# SIP Server HA Deployment Guide

SIP Server 8.1.1

12/29/2021

# Table of Contents

# SIP Server High-Availability Deployment Guide

Welcome to the *Framework 8.1 SIP Server High-Availability Deployment Guide*. This document introduces you to the concepts, terminology, and procedures that are relevant to SIP Server high-availability (HA) deployment. The information includes, but is not limited to, an overview of SIP Server HA architecture, HA workflows, and SIP Server HA-deployment procedures for Windows and UNIX operating systems.

This document can be used together with the *SIP Server Deployment Guide* during your deployment planning.

Find the information you need from the topics below.

### About the HA Methods

Learn about the different ways you can set up SIP Server HA instances.

IP Address Takeover

Windows NLB

Using SIP Proxy

Network Device-Based HA

### Deploying on Windows

Find procedures to deploy SIP Server HA on Windows servers.

IP Address Takeover

Windows NLB

Using SIP Proxy

TLS Configuration

### Business Continuity

Learn about setting up Business Continuity (BC) in your environment.

Architecture

Call Delivery

Disaster Recovery

### Deploying on UNIX

Find procedures to deploy SIP Server HA on UNIX-based servers.

IP Address Takeover on Linux

IP Address Takeover on AIX

IP Address Takeover on Solaris

Using SIP Proxy

### Advanced Features

Upgrading SIP Server HA Pair

Verifying Initialization Status in Backup SIP Servers

Enhanced HA Resilience for Network Disruptions

### Configuration Options

Consult configuration options that are specific to HA and BC deployments.

HA Configuration Options

BC Configuration Options

# New in This Release

In release 8.1.1, SIP Server HA is enhanced with the following:

- Network status monitoring.
- Recovery after network failure.
- SIP Server itself controls execution of Virtual IP scripts.
- Support of HA using SIP Proxy.
- Support of secure data transfer using TLS.
- Version 8.1.101.29: Support of agents with nailed-up connections in Business Continuity deployments.
- Version 8.1.101.49: Support of Hunt Groups with the parallel distribution strategy (simultaneous ringing) in Business Continuity deployments.
- Version 8.1.101.61: Establishing nailed-up connection on agent login.
- Version 8.1.101.75: Shared Call Appearance is supported in Business Continuity deployments.
- Version 8.1.102.58: Enhanced Procedure for Upgrading SIP Server HA Pair.
- Version 8.1.103.64: Verifying Initialization Status in Backup SIP Servers.
- Version 8.1.103.78: Enhanced disaster recovery solution for outbound calls.

## About SIP Server

SIP Server is the Genesys software component that provides an interface between your telephony hardware and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from, and are sent to, the telephony device. SIP Server is an IP-based server that can also act as a messaging interface between SIP Server clients. It is the critical point in allowing your Genesys solution to facilitate and track the contacts that flow through your enterprise.

## Intended Audience

This document primarily intended for system architects or administrators who are responsible for ensuring that systems, including SIP Server, are highly available. It has been written with the assumption that you have a basic understanding of:

- High-availability architecture
- Network design and operation
- Genesys Framework architecture and functions
- Your own network architecture and configurations

# SIP Server HA Architecture

A high-availability (HA) architecture implies the existence of redundant applications: a primary and a backup. These applications are configured so that if one fails, the other can take over its operations without significant loss of data or impact to business operations.

SIP Server supports several high-availability deployment options:

- IP Address Takeover
- Windows NLB Cluster
- Using SIP Proxy
- Network device-based HA

IP Address Takeover and Windows NLB Cluster HA options utilize the concept of a Virtual IP address. In a Virtual IP interface"based architecture, primary and backup SIP Servers are located on the same subnet, and SIP endpoints and gateways are configured to send SIP messages to SIP Server by using this single Virtual IP address. The Virtual IP address is preserved during switchover occurrences, and messages that are sent to the Virtual IP address are delivered to the SIP Server that is currently running in primary mode.

When the Management Layer detects failure of a primary SIP Server, it executes a set of corrective actions, which allows SIP messages that are destined for the failed primary SIP Server to be delivered to the backup SIP Server that has just started running in primary mode.

While SIP endpoints and gateways use a single Virtual IP address to communicate with SIP Server, Management Layer and Configuration Layer components, and T-Library clients must use a unique IP address for communication with the SIP Server and Local Control Agent (LCA) that is installed at each SIP Server host.

On Windows and UNIX, an IP Address Takeover configuration is implemented by using Virtual IP address control scripts to enable and disable Virtual IP addresses. The Windows NLB configuration uses Cluster control scripts to enable and disable Virtual IP ports.

A network device-based HA is an alternative to software-based HA configurations. The SIP Server and F5 Networks BIG-IP Local Traffic Manager (LTM) integration solution supports this type of HA configuration.

Each of these configurations is described in more detail in the following sections.

The following table summarizes SIP Server HA options, their benefits and limitations, and supported operating systems (Windows, Linux, Solaris, or AIX).

**Comparing High-Availability Options**

| HA Option | Benefits | Limitations |
|---|---|---|
| IP Address Takeover | • Supported on all operating systems | • Supports a single subnet<br>• Operations on both servers, |

| HA Option | Benefits | Limitations |
|---|---|---|
| | • Supports multiple NICs<br>• 100% Genesys components<br>• HA option of choice for reliability ratings and tests | backup and primary, must succeed<br>• Subnet equipment to accept gratuitous ARP |
| Windows NLB Cluster | • Widely deployed<br>• Thoroughly documented<br>• Supports multiple NICs | • Supports a single subnet<br>• Complexity/prerequisites<br>• Dedicated switch/VLAN |
| F5 Networks BIG-IP LTM | • Reliability<br>• Flexibility (HA and Load balancing)<br>• Supports multiple NICs | • Additional equipment cost<br>• Additional network element<br>• Highly complex configuration |
| Using SIP Proxy | • Reliability<br>• 100% Genesys Components<br>• No Virtual IP address required<br>• Supports multiple subnets<br>• Supports Active-Active Resource Manager integration | |

SIP Server also supports HA configurations in which both primary and backup SIP Server instances reside on a single host server. In this case, IP interface virtualization is not required.

# Network Design Considerations

How can you improve reliability and achieve better bandwidth and latency control for your network. During the network design phase, apply at least some of the considerations in this section.

**Note:** SIP Server High Availability Guide does not include or specify requirements for networking equipment. You the customer are responsible to deploy suitable network equipment in compliance with your organization's business and security policies.

Deployment of SIP Server HA begins with technical planning of SIP Server HA implementation. As a start, the owner of the business requirements collaborates with Network Administrators and Network Engineers that support corporate network infrastructure.

A chosen and implemented network design defines a related set of SIP Server application parameters and HA scripts settings; the design can also require adjustment of static IP routes on the SIP Server hosts.

## General Network Design Considerations

Consider the following major points during design of a network for any system, including one that will offer SIP Server High Availability:

- Scalability and modularity
- Performance
- Availability and reliability
- Security and Cost

### Scalability and Modularity

A well-designed network should be scalable. The chosen topology should be able to accommodate projected growth. A modular approach to design converts a complex system into smaller, manageable ones, simplifies implementation and ensures that it can easily isolate a failure.

### Performance

Three aspects to consider:

- Bandwidth and effective throughput are the most important aspects of network performance and response time.
- Media and Voice over IP applications impose additional demand on the Quality of Service guarantees that the network can provide.
- How scalable is the network, with respect to the performance requirements?

### Availability and Reliability

- Availability and reliability require **redundancy**. Your network equipment must be redundant to support the redundant set of Genesys Suite components, including an HA pair of SIP Servers.
- Implement a **network management system**, to monitor the health of the network, ascertain operating conditions, and isolate faults. Use standard network monitoring and management tools to monitor SIP Server networks.
- **Virtualization** is an overall trend in IT. Your hardware platform should provide virtualization to ensure redundant and high-performance network connectivity.
- Network design should accommodate **SIP Server specifics**. For instance, deployment of dual NIC is required when network devices don’t support the required Quality of Service.

## SIP Server High Availability Characteristics Essential for Network Design

In addition to the general considerations above, the unique characteristics of SIP Server HA are essential to the network design.

### Reliable Connectivity

SIP Server High Availability depends on reliable network **connectivity between SIP Servers**. SIP Server's support of Hot Standby HA is critical to call processing. Using the TCP connection between SIP Servers, Genesys processes support the synchronization of critical data from the primary to the backup. This allows the backup to resume processing with little or no loss of calls.

