PureConnect®

2018 R5

Generated:

12-November-2018

Content last updated:

6-August-2018

See Change Log for summary of changes.

GENESYS™

CIC Automated Switchover System

Technical Reference

Abstract

This content describes the CIC Automated Switchover System processes and architecture, configurations, system requirements, installation, operation, and troubleshooting.

For the latest version of this document, see the PureConnect Documentation Library at: http://help.genesys.com/cic.

Table of Contents

Introduction

Genesys recognizes the need to ensure that the Customer Interaction Center (CIC) server functions in a highly reliable, fail-safe way to prevent unplanned down time. To accomplish this goal, you can configure 2 servers so that one performs the primary CIC functions and the other maintains a mirror image of the primary server. If the primary server fails or becomes disconnected, a **switchover** occurs and the backup server takes over. In most cases, the switchover transition occurs quickly and does not disrupt communications between agents or users of the system. Replication occurs continuously between the two servers to ensure that in the event of a switchover, there is minimal data loss.

For more information about CIC security considerations that may affect your switchover configuration, see *PureConnect Security Features Technical Reference* in the PureConnect Documentation Library at http://help.genesys.com/cic.

For more information on configuring the recovery of call interactions, see *Call Recovery Feature Technical Reference* in the PureConnect Documentation Library.

CIC Switchover system processes and architecture

A switchover environment uses a pair of identical CIC servers:

- The *active server* processes all CIC interactions, such as phone calls, email, faxes, web chats, and voice mail.
- The *backup server* is a mirror image of the active server, duplicating its hardware and software, including the current configuration of CIC. The backup server regularly *monitors* the active server. It validates specific CIC subsystems and looks for the appropriate return signal from an attempted call operation. The backup server also monitors and dynamically copies any changes to the configuration of the active server. These changes include new user entries, line configuration changes, handler updates, or Interaction Attendant profiles. All of these changes keep the Directory Services (DS) tree on the backup server identical to the DS tree on the active server. The backup server also monitors and copies any changed files.

  Note:
  This document uses the terms *active server* and *backup server* to signify the switchover process as occurring between two *states* as opposed to two physical servers.

The backup server starts the switchover process immediately when it detects that the active server is not responding to TS (Telephony System) pings.

Synchronizing the registry on both servers

This section describes how the registry is synchronized on the active and backup servers.

Most of the key configuration data for CIC is stored in the CIC server registry. The configuration data is dynamic and regularly updated using Interaction Administrator and Interaction Designer, serving as an interface to AdminServer and DSServer. The backup server must maintain an identical image of the IC-related registry keys on the active server to be able to take over processing for a failed active server.

Each time the Switchover system starts on the backup server, it establishes a Notifier connection to the active server. The Switchover system then runs a recursive compare-and-update algorithm to determine whether there are differences between the DSServer registry structures between both servers. If necessary, the Switchover system updates the backup server to synchronize both servers using DS notifications.

Note:
Genesys recommends that you back up the registry regularly.

Typically, when the active server handles calls, the Switchover system on the backup server monitors changes on the active server by listening to change notifications from DSServer. Whenever a change to the configuration or CIC registry key occurs on the active server, the server broadcasts a DS notification and replicates the change to the backup server.

When a server in the switchover pair is started, it checks to see if its companion is an active server. If it cannot contact the other server or verify that it is running, it goes into fail-safe mode and starts as the active server.

Important!
Do not change or experiment with the CIC registry keys on the active or backup server unless an PureConnect Customer Care representative directs you to do so. Changing these keys can cause system failures from which CIC cannot recover or problems that are difficult to trace.

Synchronizing CIC directories on both servers

When key files are added, changed, or removed from the active server, that change must be reflected on the backup server automatically. This ensures that the backup server synchronizes with the active server.

When the CIC Switchover service is started on the backup server, it automatically starts monitoring specific default directories on the active server and mirrors all file operations to the backup server.

You can refine the list of mirrored directories by setting one or more server parameters in Interaction Administrator. For more information, see "Switchover Server parameters".

Default mirrored directories

By default, the backup server automatically mirrors the published handler directory *only once,* on startup. This directory is listed in the **Handler Path** server parameter. For example, `\I3\IC\Handlers`.

Any time a handler is published on the active server, the replication process also publishes it on the backup server.

If a switchover event occurs, the published, active handlers are identical on both servers. However, handler files in subdirectories under the `Handlers` directory are not mirrored on the backup server by default.

Audio files that are played in handlers using the `Play Audio File` tool are not replicated. When the handlers are published on the backup server, the new `.ivp` files are created. If the `WhitePages.txt` file is updated, it is automatically copied to the backup server.

If the backup server is unavailable when a change occurs to one of these directories, it replicates all aspects of the active server when it becomes available.

The other default mirrored directories are the **Resource Path** and **I3Tables Path** directories, which are continuously mirrored.

- The **Resource Path** server parameter defines the `resources` directory. For example, `\I3\IC\Resources`. This location is where system and user prompts reside along with the system white pages files.
- The **I3Tables Path** server parameter defines the `i3tables` directory (where Interaction Administrator data tables are stored). For example, `\I3|IC\Server\I3Tables`.

Custom and initial mirrored directories

You can further define the list of mirrored directories by setting the **CustomMirrorDir** and **InitialMirrorDir** server parameters in Interaction Administrator on the active server.

CustomMirrorDir

The **CustomMirrorDir** server parameter specifies one or more directories on the active server that are mirrored on the backup server. Any time a file is added, removed, or modified in one of these directories, the change is mirrored in the corresponding directory on the backup server.

The **CustomMirrorDir** server parameter includes the following directories by default:

- `+D:\I3\IC\Resources`
- `+D:\I3\IC\HostTools`
- `+D:\I3\IC\Server\LRA`
- `+D:\I3\IC\ClientSettings`
- `+C:\I3\IC\Flows`
- `+C:\I3\IC\TFTPRoot`
- `+C:\I3\IC\Provision`
- `+C:\I3\IC\Certificates\LinesAuthority`
- `+C:\I3\IC\Certificates\Email`
- `+C:\I3\IC\Server\I3RxDocs`
- `+C:\I3\IC\Server\Reports`

Note:
The plus sign (+) before the path indicates that all subdirectories of that directory are mirrored.

InitialMirrorDir

The **InitialMirrorDir** server parameter specifies one or more directories on the active server that are mirrored on the backup server when CIC starts on the backup server.

When the active server is operating correctly, the backup server does not monitor the directories that this parameter specifies.

If the directories specified by **InitialMirrorDir** contain many large files, startup of CIC on the backup server can slow down or fail. This occurs because the Switchover subsystem starts early in the CIC process tree. The remaining CIC components are not started until all the mirrored files are copied. If all the changed files are not copied within the maximum startup time allocated by the Switchover system, it does not start and CIC startup fails.

For example, the `Recordings` directory can contain large call recording files that can cause considerable network traffic if they were constantly being replicated on the backup server. You can use the **InitialMirrorDir** server parameter to check this directory for changes and update the changed files only when the backup server starts.

If you know that the initial switchover startup requires more than the allocated maximum startup time to synchronize files, contact PureConnect Customer Care for assistance. PureConnect Customer Care can help you modify the switchover startup timeout configuration in the registry.

Formatting tips

The following notes apply to both the **CustomMirrorDir** and the **InitialMirrorDir** server parameters:

- Each directory in the list is a complete local drive and directory, separated from the next by a semicolon (`;`). For example:
  `D:\I3\IC\Server\Data1; D:\I3\IC\Server\Data2`
- The maximum practical length of the sum of all of the paths entered in 1 server parameter is approximately 2000 characters.
- To mirror the directory recursively, place a plus sign (+) in front of the directory name. That directory and all its subdirectories are mirrored. For example:
  `+D:\I3\IC\Server\Data1`

Caution!
On your CIC server, do not mirror the following directories if you are using Interaction Message Store as your mail provider:
- `D:\I3\IC\Work`
- `D:\I3\IC\Logs`
- `D:\I3\IC\FBMC`

Several CIC processes write temporary files to these directories that are not needed on the backup server. Attempting to mirror these directories could cause problems.

Recommendations

To ensure that all essential CIC files are mirrored on the backup server, add one or more of the following directories to the **CustomMirrorDir** or **InitialMirrorDir** server parameters:

- `D:\I3\IC\Server\Data` (if you export Interaction Administrator configuration data)
- `D:\I3\IC\Reports` (if you customize reports)
- `D:\I3\IC\Handlers\Custom` (or wherever you create customized handlers)

Subdirectory mirroring

To mirror subdirectories, enter a plus sign (+) before the drive letter in the path. For example:
`D:\I3\Server\Data1;+D:\I3\IC\Server\Data2` means all the subdirectories under `Data2` are also monitored and mirrored on the backup server.

The + notation for subdirectory mirroring can cause a problem when you try to delete directories. If you try to delete a directory containing subdirectories that Switchover is monitoring, you receive an **Access is denied** message. Because the directory is being monitored, the OS detects that the directory is in use and thus cannot delete it completely. In fact, it does delete the lowest level of directory. So, to delete a directory called `server` that has a subdirectory called `media` that has a subdirectory called `graphics` (`\server\media\graphics`), you would have to delete `server` three times. The first delete command would remove `graphics`, the second would delete `media`, and the third delete would remove `server`.

Note:
Do not delete directories with subdirectories that you know are mirrored. If you do delete one, delete the entire entry from the mirroring list and then re-add the entry to the mirroring list.

Mirror exceptions

You can use the **MirrorExceptions** server parameter to specify the extensions of any files that you don't want to mirror. Separate multiple extensions with a semicolon. For example: `txt; gif; myext`.

The ping process

The backup server regularly monitors the active server using the following ping processes:

- TS (Telephony Systems) ping
- IP (Interaction Processor) ping

TS ping

During the TS ping process, the Switchover subsystem on the backup server sends a request through the Notifier subsystem on the active server to the TS subsystem on the active server. It then waits for a response. If the Switchover subsystem does not receive a response, it pauses for a specified amount of time (by default, 1 second) and then retries. If the second attempt is also unsuccessful, the backup server immediately starts the switchover procedure.

If you want to change either of the default timeout values, you can create and set the following server parameters in Interaction Administrator on the active server:

- **Switchover TS Timeout**: Specifies the number of seconds that the Switchover system waits from the time the ping is sent until it is marked as a TS failure. The value should be between 5 and 60 seconds. The default is 10 seconds.
- **Switchover TS Failure Retry Delay**: Specifies the number of seconds the Switchover system waits, after marking a TS failure, before sending the second ping. A second failure causes the system to switch.

  > **Note:**
  > Set this value to greater than 0 seconds. The default is 1 second.

- **Switchover Max TS Failures:** Specifies the number of TS ping failures that the Switchover system on the backup server tolerates before starting a switchover.

  > **Note:**
  > Set this value to greater than 0. The default value is 2. (Note that the error count is reset each time the Switchover system successfully receives a response from TS on the primary server.)

Frequently, a TS ping failure indicates that both the network connection and the Notifier connection have been lost, and that the TsServer is either backed up with processing requests or is unresponsive. Usually, the TsServer log is required to diagnose the root cause of the switchover event. However, you should also scan the system event logs and the Switchover log to verify that a lost network connection did not cause the ping to fail.

Successful TS ping samples

The following examples show successful TS pings.

From the Switchover log on the backup server:

Time	Topic	Message
14:15:55.661	NotifierLib	CNotifierSocketConnection::WriteWithCode : SENT Request SwitchoverService, Oid(*), Eid(TS Diagnostic Ping), ReqId(**5328**), SndId(), Size(0)

From the Notifier log on the active server:

Time	Topic	Message
14:15:55.712	NotifierLib	CRoute::LogMessage : Request[SwitchoverService][*][TS Diagnostic Ping]RI[**5328**]SI[]DL[0] From 98:SwitchoverService(SG-CLAY44A, 172.17.112.158:49273) to 70:TsServer

From the TS log on the active server:

Time	Topic	Message
14:15:55.712	NotifierLib	MessageServer::GetMessagesWithCode : RECV Request SwitchoverService, Oid(*), Eid(TS Diagnostic Ping), ReqId(**5328**), SndId(98), Size(0): ReqHandler
14:15:55.712	NotifierLib	CNotifierSocketConnection::Write : SENT Response SwitchoverService, Oid(*), Eid(TS Diagnostic Ping), ReqId(**5328**), SndId(98), Size(7)

From the Notifier log on the active server:

Time	Topic	Message
14:15:55.712	NotifierLib	CRoute::LogMessage : Response[SwitchoverService][*][TS Diagnostic Ping]RI[**5328**]SI[98]DL[7] From 70:TsServer to 98:SwitchoverService(SG-CLAY44A, 172.17.112.158:49273)

From the Switchover log on the backup server:

Time	Topic	Message
14:15:55.661	NotifierLib	MessageServer::GetMessageWithCode : RECV Response SwitchoverService, Oid(*), Eid(TS Diagnostic Ping), ReqId(**5328**), SndId(98), Size(7): SendWithRespOutOfOrder_5328
14:15:55.661	NotifierLib	ModuleByName::Ping() : Received ping from the TsServer module

TS ping failure sample

The following example shows a TS ping failure taken from the Switchover log on the backup server:

Time	Topic	Message
14:17:55.667	ModuleMonitor	ModuleByName::Ping() : Ping rejected to the TsServer module: error count [1] is within maximum [2], ping will be reissued with regular timeout
14:18:05.667	ModuleMonitor	ModuleByName::Ping() : Reached maximum error count [2] pinging the TsServer module on the main connection, resetting error count and trying the alternate connection
14:18:15.667	ModuleMonitor	Ping rejected to the TsServer module: error count [1] is within maximum [2], ping will be reissued with regular timeout
14:18:25.667	ModuleMonitor	Ping was rejected to the TsServer module: reached maximum error count [2], signaling that the module is down
14:18:25.667	PrimaryMonitor	primarymonitor::CPrimaryMonitor::process_module_monitor_event : module monitor indicated the [TsServer] module is not responding, both connections are up
14:18:25.667	PrimaryMonitor	primarymonitor::CPrimaryMonitor::ping_monitored_module : Sending up to 2 ping(s) to the TsServer module using the main connection
14:18:25.671	PrimaryMonitor	primarymonitor::CPrimaryMonitor::ping_monitored_module : Did not receive a reply from the TsServer module after 2 ping(s) on the main connection
14:18:25.671	PrimaryMonitor	primarymonitor::CPrimaryMonitor::process_module_monitor_event : Failed to ping the [TsServer] module, checking connections PrimaryMonitor
14:18:25.679	PrimaryMonitor	primarymonitor::CPrimaryMonitor::check_local_gateway_connections : Successfully pinged local gateway address [172.17.112.1], setting network connection status to 'GatewayReached'
14:18:25.679	PrimaryMonitor	primarymonitor::CPrimaryMonitor::check_net_test_connections : No NetTest addresses to ping, setting network connection status to 'NetTestUnavailable'
14:18:25.679	PrimaryMonitor	primarymonitor::CPrimaryMonitor::check_primary_address : Successfully pinged primary address [172.17.112.171], setting network connection status to 'PrimaryReached'
14:18:25.679	PrimaryMonitor	primarymonitor::CPrimaryMonitor::detect_and_signal_connection_status : module monitor indicated that the [TsServer] module is not responding (all connections are up), primary connection status is 'monitored module down', signaling the module is down
14:18:25.679	PrimaryMonitor	primarymonitor::CPrimaryMonitor::signal_primary_down : Primary connection status=[monitored module down], network connection status=[primary reached]: [TsServer] module is down, posting [event=eTSDown]
14:18:25.682	SwitchoverStates	SwitchoverState::StateBackup : Module is down, switching now and going to StatePrimary

Note:
The TS pings are failures. When the pings fail, each failure is followed by a 1-second sleep. Then a reattempt occurs after each sleep twice on the Main connection, twice on the Auxiliary connection, and twice again on the Main connection. After all pings fail, a switchover is attempted (approximately 30 seconds from the first ping transmission). The 30 seconds is the timeframe shown in the logging example above.

IP ping

In Interaction Director Switchover systems, Interaction Processor (IP) is monitored instead of TS.

The Interaction Director Server install automatically creates the following server parameters to set up an IP ping process in Interaction Director configurations. This is similar to the TS ping process in CIC configurations. You should review these server parameters in Interaction Administrator on the Interaction Director server to confirm these settings.

- **Switchover Monitoring**: The parameter is set to IP to allow IP to be monitored instead of TS. The default value is TsServer.
- **Switchover IP Timeout**: When monitoring IP, this server parameter has the same functionality as the **Switchover TS Timeout** server parameter.
- **Switchover IP Retry Delay**: When monitoring IP, this server parameter has the same functionality as **Switchover TS Retry Delay**.

Switchover system architecture

Whenever the Switchover system starts on the backup server, it first establishes a Notifier connection to the active server. It then runs a recursive compare-and-update algorithm to determine whether there are differences between the DSServer registry structures on both servers. Finally, it updates the backup server, if necessary, to synchronize the servers using DS notifications.

Note:
Genesys recommends that you back up the registry as a part of performing regular server backups. You can also back up the server's configuration using Interaction Migrator. For more information, see *Data Backup Technical Reference* and *Interaction Migrator Technical Reference* in the PureConnect Documentation Library.

Note:
The active server name is replicated and used for both servers to optimize the synchronization process. The site names for both the active server and the backup server appear in the DS tree and in Interaction Administrator. These names stay the same.

Switchover system components

The following table shows the Switchover system components.

Component	Description
`SwitchoverU.exe`	This is a CIC server subsystem that monitors the mirror server and signals the virtual switch to switch servers.
`SwitchoverCtrlU.exe`	This is the CIC client GUI module that monitors the state of the Switchover system and provides a manual Switchover command.

Switchover states

When the primary and backup servers are on the same release and running in "auto-switch" mode, this condition is called the **Active** state. When the backup server is running in "manual switch only" mode because it is on a different release than the primary server, it is in the **Upgrade** state. The **Upgrade** state has two secondary states:

- The **Upgrade Higher** state is when the backup server is on a newer release than the primary server.
- The **Upgrade Lower** state is when the backup server is on an older release than the primary server.

Both these **Upgrade** states provide limited replication. While in the **Upgrade Higher** or **Upgrade Lower** state, the backup server will not automatically become the active server in the event that the primary server experiences a failure. However, a manual switch can be performed which will manually transition the backup server into the primary state and demote the old primary server into a failed state.

For more information, see the following topics:

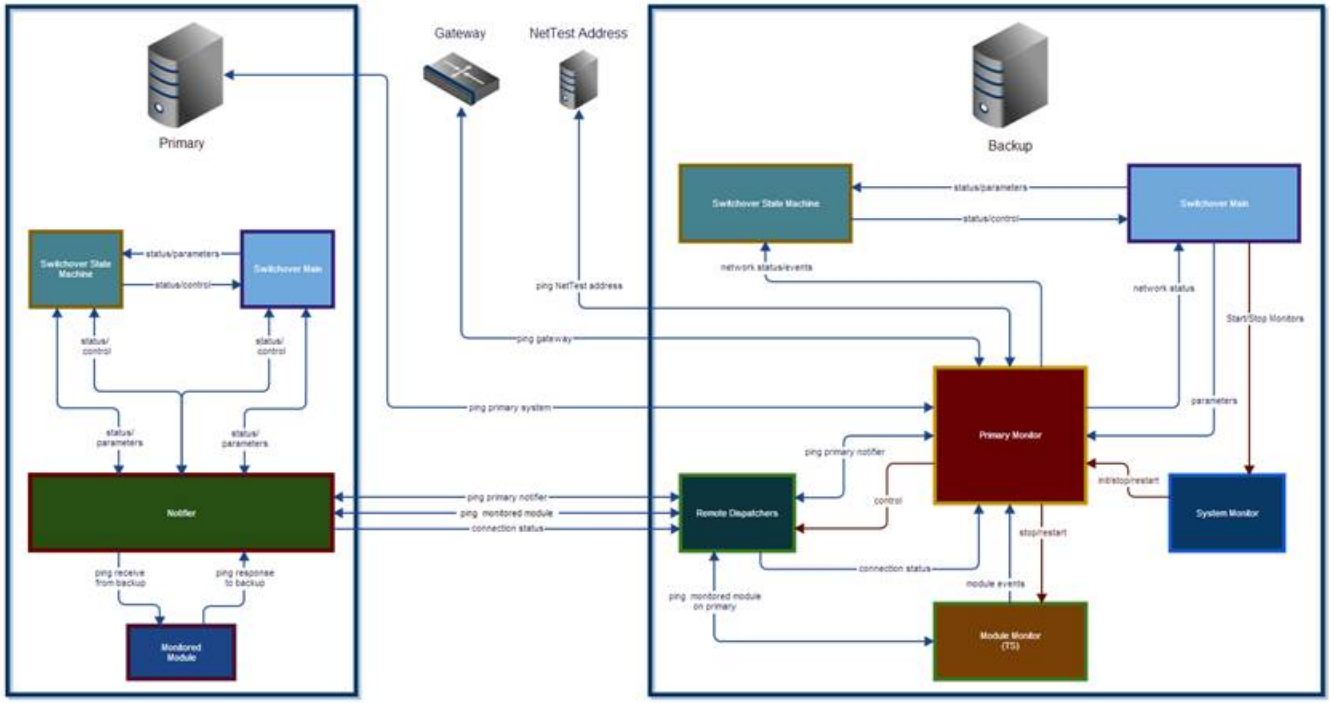
- The Switchover Control Panel
- Appendix B: Applying a release to switchover servers
- Appendix C: About the limited replication of data during an Upgrade state

Switchover Subsystem Components

The switchover subsystem consists of the following components:

- Switchover State Machine
  - Maintains state information
  - Processes events from several sources
- Switchover Main
  - Handles common tasks
  - Prepares for entering various switchover modes
- System Monitor
  - Loads and starts the primary monitor and the module monitor
- Remote Dispatchers
  - Conduits for establishing, monitoring, and using notifier connections to the primary
  - Posts events on transactions of the connections such as establishment and loss
  - Provides notifications that are integral to the switchover state machine's ability to detect connection status in real time
- Module Monitor
  - Sends routine pings to the module being monitored on the primary
- Primary Monitor
  - Is the central component for the backup
  - Sends routine pings to the notifier on the primary as a means of determining its status
  - Determines the status of the network connections and the primary server
  - Stops and restarts the module monitor when detecting the network status
  - Provides methods for determining network connection status to Switchover Main and the switchover state machine
  - Acts as the single provider for network and connection analysis

The following diagram illustrates the Switchover Subsystem components on the primary and backup installations.



The Switchover State Machine

The switchover state machine provides the various modes of operation for switchover. There are several states that switchover routinely executes. The backup and reconnecting states are affected by the optimizations that were made in CIC 2015 R1 to improve connectivity management.

When switchover is running in the primary state, it operates as the primary. Likewise, when the switchover state machine runs the backup state, it operates as the backup.

When the switchover state machine runs as the backup, and connection or module issues are detected, the Switchover system transitions to the reconnecting state in order to take specific steps to reconnect to the primary. During reconnection, the Switchover system transitions between the backup and reconnecting state depending on the conditions encountered.

Note:
The transitions to the backup state during reconnection do not indicate that the backup server has returned to operating as the backup. Transitioning between the reconnecting and backup states is normal when the backup is attempting to re-establish communications and resume normal operations.

The state machine on the backup will transition to the primary state and begin operations as the primary when any of the following occur:

1. The maximum number of reconnect attempts has been made.
2. The monitored module is determined to be down.
3. The primary is determined to be unreachable.
4. The reconnect interval has expired.

If reconnection succeeds or the monitored module is responding (in the case where reconnect was entered because the monitored module did not respond), the Switchover system will return to the backup state and performs a re-synchronization.

By default, the Switchover system will not attempt to determine if the primary is reachable when evaluating connection status. This is done to maintain legacy behavior that does not test whether the primary is reachable. You can set the following server parameters to specify the interval and the number times that the backup will try to reach the primary before deciding that it is unreachable.

- Switchover Unreachable Primary Ping Delay
- Switchover Unreachable Primary Ping Count

For more information on these server parameters, see "Switchover Server parameters".

System Monitors

There are two types of monitors used by the backup:

- The **primary monitor** handles the bulk of the connection management and status detection.
- The **module monitor** maintains contact with the monitored module running on the primary.

Primary Monitor

Purpose

The purpose of the primary monitor is to:

- Continually ping the notifier connections to the primary
- Process events from the module monitor
- Verify that the module monitor is running
- Provide diagnostics of the remote notifier connections
- Determine the network connection status of the backup
- Determine the network connection status to the primary

Responsibilities

The primary monitor continually monitors the main and auxiliary remote notifier connections to the primary by sending pings to the notifier on the primary. If any of the pings timeout or are otherwise not acknowledged, the primary monitor starts to diagnose the state of the network and connections. It posts events to the switchover state machine if there are issues with the connections or the network.

It also receives notifications from the module monitor that routinely pings the module being monitored on the primary. The module monitor will monitor the TsServer module or the IP module depending on the type of installation. The TsServer module is typically the module being monitored in a PureConnect Cloud environment.

Note:
In this document, the term *module* refers to either of the modules.

The primary monitor tracks the time between events received from the module monitor. It does this in order to provide verification that the module monitor has not stopped for an unintended reason. When any event is received from the module monitor, the primary monitor resets the internal value that tracks the time of the last event. The state machine will poll the primary monitor at regular intervals to get the status of the module monitor. When the primary monitor receives this poll request from the state machine, it calculates the amount of time since the last module monitor event and determines if the duration is past the maximum allowed. The calculation of the maximum event interval is internal and based on the frequency of the pings sent by the module monitor to the primary. The primary monitor suspends tracking the intervals between module monitor events when reconnecting and resumes it when the connections are re-established.

If the module monitor indicates that the module is down, meaning that the module monitor exhausted its number of retries, the primary monitor will evaluate the network and connections.

When the primary monitor detects that there are issues with the network or connections, it will stop the module monitor in order to avoid receiving continual notifications from the module monitor and to prevent the module monitor from causing a switchover event before the primary monitor has been able to analyze the situation.

The primary monitor is only used on the backup.

