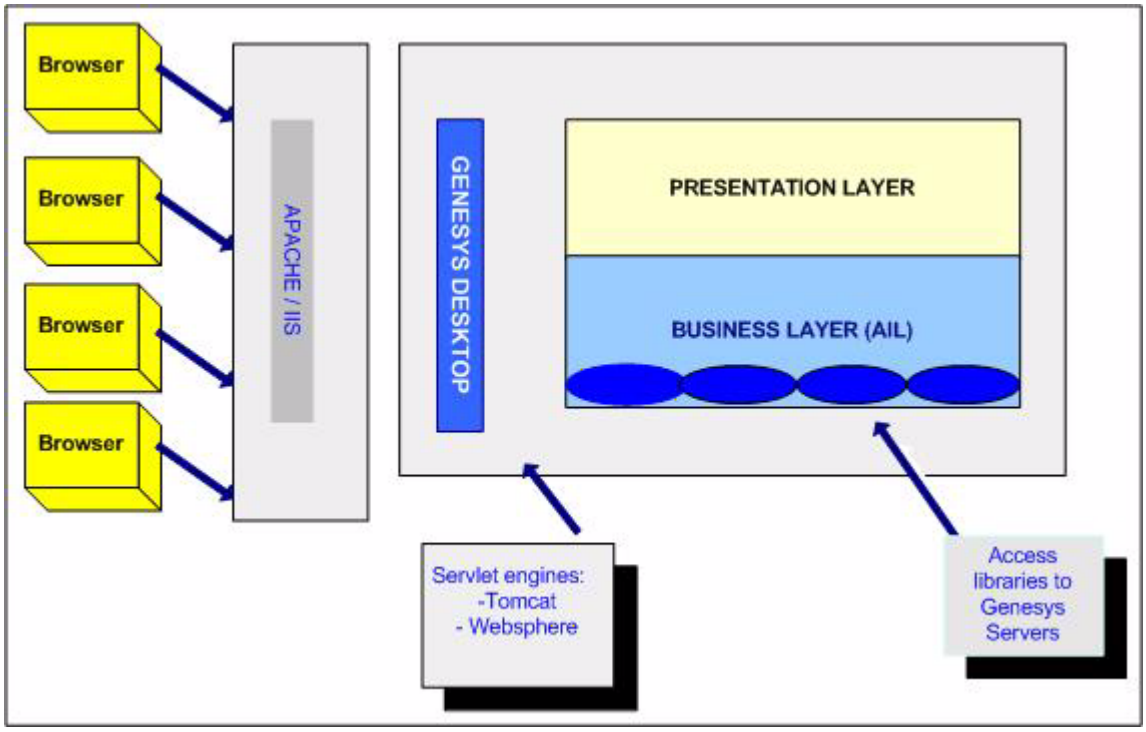


Figure 2: Genesys Desktop 7.2 Architecture

Genesys Contact Navigator 6.5

Figure 3 illustrates the architecture for Genesys Contact Navigator for DMX.

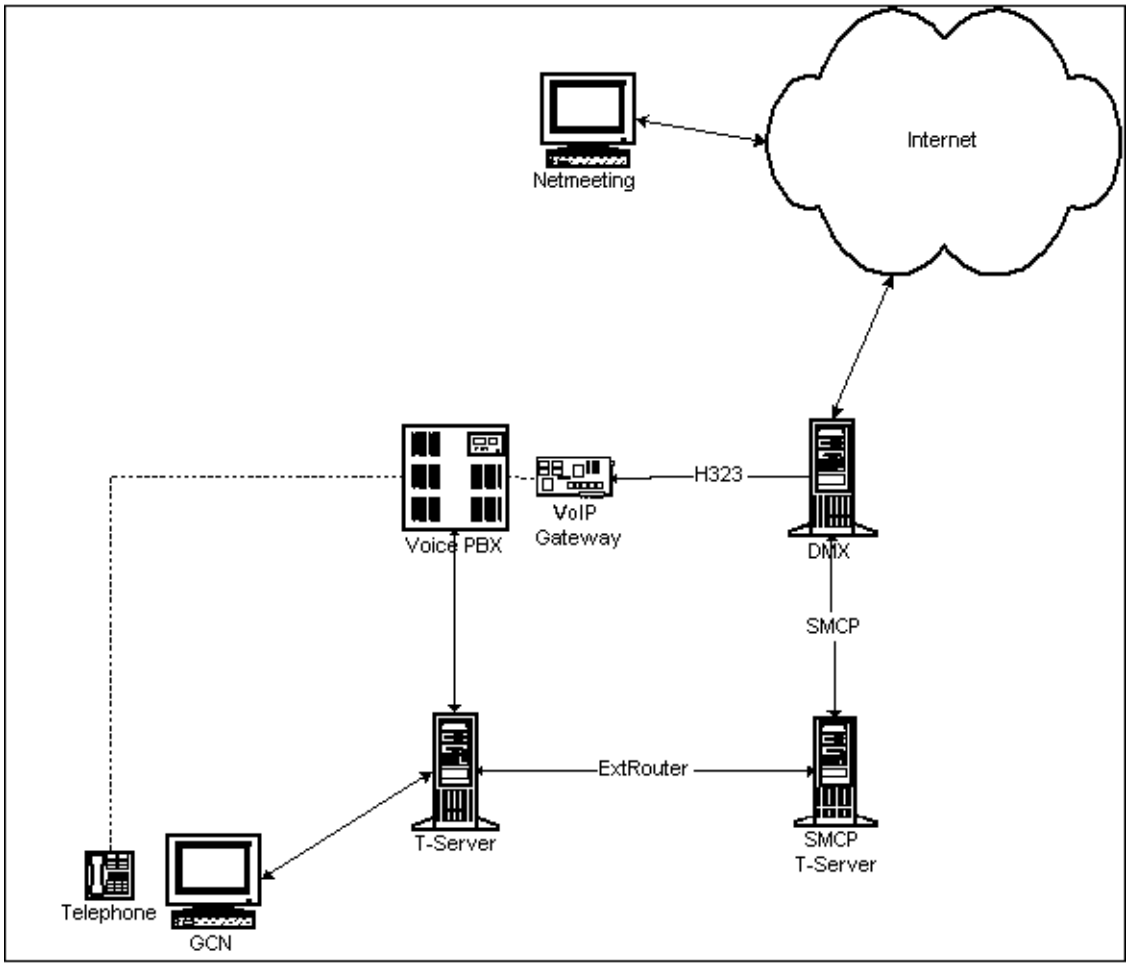


Figure 3: GCN 6.5 Architecture for DMX and Phone Switch

G*plus* Adapters

Gplus Adapter 7.2 for Microsoft CRM

Figure 4 illustrates the architecture for G*plus* Adapter 7.2 for Microsoft CRM.

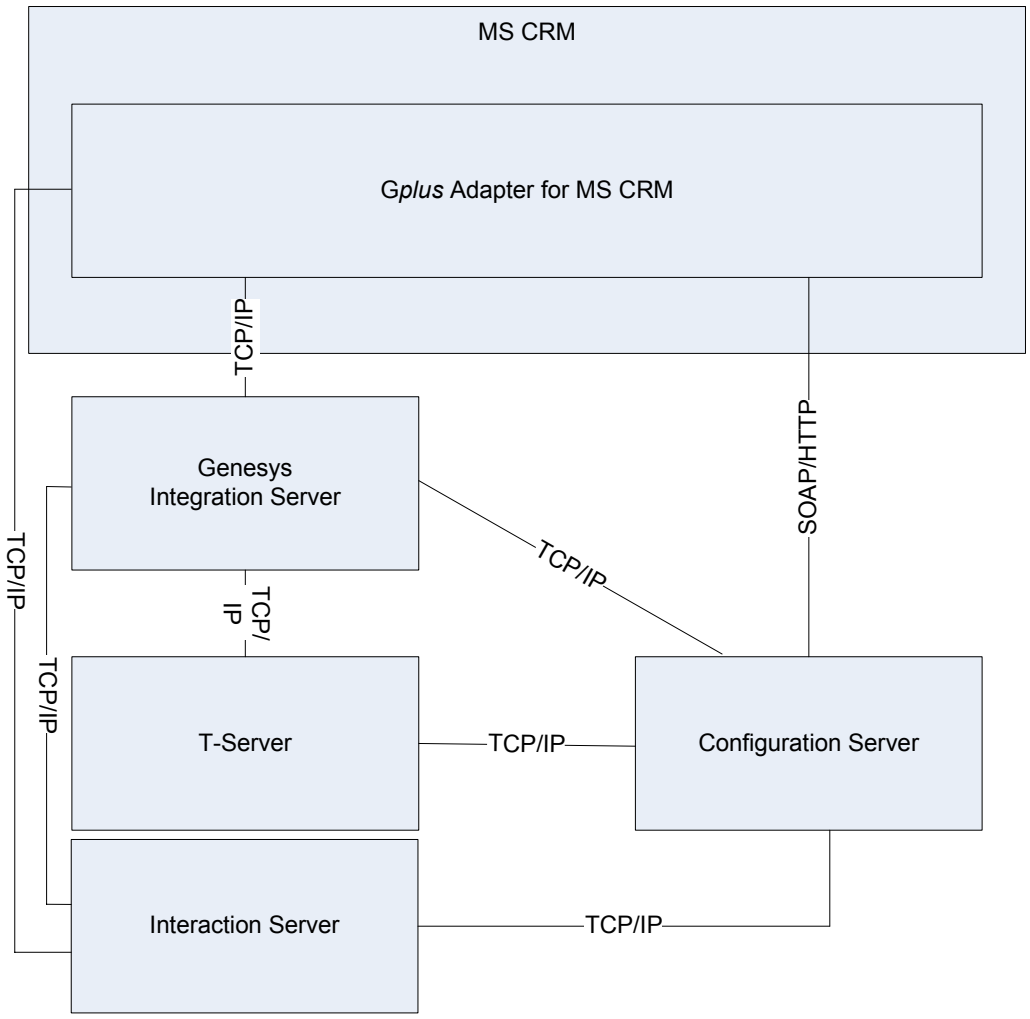


Figure 4: G*plus* Adapter7.2 for Microsoft CRM Architecture

Gplus Adapter 7.1 for mySAP ERP

Figure 5 illustrates the system overview for G*plus* Adapter 7.1 for mySAP ERP. Figure 6 illustrates its architecture.

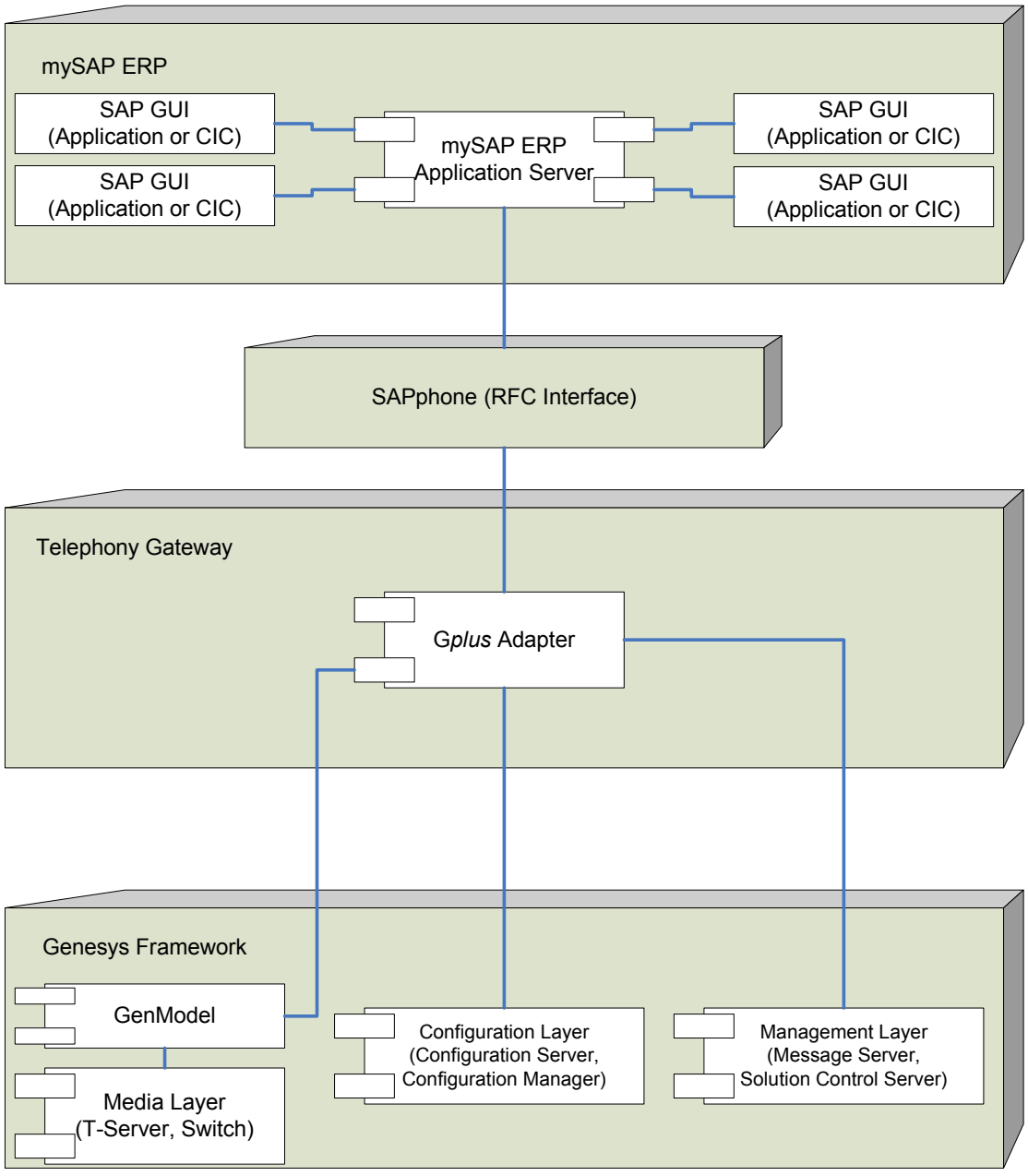


Figure 5: G*plus* Adapter 7.1 for mySAP ERP System Overview

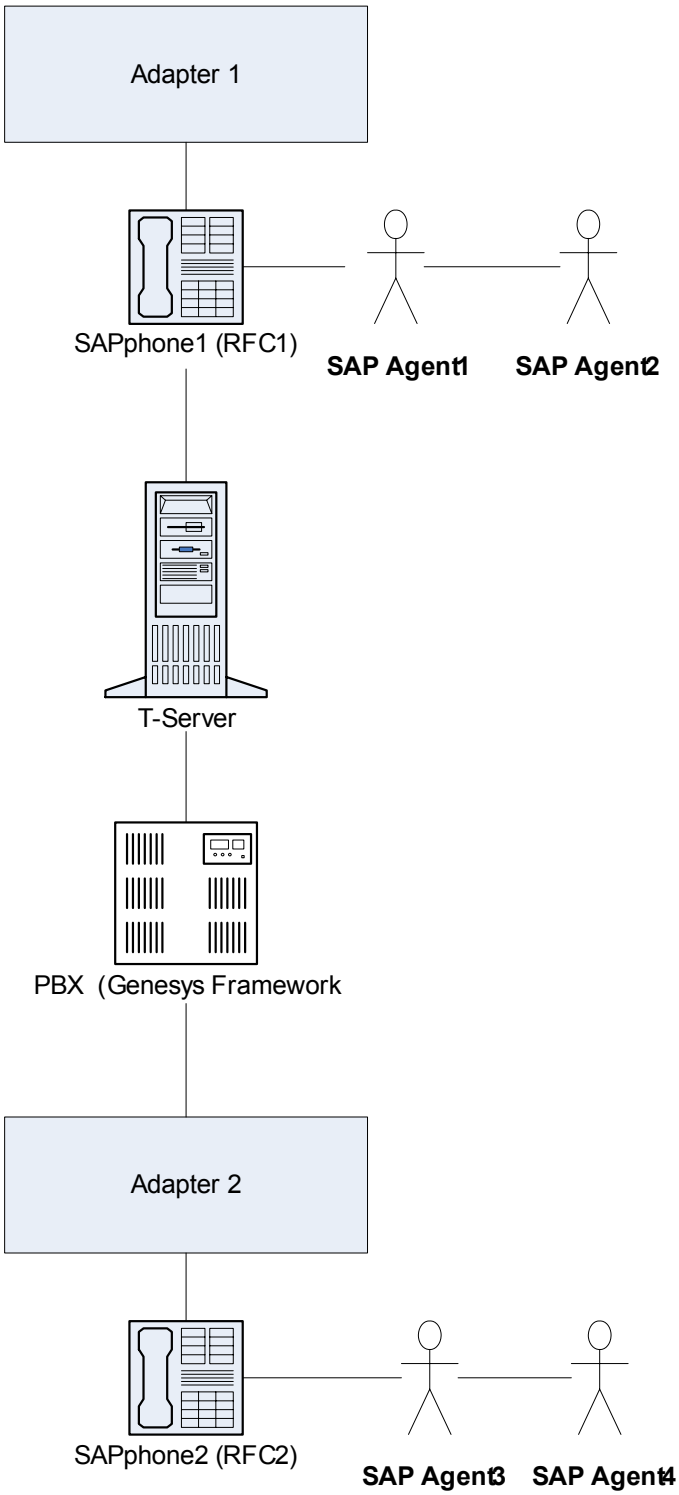


Figure 6: Gplus Adapter 7.1 for mySAP ERP Architecture for a Centralized Connection

Gplus Adapter 7.1 for PeopleSoft

Figures 7 and 8 illustrate the architecture for G*plus* Adapter 7.1 for PeopleSoft.

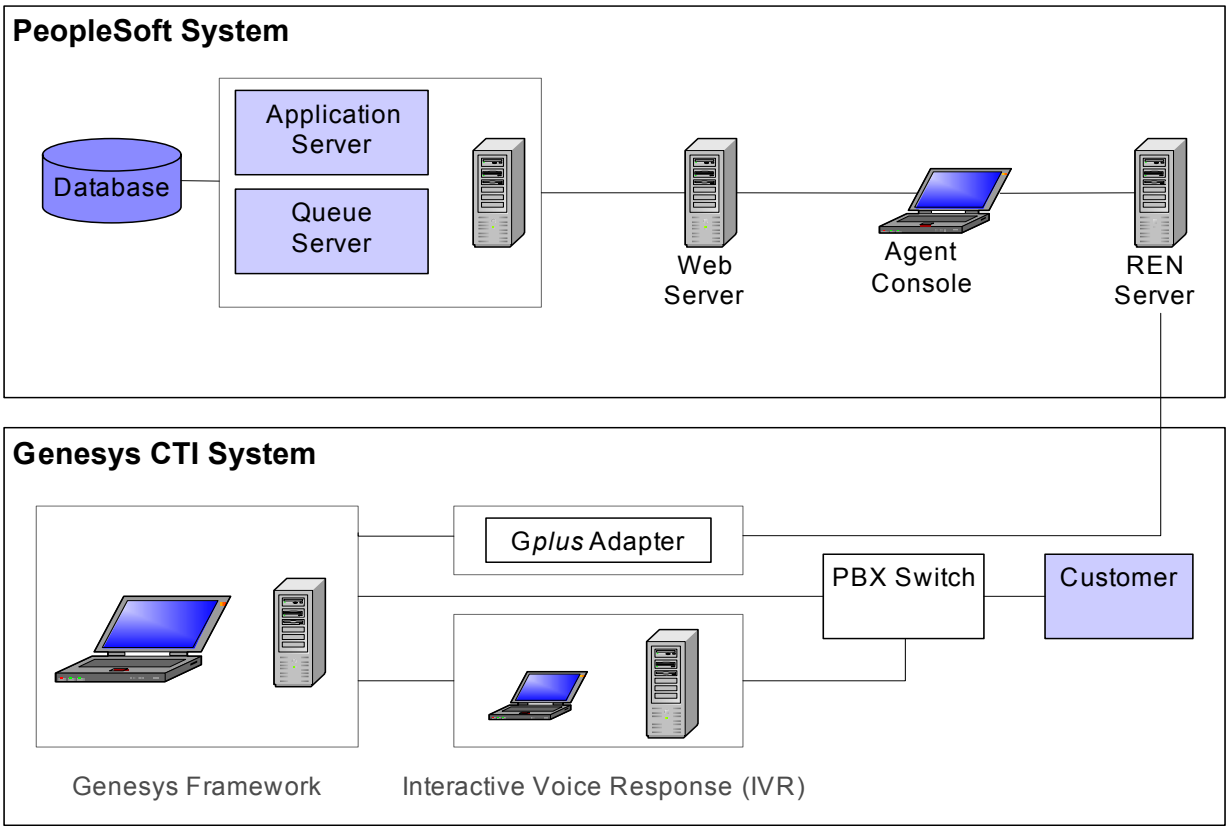


Figure 7: G*plus* Adapter 7.1 for PeopleSoft Architecture

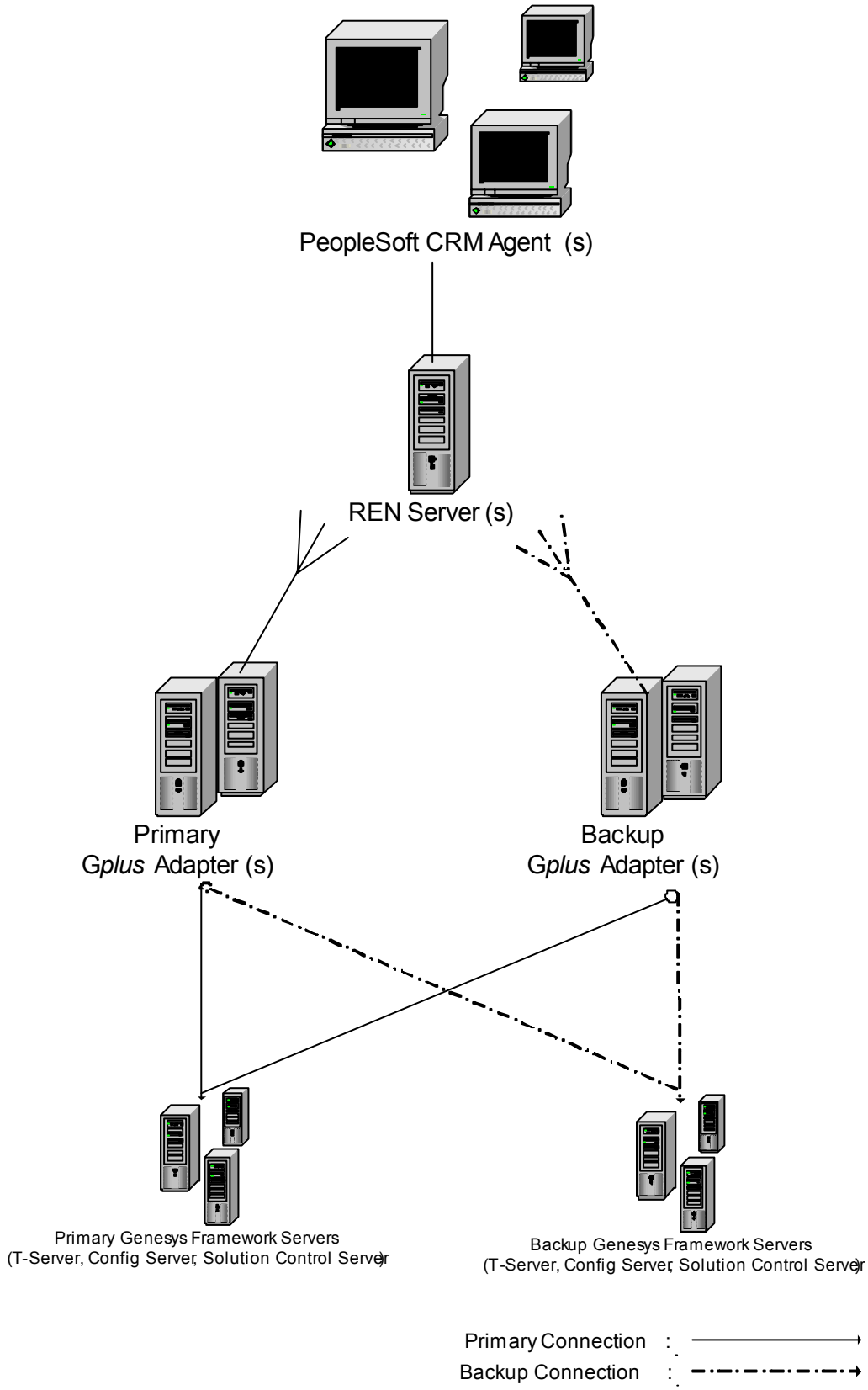


Figure 8: G*plus* Adapter 7.1 for PeopleSoft System Architecture

7.x Products

Table 2 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product. This list will be updated as more product milestones occur.

Table 2: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Genesys T-Lib SDK (Active X Desktop Toolkit, Java Desktop T-Library Package)	• T-Server information (see the entry for T-Server) • Application source code • Exact versions of the libraries • Compiler and linker settings
Gplus Adapter MySAP	• Adapter log • T-Server log
Gplus Adapter for PeopleSoft	• Request should be sent to Kevin Haselhuhn (kevinh@genesyslab.com).
Gplus Adapter for Siebel 7; Voice	• **Mandatory: Siebel Server version and platform** • Siebel Configuration expert (`.def` file) • List of used profiles (for example, voice, chat, e-mail) • Adapter logs • T-Server logs • Siebel Agent SComm log
Gplus Adapter for Siebel 7; Multimedia	• **Mandatory: Siebel Server version and platform** • Siebel Configuration expert (`.def` file) • List of used profiles (for example, voice, chat, e-mail) • Adapter logs • T-Server logs • Genesys Contact Navigator Web log

Table 2: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
Gplus Adapter for Siebel 7; Siebel E-mail	• **Mandatory: Siebel Server version and platform** • Siebel Configuration expert (`.def` file) • List of used profiles (for example, voice, chat, e-mail) • Adapter logs • ICS MS-TServer log • RouterSubmitter log
Gplus Adapter for Siebel 7; Configuration Synchronization	• **Mandatory: Siebel Server version and platform** • Siebel Configuration expert (`.def` file) • List of used profiles (for example, voice, chat, e-mail) • Adapter logs • Configuration Server log

6.x Products

Table 3 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product. This list will be updated as more product milestones occur.

Table 3: Information to Supply with 6.x Support Request

Product	Information to Supply with the Support Request
Desktop (Active X Desktop Toolkit, Java Desktop Toolkit, Simulator Test Toolkit)	• T-Server information (see the entry for T-Server). • Application source code.
GCN Thick	• Scenario of the problem. • Screenshots of desktops showing the problem. • Configuration options export and applications mentioned on `Connections` tab (screenshot). • Name(s): `IUADTrace.log` • Where: the root of the drive • How: Needs to be turned on via the registry: Navigate to: `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Trace`; then add a new string-value: `GCN/on`. **Note:** These should *only* be turned on for debugging, and should *not* be left on, since they will use a lot of resources.
GCN Web	• Scenario of the problem. • Screenshots of desktops showing the problem. • Configuration options export and applications mentioned on `Connections` tab (screenshot). • Name(s): `Business.log` (unless changed in the Configuration Layer), and `Ail.log`. • Where: `Business.log` will write in the “logs” directory of the Tomcat instance; `Ail.log` will write in the “bin” directory where Tomcat is installed. **Note:** `Business.log` is configured in the Configuration Layer; `Ail.log` is configured in the `conf` file. Typically, both are automatically configured to write. The `Ail.log` increments automatically (for example: `Ail.log.1`, `Ail.log.2`, etc.).