Your ideal network design will recover interrupted connectivity within 2-4 seconds. Longer connectivity disruption can lead to HA synchronization issues that are recoverable, but take minutes to do so.

SIP Server High Availability depends on reliable network **connectivity between Solution Control Server and SIP Servers**. As the control tool of Management Framework, SCS monitors components and assigns Primary and Backup roles across respective components—based on the availability of components.

Clients of Hot Standby SIP Servers establish parallel connections to both the primary and backup, which enables a seamless switchover when a Primary fails.

Your network design must ensure that the failure of a single network element triggers a redundant path between SCS and SIP Server becoming available with within 2-4 seconds—that's End-to-End convergence time. Longer convergence time can lead to a split-brain condition that disrupts functionality of the entire environment.

### Virtual IP and ARP tables on adjacent routers

SIP Server assigns a Virtual IP (VIP) address for SIP signaling in addition to the physical IP addresses of the network adapters, to ensure that incoming SIP calls are delivered to the primary SIP Server. Immediately following a failover, SIP signaling for all existing calls and new calls is delivered to the

new primary.

The network adapters of the SIP Servers must be connected to a single network; IP addresses from the range of this network are allocated to the physical network adapters, and to the VIP. This VIP is then assigned to the primary SIP Server, and re-assigned to the new primary following switchover.

VIP address is a configurable option of the SIP Server application in the configuration.

Flushing the Address Resolution Protocol (ARP) cache of the adjacent network router(s) ensures that VIP failover occurs immediately. Manage the VIP failover and ARP cache flushing using scripts that are aligned with HA switchover process.

In an environment where multiple redundant routers deliver SIP messages to SIP Server, the scripts must be configured to refresh ARP tables on all such adjacent routers.

## Reliable Network of Virtual IP (VLAN)

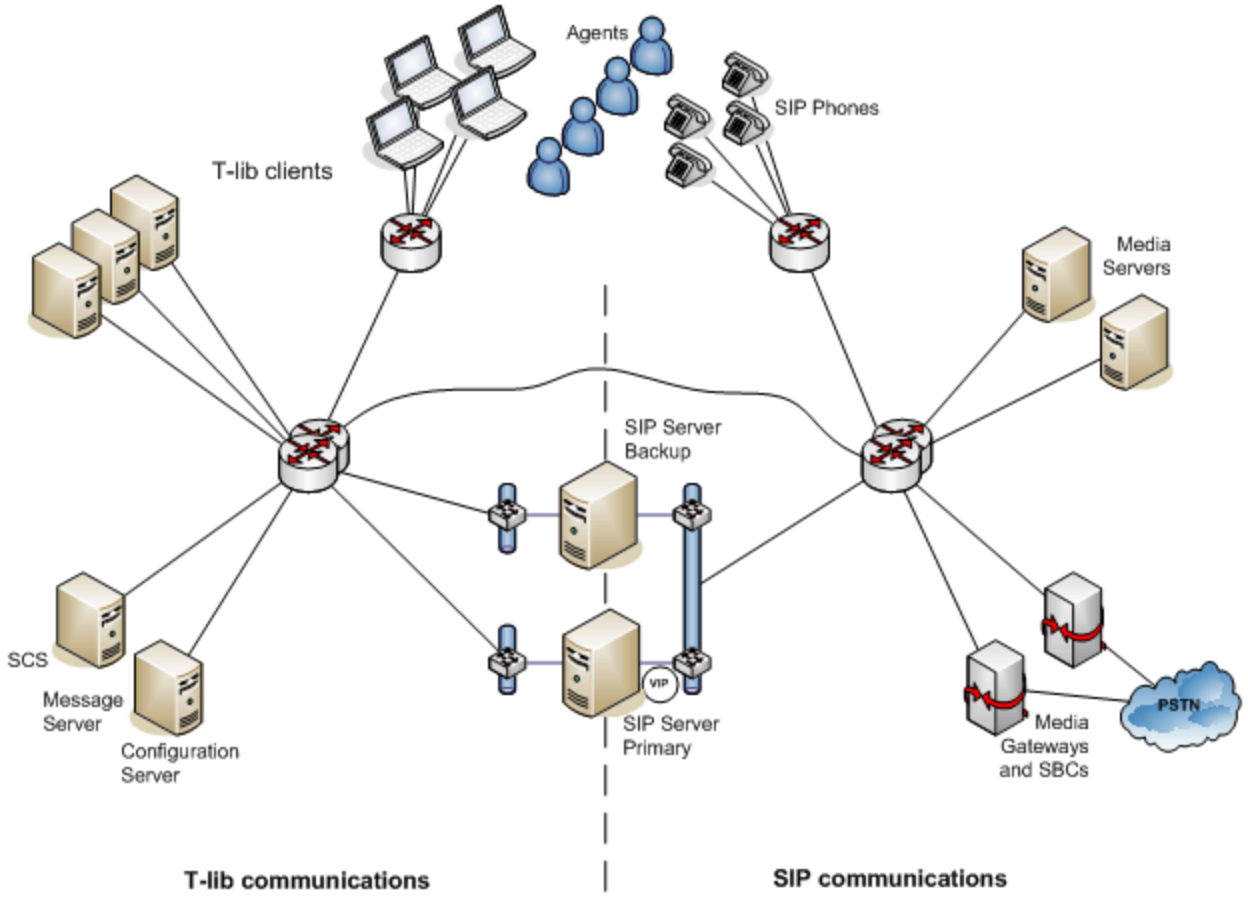
Network design must ensure that the network of VIP (VLAN) is extremely reliable.

A Layer 2 disconnect on this network can make SIP Server VIP inaccessible, sporadically or worse, to SIP devices communicating with the VIP. A VIP network split can detach one of the adjacent routers from the rest of the VLAN, making it unable to deliver to the VIP packets that arrive from various SIP devices.

Resume SIP communications with loss of HA support by manually adjusting IP routing on the detached router, as a temporary workaround. Recovery of the VIP network restores SIP communications entirely.

## Dedicated Network Infrastructure for Voice over IP and SIP Communications

Set up a dedicated network infrastructure for specific protocol communications. The network design may need to require partitioning SIP/RTP traffic and management traffic (T-Library, and so on) onto different networks. SIP Server HA does not require the use of dual-NIC hosts, but can support their use.




**Network Partitioning of T-Lib Communications and SIP Communications**

Partitioning is required in a deployment where network equipment does not support Quality of Service, i.e., does not guarantee a certain level of performance such as a required bit rate, delay, jitter, packet dropping probability and/or bit error rate.

For example, network equipment that ignores the Layer 2 Class of Service field does not provide different priorities to the data flows of different applications. Since Quality of Service guarantees are important for real-time streaming applications, and specifically for VoIP, applications must use a dedicated network (VLAN) for SIP/RTP communications, and partitioning is required.

**Note:**

Where network equipment supports a Quality of Service configuration, and where the customer makes a decision to prioritize SIP/RTP traffic with guarantees, you should set up the network equipment to look for certain TCP/IP header settings (for example, the IP precedence bit set to 5 or the DSCP bit set to 46) and to allocate the matching traffic to the proper queues.
Configure the IP precedence/DSCP bits of a SIP/RTP packet to match the values that the network equipment is configured for, and expecting.
Use the SIP Server sip-ip-tos option to define the value of the Type of Service (TOS) byte in the TCP/IP header of SIP messages that are sent by SIP Server. If undefined, use the operating system TOS.
Different network configurations treat the TOS byte as one of the following:

- A 3-bit IP precedence field, followed by a 4-bit type-of-service. The least significant bit (LSB) is unused, and set to 0. (RFC 1349)

- A 6-bit DiffServ, with the two least significant bits unused. (RFC 2474)

For more information about the Quality of Service configuration, dependencies on the application account privilege level, and the **sip-ip-tos** option of the SIP Server, see the SIP Server Deployment Guide.

## Dual-NIC (or multi-homed) hosts

Dedicated Network Infrastructure for Voice over IP Communications requires that the SIP Server host be connected to several different virtual networks (VLANs). A host connected to more than one IP network is said to be multi-homed because it has several IP addresses, on different networks.

A single hostname or Fully Qualified Domain Name (FQDN) and respective IP address is typically dedicated for management purposes for such a host. This hostname and/or respective IP address is specified in the host object in Genesys Configuration. From the perspective of the Management and Configuration Layer, the SIP Server application is running on a host with this hostname.

Other IP addresses and FQDNs can be used for specific communications, such as VoIP communications.

The illustration **Network Partitioning of T-Lib Communications and SIP Communication** (above) illustrates a deployment where management of hosts and regular data communications between applications go through one set of networks, while a different and dedicated network infrastructure is set up for VoIP communications.