Startup

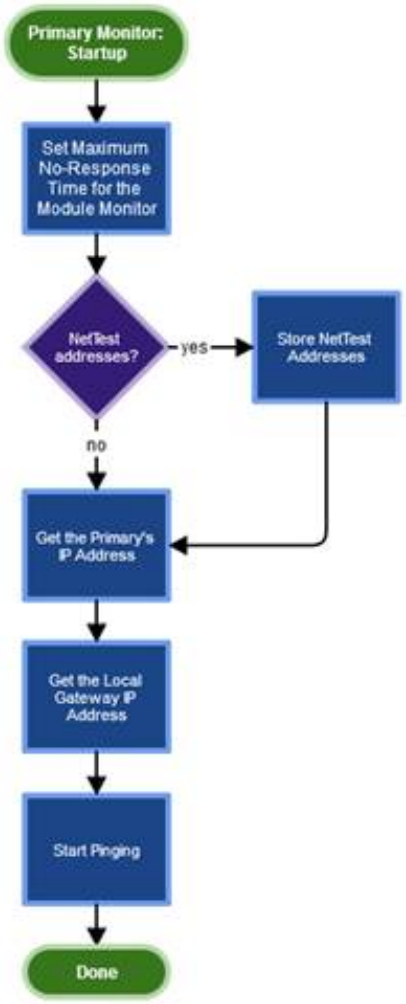
The primary monitor is started by the system monitor (SysMonitor2), which passes the service parameters queried during switchovers initialization as a backup. The parameters include:

- Timeout, delays, and ping counts
- The name of the module being monitored
- The name of the primary
- A callback into the system monitor
- The list of NetTest addresses, if configured

During startup, the primary monitor queries the system to obtain the local gateway addresses of the backup. It uses standard Windows APIs to query information about all network adapters. Each adapter query returns the interface and gateway addresses. An adapter may have no gateway address, a single gateway address, or multiple gateway addresses. The primary monitor will store all gateway addresses returned and ping each one when determining network connectivity of the backup. Local host or "empty" addresses are excluded from the list.

The primary monitor will also attempt to get the address of the server that the primary is running on. It uses this address to test if the primary's server is reachable. If the address cannot be retrieved during startup, the primary monitor will try to get it when checking the network connectivity.

The following diagram shows the startup process.



How the Primary Monitor Determines the Status of the Network and the Connection

When the primary monitor does not receive a ping reply from the notifier on the primary, it checks the following to detect the location of the problem:

- Status of the remote notifier connection
- Network status of the backup
- Network status of the primary

Detecting Status of the Remote Notifier Connections

The primary monitor first examines both of the remote notifier connections. Determining the status of either connection is made by checking its "connected" state directly. Notifier on the backup maintains state information on each connection and the primary monitor (as well as any other switchover component) can check the current status of any connection. The "connected" state value is used to evaluate if either connection is up or down.

If either connection is up, the primary monitor attempts to use them to check the status of notifier on the primary. If a closed connection is not re-established or if a connection was up and then goes down, the primary monitor then examines the network.

Detecting Network Connection Status of the Backup and Primary

To identify where there is a network issue, the primary monitor attempts the following steps:

1. First, the primary monitor pings NetTest addresses (if configured).
2. Next, the primary monitor pings the backup's local gateway (if enabled in the configuration).
3. Throughout the entire process, the primary monitor pings the server that the primary is running on (not any CIC products).

The primary monitor pings the local gateway to determine if the backup is still connected to the network. There can be multiple gateways configured for each adapter on the backup. During startup, the primary monitor attempts to enumerate all of the gateways for the adapters on the backup. The primary monitor stores all gateway addresses to use when pinging. Pinging the backup's gateway is optional; by default, it is disabled. To enable the gateway ping, set the **Switchover Disable Gateway Ping** server parameter to "No" or "0". To disable the gateway ping, set the parameter to "Yes" or "1". If you do not set the parameter, the gateway ping is disabled because some gateways block responses to pings (ICMP echoes) as a matter of security. If gateway pings are enabled and the primary monitor attempts to ping the primary's server but ping replies are blocked by the gateway, the primary monitor receives a false positive that the backup is not connected to the network. It is important to disable the primary monitor's gateway pinging if the gateway does not allow ping responses because there is no way for the primary monitor to know how the gateway is configured. However, gateway pinging is extremely valuable in determining the network connection state of the backup. If the backup's gateway responds to pings on the local network, it is strongly suggested that the backup be configured to enable gateway pinging. It is not unreasonable for the backup's gateway to respond to local pings since the backup should be on a private network.

The steps to check the network connections are taken in the following order based on the configuration of switchover on the backup. Once any step is taken, detection of the backup's network connection status is halted and no further steps are taken.

The steps to check the network connections are taken in the following order based on the configuration of switchover on the backup. Once any step is taken, detection of the backup's network connection status is halted and no further steps are taken. The steps are:

- **Gateway pings are enabled**: The primary monitor determines the backup's network connection status based on the result of pinging each gateway address. The primary monitor stops pinging the gateway addresses once a response is received or all addresses have been pinged without a response. At this point, the primary monitor stops checking the network condition and sets the network status.
  - Ping each gateway address until:
    - A ping response is received from the gateway, the network connection status is set to "Gateway Reached", and the backup's network connection is good.
    - All gateway addresses have been pinged and no responses were received, the network connection status is set to "Gateway Unreachable" and the backup's network connection is not good.
  - Network connection evaluation is stopped by the primary monitor.
- **NetTest addresses are configured**: The primary monitor makes a determination of the backup's network connection status based on the result of pinging each NetTest address. The primary monitor stops pinging the NetTest addresses once a response is received or all addresses have been pinged without a response. At this point, the primary monitor stops checking the network condition and sets the network status.
  - Ping each NetTest address until:
    - A ping response is received from a NetTest address, the network connection status is set to "NetTest Reached", and the backup's network connection is good.
    - All NetTest addresses have been pinged and no responses were received, the network connection status is set to "NetTest Unreachable", and the backup's network connection is not good.
  - Network connection evaluation is stopped by the primary monitor.
- **Ping the address of the primary's server**: The primary monitor stores the address of the primary's server during startup. If it was not able to get the primary server's address, it attempts to do so in this step. This is a standard ICMP echo sent to the IP address of the primary and is independent of any CIC application. This ping is used by the primary monitor to detect if the server running the primary is reachable.
  - If the primary server's address is not stored and the primary monitor is able to get it, ping the primary's server address and if:
    - A ping response *is received* from the primary's server address, the network connection status is set to "Primary Reached" and the backup's network connection is good. This indicates that there is an issue with the primary (CIC).
    - A ping response *is not received* from the primary's server address, the network connection status is set to "Primary Unreachable" and the backup's network connection is not good.
      - This indicates one or both of the following conditions:
        - There is a connection issue between the backup's network and the primary's network (when they're on separate networks such as in the case of a WAN configuration).
        - The primary's server is down.
      - When this happens, the primary monitor cannot determine if any of the primary's components have failed and will do one of two things:
        - Wait for a period of time or indefinitely (depending on the configuration parameters) for the primary to become reachable again.
        - Immediately switchover to become the primary.
      - The action taken when the primary is unreachable can be selected using server parameters. The default is to switch over immediately. For more information on the **Unreachable Primary Ping Count** and **Switchover Unreachable Primary Ping Delay** parameters, see "Switchover Server parameters". (The **Switchover Unreachable Primary Ping Delay** parameter is used to select immediate switchover, timed switchover, or no switchover if the primary is not reachable.)
  - Network connection evaluation is stopped by the primary monitor.

The action taken when the primary is unreachable can be selected using server parameters. The default is to switch over immediately. For more information on **the Unreachable Primary Ping Count** and **Switchover Unreachable Primary Ping Delay** parameters, see

"Switchover Server parameters". (The delay parameter is used to select immediate switchover, timed switchover, or no switchover if the primary is not reachable.)

If there is a connection issue and any of the following conditions exist:

- The primary is reachable
- The server parameters aren't configured to switch over immediately when the primary is unreachable
- Pinging the gateway is disabled

The following actions are taken:

1. The primary monitor stops the module monitor.
2. The switchover state machine enters the reconnect state.
3. A timer is scheduled that, upon execution, posts an event to the switchover state machine to initiate a switchover. This timer interval is the maximum amount of time that the Switchover system tries to reconnect to the primary before initiating a switchover. This value is set with the **Switchover Reconnect Timeout** server parameter. For more information, see "Switchover Server parameters".
4. The switchover state machine attempts to restore the connections to the primary.

If the module monitor has notified the primary monitor that it cannot communicate with the monitored module, the primary monitor takes steps to examine the network and remote notifier connections as outlined above. If they are good, it indicates that the monitored module is down. In this case, the primary monitor posts an event to the switchover state machine, which initiates a switchover.

Network Status versus Connection Status

Network and connection status are determined by the primary monitor, as described previously. They are distinct and defined, in terms of switchover, as:

- **Network Status**: The status of the physical network connection for the server running switchover in the backup state. It is independent of any switchover or CIC applications.
- **Connection Status**: The status of the both of the notifier connections between the backup and the primary. It is reflective of the network status since it depends on the physical network connection.

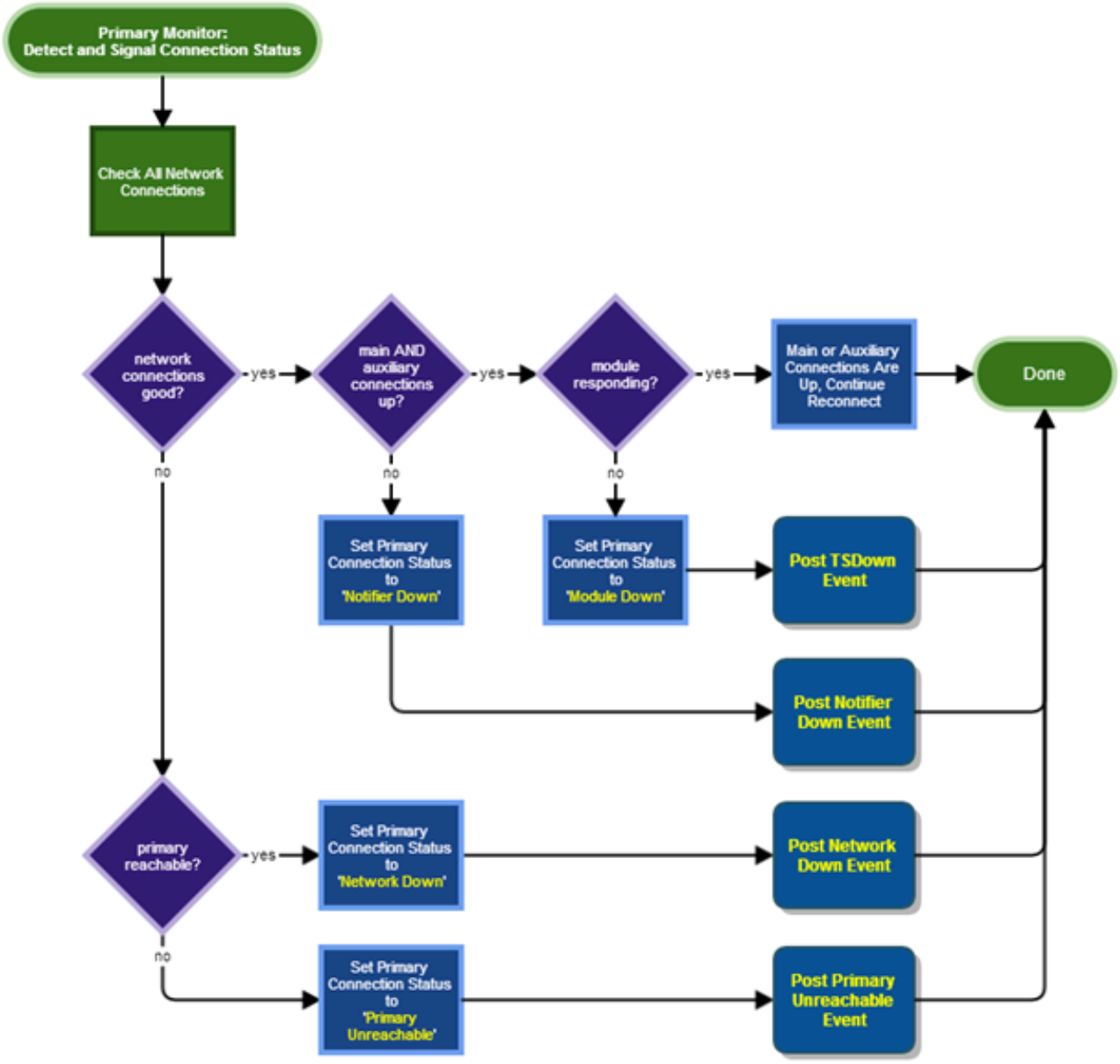
Whenever the primary monitor attempts to assess whether communications can occur between the backup and primary, the physical network connection is the mitigating factor; without the network connection, the notifier connections are unavailable. If the network connection is available, then the connection status provides further information about the state of the notifier connections. The connection status is one of the following:

- Both connections are up.
- The main connection is up (auxiliary connection is down).
- The auxiliary connection is up (main connection is down).
- Both connections are down.

Detection of the connection status includes:

- Checking the network connections
- Checking the main and auxiliary connections
- Determining if the primary's server is reachable
- Checking for no-response condition from the monitored module

If the network connection is good, the connections are checked. When the connections are up, the monitor's response status is evaluated. The primary reachable status is examined if there is an issue with the network connections to determine if there's a general network problem or just the path to the primary's server. Depending on the results of all of these checks, an event may be posted to the state machine indicating a condition that requires further reconnect processing. The diagram below illustrates the logic that determines the overall connection status.



Note that the primary is reachable even if the network connections are not good. This is because the definition of a "good" network connection includes whether or not the primary's server is reachable. If it is not, the network connection's status is "primary unreachable" and this is not a "good" condition.

This processing occurs when the primary monitor detects that it did not receive a ping from the notifier on the primary within the allotted amount of time or it detected a connection loss. When that happens, the primary monitor uses this logic to make a preliminary decision about what to do next. You can see in the backup state diagram how these events are handled. In the case of a "primary unreachable" determination, the state machine transitions to the reconnect state and tries to restore connections with the primary.

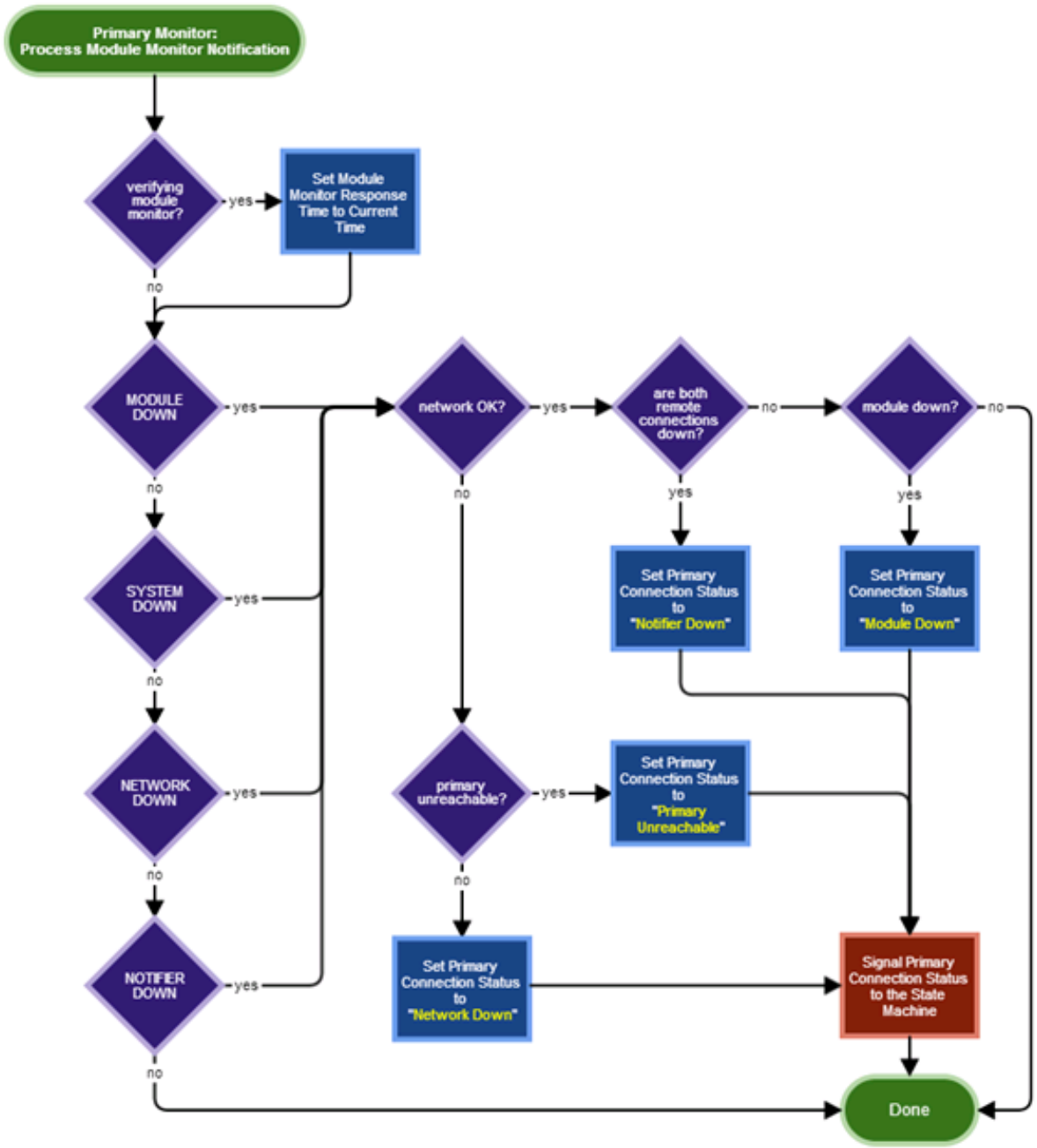
Handling Module Monitor Notifications

The primary monitor receives all notifications from the monitor module. If a notification indicates an issue with the module, network, or connections, then the primary monitor posts an event to the state machine, if required. The primary monitor can then make one of the following determinations:

- Network NOT OK:
  - **Primary Reachable**: The server running the primary can be reached, so the remote notifier is down.
  - **Primary Unreachable**: The server running the primary cannot be pinged, so the primary is unreachable.
- Network OK:
  - **Both Connections Down**: The main and auxiliary remote connections are down and the primary can be reached so the remote notifier is down.

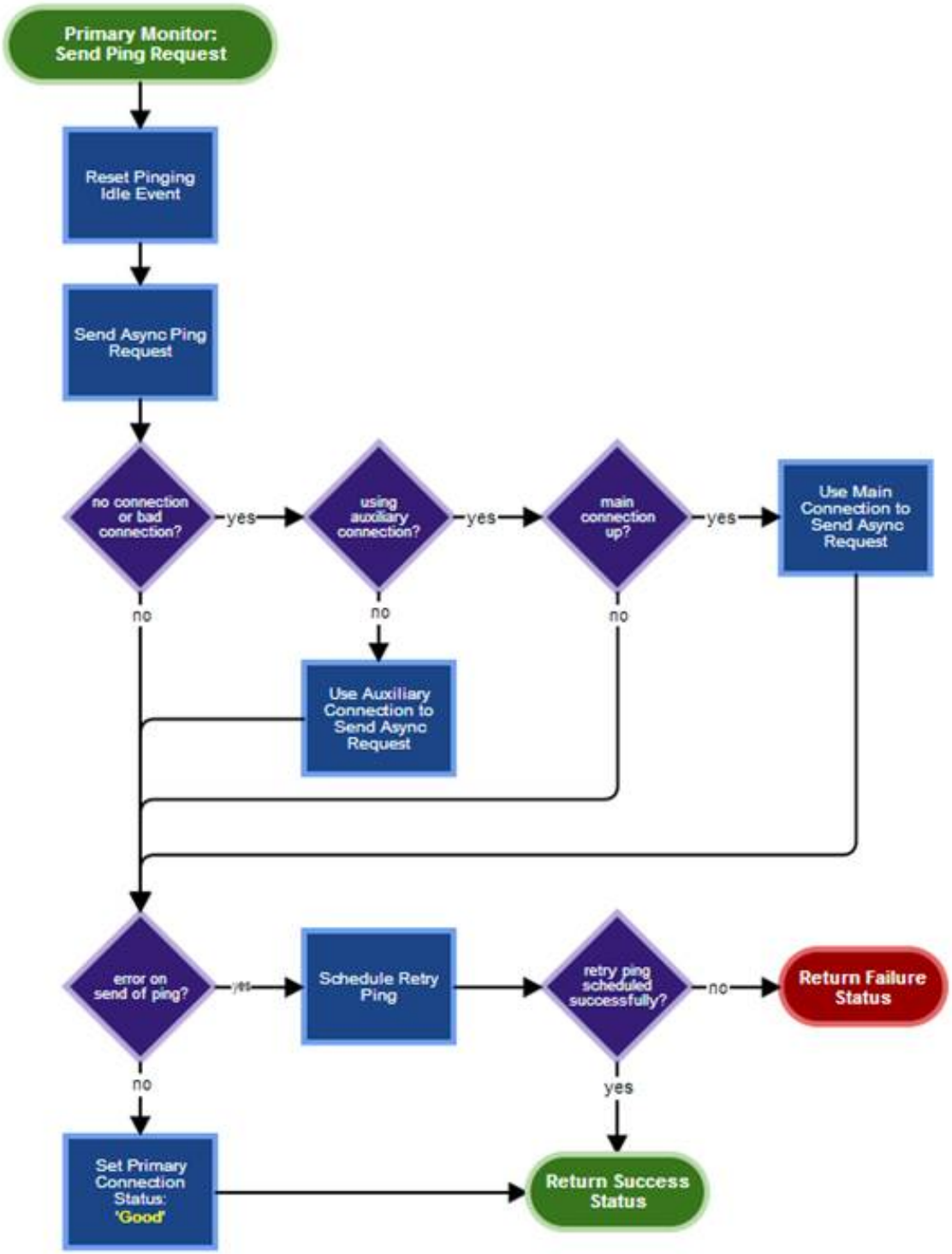
- **Both Connections Up**:
  - The Module is Down: The module cannot be pinged so the module is down.
  - The Module is Up: The module monitor indicated that the module was down but subsequent pings were answered so the module is considered to be up and there is no error.

The following flowchart illustrates this decision-making process.



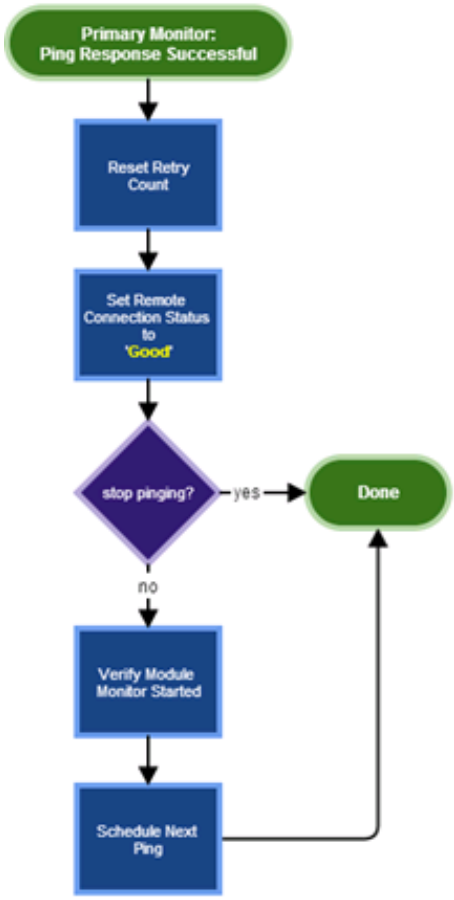
Sending Ping Requests

The primary monitor sends ping requests to the notifier on the primary at the specified ping delay interval. The primary monitor schedules a callback whose timeout is the ping delay interval. During that callback, a request is sent to the remote notifier which acts like a network ping except that the response is from the remote notifier itself.



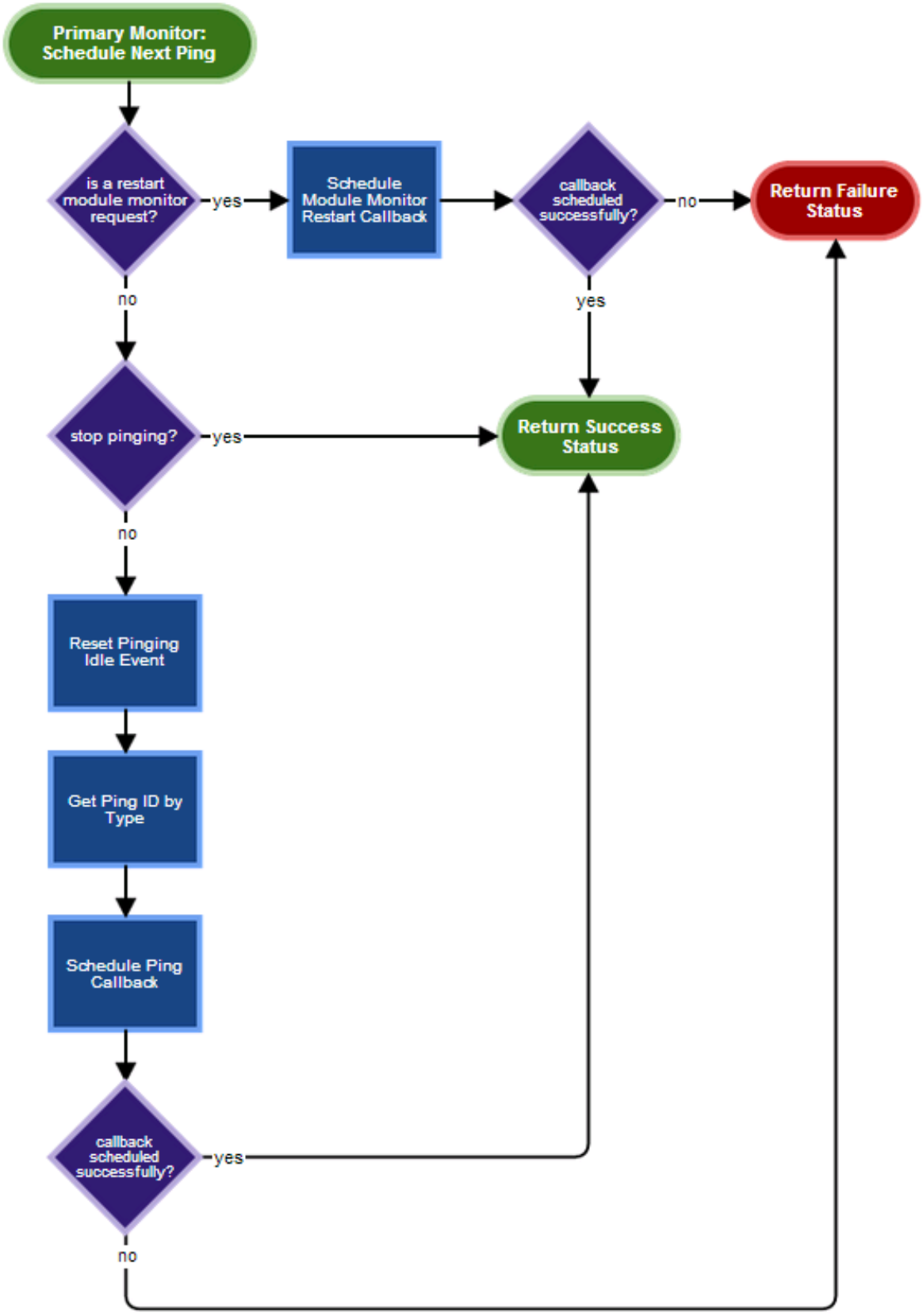
Successful Ping Response

A successful ping response occurs when the notifier on the primary sends a response within the timeout specified in the ping request. An asynchronous ping request callback of the primary monitor is called when the response is received successfully and before the timeout. The retry count is reset when a successful ping response is retrieved and the next ping is scheduled.