Table 3: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Gplus SAP Server	• `gadapter-sap.ini` and `saprcf.ini` files. • log file (defined in OUTPUTFILENAME parameter in `gsadapter-sap.ini`, DETAILSLEVEL=DEBUG_LEVEL). • DB Server information (see the entry for DB Server). • Campaign Manager information (see the entry for Campaign Manager). • MS SQL exact version and service pack. • Name(s): The name the file when saved at the time it was captured. • Where: The log is saved by selecting `File->Save As`. • How: Third Party software called "Debug View" must be downloaded from: `http://www.sysinternals.com`. **Note:** Debug view is freeware. These logs should only be turned on for debugging and not left on permanently (especially in production), since they will use a lot of resources.
Gplus SAP Server Routing	• `gadapter-sap.ini` and `saprcf.ini` files. • log file (defined in OUTPUTFILENAME parameter in `gsadapter-sap.ini`, DETAILSLEVEL=DEBUG_LEVEL). • DB Server information (see the entry for DB Server). • Interaction Router information (see the entry for Interaction Router). • Strategy used. • MS SQL exact version and service pack. • Name(s): The name the file when saved at the time it was captured. • Where: The log is saved by selecting `File->Save As`. • How: Third Party software called "Debug View" must be downloaded from: `http://www.sysinternals.com`. **Note:** Debug view is freeware. These logs should only be turned on for debugging and not left on permanently (especially in production), since they will use a lot of resources.

Table 3: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Gplus Configuration Adapter for Siebel 7	• Configuration Adapter log files. • Configuration Options Export (Configuration Manager Application). • Screen capture.
Gplus Email Adapter for Siebel 7	• MS T-Server log files. • Siebel Communications Server log files.
Gplus SAP WinClient	• Screen capture. • Internet Contact Solution Information (see the entry for Internet Contact Solution). • Name(s): The name of the file when saved at the time it was captured. • Where: The log is saved by selecting `File->Save As`. • How: Third Party software called "Debug View" must be downloaded from: `http://www.sysinternals.com`. **Note:** Debug view is freeware. These logs should only be turned on for debugging and not left on permanently (especially in production), since they will use a lot of resources.
Gplus Multimedia Adapter for Siebel 7	• MS T-Server log files. • Gplus Multimedia Adapter log files. • Siebel Communications Server log files. • GCN Web Business log files. • Screen capture. • Name(s): `Scomm log`, `Gplus log`, `business.log`, and `Ail.log`. • Where: `Business.log` will write in the “logs” directory of the Tomcat instance; `Ail.log` will write in the “bin” directory where Tomcat is installed. **Note:** `Business.log` is configured in Configuration Manager; `Ail.log` is configured in the `conf` file. Typically both are automatically configured to write. The `Ail.log` increments automatically (ex `ail.log.1`, `ail.log.2`, etc.). **Note:** This adapter integrates GCN Web into the Siebel interface.

Table 3: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Gplus Adapter for Siebel eBusiness 2000	• Screen capture. • Siebel exact version. • Application log file. • T-Server information (see the entry for T-Server). • Stat-Server information (see the entry for Stat-Server). • Internet Contact Solution information (see the entry for Internet Contact Solution) when applicable. • Debug view log files. • Name(s): The name of the file when saved at the time it was captured. • Where: The log is saved by selecting `File->Save As`. • How: Third Party software called "Debug View" must be downloaded from: `http://www.sysinternals.com`. **Note:** Debug view is freeware, these logs should only be turned on for debugging and not left on permanently (especially in production), since they will use a lot of resources.
Gplus Adapter for People Soft	• Adapter log file. • Screen capture. • T-Server information (see the entry for T-Server). • Stat-Server information (see the entry for Stat-Server). • Internet Contact Solution information (see the entry for Internet Contact Solution) when applicable. • Name(s): `log.txt`. • Where: the root of the drive. • How: Needs to be turned on via the registry: Two `dword` values must be added to registry (LogLevel and LogCategory). ◦ Navigate to [HKEY_CURRENT_USER\Software\GCTI\Gplus\6.5\PSFT]. ◦ Add "LogLevel"=dword:00000002 and "LogCategory"=dword:ffffffff **Note:** These should *only* be turned on for debugging and not left on permanently, (especially in production), since they will use a lot of resources.

Table 3: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Gplus Outbound Server Adapter for Siebel 7	• Outbound Server Adapter log files. • Configuration Options Export (Configuration Manager Application). • Screen capture.
Gplus Outbound Voice Adapter for Siebel 7	• T-Server log files. • Gplus Outbound Voice Adapter log files. • Siebel Communications Server logs. • Screen capture.
Gplus Voice Adapter for Siebel 7	• T-Server log files. • GP Voice Adapter log files. • Siebel Communications Server log files. • Screen Capture. • Name(s): `Scomm log, Gplus log` • Where: `Scomm log` is a Siebel log and writes in the Siebel server "logs" directory. The `Gplus.log` writes wherever it is configured to write in the driver parameters. The location is documented in the *Gplus Adapters 6.5 for Siebel 7 Deployment Guide* which can be found here: http://genesyslab.com/support/dl/retrieve/default.asp?item=ACD1197663705D3A970491D51B5DA2CA&view=item

Chapter

3 Framework

Products/areas within this category include:

- IP T-Servers
- Load Distribution Server
- Management Framework
- Network T-Servers
- SNMP
- T-Servers

This chapter covers the following topics:

Architecture

This section includes architecture diagrams for Framework.

Framework

Figure 9 shows connections that Framework components establish to each other and to Genesys solutions.

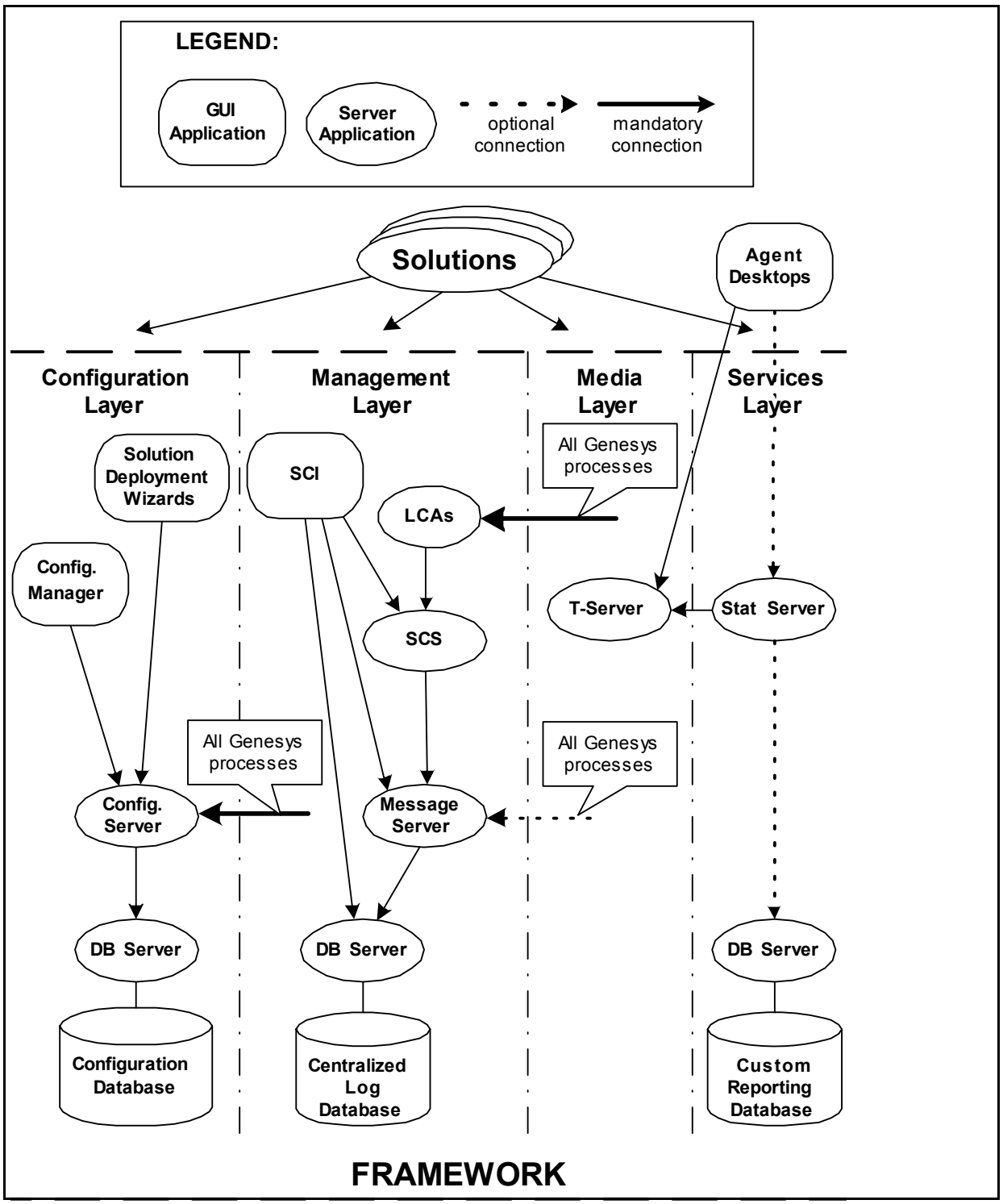


Figure 9: Detailed Framework Architecture

Configuration Layer

Figure 10 shows the structure of the Configuration Layer.

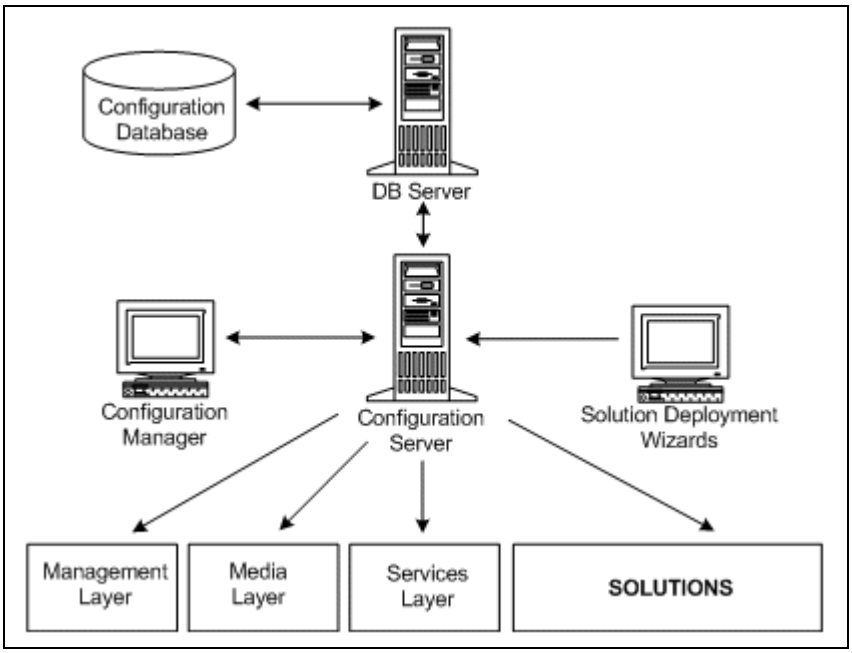


Figure 10: Configuration Layer Architecture

Management Layer

Figure 11 shows the structure of the Management Layer.

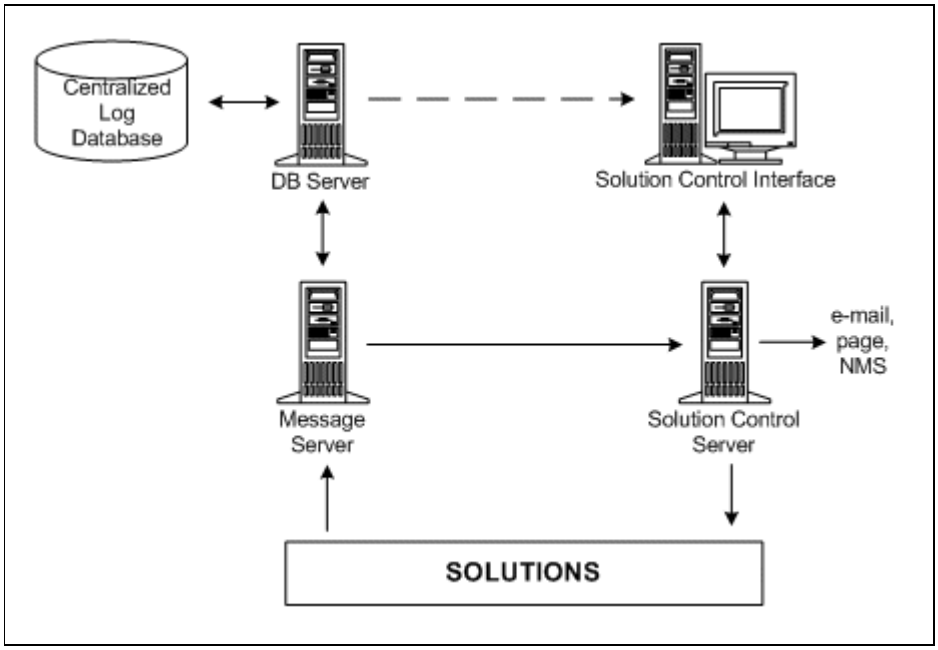


Figure 11: Management Layer Architecture

Media Layer

Figure 12 shows the structure of the Media Layer.

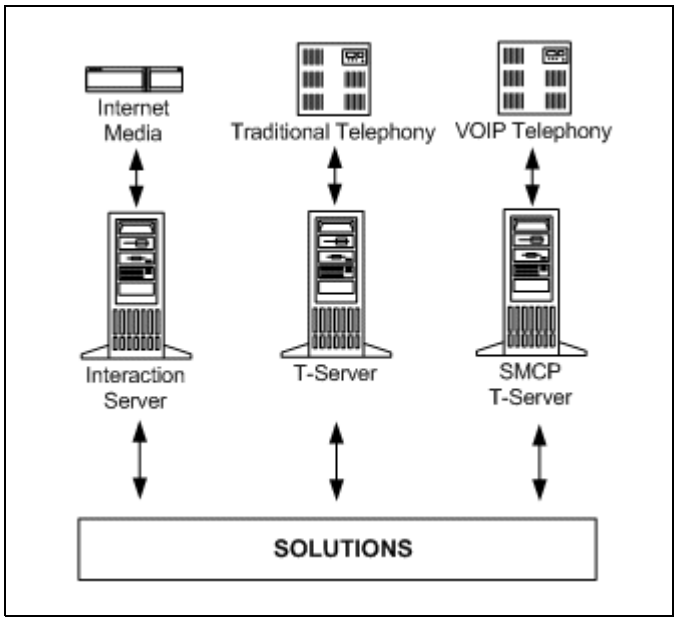


Figure 12: Media Layer Architecture

Services Layer

Figure 13 shows the structure of the Services Layer.

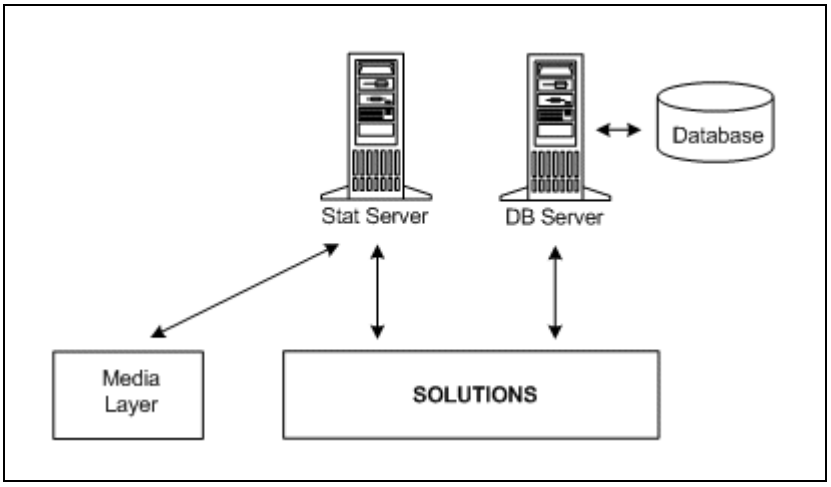


Figure 13: Services Layer Architecture

7.x Products

Table 4 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product. This list will be updated as more product milestones occur.

Table 4: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Configuration Manager	• Configuration Server information (see the entry for Configuration Server) • DB Server information (see the entry for DB Server). • Configuration Manager screen captures that show the problem
Configuration Server	• Configuration Server configuration file • Configuration Server log file covering the period when the problem occurred • DB Server information (see the entry for DB Server) • Configuration Database (Configuration Manager) export
Configuration Conversion Wizard	• Export of the Configuration Database (Configuration Manager) to be converted • DB Server information (see the entry for DB Server) • CCW log file
Configuration Import Wizard	• Source file to be imported • Screen captures that show the problem • DB Server log files covering the period when the problem occurred • Configuration Server log files covering the period when the problem occurred • Configuration Database (Configuration Manager) export
DB Server	• DB Server configuration • DB Server log files covering the period when the problem occurred
HA Proxy	• HA Proxy configuration options • HA Proxy log files with Debug level detail covering the period when the problem occurred • T-Server information (see the entry for T-Server)

Table 4: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
License Manager	• Application log files covering the period when the problem occurs (from the application that experiences problems with licensing) • License file • A listing of the environment settings • License Manager log file covering the period in which the problem occurred • License Manager start-up file
Load Distribution Server	• LDS Configuration • LDS related configuration options in Receivers if configured ([LDS] section in Universal Routing Server(s) or Call Concentrator (s)) • LDS logfile covering the period for when the problem occurred • TServer(s) that LDS is configured to connect to; log file covering the period for when the problem occurred • LDS receivers log file (either Universal Routing Server(s) or Call Concentrator (s))
Local Control Agent	• LCA log files covering the period when the problem occurred
Message Server	• Message Server configuration • Message Server log file covering the period when the problem occurred • Information regarding DB Server responsible for Log Database (see the entry for DB Server) • LCA information (see the entry for LCA) if applicable
Network T-Servers	See the entry for T-Servers
Solution Control Interface	• Screen captures that show the problem • Solution Control Server information (see the entry for Solution Control Server)
Solution Control Server	• Solution Control Server configuration • Solution Control Server log files covering the period when the problem occurred • Message Server information (see the entry for Message Server) if applicable • LCA information (see the entry for LCA) if applicable

Table 4: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
T-Servers Network T-Servers	• T-Server configuration • T-Server log files with Debug level detail covering the start-up of the T-Server • T-Server log file with Debug level detail covering the period when the problem occurred
T-Server - ISCC (Inter Server Call Control)	• Local ISCC configuration • Remote ISCC configuration • Local T-Server information (see the entry for T-Server) • Remote T-Server information (see the entry for T-Server)

6.x Products

Table 5 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product. This list will be updated as more product milestones occur.

Table 5: Information to Supply with 6.x Support Request

Product	Information to Supply with the Support Request
Configuration Manager	• Configuration Server information (see the entry for Configuration Server) • DB Server information (see the entry for DB Server) • Configuration Manager screen captures
Configuration Server	• Configuration Server configuration start-up file • Configuration Server log file covering the period in which the problem occurred • DB Server information (see the entry for DB Server) • Configuration Database export (Configuration Manager)
Configuration Conversion Wizard	• CCW configuration • Export of the Configuration Database (CME) to be converted • DB Server information (see the entry for DB Server) • CCW log file

Table 5: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Configuration Import Wizard	• Source file to be imported • Screen capture covering the period in which the problem occurred
DB Server	• DB Server configuration • DB Server log file covering the period in which the problem occurred (preferably where the configuration option `verbose` has been set to `3`)
HA Proxy	• HA Proxy configuration • HA Proxy log files • T-Server log files
License Manager	• License file • A listing of the environment settings • License Manager log file covering the period in which the problem occurred • License Manager start-up file
Load Distribution Server	• LDS Configuration • LDS related configuration options in Receivers if configured ([LDS] section in Universal Routing Server(s) or Call Concentrator (s)) • LDS logfile covering the period for when the problem occurred • TServer(s) that LDS is configured to connect to; log file covering the period for when the problem occurred • LDS receivers log file (either Universal Routing Server(s) or Call Concentrator (s))
Local Control Agent	• LCA log which can be created by redirection of the LCA output to a file: ◦ On Windows: LCA 4999 2>log.file ◦ On Unix: LCA 4999 > log 2>&1 • If LCA runs as Windows service the output cannot be redirected

Table 5: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Message Server	• Message Server configuration • Message Server log file covering the period up to when the problem occurred • Information regarding DB Server responsible for Log Database (see the entry for DB Server) • LCA information (see the entry for LCA) if applicable
Network Overflow Manager	• NOM configuration • NOM log file covering the period in which the problem occurred • Local T-Server information (see the entry for T-Server) • Remote T-Server information (see the entry for T-Server) • Local and remote T-Server log files with Debug level detail
Solution Control Interface	• Screen capture • Solution Control Server information (see the entry for Solution Control Server)
Solution Control Server	• Solution Control Server configuration • Solution Control Server log file covering the period up to when the problem occurred (preferably where the configuration option 'verbose' has been set to 'all') • Message Server information (see the entry for Message Server) if applicable • LCA information (see the entry for LCA) if applicable
T-Server	• T-Server configuration • T-Server log file covering the start-up of the T-Server with Debug level detail • T-Server log file covering the period when the problem occurred with Debug level detail
Wizards	• Screen Shots • Configuration Manager export file

Chapter

4 Informiam

Products/areas within this category include:

- Call Analyzer
- Workforce Utilization
- Frontline Advisor
- Historical Advisor
- LightSpeed
- Silverado
- ITOps

This chapter covers the following topics:

Architecture

This section includes architecture diagrams for the Informiam product line. Figure 14 illustrates the Informiam architecture.

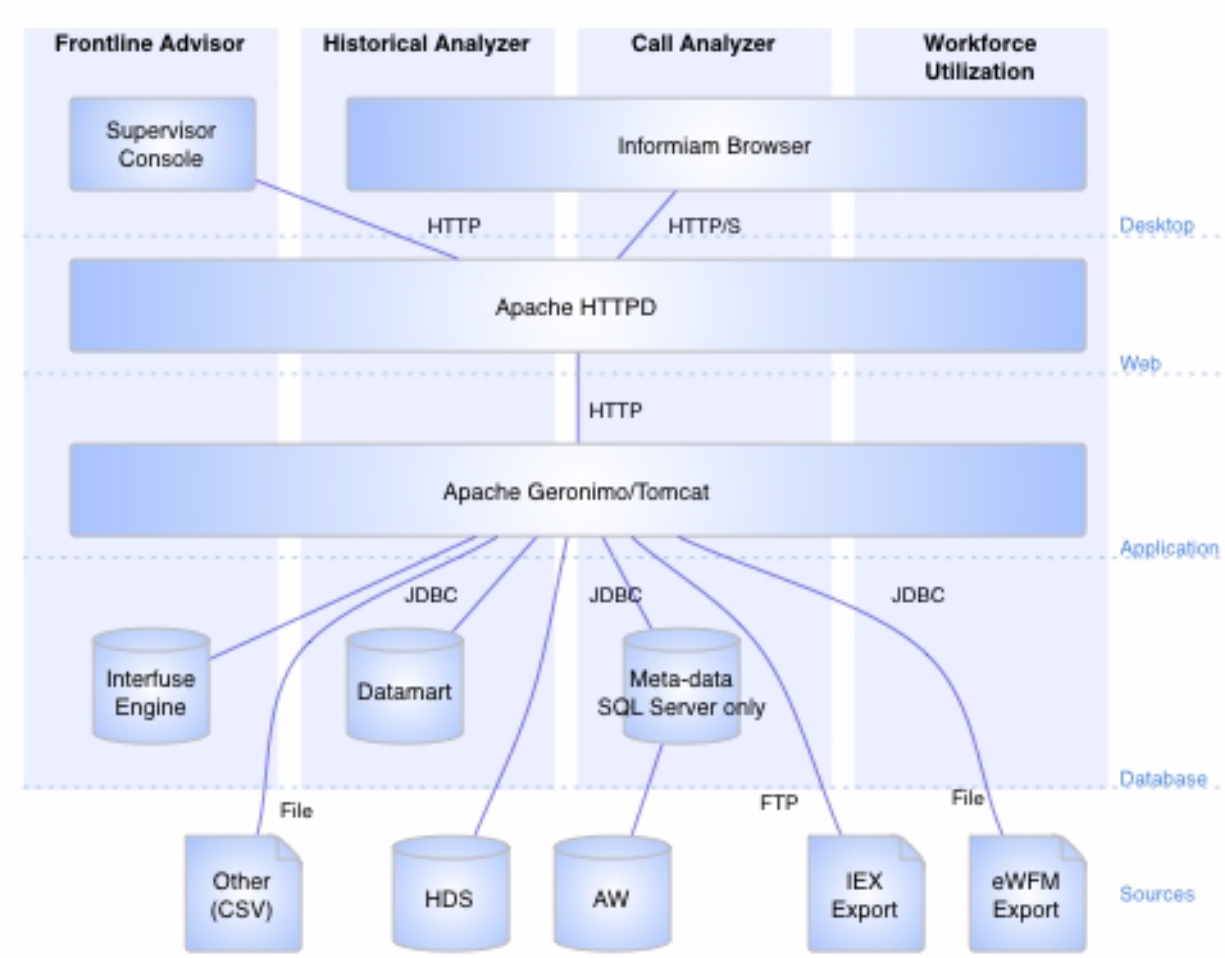


Figure 14: Architecture

Figure 15 illustrates the architecture for a large enterprise using Informiam software.

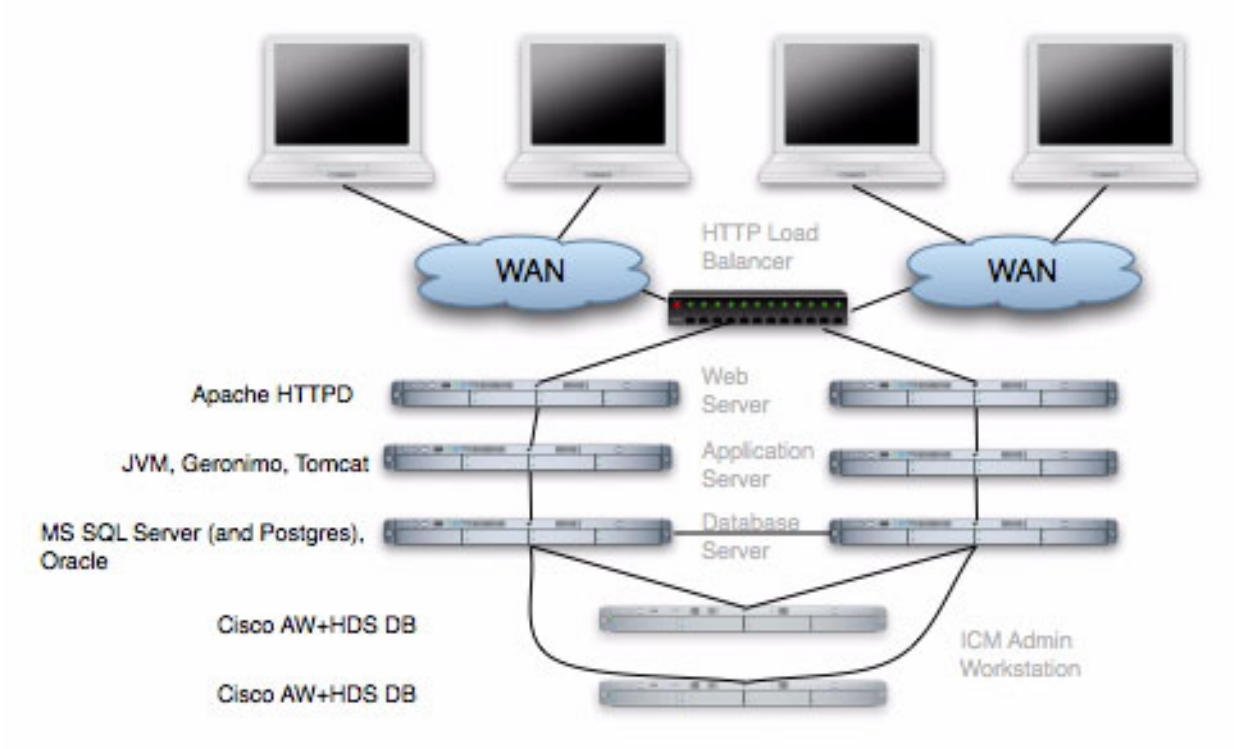


Figure 15: Large Enterprise Architecture

2.x Products

Table 6 details the product-specific information that should be supplied when logging a support request in relation with a particular Informiam product. This list will be updated as more product milestones occur.