The two SIP servers in that HA configuration are connected to both networks. Each SIP Server has a NIC that is used for the SIP communication, and a second NIC that is used for other kinds of communication with various components; for example, Management Layer and Configuration Layer components, as well as any T-Library clients.

### Network IP routing for delivery of traffic to SIP Server VIP

Configure SIP devices such as SIP endpoints, SIP Proxy, Media Servers, SBCs, and Media Gateways, to send SIP messages to SIP Server, by using a single Virtual IP address.

- In dual NIC deployments, where a SIP Server is connected to a dedicated network for VoIP and SIP communications, the VIP address is assigned from the range of the respective VoIP network.SIP messages sent to VIP are delivered by network routers according to their respective routing tables, and by adjacent routers according to ARP tables. Systems that do not participate in SIP communications must be located on networks that do not overlap with networks of SIP devices.

### Static IP Routes on SIP Server Hosts

To use dual NICs, you must also configure the IP parameters associated with the SIP NIC within each host. This configuration includes the IP gateway to use for egress IP routing of SIP traffic. It is required to ensure that outgoing SIP traffic is sent through the correct NIC.

RFC 1122 describes the Strong and Weak host models for a multi-homed host that is not acting as a router. These models define whether sent network traffic must be associated with the network interface. The IPv4 implementation in Linux uses the weak host model.

### Deploying on Linux

When you deploy SIP Server on an OS that uses a Weak host model, Genesys recommends configuring on the host a single default route that points to the IP gateway on the regular data network.

Static routes for networks of SIP devices such as SIP endpoints, SIP Proxy, Media Servers, SBCs, and Media Gateways, are configured on a dual-NIC host via the adjacent IP gateway on the dedicated VoIP network.

Identify each network of SIP devices to be reachable through the gateway on the VoIP network and configure its static route.

### Deploying on Windows Server 2008 and later

When you deploy SIP Server on an OS that uses the Strong host model, Genesys recommends configuring a separate default route for each NIC. The first default route on the data NIC must have a better metric (i.e., be preferred) and point to the IP gateway on the regular data network. The second default route on the SIP NIC must point to an adjacent IP gateway on the dedicated VoIP network.

You do not need to configure static routes for networks of SIP devices, because the OS itself will use the SIP NIC default routing based on the source address of the SIP packet set by the SIP Server as its VIP address.

## Asymmetric routing and imperfect partitioning of SIP traffic

SIP Server sends SIP messages to SIP devices using a Virtual IP address, and expects that SIP devices will send SIP messages to the VIP. VIP is one of the IP addresses assigned to SIP NIC of Primary SIP Server.

From the network perspective, symmetric routing means that packets traversing a NIC in either direction are sourced from--or destined to—an IP address of the NIC.

As described above, the Strong host model implemented in Windows Server 2008 and later allows one routing table per NIC. A correct configuration of NIC-level routing tables on Windows 2008 host will ensure symmetric communications, because SIP Server originates some data connections to other systems; routes to those destinations are thus relatively easy to configure via the correct NIC and the adjacent IP gateway on the regular data network.

In an environment where a remote host communicates with SIP Server using both SIP protocol and T-Library protocol, it is impossible to properly segregate SIP and T-Library traffic at the SIP Server host with a Linux operating system. Asymmetry of routing occurs because the Weak host model sends packets to the network according to its routing table of the host, and it will send packets through a NIC regardless of the originating IP or the protocol of communications.

An example of such a remote system is an agent’s computer that provides both desktop and SIP Phone functionality. Genesys recommends that in this environment, you use dedicated Voice over IP network only for delivery of SIP messages from such systems to the SIP Server VIP, while the routing table on the SIP Server host directs SIP packets from the SIP Server via the over NIC to the adjacent IP router on the regular data network.

Network access control should permit asymmetric traffic.

# HA Redundancy Types

When you deploy a SIP Server HA configuration, you can choose a hot-standby or warm-standby redundancy type, both are supported for the Virtual IP interface–based HA configuration.

The redundancy-type selection is made in the Configuration Layer or Genesys Administrator when you configure the primary SIP Server.

When you deploy a hot-standby configuration, there are additional steps for enabling data synchronization between the primary and backup SIP Servers. Configuration steps for both hot- and warm-standby redundancy types are included in the deployment procedures that are provided in SIP Server HA Deployment.

## Hot-Standby Redundancy Type

Genesys uses the expression *hot standby* to describe the high-availability configuration in which a backup-server application remains initialized, clients connect to both the primary and backup servers at startup, and the backup-server data is synchronized from the primary server.

Data synchronization and existing client connections to the backup server guarantee a higher degree of availability. Data synchronization includes information about calls, device states, monitoring subscriptions, and agent states.

SIP Server supports Hot Standby mode for established calls, calls that are in the ringing state, and calls that are parked on a Routing Point. All telephony functions can be performed on synchronized calls after a switchover.

While the hot-standby redundancy type provides a higher degree of availability than the warm-standby redundancy type, hot standby has limitations that include the following:

- Client requests that are sent during the time in which a failure occurs until switchover completes might be lost.
- IP requests that are sent by SIP endpoints during the failure and switchover might be lost.
- Some T-Library events might be duplicated or lost.
- The Client request `Reference ID` might be lost for client requests that are received just before a failure occurs and processed after the switchover completes.

Starting with version 8.1.102.58, primary and backup SIP Servers, after establishing the HA connection, will synchronize missing calls to the backup SIP Server. Some limitations apply. See Enhanced Procedure for Upgrading of SIP Server HA Pair for details.

When you deploy an HA configuration of the hot-standby redundancy type, Genesys recommends that Advanced Disconnect Detection Protocol (ADDP) be configured on the connection between the primary and backup SIP Servers. The primary SIP Server uses this connection to deliver synchronization updates.

## Warm-Standby Redundancy Type

Genesys uses the expression *warm standby* to describe the high-availability configuration in which a backup-server application remains initialized and ready to take over the operations of the primary server.

Unlike the hot-standby redundancy type, there is no propagation or synchronization of information from the primary SIP Server to the backup SIP Server about calls, devices, monitoring subscriptions, and agent states.

# IP Address Takeover

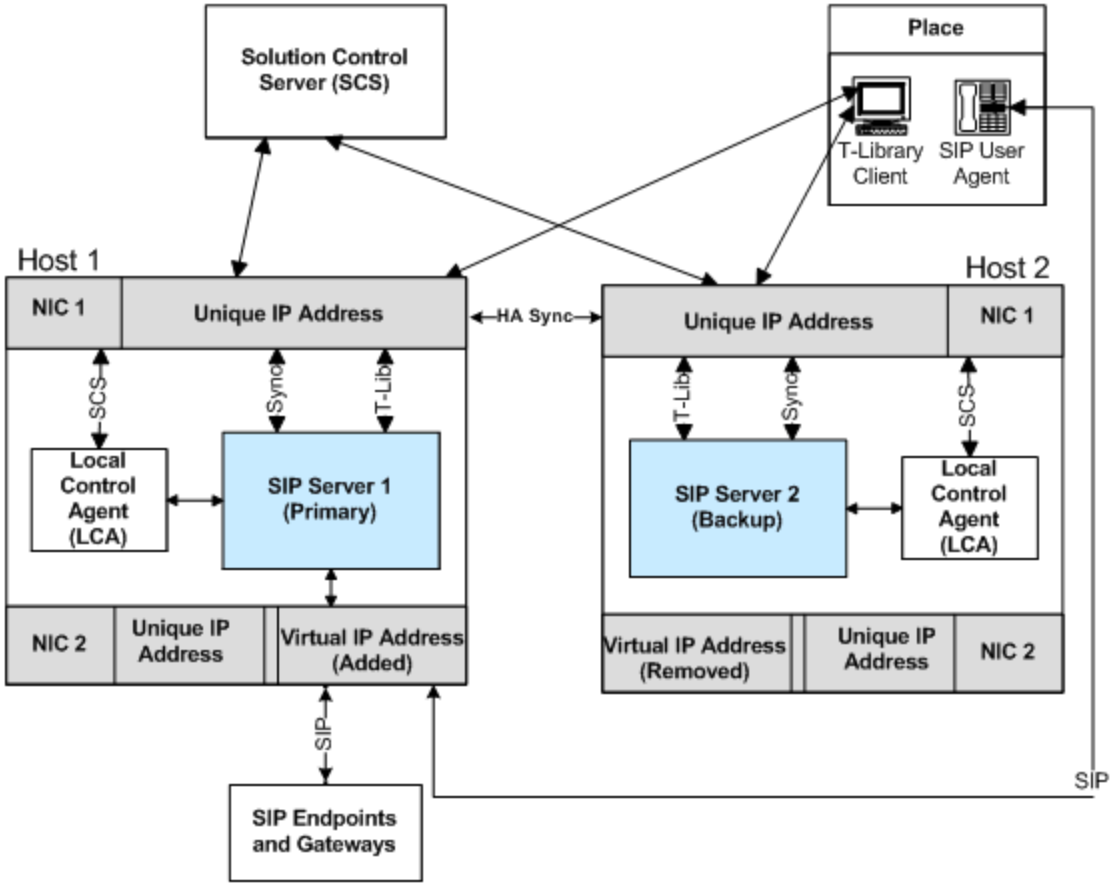
## Windows and UNIX Platforms

High availability of the service for SIP communications requires that the IP address of SIP Server is always accessible by other SIP components, is operational on the SIP Server currently running in primary mode, and is transferred to the other server in case of failover or switchover.