After a ping has been received successfully, another ping request callback is scheduled to send the next ping after the required delay.

The primary monitor method that schedules the next ping also acts as a receiver for requests to asynchronously restart the module monitor. There are conditions where the primary monitor cannot synchronously restart the module monitor. In those cases, a request is scheduled and this method will identify those requests and restart the module monitor. The method performs no other processing after the restart.



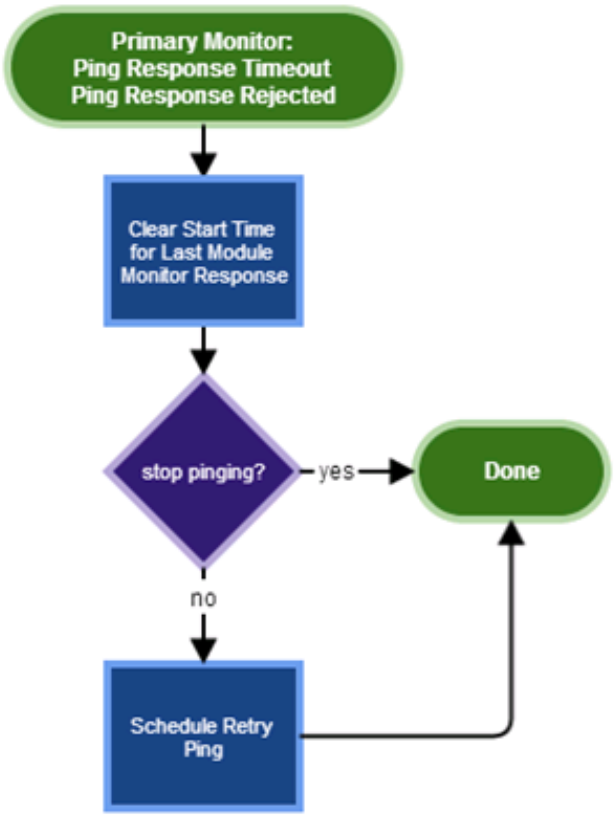
Non-Successful Ping Responses

Other responses are considered to be non-successful and appropriate action is taken if applicable. There are callbacks for each of the unsuccessful responses:

- **Timeout**: This response represents the potential loss of a remote notifier connection or an issue with the notifier on the primary.

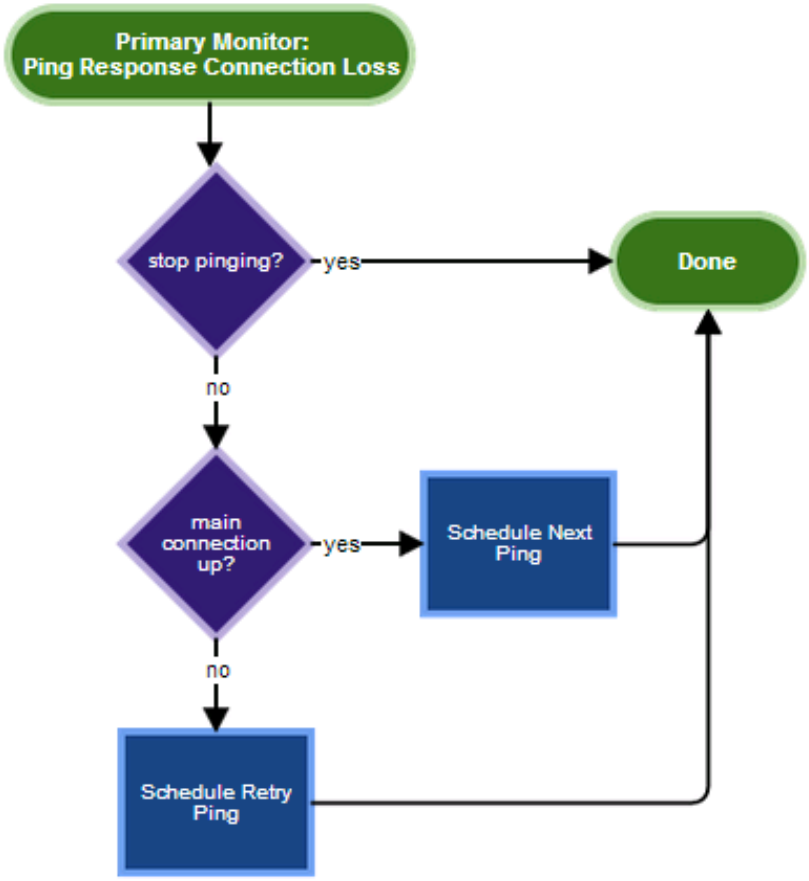
It triggers the retry logic that begins the process of sending retry pings.

- **Rejected**: Similar to the timeout response. The diagram below represents both the timeout and rejected response handling.



- **Connection Loss**: This response represents the potential loss of a connection to the notifier on the primary or an issue with the notifier on the primary.
  - If the main connection is up, this response could indicate that the auxiliary connection went down or there was a momentary drop of the main connection but it was recovered. In this case, a standard ping is sent.
  - If the main connection is down, the primary monitor treats this as a potential reconnect condition and sends a retry ping.

  The following diagram illustrates how this response is handled.



- **Cancelled**: No operations are performed upon receipt of this response because the primary monitor will cancel any outstanding pings when it is stopping (which generates this response).

A retry ping is sent for an unsuccessful response. If the retry count has reached the maximum, no retry ping is sent and error processing starts to diagnose the state of the local network and remote connections to the primary.

Module Monitor

Responsibilities

The module monitor is responsible for monitoring the selected module on the primary. In most cases, TsServer is the module monitored. However, there are some configurations that monitor IP.

> **Note:**
> For the purposes of this document, the term *module* refers to either the TsServer or IP because the Switchover system does not distinguish between any module. It just stores the module's name.

Functionality Provided

The module monitor provides a mechanism to determine if the module is still operating on the primary. The definition of "operating" is that the module responds to the pings transmitted by the module monitor.

The module monitor sends pings at a specific interval to the monitored module on the primary. If there is no a response to a ping, the module monitor begins its retry logic that sends additional pings to the module. If all of the retry pings fail, the module monitor sends a notification to the primary monitor.

Changes from Previous Implementation

In previous implementations, the module monitor made its requests using only the main connection. This design modifies the module monitor to attempt to use the auxiliary connection if the ping was sent on the main connection and no response was received within

the expected time interval. The purpose is to determine whether the module can be reached on the auxiliary connection in the event the main connection is down. This is to help determine if the module is down or if there is a notifier connection issue.

Startup

The module monitor is started during the initialization of switchover on the backup. The SysMonitor2 object loads the system monitor DLL and starts initialization of the monitor. If NetTest addresses are configured, they are passed along with the name of the monitored module to the routines that start the module monitor. A dedicated thread object is started that times out at the ping interval and calls the module monitor's ping routine.

Ping

The module monitor transmits a ping at the configured interval to the monitored module in its Ping method. The module sends its current process ID (PID) in a response ping to the module monitor. The module monitor extracts the PID from the response and stores it to the module PIDs over time to determine if the module has been restarted. Each execution of the module will have a unique PID on the primary server.

By default, the module monitor pings the module via the main notifier connection that switchover (the backup) established when it started.

- If the number of unsuccessful ping responses reaches the maximum error count, it resets the error count. The module monitor continues pinging on the auxiliary connection.
- If a successful ping is received without reaching the maximum error count, it resets the error count to zero. The module monitor resumes using the main connection.
- If the ping response failure count reaches the maximum error count while using the auxiliary connection, the module monitor reverts its configuration back to use the main connection the next time it pings the module. It posts a MODULE_DOWN event.

The purpose of the transition to the auxiliary connection is to further diagnose the cause of the ping failures. In most cases, when the main connection is down, the auxiliary is down as well. If the issue is only with the main connection, the use of the auxiliary is successful and the module monitor averts a false determination that the module is down. This provides an additional level of redundancy when supervising the module on the primary.

The module monitor determines that the module has been restarted when the PID from the latest response does not match the last PID received and the last PID is not zero (it is not the first ping response). There is a defined window during which the PIDs can vary without causing a switchover. If the PIDs have changed more than allowed within this time, the module is restarting too frequently, which indicates an issue with the module. In this case, the error count is set to the maximum.

The Ping method of the module monitor returns an integer value to the thread object that it is called from. The Ping method's return value indicates the result of the ping:

- A return value of 0 indicates that the ping was successful or the message to the module was rejected since the state of the module cannot be determined in this case.
- A non-zero return value is the number of ping errors that occurred and indicates that a retry callback is required.

The return value also determines how the thread object schedules the next invocation of the Ping method:

- A return value of 0 causes the thread object to schedule another callback at the normal ping interval.
- A non-zero value causes the thread object to schedule a callback at the retry interval.

A response error occurs when the ping response has not been received in the configured ping interval (the thread timed out and there is no message) or the ping response is empty (no PID information). The error count is incremented and, if the count has reached the maximum error count, the connection in use is checked. If the module monitor is using the main connection, it resets the error count and will use the auxiliary connection.

The monitor posts a `SYSTEM_OK` event when the ping response is received successfully and the module is not restarting too frequently. It posts the `MODULE_DOWN` event when:

- The maximum sequential restart count has been reached.
- The maximum restart count has been reached.
- The maximum number of response errors have occurred (for example, it timed out when waiting for a ping response) AND it is currently using the auxiliary connection.

UDP Monitor

As of 2015 R1, The UDP monitor is no longer used in switchover. Its functionality is not required with the introduction of the primary monitor. Existing parameters for the UDP monitor are ignored and have no effect.

State Machine Events and Handling

This section covers the most common switchover states.

Primary State

The primary state provides all the logic for switchover when it runs as the primary.

Backup State

Running in the backup state, switchover pings notifier on the primary, monitors the main and auxiliary connections, and supervises the monitored module as described already. It processes a number of conditions in addition to status of the primary. Besides going to the primary state on either a manual or automatic switchover or the reconnecting state, it can also transition to the shutdown, error, or stopping state depending on the events detected.

How Primary Monitor Events are Processed in the Backup State

This section describes how the switchover Backup state handles the events from the primary monitor.

- **Network Down**
  The state machine goes to the Reconnecting State to attempt reconnection with the primary.
- **Module Down**
  1. If the backup is in manual switchover mode, the state machine goes to the stopping state and halts further processing.
  2. CIC is not starting up, so the backup switches to the Primary State and begins execution as the primary.
  3. CIC is starting up, so a switchover to the Primary State is scheduled and will occur after CIC has completed startup.
- **Notifier Down**
  1. If the network is down, the primary monitor and the module monitor are stopped and the state machine goes to the Reconnecting State.
  2. If the backup is in manual switchover mode, the state machine goes to the Reconnecting State.
  3. If both the main and auxiliary remote notifier connections are down, the primary monitor and the module monitor are stopped and the state machine goes to the Reconnecting State.
  4. The network is okay, backup is in automatic switchover mode, and at least one of the remote notifier connections is up, the primary monitor and the module monitor are stopped and the state machine goes to the Reconnecting State.
- **Primary Unreachable**
  The primary monitor and the module monitor are stopped, and the state machine goes to the Reconnecting State.

The state machine transitions to a state other than reconnecting only in the case of a `Module Down` event. If the primary monitor has analyzed the state of the network and connections to determine that there are not any other issues, the `Module Down` notification that the module monitor sent to the primary monitor indicates that the module is actually down. In that case, a switchover is required.

Reconnecting State

The reconnecting state is entered when the backup state detects an interruption with the notifier or networks connections or the monitored module does not respond to ping requests. Switchover transitions between the reconnecting and backup states when attempts to reconnect are underway.

Other States

There are other states of the switchover state machine. This section provides a brief synopsis of each.

The Init State

The Init state is the first state that switchover enters when it starts up. The main switchover object determines the service mode and posts an event to the state machine. The Init state receives the event and transitions to the appropriate state.

The Upgrade Higher State

The Upgrade Higher state is entered if the local release is higher than the remote version. It behaves like the backup state but with reduced functionality.

The Upgrade Lower State

The Upgrade Lower state is entered if the local release is lower than the remote release. It behaves like the backup state but with reduced functionality.

The Inactive State

The Inactive state is entered when switchover reaches a point where it is no longer actively processing events.

The Stopping State

The Stopping state is entered when switchover is shutting down.

The Error State

The Error state is entered when switchover has encountered an error condition.

Remote Notifier Connections

The remote notifier connections are established by switchover when it starts in the backup mode. The connections are maintained as long switchover is running. They are used to communicate with notifier on the primary.

Redundancy

There are two remote notifier connections established with notifier on the primary: the main connection and the auxiliary connection. The main connection is used for all communications by default. The auxiliary is used when there are issues with the main connection. The auxiliary is used to determine if communications with the remote notifier are still available in order to diagnose errors when using the main connection. The primary and module monitors utilize the auxiliary when they are unable to receive messages from the remote notifier on the main connection.

Behavior on Socket Closures

Socket closures typically result in the loss of connection with the remote notifier. Notifier on the backup attempts to reconnect to the primary when this happens as part of its recovery operations.

Recovery

The remote notifier connections are actively monitored. If a connection goes down, attempts are made establish it again. The state machine receives notifications that whenever the state of a connection changes. Actions taken by switchover in response to connection changes depend on the current state.

Recovery of ACD email, chat, and callback interactions during switchover

Starting in IC 4.0 SU 3, the Interaction Recovery Service subsystem supports recovery of email, chat, and callback interactions as described in the following sections. Before SU 3, those interactions, including any work in progress, were lost during a switchover. Email interactions were requeued as new interactions, chat users had to reconnect and be requeued to an agent, and callbacks were lost with no method for recovery.

The Interaction Recovery Service subsystem replicates the creation of interactions and processes them to take the appropriate action based on the interaction state. For example, interactions in a connected state on a user queue do not change and ACD automatically reprocesses interactions in an offering state on a workgroup queue.

Other subsystems use data from the Interaction Recovery Service subsystem to create and maintain mirrored interactions on the backup server.

Enable the Interaction Recovery Service

To enable the Interaction Recovery Service, open Interaction Administrator and then open the **Server Parameters** container. Add the parameter for each type of interaction that you want:

- **Mail Interaction Recovery Enabled**
- **Chat Interaction Recovery Enabled**
- **Callback Interaction Recovery Enabled**
- **SMS Interaction Recovery Enabled**

For more information on these server parameters, see "Optional Switchover Server parameters".

Recovery of email interactions

Previously following a switchover, email interactions were requeued as new interactions. Starting with IC 4.0 SU 3, the Interaction Recovery Service subsystem recovers email interactions with the following caveats:

- Email interactions generated by agents lose HTML formatting and convert to plain text. Any attachments are lost.
- Following the switchover, email interactions get new IDs.
- When a switchover occurs during the synchronization process, the interaction state could be lost.

The following table provides configuration information for the recovery of email interactions.

Enabled by default?	No. Requires a server parameter.
Server parameter	**Mail Interaction Recovery Enabled** This parameter must be set to 1. For more information, see "Optional Switchover Server parameters".
Requires a subsystem restart?	No. When the backup server starts or the parameter is enabled, the Interaction Recovery Service subsystem performs a full synchronization of email interactions with the active server.

Note:
For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions".

Recovery of chat interactions

Previously, following a switchover, chat users had to reconnect and wait for an agent. Starting with IC 4.0 SU 3, the Interaction Recovery Service subsystem recovers chat interactions with a transition that is almost seamless. Once switchover occurs, the WebProcessor subsystem prepares the mirrored interactions.

Note the following:

- Automatically generated status messages are lost after switchover. However, the switchover process replicates all of the other texts that are exchanged during the chat session.
- Files that were transferred during the chat session are not available after switchover.
- The switchover behavior of the CIC clients is the same as it was in switchovers before IC 4.0 SU 3.
- All chat responses typed during the switchover are maintained. They are not lost.

The following table provides configuration information for the recovery of chat interactions.

Enabled by default?	No. Requires a server parameter.
Server parameter	**Chat Interaction Recovery Enabled** Set this parameter to 1. For more information, see "Optional Switchover Server parameters".
Requires a subsystem restart?	Yes. Restart the WebProcessor subsystem on the active server and reboot the backup server. After the parameter is enabled and the backup server has restarted, the Interaction Recovery Service subsystem performs a full synchronization of chat interactions with the active server.

Note:
For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions".

Recovery of callback interactions

Previously, following a switchover, callback interactions were lost and not recoverable. Starting with IC 4.0 SU 3, the Interaction Recovery Service subsystem recovers callback interactions. Note the following:

- Recovery processing of callback interactions is similar to the recovery processing of chat interactions.
- The callback window temporarily disappears while the CIC client tries to reconnect.

The following table provides configuration information for the recovery of email interactions.

Enabled by default?	No. Requires a server parameter.
Server parameter	**Callback Interaction Recovery Enabled** This parameter must be set to 1 For more information, see "Optional Switchover Server parameters".
Requires a subsystem restart?	Yes. Restart the WebProcessor subsystem on the active server and reboot the backup server. After the parameter is enabled and the backup server has restarted, the Interaction Recovery Service subsystem performs a full synchronization of chat interactions with the active server.

Note:
For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions".

Recovery of SMS interactions

Previously, following a switchover, SMS users had to reconnect and wait for an agent. Starting with CIC 2016 R4, the Interaction Recovery Service subsystem recovers SMS interactions with a transition that is almost seamless. Once switchover occurs, the WebProcessor subsystem prepares the mirrored interactions.

Note the following:

- Automatically generated status messages are lost after switchover. However, the switchover process replicates all of the other texts that are exchanged during the SMS session.
- The switchover behavior of the CIC clients is the same as it was in switchovers before CIC 2016 R4.
- All SMS responses typed during the switchover are maintained. They are not lost.

The following table provides configuration information for the recovery of SMS interactions.

Enabled by default?	No. Requires a server parameter.
Server parameter	**SMS Interaction Recovery Enabled** Set this parameter to 1. For more information, see "Optional Switchover Server parameters".
Requires a subsystem restart?	Yes. Restart the WebProcessor subsystem on the active server and reboot the backup server. After the parameter is enabled and the backup server has restarted, the Interaction Recovery Service subsystem performs a full synchronization of SMS interactions with the active server.

Note:
For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions".
For information about why SMS chats may not be retained during a switchover even when this parameter is set, see "SMS chats are not retained during a switchover".
The recovery of SMS generic objects requires that you also configure the IonNotifier parameter. For information, see *Call Recovery Feature Technical Reference* in the PureConnect Documentation Library.

A note about the loss of duration information for interactions

When you enable the **Mail Interaction Recovery Enabled, Chat Interaction Recovery Enabled, or Callback Interaction Recovery Enabled** server parameter, every time an interaction is created on the active server, a corresponding "shadow" interaction is created on the backup server. If a switchover occurs, the interaction on the active server is automatically discarded. The "shadow" becomes the new active interaction. When you restore the switchover pair, the new backup automatically makes a new shadow interaction.

You may notice a discrepancy in the duration of the interaction if you look in IC Business Manager or at the Time in Queue value for the interaction.

The duration is the time that the interaction has existed, regardless of whether it is a shadow or active interaction. Because the second shadow was created after the first active and first shadow, the duration that the second shadow interaction has existed will be different than the original interaction and the first shadow. This is a known limitation of the switchover process.

Example of how loss of duration appears

1. Active1 and Shadow1 are created at 5 AM.
2. Switchover happens at 6 AM. Shadow1 becomes Active2.
3. Switchover pair is restored 7 AM. Shadow2 is created based on Active2.
4. Another switchover happens at 8 AM. Shadow2 becomes Active3.
5. Active3 duration is listed as 1 hour. Customer believes it should be 3 hours because the email originally came into the system 3 hours ago.

Recovery of statistical data

During normal processing, the primary server computers and caches statistical data which is saved into the database/PMQ periodically.The backup server does not receive any event so it does not have any statistical data. As a result, when a switchover occurs the primary server and the backup server have different statistics.

To address this, you can enable the Interaction Recovery Service. When the Interaction Recovery Service runs, the Statserver on the backup server receives the same event notifications as the primary server. Because the same event notifications are stored on both servers, the statistical data on both servers is valid.

Note:
In order for the Statserver to work, you must enable the Interaction Recovery Service. For information, see "Enable the Interaction Recovery Service".

Note:
The Interaction Recovery Service supports only emails, chats, and callbacks. Therefore statistical data can be generated only for these types of interactions. Statistical data for calls is not supported. For more information, see "Recovery of ACD email, chat, and callback interactions during switchover".

Location of log data

During normal operations, the primary server (Server A) sends its log data to the database. The backup server (Server B) sends its log data to a CSV file. When a switchover occurs, Server B becomes the primary server, it flushes log data collected before switchover to CSV file, then sends new log data to the database.

The timespans of the database records reflect the switchover. For example, suppose the standard duration of a database log record is 1800 seconds (30 minutes). However, a switchover occurs 15 minutes into the logging process. Instead of a single log record for 1800 seconds, there would be 2 log records, each for 900 seconds.

The CSV log files are stored in I3\IC\CSVLogs. The CSV file is automatically overwritten every week. To keep a backup copy of the file, copy it to a different location.

If disk space is a concern, you can stop the backup server from sending its log data to the CSV log file. To do this, add the **StatServer_DisableQPSLoggingOnBackup** parameter and set its value to **Yes**. You must restart the Statserver on the backup server in order for this parameter to take effect.

Note:
When a switchover occurs, the log data from Server B is automatically sent to the CSV log file, regardless of the setting of the **StatServer_DisableQPSLoggingOnBackup** parameter. Also, if the Interaction Recover Service is not enabled, no data is logged to the CSV file because the Statserver does not receive any notifications.

Tracker Server logging

Beginning in SU 5, the Tracker Server actively monitors email interactions, chat interactions, and callback interactions on both the primary server and the backup server in order to capture the interaction data. This interaction data is logged in the Interaction Summary table and the Interaction Segment Detail table. Because the Tracker Server logging is active on both the primary server and the backup server, CIC captures the full history of these interaction types.

Tracker Server logging

Beginning in SU 5, the Tracker Server actively monitors email interactions, chat interactions, and callback interactions on both the primary server and the backup server in order to capture the interaction data. This interaction data is logged in the Interaction Summary table and the Interaction Segment Detail table. Because the Tracker Server logging is active on both the primary server and the backup server, CIC captures the full history of these interaction types.

Tracker Server logging

Beginning in SU 5, the Tracker Server actively monitors email interactions, chat interactions, and callback interactions on both the primary server and the backup server in order to capture the interaction data. This interaction data is logged in the Interaction Summary table and the Interaction Segment Detail table. Because the Tracker Server logging is active on both the primary server and the backup server, CIC captures the full history of these interaction types.

Identifying recovered interactions in the database

The primary server and the backup server share the InteractionIdKey in the database. When spanned interaction data is logged to the database, the sequence number column (seqno) is incremented to 1 in the following tables: Interaction Summary, Interaction Segment Detail, and Interaction Wrapup. Interaction records with the sequence number of **1** are the recovered interactions that have been shared between the primary server and the backup server.

Installation and configuration

This section describes how to install and configure a new Switchover system.

Switchover licensing

CIC production licenses include the information for both servers in a switchover pair. This single license file can be applied to both machines. For information on how to generate, apply, and update your license file, see *PureConnect Licensing Technical Reference* in the PureConnect Documentation Library.

Switchover Server requirements

Before you install and configure a new CIC Switchover system, you must have two identically configured CIC servers. The CIC servers must be identical in every respect, including:

- An identical amount of RAM, disk space, number, and names of drives, and hard drive partitions
- Operating system software and service packs, including identical services running (for example, SNMP)
- All software (operating system and all applications, including the CIC server) must be on the same drives and use identical paths
- CIC product software release and update
- CIC administrator account name and password (for example, ICAdmin)
- CIC components and site names (the site name is case-sensitive)
- Application software, including email clients that use identical mailboxes
- On the same network, each CIC server needs at least one network card to communicate over the network
- Members of the same domain; a domain controller must be installed and configured to provide DNS and DHCP
- Immediate access to the same CIC resource files (for example, contact databases, report logs, and voice mail recordings) on any separate database and recording servers
- Regional settings (time zones)

Exception:
The two servers *must* have *different* machine names and IP addresses, because both servers remain accessible regardless of which is the active server and which server is the backup server.