Table 6: Information to Supply with the Support Request

Product	Information to Supply with the Support Request
Call Analyzer	• Source of Calling Data. • Detailed description of the issue, and how to reproduce it, if applicable • Informiam Player screen captures that show the problem.
Workforce Utilization	• Source for Forecast and Staffing information. • Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.

Table 6: Information to Supply with the Support Request (Continued)

Product	Information to Supply with the Support Request
Frontline Advisor	• Source of Staffing Data. • Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.
Historical Analyzer	• Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.
LightSpeed	• Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.
Silverado	• Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.
ITOps	• Detailed description of the issue, and how to reproduce it, if applicable. • Informiam Player screen captures that show the problem.

Chapter

5 Multimedia

Products/areas within this category include:

- 3rd Party Routing for Siebel E-mail
- E-mail Interaction
- Internet Contact Solution (ICS) IKnow
- ICS Web Collaboration
- Internet Contact Solution
- Content Analyzer
- Multi-Channel Routing
- Open Media Interaction
- Web Interaction

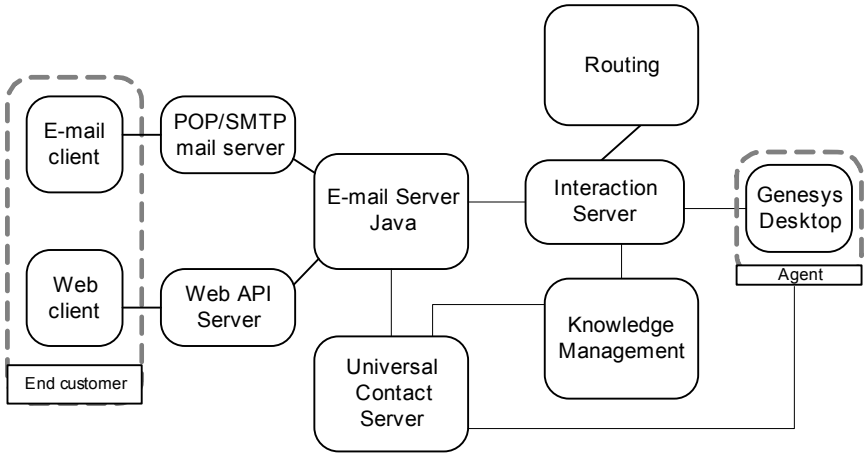
This chapter covers the following topics:

Architecture

This sections contains graphics for some of products mentioned in this chapter. Please refer to the Deployment Guide for the respective products for additional information.

Multimedia 7.2

Figure 16 illustrates the architecture for Multimedia 7.2.



Each Genesys component also connects to Configuration Server database for configuration data.

Figure 16: Multimedia 7.2 Architecture

Internet Contact Solution 6.x

Figure 17 is an overall diagram of the components involved in web interactions for Internet Contact Solution.

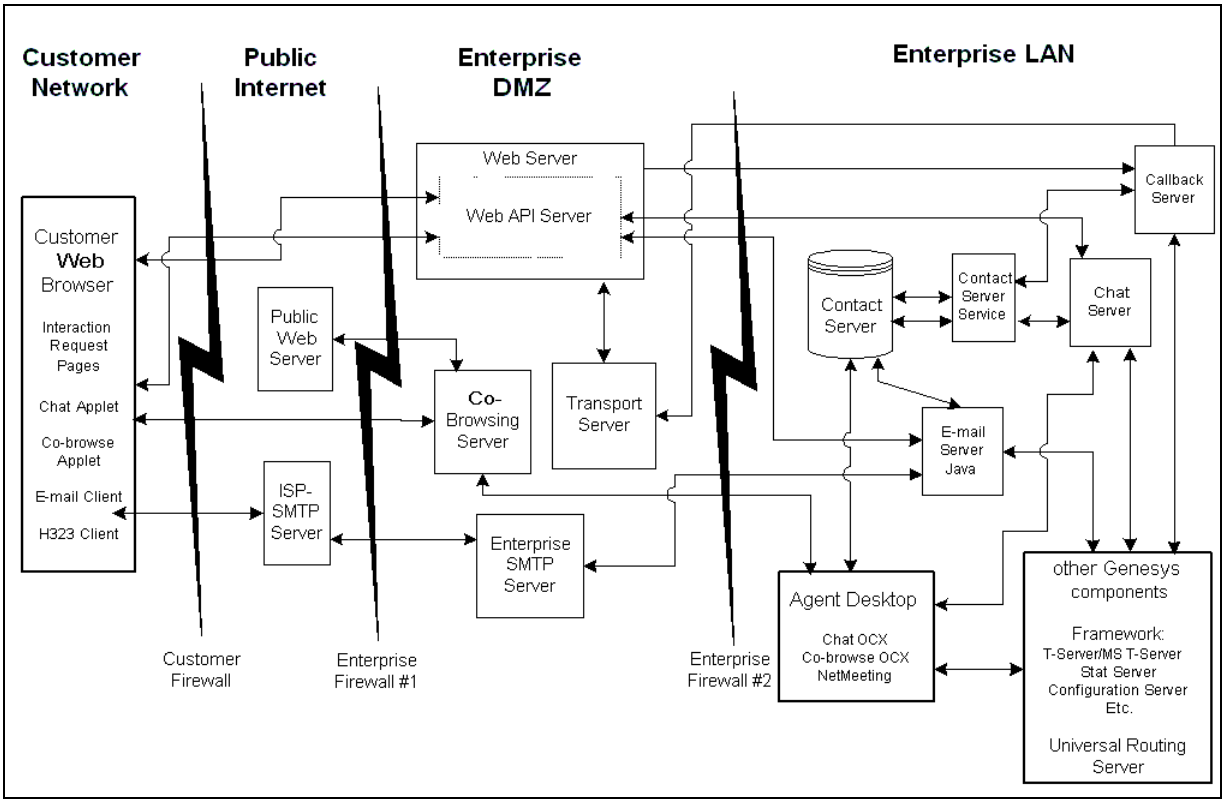


Figure 17: Internet Contact Solution 6.x Architecture

7.x Products

Table 7 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product. This list will be updated as more product milestones occur.

Table 7: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Multi-Channel Routing/ Multimedia	• Interaction Server log • Universal Contact Server log • Log of Media Server affected (for example, chat, e-mail, and so on), if applicable • Genesys Agent Desktop log, if applicable • If there are routing problems: ◆ Universal Routing Server log ◆ Export of Strategies and Business Processes
Multi-Channel Routing Knowledge Manager	• Universal Contact Server log • Knowledge Manager log • Training Server log, if applicable

6.x Products

Table 8 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product. This list will be updated as more product milestones occur.

Table 8: Information to Supply with 6.x Support Request

Product	Information to Supply with the Support Request
Internet Contact Solution - Email Inbound	• T-Server information (see the entry for T-Server) • Interaction Router information (see the entry for Interaction Router) • Strategy (`.rbn`) files that were loaded • Media Link log file covering the period in which the problem occurred • E-mail Server log file covering the period in which the problem occurred (in case of e-mail via client's application) • Trace file (typically stored in the GCTI \Trace directory) covering the period when the problem occurred • `Problematic.msg` file if applicable (in case of e-mail via the client's application) • WIRS Log covering the period in which the problem occurred (in case of e-mail via Web) • DBServer log file covering the period in which the problem occurred
Internet Contact Solution - Email Outbound	• E-mail Server log file covering the period in which the problem occurred • Trace file (typically stored in the GCTI \Trace directory) covering the period in which the problem occurred • Problematic.msg file, if applicable • DBServer log file covering the period in which the problem occurred

Table 8: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Internet Contact Solution - Chat	• T-Server information (see the entry for T-Server) • Interaction Router information (see the entry for Interaction Router) • Strategy (`.rbn`) files that were loaded • Media Link log file covering the period in which the problem occurred • Chat Server log file covering the period in which the problem occurred • Socket Server log file covering the period in which the problem occurred • Trace file (typically stored in the GCTI \Trace directory) covering the period when the problem occurred • WIRS Log covering the period when the problem occurred • JRun log files • JRun 'local.properties' file

Table 8: Information to Supply with 6.x Support Request (Continued)

Product	Information to Supply with the Support Request
Internet Contact Solution - Call Back or VoIP	• T-Server information (see the entry for T-Server) • Callback Server log covering the period in which the problem occurred • WIRS Log covering the period in which the problem occurred • Interaction Router information (see the entry for Interaction Router) • Strategy (`.rbn`) files that were loaded • Socket Server log file (if tunneling is used) • Media Link log file covering the period in which the problem occurred • DBServer log file covering the period in which the problem occurred
Internet Contact Solution - Agent Desktop	• Information if it is customized or standard Desktop • Trace file (typically stored in the GCTI \Trace directory) covering the period when the problem occurred • Screen capture of error messages or GUI problems if applicable. • Media Link log file covering the period when the problem occurred • DB Server log file covering the period when the problem occurred

Chapter

6 Outbound

Products/areas within this category include:

- Outbound Contact

This chapter covers the following topics:

Architecture

Figure 18 shows an architecture diagram of Outbound Contact with Call Process Detection (CPD) from a switch.

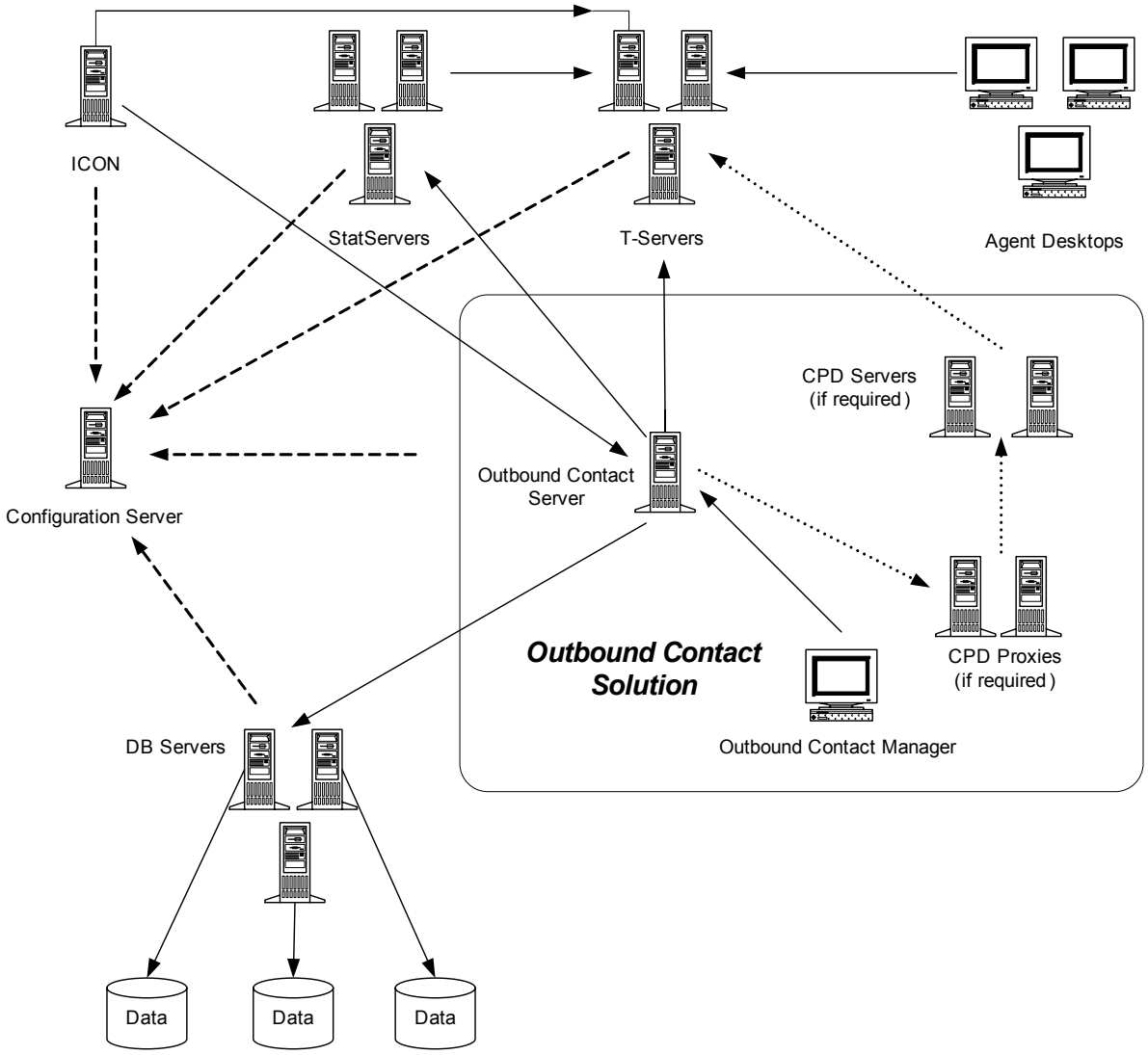


Figure 18: Outbound Contact Architecture

Figure 19 shows an architecture diagram of Outbound Architecture with CPD from a dialogic board.

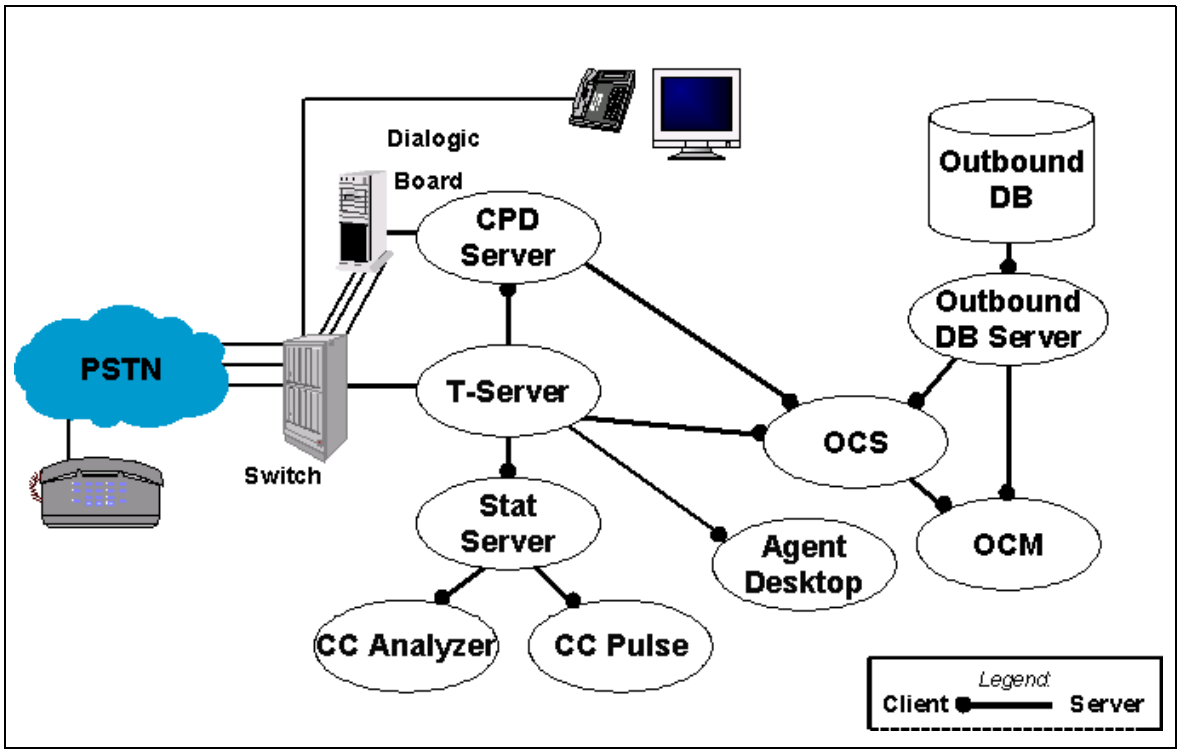


Figure 19: Outbound Architecture with CPD from a Dialogic Board

7.x Products

Table 9 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product. This list will be updated as more product milestones occur.

Table 9: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Outbound Contact Server	• Outbound Contact Server log • T-Server log • In some cases, export of the Calling Lists • If CPD Server is the user, the Call Progress Detection Server log

Table 9: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
Outbound Contact Manager (OCM)	• OCM screenshot • An export of the Calling Lists • DB Server log
Call Progress Detection (CPD) Server	• Call Progress Detection Server log • Outbound Contact Server log • T-Server log • If there is a tone detection problem, Calls Recordings

6.x Products

Table 10 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product. This list will be updated as more product milestones occur.

Table 10: Information to Supply with 6.x Support Request

Product	Information to Supply with the Support Request
Outbound Contact Server (OCS)	• OCS log file covering the period in which the problem occurred • T-Server information (see the entry for T-Server) • DB Server information (see the entry for DB Server) • Screen capture if configuration issue
Outbound Contact Manager (OCM)	• Screen capture • Call Lists exports, if applicable • DB Server information (see the entry for DB Server)

Chapter

7 Reporting

Products/areas within this category include:

- CC Analyzer/CCPulse+
- Call Concentrator
- Genesys Info Mart
- Real-Time Metrics Engine
- Stat Server
- Reporting Templates

This chapter covers the following topics:

Architecture

This section includes architecture diagrams for Reporting.

Reporting Layer

Figure 20 illustrates reporting as part of the CIM (Customer Interaction Management) components. Figure 21 illustrates the structure of the Reporting architecture.

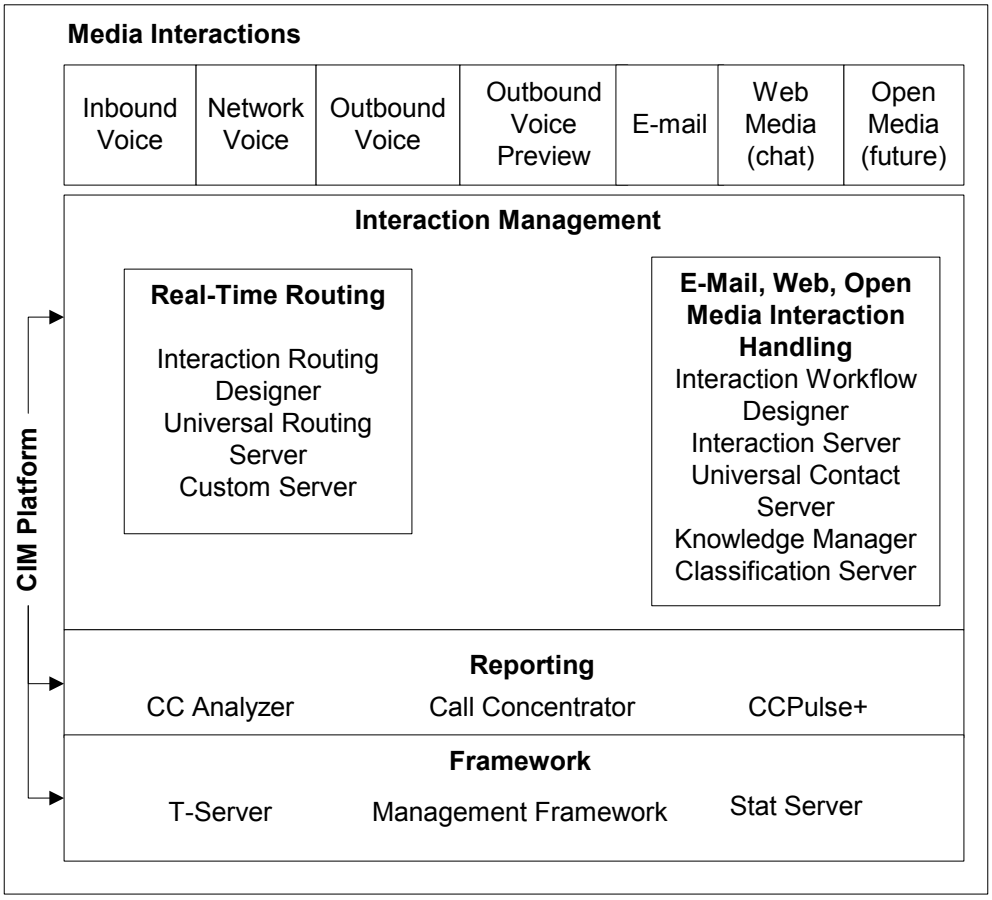


Figure 20: Reporting as Part of the CIM Platform

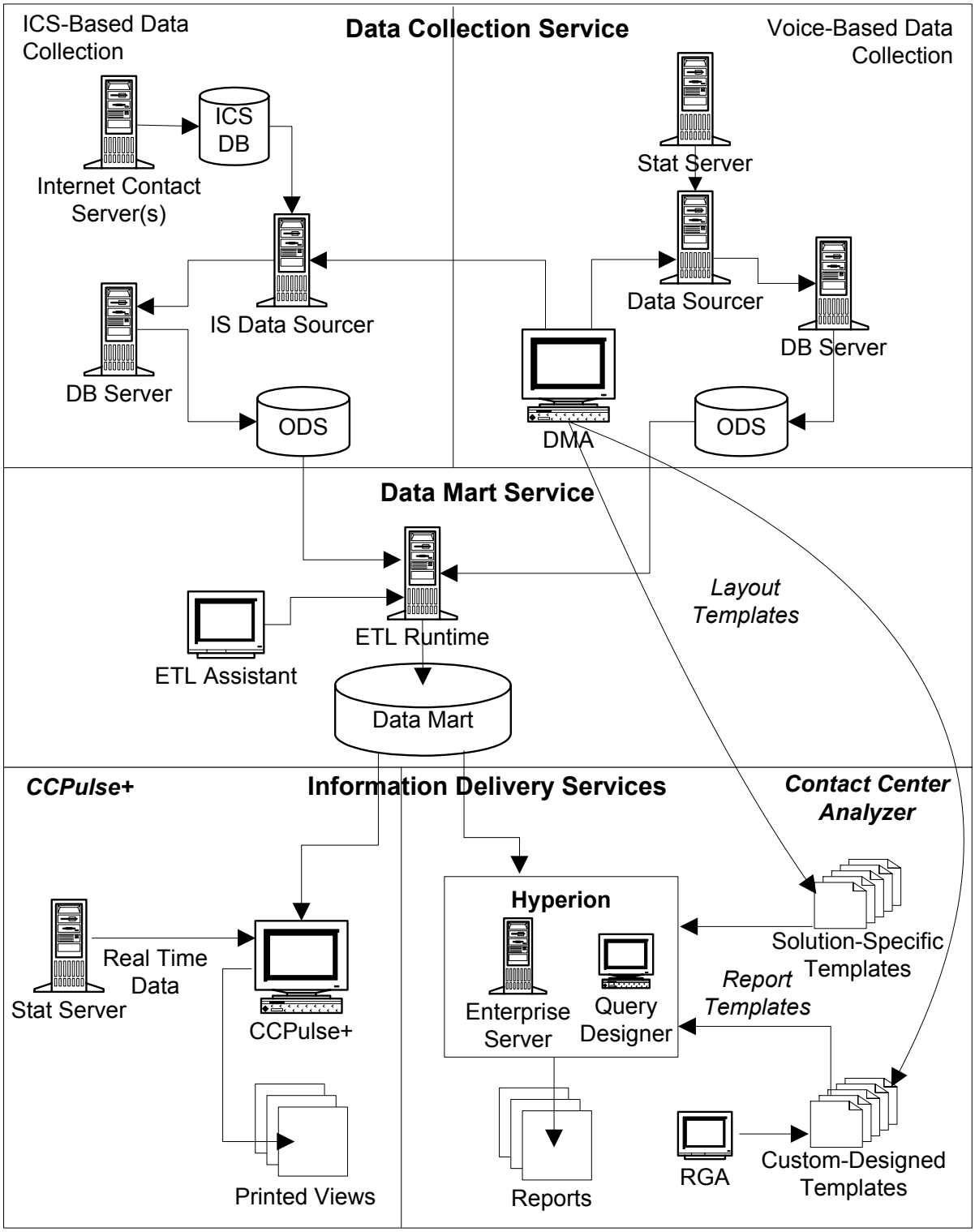


Figure 21: Reporting Architecture

Genesys Info Mart 7.2

Figure 22 illustrates the architecture for Genesys Information 7.2.

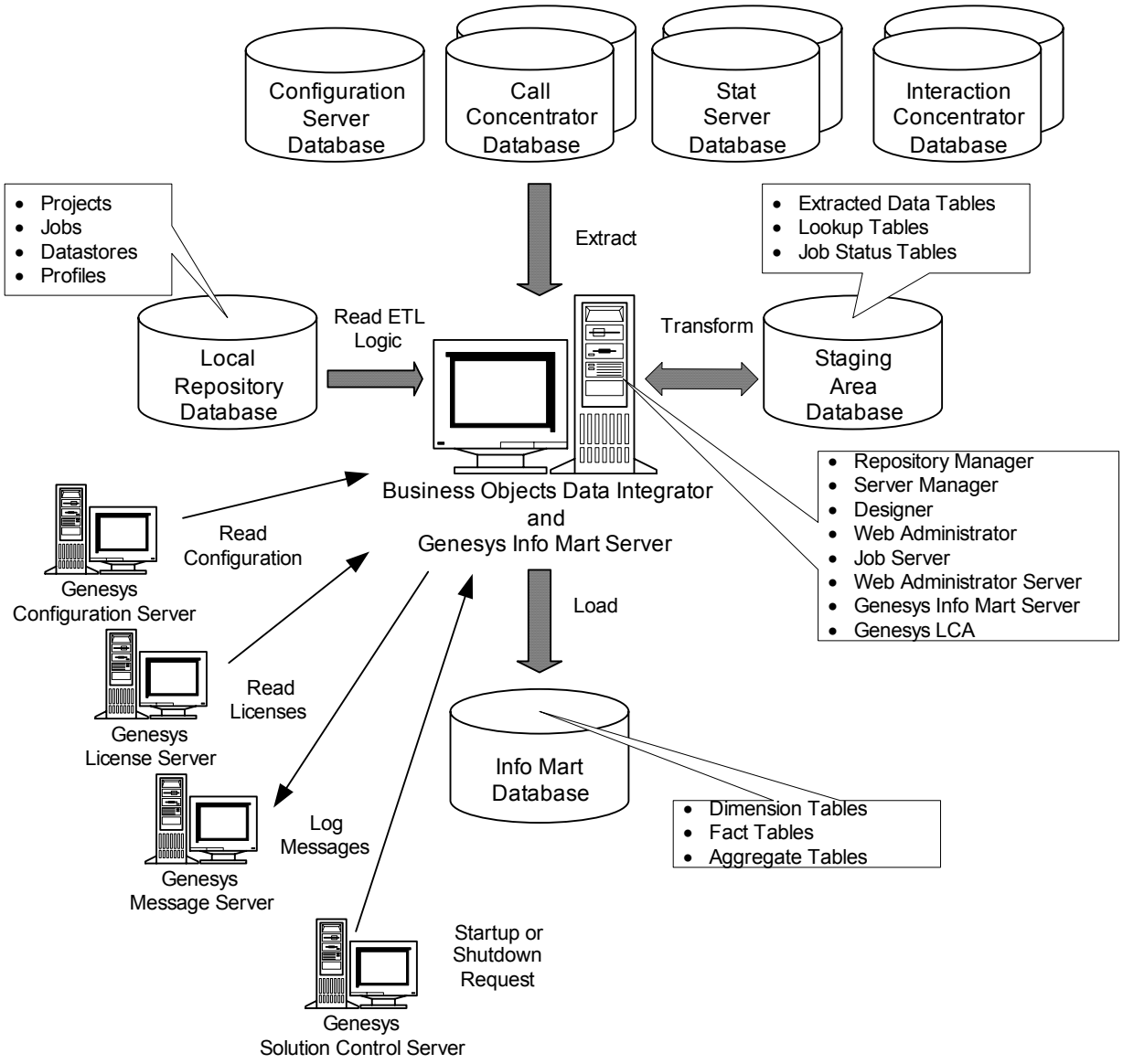


Figure 22: Genesys Info Mart 7.2 Architecture

Call Concentrator 7

Figure 23 illustrates the data sources from which Call Concentrator collects information.