There are two approaches for the IP Address Takeover HA configuration:

- Linux and Solaris platforms use the Virtual IP address as the IP address configured on a logical sub-interface on the network interface card (NIC).
  - Logical sub-interface with the Virtual IP address is enabled on the server that is running in primary mode.
  - Logical sub-interface with the Virtual IP address is disabled on the server that is running in backup mode.
- Windows and AIX platforms use the Virtual IP address as an additional (or alias) IP address configured on the NIC.
  - Virtual IP address is added to the NIC configuration on the server that is running in primary mode.
  - Virtual IP address is deleted from the NIC configuration on the server that is running in backup mode.

The **HA Configuration with One NIC** figure shows an IP Address Takeover configuration using one NIC.




HA Configuration with One NIC

There are two SIP Server hosts on the same subnet, each of them has two logical IP interfaces set up on the NIC connected to the subnet. Each host has a unique IP address that is configured on the main logical IP interface. The second IP interface (a sub-interface) is configured with the IP address that is shared by the hosts and called the Virtual IP address. The second IP interface is enabled only on one host at a time.

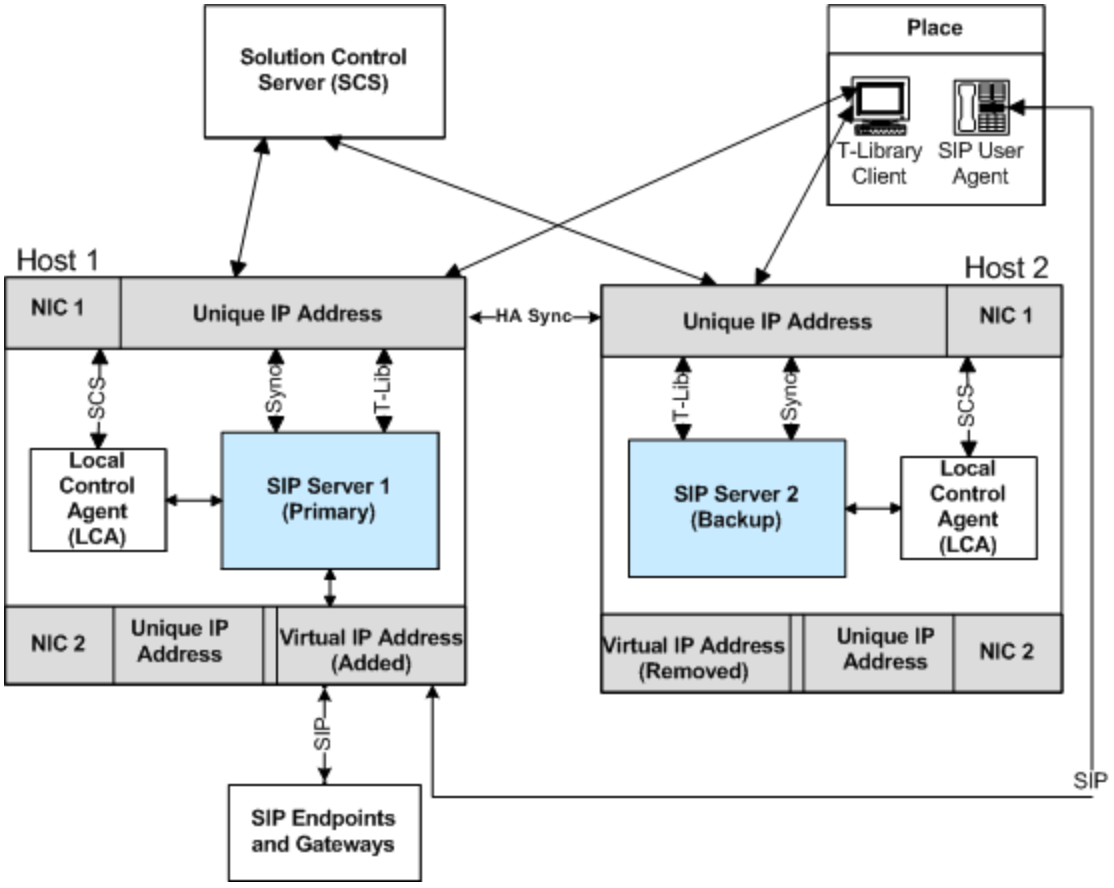
The IP interface with the unique IP address is always active. Management Layer and Configuration Layer components, and T-Library clients use the unique IP address for communication with the SIP Server and LCA.

SIP endpoints and gateways use the Virtual IP address to send SIP messages to SIP Server. The IP interface with the Virtual IP address is only enabled on the host on which SIP Server is running in primary mode. The IP interface with the Virtual IP address is disabled on the host on which SIP Server is running in backup mode.

In the IP Address Takeover configuration, the IP interface with the Virtual IP address is enabled and disabled by using the Virtual IP address control scripts.

The IP Address Takeover HA can be configured using either one network interface card (NIC), or multiple NICs.

The **HA Configuration with Two NICs** figure shows an IP Address Takeover configuration using two NICs.




HA Configuration with Two NICs

In a deployment with two NICs, one NIC (NIC 2 in the above figure) is used for the SIP communication, while the second NIC (NIC 1 in the above figure) is used for other kinds of communication with various components"for example, Management Layer and Configuration Layer components, as well as any T-Library clients. Solution Control Server (SCS) manages and monitors the SIP Server application through NIC 1 (dedicated to other non-SIP communication).

Although, the unique IP address of NIC 2 is not used, the Virtual IP address is configured on NIC 2 or its sub-interface. Monitoring of the connectivity through NIC 2 can be done by means of the SIP traffic monitoring feature. (See SIP Traffic Monitoring.)

See the IP Address Takeover HA Workflows for step-by-step descriptions of manual switchover, primary SIP Server failure, and primary SIP Server disconnect workflows. For deployment procedures, see:

- Deploying HA on Windows
- Deploying HA on AIX
- Deploying HA on Solaris
- Deployng HA on Linux

## IP Address Takeover HA Notes

- In an IP Address Takeover configuration, the Virtual IP address control scripts are used to add and delete the Virtual IP address to achieve a switchover. On Windows platform, the scripts use a Netsh command. Improper execution of this command may impact the SIP Server switchover time, as follows:
  - If the `Netsh` command fails to execute on either SIP Server host, the switchover will fail. For example, the `Netsh` command fails if any NIC properties are opened.
  - The `Netsh` command may take up to five seconds to execute. The execution time depends on the hardware and software characteristics of the host.With some network adapters the execution time can be significantly longer.
- Some hosts on the subnet may not be able to connect to the primary SIP Server after a switchover. Disabling the Virtual IP address at one host and enabling it at another changes the relationship between the MAC address and Virtual IP address. If an Address Resolution Protocol (ARP) announcement fails, the ARP table on some hosts on the subnet is not updated.