If you have not already done so, fulfill CIC server requirements and pre-installation procedures on the servers you have designated as the initial active and backup servers. For more information, see *C"I"*C Server in C*IC Installation and Configuration Guide* in the PureConnect Documentation Library.

Server group secure connections with subsystems

CIC servers require SSL protocol-enabled connections and public/private key certificates for secure communication with remote subsystems such as Interaction Media Servers, ASR servers, CIC web servers, and Interaction Remote Content Service servers.

During the CIC server installation, the following files are created in the `\I3\IC\Certificates\ServerGroup` directory:

- A server group certificate authority (ServerGroupCertificate.cer) that issues certificates for all authorized remote subsystems.
- A server group private key (ServerGroupPrivateKey.bin). Tightly guard the private key on the local machine.
- A server group public key (ServerGroupPublicKey.bin). The public key is widely distributed. A message encrypted with the public key can be decrypted only with the corresponding private key.

If your company has already established its own root certificate authority and manages its own certificates, you can use your own server group certificate and private key. CIC provides certificate management tools for creating new certificates and installing your own certificates.

Important!
SwitchoverServer pairs must use identical server group certificate and private keys to connect remote subsystems successfully to both the active and backup servers. The server group certificate and private key are configured when you run IC Setup Assistant on the active and backup servers during a new or upgrade installation. See "Server group certificate and private key" for the specific procedures for securely synchronizing the server group certificate and private key on your active and backup servers.

For more information about CIC server and remote subsystem security and other PureConnect security features, see the *PureConnect Security Features Technical Reference* in the PureConnect Documentation Library.

Install CIC on the Switchover Server pair

This section describes how to perform a new CIC 2015 R1 or later installation on a Switchover Server pair.

Download and copy the CIC .iso to a file server

CIC releases are distributed as `.iso` files. We recommend that you store the CIC release `.iso` file on a file server to avoid having to copy the `.iso` file to multiple servers.

1. Download the latest CIC release `.iso` file from the PureConnect Product Information Download page at https://my.inin.com/products/Pages/Downloads.aspx.
2. Copy the `.iso` file to a file server (non-CIC server) with a high bandwidth connection to the server(s) onto which you will be running the CIC installs.
3. Mount the `.iso` and share the contents to make them accessible to those servers.

Install the initial active and backup servers

1. Make sure you have fulfilled the CIC server prerequisites as described in "CIC Server" in *PureConnect Installation and Configuration Guide*.
2. Run `Install.exe` to run the CIC Server install and other required installs on the **initial active server** as generally described in "CIC Server Installation" in *PureConnect Installation and Configuration Guide* and in "Switchover notes for the CIC Server install" in this document.

   `Install.exe` is an enhanced tool that simplifies and automates many aspects of the manual install and update process.

   > **Important!**
   > When `Install.exe` accesses the `\Installs` directory across a network share as recommended, the utility copies the installs to the server's local temp directory, then executes from there. Executing individual installs from a directory across a network share is not recommended.
3. When the CIC Server install on the **initial active server** completes, click the **Setup Assistant** button to launch IC Setup Assistant.
4. Run IC Setup Assistant on the **initial active server** as generally described in "IC Setup Assistant" in *PureConnect Installation and Configuration Guide* and in "Switchover notes for IC Setup Assistant" in this document.
5. When IC Setup Assistant on the **initial active server** completes, **do not restart the server**. Instead, choose **No, I will restart my computer later** and click **Finish**. This allows `Install.exe` to continue to install the other required installs on the initial active server.
6. When `Install.exe` completes, restart the **initial active server** to complete the CIC server installation and start CIC services.
7. Repeat steps 1 through 6 on the **initial backup** server.

Switchover notes for the CIC server install

When you run the CIC server install, select the same components and settings on both the initial active backup servers:

- Select the same admin user name in the **Domain User Validation** dialog box on the initial active and backup servers. However, the two servers *must* have different computer names and IP addresses. This is because the backup server is still accessible using TCP/IP while the active server is active, and the active server is still accessible using TCP/IP while the backup server is active.
- Select the same CIC server **Destination Folders** on the initial active and backup servers. These folders include the same **Install Directory** (default `\I3\IC`). The Switchover system requires that the CIC server be installed on the same drive and path on both the active server and the backup server. Remote subsystems cannot successfully connect to the switchover pair unless the `\I3\IC\Certificates\ServerGroup` directory is on the same drive and path on both servers.
- The CIC server installation contains no dialog boxes that are specific to the Switchover system.

Switchover notes for IC Setup Assistant

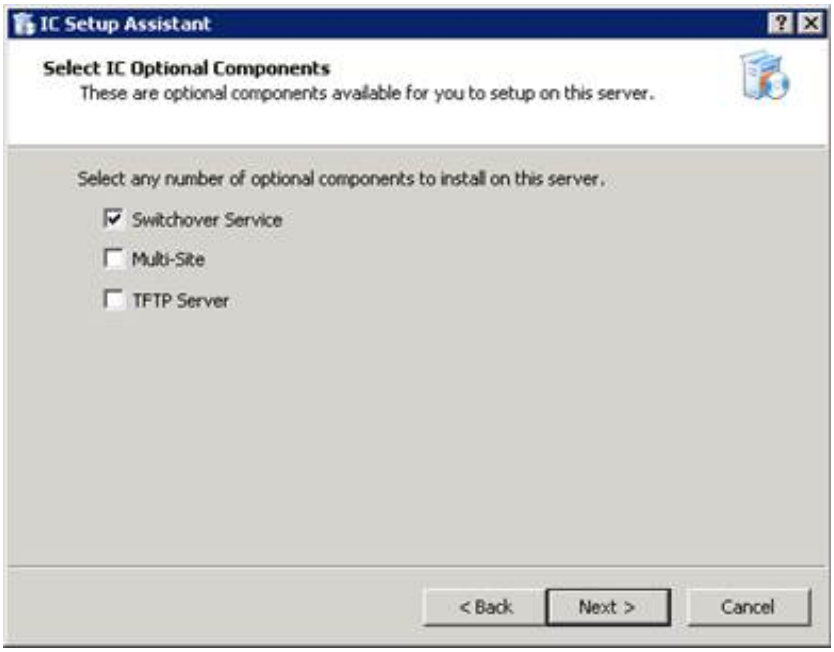
Make sure that you select the same configuration options on both the initial active and backup servers.

This section describes specific switchover-related configuration in IC Setup Assistant.

Note:
This section uses the terms "active server" and "backup server" synonymously with the terms "Switchover A" and "Switchover B." Both sets of terms refer to the servers you *intend to be* the initial active server and the initial backup server.

Select CIC optional components

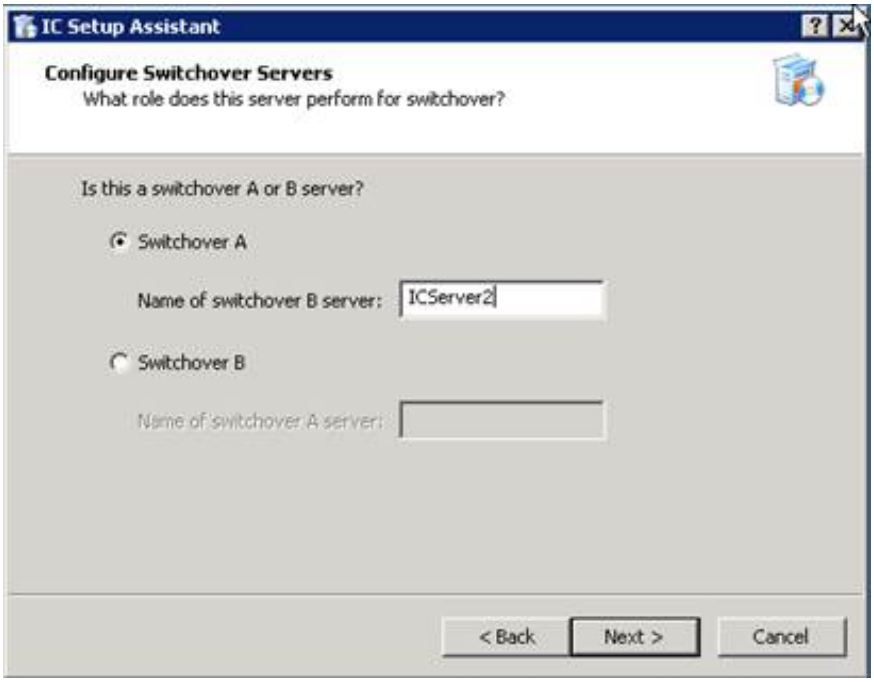
In the **IC Optional Components** dialog box, click **Switchover Service**.



Configure switchover servers

Configure the role this CIC server performs for switchover.

In this example, "ICServer1" is the *intended* initial active server or "Switchover A", and "ICServer2" is the *intended* initial backup server or "Switchover B."



To configure the active and backup servers, perform the following instructions.

Configure the active server

Switchover A

Select this option when you run Setup Assistant on the server you have determined to be the initial active server or "Switchover A" server (in this example, "ICServer1").

Name of switchover B server

Type the computer name of the initial backup server or "Switchover B" server. In this example, the computer name is "ICServer2."

Give the backup server a name that is different from the active server name. **Do not type the IP address or the fully qualified domain name.**

The entry in this box populates the required **SwitchoverServer B** server parameter in Interaction Administrator.

Configure the backup server

Switchover B

Select this option when you run Setup Assistant on the server you have determined to be the initial backup server or "Switchover B" server (in this example, "ICServer2").

Name of switchover A server

Type the computer name of the initial active server or "Switchover A" server. In this example, the computer name is "ICServer1."

Give the active server a name that is different from the backup server name. **Do not type the IP address or the fully qualified domain name.**

The entry in this box populates the required **SwitchoverServer A** server parameter in Interaction Administrator.

Confirm the SwitchoverServer configuration

After running IC Setup Assistant on the initial active and backup servers, configure the **SwitchoverServer A** and **B** server parameters as shown in the following example:

On ICServer1:

SwitchoverServer A = ICServer1

SwitchoverServer B = ICServer2

On ICServer2:

SwitchoverServer A = ICServer1

SwitchoverServer B = ICServer2

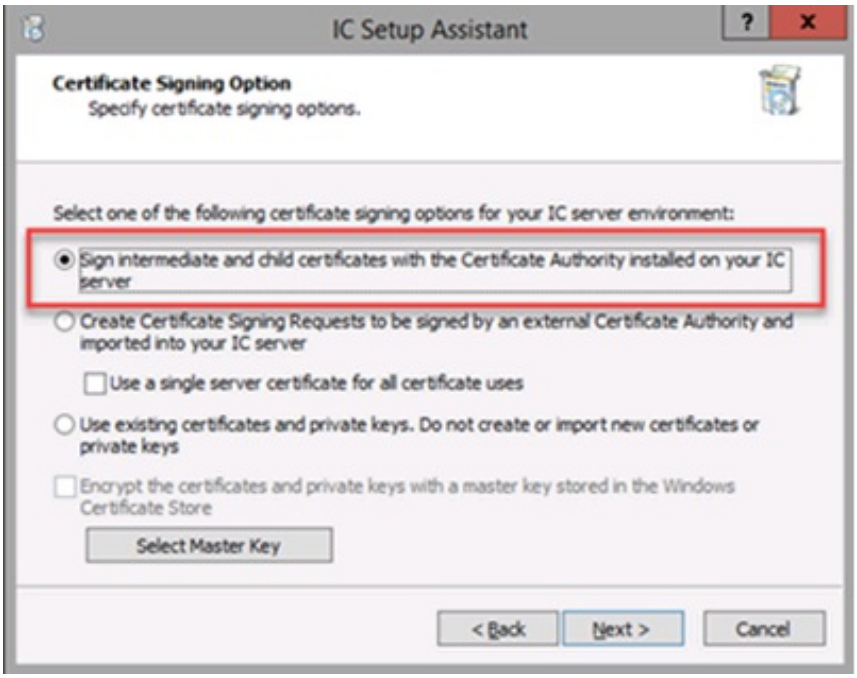
If the **SwitchoverServer A** and **B** server parameters are not set correctly, the Switchover system cannot determine which server is the active server and which one is the backup server. As a result, IC does not start successfully.

Server group certificate and private key

CIC servers require a server group certificate and private key for secure communications with remote subsystems such as ASR servers and web servers. During the CIC server installation, a server group certificate authority file and a server group private key file are automatically created in the `\I3\IC\Certificates\ServerGroup` directory on the CIC server.

Switchover pairs must use *identical* server group certificates and private keys to connect remote subsystems successfully to both the active server and the backup server.

From the **Certificate Signing Option** screen, select the first option **Sign intermediate and child certificates with Certificate Authority installed on your IC server**.

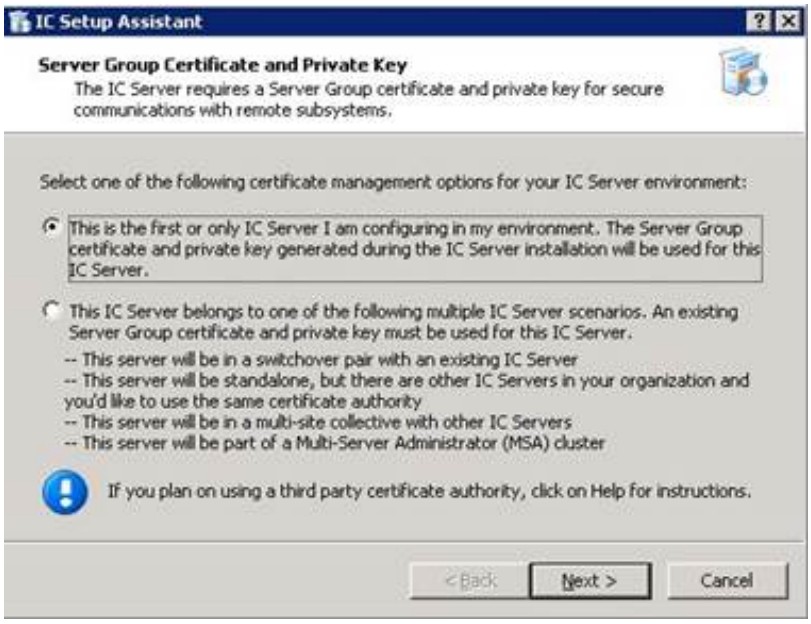


The **Server Group Certificate and Private Key** screen appears.

To configure the active server and the backup server for the server group certificate and private key, perform the following instructions.

Configure the initial active server

1. Select the **first option** if this CIC server is the initial active server. No further configuration is necessary. IC Setup Assistant uses the server group certificate and private key that you automatically generated during the CIC server installation.



> **Note:**
> If you plan to use a third-party certificate authority, do *not* select this option. Select the second option instead so you can securely copy your own server group certificate and private key files to the initial active server.

2. Click **Next** to continue with IC Setup Assistant.

Configure the initial backup server

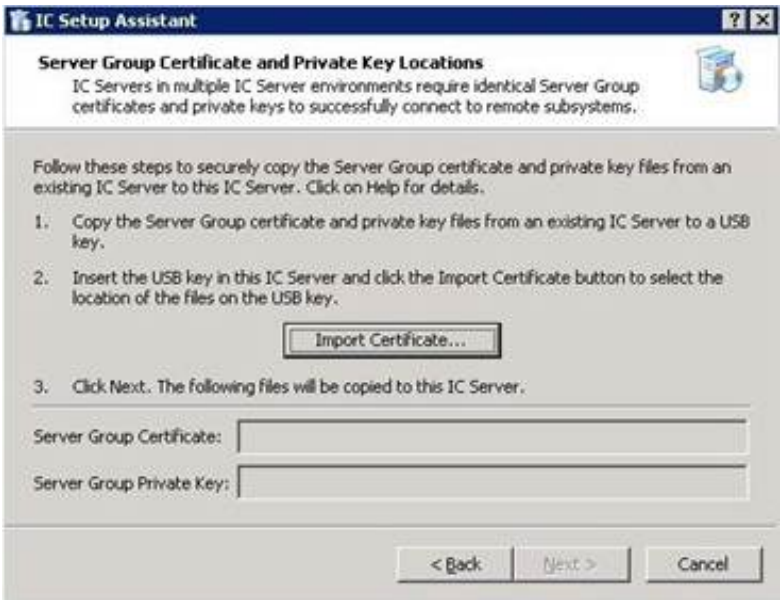
1. Select the second option if this CIC server is the initial backup server.

2. Click **Next**. Securely copy the server group certificate and private key from the initial active server to the initial backup server by using the next dialog box.

Note:
If you plan to use a third-party certificate authority, select this option and click **Next**. Then securely copy your own server group certificate and private key files to the initial backup server by using the next dialog box.

Server group certificate and private key locations

The following dialog box appears if you selected the second option in the **Server Group Certificate and Private Key Locations** dialog box.



Configure the initial backup server

To securely copy the server group certificate and private key files from the initial active server to the initial backup server using a USB key, complete this procedure.

1. With IC Setup Assistant set on this dialog box, insert the USB key in the initial active server.
2. Navigate to the `\I3\IC\Certificates\ServerGroup` directory on the initial active server.

   Note:
   If you are using your own server group certificate and private key, navigate to your preferred directory locations for the server group certificate (`ServerGroupCertificate.cer`) and server group private key (`ServerGroupPrivateKey.bin`).
3. Copy the entire `\I3\IC\Certificates\ServerGroup` directory to the USB key.

   If you are using your own server group certificate and private key, copy the server group certificate and private key you want to use to the USB Ejectkey.
4. the USB key from the initial active server.
5. Insert the USB key into initial backup server.
6. In the **Server Group Certificate and Private Key Locations** dialog box, click **Import Certificates**. The **Import Certificate** dialog box opens.

7. Navigate to the locations of the server group certificate and private key files on the USB key in the **Certificate Path** and **Private Key Path** boxes, for example:
   `F:\ServerGroup\ServerGroupCertificate.cer`
   `F:\ServerGroup\ServerGroupPrivateKey.bin`
   Keep the default Type and Format settings. Setup Assistant backs up the existing certificate/private key files before overwriting them.

   Note:
   If you are using your own server group certificate and private key, specify the **Type** and **Format** information, and whether the private key is password protected.

8. Click **OK**.
   The **Server Group Certificate and Private Key Locations** dialog box appears. It shows the paths of the server group certificate and private key files on the USB key that are copied to this CIC server.

9. Continue with IC Setup Assistant until it completes. The server group certificate and private key files are copied from the USB key to the CIC server during the **Commit** process.
10. Eject the USB key from the initial backup server.
11. Store the USB key in a secure location for backup purposes.

Troubleshooting

Do not manually copy the server group certificate and private key files from the designated existing CIC server to this CIC server. This method can lead to errors.

If errors occur, rerun IC Setup Assistant and follow the procedure described in this section. If IC Setup Assistant fails to start the CIC server processes (Notifier, DSServer, and AdminServer), see the PureConnect Knowledge Base article "How to Recover from Lost Certificates" (https://my.inin.com/Support/Pages/KB-Details.aspx?EntryID=Q120576310201905). This article describes how to regenerate the default certificates.

Complete Setup Assistant

After you commit your configuration choices and IC Setup Assistant saves the configuration, the **IC Setup Assistant** dialog box shows that the process is completed.

Use the report that IC Setup Assistant generates to ensure that the settings selected on the backup server are identical to the settings on the active server:

- When you finish running IC Setup Assistant on the active server, click **View Report** and print the report that Setup Assistant generates. This report shows the configuration settings that you selected.
- When you run IC Setup Assistant on the backup server, use the report generated on the active server to ensure that you make the same selections on the backup server.

Important!
Do not restart the computer at this time. Instead, choose **No, I will restart my computer later** and click **Finish**. This allows `Install.exe` to continue to install the other required installs on the server.
When `Install.exe` completes, restart the server to complete the CIC server installation and start CIC services.

Additional switchover configuration in Interaction Administrator

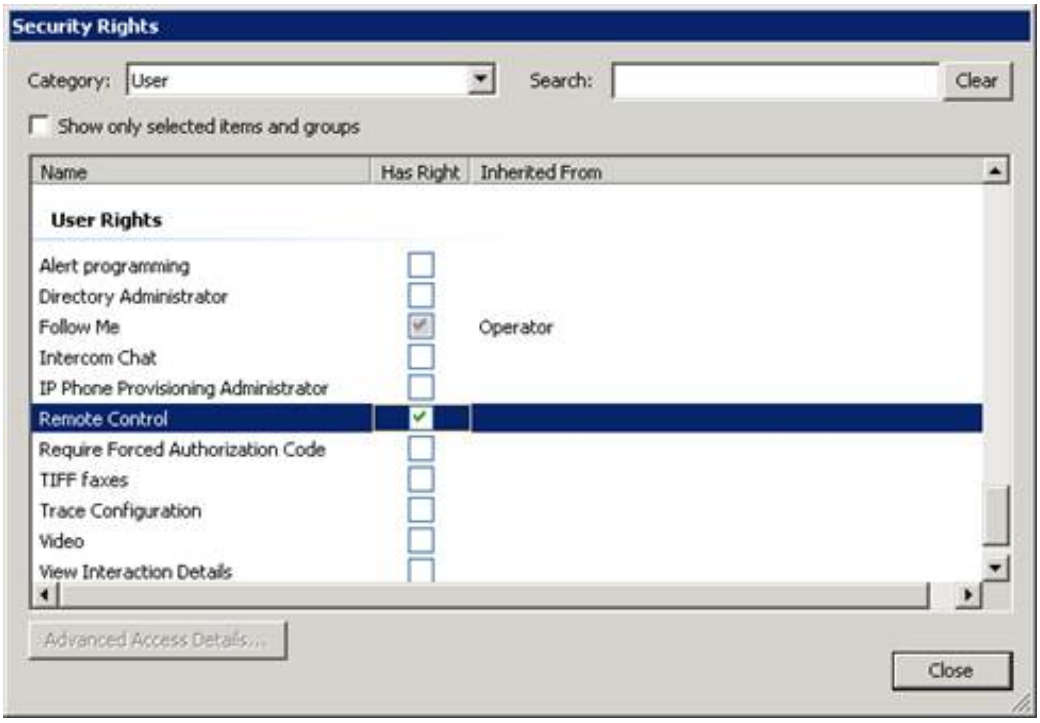
This section addresses additional switchover configuration in Interaction Administrator.

- **Make configuration changes in Interaction Administrator on the active server only**. All changes made to the DS tree using Interaction Administrator on the active server are replicated to the backup server.
- **Do not run Interaction Administrator on the backup server**. Configuration changes made on the backup server apply only to that server (are not mirrored to the active server), and are overwritten if the backup server is restarted. In addition, not all of the server subsystems are actively running on the backup server and the changes are not always recognizable.

Remote Control user rights

You can use the Switchover Control Panel to monitor the Switchover system on the backup server and start a manual switchover. To do this, assign **Remote Control** user rights to the administrator responsible for starting the switchover.

This user right is assigned in Interaction Administrator, in **the Security Rights** dialog box. This user right enables the administrator to run the Switchover Control Panel remotely, on the backup server.



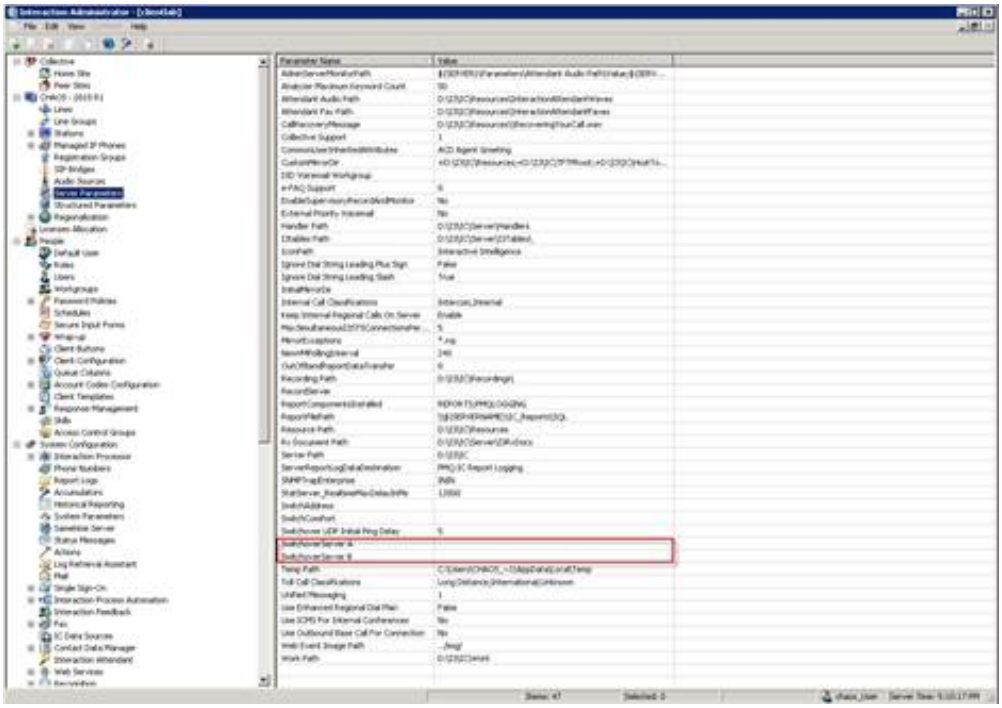
Make this configuration change on the active server only. All changes made in Interaction Administrator on the active server are automatically replicated to the backup server.

Switchover Server parameters

The system administrator can customize the Switchover subsystem behavior by modifying or adding **required** and **optional** Switchover system parameters in the **Interaction Administrator Server Parameters** container.

Make configuration changes to Switchover Server parameters on the active server only. All changes made in Interaction Administrator on the active server are automatically replicated to the backup server.

Note:
You can set additional server parameters to customize how data is replicated during a switchover. For more information about how those server parameters, see "Server parameters for customizing how data is replicated".



Required Switchover Server parameters

Required Switchover Server parameters are set in IC Setup Assistant as part of the initial CIC server installation and configuration.

The administrator can modify these required switchover system parameters in the **Interaction Administrator Server Parameters** container. (Alternatively, you can rerun IC Setup Assistant. Click **Options**, and then click **Proceed**. Click **Switchover Service**, and then click **Next**.)