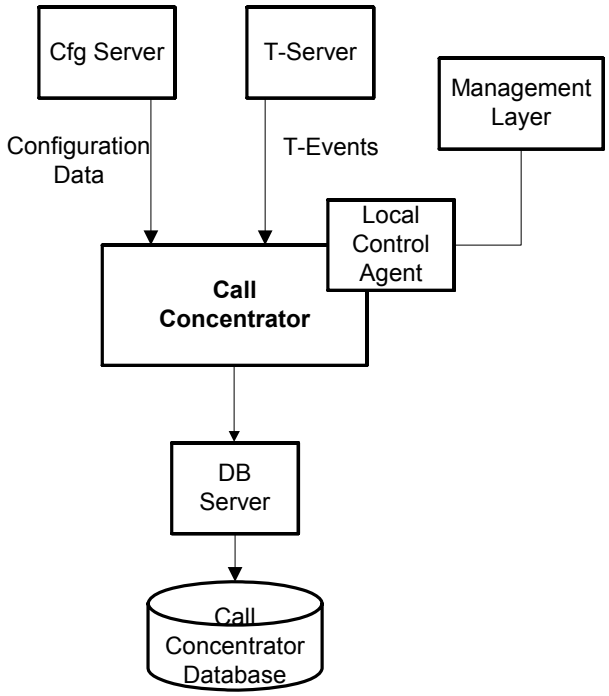


Figure 23: Call Concentrator Data Sources

7.x Products

Table 11 details the product-specific information that should be supplied when logging a support request for a problem with a particular Genesys 7.x product.

Table 11: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Brio Broadcast Server	• Screen capture of the problem if applicable • Broadcast Server log: `BQServer.log` • Broadcast Server logs reflecting a particular Job execution details if applicable; such log file names contain a job ID and the Server name and always have an extension “log” • The report file that introduced the problem
Brio OnDemand Server	• Screen capture of the problem if applicable • OnDemand Server ini file: `ODS.ini` • OnDemand Server logs: `ODSManager.log`, `ODSNode.log`, `DbgPrint` (log files whose names start with “DbgPrint” symbols), preferably where the configuration option BQ_START_LOG has been set to ‘debug’) • The report file that introduced the problem
Brio Query Designer	• Screen capture of the problem if applicable • The report file that introduced the problem
CCPulse+	• Screen capture • Stat Server information (see the entry for Stat Server) • T-Server information (see the entry for T-Server) • CCPulse Storage files (references for the Storage files are stored in the CCPulse+ configuration options)
Call Concentrator	• Call Concentrator configuration • Call Concentrator log files covering the period when the problem occurred • T-Server(s) log files covering the period when the problem occurred • Load Distribution Server log files covering the period when the problem occurred (if applicable) • Configuration Database (Configuration Manager) export • DB Server information (see the entry for DB Server)-copies/extracts of the CCON tables (GCDR, SCDR, etc.)

Table 11: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
CCA Data Sourcer	• Screen capture of Data Modeling Assistant if it indicates the problem • Data Sourcer configuration • Data Sourcer log covering the period in which the problem occurred (preferably from startup) • Stat Server information (see the entry for Stat Server) • RDBMS type and version
CCA ETL Runtime	• ETL Runtime configuration (exported from Configuration Manager) • ETL Runtime configuration (`*.properties`) • ETL Runtime log covering the period in which the problem occurred (preferably from startup) or CCA Starter log in case CCA Starter is used to launch ETL Runtime • Screen capture of the report if it indicates the problem • The report file saved with query results if the report indicates the problem (in case Brio Query Designer is used for reports generation) • JRE version • RDBMS type and version
CCA IS Data Sourcer	• Screen capture of Data Modeling Assistant if it indicates the problem • IS Data Sourcer configuration • IS Data Sourcer log covering the period in which the problem occurred (preferably from startup) • Contact Server application configuration • JRE version • RDBMS type and version
CCA Reporting Templates	• Screen capture of the report indicating the problem • The report file saved with query results
CCA Starter	• CCA Starter configuration • CCA Starter log

Table 11: Information to Supply with 7.x Support Request (Continued)

Product	Information to Supply with the Support Request
Genesys Info Mart	• Business Objects Data Integrator job logs (Trace, Monitor, and Error) for a particular job or a set of jobs, which ran during the period when the problem occurred. Separate log files for each job are stored in the Log subdirectories of the Data Integrator install directory. In the Log/jobserver_name/repository_name subdirectory, zip `*mm_dd_yyyy*.txt*` files after substituting the appropriate date values. Also, zip `*.txt*` in the Log subdirectory. • `DSCosnfig.txt` file in the Bin subdirectory of the Data Integrator install directory. • Genesys Info Mart local log and configuration files in the Info Mart install directory (zip `gim_etl*.*` files). • Software and hardware configuration information for Job Server machine, database client, and database servers. • Depending on the symptoms of the problem, Genesys Engineering may request full or partial dumps of Info Mart's staging area database. In some cases, full or partial dumps of the Info Mart's data source databases (Configuration Server, Call Concentrator, and Stat Server) may be required. Also, partial dumps of the Info Mart database may be required.
Stat Server	• Stat Server configuration • Stat Server log file covering the period up to when the problem occurred (preferably where the configuration option "DebugLevel" has been set to "all"); this should try to include relevant agent logins, other client (IR, CCPulse, and so on) connections which include the OpenStat requests • T-Server information (see the entry for T-Server) • Stat Server table dumps if applicable • DB Server information if applicable (see the entry for DB Server)

6.x Products

Table 12 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 12: Information to Support with 6.x Service Request

Product	Information to Supply with the Support Request
• Brio Broadcast Server	• Screen capture of the problem if applicable • Broadcast Server log: `BQServer.log` • Broadcast Server logs reflecting a particular Job execution details if applicable; such log file names contain a job ID and the Server name and always have an extension “log” • The report file that introduced the problem
• Brio OnDemand Server	• Screen capture of the problem if applicable • OnDemand Server ini file: `ODS.ini` • OnDemand Server logs: `ODSManager.log`, `ODSNode.log`, `DbgPrint` (log files whose names start with “DbgPrint” symbols), preferably where the configuration option BQ_START_LOG has been set to “debug”) • The report file that introduced the problem
Brio Query Designer	• Screen capture of the problem if applicable • The report file that introduced the problem
Call Center Pulse	• Screen capture • Stat Server information (see the entry for Stat Server) • T-Server information (see the entry for T-Server) • CCPulse Storage files (references for the Storage files are stored in the CCPulse configuration options)
Call Concentrator	• Call Concentrator configuration • Call Concentrator log covering the period in which the problem occurred (preferably where the configuration option 'DebugLevel' has been set to 'all') • T-Server information (see the entry for T-Server) • DB Server information (see the entry for DB Server) • Copies/extracts of the CCON tables (GCDR, SCDR, etc.)

Table 12: Information to Support with 6.x Service Request

Product	Information to Supply with the Support Request
CCA Data Sourcer	• Screen capture of Data Modeling Assistant if it indicates the problem • Data Sourcer configuration • Data Sourcer log covering the period in which the problem occurred (preferably from startup) • Stat Server information (see the entry for Stat Server) • RDBMS type and version
CCA ETL Runtime	• ETL Runtime configuration (exported from Configuration Manager) • ETL Runtime configuration (`*.properties`) • ETL Runtime log covering the period in which the problem occurred (preferably from startup) or CCA Starter log in case CCA Starter is used to launch ETL Runtime • Screen capture of the report if it indicates the problem • The report file saved with query results if the report indicates the problem (in case Brio Query Designer is used for reports generation) • JRE version • RDBMS type and version
CCA IS Data Sourcer	• Screen capture of Data Modeling Assistant if it indicates the problem • IS Data Sourcer configuration • IS Data Sourcer log covering the period in which the problem occurred (preferably from startup) • Contact Server application configuration • JRE version • RDBMS type and version
CCA Reporting Templates	• Screen capture of the report indicating the problem • The report file saved with query results

Table 12: Information to Support with 6.x Service Request

Product	Information to Supply with the Support Request
CCA Starter	• CCA Starter configuration • CCA Starter log
Stat Server	• Stat Server configuration • Stat Server log file covering the period up to when the problem occurred (preferably where the configuration option 'DebugLevel' has been set to 'all'); this should try to include relevant agent logins, other client (IR, CCPulse, and so on) connections which include the OpenStat requests • T-Server information (see the entry for T-Server) • Stat Server table dumps if applicable • DB Server information if applicable (see the entry for DB Server)

Note: After purchasing the Reporting Option, you must obtain a Brio license from Genesys Order Management (at orderman@genesyslab.com) to use the tools. Under this license, you can use Brio tools to access the CC Analyzer data source only. To obtain additional Brio licenses or use Brio to access non-CC Analyzer data sources, contact Hyperion at www.hyperion.com.

Chapter

8 Routing

Products/areas within this category include:

- Universal Routing
- Voice CallBack

This chapter covers the following topics:

Architecture

This section contains architecture diagrams for the products listed above.

Enterprise Routing 7.x

Figure 24 shows the general architecture for Enterprise Routing.

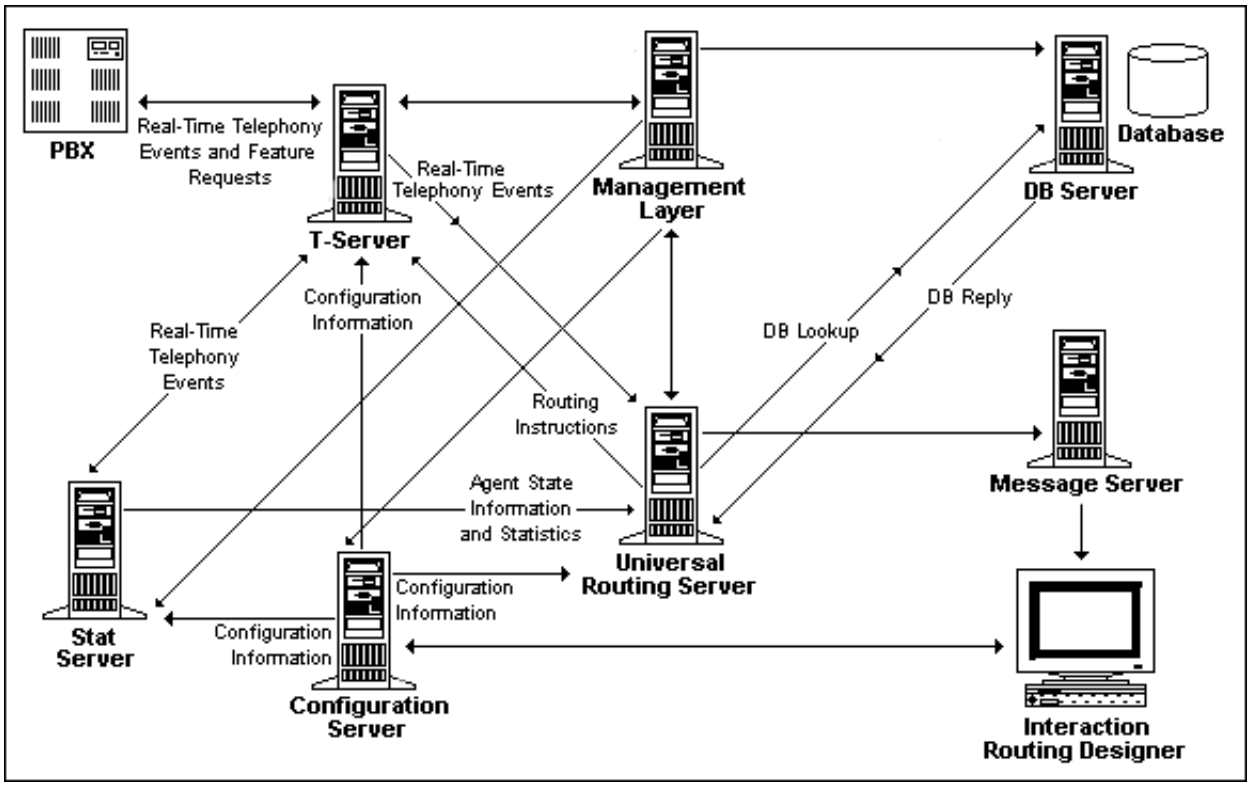


Figure 24: Enterprise Routing Architecture

Voice Callback 7.1

Figures 25, 26, and 27 illustrate Voice Callback (VCB) architecture in various configurations.

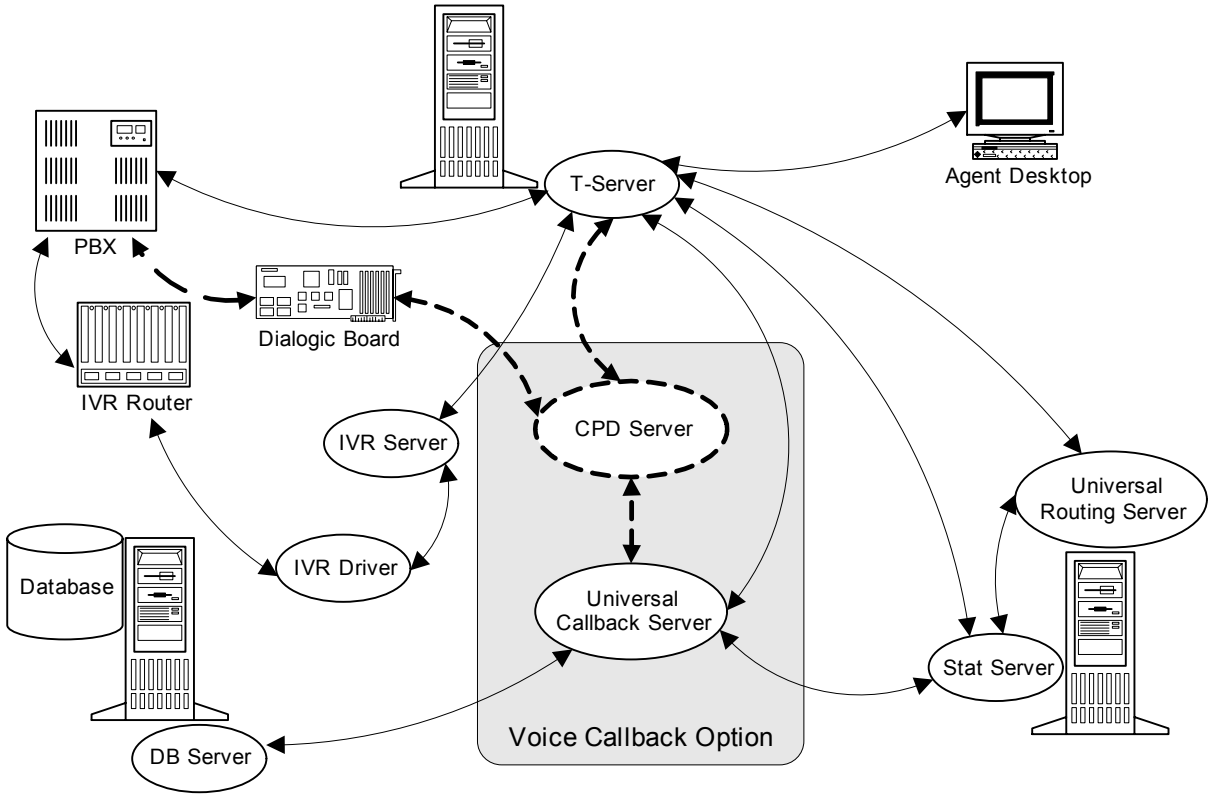


Figure 25: Interaction Between VCB and Other Components in IVR Behind--the-Switch Mode

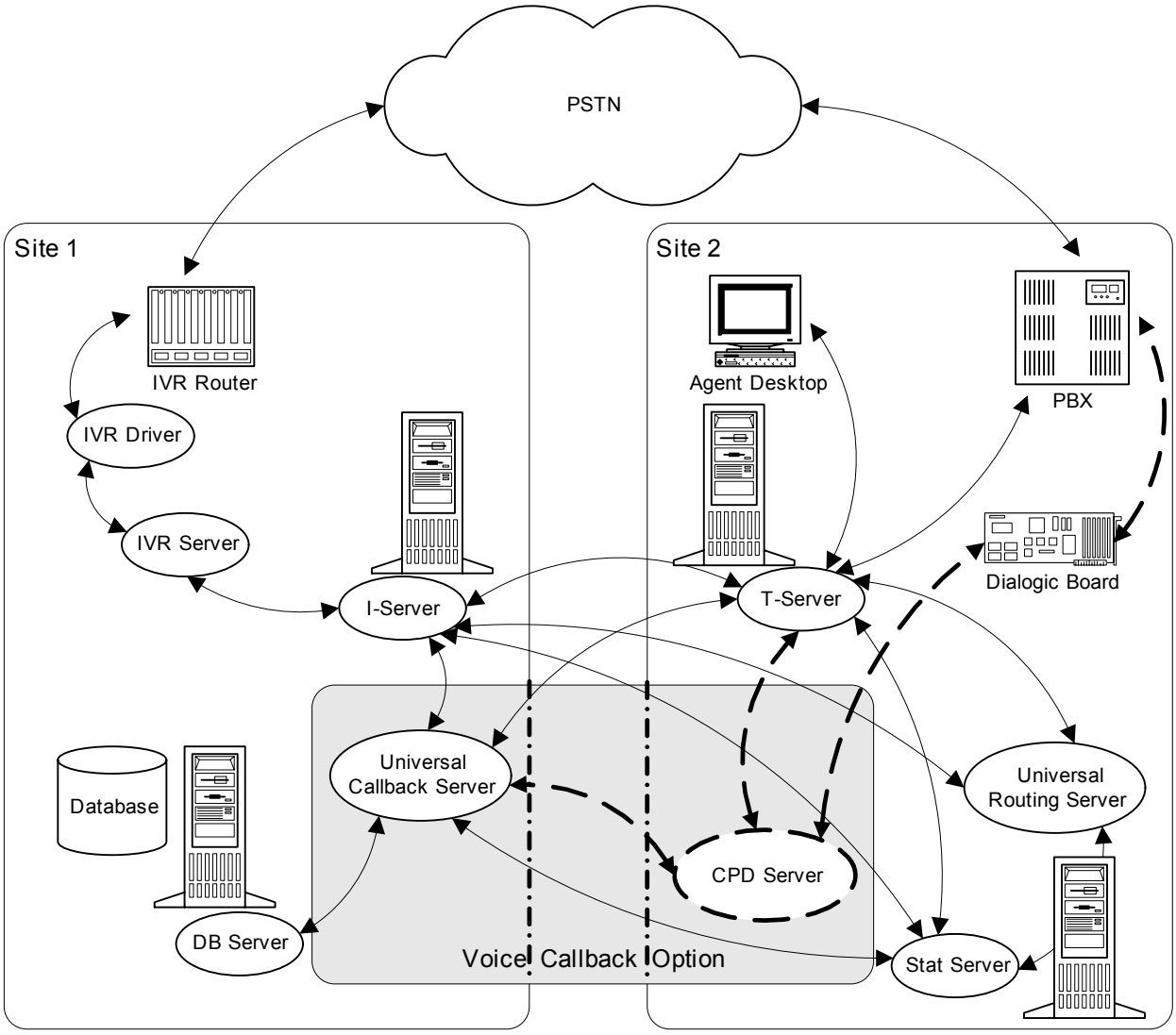


Figure 26: Interaction Between VCB and Other Components in IVR In-Front-of-the-Switch Mode

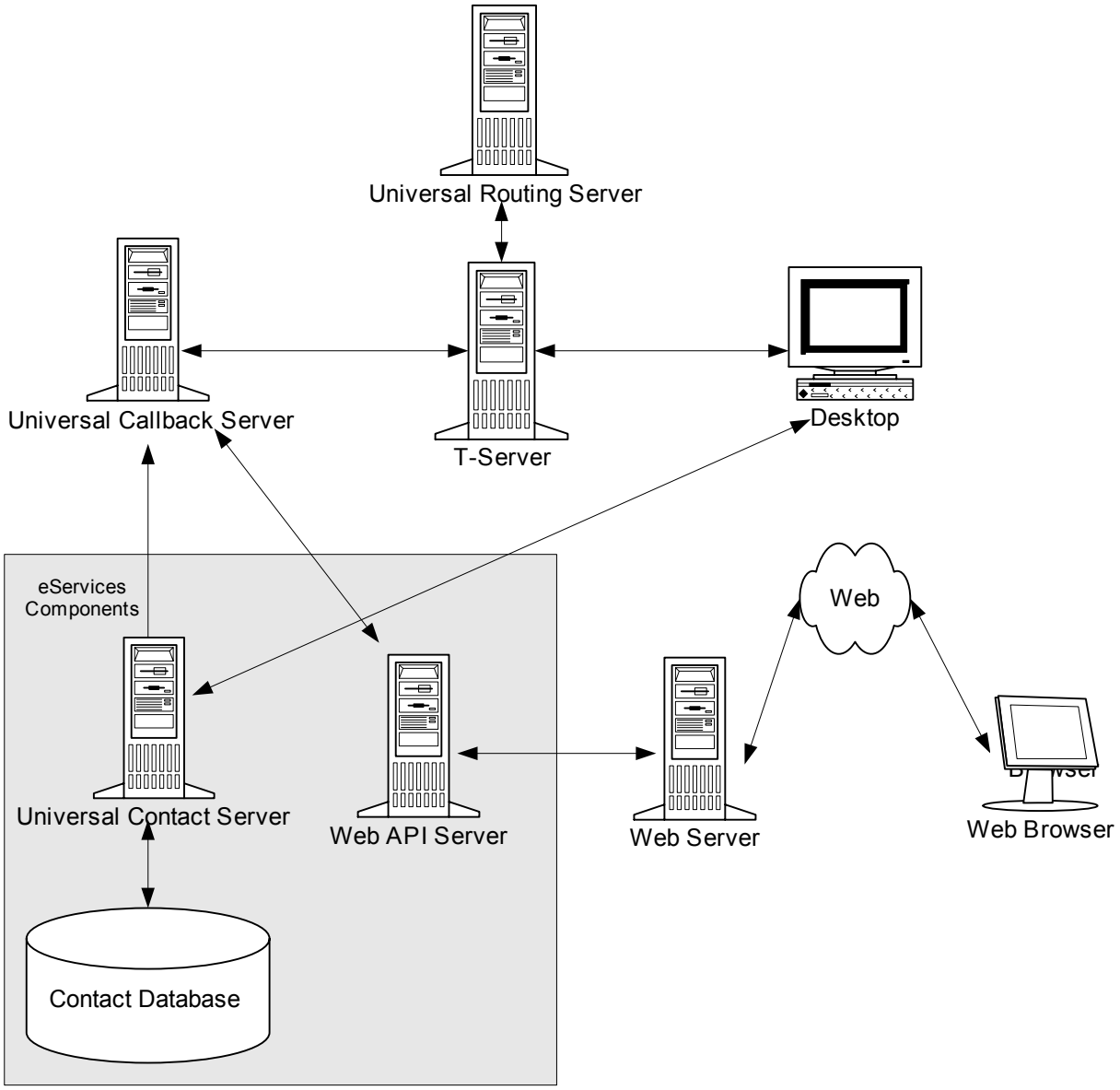


Figure 27: Callback Requests Between Web MCR Components

7.x Products

Table 13 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product.

Table 13: Information to Supply with 7.x Support Request

Product	Information to Supply with the Support Request
Interaction Routing Designer	• Screen captures that show the problem • Export of the strategy that demonstrates the problem (`*.zcf` file)
Universal Routing Server	• Universal Routing Server configuration • Universal Routing Server log files with Debug level detail covering the period when the problem occurred • Stat Server information (see the entry for Stat Server) • T-Server information (see the entry for T-Server) • DB Server information (see the entry for DB Server) • Export of the strategies that were loaded (`*.zcf` files)
Voice Callback	• Universal Callback Server configuration • Universal Callback Server log files with Debug level details covering the period of time when the problem occurred • T-Server information (see the entry for T-Server) • DB Server information (see the entry for DB Server) • Stat Server information (see the entry for Stat Server), if applicable • Call Progress Detection Server information (see the entry for CPD Server), if applicable • Universal Routing Server information (see the entry for URS Server), if applicable

6.x Products

Table 14 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 14: Information to Supply with 6.x Support Request

Product	Information to Supply with the Support Request
External Router	• Local External Router configuration • Remote External Router configuration • Local T-Server information (see the entry for T-Server) • Remote T-Server information (see the entry for T-Server) • Log files for the local and remote T-Servers with Debug level detail • Start-up log files for both T-Server with Debug level detail
Interaction Routing Designer (Strategy Builder)	• Screen capture • Strategy (`.rbn`) file that demonstrates the problem • Configuration Database
Universal Routing Server (Interaction Router)	• Interaction Router configuration • Interaction Router log file with Debug level detail covering the period when the problem occurred • Stat Server information (see the entry for Stat Server) • T-Server information (see the entry for T-Server) • DB Server information (see the entry for DB Server) • Strategy files that were loaded

Chapter

9 Voice Self Service

Products/areas within this category include:

- Genesys Studio
- Genesys Voice Platform
- Genesys Voice Platform DE
- Genesys Voice Platform EE
- Genesys Voice Platform NE
- Genesys Voice Platform SE
- Voice Platform Third Party Products
- IVR Interface Option
- Voice Treatment Option
- VoiceGenie

This chapter covers the following topics:

Architecture

This section contains graphics for some of the products mentioned in this chapter. Please refer to the Deployment Guide for each of the respective products for additional information.

Genesys Voice Platform

For a description of the architecture associated with Genesys Voice Platform, including Genesys Studio, not provided in this section, see the associated documentation.

IVR Interface Option

Figure 28 shows an IVR-Behind-Switch Configuration, a basic configuration in which the call activity on IVR channels can be monitored by a T-Server, which is connected to the premise switch. Figure 29 shows an IVR-In-Front-Switch Configuration.

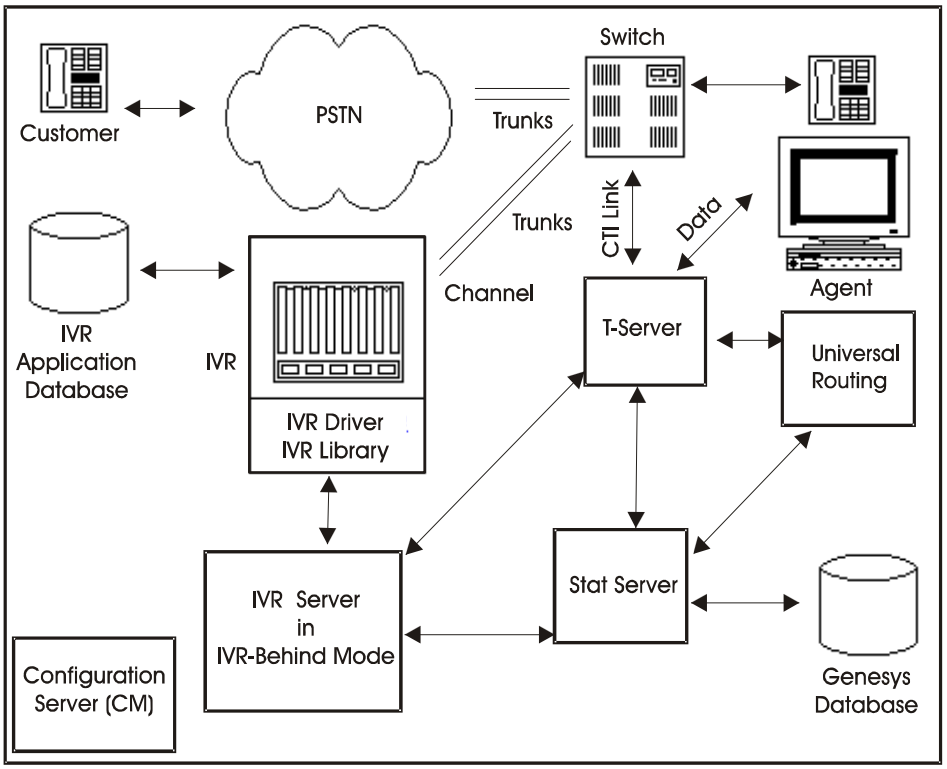


Figure 28: IVR-Behind-Switch Configuration

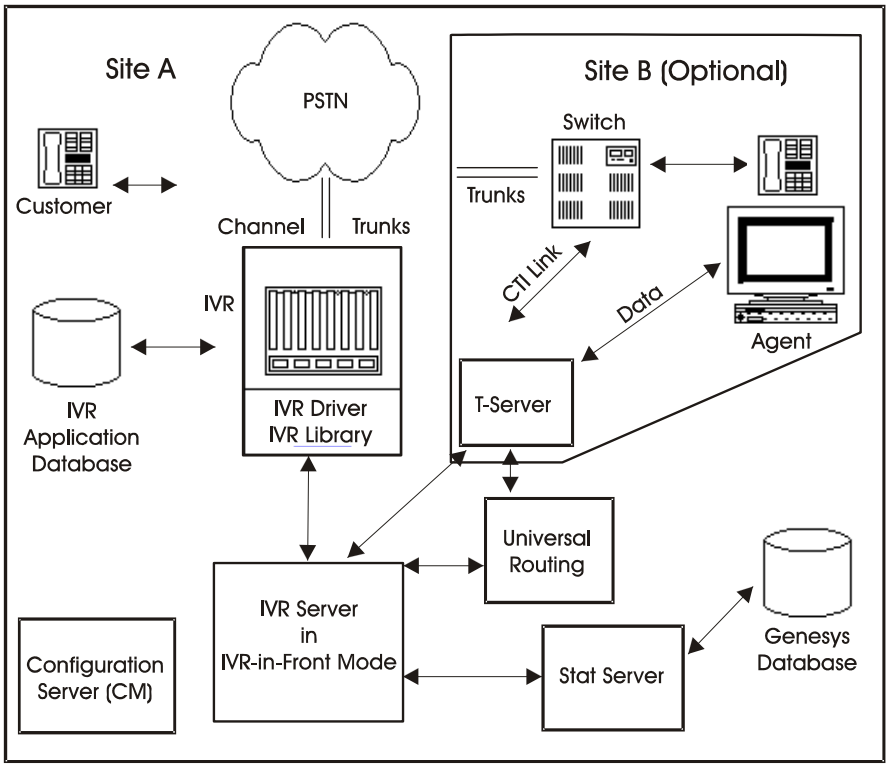


Figure 29: IVR-In-Front Switch Configuration

Figure 29 does not reflect all Framework and Routing connections between components. See their respective sections for that information.