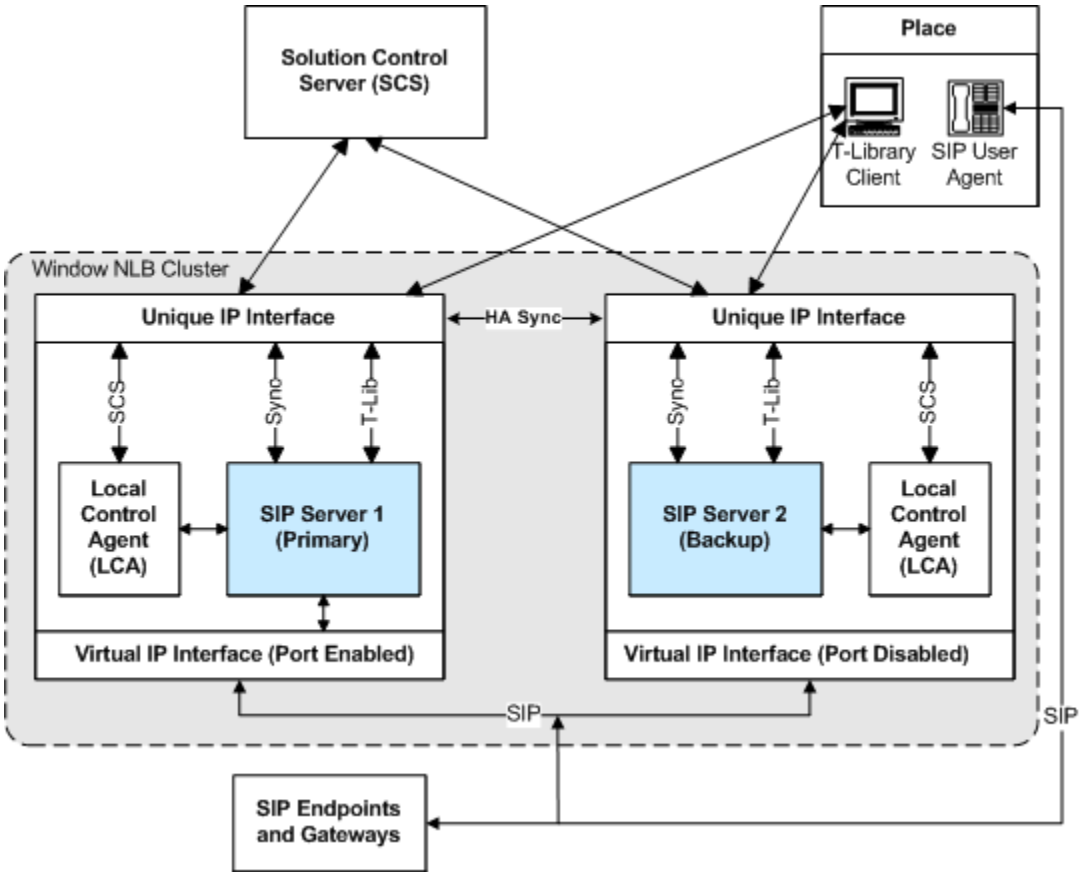
See the Prerequisites section for information about basic requirements and recommendations for deploying an IP Address Takeover HA configuration in a particular operating system.

# Windows NLB Cluster

A SIP Server HA configuration using Windows Network Load Balancing (NLB) configuration is an alternative to a Windows IP Address Takeover configuration.

Microsoft's NLB cluster technology allows you to configure cluster hosts to receive requests at a single Virtual IP address. SIP endpoints and gateways are configured to send all requests to SIP Server by using this single Virtual IP address. The Windows NLB cluster technology delivers the requests to the SIP Server that is running in primary mode and reroutes traffic to the backup SIP Server when a failure is detected.

The **HA Windows NLB Cluster Configuration** figure shows a SIP Server HA configuration that uses Windows NLB. SIP endpoints and gateways are configured to communicate with SIP Server by using a single Virtual IP address, and the SIP Server port is enabled only at the SIP Server that is running in primary mode. When a switchover to the backup SIP Server occurs, the port at the backup SIP Server host is enabled, and traffic is directed to the active SIP Server.




HA Windows NLB Cluster Configuration

The Management Layer uses a Windows NLB utility (`wlbs.exe` or `nlb.exe`) to enable and disable ports that are occupied by SIP Server. The NLB utility is initiated by Cluster control scripts that are triggered by SIP Server Alarm Conditions that are configured for SIP Server log events that occur

when a SIP Server changes its mode from primary to backup or from backup to primary.

Windows NLB can be configured to distribute incoming requests by using either the Unicast or the Multicast method. When you deploy a SIP Server HA configuration, you must define the method that you want to use.

Unicast and Multicast methods are described in the following sections.

See Windows NLB Cluster HA Workflows for step-by-step descriptions of manual switchover, primary SIP Server failure, and primary SIP Server disconnect workflows. For deployment procedures, see Windows NLB Cluster HA Deployment.

## Unicast Method

In the Unicast method, all NLB cluster hosts share an identical unicast MAC address. NLB overwrites the original MAC address of the cluster adapter by using the unicast MAC address that is assigned to all of the cluster hosts. Unicast NLB nodes cannot communicate over an NLB-enabled network adapter. In the Unicast method, all switch ports are flooded with NLB traffic, including ports to which non-NLB servers are attached. A workaround for this issue is to place cluster hosts on separate VLANs.

## Multicast Method

In a Multicast configuration, each NLB cluster host retains the original MAC address of the network adapter. In addition to the original MAC address of the adapter, the adapter is assigned a multicast MAC address that is shared by all cluster hosts. Client requests are sent to all cluster hosts at the multicast MAC address. Considerations for implementation of the Multicast distribution method include the following:

- Upstream routers might require a static Address Resolution Protocol (ARP) entry. Without an ARP entry, routers might not accept an ARP response that resolves unicast IP addresses to multicast MAC addresses.
- Without Internet Group Management Protocol (IGMP), switches might require additional configuration to define which ports the switch should use for multicast traffic.
- Upstream routers might not support mapping of a unicast IP address (the cluster IP address) to a multicast MAC address. In this case, you might be required to update or replace your router in order to use the Multicast method.