Server Parameter Name	Type	Description
SwitchoverServer A	Packaged server parameter	This parameter specifies the name of the SwitchoverServer that is designated as the initial active server. This server comes up as active first and remains so until the first switchover event.
SwitchoverServer B	Packaged server parameter	This parameter specifies the name of the SwitchoverServer that is designated as the initial backup server. This server comes up as backup first and remains so until the first switchover event.

Optional Switchover Server parameters

The administrator can add or modify optional server parameters in the **Interaction Administrator Server Parameters** container to customize the Switchover subsystem behavior. None of these parameters are required. If you do not add these parameters, CIC uses the default values. The default values define monitoring practices that are adequate for most installations.

Note:
Packaged server parameters are pre-configured with default settings.

Server Parameter Name	Type	Description
Callback Interaction Recovery Enabled	General optional server parameter	To enable switchover support for callback interactions, add this parameter and set it to `1`. This server parameter is available in CIC 4.0 SU 3 and higher releases. By default this parameter is set to `0` or `Off`. **Note:** For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions".
Chat Interaction Recovery Enabled	General optional server parameter	To enable switchover support for chat interactions, add this parameter and set it to `1`. This server parameter is available in CIC 4.0 SU 3 and higher releases. By default this parameter is set to `0` or `Off`. **Note:** For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions" **Note:** CIC does not support SMS resiliency when the **Chat destination** option is selected.
CustomMirrorDir	Packaged server parameter	This parameter specifies one or more directories on the active server that are mirrored on the backup server. These parameters are mirrored in addition to the default set of mirrored directories. Any time a file is added, removed, or modified in one of these directories, the change is mirrored in the corresponding directory on the backup server. Separate each directory in the list with a semicolon (;). To mirror the directory recursively (including directory additions and deletions), place a + in front of the directory name. For example: `+D:\I3\IC\ImportantDir` To stop recursive monitoring, remove the +.
Custom Upgrade Attribute Exceptions	Customizable server parameter	For more information, see "Appendix C".
Custom Upgrade File Synchronization Directories	Customizable server parameter	For more information, see "Appendix C".
Custom Upgrade File Synchronization Exceptions	Customizable server parameter	For a description, see "Appendix C".
Custom Upgrade Synchronization Directories	Customizable server parameter	For a description, see "Appendix C".

ForceSwitchoverFQDNs	General optional server parameter	This parameter enables the Switchover system to override the system-generated names for the switchover pair, which it automatically resolves. When this parameter is set to `Yes` or `1`, the Switchover system instead uses the names that the system administrator specifies in the **SwitchoverServerFQDN A** and **SwitchoverServerFQDN B** server parameters. **Note:** If this server parameter is missing or disabled, then Switchover will try to automatically resolve the FQDNs from the NetBIOS. For more information about the use of this system parameter, see "Win32 CIC client machines outside the LAN cannot re-connect".
InitialMirrorDir	Packaged server parameter	This parameter specifies one or more directories on the active server that are mirrored on the backup server when the CIC server starts, in addition to the default mirrored directories. Separate each directory in the list with a semicolon (`;`). If you want the directory mirrored recursively (including directory additions and deletions), place a + in front of the directory name. For example: `+D:\I3\IC\ImportantDir`
Mail Interaction Recovery Enabled	General optional server parameter	To enable switchover support for email interactions, create this parameter and set it to `1`. **Note:** For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions". This server parameter is available in CIC 4.0 SU 3 and higher releases. By default this parameter is set to `0` or `Off`.
MirrorExceptions	Packaged server parameter	This parameter specifies the extensions of file types that you do not want to mirror. Separate multiple extensions with semicolons (`;`)> For example: `txt; gif; myext`.
Server A Address	General optional server parameter	To specify the IP address of the dedicated Switchover NIC on SwitchoverServer A in a dual or multiple NIC configuration, add this parameter. When **Server A Address** and **Server B Address** are set, the Switchover system uses these addresses exclusively to direct its traffic.
Server B Address	General optional server parameter	To specify the IP address of the dedicated Switchover NIC on SwitchoverServer B in a dual or multiple NIC configuration, add this parameter. When **Server A Address** and **Server B Address** are set, the Switchover system uses these addresses exclusively to direct its traffic.

SMS Interaction Recovery Enabled	General optional server parameter	To enable switchover support for SMS interactions, add this parameter and set it to `Yes` or `1`. This server parameter is available in CIC 2016 R4 and higher releases. By default this parameter is set to `0` or `Off`. **Note:** For information about a known side effect of enabling this server parameter, see "A note about the loss of duration information for interactions" The recovery of SMS generic objects requires that you also configure the IonNotifier parameter. For information, see *Call Recovery Feature Technical Reference* in the PureConnect Documentation Library.
StatServer_DisableQPSLoggingOnBackup	General optional server parameter	To disable the backup server from sending its log data to the CSV file, add this parameter and set its value to `Yes`. For more information, see "Location of log data".
Switchover Disable Gateway Ping	General optional server parameter	To enable the gateway ping, set this server parameter to `No` or `0`. To disable the gateway ping set the parameter to `Yes` or `1`. For more information about using this server parameter, see "Detecting Network Connection Status of the Backup and Primary" in Primary Monitor.
Switchover DS Request Timeout	General optional server parameter	To specify the timeout length (in seconds) for DS requests that are sent by the backup server to the primary server, add this parameter. The requests can be sent during either the initial startup of the backup server or the resynchronization with the primary server. The default value is 120 seconds.
Switchover File Monitor Health Check Interval	General optional server parameter	Set this parameter to the number of seconds between each health check request that is sent from the backup server to the File Monitor on the primary server. To turn off the health check request, set this parameter to `0`. If no value is specified, the default value is 60 seconds. This parameter works with the Switchover **File Monitor Health Check Timeout** parameter. For more information, see "Configuration options for File Monitor Health Checks".
Switchover File Monitor Health Check Timeout	General optional server parameter	Set this parameter to the number of seconds that the backup server gives File Monitor to respond to the health check request before it times out and traces the failure. If no value is set, the default value is 10 seconds. This parameter works with the Switchover **File Monitor Health Check Interval** parameter. For more information, see "Configuration options for File Monitor Health Checks".
Switchover IP Retry Delay	General optional server parameter	Add this parameter, if necessary, for use with Interaction Director Switchover systems. When monitoring IP, this server parameter has the same effect as **Switchover TS Failure Retry Delay**. The Interaction Director server install automatically creates this server parameter. Genesys recommends that you review this server parameter in Interaction Administrator on the Interaction Director server to confirm the setting.

Switchover IP Timeout	General optional server parameter	Add this parameter, if necessary, for use with Interaction Director Switchover systems. When monitoring IP, this server parameter has the same effect as **Switchover TS Timeout**. The Interaction Director server install automatically creates this server parameter. **Note:** Confirm the setting of this server parameter in Interaction Administrator on the Interaction Director server.
Switchover Max Restarts	General optional server parameter	To specify the maximum number of times in a restart period that a new process ID can be returned in the TS ping notification before a restart occurs, add this parameter. By default, this value is `2`.
Switchover Max Restarts Period	General optional server parameter	To specify the time period (in seconds) during which the Switchover system counts TS ping notifications that contain new process IDs, add this parameter. By default, this value is `300` (5 minutes).
Switchover Max Sequential Restarts	General optional server parameter	To specify the maximum number of sequential times that a new process ID can be returned in the TS ping notification before a switch occurs, add this parameter. By default, this value is `2`.
Switchover Max TS Failures	General optional server parameter	To specify the number of TS ping failures the Switchover system on the backup server tolerates before starting a switchover, add this parameter. **Note:** Set this value greater than 0. The default value is `2`. **Note:** The failure count is reset each time the Switchover system successfully receives a response from TS on the primary server.
Switchover Monitoring	General optional server parameter	Add this parameter, if necessary, for use with Interaction Director Switchover systems. The Interaction Director server install automatically creates this server parameter. It sets up an IP ping process in Interaction Director configurations, which are similar to the TS ping process in CIC configurations. The default value is TsServer. **Note:** Confirm the setting of this server parameter in Interaction Administrator on the Interaction Director server.

Switchover NetTest A	General optional server parameter	Add this parameter, if necessary, for switchover in WAN environments. It applies to **Pure SIP** configurations only. **Switchover NetTest A** specifies the name or IP address of a computer on the same network segment as **SwitchoverServer B**. The Switchover system uses the IP address on **SwitchoverServer A** when **SwitchoverServer A** is the backup server. Whenever a failure condition is detected, the Switchover system on the backup server uses ICMP echo to ping this IP endpoint. It must find the IP endpoint on the same network segment as the active server. If the Switchover system cannot ping this endpoint, it assumes that the active server is still operable and doesn't switch because there a WAN failure. **Important!** Since the Switchover system no longer has a network connection (and thus cannot replicate changes), it logs an error to the event log and shuts down processing. Restart the backup server, so that the Switchover system can resume its monitoring and replication. Recommendation: The value for **Switchover NetTest A** is the closest *pingable* (ICMP echo) IP address to **SwitchoverServer B** from **SwitchoverServer A**.
Switchover NetTest B	General optional server parameter	Add this parameter, if necessary, for switchover in WAN environments. It applies to **Pure SIP** configurations only. This parameter specifies the name or IP address of a computer on the same network segment as **SwitchoverServer A**. The Switchover process on **SwitchoverServer B** uses the IP address when **SwitchoverServer B** is the backup server. Recommendation: The value for **Switchover NetTest B** is the closest *pingable* (ICMP echo) IP address to **SwitchoverServer A** from **SwitchoverServer B**.
Switchover NetTest Timeout	General optional server parameter	Add this parameter, if necessary, for use with Switchover in WAN environments. It applies to *Pure SIP* configurations only and is used with **Switchover NetTest A** and **Switchover NetTest B**. This parameter specifies the amount of time (in seconds) Switchover waits for the ICMP echo to return. By default, this value is `1` second.
Switchover Notifier Reconnect Delay	General optional server parameter	Specifies the interval in seconds that the Notifier connections will wait to re-establish a new connection after a loss. Lower values can improve reconnection response during short periods of connection los with the primary monitor. The default value is `5`. The minimum value is `5`. The maximum value is `60`.
Switchover Ping on Aux Connection	General optional server parameter	This parameter moves the TS ping from the main data connection to the auxiliary connection. By default, this parameter is set to `0`, which means it is not enabled. **Note:** To enable QoS on the ping on the auxiliary connection (not the main connection), be sure that both the **Switchover Ping on Aux Connection** and the **Switchover Use QoS For Ping** parameters are enabled. If only the **Switchover Use QoS For Ping** parameter is enabled, QoS is not used on the ping.

Switchover Primary Monitor Ping Delay	General optional server parameter	Specifies the delay in seconds between the primary monitor pings to the notifier on the primary monitor. The default value is `0`. The maximum value is `300`.
Switchover Primary Monitor Retry Ping Delay	General optional server parameter	Specifies the delay in seconds between pings when the primary monitor is in retry mode. The default value is `0`. The minimum value is `0`. The maximum value is `300`.
Switchover Primary Monitor Retry Count	General optional server parameter	Specifies the number of times the primary monitor will send retry pings before it begins diagnosing the connection issues. The default value is `2`. The minimum value is `1`. The maximum value is `50`.
Switchover Primary Monitor Timeout	General optional server parameter	Specifies the timeout value in seconds for a ping from the primary monitor on the backup to the notifier on the primary. If a ping is not received in this time frame, the primary monitor will then begin its retry mode. The default value is `0`, which indicates that the value will be one half of the monitored module timeout whose default value is `10` seconds. The maximum value is `300`.
Switchover QoS DSCP	General optional server parameter	When **Switchover Use QoS For Ping** parameter is enabled, add this parameter to set the value in the QoS byte. Differentiated Services Code Point (DSCP) is the 6 most significant bits of a packet. You can use DSCP to prioritize QoS traffic on Switchover. **Note:** To enable QoS on the auxiliary connection ping, enable both the **Switchover Ping on Aux Connection** and the **Switchover Use QoS For Ping** parameters. If only the **Switchover Use QoS For Ping** parameter is enabled, QoS is not used on the ping.
Switchover Reconnect Timeout	General optional server parameter	Specifies the duration in seconds that switchover on the backup will attempt to reconnect with the primary. This timeout begins once the primary monitor has diagnosed the connection and signaled the appropriate event to the switchover state machine. Therefore, the actual duration from the time connections issues were first detected to the time the backup gives up and switches over will be longer than this because there is the interval where the retry pings are sent and then the network checks all made by the primary monitor. This can take around 15 seconds if the backup is not connected to the network or 70 seconds if the primary is not connected to the network. A value of `0` indicates an immediate switchover when a connection is lost. A value greater than `0` indicates the number of seconds that the timer will be set to expire. The default value is `30`. The minimum value is `0`. There is no maximum value. **Note:** This parameter is new in CIC 2015 R# releases and up. It was known as **Switchover Reconnect Delay** from 4.0 SU4 through 4.0 SU6.
Switchover TS Failure Retry Delay	General optional server parameter	To specify the number of seconds that the Switchover system waits, after marking a TS failure, before sending the second ping, add this parameter. The system switches once the failure count exceeds the value stored in the **Switchover Max TS Failures** parameter, which defaults to `2`. **Note:** Set this value to greater than `0` seconds. The default is `1` second.

Switchover TS Timeout	General optional server parameter	To specify the number of seconds that the Switchover system waits from the time the ping is sent until it is marked as a TS failure, add this parameter. This parameter also specifies the number of seconds that the Switchover system waits after a TS success before it sends another ping. Set this value between `5` - `60` seconds. The default is `10` seconds.
Switchover Unreachable Primary Ping Count	Optional server parameter	Specifies the number of times that a ping set is sent to the primary before switching over. A ping set consists of one or more pings sent during a single attempt to detect the primary's system on the network. Pings will be sent until the primary responds or the maximum number of ping attempts is reached. This count is not the number of pings sent in a single set when trying to contact the primary; it is the maximum number of ping sets that are sent to the primary before a switchover will occur. The delay between sending ping sets is defined by the **Switchover Unreachable Primary Ping Delay** parameter. If you enter values `0`-`3`, the switchover system sends 3 additional ping sets to the primary server. If these attempts fail, the server is considered unreachable and a switchover is initiated. If you enter a value of `-1`, it results in unlimited attempts until the primary server is reached. In this case, if the connection issue is determined to be an unreachable primary server, switchover will not occur since the backup server will keep waiting for the primary server to be reachable again. **Note:** Use a value of `-1` only if a switchover should never occur as long as the primary server is reachable. In many cases, the switchover occurs after the Notifier timeout occurs, not as a result of the unreachable primary pings. The default value is `0`. The minimum value is `-1`. There is no maximum value.
Switchover Unreachable Primary Ping Delay	Optional server parameter	Specifies the interval in seconds between sending ping sets to the primary monitor when it is unreachable. See the **Switchover Unreachable Primary Ping Count** parameter for the definition of a ping set. The default value is `10`. The minimum value is `1`. The maximum value is `300`.
Switchover Use QoS for Ping	General optional server parameter	To customize QoS for the TS ping on the auxiliary connection, add this parameter and set it to `Yes` or `1` to enable it. Use this parameter to set the priority of ping (echo request and echo reply) packets. You can make further customizations by using the **Switchover QoS DSCP** parameter. When enabling DSCP tagging, `AF41` (DSCP 34) is tagged by default. To change the value, set it to any of the tagging classes. **Note:** To enable QoS on the ping on the auxiliary connection (not the main connection), enable both the **Switchover Ping on Aux Connection** and the **Switchover Use QoS For Ping** parameters. If only the **Switchover Use QoS For Ping** parameter is enabled, QoS is not used on ping.

SwitchoverServerFQDN A	General optional server parameter	When the **ForceSwitchoverFQDNs** server parameter is enabled, then the **SwitchoverServerFQDN** A server parameter contains the fully qualified domain name of the Switchover Server A. For more information, see "ForceSwitchoverFQDNs and Win32 CIC client machines outside the LAN cannot re-connect" in Problems with the Switchover system running improperly.
SwitchoverServerFQDN B	General optional server parameter	When the **ForceSwitchoverFQDNs** server parameter is enabled, then the **SwitchoverServerFQDN B** server parameter contains the fully qualified domain name of the Switchover Server B. For more information, see "ForceSwitchoverFQDNs and Win32 CIC client machines outside the LAN cannot re-connect" in Problems with the Switchover system running improperly.

Dynamic monitoring of system parameters

As of IC 4.0 SU 5, the following server parameters are monitored dynamically. If one of these parameters is changed on the primary server, its new value takes effect immediately. You do not need to restart the backup server in order for the new value to take effect.

- CustomMirrorDir
- Switchover Max TS Failures
- Switchover TS Failure Retry Delay
- Switchover TS Timeout

For more information, see "Optional Switchover Server parameters".

Server and system parameters for CIC resources on other servers in the CIC network

Contact databases, report logs, and voice mail recordings can have significant resource requirements. They are usually stored on separate servers on the network, for example, database server, and voice mail compression server.

The CIC resources on these backup servers are usually updated regularly. Both the active and backup servers must have immediate access to these CIC resources on the backup servers for mirroring purposes.

Pointers to these CIC resources are set in the path specifications that are defined in the server and system parameters on the CIC server.

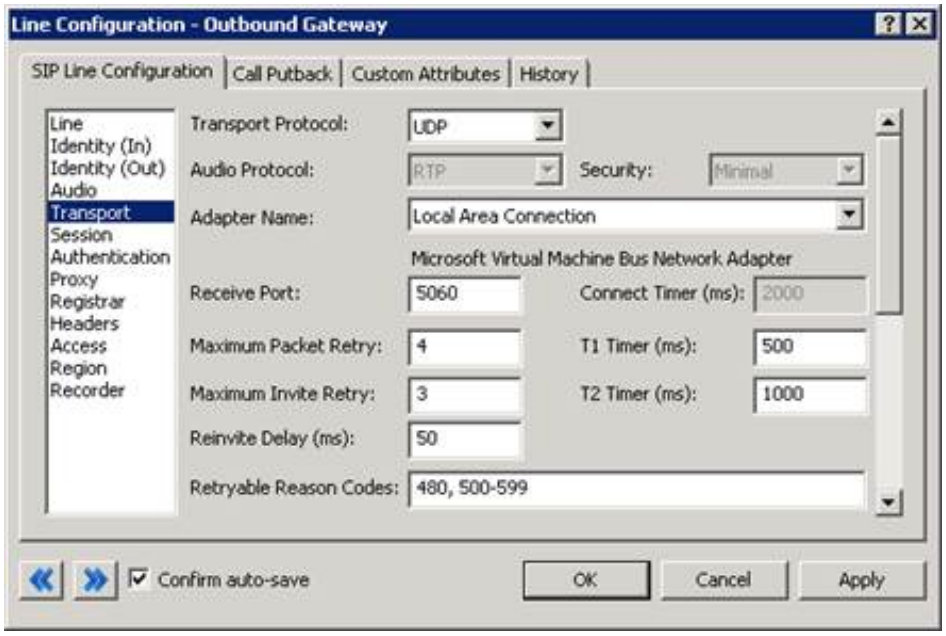
Set the server and system parameter values for these CIC resources in Interaction Administrator on the active CIC server only. All changes made in Interaction Administrator on the active server are replicated to the backup server.

SIP line NIC configuration

SIP lines use the Windows **Network Connection** name to identify the NIC to listen for SIP traffic.

If you assigned *friendly names* or aliases to the network connections, then complete the following steps to associate the SIP lines with an assigned network connection name on the active server in the **SIP Line Configuration**> **Transport** dialog box in Interaction Administrator:

1. In Interaction Administrator, access the **SIP Line Configuration** dialog box for the appropriate SIP line and in the **SIP Line Configuration** tab, click **Transport**.
2. In **Adapter Name** box, click the assigned name of the network interface card (NIC) to be used for VoIP communications



When you assigned *friendly names* to the Windows network connections, you also assigned identical names on both the active and backup servers. (To be identical, the names have to use the same capitalization, punctuation, and the use of spaces.) Assuming those names are identical, the Switchover system now replicates the assigned name in the **SIP Line Configuration** dialog box on the backup server.

(Optional) Create custom handlers for switchover

Partners can use the following switchover-related tools to create custom handlers for certain customer implementations. These tools are set in Interaction Designer. For more information, see the Interaction Designer Help in the PureConnect Documentation Library.

Tool	Description
Query Backup tool	The Query Backup tool can be used in any handler to ask the host CIC server if it is running as a backup SwitchoverServer. If the answer is `True`, the handler takes a different path to avoid duplicating the processing that is required on the active server (for example, statistics logging). After the backup server takes over after a switchover event, the Query Backup tool on that server returns `False`. It also enables functionality that was prevented on that server while it was in backup mode.
Switchover Event initiator	Use the Switchover Event initiator to start a handler on the host server whenever a switch occurs. You can configure it to trigger on either of the following types of events: • A `Commence` event, which tells the backup server to become active • A `Discontinue` event, which tells the active server to cease operations **Note:** A `Discontinue` notification is not guaranteed.

Install the Switchover system on an existing CIC system

If you already have a production CIC server, and you want to add the Switchover system to it, complete this section.

Prepare the backup server

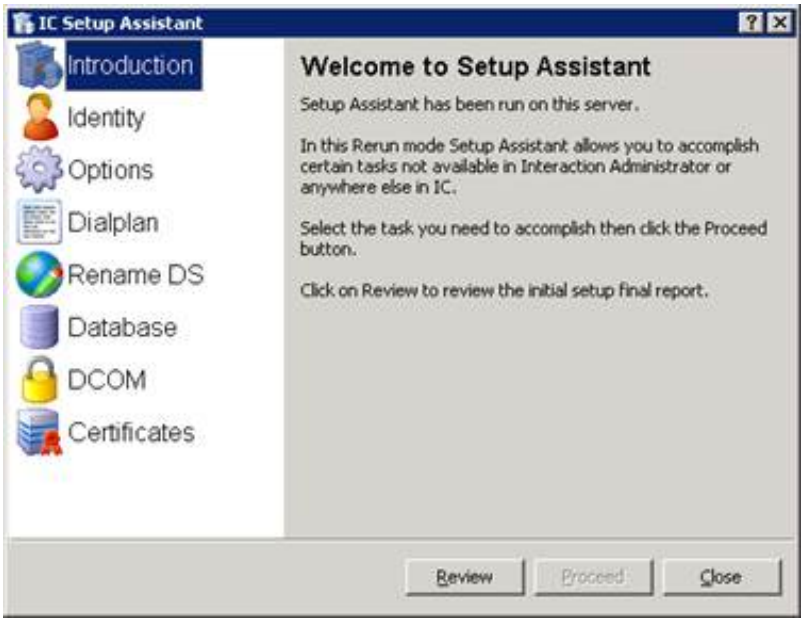
1. If you have not already done so, **fulfill CIC server and Switchover-specific requirements** and pre-installation procedures on the new backup server. For more information, see "Switchover Server requirements".

   The backup server must be identical to the production (active) CIC server in every respect. Only the computer names and IP addresses must be different between the 2 servers.
2. Follow the instructions in "Install CIC on the Switchover Server pair" to install **CIC on the backup server**. When you complete those instructions, you run the CIC server install, install the PureConnect Documentation Library, and apply the most recent service update.

   Note:
   Do not run IC Setup Assistant to configure the backup server yet (it is shown as the last step in the New Installation Task List). Perform this final step later.

Configure the Switchover system on the active server

1. Apply the most recent CIC release on the production (active) CIC server. Either use Interactive Update or manually download and apply the appropriate files from the PureConnect Customer Care website.
2. Run the IC Setup Assistant on your production (active) CIC server. To do this, select **Start > Programs > PureConnect > IC Setup Assistant**.



3. Click **Options** and follow the instructions in "Switchover notes for IC Setup Assistant".

Configure the Switchover system on the backup server

This step is also required for new installs.

1. Run the IC Setup Assistant on your production (active) CIC server by selecting **Start > Programs > PureConnect > Setup Assistant**.

   IC Setup Assistant appears in **Rerun** mode.
2. Click **Options** and follow the instructions in "Switchover notes for IC Setup Assistant".

Configure the SwitchoverServer A and B server parameters

Configure the server parameters as shown in the following example:

On ICServer1

SwitchoverServer A = ICServer1

SwitchoverServer B = ICServer2

On ICServer2

SwitchoverServer A = ICServer1

SwitchoverServer B = ICServer2

If the **SwitchoverServer A** and **B** server parameters are not set correctly, the Switchover system cannot determine which server is the active server and which one is the backup server. As a result, CIC does not start successfully.

Connect the Switchover system

In *Pure SIP* configurations, the first server that you start becomes the active server. The second server that you start becomes the backup server.

The virtual switch, which is a software module in the Switchover system, designates the servers as active or backup based on the startup order.

Configure switchover in WAN environments

Often, it is desirable to have a duplicate CIC server in a geographically distant location to ensure that services are readily available in the event of a disaster.

The default switchover configuration depends heavily on a fast, reliable connection between the two servers and a switchover time of 30 seconds or less. However, in a WAN environment, the default switchover configuration can result in *false positives*, or the Switchover system can interpret a failure in the network link as a CIC server failure. In this case, the active server is unavailable. When a connection to the backup server location is lost, the backup server switches over. Once the connection is re-established, either the active server shuts down and all calls are lost, or you end up with two active servers.

Call Recovery feature

The Call Recovery feature requires that both servers in a switchover pair reside at the same geographic location. Do not use Call Recovery in an environment with a distributed (WAN) switchover configuration.

For all other types of interactions (callbacks, chats, and emails), CIC supports full recovery during a switchover in a WAN environment.

For more information about call recovery, see *Call Recovery Feature Technical Reference* in the PureConnect Documentation Library.

Switchover NetTest server parameters

A set of server parameters enables you to configure a second address to test before switching over to the backup server. If that address cannot be reached, CIC assumes that the network is down and the system does not switch to the backup server.

- **Switchover NetTest A** specifies the name or IP address of a computer on the same network segment as **SwitchoverServer B**. The Switchover system on **SwitchoverServer A** uses the computer name or IP address when **SwitchoverServer A** is the backup server.