Voice Treatment Option

Figure 30 shows the VTO architectural configuration.

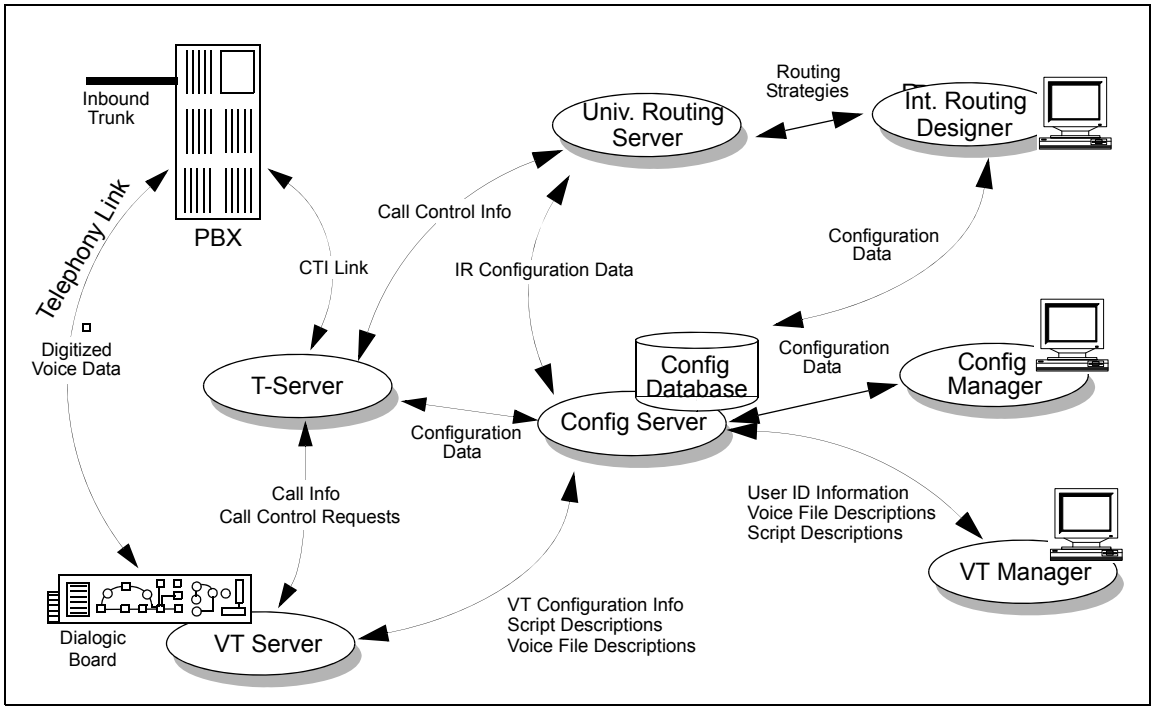


Figure 30: Voice Treatment Option Architecture

VoiceGenie

This section describes the following VoiceGenie configurations: All-in-One, One Management/Database Server, Two Management/Database Servers, and Operation, Administration, and Management (OA&M).

All-in-One

In this configuration the Database Server, Management Server and other VoiceGenie software (for example, VoiceXML Platform) are located on one machine.

Note: This architecture is not approved for production deployment purposes and should only be used in a lab or on a trial basis.

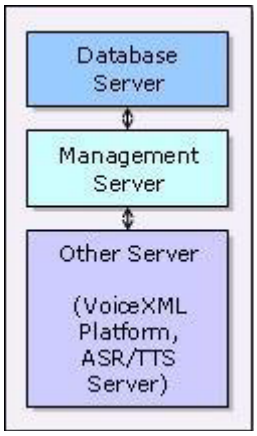


Figure 31: All-in-One

One Management/Database Server

In this configuration the Database Server (such as MySQL) and Management Server (such as CMP Server) are located on one machine. This one machine handles all requests from one or more other servers in the deployment.

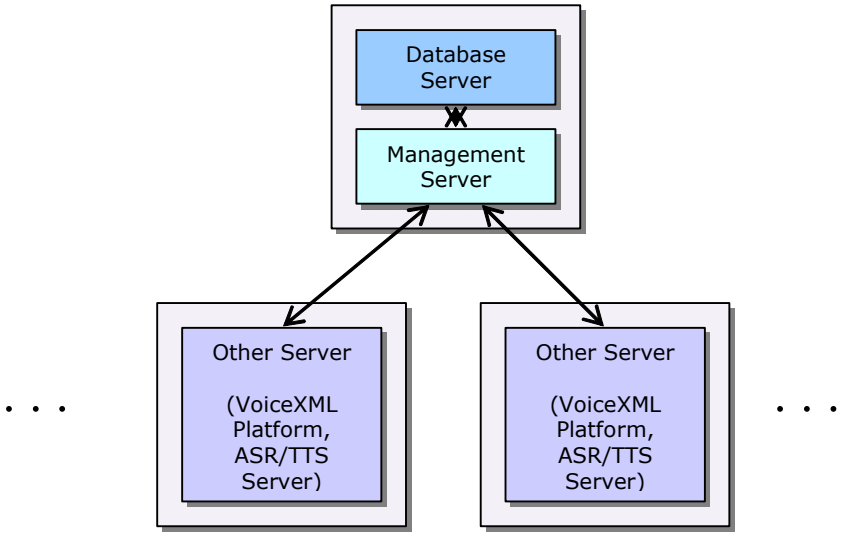


Figure 32: One Management/Database Server

Two Management/Database Servers

In this configuration a redundant pair of Management Servers exists with each Management Server having an onboard Database Server. Note that in this case replication is set up between the two databases.

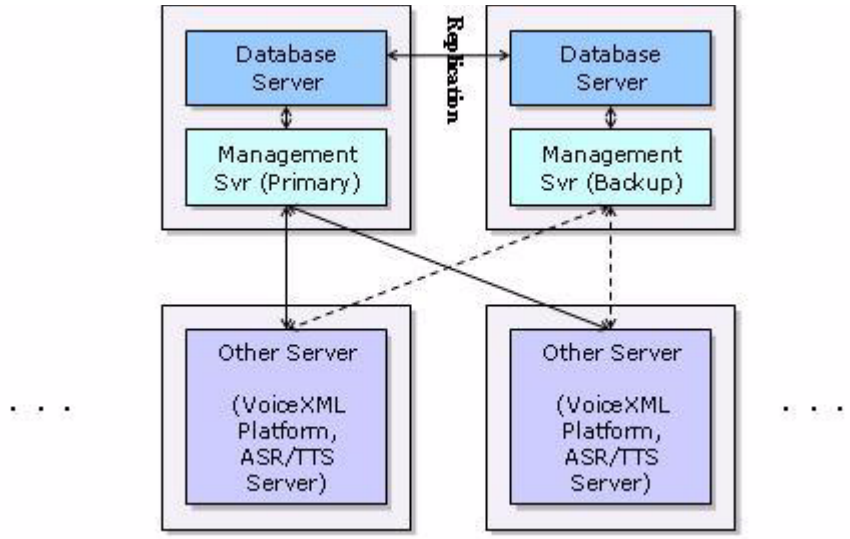


Figure 33: Two Management/Database Servers

Operation, Administration and Management (OA&M)

The following diagram illustrates the architecture and distribution of the various OA&M components as well as the Media Platform in an "all-in-one" setup. For example, the CMP Proxy & CLC, CMP Server, SMC, VoiceGenie SNMP and the rest of the VoiceGenie components are installed on a single server.

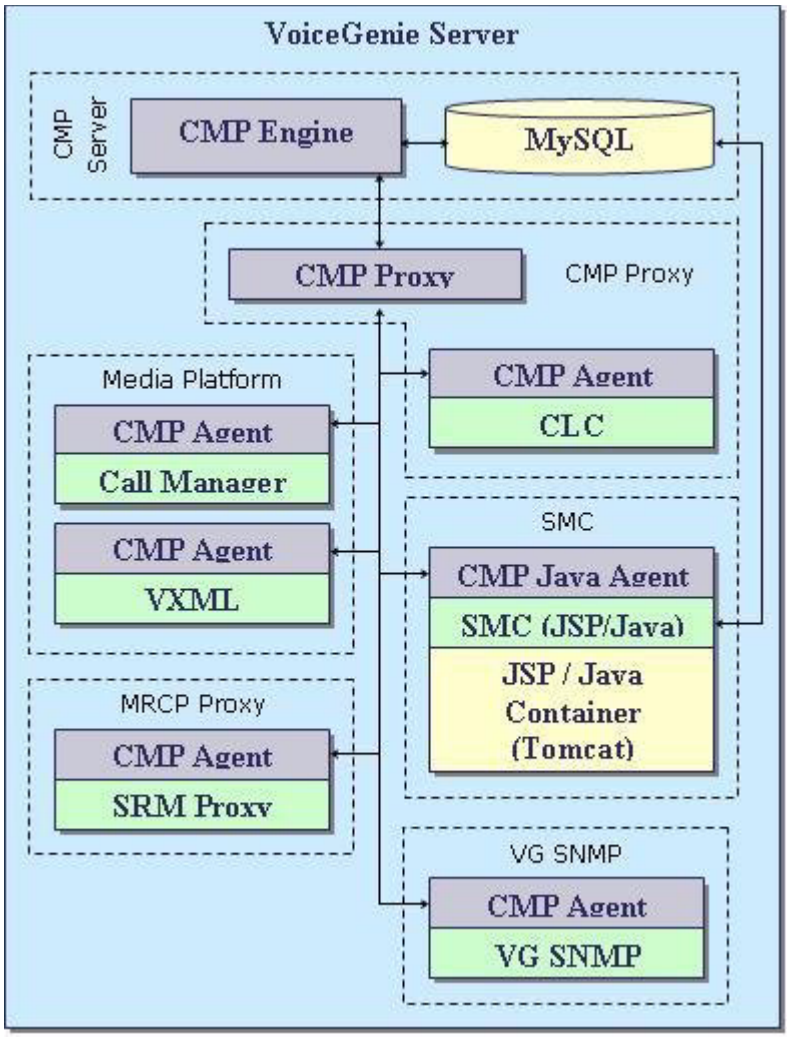


Figure 34: Operation, Administration and Management (0A&M)

For details about the OA&M architecture and component details, please refer to the following documents:

VoiceGenie 7 OA&M Framework User Guide

VoiceGenie 7 OA&M Framework – SMC Guide

VoiceGenie 7 OA&M Framework – CLC Guide

VoiceGenie 7 OA&M Framework – SNMP Guide

7.x Products

Table 15 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product.

Table 15: Information to Supply with 7.x Support Requests

Product	Information to Supply with the Support Requests
IVR-Suite	• IVR Interface Server configuration (preferable option `print_options` has been set to `yes`) • IVR Interface Server log file covering the startup of the IVR Interface Server with verbose logging • IVR Interface Server log file covering the period when the problem occurred with verbose logging • IVR Driver log file covering the connection of the IVR Driver to IVR Interface Server with `log_print_level` set to `xml` • IVR Driver log file covering the period when the problem occurred with `log_print_level` set to `xml` • T-Server information (see the entry for T-Server)
Genesys Voice Platform	See the next section

Genesys Voice Platform 7.x Logging Detail Discussion

This section describes Genesys Voice Platform (GVP) and its logging capabilities.

GVP Is a Multi-Component System

There are two types of GVP systems: one box installation (GVP:EE, GVP:DE and GVP:SE) and multi-box installation (GVP:NE). All run-time log files can be found in the Log subdirectory of the GVP installation directory. By default logs are located in this directory:

```
C:\CN\Log
```

There are many components in the GVP. Each component that is running as a process will be writing its own log file.

If you use multi-box installation, GVP components run on different servers and you will need to search for the logs on all of the machines on which GVP components are installed. The path to the Log directory is always the same:

```
C:\CN\Log
```

GVP:NE Reporter generates logs in the subfolders of the cn\log directory. This is an exception.

Overview of GVP Components

Every server on which GVP components are installed has several GVP processes running on it. There are a number of processes existing on all GVP components. Other processes are unique for a particular server. The list of the processes generating the logs, which are usually being requested by Technical Support, is provided in the next section. Not all GVP processes are mentioned. This list will be updated as changes occur.

Common Processes

This list describes the processes GVP uses that generate logs.

- *WatchDog:* Main GVP process starting all other processes. It controls all GVP processes during run time and restarts the failed ones.

  The logs generated by this component can show if all processes were running all the time or some of them were restarted.
- *PageCollector:* Process responsible for obtaining information from the WebServers through the HTTP protocol. It can be voice application pages and resources, as well as internal GVP HTTP transactions.

  The logs of this module represent the communication issues between the GVP components and the web server; for example, delays, missing pages, authorization problems, and so on.
- *NetMgt:* Net Management is a SNMP client running on each GVP server. All SNMP traps are printed out in the NetMgt log files. This can be the first place you go to monitor your system functionality.

Unique Processes

- *PopGateway:* The module controlling the telephony and VoIP interfaces, ASR and TTS resources, and communication with the Dialogic board.

  The logs generated by this process are required for most problems. These logs can be used to troubleshoot the following:
  - Call control (both telephony and VoIP)
  - VXML browsing
  - ASR and TTS control
  - Voice streaming
- *CFA (Call Flow Assistant):* This is a high-level call control module. It is used to control complicated call scenarios, such as different types of transfers, interconnection with Genesys' CTI network, and so on.

  The logs generated by this module are not used very often but can be very useful in troubleshooting scenarios mentioned previously.

- *ISvrClient (IVR Server Client):* VCS component in the GVP:EE and GVP:DE. This module is a VCS interface to the Genesys' CTI network. It is connected to the IVR Server.

  The logs generated by ISvrClient are always required if the problem is related to the GVP communication with the CTI network.
- *GQA (Genesys Queue Adapter):* The same as ISvrClient, but used in the GVP:NE.
- *VWPS (Voice Web Provisioning System):* Component of the GVP:NE. The logs for this component show all the changes made in the GVP:NE configuration database. These logs also show how other components download their configuration parameters during the startup.

Format of the GVP Log File Names

In most cases the module name is used as a log file name. GVP log file names are constructed based on the following format:

```
<ComponentName><WeekDay><SequenceNumber>.log
```

For example, log files generated by the component called PopGateway1 have the names:

- `PopGateway1Thu132.log`
- `PopGateway1Thu133.log`
- and so on

Exceptions are the logs generated by the GQA and PM processes, which run on the VWM machine (GVP:NE). Dedicated GQA and PM processes run for each GVP:NE customer. The following naming conventions are used in those 2 modules

- `<reseller>_<customer>_gqa.log`
- `<reseller>_<customer>_pm.log`
- `<reseller>_<customer>_gqaMon12.log`
- `<reseller>_<customer>_gqaTue23.log`

How GVP Generates the Logs

The rule GVP uses to create log files is common for all GVP components. All logs are stored in the Log directory for one week (7 days) and then are overwritten at the end of that week.

The name of the file where the GVP component writes the information to the log includes only the component name (for example, `WatchDog.log`, `PageCollector.log`, `NetMgt.log`, `PopGateway1.log`).

Remember that there could be several PopGateway components in one VCS. So the names of those components include a component index: `PopGateway1`, `PopGateway2`, and so on.

The GVP component writes to the current log file until it reaches the maximum size defined in the configuration file (default is 256KB). Then this file is stored

with the name, which will be unique for one week. When the system is first started, the PopGateway log file name includes the day of the week. For example, if today is Friday and this is the first day the system is started, the log file name will be `PopGateway1Fri.log`.

The log files for the next day be:

- `PopGateway1Fri1.log`
- `PopGateway1Fri2.log`
- and so on.

If your system can run over the weekend, without any help from outside, you should see the following logs when you come to your office on Monday morning:

- `PopGateway1Fri<xxx>.log`
- `PopGateway1Sat.log`
- `PopGateway1Sat1.log`
- `...`
- `PopGateway1Sat<xxx>.log`
- `PopGateway1Sun.log`
- `PopGateway1Sun1.log`

  and so on.

Log Levels

All messages in the GVP log files have different log levels assigned to them. There are 5 levels of logging:

- Error (lowest level)
- Warning
- Information
- Debug
- Full (highest level)

Names of the logging levels are comprehensive and do not require any additional comments. The GVP GUI allows you to select a component and choose a logging level for it.

The higher the logging level (full is the highest level), the more information will be printed in the log files. By default, log levels for all components are set to Error level.

Warning! Do not use the Full logging level in the production environment. It can affect system performance and fill up your hard drive very quickly.

There is one more logging level which allows you to define the logging level for the subcomponents of a particular GVP component. This level is used very

often for troubleshooting in the production environment. It can help to minimize the amount of logging and filter out unnecessary messages. You should be an advanced GVP user and to understand internal GVP architecture to use the Custom logging level. Here is one example showing how to capture all messages related to the telephony and ASR interfaces in the PopGateway1 process:

- Process: `PopGateway1`
- Log Level: `Custom`
- Log Flags: `10:*; 53:*`

Elements of a Line

Here is a typical line from the GVP component log file:

```
[2004/02/16 12:27:01.877] D44  TelephonyMgr.cpp:10580 C=10:L=8:U=920
[:N_dtiB2T8:P_dmv] logPortData:     FWPortSt = InService       |
PortObjSt = InService       |     BrPortSt = InService
```

The format of this line is as follows:

```
<timstamp> <Thread ID> <Source File> <Component-Level-Unit> <Info>
```

Each of these formats is described in detail below.

<timestamp>

The time in the GVP logs is always given in Greenwich mean time (GMT).

<Thread ID>

There is not a direct correlation between the ThreadID and the call:

- ThreadID can be reused for different calls.
- One call is processed in many different threads even in one component.

<Source File>

This format provides source information that is valuable to Genesys Technical Support.

<Component-Level-Unit>

This format provides very important information in a log line. Genesys suggests that you pay attention only to the messages with the Error (L=1) and Warning (L=2) levels. All other messages are printed out for debugging purposes only and most likely do not indicate any problem even if they say "ERROR".

Component: The subcomponent ID. See “List of Modules and Units for Custom Logging” on page 101 for the list of available IDs.

Level: The severity level of the log line. Table 16 shows the relationship between the Log Level ID and the Log Level name.

Table 16: Log Level Name and Log Level ID Values

Log Level Name	Log Level ID
Error	1 (0 x 1)
Warning	2 (0 x 2)
Information	4 (0 x 4)
Debug	8 (0 x 8)
Full	16 (0 x 10)

Unit: This is a log key addressing some functional area. This field is explained in the "List of Modules and Units for Custom Logging" on page 101.

<Info>

This format may provide some text explaining the problem or the possible concern. However, this format may also include symbols. The text and symbols in this format are useful for Genesys Technical Support.

Log Default Settings

By default all GVP components are set to Error level logging. The default log file size is 256KB. You can change both the level setting and the log through the configuration file.

Look for the following parameters to change the default settings:

- `logfile=tts_speechify.log`
- `loglevels=*:0x3`
- `logmaxsize=262144`

  Where:

  - `logfile`: log file name
  - `loglevels`: log flags are explained in Custom Logging Level for GVP Components
  - `logmaxsize`: maximum size of the log file in bytes.

Do not forget to set the `localconfig` parameter to `1` to make the GVP component use the settings from the configuration file. Otherwise it will download the settings from your configuration database (VWPS or VPM).

Custom Logging Level for GVP Components

GVP's custom logging feature provides you with various ways to filter out logging messages, which are printed in the log files. This feature provides you with the requested troubleshooting information with minimal CPU usage and smaller log files.

Custom logging is designed to be used by advanced GVP users only. This document explains basic principles of custom logging and provides some tips for custom logging levels used for troubleshooting popular issues. Contact Genesys Technical Support to get the appropriate custom logging settings for your particular issue.

The custom logging level is defined using binary masks. Each bit in this mask enables/disables the appropriate log level. Table 17 shows the relationship between the Log Level ID and the Log level name.

Table 17: Log Level Name and Log Level ID Values

Log Level Name	Log Level ID
Error	1 (0 x 1)
Warning	2 (0 x 2)
Information	4 (0 x 4)
Debug	8 (0 x 8)
Full	16 (0 x 10)

Several masks can be applied at the same time to enable several logging levels. In this case masks are combined using logical OR:

```
Warning + Error = 0x1 OR 0x2= 0x3
All messages = 0x1 OR 0x2 OR 0x4 OR 0x8 OR 0x10 = 0x1F
```

There are two formats for custom logging: module:level and unit.

module:level

This format is used to control the log messages generated by a particular internal module in one of the GVP processes. Each module has an ID number.

For example, `10` is used for Telephony Manager. Table 18 shows how to enable a different logging level for Telephony Manager.

Table 18: Telephony Manager Logging

Combination Masks	Log Level ID
Warning + Error:	10:0x3
All messages:	10:0x1F

Wildcards can be used to define the custom logging. Table 19 shows the following characters are allowed:

Table 19: Character Definitions

Character	Definition
*	everything
!	negation sign

Table 20 shows several examples on how to define custom logging using wildcards:

Table 20: Custom Logging Examples

Example	Definition
*:0x3 - Error + Warning	for all modules
10:*	all messages for telephony manager (the same as 10:0x1F)
!*	disable all logging
10:!*	disable logging for the Telephony Manager

In addition, several custom logging masks can be applied sequentially. For example:

```
*:0x3,10:*
```

This mask means that for all modules default logging is enabled (Error + Warning) and all messages for the Telephony manager will be printed.

Note: It is very important to be aware that a new logging level can be combined with the an existing logging level using logical `OR`. For example, if you need to reduce the amount of logging, then the existing log should be reset to the lowest level first and only after the new (reduced) level can be applied.

Example:

- Existing logging level: `*:1F` (all messages are enabled for all modules). This is required to reset the logging to default. The following mask should be applied:

  `*:!*,*:0x3`

  Where
  - First mask (`*:!*`) disables all messages enabled through the module:level format for all modules.
  - Second mask (`*:0x3`) increases the logging to the default level (Error+Warning).

unit

This is another Genesys format that can be used to set custom logging levels. The logging level is defined with only one number in this case. This number identifies a particular group of logging messages.

- For example, to see only the messages sent between the ISvrClient and IServer in the ISvrClient log, the following custom logging can be used: `1000`
- Wildcards can be used with this logging format as well. For example, the following setting disables all unit logging for the process: `/*`

GVP Troubleshooting with Custom Logging

This section provides several examples showing the custom logging that should be used for particular GVP problems. It is very important to remember that any extended logging increases the CPU usage and requires more space for the log files on your hard drive. Consult with Genesys Technical Support before applying any extended logging in a production environment. It can be also useful to test the extended logging in the lab first. In any case, server performance (CPU and memory utilization and also the free space on your hard drive) should be closely monitored after applying a new logging level.

Telephony Problems

Telephony problems like stuck ports, ring-no-answer scenarios, dropped calls, and so on usually require full logging for the Telephony Manager module in the PopGateway (VCS): `10:*`

SIP Signaling

All signalling issues in the VoIP-based GVP system should be investigated on 2 levels: IPCS-PopGateway and VWM-SipSessionManager (SSM). In both cases, the following custom log in is required: `40:*,43:*,45:*`

GQA/ISvrClient Messaging

Troubleshoot GVP with Framework integration problems on the GQA in the GVP:NE system or ISvrClient (I-Server Client) in the GVP:EE. The following custom logging should be enabled for those processes: `1000`

Application Call Flow

If it is necessary to monitor how GVP is processing the application pages, enable the logging described in the next section should in the VCS for the PopGateway process.

Best Practices in Setting the Log Level

The first step in collecting log files is to set the log level properly. If you need detailed instructions on the logging level, please contact Genesys Technical Support.

The best way to set the log level for any GVP component is through the component GUI running on the GVP Host, port 9810:

`http://<component-ip>:9810`

To set the log level, do the following:

1. Go to the `Management > Log`.
2. Select the component from the drop box and set the appropriate log level. The log level will be changed immediately. You do not need to restart the WatchDog to make new settings work. Otherwise, if you restart the WatchDog, all log levels will be set to default.
3. In the following two cases, set the log level in the configuration file (`pop.ini, telera.ini, vwm.ini, vwps.ini, voip.ini`):
   - If you want to capture the initialization process on a level higher than the default logging level.
   - If you think that the system can be restarted by itself but you want it to continue to write the logs on the customized log level.

Best Practices in Collecting Log Files

If you do not want to get into the details on how GVP log files are named and stored, then follow these simple instructions.

1. Set the required log level (see "Best Practices in Setting the Log Level").
2. Make a test to reproduce the problem.

3. Sort the files by modification date.
4. Send all files generated during your test to Genesys Technical Support.

GVP Installation Logs

Log files described in this document are the run time log files generated when the system is receiving calls. GVP also generates the log files during the installation. Those log files can help to identify the installation problem. They can show that prerequisite software is not installed, for example. Those files are usually stored in the following directory:

```
C:\Documents and Settings\Administrator\Local Settings\Temp
```

Names of those log files are different but usually include the GVP server name. For example:

```
Voice Communication Server Setup.log
```

List of Modules and Units for Custom Logging

Table 21 shows the module list. Table 22 shows the unit list.