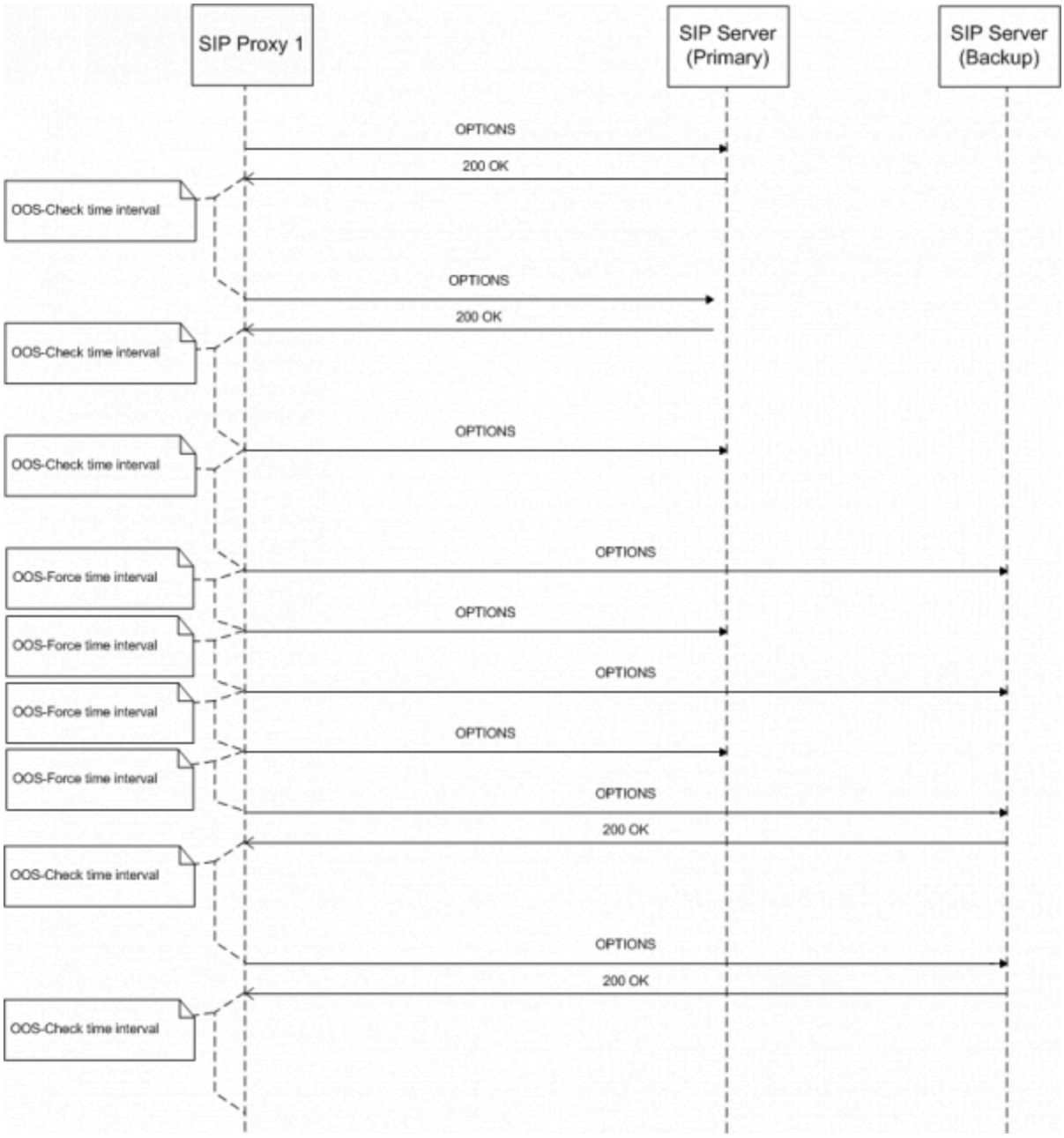
# Using SIP Proxy

SIP Proxy provides high availability for a primary/backup SIP Server HA pair without requiring a virtual IP address. A pool of SIP Proxies is defined for each SIP Server HA pair. Each SIP Proxy instance monitors all known SIP Server HA pairs to determine which SIP Server is currently active and which is backup. Incoming SIP messages are forwarded to the primary SIP Server. It is the responsibility of external SIP user agents to select a SIP Proxy instance based either on DNS or static configuration of multiple IP addresses, and to fall back to an alternate instance if the selected instance of SIP Proxy is not responding. The SIP Server HA pair is configured to use the SIP Proxy FQDN (resolved into a single or multiple SRV records) specified in the SIP Outbound Proxy DN of type Voice over IP Service.

## How It Works

SIP Proxy uses two timeouts configured at the Application level, with the `oos-check` and `oos-force` configuration options. The `oos-check` option defines the timeout that SIP Proxy uses before placing an unresponsive SIP Server in out-of-service state. The `oos-force` option defines the timeout that SIP Proxy uses when it does not know which SIP Server in the HA pair is active.

SIP Proxy pings each HA pair using OPTIONS messages. First, SIP Proxy sends an OPTIONS message to the SIP Server that is configured as primary in the HA pair. If this primary SIP Server responds during the configured `oos-check` timeout, then SIP Proxy waits for this timeout to expire before sending the next OPTIONS message, after which SIP Proxy resets the `oos-check` timeout. If the SIP Server does not respond before the timeout expires, SIP Proxy activates the `oos-force` timeout (usually shorter than `oos-check`) and starts sending OPTIONS messages alternatively to both servers in the HA pair, resetting the time between each attempt, until one of them begins to respond. When one of the SIP Servers responds to the OPTIONS message, SIP Proxy resets the `oos-check` timeout.




See SIP Proxy-based HA Workflow for primary-to-backup switchover steps. For a deployment procedure, see HA Deployment Using SIP Proxy.

For more information, refer to the SIP Proxy 8.1 Deployment Guide.

# Network Device-Based HA

An alternative to software-based Virtual IP interface configurations is a hardware-based Virtual IP configuration that uses an external network device.

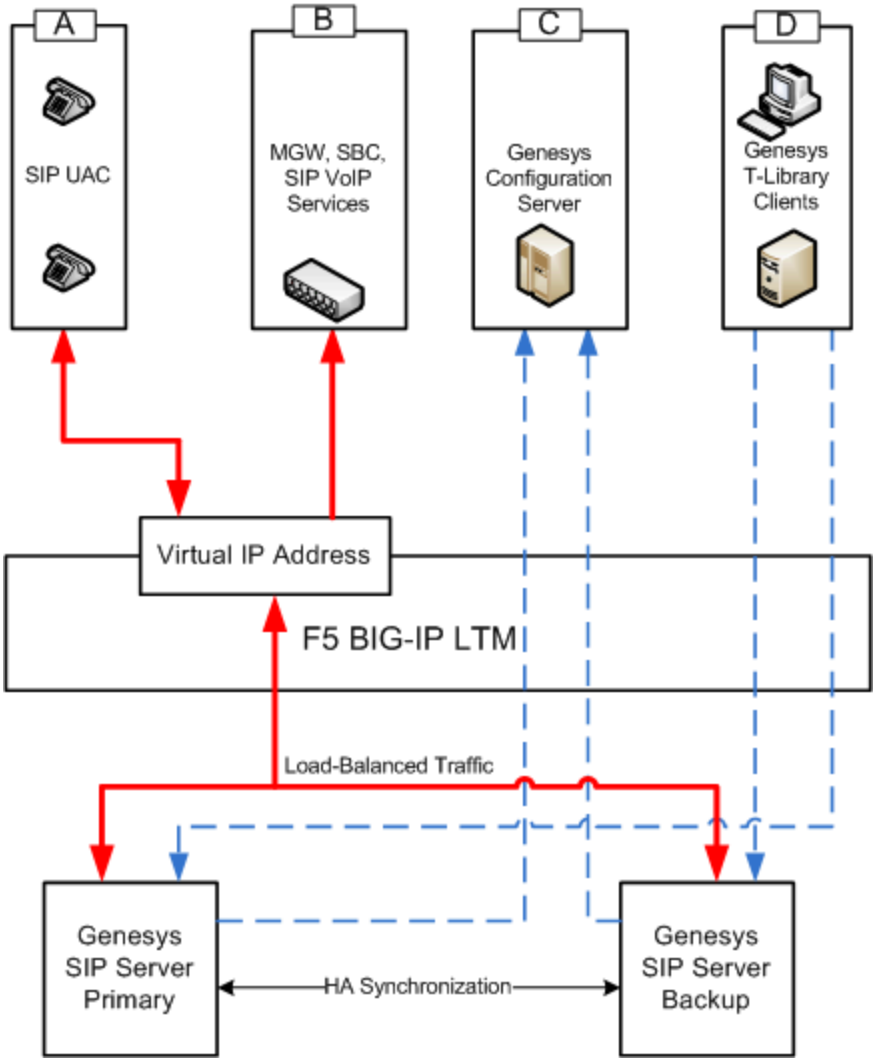
Benefits of using a network hardware device include the following:

- Less complex configuration: Alarm Reactions and Alarm Conditions are not required.
- There is no switch flooding, as there might be with a Windows NLB Unicast configuration.
- A single network device can support multiple SIP Server HA pairs.

Disadvantages might include the cost of a network device and the configuration that is required for Secure Network Address Translation (SNAT).

A network device works by presenting a shared Virtual IP address. SIP endpoints and gateways are configured to communicate with this single Virtual IP address. When the network device receives a request at the Virtual IP address, it routes the request to the SIP Server that is running in primary mode.

The SIP Server and the F5 Networks BIG-IP Local Traffic Manager (LTM) integration solution supports this type of HA configuration as shown in the **HA Configuration Using F5 Networks BIG-IP LTM** figure. F5's BIG-IP LTM monitors the primary SIP Server by sending an OPTIONS request to the SIP Server at configured intervals and listening for a response.




HA Configuration Using F5 Networks BIG-IP LTM

For more information about a SIP Server HA configuration that uses the F5 Networks BIG-IP LTM, refer to the Framework 8.1 SIP Server Integration Reference Manual. This guide describes configuration steps that are required to implement a hot-standby SIP Server HA configuration that runs behind an F5 Networks BIG-IP LTM.

# Other HA Enhancements

SIP Server supports several additional capabilities related to high-availability deployments.



## Single Host HA Deployment

Starting with version 8.0, SIP Server supports deploying both primary and backup SIP Server applications, as well as the Stream Manager or Media Server application, on the same physical host. Benefits of using the single host HA configuration include the following:

- Efficient use of the hardware equipment.
- Less complex configuration: Virtual IP address control scripts, Alarm Reactions, and Alarm Conditions are not required.

However, this type of HA configuration is supported only for small-size deployments—100 seats or less.

## Synchronization of Contact Between SIP Server HA Pair

SIP Server 8.x synchronizes the SIP registration `Contact` header for a particular device across both primary and backup instances of SIP Server. The primary SIP Server sends the contact information to the backup SIP Server using the HA link, as well as through the Configuration Server.

## SIP Traffic Monitoring

SIP Server 8.x supports SIP traffic monitoring for enhanced reliability. When configured, SIP Server monitors incoming SIP traffic and can initiate a switchover after a configurable length of time during which no SIP messages are received.

In deployments where two NICs are used, one NIC is dedicated to SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC.

The SIP traffic monitoring feature allows the primary SIP Server to monitor the network connectivity through the NIC that is responsible for SIP communication, to recognize connectivity issues that impact the SIP service, and to initiate reactions that result in recovery of the service.