  Whenever a failure condition is detected, the Switchover system on the backup server attempts to ping (ICMP echo) the IP endpoint found on the same network segment as the active server. If the Switchover system cannot ping this endpoint, it assumes that the active server is still operable and it does not cause a switchover.

  Important!
  Since the Switchover system no longer has a network connection, and thus cannot replicate changes, it logs an error to the event log and shuts down processing. To restart switchover monitoring and replication, you must restart the backup server.

To determine the value for **Switchover NetTest A,** choose the closest *pingable* (ICMP echo) IP address to **SwitchoverServer B** from **SwitchoverServer A**.

- **Switchover NetTest B** specifies the name or IP address of a computer on the same network segment as **SwitchoverServer A**. The Switchover system on **SwitchoverServer B** uses the computer name or IP address when **SwitchoverServer B** is the backup server.

  To determine the value for **Switchover NetTest B**, choose the closest *pingable* (ICMP echo) IP address to **SwitchoverServer A** from **SwitchoverServer B**.
- **Switchover NetTest Timeout** specifies the amount of time in seconds that the Switchover system waits for the ICMP echo to return. By default, this value is one second. **Switchover NetTest Timeout** is used with the **Switchover NetTest A** and **Switchover NetTest B** server parameters.

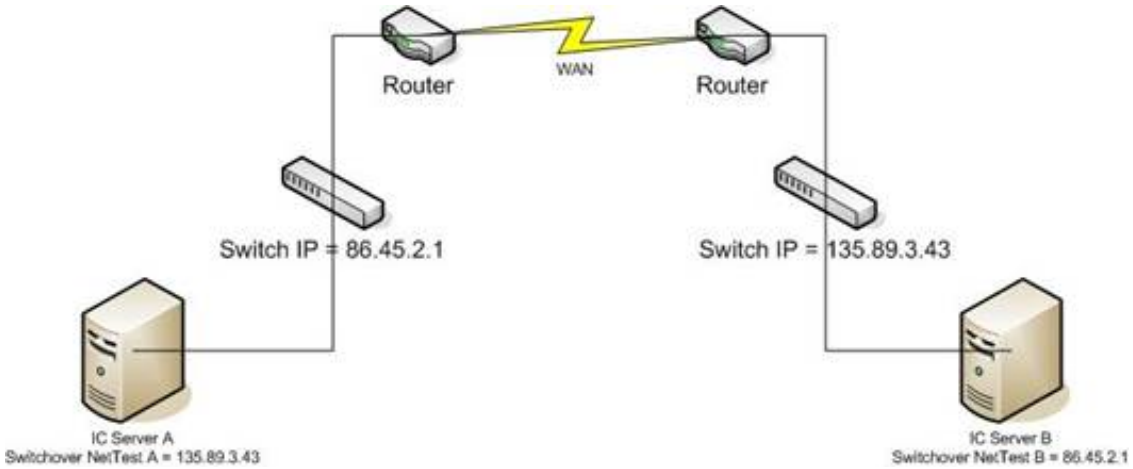
For example, when **SwitchoverServer A** is the backup server, it uses the **Switchover NetTest A** server parameter to test WAN connectivity.

Time	Message
15:52:05.437_0755	ServiceParameters::GetParametersFromRegistry: NetTest Server 1=135.89.3.43
15:52:05.437_0756	ServiceParameters::GetParametersFromRegistry: NetTest Server 2=86.45.2.1
15:52:05.437_0757	ServiceParameters::GetParametersFromRegistry: NetTest Server Address=135.89.3.43

When **SwitchoverServer B** is the backup server, it uses the **Switchover NetTest B** server parameter to test WAN connectivity.

Time	Message
15:41:45.961_0548	ServiceParameters::GetParametersFromRegistry: NetTest Server 1=135.89.3.43
15:41:45.961_0549	ServiceParameters::GetParametersFromRegistry: NetTest Server 2=86.45.2.1
15:41:45.961_0550	ServiceParameters::GetParametersFromRegistry: NetTest Address=86.45.2.1

To determine the value for **Switchover NetTest A**, choose the closest *pingable* (ICMP echo) IP address to **SwitchoverServer B** from **SwitchoverServer A.** To determine the value for **Switchover NetTest B**, choose the closest *pingable* (ICMP echo) IP address to **SwitchoverServer A** from **SwitchoverServer B**. The following figure illustrates this configuration.



Additional suggestions for reducing false positives

To further reduce the occurrence of false positives do the following:

- Run the Switchover system in **Manual** mode using the **ManualSwitchOnly** command-line parameter.
- Increase the value of the **Switchover TS Timeout** server parameter. This change allows more time for a response before the TS ping is considered to have failed.
- Increase the value of the **Switchover TS Failure Retry Delay** server parameter. This change provides the network more recovery time between the first and second failed TS pings.
- Set the **Switchover Ping on Aux Connection** server parameter to `Yes` or `1` to move the TS ping from the main data connection to the auxiliary connection.
- Set the **Switchover Use QoS For Ping** server parameter to `Yes` or `1` to set the priority of the ping (echo request and echo reply) packets.
- Balance the speed of response and false positives. If you set the values too high, switchover may not occur for many minutes after the primary server fails. If you set the values too low, a switchover may occur because the route between the servers was temporarily delayed.

If the Switchover system remains in **Automatic** mode, keep in mind that if the backup server cannot contact the active server, it cannot disable it. Also, CIC clients may not be able to connect to the backup server across the WAN. If a WAN link is severed, CIC clients on each side of the break may log on to different servers. When the WAN link is re-established, the backup server notifies the active server that it is no longer active.

Additional WAN switchover configuration

Appendix A illustrates a sample WAN Switchover configuration and provides the configuration procedures for VLANs, switch trunking, ISL802.1Q subinterfaces, static routes, and QoS.

Operation

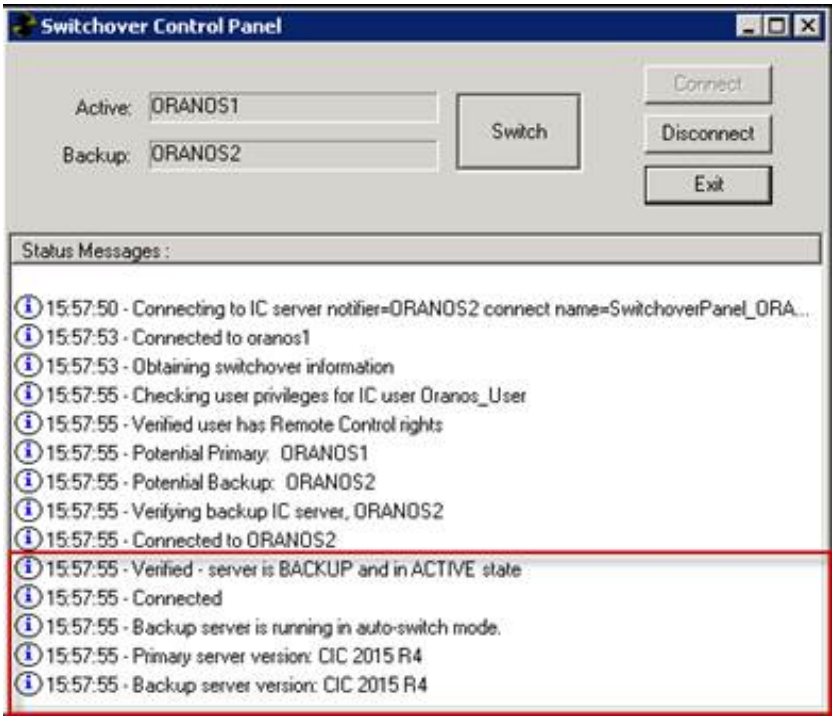
The Switchover Control Panel

After the CIC system has been installed and configured for a switchover pair, a menu entry for the Switchover Control Panel appears in **Start** > **Programs** > **PureConnect** >**Switchover.** This appears on both the active and backup servers.

The Switchover Control Panel is the graphical interface that communicates with the active and backup servers and displays information regarding the current state of each server in a switchover pair. If the two servers are running on different releases, it indicates that the backup server is running against a primary server with a higher or lower SU or release number. This condition is called the **Upgrade** state. You can also use the Switchover Control Panel to start a controlled switchover manually.

Active state

In the **Active** state, the **Switchover Control Panel** dialog box indicates that both servers are running in *auto-switch* mode and are on the same release.



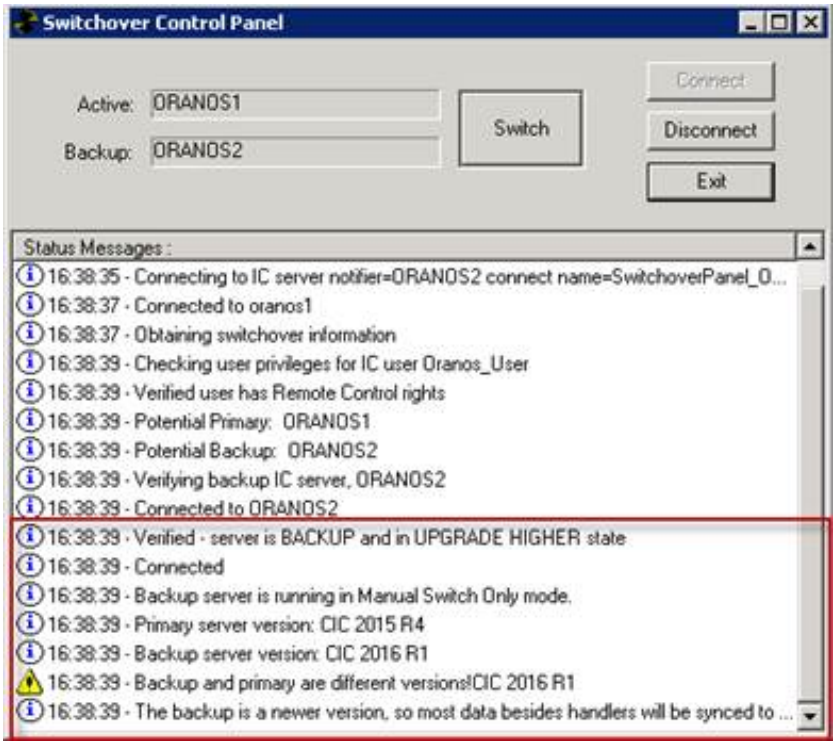
Upgrade states

While in an **Upgrade** state, the Switchover Control Panel indicates that the backup server is running in *manual switch only* mode. This is because the backup server is on a different release than the primary server.

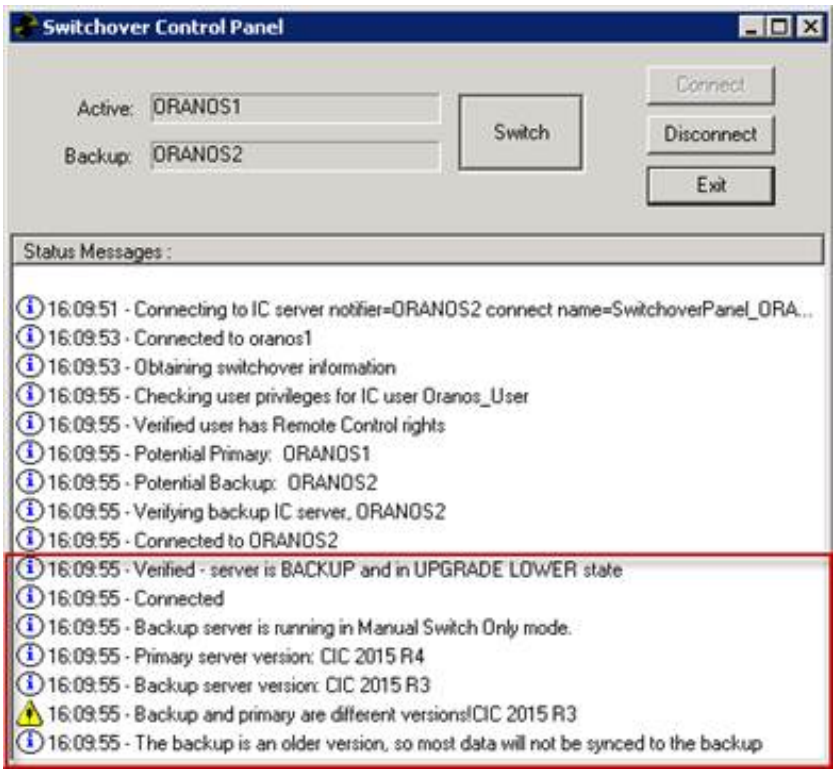
> **Warning:**
> The backup server does not become the active server if the primary server experiences a failure when running in this state.

The **Upgrade** state is either **Upgrade Higher** or **Upgrade Lower**, depending upon whether the backup server is running a higher or lower release than the primary server. For more information about the upgrade states and how to configure which data is replicated, see "Appendix C".

- The **Upgrade Higher** state occurs when the backup server is on a newer release than the primary server.



- The **Upgrade Lower** state occurs when the backup server is on an older release than the primary server.



Note:
To view and use the Switchover Control Panel, assign Remote Control user rights in Interaction Administrator to the administrator responsible for starting the switchover.

Best practice: perform a scheduled switchover regularly

Manually perform a scheduled switchover on a regular basis, for example, every 30 days. This accomplishes several goals:

- It exercises the switchover process, ensuring that CIC client applications are reconnecting to each server correctly and that the telephony circuits continue to function.
- It ensures that the replication of files and configuration is occurring properly.
- You verify that switchover failure detection is working correctly. To do this, start a manual switchover through the Switchover Control Panel. Alternatively, simulate a network failure of the active server or a services failure on the active server.

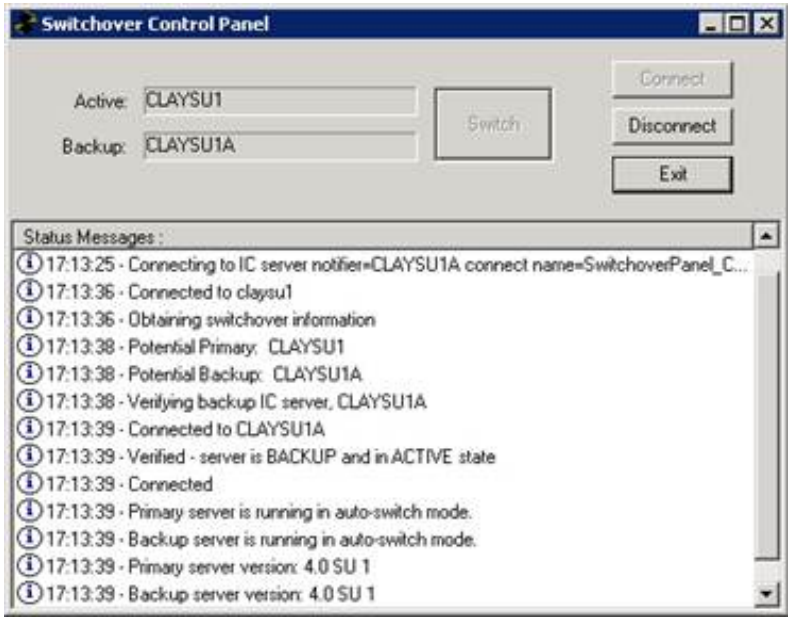
Manually start a switchover on the backup server

This section explains how to start a switchover manually on the backup server, for example, in a testing situation, in the Switchover Control Panel. The Switchover Control Panel is the graphical interface that monitors and controls the Switchover system on the backup server. Instructions are also provided for manually starting a switchover from the command line.

To avoid data loss during a manual switchover, be sure to read the *File replication warnings* section.

Manually start a switchover in the Switchover Control Panel

1. If you have not already done so, assign **Remote Control** user rights to the administrator who starts the switchover. This user right is assigned in Interaction Administrator, in the **Security Rights** dialog box.
2. On the backup server, select **Start** > **Programs** > **PureConnect** > **Switchover**.



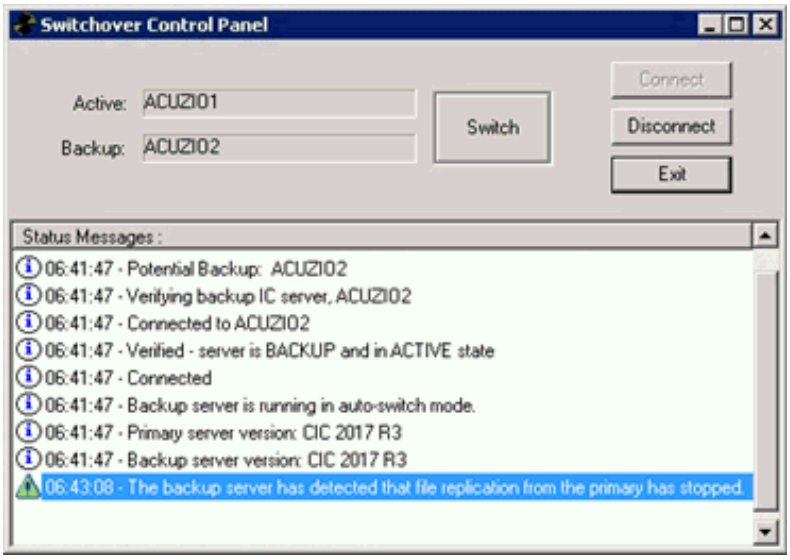
   The Switchover Control Panel displays the names of the active and backup servers and the current connection state to each of those servers.
3. Click **Switch**.
   A confirmation dialog opens.

4. Click **Yes**.
   A message is sent to the backup server to start a switch. When the switchover occurs, the backup server stops mirroring the registry and specified directories on the active server. It also logs a message in the application event log. The status of the switchover process appears in the **Status Messages** window on the **Switchover Control Panel** dialog box.

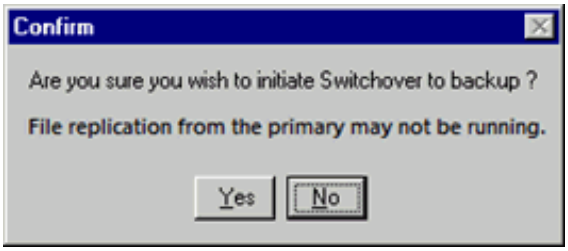
File replication warnings

For a successful switchover to occur, file replication must be current and running. If it isn't, data loss could occur.

If file replication is not running and you start a switchover manually on the backup server, you'll see a warning message in the Switchover Control Panel.



If you miss the warning in Switchover Control Panel and click **Switch**, you'll see a second warning message in the confirmation dialog. Click **No** to halt the switchover.



Manually start a switchover from the command line

To start a switch from the command line, run the Switchover Control Panel executable with the following options:
`SwitchoverCtrlU.exe /Immediate /Notifier`

It starts, switches, and stops automatically.

Run `SwitchoverCtrlU /?` to view the all the options available for this tool.

Note:
- Only a master administrator can run the **SwitchoverCtrlU.exe** tool.
- Before you start a switchover from the command line, you should check the Switchover Control Panel for warning messages.
- When you use Control Panel to force the backup server to switch immediately with the `/Immediate` flag, the **Remote Control** User right is not checked. This right is also not checked if there is no primary server.
- No CIC user account is required to connect to only the backup machine.

Modify switchover start and run behavior using command-line parameters

In certain circumstances, you have to edit the CIC process tree manually to modify the Switchover system *start and run* behavior on a single computer in the switchover pair. This section describes how you can use two command-line parameters for this purpose.

Command-line parameter	Description
`/ForceBackup`	This parameter forces server into backup mode.
`/ManualSwitchOnly`	This parameter disables switching by the monitoring system.

Note:
Command-line parameters are not case-sensitive.

Start switchover in Manual mode

In some situations, for example as part of a test scenario, you need to retain full control over when CIC switches from the active to the backup server. In this case, use the `/ManualSwitchOnly` command-line parameter to start switchover in **Manual** mode.

Note:
This mode requires a restart to take effect.

When the Switchover system is in **Manual** mode, it starts on the backup server and performs the initial and ongoing file and registry copies, mirroring the active server. However, it does **not** start monitoring the critical subsystems (for example, TsServer or Notifier) for failure on the active server. A switchover occurs only if you click the **Switch** button on the Switchover Control Panel.

Warning!
Adding this command-line argument to the Switchover system disables it from automatically switching to the backup server when a critical subsystem ever fails on the active server. **Do not use Manual mode for typical operations in business-critical environments.**

To modify the command line on the Switchover system, so that it starts in Manual mode:

1. Use regedt32 to update DS and navigate to the following key:

```
HKEY_LOCAL_MACHINE\
   SYSTEM\
      CurrentControlSet\
         Services\
            Interaction

Center\
                  ProcessTree\
                     Level3\
                        SwitchoverService
```

2. With the **SwitchoverService** key selected in the left pane, double-click the **CommandLineArguments** entry in the right pane.
3. When the **String Editor** dialog box appears, type the `/ManualSwitchOnly` command-line parameter and then click **OK**.

Apply a new CIC release to an existing switchover pair

For instructions on applying new CIC releases to an existing Switchover pair, see "Appendix B".

Interaction Message Store and switchover

When your CIC implementation contains a switchover pair, Genesys recommends that you **do not** include the Interaction Message Store root directory in the list of replicated directories.

Instead, put the Interaction Message Store on a network-based file share that is accessible to both of the servers in the switchover pair. Genesys also recommends that the file share exist on the same LAN as the CIC servers. If the file share is on a WAN, delays can occur with certain TUI operations. If a switchover occurs, the backup CIC server can still reach the message store on the file share, and the site continues to work.

Configuration options for File Monitor health checks

In rare cases, File Monitor can become unresponsive or shut down unexpectedly. If a switchover occurs before File Monitor is restarted, the latest files will not be replicated to the backup server. A health check has been added in 2015 R3 to make these types of File Monitor failures more visible.

Two system parameters are used with the File Monitor health check: **Switchover File Monitor Health Check Interval** and **Switchover File Monitor Health Check Timeout**. These parameters govern how often the File Monitor health check occurs and when a failure message is written to the event log. For more information, see "Switchover Server parameters".

Return the Switchover service to a functioning state after a switch occurs

Once a switchover occurs, the automatic failover process ceases to work. To return Switchover to a functioning state, you must follow these steps:

1. Determine if the former *active* server has malfunctioned. If it has, fix the problem.
2. Reboot the former *active* server. When it reboots, it will detect that there is already an active server on the network and it will become the backup server.

Troubleshooting

This section provides information to determine the cause of any problems you may experience with the Switchover system.

Problems with switchover starting improperly

This section addresses questions regarding why the Switchover system is not starting properly.

Why does the server always come up active?

Upon starting, the Switchover system tries to determine the correct role of the server on which it is running: active or backup. Two issues may arise from this:

- The Switchover system has trouble communicating in a *pure SIP* environment
- The Switchover system misdiagnoses the state of the server

Switchover system has trouble communicating in a Pure SIP environment

On the first CIC server that starts up, the Switchover subsystem attempts to connect to port 3633 on the opposite server. Port 3633 is the *virtual switch port*. The Switchover subsystem then asks for the current state of the Switchover subsystem on that server. If the Switchover subsystem on the first server cannot communicate with the Switchover system on the opposite server, the first CIC server starts up in active mode.

To address this issue:

- Verify that you can ping the opposite server from the current server.
- If you are using a dual configuration or a multiple NIC configuration, verify that the **Server A Address** and **Server B Address** server parameters are correctly set in Interaction Administrator.
- Verify that the Switchover system is running on the opposite computer.

Why doesn't switchover start on the backup server?

This section explains the messages that may appear in the Switchover log relating to the Switchover system not starting on the backup server. You can view the Switchover log on the backup server under the Server log directory or in the Switchover Control Panel under **Status Messages**.

Switchover is not active in the process tree

Switchover, the SwitchoverFileMonitor subsystem, or both are inactive in the process tree.

Switchover failed to authenticate with Notifier on the active server

The following are the possible causes of this issue:

- The SwitchoverServer A and SwitchoverServer B server parameter names are reversed.
- No active server exists.
- The active server may still be starting.
- The active server may be in *stale* (inactive) mode.
- No CIC user is associated with the Windows NT domain user under which the CIC service is running (or the entry is incorrect).
- DCOM is disabled.

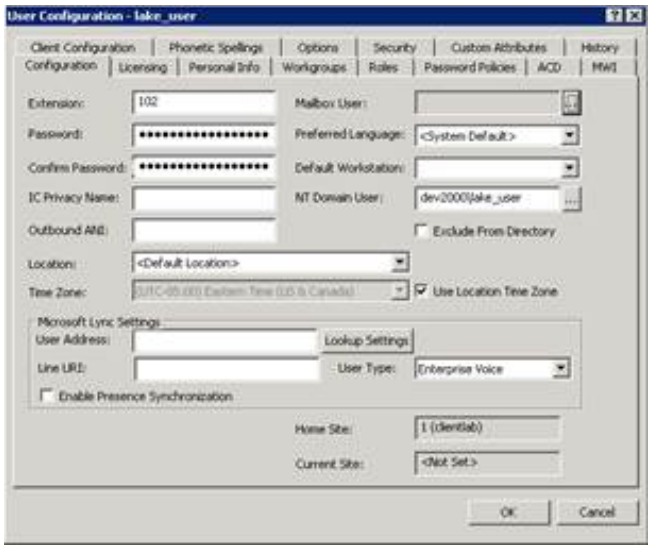
To address this issue, complete one or both the following procedures:

- Verify that a valid CIC user account is entered for the Windows NT domain user.
- Verify that DCOM is enabled.