Table 21: Module List

Unit	Value
Telephony Manager (PopGateway/VCS)	10
Processing of Application Pages (PopGateway/VCS)	12
SIP stack Manager (PopGateway/IPCS, SSM/VWM)	40
SIP Session Manager (PopGateway/IPCS, SSM/VWM)	43
SIP stack (PopGateway/IPCS, SSM/VWM	45

Table 22: Unit List

Unit	Value
VXMLcall trace (PopGateway/VCS+IPCS)	440
IServer-ISvrClient messaging (GQA/VWM, ISvrClient/VCS)	1000

6.x Products

Table 23 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 23: Information to Supply with 6.x Support Requests

Product	Information to Supply with the Support Requests
Genesys Voice Portal	• Full version of GVP and any hot-fixes that have been applied • OS version of GVP server, Service Pack, IE version and IIS version • CPU, memory, hard disk space, machine type of GVP server • Configuration Layer configuration dump • URS Strategy (`.rbn` or `.zcf` file) or screen captures showing the strategy in IRD • All logs from \Cn\log on GVP VCS • I-Server Client log with logging level set to custom (1000) or full logging. • IVR Server logs, T-Server logs, and URS logs (debug logging level) • Zipped :\CN_VPM\Web\VPM\Database folder • The configured files for dialogic (`.config`, `.pcd`, `.fcd`) files are located in the \program files\dialogic\data • If behind the switch - PBX switch configuration • TTS and or ASR services being used and which vendor • Whether any anti-virus software; for example, URLScan is running `pop.ini`

Table 23: Information to Supply with 6.x Support Requests (Continued)

Product	Information to Supply with the Support Requests
IVR-Suite	• IVR Interface Server configuration (preferable option `print_options` has been set to `yes`) • IVR Interface Server log file covering the startup of the IVR Interface Server • IVR Interface Server log file covering the period when the problem occurred • IVR Driver log file covering the connection of the IVR Driver to IVR Interface Server • IVR Driver log file covering the period when the problem occurred • T-Server information (see the entry for T-Server)
VWAP	• Full version of VWAP and any hot-fixes that have been applied. • If the problem is with call processing, turn logs to FULL for pop-gateway, page-collector, and CFA; make 1 call and send the pop-gateway, page-collector, and CFA logs for this call from the \cn\log directory. Include time and session ID of call. Also include the `pop.ini` file. • If the problem is with a VWM component, turn up logging for process to FULL, allow the problem to reoccur, and send the logs for the component from the \cn\log directory. Also include the `vwm.ini` file. • If the problem is with a component GUI, screens shot of the problem and include a description of the issue.

VoiceGenie

Media Platform Diagnostics

Diagnostics Most Frequently Needed to Assist You

This section outlines the pieces of information most frequently requested by Genesys Technical Support. On many systems, the collection of some/all of this information is already enabled. On others, it can be enabled during problem reproduction. Depending on space, you may want to enable more of these items during periods of development, testing, or monitoring, in case a problem occurs that cannot be reproduced. We are able to resolve most issues with these items.

vginfo

Use: This file lists the contents of many configuration files and script results from your system. If a system is having problems after an installation or any configuration change, this allows Genesys Technical Support to look at aspects of your system configuration without asking you to send individual files and outputs.

Helpful Tip: Before making any configuration changes, it is always a good idea to save a `vginfo` of the platform in a good state. That way, if the changes cause any problems, it will be easier to identify how to reverse the changes.

Generating from the Web Management Console in VG 6.0+:

- Select the `Operations` tab
- Select `Get Platform Info`
- Select your system from the `Platform` drop-down list
- Select `Get Platform Info`
- Send the generated file as an attachment to your response

Generating from the Command Line in VG6.0+:

Issue the following commands while logged into your system as the "root" user:

```
cd /usr/local/cmp-proxy/scripts
./vginfo_linux.sh <hostname>.out
```

(replacing `<hostname>` with the host name of your system)

The location of the generated file will be displayed on the screen.

Notes

- In VG6.x: Each time a `vginfo` file is generated, it will be larger than the previous one, because it will contain a growing amount of CMP database backup information. The system stores backup information in:

  ```
  /usr/local/cmp-server/config/
  ```

  There will be multiple files named `cmp_database_backup.*.sql`. You can delete all of these except the most recent one (or save the others somewhere else). By keeping only a single backup file, your `vginfo` files will not increase in size each time you re-generate.
- In VG7.x on Windows 200x: To generate a `vginfo` file, the following folder must exist:

  ```
  C:\VoiceGenie\cmp\cmp-proxy\scripts\sys_info\
  ```

  This is where the generated `vginfo` will be put. In VG7.x on Windows 200x, this folder does not exist by default. You will need to manually create this directory before you can generate a `vginfo` for the system.

- In VG7.x on Windows 2003: While running the `vginfo` script, one function will not return correctly, resulting in an incomplete `vginfo`. If you are using Windows 2003, please do the following:
  - Open `C:\VoiceGenie\cmp\cmp-proxy\scripts\vginfo_w2k.wsf`.
  - Look for the following section:

```
Function PrintSoftwareInfo
echo_file "Name " & vbTab & "Version "
Set colSoftware = objWMIService.ExecQuery _
("Select * from Win32_Product")
For Each objSoftware in colSoftware
echo_file objSoftware.Name & vbTab & objSoftware.Version
Next
End Function
```

  - Add the line "`On Error Resume Next`" just below the function declaration, so the function looks like:

```
Function PrintSoftwareInfo
On Error Resume Next
echo_file "Name " & vbTab & "Version "
Set colSoftware = objWMIService.ExecQuery _
("Select * from Win32_Product")
For Each objSoftware in colSoftware
echo_file objSoftware.Name & vbTab & objSoftware.Version
Next
End Function
```

CLC Health Output

Use: Doing a CLC (Command Line Console) `health` query will provide the status of all the components of the system, which can explain why certain errors/behaviors are occurring, and can give an idea of where we should start troubleshooting. If a problem occurs, this information should be collected before the system is restarted/rebooted.

Collecting the Information: There are two options:

1. Start up the CLC interface session, and then enter the `health` query:

```
clc (or 'telnet localhost 8999' on Windows)
health
[ enter "e" to exit ]
```

   then send a screen shot of the output.

2. On Linux, there is a `clccmd` script, to run queries without starting a CLC session:

```
/usr/local/cmp-proxy/bin/clccmd health > healthOut.txt
```

   then send the resulting `healthOut.txt` file.

pw_metricsfile/pw_logfile

Use: The `pw_metricsfile` provides a log of how the application executed as the user moved through a call. It shows the navigation through pages, dialogs, and form items. It shows prompts that are played, recognition results, events, variable evaluation, and so on. The `pw_logfile` (Linux only) contains details about component alarms and status changes.

Controlling the Level of Detail: The level of detail in the `pw_metricsfile` depends on the `metricslevel` property. Refer to the following for details on the different levels:

`http://developer.voicegenie.com/reference.php?ref=properties#metricslevel`

To change the level (5 is the highest), add the `metricslevel` property

- To `/usr/local/phoneweb/config/defaults.vxml` (`C:\VoiceGenie\mp\config\defaults.vxml on Windows 200x`),
- Or to your application (which will override any setting in defaults.vxml)

For example: `<property name="metricslevel" value="5"/>`

These files are saved in `/usr/local/phoneweb/logs/` (`C:\VoiceGenie\mp\logs\ on Windows 200x`).

tmp files

Warning! `Tmp` files can impact performance and should not normally be used in production.

Use: The `tmp` files consist of all the resources that VoiceGenie fetches or generates during a call. The fetched VoiceXML pages are the most helpful, allowing us to confirm expected application behavior, clarify error cases, and reproduce problems. For applications using server-side technologies, this allows us to look at the generated VoiceXML pages, rather than the source .jsp, .asp, .perl, or another format. The HTTP request/response headers are useful for investigating fetching/caching issues. The `tmp` files also provide some information related to ASR and TTS.

Enabling Saving tmp Files: To enable saving `tmp` files, add the '`savetmpfiles`' property

- To `/usr/local/phoneweb/config/defaults.vxml` (`C:\VoiceGenie\mp\config\defaults.vxml on Windows 200x`),
- Or to your application (which will override any setting in `defaults.vxml`)

For example: `<property name="savetmpfiles" value="0xffff"/>`

The `tmp` files will be saved in `/usr/local/phoneweb/tmp/` (`C:\VoiceGenie\mp\tmp\` on Windows 200x). For each call, the files will be saved in a subdirectory named `<sessionID>`.

To disable saving `tmp` files, remove or comment out the property.

VoiceGenie Component Tracing

Warning! VoiceGenie component tracing can impact performance and should not normally be used in production.

Use: When an issue is escalated to development, we typically require tracing for one or more components of the software. These traces let the developers see great detail about how the software executed and, in many cases, can help the developers identify the root cause of a problem in the software.

Enabling Tracing: In 6.4.x and 7.x, you can either enable tracing temporarily (using CLC), or on an ongoing basis (using the System Management Console, VMC/SMC):

1. To enable tracing temporarily (for example, until the next `vgstop`) you would use the CLC interface:

   `clc` (or `telnet localhost 8999` on Windows)
   `tracelevel <service> localhost - enable`
   [enter "e" to exit]

   where `<service>` is the name of the component for which tracing is needed. For example, to enable `callmgr`, `vxmli`, and `iproxy` tracing, you would enter:

   ```
   tracelevel callmgr localhost - enable
   tracelevel vxmli localhost - enable
   tracelevel iproxy localhost - enable
   ```

   To disable tracing, repeat commands with `disable` instead of `enable`.

2. To enable tracing on an ongoing basis, so that it stays enabled until you manually disable it, you must use the VMC/SMC interface:
   - Log in to VMC/SMC
   - Click on `Configuration` tab
   - Click on component name in left-hand menu (for example, Call Manager, VoiceXML Interpreter, Web Proxy)
   - Select radio button for configuration name (for example, default)- click `Edit` button

     In 6.4.x:
     Change: `cmp.trace_flag = FALSE`
     To: `cmp.trace_flag = TRUE`

     In 7.x:
     Find the '`cmp.trace_flag`' parameter, make sure it is checked, and select radio button "`Tracing/Debugging On Depending on Masks`"
   - Click `Update` button

   Then restart the VoiceGenie software for the change to take effect.

   To disable tracing, repeat the above to set the parameter back to `FALSE` or "`Tracing/Debugging Always Off`".

Note:

When enabling Call Manager (`callmgr`) tracing, you may be asked to turn on SIP or H.323 logging as well. SIP/H.323 logging must always be enabled using the VMC/SMC interface. If you intend to enable `callmgr` tracing through CLC, make sure you enable SIP/H.323 logging first and then restart, before enabling `callmgr` tracing through CLC.

- Log in to VMC/SMC
- Click on Configuration tab
- Click on Call Manager in left-hand menu
- Select radio button for configuration name (such as default)
- Click `Edit` button

  In 6.4.x:
  Add one of the following lines:
  - `sip.logmsgs=1`
    (to enable SIP logging)
  - `h323.logging=q931 h2250cs h245 RAS h4501`
    (to enable H.323 logging)

  In 7.x:
  - Find the '`cmp.log_4`' parameter, make sure it is checked, then click `show`, then make sure all check boxes in the `file` column are checked.
  - For H.323, you must also find the `h323.logging` parameter, make sure it is checked, and set to `q931 h2250cs h245 RAS h4501`
- Click `Update` button

  You will need to restart the VoiceGenie software for these changes to take effect. However, you can leave these changes enabled. SIP/H.323 logging will only be performed when `callmgr` tracing is explicitly enabled as well.

trc.log/trc.logprv (for Open Speech Recognizer)

Use: These are Open Speech Recognizer (OSR) trace files that show details about why errors occur. They provide information related to licensing, grammar fetching, recognition sessions, dictionaries, and so on. This is usually the quickest way to pinpoint the general source of a problem with OSR.

These files are logged automatically. They are in the main OSR directory ($SWISDK).

Helpful Tip

It is always a good idea for the system administrator(s) to keep a log book. This document should contain any responses used for the initial configuration (or at least those which were different from the defaults), as well as any manual changes that were made afterwards. Also, append the information about any subsequent changes to the system in the log book. For example:

- If you change from the default `4ESS ISDN` switch type, you should make a note.
- You should record whether or not you have chosen `STRICT CONFORMANCE`.

Other Useful Information

Introduction

Prior to placing a VoiceGenie platform into production, there are a number of configuration elements that should be verified. Ensuring that these are properly configured prior to service turn-up will avoid potential service interruptions resulting from a misconfiguration.

This document applies to VoiceGenie software running on approved hardware, with the Red Hat Linux 3.0 or Advanced Server 3.0 operating systems in PSTN (Dialogic) and VoIP configurations. For periodic maintenance recommendations for earlier releases (particularly those based on Red Hat Linux 7.2), or for our Windows release, contact Genesys Technical Support.

Summary of Risks

The following potential risks exist, and are referred to in the information below.

- Disk space exhaustion - Call processing will halt.
- Performance degradation - Callers may experience undue latency. Recognition may be affected.
- Server shutdown - Inbound calls will be rejected.
- Platform compromised - May result in complete system corruption.

Platform Checklist

This section includes a list of items to be inspected either manually, or to be checked with a VoiceGenie-provided script. Each item includes a description of the item, the risks associated with it, and how to ensure that it is configured properly.

Ensure 'savetmpfiles' is Disabled

What it Means

This VoiceXML property saves all intermediate files related to VoiceXML page processing, and can provide useful information for debugging of a complex application. Note that this property can be set in any location in an application, or as part of the platform configuration itself.

To ensure this is turned off, please check the `defaults.vxml` file(s), the application root document, as well as each page in the application. If you are using `savetmpfiles` for debugging purposes, be sure to periodically purge the `/usr/local/phoneweb/tmp` directory.

The Risks are:

- Disk space exhaustion
- Performance degradation
- Call processing issues (for systems with slow disk subsystems, or for large disks)

How to Check

The '`savetmpfiles`' property can be defined on the platform in the application defaults file (usually `/usr/local/phoneweb/config/defaults.vxml`), or within the application. Look for the following line:

```
<property name="savetmpfiles" value="0xfff"/>
```

The value is typically set to '`0xfff`' for some kinds of debugging, but any non-zero value will save particular kinds of temporary files in the `/usr/local/phoneweb/tmp` directory.

For any production system, the value of this property should be zero, or the line should not exist at all:

```
<property name="savetmpfiles" value="0x000"/>
```

In order to confirm that this is configured properly, you should observe that the `/usr/local/phoneweb/tmp` directory on the platform is empty when there are no calls in progress. There may exist some small number of directories that have been created when calls are improperly terminated. Check the dates of these directories to determine if they can be removed.

Turn VoiceGenie Tracing Off

What it Means

VoiceGenie tracing is only intended to be used to resolve platform issues when so instructed by Genesys Technical Support. Disabling of tracing will reduce the overall load on the system and the system will be less likely to experience problems. In addition, very large trace files, or enabling of full tracing (under load) on systems with slow disk subsystems, can lead to call processing issues.

The Risks are:

- Performance impact
- Potential disk space exhaustion (if rotation is misconfigured)
- Call processing issues (for systems with slow disk subsystems, or for very large trace files)

How to Check VoiceGenie tracing is controlled with log settings in component configuration files, or using the CLC. Whenever the software starts, each component examines its own log setting to determine whether tracing should be enabled or disabled. The configuration files are modifiable using the SMC Configuration Utility and exist for all platform components. The tracing is enabled with the `cmp.trace_flag` setting (either `Always Off` or `On Depending on Masks`). The default setting will be for `Always Off`.

Required Action While in production, all tracing should be disabled. If you notice that tracing is enabled for a component; and that this tracing is not required by VoiceGenie to debug a particular issue, you should arrange to disable the tracing and restart the system at your earliest convenience.

Turn Dialogic Tracing Off

What it Means Dialogic tracing is only intended to be used to resolve platform issues when so instructed by Genesys Technical Support. Disabling of tracing will reduce the overall load on the system and the system will be less likely to experience problems.

The Risks are:

- Performance impact
- Potential disk space exhaustion (if rotation is misconfigured)
- Platform Stability

How to Check Dialogic tracing is controlled with the CallManager configuration file in the SMC. The `DLGC_TRACE_BOARD=0` should be set to 0. Any non-zero number will cause the `/usr/local/phoneweb/logs/dlgc_trace.dat` to be written too.

Dialogic tracing can also be enabled directly in the Dialogic software. To confirm that the tracing is not enabled, you should check the settings in the following files, using the following procedure:

1. `/usr/dialogic/cfg/cheetah.cfg` if existing should contain the following line:

   ```
   Logger.Channels = "-DEBG-INFO-APPL-WARN+EXCE+ERR1+ERR2"
   ```

2. `/usr/local/phoneweb/.profile` should not contain the following line:

   ```
   GC_PDK_START_LOG="filename: pdklog.log; loglevel: ENABLE_DEBUG"
   ```

3. `/usr/dialogic/cfg/RtfConfigLinux.xml` should have the majority of the `mlabel` entries set to `state ="0"`.

Note: In some releases, the `/usr/dialogic` directory is named `/usr/ct_intel`.

Required Action While in production, Dialogic tracing should be disabled.

Make Sure System Log Rotation Is Working

What it Means If system log rotation is not configured properly, log files may become large. It then becomes more costly for the operating system to seek to the end of the file and there is more load on the system.

The Risks are:

- Performance impact
- Potential disk space exhaustion (if rotation is misconfigured)

How to Check

There are two methods to check that log rotation is configured correctly. By inspecting the files themselves, you can observe whether or not rotation is occurring. Each file should have multiple instances. For example:

```
/usr/local/phoneweb/logs/pw_logfile
/usr/local/phoneweb/logs/pw_logfile.0
/usr/local/phoneweb/logs/pw_logfile.1
/usr/local/phoneweb/logs/pw_logfile.2
```

There will typically be a maximum of five files, although this depends upon the rotation configuration and the type of file (the default setting is to keep 59 copies of `/usr/local/phoneweb/logs/pw_metricsfile*`).

The second method of checking is to ensure that the rotation is actually configured. All log file rotations, except for squid, are controlled by short configuration files in the `/etc/logrotate.d` directory. In this directory, there should be a configuration file called `pw_logfile` which contains the following:

```
/bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null
|| true
```

This tells the system to rotate the log file every day if it is not empty (`daily` and `notifempty` options). The old log files will not be compressed since doing this could cause performance problems if the log files were large (`nocompress` option). The final section of the file restarts the `syslog` server so that it recognizes the new file.

There is another configuration file named `vg-scriptmanager` which contains the following:

```
/var/log/vg-scriptmanager.log {
        notifempty
        nocompress
        weekly
}
```

Similarly, there should be a file called `/etc/logrotate.d/syslog` which rotates the main system log files. The contents of this file are listed below:

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler
/var/log/boot.log /var/log/cron {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2>
/dev/null || true
    endscript
}
```

Various VoiceGenie log files are rotated and managed using the `/etc/crontab` file. Depending on the components installed on the system, the log file will look a bit different. A typical configuration file may look similar to the following:

```
16 4 * * * root find /usr/local/ccp-ccxml/logs/* -mtime +13 -exec rm
-f {} \;
16 4 * * * root find /usr/local/ccp-proxy/logs/* -mtime +13 -exec rm
-f {} \;
16 4 * * * root find /usr/local/ccp-rm/logs/* -mtime +13 -exec rm -f
{} \;
12 20 * * * pw /usr/java/jdk/bin/java -jar /usr/local/cmp-
db/bin/dbadmin.jar backup
29 20 * * * pw /usr/java/jdk/bin/java -jar /usr/local/cmp-
db/bin/dbadmin.jar cleanup
0 20 * * * pw /usr/local/vg-tools/server/scripts/run-cleanup.sh
0 20 * * * pw /usr/local/vg-tools/server/scripts/summarization.sh
12 4 * * * pw /usr/java/jdk/bin/java -jar /usr/local/cmp-
db/bin/dbadmin.jar backup
6 * * * * pw /usr/java/jdk/bin/java -jar /usr/local/cmp-
db/bin/dbadmin.jar summarize
29 3 * * * pw /usr/java/jdk/bin/java -jar /usr/local/cmp-
db/bin/dbadmin.jar cleanup
32 2 * * * pw find /usr/local/cmp-db/scripts/ -name
'cmp_db_backup_*.sql' -mtime +13 -exec rm -f {} \;
13 4 * * * root find /usr/local/tomcat/logs/ -name 'localhost*txt' -
mtime +13 -exec rm -f {} \;
13 4 * * * root find /usr/local/tomcat/logs/ -name 'cmpagent*log' -
mtime +13 -exec rm -f {} \;
13 4 * * * root find /usr/local/tomcat/logs/ -name 'catalina*txt' -
mtime +13 -exec rm -f {} \;
13 4 * * * root find /usr/local/tomcat/logs/ -name 'catalina*out' -
mtime +13 -exec rm -f {} \;
10 4 * * * root find /usr/local/cmp-proxy/logs -name
'CMP.log.cmpproxy*' -mtime +13 -exec rm -f {} \;
10 4 * * * root find /usr/local/phoneweb/logs -name 'pw_logfile*' -
mtime +59 -exec rm -f {} \;
0 1 * * * pw /usr/local/squid/bin/squid -k rotate
10 4 * * * root find /usr/local/phoneweb/logs -name
'pw_metricsfile*' -mtime +59 -exec rm -f {} \;
```

The squid proxy server log is rotated using Squid's internal log rotation mechanism, which is invoked from the `cron` process. From the `crontab` entry above:

```
0 1 * * * /usr/local/squid/bin/squid -k rotate
```

This line configures the system to rotate the squid logs once a day. There may exist some other rotation settings in the `pw` users' `crontab`. You can check if any rotations are enabled by (as user pw) querying `crontab` using `crontab -l` and looking for the following entry:

```
5 2 * * * find /usr/local/phoneweb/cache/tmp/ -mmin +180 |xargs
/bin/rm -f
5 1 * * * find /usr/local/srm-server/logs/log.realspeak_host* -mtime
+2 |xargs /bin/rm -f
```

Ensure Metrics Files are Managed Properly

What it Means The metrics files are stored in the `/usr/local/phoneweb/logs` directory, and include all files with the prefix `pw_metricsfile`. These files are rotated by the VoiceGenie software (the CMP Proxy) once a day.

It is also necessary to ensure that the files are periodically purged, and frequently enough if the size of each `pw_metricsfile` is large. This is done with a `crontab` entry:

```
10 4 * * * root find /usr/local/phoneweb/logs -name
'pw_metricsfile*' -mtime +59 -exec rm -f {} \;
```

How to Check Periodically examine the `/usr/local/phoneweb/logs` directory to ensure that there are no metrics files older than 59 days, and that the size of the metrics file is not so large that the disk space will be consumed if there were 59 days worth of files.

Ensure Application Logging is Properly Configured

What it Means This VoiceXML property saves all intermediate files related to VoiceXML page processing, and can provide useful information for debugging of a complex application. Note that this property can be set in any location in an application, or as part of the platform configuration itself.

To ensure this is turned off, please check the `defaults.vxml` file, the application root document, as well as each page in the application.

The Risk is:

- Disk space exhaustion

How to Check The `metricslevel` property can be defined on the platform in the application `defaults` file (usually `/usr/local/phoneweb/config/defaults.vxml`), or within the application. Look for the following line:

```
<property name="metricslevel" value="3"/>
```

The value is typically set to values between zero and seven. Values above three should never be used in production - they are useful only for debugging.

In order to confirm that this is configured properly, you should observe the contents of the metrics file - `/usr/local/phoneweb/logs/pw_metricsfile`. The generated contents should match your expectation of the configured metrics level. See the *System Reference Manual* for further details on the information logged at each metrics level.

Confirm Platform Licensing

What it Means It is critical to ensure that you have requested and installed your permanent license keys. In particular, the following components require separate license keys:

- VoiceGenie Platform
- SpeechWorks OSR ASR

- Nuance 8.5 ASR
- RealSpeak TTS
- Rhetorical TTS
- Telisma ASR

Genesys and third party suppliers may issue temporary license keys as part of the evaluation or purchase process. It is important to ensure that these are replaced with permanent keys prior to entering production.

The Risk is:

- Server shutdown on license expiry

How to Check

Genesys issues license keys for VoiceGenie in a text file format. This data is stored in the file:

```
/usr/local/phoneweb/config/vglicense.txt
```

Here is a sample license.

```
vggateway in 2037/12/12 100
vggateway out 2037/12/12 100
vggateway asr 2037/12/12 100
vggateway tts 2037/12/12 100
signature=6D61CE2A03FAC3D9EA7E8938CCE5908CA5EE47A1CB5C5AF81740D6D61
CE2A03FAC3D9EA7E8938CCE5908CA5E
```

The important components are the expiration dates, and license counts. Ensure that the expiration date meets your requirements, and that the license count is accurate.

There are a number of different licensing mechanisms in use by various third parties. The following is a list of locations of the various license files:

Nuance (formerly SpeechWorks) OSR ASR

This may exist on the telephony server in a stand-alone configuration or on both the telephony server and ASR server(s) in a Client-Server configuration.

On systems running Linux, the license is named as follows:

```
/usr/local/SpeechWorks/license.lic
```

Here is a sample TEMPORARY license:

```
# This is a license issued by Speechworks Intl of Boston Ma.
# This license certificate authorizes you to use the Speechworks
#software specified below.
# This license created to fulfill order OR487, ID W2083

# This is your OSR license
# Created by GTlicensing on 2003-06-02 00:00:00.0


SERVER this_host ANY 27000
VENDOR swilmgrd
```

```
USE_SERVER
INCREMENT osr_swirec swilmgrd 1.1 29-nov-2003 24 ISSUED=02-Jun-2003
\
SIGN="108C 47CC 1460 B562 9750 00AB 4D63 5D93 0D5C 90BC 6615 \
5CCE DAF7 D4F8 CC2B 0B67 C0B8 C5CD FF49 A2D1 3A4F C707 0819 \
6FD7 1C24 12E4 0C0E 75F1 7F9B F953" SIGN2="018B 4D9D C6D0 EF32 \
B98D BE0F E115 1B9A C5DA 938F 1A03 AAB2 8077 136F 2865 1C83 \
6FF3 3426 2A6B DBDD B971 D0D1 DE7E A0F3 24E2 2123 358C 302D \
F81F 06AC"
INCREMENT osr_swiep swilmgrd 1.1 29-nov-2003 24 ISSUED=02-Jun-2003 \
SIGN="1583 2E85 9B33 B121 28C4 171B 8AF4 2D16 B69F F120 67CC \
0644 3703 412F AE6F 1AB5 5F74 B5B1 EBE3 02C8 AADE 7FB3 10F6 \
B424 77E4 2810 B5B2 C6AC 1A64 43B1" SIGN2="1A29 B2F9 5282 B0D6 \
0BAF 7115 76DD 8707 E167 1452 2EA4 2BFA 74E7 8034 9571 1891 \
2CC4 A7D8 AABE 7457 89FC A30D 237B FD35 DB66 6858 8133 53A0 \
7329 64F4"
```

Important information about this license file and how you can use the information to determine if your license is temporary or permanent is described below.

- *ANY* - this license can be run on any system; if the license is fixed to a system, you would see the MAC address here
- *osr_swirec* - this section of license applies to the SpeechWorks Recognizer Server
- *license osr_swiep* - this section of the license applies to the SpeechWorks EndPointer license
- *29-nov-2003* - this is the expiration date of the license; if the license is permanent, you would see 'permanent'
- *24* - this is the number of ports provided by this license

Nuance 8.5 ASR (on W2K Servers only)

Here is a sample license file:

```
SN: 2030123005
HostLock: anyhost
Port: 8470
Checksum: 612jree95f24

# num          product          version        expiration
# ---          -------        -----------     -----------
  100          sp-chan        800     899      1-sep-2003
  100          v-chan         800     899      1-sep-2003
```

Important information about this license file and how you can use the information to determine if your license is temporary or permanent is described below.

100 - this is the number of ports provided by this license

1-sep-2003 - this is the expiration date of the license, if the license is permanent, you would see '***31-dec-2037***

Here is a sample license key:

ncr85-200-2050823002-a-2x12-c63653157b5d

Important information about this license file and how you can use the information to determine if your license is temporary or permanent is described below.

ncr85 - Channel restricted license for Nuance 8.5

200 - 200 port license

2050823002 - Serial Number

a - Hostlock (a for anyhost)

2x12 - Expiration date (where 2 is day of week, x is for December, 12 is added to 1990 to get the year). Note: a: January, b: February, c: March … with x: December

c63653157b5d - Checksum

Rhetorical TTS

This may exist on the telephony server in a stand-alone configuration or on both the telephony server and TTS server(s) in a Client-Server configuration. On systems running Linux, the license is named the following:

```
/usr/local/rhetorical/license.txt
```

Here is a sample license:

```
FEATURE rvoice_server rhetld 4.0 22-aug-2003 uncounted \
    HOSTID=000347f1517b SIGN="031E 3FBF 9523 022C 8E40 BC61 3071 \
    375F 6616 C34F 1500 05F5 C39E 525C 00A3 5152 2433 6FC1 A334 \
    FC72 333A" SIGN2="0133 1D24 DFB3 FBEB FB58 0C20 786B 4800 4B5D \
    C02E 9203 AABE 2704 CEF7 B3DC 34AD CBC3 0A52 E26A 75F2 9AA8"
FEATURE rvoice_en_ga_f05 rhetld 4.0 22-aug-2003 uncounted \
    HOSTID=000347f1517b SIGN="0298 287C 1B16 2DAB E40B 061C 8FF9 \
    F9CE 43F8 BF9E 6001 AF43 11AC A048 B492 4650 8032 DCCE 3C08 \
    273F DB7B" SIGN2="036A 71DE CA67 5687 4281 5D79 8444 4B24 5CA4 \
    F30F 5002 18F2 B3C3 4285 6CDB 4B07 1D64 9A94 E3B8 F28A 1A04"
FEATURE rvoice_en_ga_f05_usaddress rhetld 4.0 22-aug-2003 uncounted \
    HOSTID=000347f1517b SIGN="02D9 AE31 D1EF 73A9 B626 99C8 9606 \
    E196 0E8C 9848 C501 CF2C 1D56 970D ADB0 3B83 0BAC 6700 504B \
    D022 3C9A" SIGN2="0233 D8B8 DA7A B3A6 6E93 EAD8 A19D 7662 BBAA \
    2123 8602 8722 97A0 E45A C175 46C7 71F9 AE35 ABDE 151C B82B"
```

Important information about this license file and how you can use the information to determine if your license is temporary or permanent is described below.

rvoice_server - this section of the license applies to the Rhetorical server license

rvoice_en_ga_f05 - this section of the license defines that the en_ga_f05 voice is licensed (note that you require a license for each voice you intend to use on the platform)

rvoice_en_ga_f05_usaddress - this section of the license defines that the en_ga_f05_usaddress voice is licensed (note that you require a license for each voice you intend to use on the platform)

4.0 - this is the Rhetorical version that the license will work with

22-aug-2003 - this is the expiration date of the license; if the license is permanent, you would see 'permanent'

Realspeak TTS

This may exist on the telephony server in a stand-alone configuration or on both the telephony server and TTS server(s) in a Client-Server configuration.

On systems running Linux, the license may be named as follows:

```
/usr/local/SpeechWorks/license.lic
/usr/local/Scansoft/license.lic
```

Here is a sample license:

```
SERVER this_host ANY 27000
VENDOR swilmgrd
USE_SERVER
INCREMENT speechify_switts swilmgrd 4.0 20-may-2006 200 \
        ISSUED=21-Nov-2005 SIGN="036B 28A8 154F E5D1 EB20 3A08 37B6 \
        CBBB AA93 F27B 066C 52F9 F9D5 4A8D 78B8 1B28 836F EA51 FE9A \
        2A5A B2B6 878E 59A2 3069 C794 6D7F 4B4D A431 6024 E543" \
        SIGN2="0E2E CBCF 5251 A1F6 3A3C 6CF0 E1B6 59E9 0053 5563 C01C \
        2F63 D3C2 B8D7 C114 1A43 7CDE 32D1 2208 E0BE A330 A91B AA4D \
        B304 442C DF53 4D6F 45E2 5CBF 3DD3"
```

Important information about this license file and how you can use the information to determine if your license is temporary or permanent is described below.

ANY - this license can be run on any system; if the license is fixed to a system, you would see the MAC address here

speechify_switts - this section of license applies to the SpeechWorks Realspeak TTS Server license

20-may-2006 - this is the expiration date of the license; if the license is permanent, you would see 'permanent'

200 - this is the number of ports provided by this license

Note: The Realspeak license may be merged with the Scansoft OSR license if the OSR is running on the same system as the Realspeak TTS

Ensure Tuning/Analysis Directories are Managed

What it Means

There are a number of standard directories that are used to collect tuning data, or as part of advanced applications. These directories may contain utterance audio data, full or partial call recordings, or other data related to call processing.

Note that it is possible to configure application specific utterance and full call recording directories. If you are using these features in your application, use the techniques described below to monitor these directories (size and number of inodes used). Also ensure that data is purged or migrated off board in a timely manner, and as required by your application.

How to Check

Directory size can be checked manually as follows:

```
du -s <directoryname>
```

For example:

```
du -s /usr/local/phoneweb/utterance
```

will check the directory and report the size in kilobytes.

Inode availability can be checked manually as follows:

```
df -i
```

Resulting in output similar to the following:

```
Filesystem            Inodes   IUsed   IFree IUse% Mounted on
/dev/hda1             536448   65536  470912   13% /
none                   47831       1   47830    1% /dev/shm
/dev/hda2           12976128    8203 12967925    1% /usr/local
/dev/hda3           1048576    1203 1047373    1% /var
```

Should the number of inodes (IUse%) be greater than 10% in the `/usr/local` directory, proper file management may not be set up. This would most likely be due to a large number of files in the `/usr/local/phoneweb/tmp` directory. This should be investigated further and `savetmpfiles` should be disabled in accordance with the description earlier in this document.

Clean the Disk

What it Means

During testing and debugging, it is often the case that tracing and logging have been enabled to resolve problems. It is prudent to clean up the disk prior to entering production.

Potential offenders are shown in the table below.

Table 24: Standard Directories

Purpose	Location
Utterance Recording	`/usr/local/phoneweb/utterance`
Recorded Data	`/usr/local/phoneweb/record`
Full Call Recording	`/usr/local/phoneweb/callrec`
Temporary System Storage	`/tmp`
Temporary Application Storage	/usr/local/phoneweb/tmp
Trace Data	`/usr/local/phoneweb/logs/CMP.log*`
Metrics Data	`/usr/local/phoneweb/logs/pw_metrics*`
System Log Data	`/usr/local/phoneweb/logs/pw_logfile*`
CMP Server	`/usr/local/cmp-server/logs/CMP.log*`
CMP SMC	`/usr/local/cmp-smc/logs/CMP.log*`
CMP Proxy	`/usr/local/cmp-proxy/logs/CMP.log*`
CMP Database	`/usr/local/cmp-db/scripts/*backup*`
Database	`/var/lib/mysql/mysql/*`
Database NDM	`/var/lib/mysql/NDM/*`
Database CallHistory	`/var/lib/mysql/CallHistory/*`
SRM Server	`/usr/local/srm-server/logs/*`
Speechworks Utterances	`/usr/local/SpeechWorks/OpenSpeechRecognizer/data/`
Undelivered Email	`/var/spool/mqueue/*`

The Risk is:

- Reduced Efficiency

How to Check

Use `du -s` to confirm the size of the directories. Ensure that these directories have been emptied prior to entering production.

Optimize CMP Thresholds for Restarting Components

What it Means The VoiceGenie platform is a highly optimized VoiceXML execution environment. However, different configuration profiles can have various effects on system memory performance. If running a system with a large number of TTS resources and/or a large complex grammar(s), a review of the setting for the SRM Server restart thresholds is recommended. These thresholds should be configured to be as large as the system memory. The optimal setting should be 2.5GB or the maximum physical memory (whichever is lower).

The Risk is:

- Process restarts

How to Check This configuration will require manual modification of the `CMP Proxy configuration` file that is targeted to the system hosting the SRM Server software. From the `SMC -> Configuration -> CMPProxy` window, identify which `CMPProxy` is targeted to the system with the SRM Server software. Edit the file, locate and change the following settings:

Figure 35: srms_limits

The setting should be modified to 95|2000|10000 for a system with 2GB of memory, and to 95|2500|10000 for a system with more than 2GB of memory. The setting should be updated, and the system should be restarted.

Perform Failure Mode Testing

What it Means As part of the installation qualification process prior to entering production, prepare a test plan to ensure that any potential failure modes have been addressed. This will ensure that the system behaves as intended in the event of a failure somewhere in the architecture.

How to Check Methodology will depend on the back-end systems to which the platform is connected. Your Professional Services consultant may be able to offer services to improve the robustness of your deployment.

Perform Load Testing

What it Means The VoiceGenie platform is a highly optimized VoiceXML execution environment. However, each VoiceXML application can have different performance characteristics, and thus should be tested under load as part of application development and certification. This will ensure that any potential bottlenecks or problems in the architecture can be identified and corrected early in the process.

How to Check Please contact your Professional Services consultant if you require assistance determining the maximum load of your system.

Platform Security Audit

What it Means You should ensure that your platform has been secured prior to entering production.

How to Check Here is a list of things to check:

- Have the default passwords been changed?
- Has the firewall been enabled?
- Have you disabled unneeded services (telnet, ftp, etc.)?

Application Checklist

Most elements are part of the platform configuration. However, the following elements may also be part of your application, and should be checked as described above:

- '`savetmpfiles`' property
- '`metricslevel`' property
- Ensure `Tuning/Analysis` Directories are maintained

Summary

The VoiceGenie platform has been engineered for very high availability and uptimes. Adherence to these guidelines will aid in achieving this in production.

Chapter

10 SDK

Products/areas within this category include:

- Agent Desktop .NET Toolkit
- Genesys Interface Server
- Interaction SDK
- IVR SDK
- Platform SDK
- Simulator Test Toolkit
- T-Library SDK

This chapter covers the following topics:

Architecture

This section includes the architectural diagram for Genesys Interface Server. No other products in this section have associated architectural diagrams.

Genesys Interface Server

Figure 36 illustrates the architectural diagram for Genesys Interface Server (GIS) 7.1.

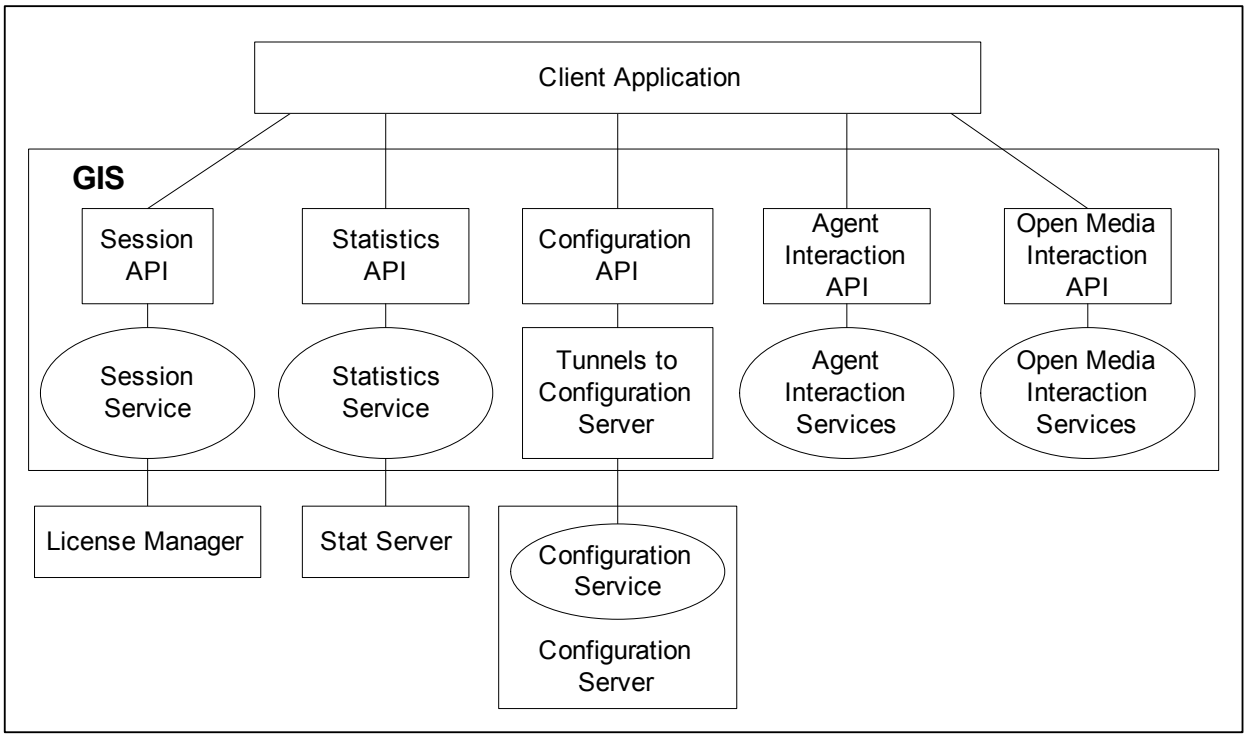


Figure 36: Genesys Interface Server 7.1 Architecture

6.x and 7.x Products

Table 25 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 25: Information to Supply with 6.x/7.x Support Requests

Product	Information to Supply with Support Requests
Genesys Interface Server_Samples (Clients)	• GIS_Core information (see the entry for GIS_Core) • Stat Server information (see the entry for Stat Server) • Screen capture covering the period in which the problem occurred • Source code of the custom functionality - methods, classes - implemented over Genesys

Table 25: Information to Supply with 6.x/7.x Support Requests

Product	Information to Supply with Support Requests
Genesys Interface Server Core	• GIS configuration • GIS log file covering the period in which the problem occurred (preferably with debug level set to 'debug')
Interaction SDK	• Interaction SDK log (configured separately) • T-Server logs • MCR (Multi-Channel Routing) suite logs (Interaction Server, Chat Server, and Universal Contact Server)

Chapter

11 Workforce Management

Products/areas within this category include:

- Workforce Management

This chapter covers the following topics:

Architecture

Figure 37 illustrates the architecture for Workforce Management 7.x

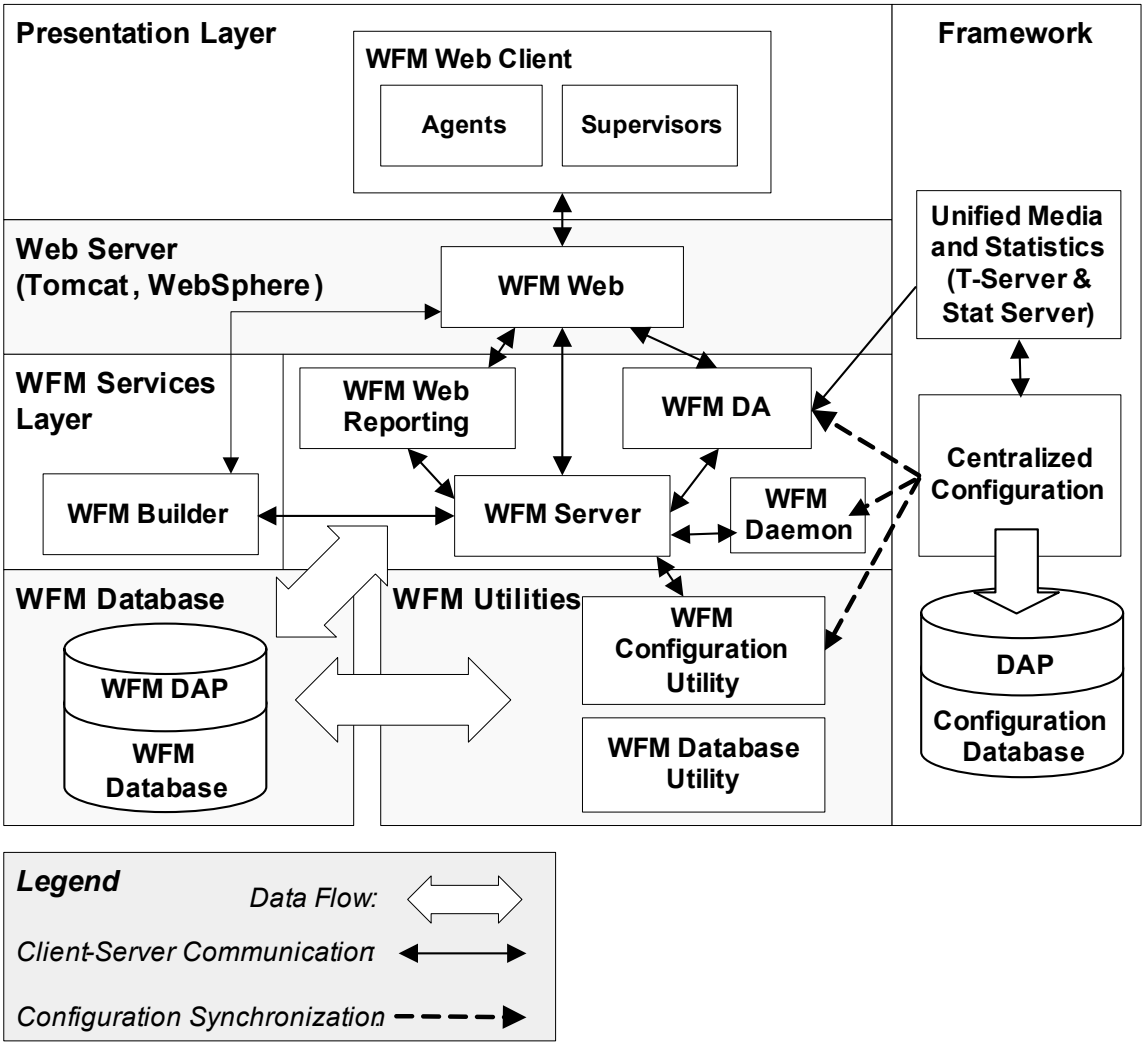


Figure 37: Workforce Management 7.x Architecture

Figure 38 illustrates the architecture of Workforce Management 6.x.

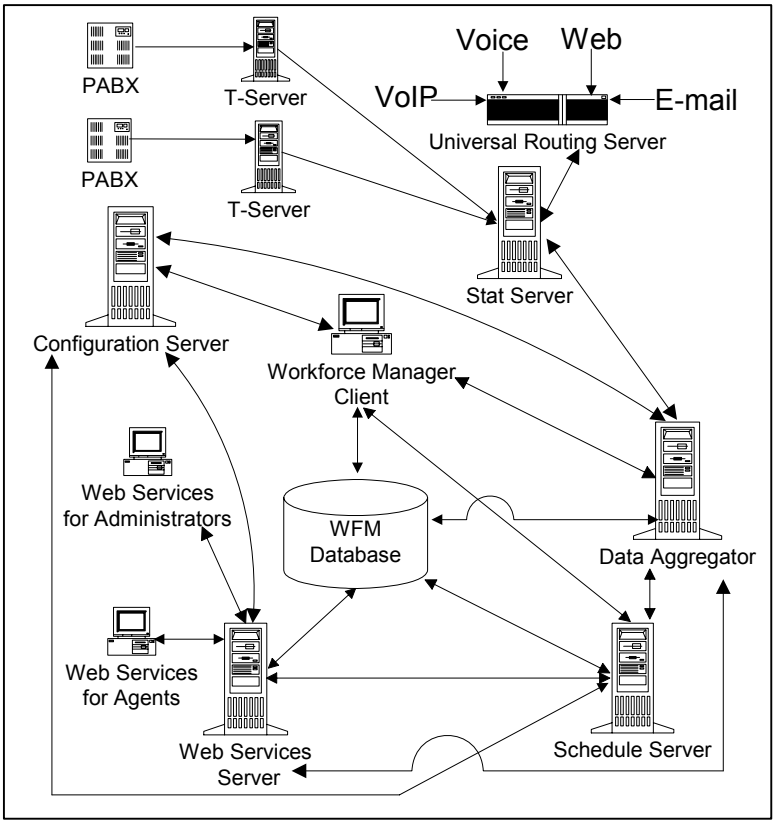


Figure 38: Workforce Management 6.x Architecture

7.x Products

Table 26 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product..

Table 26: Information to Supply with 7.x Support Requests

Product	Information to Supply with Support Requests
WFM Configuration Utility	• Exact version (screenshot: `Help->About`) • Screenshots indicating problem (error\warning or reproduce scenario) • WFM DB Backup[a] • WFM Client application configuration option settings exported from Configuration Manager
WFM Web	• Exact version (screenshot: Help->About) • Exact version of WFM Server (WFMserver.exe -v) • J2SDK on server host and JRE versions on client host • Exact version of Tomcat (and whether it was installed as a console or a service) or WebSphere • Logs: WFM Web, WFM Server, Tomcat/WebSphere stdout, and stderr • Screenshots indicating problem (error/warning or reproduce the scenario) • WFM DB Backup[a] • WFM Web application configuration option settings exported from Configuration Manager
WFM Server	• Exact version of WFM Server (`WFMserver.exe -v`) • Logs: WFM Server and correspondents component logs which are lead to problem[b] • Screenshots indicating the problem: error/warning or reproduce the scenario if applicable/possible • WFM DB Backup[a] • WFM Web application configuration option settings exported from Configuration Manager

Table 26: Information to Supply with 7.x Support Requests (Continued)

Product	Information to Supply with Support Requests
WFM Builder	• Exact version of WFM Builder (`WFMBuilder.exe -v`) • Screenshots indicating the problem (error/warning or reproduce the scenario) • WFM DB Backup which contains the problem scenario; where possible reproduce the problem • WFM Builder and WFM Server application configuration option settings exported from Configuration Manager • Logs for the following: ◆ WFM Builder ◆ `builder-<date>-<time>.log` ◆ `sword-<date>-<time>.log` To produce full builder logging, set these options as follows: ◆ `Log\x-ScheduleBuilderOutputTrace` equal to `yes`. ◆ `Log\x-ScheduleBuilderTrace` equal to `yes`. ◆ `Log\x-SwordTrace` equal to `yes`. ◆ `Log\x-ScheduleLogPath` equal to any folder where you would like place these log files. ◆ `Log\x-ScheduleMaxLogs` equal to the maximum number of files that will be created in that folder. The default value is `1000`.
WFM Data Aggregator	• Exact version of WFM Data Aggregator (`DA.exe -v`) • Screenshots indicating problem (error/warning or reproduce the scenario) • WFM DB Backup[a] • WFM Data Aggregator and Stat Server applications configuration option settings exported from Configuration Manager • Logs from the following: ◆ Data Aggregator ◆ Stat Server ◆ WFM Server ◆ DBDumpFile (if any)

Table 26: Information to Supply with 7.x Support Requests (Continued)

Product	Information to Supply with Support Requests
WFM Database Utility	• Exact version (screenshot of the initial screen) • Screenshots indicating the problem (error/warning or reproduce the scenario) • WFM DB Backup[a] • WFM Client application configuration option settings exported from Configuration Manager • Database Utility logs for the appropriate action (different logs are generated for backup, restore, cleanup, migration)
WFM Report Server	• Exact version of WFM Report Server (`WFMReports.exe -v`) • Exact version of WFM Server (`WFMserver.exe -v`) • Screenshots indicating the problem (error/warning or reproduce the scenario which reports the cause of the problem) • WFM DB Backup[a] • WFM Report Server and WFM Server application configuration option settings exported from Configuration Manager • Logs from the following: ◆ WFM Report Server ◆ WFM Server

a. If the problem is easily reproducible, providing DB backup is optional. However, you, as the customer, must be ready to provide it if requested by Technical Support.

b. If you, as the customer, are able to identify any bindings; otherwise, provide all WFM component logs covering the problem for one period.

6.x Products

Table 27 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 27: Information to Supply with 6.x Support Requests

Product	Information to Supply with Support Requests
Workforce Manager	• Full version info of WFM and Configuration Server • WFM database export (an MDB file created by the WFM Backup/Restore utility - brutil.exe) or WFM database dump created with DBMS • If problem is with schedules, send schedule log files (SchFile key value in Log branch on Options tab), schedule server ini file (SchServer.ini) and Claire log file (ClaireFile key value in Log branch on Options tab) • If problem is with Adherence or Data aggregator, send Data aggregator log files covering the period when the problem occurred, Data aggregator ini file (DAConfig.ini), log file(s) produced by the WFM (Standard, Trace, Debug keys values in Log branch on Options tab), Stat Server information (see the entry for Stat Server) • CCPSF logs from the workstation where the problem occurred • Screen captures showing the problem are very helpful • If problem is with Web Services, send Web Services log file and IIS log file If problem is with Data Importer, send the comma separated (`.csv`) data file being used

Chapter

12 Other

Products/areas within this category include:

- Genesys Enterprise Telephony Software (GETS)
- WFM Blue Pumpkin Integration
- Call Director Route
- Call Director Voice
- CallPath
- Expert Contact
- Express
- IP Media eXchange
- Universal Workflow
- Other

This chapter covers the following topics:

Architecture

This section contains architectural diagrams for some of the products listed earlier. For all those not included here, see their respective documentation for architectural descriptions.

GETS 7.2

Genesys Enterprise Telephony Software (GETS) is essentially a translation device between Microsoft's Live Communication Server (LCS) 2005 and an enterprise PBX using the CSTA-over-SIP communication protocol.

LCS 2005 provides your business with enterprise-ready instant messaging (IM), presence awareness, and an extensible platform that connects people, information, and business processes, enabling better decisions faster. With a familiar user experience integrated into Microsoft Office System programs, LCS 2005 allows people to communicate without the constraints of geography, office location, or time zone.

Figure 40 is a high-level functional diagram of the Microsoft Live Communications Server 2005-based Genesys GETS solution. GETS bridges the data and telephony worlds allowing for the integration of telephony into the Microsoft Office Communicator.

Note: Microsoft Live Communications Server is not a Genesys product, however. As the GETS solution is based on the integration to the Microsoft Live Communications Server, it is a key component of the solution.

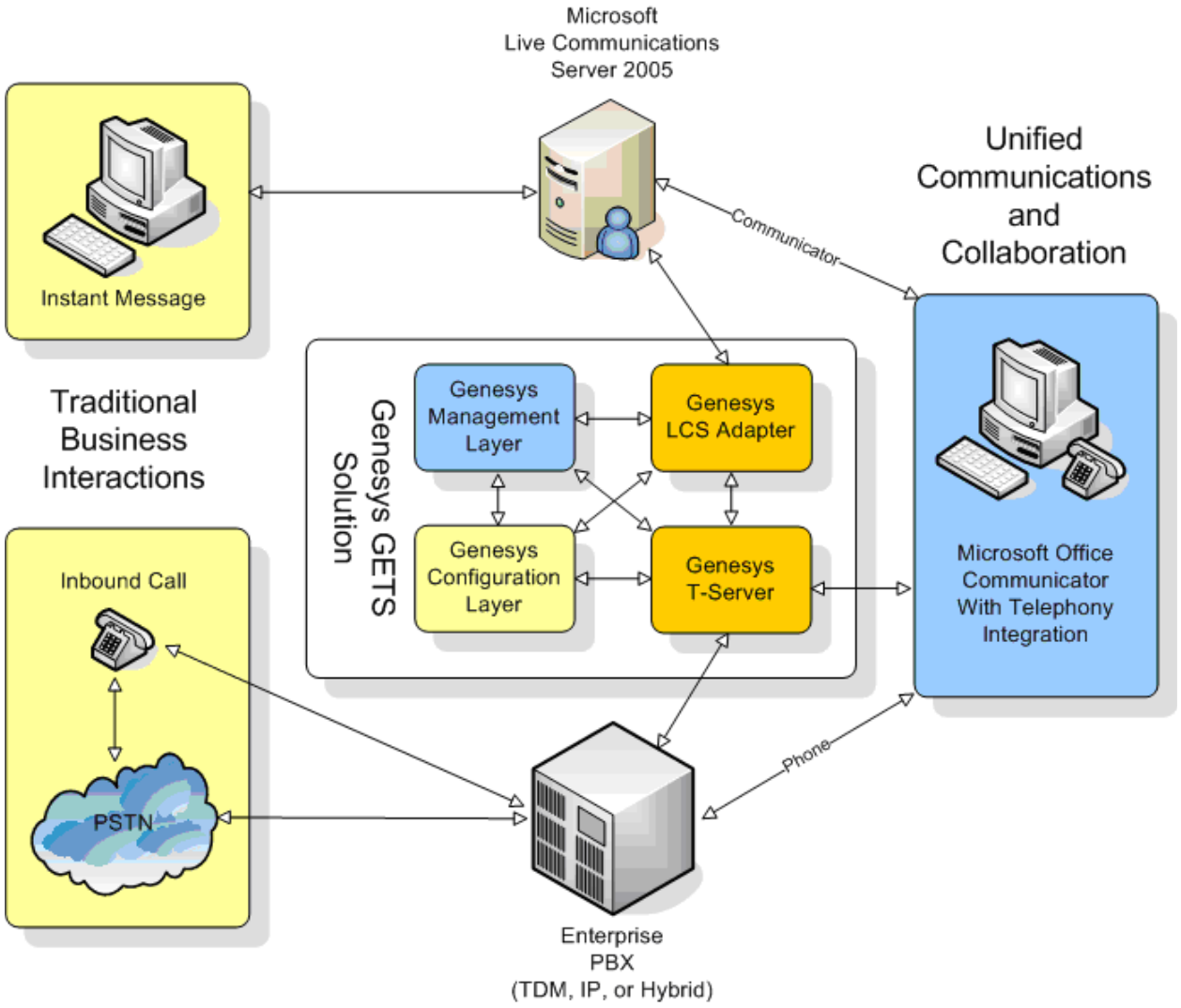


Figure 39: GETS 7.2 High-Level Architecture

GETS includes the following components:

- LCS Adapter: This works with Genesys T-Server and Microsoft Live Communications Server to enable telephony functionality in the Windows Microsoft Office Communicator.
- ETDB Synchronization Utility: This facilitates the synchronization of the GETS Enterprise Telephony Database with Microsoft's Active Directory.

Figure 40 illustrates a relationship between these components and Microsoft LCS 2005.

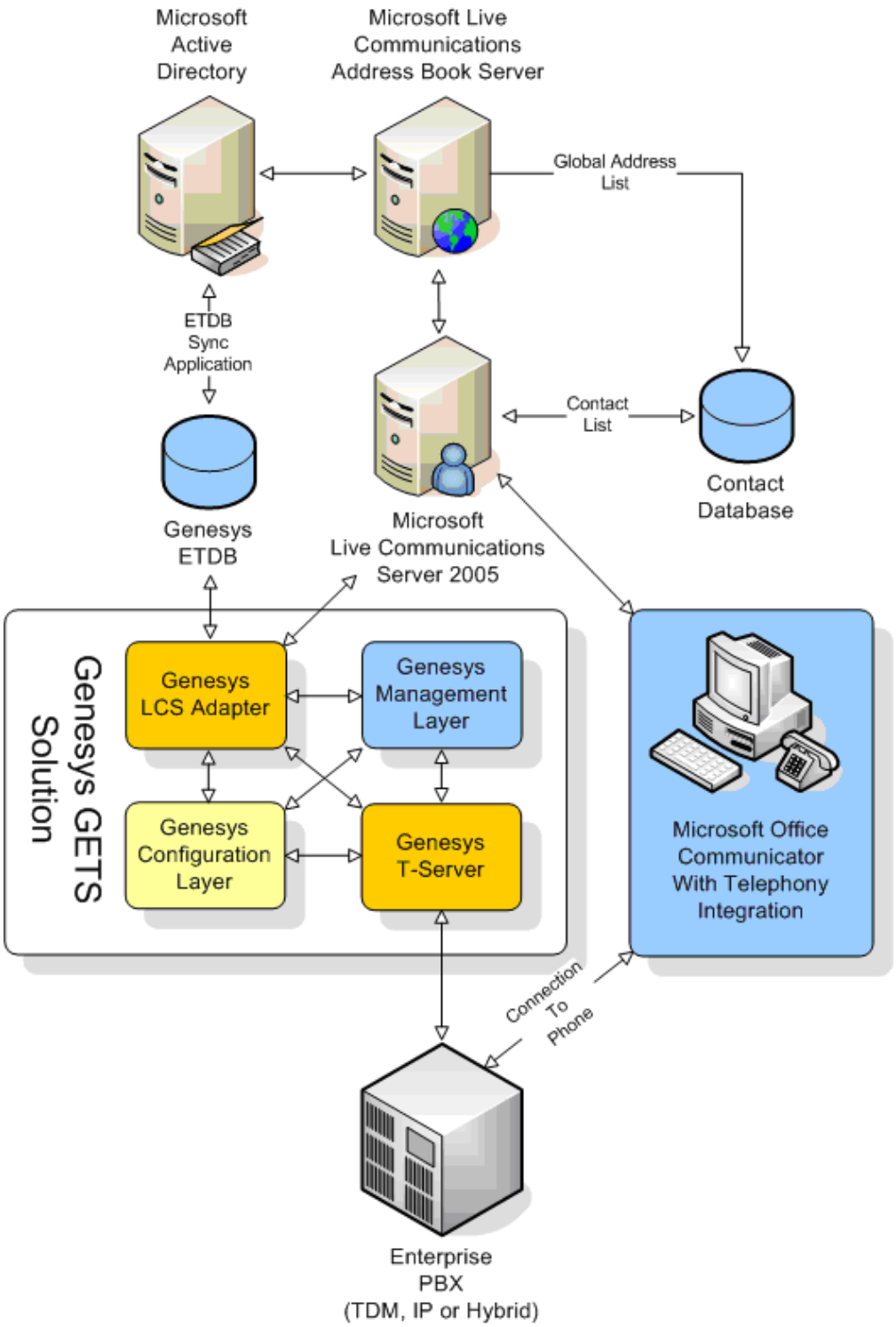


Figure 40: LCS Adapter and ETDB Synchronization Utility

The Genesys GETS/Microsoft LCS 2005 Solution topology potentially encompasses a variety of components from an end-to-end perspective. Figure 41 presents a perspective of where the Genesys GETS fits into the overall picture with a Microsoft Live Communication Server 2005 Implementation Topology.

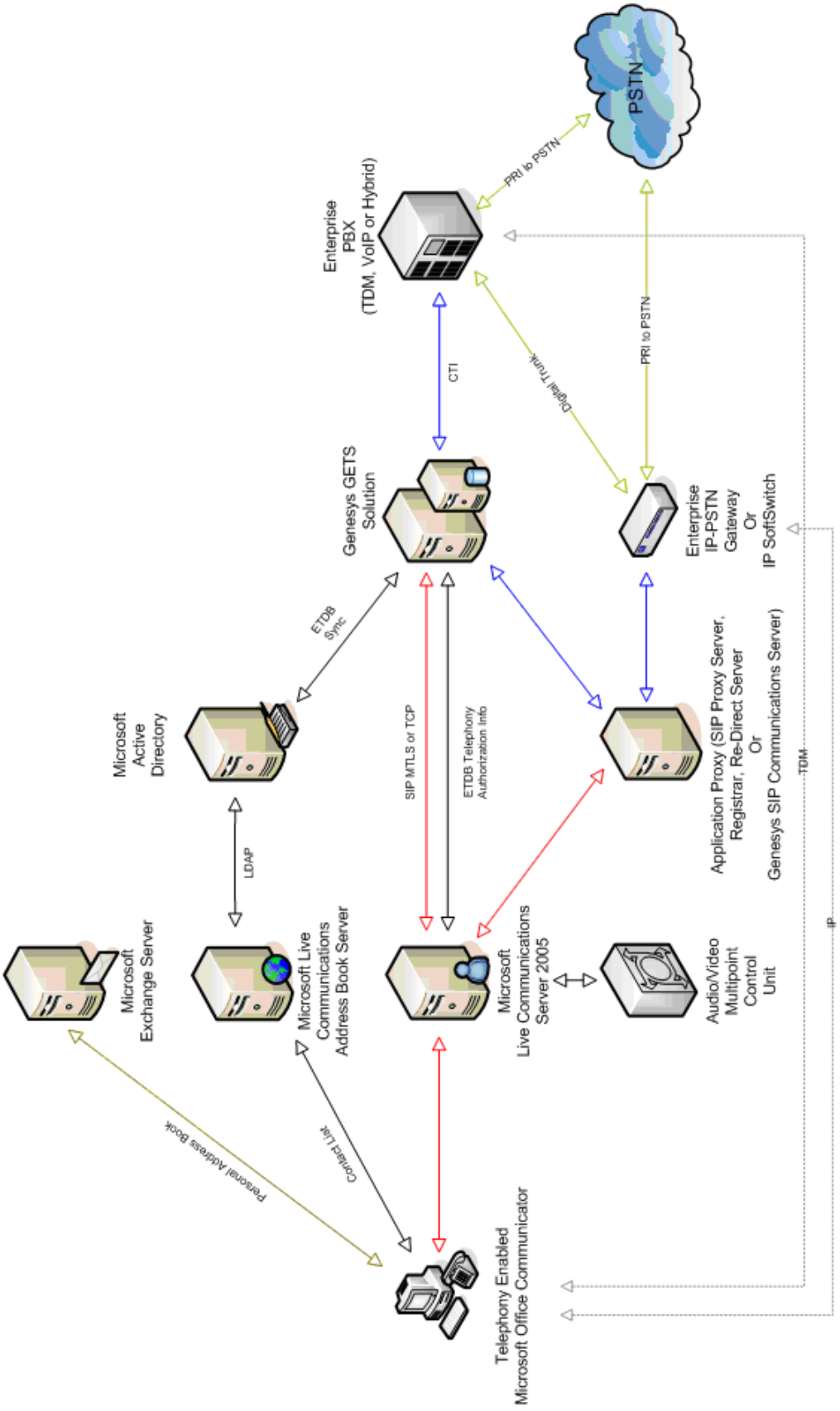


Figure 41: GETS/Microsoft LCS 2005 Solution Topology

The Microsoft components include:

- Microsoft Office Communicator
- Microsoft Active Directory
- Microsoft Exchange Server

Other components involved in Microsoft LCS and GETS include:

- PBX (Private Branch Exchange)
- IP-to-PSTN Gateway
- Application Proxy
- Genesys SIP Communication Server
- SIP Proxy
- SIP Redirect Server
- SIP Registrar
- Audio/Video Multipoint Control Unit

Note: For descriptions of the components, see the *Microsoft Office Communicator 2005 Planning and Deployment Guide,* available from Microsoft's website. For Genesys components, see the *Genesys 7.2 GETS for Microsoft LCS 2005 Administrator's Guide.*

Blue Pumpkin Integration

Figure 42 illustrates the architecture of Blue Pumpkin Integration 7.1.

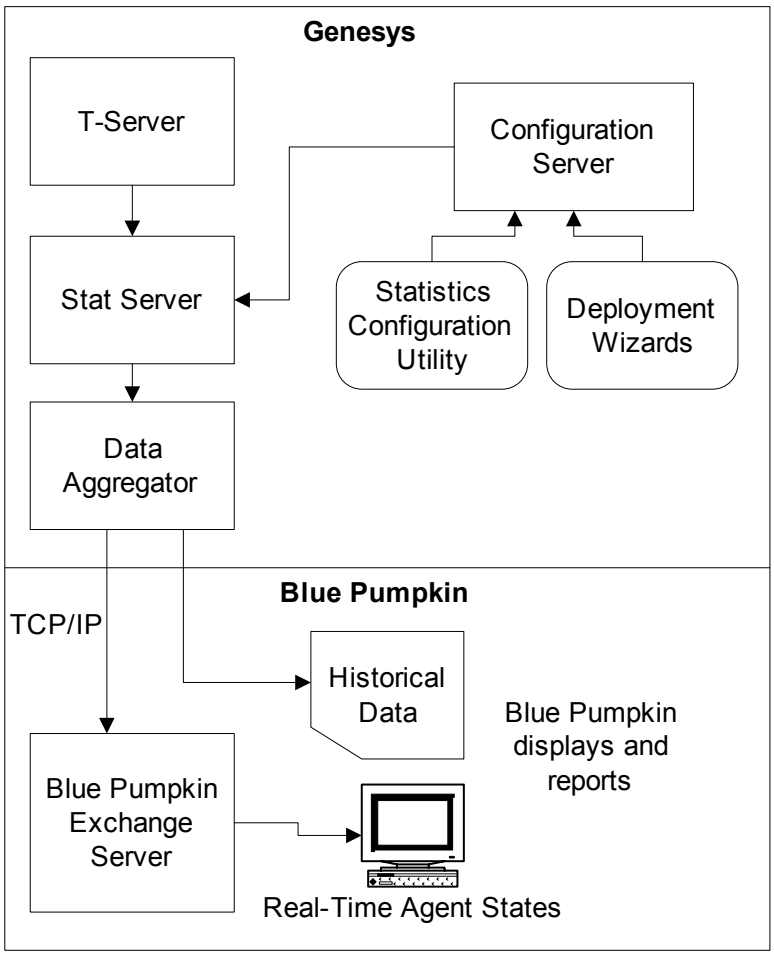


Figure 42: Blue Pumpkin Integration Architecture

Expert Contact

Figure 43 illustrates the architecture for Expert Contact 7.2 in a premise-based environment.

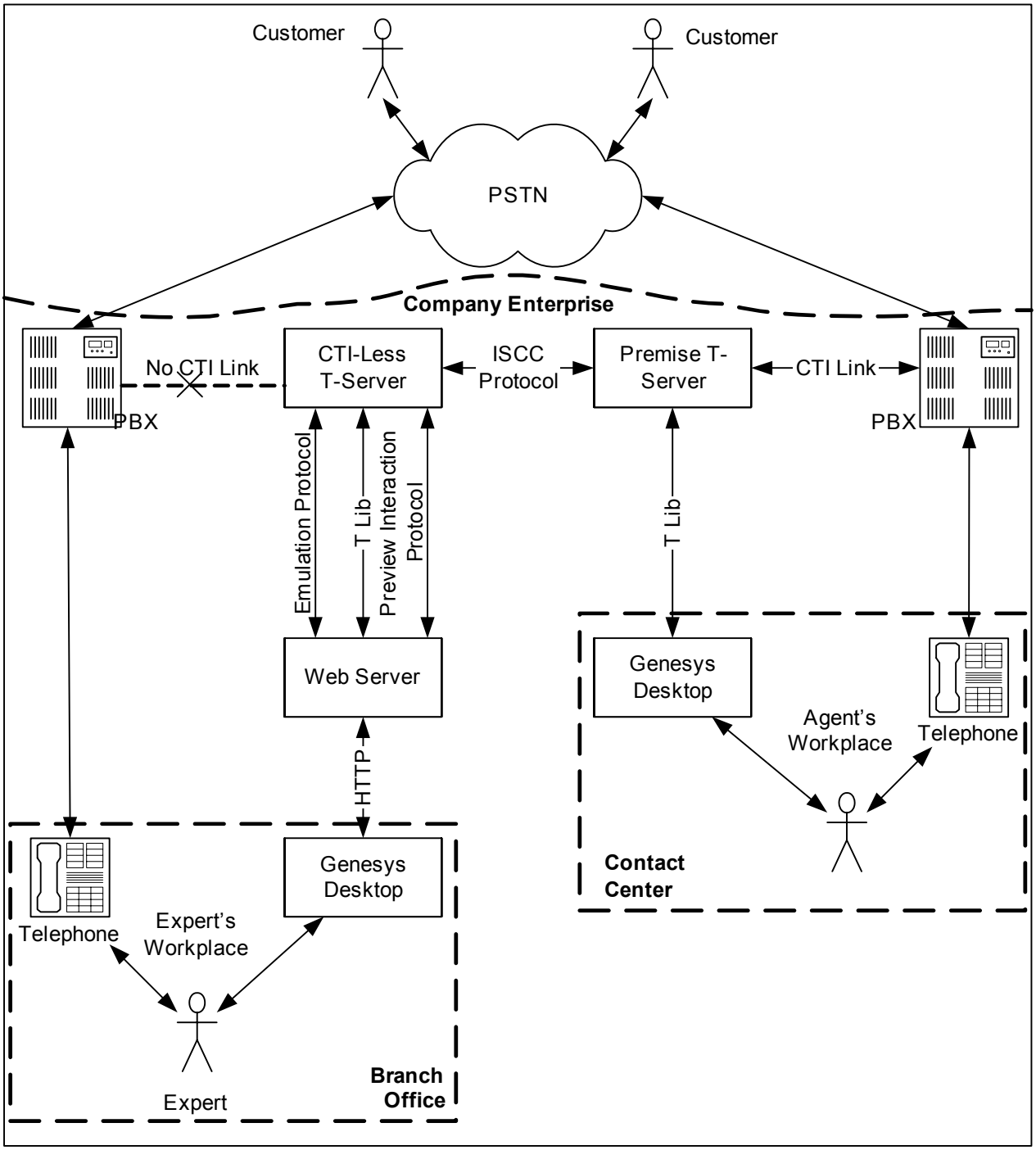


Figure 43: Premise-based Environment - Expert Contact 7.2 Architecture

IP Media eXchange

Figure 44 illustrates the architecture for IPMX 7.0.

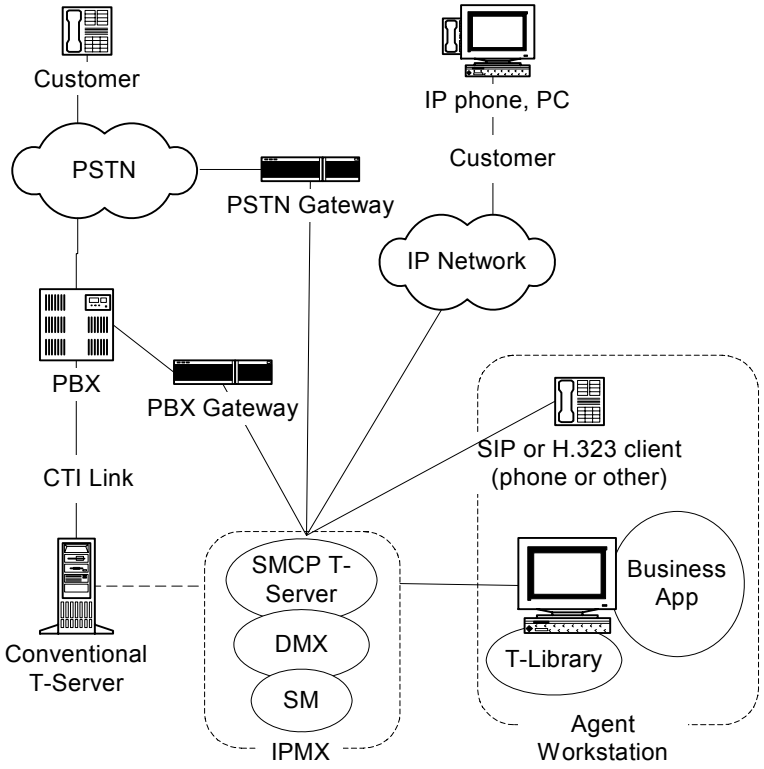


Figure 44: IPMX 7.0 Architecture

CallPath

Figure 45 illustrates the architecture for CallPath 6.5.

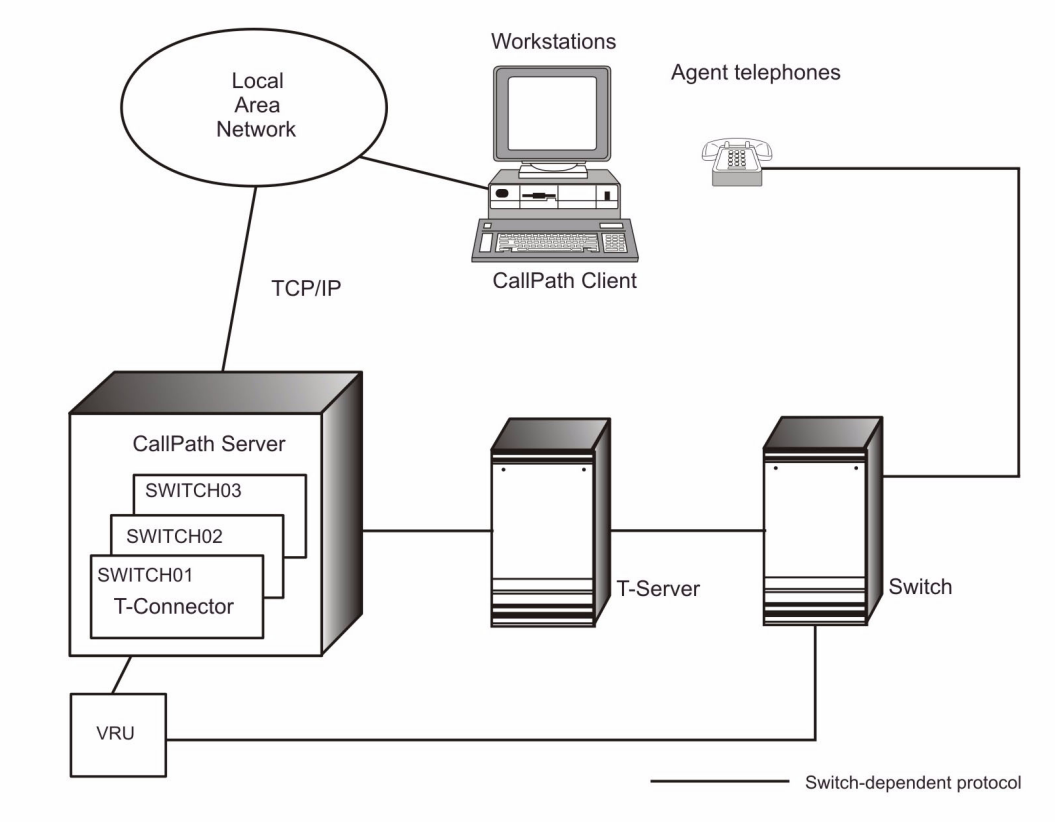


Figure 45: CallPath 6.5 Architecture

7.x Products

Table 28 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 7.x product.

Table 28: Information to Supply with 7.x Support Requests

Product	Information to Supply with Support Requests
GETS	• LCS Adapter configuration • LCS Adapter log files using the `x-server-trace-level` option set to the value of `3` for the time period when the problem occurred. This option sets the default value for all troubleshooting-related log options that are unique to LCS Adapter, which includes `x-server-sip-trace-level`, `x-serversiplib-trace-level`, `x-server-gcti-trace-level`, `x-servercsta-trace-level`, and `x-server-config-trace-level` options. See the *Genesys 7.2 GETS for Microsoft LCS 2005 Administrator's Guide* for more information. • T-Server information (see the entry for T-Server) • ETDB Synchronization Utility configuration, if applicable • ETDB Synchronization Utility log files with debug level details covering failed or incomplete synchronization session, if applicable

Table 28: Information to Supply with 7.x Support Requests (Continued)

Product	Information to Supply with Support Requests
WFM Blue Pumpkin Integration - WFM BPI Data Aggregator BPI Statistic Configuration Utility	• Screenshots indicating problem (error, warning, or reproduce the scenario) • WFM Data Aggregator and Stat Server applications configuration option settings exported from Configuration Manager • Logs for the following: ◦ WFM Data Aggregator ◦ Stat Server • `*.bpi` files if they indicate the problem; files should correspond to the Data Aggregator logs • Version of WFM Data Aggregator (`DA.exe -v`) • Version of Statistic Configuration Utility (`Help > About`) • Version of Stat Server • Blue Pumpkin version in use • OS versions, including service pack, used on the machine where the WFM BPI components are installed
IP Media eXchange	• SMCP T-Server, DMX, Stream Manager configuration option settings exported from Configuration Manager. • SMCP T-Server, DMX, Stream Manager log files with Debug level detail covering the start-up of the component • SMCP T-Server, DMX, Stream Manager log files with Debug level detail covering the period when the problem occurred • Information about IP endpoints and VoIP gateways (Model and firmware version)

6.x Products

Table 29 details the product-specific information that should be supplied when logging a support request in relation to a problem with a particular Genesys 6.x product.

Table 29: Information to Supply with 6.x Support Requests

Product	Information to Supply with Support Requests
CallPath Base Server	• Screen capture • CallPath Base Server Error log(s) • CallPath Real-time trace covering the start-up of the Server • CallPath Realtime trace covering the period in which the problem occurred • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only)
CallPath Enterprise Client	• Screen capture • CallPath Enterprise Client traces (`csebclnt.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise • Method=SHARED_MEMORY) getting `logclnt.fil` and `logbclnt.*` • `Cse*.ini` files • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only)
CallPath Enterprise Client for Siebel Systems	• Screen capture • CallPath Enterprise Client traces (`csebclnt.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting logclnt.fil and logbclnt.* • `Cse*.ini` files • CallPath Base Server logs

Table 29: Information to Supply with 6.x Support Requests (Continued)

Product	Information to Supply with Support Requests
CallPath Enterprise Dialer and Predictive Dialer	• Screen capture • CallPath Enterprise Server errorlog (`skberr`) • CallPath Enterprise Server traces (`csesskbr.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting `logskbr.fil` and `logbskbr.*` and `skbrlog` and `skbrblog.*` • `Cse*.ini` files • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise DDE	• Screen capture • Turn on debug for `AZADDE.EXE` with /debug flag and go to options/logging and select both file and screen. • `Azatads.log` and `azadde.log` • `Cse*.ini` and `aza*.ini` files • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • CallPath Base Server logs • Failure description
CallPath Enterprise HAT Facility	• Screen capture • Turn on debug for `AZAHMENU.EXE` with /debug flag and go to configure/message logging and select both file and screen. • `Azatads.log` and `*.HAT` files • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • CallPath Base Server logs • Failure description

Table 29: Information to Supply with 6.x Support Requests (Continued)

Product	Information to Supply with Support Requests
CallPath Enterprise Intelligent Routing	• Screen capture • CallPath Enterprise IR logs (`azairf.ini` and `azairdb.ini` having Level=ON, Method=FILE) producing `logirf.*` and `azairdb.ini` producing `logirdb.*` • `Cse*.ini` and `aza*.ini` files • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • CallPath Base Server logs • Failure description
CallPath Enterprise Interface	• Screen capture • CallPath Enterprise Server errorlog (`cperr`) • CallPath Enterprise Interface traces (`csebcp.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting `logcp.fil` and `logbcp.*` along with `cplog` and `cpblog.*` logs • `Cse*.ini` files • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise JTAPI	• CallPath Enterprise JTAPI logs making sure `csebjtpi` is started with /t /d flags (`csebjtpi.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARE_MEMORY) getting JTAPI.* • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • `Cse*.ini` files • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise Reporter	• `Reporter.*` files (including `reporter.cfg` and `reporter.out`) • Capture file (which includes the failure time) • CallPath Enterprise Interface logs (see CallPath Enterprise Interface)

Table 29: Information to Supply with 6.x Support Requests (Continued)

Product	Information to Supply with Support Requests
CallPath Enterprise Skills Base Routing	• Screen capture • CallPath Enterprise Server errorlog (`skberr`) • CallPath Enterprise SKBR traces (`csesskbr.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting `logskbr.fil` and `logbskbr.*` and `skbrlog` and `skbrblog.*` • `Cse*.ini` files • CallPath Enterprise Interface logs (see CallPath Enterprise Interface) • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise Server	• Screen capture • CallPath Enterprise Server errorlog (`cperr`) • CallPath Enterprise Server traces (`csebserv.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting `logserv.fil` and `logbserv.*` • `Cse*.ini` files • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise VRU Connections (all VRUs)	• CallPath Enterprise Client traces (`csebclnt.ini` having Level=ON, Method=FILE (if core/drwtsn32 - otherwise Method=SHARED_MEMORY) getting `logclnt.fil` and `logbclnt.*` • `Cse*.ini` files • `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • CallPath Base Server logs (see CallPath Base Server)
CallPath Enterprise VRU Connections for DirectTalk AIX	• AIX system trace “trace -a -1” • DirectTalk for AIX “dtProblem” log file • CallPath Enterprise Interface logs (see CallPath Enterprise Interface logs) and CallPath Base Server logs (see CallPath Base Server)

Table 29: Information to Supply with 6.x Support Requests (Continued)

Product	Information to Supply with Support Requests
CallPath Enterprise Web Connection	• `errpt -a > errpt.txt` or `drwtsn32.log` • `lslpp -L > lslpp.txt` (AIX only) • `Jtcblog` and `csevacd.log` • `Cse*.ini` files • CallPath Enterprise JTAPI logs (see CallPath Enterprise JTAPI)
CallPath Phone for JAVA	• Screen capture • CallPath Enterprise JTAPI logs (see CallPath Enterprise JTAPI) • `Cse*.ini` files
CallPath SwitchServer/2	CallPath SwitchServer/2 system errorlog and trace