An Application-level configuration option, **sip-pass-check**, must be configured to enable this functionality. In addition, at least one service device must be configured for Active Out-Of-Service Detection by using **oos-check** and **oos-force** configuration options. See the *Framework 8.1 SIP Server Deployment Guide* for information about the Active Out-Of-Service Detection feature description.

When it is set to `true`, the **sip-pass-check** option enables tracking of SIP messages that reach the primary SIP Server, including responses from SIP devices (DNs) that are monitored by SIP Server by using the **oos-check** and **oos-force** options.

The primary SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS when all devices configured with the Active OOS check have failed and no other SIP messages have been received for a period of time. The period of time is calculated as the maximum of the sums of the **oos-check** and **oos-force** option values configured for service DNs (if **oos-force** is less than 5, 5 is used). When SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS, SCS switches the primary SIP Server to the backup role, and SIP Server reports the SERVICE_RUNNING status to LCA/SCS. The backup SIP Server becomes the primary, and starts monitoring SIP traffic.

If both the primary and backup servers receive no SIP traffic, a switchover would occur each time that the effective out-of-service timeout expires. To prevent frequent switchovers in this case, SIP Server detects the "double switchover" condition and doubles the effective out-of-service timeout each time that the double switchover happens"up to four times greater than the initially calculated timeout, or until one of the two servers detects SIP traffic. As soon as SIP traffic is detected, the server that detected the traffic remains the primary SIP Server and continues normal operation.

## Monitoring Critical Conditions

You can use Genesys Administrator to check the current running status of SIP Server. Starting in release 8.1.0, SIP Server displays its state as `Running` in Genesys Administrator in cases where it is unable to open a listening port, and it is configured as one instance in a High Availability (HA) pair. Prior to release 8.1.0, (release 8.0.4 and earlier), in this same scenario SIP Server displayed its status as `UNAVAILABLE`.

To monitor problems with binding a listener (SIP Server is running but unable to open a listening port), Genesys recommends that, for each SIP Server instance, you configure an Alarm Condition for the log event `00-04200`. For more information, consult the Solution Control Interface (SCI) help topic, "Using Log Events for Alarm Detection".

To ensure that administrators do not miss the alarm, Genesys recommends that you configure automatic clearing of the activated alarm in accordance with business processes and the schedule of the customer administrator.

The recommended configuration of an Alarm Condition for `00-04200` enables monitoring of a wide range of events that are critical for both SIP Server functionality and for service availability. This includes problems that might occur when binding a listener, unexpected terminations, or unauthorized terminations of the SIP Server process.

In Genesys Administrator, alarms that are detected and activated can be observed through a

dedicated view, providing a central location for observing all alarms that occurred in the entire environment.

If required, an alarm reaction can be configured to notify administrators automatically when a critical condition occurs.

After the administrator investigates and resolves the problem, they must manually clear the alarm condition.

If the problem occurred due to a temporary outage (for example, a network switch reboot), SIP Server remains in the `Running` state, ensuring availability of the HA pair once the network switch is recovered; in release 8.0.4, SIP Serer required a manual restart to return to the Running state.

In release 8.0.4, if both SIP Server instances encountered a problem when binding a listener, both instances in the HA pair remained in `UNAVAILABLE` status, requiring a manual operation to resume the service. In release 8.1.0, SIP Server instead switches the primary role between the two HA instances and resumes the service as soon as one of the instances is able to open a listening port.

## Network Status Monitoring

### SCS connection monitoring

To enable monitoring of the SCS connection status, set the value of the SIP Server Application option **control-vip-scripts** to `true`. If the connection to SCS is not available and both SIP Servers in the HA pair are running as primary, one of them will enforce switching its role to the backup.

### Virtual IP address monitoring

To enable Virtual IP address monitoring for the IP Address Takeover configuration, set the value of the SIP Server Application option **sip-iptakeover-monitoring** to `true`. The primary SIP Server monitors the presence of the Virtual IP address on its host. The backup SIP Server monitors the absence of the Virtual IP address on its host. The corresponding Virtual IP script is executed if misconfiguration is detected. If the problem persists, SIP Server reports the `Service Unavailable` status. The Standard-level log event 00-52029 or 00-52030 is generated when the failure or success, respectively, of a Virtual IP address is detected.

### NIC status monitoring

To enable NIC status monitoring, set the value of the SIP Server Application option **tlib-nic-monitoring** to `true`. Both primary and backup SIP Servers monitor the status of the NIC associated with their Application objects in the configuration environment. This allows SIP Server to enforce switching to backup in case of NIC failure.

### SIP NIC status monitoring

To enable SIP NIC status monitoring in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), set the value of the SIP Server Application option **sip-nic-monitoring** to `true`. The IP address of the SIP NIC must be configured using the **sip-nic-address** option. SIP Server reports the `Service Unavailable` status if failure is detected. The Standard-level log event 00-52027

or 00-52028 is generated when the failure or success, respectively, of a SIP NIC is detected.

# SIP Server HA Workflows

These topics describe workflows for SIP Server HA Architectures:

- IP Address Takeover
- Windows NLB Cluster
- Using SIP Proxy

The workflows provide a step-by-step account of events that occur during a manual switchover, during a primary SIP Server failure, and during a primary SIP Server disconnection.

For configuration and deployment information that are referred to in the SIP Server HA workflows, see SIP Server HA Deployment.

# IP Address Takeover HA Workflows

The **HA Configuration with One NIC** figure shows an IP Address Takeover configuration prior to a switchover:

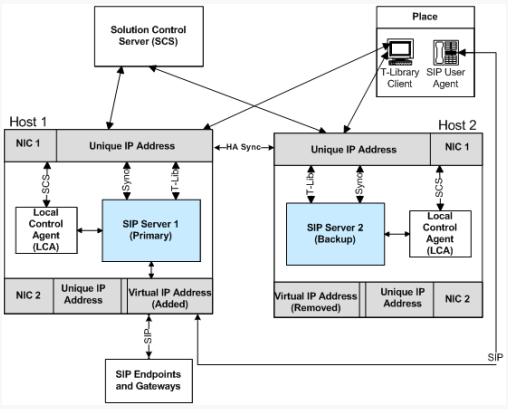
### State Prior to Switchover

- SIP Server 1 is in primary mode.
- SIP Server 2 is in backup mode.
- The Virtual IP address at the primary SIP Server (SIP Server 1) is enabled.
- The Virtual IP address at the backup SIP Server (SIP Server 2) is disabled.

### State After a Switchover

To see what happens in different scenarios, see the following:

- Manual-Switchover Workflow
- Primary Server-Failure Workflow
- Primary Server-Disconnected Workflow

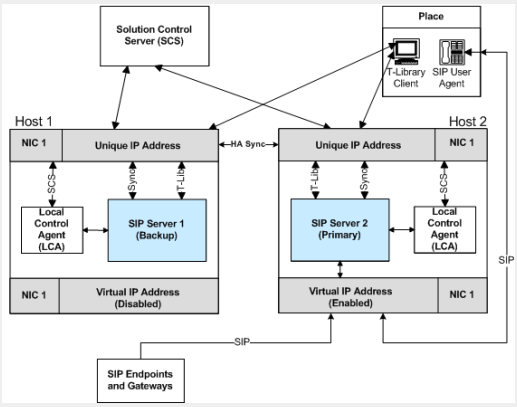


HA Configuration with One NIC

## Manual-Switchover Workflow

The following steps describe a primary to backup-switchover workflow for a IP Address Takeover configuration (the **HA Configuration After a Switchover** figure represents the end state of the workflow):

1. The switchover is initiated manually from the Solution Control Interface (SCI).
2. Through LCA, the SCS instructs the primary SIP Server (SIP Server 1) to go into backup mode.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Virtual IP address control script on its own host.
5. The Virtual IP address control scripts disable the Virtual IP address on the SIP Server 1 host (Host 1) and enable the Virtual IP address on the SIP Server 2 host (Host 2).