To verify that a valid CIC user account is entered for the Windows NT domain user:

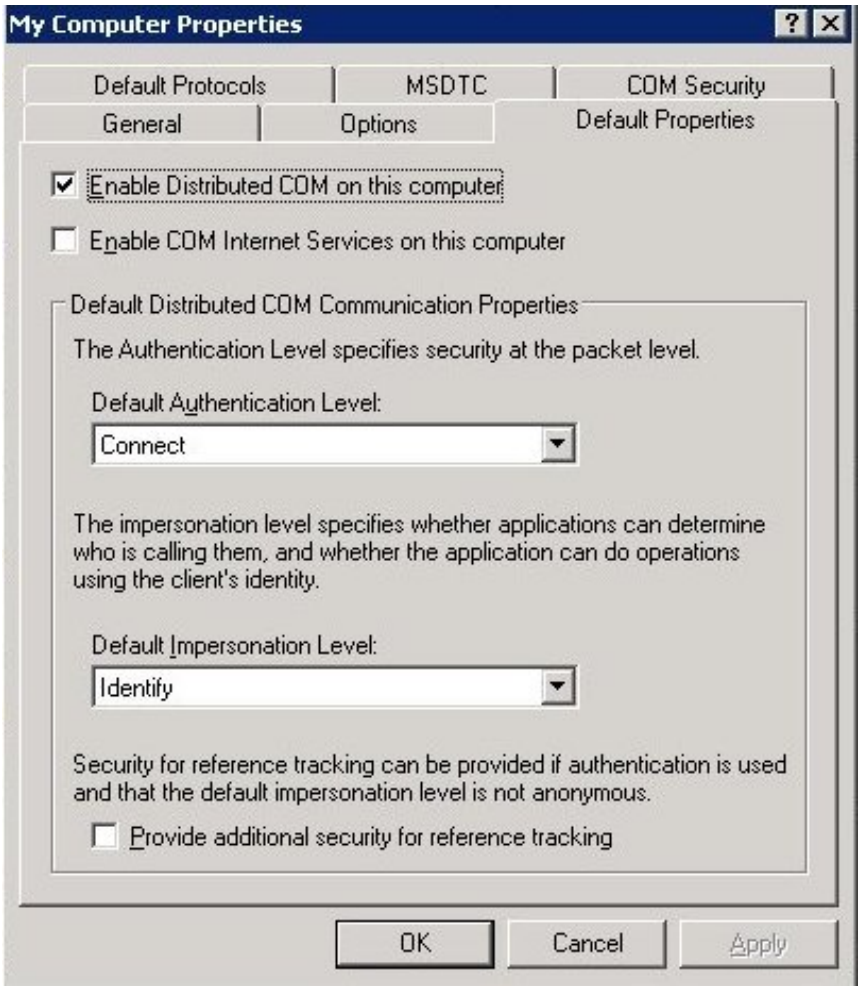
1. In Interaction Administrator, in the **User Configuration** dialog box, click the **Configuration** tab.
2. Verify that the correct user name appears in the **NT Domain User** box.

The following example shows the CIC administrator account and the Windows NT domain user under which the CIC service is running are `lake_user`.



To verify that DCOM is enabled:

1. From the **Start** menu, run `dcmcnfg`.
2. Click **Component Services,** point to **Computers**, and then click **My Computer**.
3. Right-click and then click **Properties.**
4. Click the **Default Properties** tab.
5. Verify that **Enable Distributed COM** is selected on this computer.



Problems with the Switchover system running improperly

This section addresses why the Switchover system is not running properly.

Why aren't changes replicating?

The Switchover system isn't running on the backup computer

If the Switchover system isn't running in **Backup** mode on any computer, replication does not occur. This can be caused by either of the following conditions:

- The Switchover system is running in **Active** mode on the backup server.
- The Switchover system is not starting on the backup server.

Switchover encountered an error during replication

Check the event log for any errors that the Switchover system may have encountered. If an unexpected error occurred, the event log may contain the following entry:

```
SelfMonitor - Detected xxx thread stop. Contact Support.
```

Why didn't a switchover occur?

A non-monitored subsystem is causing the problem

The Switchover system monitors the following conditions to determine whether a switch should occur:

- **TS ping** — to determine if TS or Notifier has stopped, lost its connection, or is so unresponsive that it can no longer handle requests.

It is possible that another subsystem, such as IP, has problems that are severe enough to render the server unusable. However, the Switchover system does not start a switchover because the subsystems that it monitors are responding correctly.

A restart of the backup server hasn't completed

A restart of the backup server hasn't completed or a critical subsystem is not running on the backup server.

A switchover does not occur while the backup server is starting or if a critical subsystem is not running on the backup server.

There is no backup server

Most often a switchover does not occur because the Switchover system is not running. After a switchover, there remains one active computer and one *stale* computer. The *stale* computer is inactive, but it is not in **Backup** mode. Therefore, it is not watching the active computer.

To address this issue, verify this scenario using one of these methods:

- Check the application event logs on both servers for successful starts of the Switchover system in the backup role. Verify that there have been successful switchovers. Form a timeline of the events.
- Use the Switchover Control Panel.

To make the *stale* computer resume watching the active computer, restart the *stale* computer.

Why didn’t things come up after a switch occurred?

Did a switchover occur?

In some cases, a switchover was not even attempted.

To address this issue:

Check the event log to verify that a switchover was attempted. It is possible that a failure occurred while the Switchover system was not running. Therefore, a backup computer is not running now. If this is the case, determine why a switchover did not occur.

Why do certain lines and stations fail to work after a switch?

Line and station configurations are not correct after the switchover.

To address this issue:

Verify that the line and station configurations are correct in Interaction Administrator after the switchover. Attempt to deactivate and then reactivate the problematic line or station. Check the TS log for errors.

Why did a switchover occur?

The event log is the fastest way to determine why a switchover occurred. Be sure to check the event log on both computers. If the backup server can still communicate with the active server, it updates the event log on the active server. Otherwise, it updates the event log only on the backup server.

After each switchover, you should examine the **Switchover subsystem log from the Backup server** for an entry that contains “Switchover Service: Switch Initiated.” Immediately before this entry should be a message that states why the switchover occurred. It can be one of the following:

- **TS Ping Failure** - The Switchover system lost communications with TSServer on the active computer.
- **Manual Switchover** - Something other than standard diagnostics started the switchover. For example:
  - The watchdog timer or hardware tests on TSServer
  - A user who used the Switchover Control Panel

TS Ping Failure

The Switchover system lost communications with TSServer on the active computer.

This occurs when TSServer sent a TSP packet, and it failed to make it to the backup computer.

To address this issue:

Check the TS log on the active server to determine what it was doing at the time. If you don’t see the ping request, check for more information in the Notifier log if the NOTIFIERLIB subtopic is at NOTES (80) or higher.

Here is a sample of a TS ping failure, taken from the backup Switchover log on the backup server:

Time	Topic	Message
14:40:**00**.402	SystemMonitor	[Enter] PingModule::ModuleByName::Ping: TsServer error count=0 timeout=**10000**
14:40:**10**.452	SystemMonitor	[Error] error pinging TsServer count=1
14:40:10.452	SystemMonitor	[Error] error in ping count=**1**
14:40:**10**.452	SystemMonitor	[Error] scheduling retry in **1000** ms
14:40:**11**.453	SystemMonitor	[Enter] PingModule::ModuleByName::Ping: TsServer error count=1 timeout=**10000**
14:40:21.483	SystemMonitor	[Error] exceeded max error count - signaling system down
14:40:**21**.503	SystemMonitor	[Error] error in ping count=**2**
14:40:21.503	SystemMonitor	[Error] maximum error count reached - not scheduling retry
14:40:21.543	Switchover	[Enter] SwitchoverState::StateBackup: event=eTSDown
14:40:21.543	Switchover	[Error] SwitchoverMain::StatusMessage: Backup server switching to primary mode

Note:
In this example the two pings are failures; the first ping fails, and after a one-second sleep, a second attempt fails. After the second failure, a switch is attempted 21 seconds after the first ping transmission.

Manual Switchover

Something other than the Switchover system's standard diagnostics started the switchover.

For example:

- The watchdog timer or hardware tests on TSServer forced the switchover through its own diagnostics.
- A user forced the switchover using the Switchover Control Panel.

To address this issue:

To determine if TS forced the switchover, check the TS log on the computer that was formerly the active server around the time this switchover occurred. The following entries illustrate how the time of a switchover is indicated in the TS log.

Time	Topic	Message
20:26:52.069	Switchover	[Enter] SwitchoverState::StateBackup: event=eInternalSwitchReq
20:26:52.069	Switchover	[Error] SwitchoverMain::StatusMessage: Backup server switching to primary mode

Often you need to find specific details about a switchover, such as the exact time it occurred.

1. Open the Switchover log file on the computer that was the backup server before the switchover occurred.
2. Near the end of the file, search for `Initiating Connections Switch`.
3. Just before this line, you should see a line that indicates why the backup computer switched over.

Problems noticed after a switchover occurs

Agent ACW statuses do not switch to Available after the specified ACW period ends

If an agent in an ACD queue is in an ACW status at the time a switchover occurs, the status of the agent is not automatically set to Available after the specified ACW period ends.

To address this issue:

The agent has to change his or her status to **Available** manually. Supervisors should check for agents who have forgotten to change their statuses after the switchover event.

Problems noticed with interaction recovery

Automatic status changes do not operate as expected

Automatic status changes linked with the handling of ACD interactions may not operate as expected following a switchover. For example, agents in an on-call status at the time of a switchover may not automatically return to Available when their current interaction is disconnected and will need to manually change their status.

To address this issue:

The next time the agent receives an ACD interaction, the automatic status changes should resume as expected.

Win32 CIC client programs outside the LAN cannot re-connect

When you configure your switchover servers, the server names you specify are NetBIOS names. For example, IndyServer1. For each NetBIOS name, there is a corresponding FQDN (fully-qualified domain name) that identifies the exact location of the server on your network. If necessary, you can also use a command line switch to specify the name of the FQDN of the server.

Beginning with 2015 Release 2, when a CIC client machine successfully connects to the switchover server, either the NetBIOS or FQDN versions of the server name are cached on the CIC client machine, depending on which form was used to connect. When the server attempts to connect, the client tries the most recently used server first and then the other in the case of a failure. This simplifies things for the user in the case of a Switchover event because the user does not have to manually specify which server to connect to.

If for some reason the FQDNs of the switchover servers cannot be detected or are detected improperly, you can use the **ForceSwitchoverFQDNs**, **SwitchoverServerFQDN A** and **SwitchoverServerFQDN B** parameters to force the switchover system to return the server names to the CIC client so they can be properly cached. For more information, see "Required Switchover Server parameters".

SMS chats are not retained during a switchover

If SMS chats are not retained during a switchover, and the **SMS Interaction Recovery Enabled** server parameter is set, it may be because the broker is disabled or does not have an outbound route configured. This can happen if the broker's contract has been terminated, or if the configuration of either the proxy or broker has been changed. Both of these situations are beyond the control of CIC.

To address this issue:

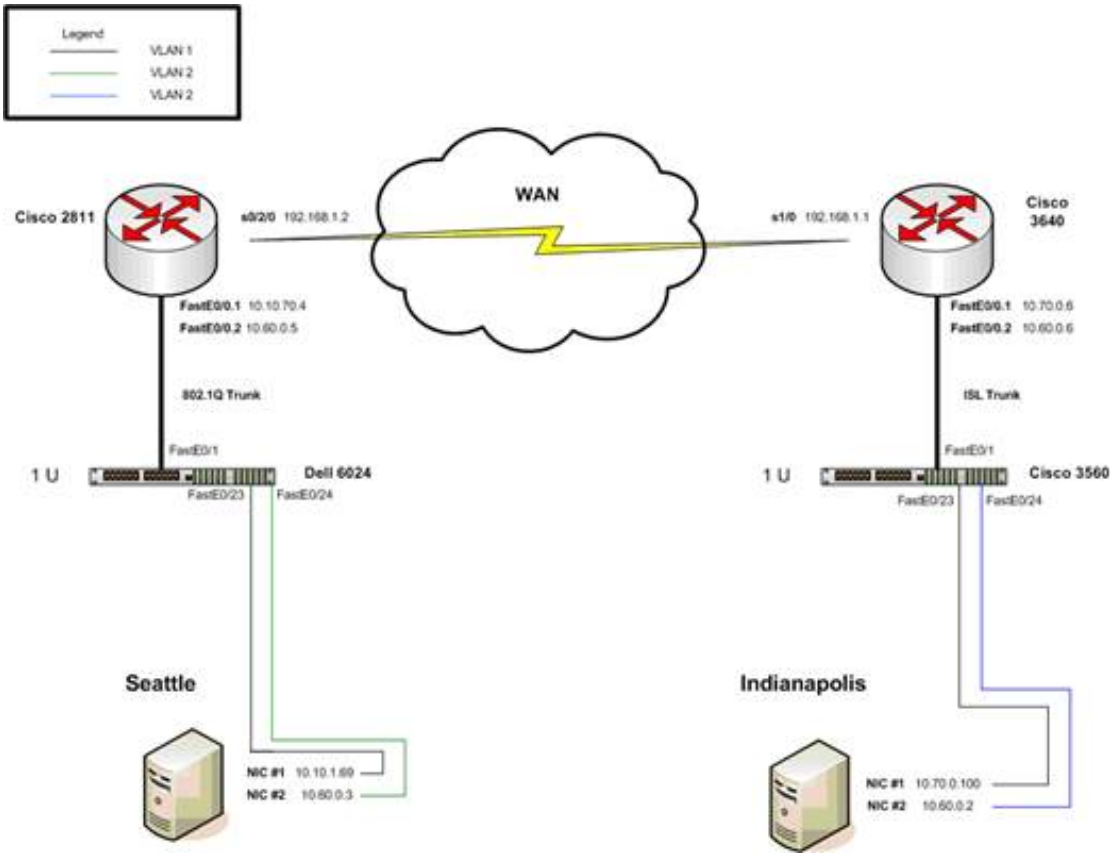
Review the SMS log to determine why the route was not recreated or why the send was unsuccessful.

Appendix A: Additional WAN Switchover Configuration

The "Configure Switchover in WAN environments" section in this document discusses the **NetTest** server parameters and additional suggestions for reducing false positives for switchover pairs in a WAN environment.

This appendix illustrates a sample WAN switchover configuration and provides the configuration procedures for VLANs, switch trunking, ISL/802.1Q sub-interfaces, static routes, and QoS.

Sample WAN Switchover configuration



This diagram illustrates a sample WAN switchover configuration for one side of the network. The same configuration is required for the other side of the network. Configure the following components:

- VLANs
- Switch trunking
- Subinterfaces on the router for the encapsulation
- Static routes
- Quality of Service (QoS)

VLANs

This section describes Virtual Local Area Network (VLAN) configuration with Cisco switches and Dell switches.

Cisco switches

Separate subnets are used, so that routing is handled correctly. Use a layer 3-capable switch and create the subnets on different VLANs. Then route the Secondary NIC on the CIC servers (10.60.0.2 and 10.60.0.3) over the WAN so that they can communicate. It is not necessary for the CIC servers to reside in the same numeric VLAN.

To create VLANs with different subnets:

In the switch CLI (telnet or other connection), enter the following configuration commands, one on each line. End with `Ctrl+Z`.

```
3560# configure terminal
3560(config)# int vlan 1
3560(config-if)# ip address 10.70.0.1 255.255.0.0
3560(config-if)# exit
3560(config)# ip default-gateway 10.70.0.6
3560(config)# end
3560(config)# int vlan 2
3560(config-if)# ip address 10.60.0.1 255.255.0.0
3560(config-if)# exit
```

In this example, two VLANs are created and assigned a subnet range of 10.70.*x.x.* and 10.60.*x.x.* Also a default gateway is created for the switchover.

Place the port that is connected to your SwitchoverServer NIC into its own VLAN. In this example, the SwitchoverServer is using FastEthernet 0/24. FastEthernet 0/24 plugs into the CIC servers Second NIC (Example 10.60.0.2)

```
3560(config)# int fastEthernet 0/24
3560(config-if)# switchport access vlan 2
```

You can place the primary NIC on VLAN 1 as you normally do (Example: FastEthernet 0/23).

Dell switches

Separate subnets are used, so that the routing is handled correctly. Use a layer 3-capable switch and create the subnets on different VLANs. Then route the Secondary NIC on the CIC servers (10.60.0.2 and 10.60.0.3) over the WAN so that they can communicate. It is not necessary for the CIC servers to reside in the same VLAN.

To create VLANs with different subnets:

```
console>enable
console# configure
console(config)# vlan database
console(config-vlan)# vlan 2
console(config-vlan)# exit
```

With Dell, create the VLAN before giving it an IP Address in the VLAN Database:

```
console(config)# int vlan 2
console(config-if)# ip address 10.60.0.1 255.255.0.0
console(config)# int ethernet g24
console(config-if)# switchport access vlan 2
```

Switch trunking

This section describes switch trunking configuration with Cisco switches and Dell switches.

Cisco switches

Enable trunking on the switchover so that the Switchover system can talk to the router. Use a subinterface on the router so that the switchover connection does not require a dedicated WAN interface. By using a subinterface, you can use the existing connection and encapsulate the subnets.

Cisco uses ISL but can also use IEEE standard 802.1Q. Both have been tested.

Enable the trunk on the switch that connects to the router's Fast Ethernet port. In this example, the router's Ethernet port is FastEthernet 0/0:

```
3560# configure terminal
3560(config)# int fastEther0/1
3560(config-if)# switchport mode trunk
```

Next enter the trunking encapsulation. Use ISL on Cisco Switches. This example also adds the VLANs to trunk on the port.

```
3560(config-if)# switchport trunk encapsulation isl
3560(config-if)# switchport trunk allowed vlan all
3560(config-if)# exit
```

Dell switches

Enable trunking on the switchover so that the Switchover system can talk to the router. Use a subinterface on the router so that the switchover connection does not require a dedicated WAN interface. By using a subinterface, you can use the existing connection and encapsulate the subnets.

This example uses IEEE standard 802.1Q:

```
console> en
console# configure
console(config)#
console(config)# interface ethernet g1
console(config-if)#
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add

all
```

ISL/802.1Q subinterfaces

This section describes how to configure subinterfaces on the router for encapsulation.

This example is for a Cisco Catalyst 3640:

```
2811# configure terminal
```

Enter configuration commands, one on each line. End with `Ctrl+Z`.

This configuration is using the Fast Ethernet connection on the router that is connected to the Switch Trunk port from the preceding trunking section. Also select FastEthernet 0/0 for the trunk configuration. This connector plugs into the Switch-port FastEthernet 0/1.

Notice that no IP address is specified on the main interface.

```
Cat3640(config)# int FastEthernet 0/0
Cat3640(config-if)# no shut
Cat3640(config-if)# exit
```

Enable trunking on the subinterface FastEthernet 0/0.1.

The actual trunks are configured on the subinterfaces.

```
Cat3640(config)# int FastEthernet 0/0.1
```

Enter the trunking encapsulation as either ISL or dot1q (if you were working with a Dell switch for instance)

```
Cat3640(config-subif)# encapsulation isl 1
```

Give the subinterfaces IP addresses for routing over the network. Configure L3 information on the subinterface 0/0.1.

```
Cat3640(config-subif)# ip address 10.70.0.6 255.255.0.0
Cat3640(config-subif)# exit
```

This address (10.70.0.6) is the Default Gateway for VLAN1.

Now enable trunking on the subinterface FastEthernet 0/0.2.

```
Cat3640(config)# int FastEthernet 0/0.2
Cat3640(config-subif)# encapsulation isl 2
```

Enter the trunking encapsulation ISL. Notice that this trunking matches the second VLAN on the switch that is being routed. Again, if this trunking was for working with a Dell switch, the encapsulation would be `dot1q`.

Configure L3 information on the subinterface 0/0.2:

```
Cat3640(config-subif)# ip address 10.60.0.6 255.255.0.0
Cat3640(config-subif)# exit
Cat3640(config)# ^Z
```

This address (10.60.0.6) is the Default Gateway for VLAN2.

You can check the configuration to make sure that you have 2-way communication with the following command:

```
Cat3640# show vlans

Virtual LAN ID: 1 (Inter Switch Link Encapsulation)
   vLAN Trunk Interface:   FastEthernet0/0.2
   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.70.0.6               274083             164096
Virtual LAN ID:  5 (Inter Switch Link Encapsulation)
   vLAN Trunk Interface:   FastEthernet0/0.1
   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.60.0.6               370687             623107
Cat3640#
```

Configuring a Dell switch trunk port requires 802.1Q encapsulation, as shown in this example:

```
Delta# show vlans

Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)
   vLAN Trunk Interface:   FastEthernet0/0.1
```

This switch trunk port is configured as native VLAN for the following interface(s):

```
FastEthernet0/0
   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.10.70.4             1881760             483783
        Other                                          0               8027
   1890808 packets, 554876237 bytes input
   491810 packets, 110471839 bytes output
Virtual LAN ID:  5 (IEEE 802.1Q Encapsulation)
   vLAN Trunk Interface:   FastEthernet0/0.2
   Protocols Configured:   Address:              Received:        Transmitted:
           IP              10.60.0.5               977968             495206
        Other                                          0              20078
   977968 packets, 680607031 bytes input
   515284 packets, 115591709 bytes output
```

Static routes

If necessary, you can create static routes for the router to send the switchover traffic to the other side of the router. In the sample illustration in this appendix, the output shows a static route from the Switchover system (10.60.0.2) going to the Switchover system on the other side of the router (10.60.0.3). This route tells the router to send this match out the serial link. The following command is an example of how to add a static route:

```
2811(config)# ip route 10.60.0.3 255.255.255.255 Serial0/2/0
```

Adding the next hop at the end is also optional, but not done in this example. A route is needed on the other side for the inverse when 10.60.0.2 needs to be able to find 10.60.0.3.

```
  Delta# show ip route
  Codes: C - connected, S - static, R - RIP, M - mobile,

B - BGP
         D - EIGRP,

EX - EIGRP external, O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA

external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external

type 1, E2 - OSPF external type 2
         i - IS-IS,

su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
         ia - IS-IS

inter area, * - candidate default, U - per-user static

         route
         o - ODR, P

- periodic downloaded static route
  Gateway of last resort is 10.10.0.1 to network 0.0.0.0
   *   10.0.0.0/8 is variably subnetted,

10 subnets, 3 masks
  C       10.10.0.0/16

is directly connected, FastEthernet0/0.1
  R       10.8.1.0/24

[120/1] via 10.10.0.1, 00:00:22, FastEthernet0/0.1
  R       10.0.0.0/16

[120/1] via 10.10.0.1, 00:00:22, FastEthernet0/0.1
  R       10.6.1.0/24

[120/1] via 10.10.0.1, 00:00:22, FastEthernet0/0.1
  R       10.1.6.0/24

[120/1] via 10.10.0.1, 00:00:22, FastEthernet0/0.1
  R       10.20.0.0/16

[120/1] via 10.10.0.1, 00:00:22, FastEthernet0/0.1
  S       10.60.0.6/32

is directly connected, Serial0/2/0
  S       10.60.0.3/32

is directly connected, Serial0/2/0
  C       10.60.0.0/16

is directly connected, FastEthernet0/0.2
  S       10.70.0.0/16

[1/0] via 192.168.1.1, Serial0/2/0
  C    192.168.1.0/24 is directly connected,

Serial0/2/0
  S*   0.0.0.0/0 [1/0] via 10.10.0.1, FastEthernet0/0.1
  2811#
```

A default route is also required. A good way to establish a default route with a subinterface is as follows:

```
  2811(config)# ip route 0.0.0.0 0.0.0.0 FastEthernet0/0.1

10.10.0.1
```

Notice that the next hop was added so that the traffic knows where to go when it uses the subinterface.

Quality of Service (QoS)

Switchover traffic is limited to one subnet (10.60.0.0 in this case). You can use QoS to identify and manage the data flow. The following configurations are required on both sides of the router:

Classifying

```
  CatCat3640> en
  CatCat3640# config t
  CatCat3640(config)# access-list 101 permit ip 10.60.0.3

0.0.0.0 10.60.0.2 0.0.0.0
  CatCat3640(config)# access-list 101 permit ip 10.60.0.2

0.0.0.0 10.60.0.3 0.0.0.0
  CatCat3640(config)# class-map switchover-traffic
  CatCat3640(config-cmap)# match access-group 101
```

This example shows how to use an access list to classify traffic from the secondary NICs on the Switchover systems. To ensure that both sides are marking the packets, complete this work on both sides of the routers.

Marking and reserving bandwidth

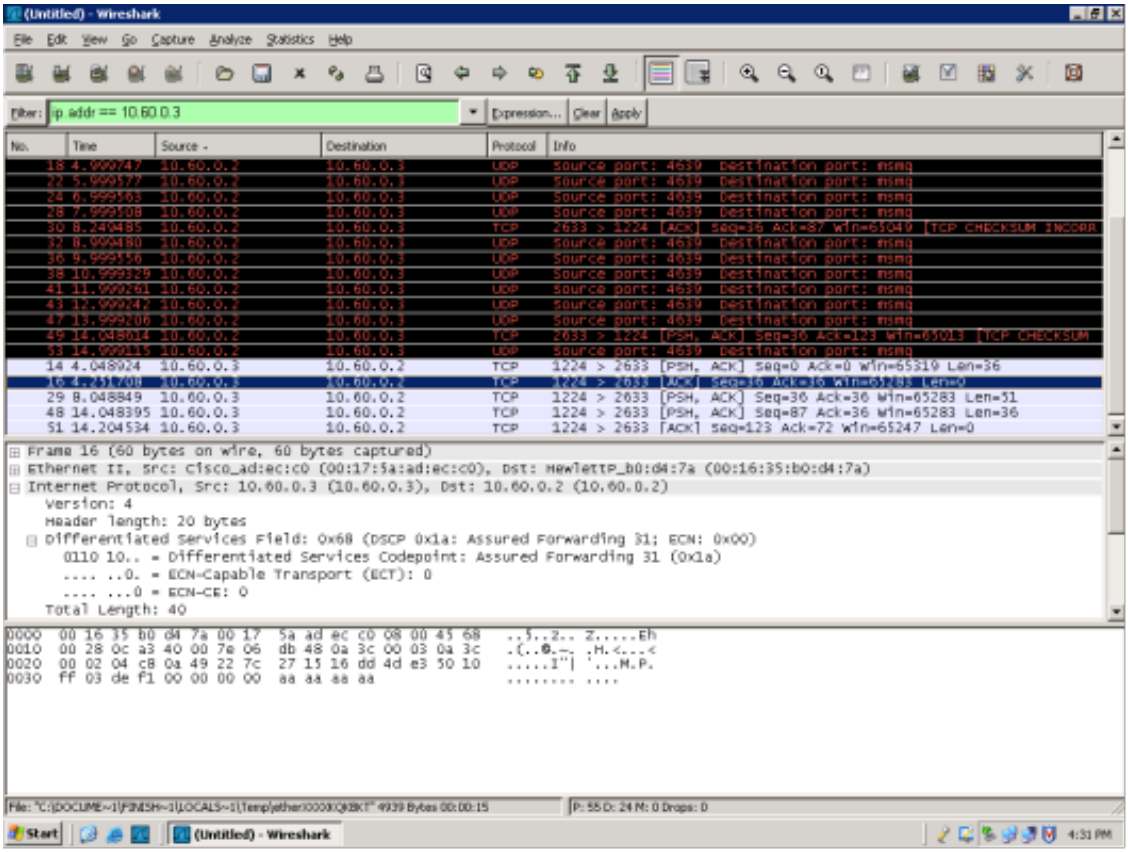
```
  CatCat3640(config)# policy-map switchover
  CatCat3640(config-pmap)# class switchover-traffic
  CatCat3640(config-pmap-c)# bandwidth 1024
  CatCat3640(config-pmap-c)# set dscp af31
  CatCat3640(config-pmap-c)# exit
  CatCat3640(config-pmap)# class class-default
  CatCat3640(config-pmap-c)# fair-queue
  CatCat3640(config-pmap-c)# random-detect
  CatCat3640(config)# int serial 1/0
  CatCat3640(config-if)# service-policy output switchover
  CatCat3640# show policy-map interface serial 1/0 output
```

In this example, a policy map is created and the switchover-traffic class is configured so that traffic is marked and 1 megabit of bandwidth is reserved for the link. The policy is confirmed by using the `show` command:

```
  Cat3640# show policy-map interface serial 1/0 output
   Serial1/0
    Service-policy output: switchover
      Class-map: Switchover (match-all)
        350028 packets, 71328923

bytes
        5 minute offered

rate 90000 bps, drop rate 0 bps
        Match: access-group

101
        Queueing
          Output

Queue: Conversation 265
          Bandwidth

1024 (kbps) Max Threshold 64 (packets)
          (pkts

matched/bytes matched) 30742/45374387
          (depth/total

drops/no-buffer drops) 0/0/0
        QoS Set
          dscp

af31
```

```
            Packets

marked 350028
      Class-map: class-default (match-any)
        148854 packets, 16748633

bytes
        5 minute offered

rate 0 bps, drop rate 0 bps
        Match: any

   Queueing
          Flow

Based Fair Queueing
          Maximum

Number of Hashed Queues 256
          (total

queued/total drops/no-buffer drops) 0/0/0
           exponential

weight: 9
    class    Transmitted      Random

drop      Tail drop    Minimum

Maximum  Mark
             pkts/bytes       pkts/bytes

      pkts/bytes    thresh

 thresh  prob
        0  148855/16748938        0/0             0/0           20      40  1/10


        1       0/0               0/0             0/0           22      40  1/10
        2       0/0               0/0             0/0           24      40  1/10
        3       0/0               0/0             0/0           26      40  1/10
        4       0/0               0/0             0/0           28      40  1/10
        5       0/0               0/0             0/0           30      40  1/10
        6       0/0               0/0             0/0           32      40  1/10
        7       0/0               0/0             0/0           34      40  1/10
     rsvp       0/0               0/0             0/0           36      40  1/10
```

You can use a tool such as Wire Shark to examine the packets that pass through the router to ensure that the policy is working correctly. In the following example, the packets are marked with `AF31` priority.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr == 10.60.0.3
Expression... Clear Apply
No. Time Source Destination Protocol Info
18 4.999747 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
22 5.999577 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
24 6.999363 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
28 7.999508 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
30 8.249485 10.60.0.2 10.60.0.3 TCP 2633 > 1224 [ACK] Seq=36 Ack=87 Win=65049 [TCP CHECKSUM INCORR
32 8.999480 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
36 9.999536 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
38 10.999329 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
41 11.999261 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
43 12.999242 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
47 13.999206 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
49 14.048614 10.60.0.2 10.60.0.3 TCP 2633 > 1224 [PSH, ACK] Seq=36 Ack=123 Win=65013 [TCP CHECKSUM
53 14.999115 10.60.0.2 10.60.0.3 UDP Source port: 4639 Destination port: msmq
14 4.048924 10.60.0.3 10.60.0.2 TCP 1224 > 2633 [PSH, ACK] Seq=0 Ack=0 Win=65319 Len=36
16 4.251708 10.60.0.3 10.60.0.2 TCP 1224 > 2633 [ACK] Seq=36 Ack=36 Win=65283 Len=0
29 8.048849 10.60.0.3 10.60.0.2 TCP 1224 > 2633 [PSH, ACK] Seq=36 Ack=36 Win=65283 Len=51
48 14.048395 10.60.0.3 10.60.0.2 TCP 1224 > 2633 [PSH, ACK] Seq=87 Ack=36 Win=65283 Len=36
51 14.204534 10.60.0.3 10.60.0.2 TCP 1224 > 2633 [ACK] Seq=123 Ack=72 Win=65247 Len=0
Frame 16 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Cisco_ad:ec:c0 (00:17:5a:ad:ec:c0), Dst: HewlettP_b0:d4:7a (00:16:35:b0:d4:7a)
Internet Protocol, Src: 10.60.0.3 (10.60.0.3), Dst: 10.60.0.2 (10.60.0.2)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x68 (DSCP 0x1a: Assured Forwarding 31; ECN: 0x00)
0110 10.. = Differentiated Services Codepoint: Assured Forwarding 31 (0x1a)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 40
0000 00 16 35 b0 d4 7a 00 17 5a ad ec c0 08 00 45 68 ..5..z.. Z.....Eh
0010 00 28 0c a3 40 00 7e 06 db 48 0a 3c 00 03 0a 3c .(..@.~. .H.<...<
0020 00 02 04 c8 0a 49 22 7c 27 15 16 dd 4d e3 50 10 .....I"| '...M.P.
0030 ff 03 de f1 00 00 00 00 aa aa aa aa ....
P: 55 D: 24 M: 0 Drops: 0
Start
(Untitled) - Wireshark
4:31 PM

Appendix B: Applying a release to switchover servers

This procedure describes how to apply a release to switchover servers running CIC 4.0, including CIC 2015 R1 and higher. This differs from the procedure for earlier releases of CIC.

In CIC, updates can be pushed out using a feature called Interactive Updates. Each CIC server operating in a switchover environment contains an Interactive Update Client Configuration application. You must use this application to configure how the CIC server pulls the updates from the provider server.

Genesys recommends configuring the Update Configuration on the CIC client to download the updates automatically. You then install the updates manually.

This process causes some server downtime. The downtime is minimal, but the process allows for the installation to be done on one or both of the CIC servers in the switchover pair.

This example uses server names Server A and Server B. Assume that Server A is running in primary mode, and Server B is running in backup mode.

Further, assume that Server A and Server B are completely synced before the release is installed (that is, Server B is a valid backup server when this process is started). In IC 4.0 SU 1 and later, complete syncing between the servers occurs only when they are both on the same build release.

Note:
This procedure refers to steps necessary for sites that use Interaction Process Automation (IPA). For more information on the "persistence directory", see *Interaction Process Automation Technical Reference* in the PureConnect Documentation Library.

Upgrading Windows on the switchover pair

If you upgrade the switchover pair to a different release of Windows during the upgrade process, be aware of the following things:

- **EXTREMELY IMPORTANT:** The primary and backup server must have identical network adapter names.
- **CAUTION**: This scenario could cause loss of data due to the nature of the upgrade method. For more information about possible data loss, and how to configure which data is replicated, see "Appendix C".
- You do not have to re-run Setup Assistant on the primary server. This would result in downtime, so you should avoid re-running it. However, in order to avoid re-running it, the computer name of the backup server **must** remain the same throughout the upgrade process. This allows the Server Group certificate information from the primary server to remain correct.
- The same domain user that was used to set up the primary server must also be used to set up the backup server.

Applying a release to CIC switchover servers for releases CIC 2015 R1 and greater

1. Stop the CIC service on Server B.
2. Set the CIC service to manual on Server B.
3. Run the release install on Server B.
4. Restart Server B.
5. Start CIC Service on Server B.
   Server B comes up as backup in **upgrade state higher**.
6. Open the Switchover Control Panel on Server A from the Start Menu (**Start > All Programs> PureConnect> Switchover**) and verify that Server A is the active server and Server B is the backup server, running in **upgrade state higher**.
7. Click **Switch**.
   Server B becomes the new Active server. (Minimal downtime begins while services switch over to the Backup server.)
8. Restart Server A and start the CIC Service, if you want to have it available for a manual switchover.
9. Test the functionality on Server B with the updated release. Make sure that you are satisfied with it before proceeding.
10. Determine whether release performance is acceptable:
    a. If you are satisfied with the new release on Server B, stop the CIC Service on Server A, install the new release, and then start the CIC service. Server A comes up in **Backup** mode.
    b. If not satisfied with the new release, open the Switchover Control Panel and press the **Switch** button. Server A becomes the primary server running the old release.
11. Set CIC service on Server B to **Automatic** mode.

The following chart illustrates the sequence of these steps on each server.

Server A (primary)	Server B (backup)
	1. Stop the CIC service.
	2. Apply the release.
	3. Restart the server.
	4. Start the CIC service backup in **upgrade state higher**.
5. Open Switchover Control Panel	
6. Click **Switch**.	The server becomes the active server.
During this time there is a short downtime.	
7. Restart the CIC service.	
8. Test the release functionality.	
9. Do the following: a. Apply the release and restart Server A (backup) b. Click **Switch**.	
	10. Set CIC to "auto".
Server A (backup) with release	Server B (primary) with release

Appendix C: About the limited replication of data during an Upgrade state

Upgrade states on the backup server

When you start a backup server against a primary server, the Switchover system on the backup server automatically enters one of the following **Upgrade** states if the releases on the servers are different.

Release on the primary server	Release on the backup server	Backup server upgrade state
Older	Newer	**Upgrade state higher**
Newer	Older	**Upgrade state lower**

Note:
The Switchover Control Panel indicates whenever a backup server enters either **Upgrade** state, as well as the reason why it entered **Upgrade** state.

How data is replicated when the servers are on different releases

When the backup server is in the **Upgrade state higher**, almost all data on the primary server is replicated except for those items that you specifically opt-out. User DS data, user status, and all folders that you specify in the **CustomMirrorDir** parameter are replicated. Handlers are **not** replicated in either Upgrade mode.

When the backup server is in **Upgrade lower state**, only the data that you specifically opt-in are replicated.

For more information on how to designate opt-in and opt-out data, see "Server parameters for customizing how data is replicated".

While Switchover is in **Upgrade** state active monitoring of the primary server does not occur; therefore automatic switchovers do not occur. The Switchover Control Panel indicates that the backup server is in "manual switch only" mode.

Server parameters for customizing how data is replicated

Server parameters Upgrade lower state

The following table describes the server parameters that you can use to customize how data is replicated when the switchover servers are in **Upgrade Lower** state.

Note:
These server parameters apply only when the backup server is in the **Upgrade lower state**.

Server Parameter Name	Description
Custom upgrade synchronization directories	This server parameter includes semicolon-delimited DS paths that you want to replicate. The replication is recursive, so that all objects under the specified paths are replicated. Example value: `${CONFIG}\Users;${CONFIG}\Passwords` By default, this parameter monitors the following DS paths: • `${CONFIG}\Users` • `${CONFIG}\Passwords` • `${CONFIG}\Workgroups` • `${CONFIG}\Roles` • `${CONFIG}\Default User` • `${SERVER}\Workstations` • `${CONFIG}\ProcessAutomation` Use this parameter to specify the paths you want to monitor in addition to the default paths listed above.
Custom upgrade attribute exceptions	By default, this parameter is empty. You can use this server parameter to specify a list of attributes that are **excluded** in the replication process. The list must be a semicolon-delimited list of DS Class names followed by comma-separated attribute names enclosed in parentheses. `Example value: User(Workgroups, Extension);Workgroup(Members, View User Queue List).`
Custom upgrade file synchronization directories	Set this parameter to enable file mirroring of specific directories that you want to replicate. By default, this parameter includes the `+C:\I3\IC\Flows` directory.
Custom upgrade file synchronization exceptions	Use this parameter to specify a different list of exceptions in the **Upgrade** state to apply to the directories that you set in the **Custom Upgrade File Synchronization Directories** parameter. This server parameter works like **MirrorExceptions**. If you do not set this parameter, it defaults to the exceptions that you set in the **MirrorExceptions** parameter.

Server parameters for Upgrade higher state

During the **Upgrade higher** state, all changes on the primary server are replicated to the backup server except for the following exceptions:

- Files and DS entries related to handlers are not replicated.
- Phone DS data is not replicated.
- DS entries that are updated by the install scripts are not replicated.

The following table describes the server parameters that you can use to customize how data is replicated when the switchover servers are in **Upgrade Higher** state.

Server Parameter Name	Description
Switchover Upgrade Higher DS Exclusions	Use this parameter to specify additional DS path exceptions. Use the same format as the **Custom Upgrade Synchronization Directories** parameter. By default, this server parameter is empty.
Switchover Upgrade Higher File Exclusions	Use this parameter to specify additional file directory path exceptions. Use the same format as the **CustomMirrorDir** server parameter. By default, this server parameter is empty.

Caution: Avoid manual switchovers while in either upgrade state

When a switchover pair is in either **Upgrade state higher** or**Upgrade state lower**, the only way a switchover can occur is if it is performed manually. An unexpected, automated switchover cannot occur.

Caution!
You should minimize the time you run CIC servers in either upgrade state higher or upgrade state lower. Avoid running in upgrade state lower whenever possible. While running in either upgrade state, you can lose configuration data and mirrored files.

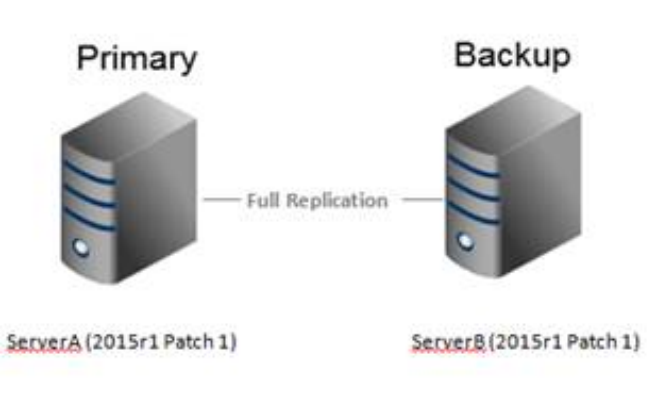
- If you update the backup server to a newer code release, you will be running in the **Upgrade state higher**. Configuration changes that impact the opt-out DS configuration areas and files will not be replicated to the backup server.
- If you switch back to the original primary server while the backup server is running a newer code release, you will be running in **Upgrade state lower**. Only a limited set of configuration data will be replicated. Additionally, only the DS configuration areas and files listed in the opt-in parameters will be replicated.
- In both upgrade states, handler publishes are not replicated. If you are running custom handlers, you should publish those directly onto the backup server after the server is brought up running in **Upgrade state higher**.

Note:
If the backup server is reverted to the previous release of code when it is running in **Upgrade state lower**, any changes made to DS configuration and files that are not replicated as part of the opt-in switchover server parameters are lost.

Example of data loss during a manual switchover while in Upgrade state

The following example illustrates how data could be lost while the servers are in an **Upgrade** state.

Step	Description

Step 1: Both servers are running 2015 Release1 Patch1.	
Step 2: CIC is stopped on ServerB, and 2015 Release 1 Patch 2 is applied. CIC is then started on Server B. ServerB enters the **Upgrade state higher**.	
Step 3: While the servers are in the **Upgrade state higher** some DS configuration data is changed through Interaction Administrator, an IceLib app, or a handler.	DS data will be replicated to the backup server as long as it is not excluded by a class or attribute identified in the opt-out switchover server parameter, **Switchover Upgrade Higher DS Exclusions**. Changes to files in the CustomMirrorDir paths will be replicated unless they are excluded by the opt-out switchover server parameter, **Switchover Upgrade Higher File Exclusions**. Handler publishes on the primary are not replicated to the backup. Any custom handlers needed on the updated backup should be published with a connection directly to the backup server before manually switching to this server. For more information on the default values of the server parameters, see "Server parameters for customizing how data is replicated".
Step 4: An administrator performs a manual switchover, and ServerB becomes the primary server. CIC is restarted on ServerA, so it is now the backup server running in the **Upgrade state lower**.	

Step 5: While the servers are in the **Upgrade state lower** some DS configuration data is changed through Interaction Administrator, an IceLib app, or a handler.	This DS data will **not** be replicated to the backup server unless it is a DS path identified in the opt-in switchover server parameters, **Custom Upgrade Synchronization Directories** and **Custom Upgrade attribute exceptions**. Changes to files in the CustomMirrorDir paths will not be replicated unless they are included in the opt-in switchover server parameter, **Custom Upgrade file synchronization directories**. Handler publishes on the primary are not replicated to the backup. For more information on the default values of the server parameters, see "Server parameters for customizing how data is replicated".
Step 6: An administrator performs a manual switchover. ServerA becomes the primary server running the old release. CIC on ServerB is restarted, and it becomes the backup server running in the **upgrade state higher**.	Any changes made while in the **upgrade state lower** that were not included in the opt-in server parameters will be lost.

Appendix D: Interaction Process Automation (IPA) and switchover

Interaction Process Automation (IPA) extends existing IP communications technology to encompass process automation.

For more information about IPA architecture, components, licensing, and related topics, see *Interaction Process Automation Technical Reference* in the PureConnect Documentation Library.

For more information, see *Interaction Process Automation Technical Reference*.

Change Log

The following changes have been made to this document since Interaction Center 4.0 product availability.

Date	Change
19-March-2012	• In "CIC Switchover system processes and architecture", added Switchover States section. • In "Install and configure a new CIC Switchover system" under Optional Switchover Server Parameters, updated the Switchover Use QoS For Ping server parameter. • In "CIC Switchover system operation and additional installation/update procedures" under Additional suggestions for reducing false positives , updated the list to include "Switchover Ping on Aux Connection" and "Switchover Use QoS For Ping". • "Troubleshooting", under Why didn't a Switchover occur, removed issue: The monitored subsystem was restarted quickly. • Appendix B, Interaction Process Automation (IPA) and Switchover, renamed this section to Appendix C. • Appendix B, Upgrade State and Switchover, added this section. • Updated copyright statement.
27-February-2013	• In Introduction, added information about functional changes in IC 4.0 SU 3. • Added Appendix B for applying service updates. Old Appendix B became C, and so forth.
09-April-2013	• In "CIC Switchover system operation and additional installation/update procedures," under Manually start a Switchover from the command line, added statement about the Remote Control User right with respect to forcing a backup. • In Appendix D, Interaction Process Automation (IPA) and Switchover, updated the description of the *Interaction Process Automation Technical Reference*.
05-July-2013	• In "CIC Switchover system processes and architecture," added the section Recovery of ACD email, chat, and callback interactions during Switchover. • In "Install and configure a new CIC Switchover system" under Optional Switchover Server parameters, specified that the mail, chat, and callback parameters were added in IC 4.0 SU 3.

20-August-2013	• In Optional Switchover Server parameters:
	  ◦ Updated **CustomMirrorDir** system parameter.
	  ◦ Added the **Switchover Max TS Failures** system parameter.
	  ◦ Added the **Switchover Max UDP Failures** system parameter.
	  ◦ Updated **Switchover UDP Maximum Ping Delay** system parameter.
	  ◦ Added **Enable Switchover Upgrade Mode** system parameter.
	  ◦ Updated **Switchover TS Failure Retry Delay** system parameter.
	  ◦ Updated the **Switchover TS Timeout** system parameter.
	  ◦ Updated **Switchover UDP Maximum Ping Delay** system parameter.
	  ◦ Updated **Switchover UDP Monitor** system parameter.
	  ◦ Added **Switchover UDP Normal Retry Delay** system parameter.
	• Added new section, Dynamic monitoring of system parameters.
	• Updated document formatting to use new template.
	• Ran Acrolinx and updated wording accordingly.

27-January-2014	Updated copyright information
04-February-2014	• Removed **Enable Switchover Upgrade Mode** system parameter. • Updated the "Appendix C" to reflect SU 5 functionality. • Added **Switchover Use WAN Optimizations for DS Sync** parameter. • Added **Switchover Use Compression For DS Sync** parameter. • Added **Switchover DS Request Timeout** parameter. • Added **Switchover Use Compression for DS Request Sync** parameter. • Added **Switchover Use WAN Optimizations for DS Sync** parameter.
23-February-2014	Added the Recovery of statistical data and Tracker Server logging sections.
01-May-2014	Added the **Enable Switchover Upgrade Mode** system parameter.

07-May-2014	Added the **SwitchoverServerFQDN A**, **SwitchoverServerFQDN B**, and **ForceSwitchoverFQDNs** server parameters
20-May-2014	Added a space between Switchover Max TS Failures to address SCR IC-121905

07-July-2014	• Removed all references to UDP.
	• Added section on the Switchover Subsystem Components.
	• Added new system parameters:
	  ◦ **Switchover Primary Monitor Timeout**
	  ◦ **Switchover Primary Monitor Ping Delay**
	  ◦ **Switchover Primary Monitor Retry Ping Delay**
	  ◦ **Switchover Primary Monitor Retry Count**
	  ◦ **Switchover Unreachable Primary Ping Delay**
	  ◦ **Switchover Unreachable Primary Ping Count**
	  ◦ **Switchover Notifier Reconnect Delay**
	  ◦ **Switchover Reconnect Timeout**

14-September-2014	Updated documentation to reflect changes required in the transition from version 4.0 SU 6 to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Interactive Intelligence Product Information site URLs, and copyright and trademark information.
18-September-2014	Addressed SCR IC-125238 by clarifying that the Callback Interaction Recovery Enabled server parameter should be set to a nonzero integer.
26-September-2014	Deleted all references to the **Enable Switchover Upgrade Mode** server parameter. Updated the screenshot for the **Line Configuration** dialog box.
30-September-2014	Added the section, Upgrading Windows on the Switchover pair.
01-December-2014	Updated the description of the Chat Interaction Recovery Enabled parameter regarding SMS resiliency.
04-December-2014	Updated (and renamed) Appendix C: Upgrade state and limited replication of data with information about limited data replication. Added the new section, Caution: Avoid manual switchovers in Upgrade state.
06-December-2014	Updated the Troubleshooting section with, Win32 client programs outside the LAN cannot re-connect.
19-December-2014	Updated the title page to reflect the R2 release and current date.
15-January-2015	Updated the Copyright and Trademark Information
19-January-2015	• Added the section Configuration options for File Monitor Health Checks • Added the parameters **Switchover File Monitor Health Check Interval** and **Switchover File Monitor Health Check Timeout** .
28-April-2015	• Updated the title page with the new logo. Updated the Copyright and Trademark Information. Updated references to "client" to "CIC client." • Corrected the description of the Switchover Disable Gateway Ping system parameter. • Added the Switchover Disable Gateway Ping system parameter to the table of system parameters.
26-May-2015	Updated the section "Effect of a switchover on servers and clients in a 'Pure SIP' configuration" to reflect a more accurate switchover duration (3-5 seconds) and the fact that during a switchover, no calls are disconnected.
29-May-2015	Rewrote Appendix C to reflect current behavior when servers are in different upgrade states.
31-July-2015	Revised index entries
25-August-2015	• Updated the default values of the following parameters: Switchover Ping on Aux Connection, and Switchover DS Request Timeout • Removed the reference to SU5 for Switchover DS Request Timeout parameter because that parameter predated that release. • Removed the parameters Switchover Use Compression for DS Sync, Switchover Reconnect Delay, and Switchover Use WAN Optimizations for DS Sync.

25-September-2015	Added the section, A note about the loss of duration information for interactions.
06-November-2015	Updated the sections, Recovery of chat interactions and Recovery of callback interactions with information about the need to restart the WebProcessor subsystem on the active server and reboot the backup server.
12-November-2015	Added the troubleshooting section, Problems noticed with interaction recovery.
17-December-2015	Added the section, Return the Switchover service to a functioning state after a switch occurs.
17-December-2015	Removed "CIC Switchover system configuration". Reorganized content in other sections for better readability and flow.
03-March-2016	• Updated the Copyright page. • Updated the TS ping failure sample section. • Updated the description of the Switchover Unreachable Primary Ping Count parameter.
08-March-2016	• Added the section Recovery of SMS interactions. • Updated the section, Optional Switchover Server Parameters with the parameter, **SMS Interaction Recovery Enabled**.
09-March-2016	Added the section SMS chats are not retained during a switchover.
06-April-2016	Updated the section Recovery of SMS interactions with the note about the need to configure the **IonNotifier** parameter and the implications for generic SMS objects.
20-April-2016	Updated the Switchover Server Parameters section with a note about the previous name of the **Switchover Reconnect Timeout parameter**.
07-March-2017	• Added the section, File replication warnings. • Reorganized content in the Manually start a switchover on the backup server section. • Removed reference to future software change request in Automatic status changes do not operate as expected. Updated the Copyright page.
29-March-2017	Corrected typo in Win32 CIC client programs outside the LAN cannot re-connect section.
05-June-2017	Updated "Detecting Network Connection Status of the Backup and Primary" section in The Switchover State Machine to clarify steps.
02-August-2017	• Removed from Recovery of SMS interactions section that SMS interactions are recovered only during a manual switchover. • Clarified the description for **Custom Upgrade Synchronization Directories** server parameter in Optional Switchover Server parameters to indicate the paths you specify are replicated in addition to the paths monitored by default.
17-August-2017	Rebranding. Updated references to IC, Interactive Intelligence, CIC, PureConnect. Updated title page and copyright page.
06-September-2017	Updated Why did a switchover occur? section to include that you should examine the Switchover subsystem log from the Backup server for an entry that contains “Switchover Service: Switch Initiated.”
12-January-2018	Conversion to HTML
6-August-2018	Updated Server group certificate and private key topic to include Certificate Signing Option screen of Setup Assistant.