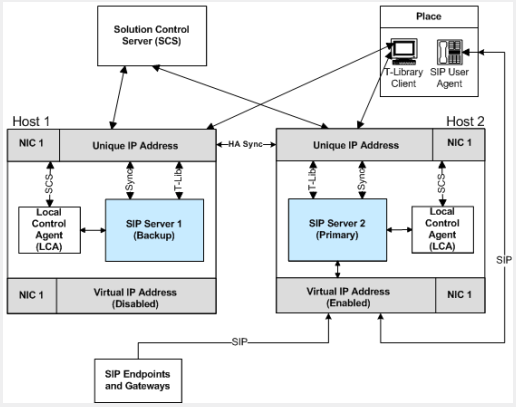


HA Configuration After a Switchover

## Primary Server-Failure Workflow

The following steps describe a primary server-failure workflow for an IP Address Takeover configuration (the **HA Configuration After Primary Server Failure** figure represents the end state of the workflow):

1. The primary SIP Server (SIP Server 1) fails.
2. LCA detects the primary SIP Server failure and reports it to the SCS.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Virtual IP address control script on its own host.
5. The Virtual IP address control scripts disable the Virtual IP address on the SIP Server 1 host (Host 1) and enable the Virtual IP address on the SIP Server 2



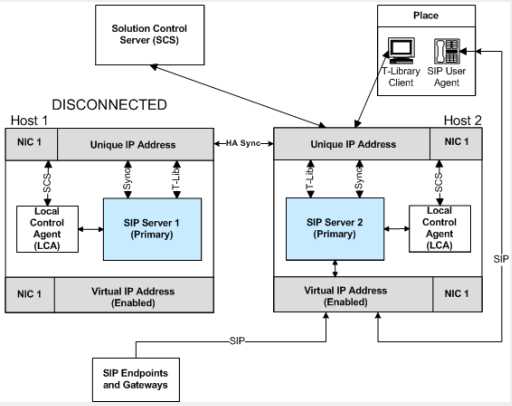
HA Configuration After Primary Server Failure

host (Host 2).

## Primary Server-Disconnected Workflow

The following steps describe a primary server-disconnected workflow for an IP Address Takeover configuration (the **HA Configuration After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The SCS detects that the connection to the primary SIP Server host (Host 1) has been lost.
2. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
3. Each SIP Server instructs LCA to launch the Virtual IP address control script on its own host.



HA Configuration After a Primary Server is Disconnected

Because SIP Server 1 is disconnected, the script that disables the Virtual IP address on Host 1 cannot be run. When the connection to SIP Server 1 has been restored, the following workflow will occur (not represented in the **HA Configuration After a Primary Server is Disconnected** figure above):

1. The SCS detects that the connection to the SIP Server 1 host has been restored.
2. The SCS discovers that both SIP Servers are running in primary mode.
3. Through LCA, the SCS instructs SIP Server 1, whose connection was just restored, to go into backup mode.
4. SIP Server 1 instructs LCA to launch the Virtual IP address control script on its own host.
5. The Virtual IP address control script runs on the SIP Server 1 host and disables the Virtual IP address.

# Windows NLB Cluster HA Workflows

The **HA Windows NLB Cluster Configuration** figure shows a Windows NLB Cluster configuration prior to a switchover.

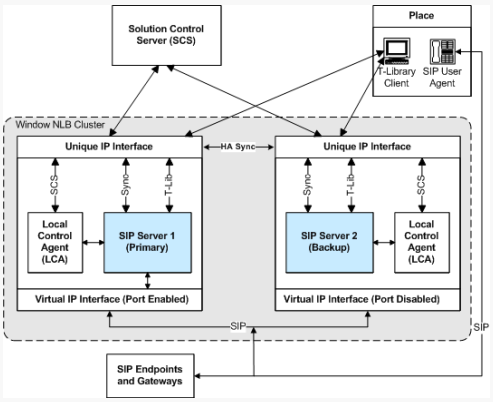
### State Prior to Switchover

- SIP Server 1 is in primary mode.
- SIP Server 2 is in backup mode.
- The SIP port is enabled at the primary SIP Server (SIP Server 1).
- The SIP port is disabled at the backup SIP Server (SIP Server 2).

### State After a Switchover

To see what happens in different scenarios, see the following:

- Manual-Switchover Workflow
- Primary Server-Failure Workflow
- Primary Server-Disconnected Workflow 1
- Primary Server-Disconnected Workflow 2

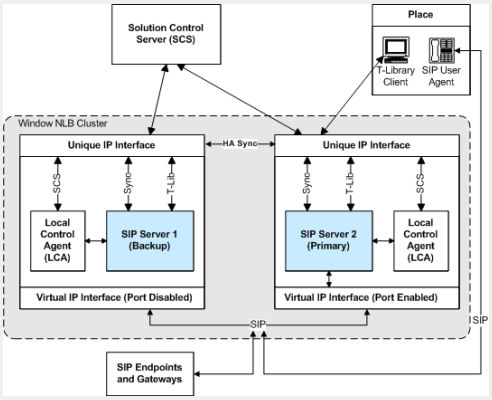



HA Windows NLB Cluster Configuration

## Manual-Switchover Workflow

The following steps describe a switchover workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After a Switchover** figure represents the end state of the workflow):

1. The switchover is initiated manually from the Solution Control Interface (SCI).
2. Through Local Control Agent (LCA), the Solution Control Server (SCS) instructs the primary SIP Server (SIP Server 1) to go into backup mode.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Cluster control script on its own host.
5. The Cluster control scripts run NLB utilities that disable the Virtual IP port on SIP Server 1 and enable the Virtual IP port on SIP Server 2.

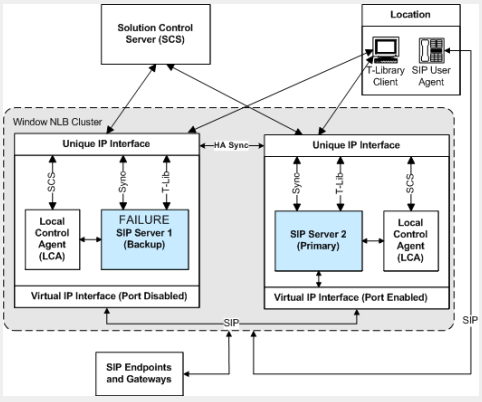


HA Windows NLB Cluster Configuration After a Switchover

## Primary Server-Failure Workflow

The following steps describe a primary server-failure workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After Primary Server Failure** figure represents the end state of the workflow):

1. The primary SIP Server (SIP Server 1) fails.
2. LCA detects the primary SIP Server application failure and reports it to the SCS.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Cluster control script on its own host.
5. The Cluster control scripts run Windows



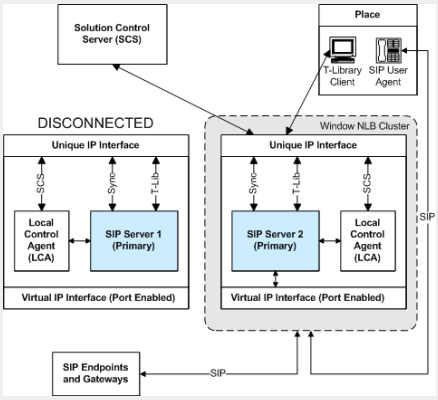
HA Windows NLB Cluster Configuration After Primary Server Failure

| | |
|---|---|
| NLB utilities that disable the Virtual IP port on SIP Server 1 and enable the Virtual IP port on SIP Server 2. | |

## Primary Server-Disconnected Workflow 1

The following steps describe a primary server-disconnected workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The SCS detects that the connection to the primary SIP Server host (SIP Server 1) has been lost.
2. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
3. Each SIP Server instructs LCA to launch the Cluster control script on its own host.
4. Because SIP Server 1 is disconnected, the Cluster control script that is used to disable the Virtual IP port on SIP Server 1 cannot be executed, and the port remains enabled. The Cluster control script is able to run on SIP Server 2 and the Virtual IP port is enabled.




HA Windows NLB Cluster Configuration After a Primary Server is Disconnected

When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in the **HA Windows NLB Cluster Configuration After a Primary Server is Disconnected** figure, above):

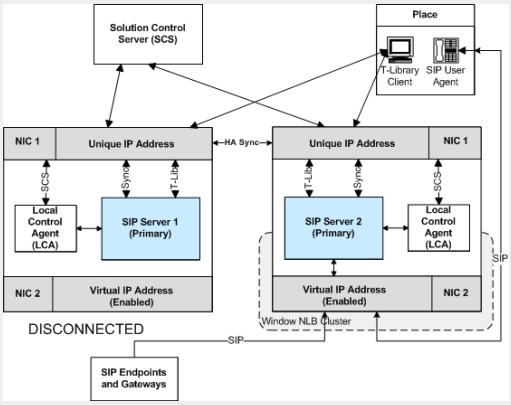
1. The SCS detects that the connection to SIP Server 1 host has been restored.
2. The SCS discovers that both SIP Servers are running in primary mode.

3. Through LCA, the SCS instructs SIP Server 1, whose connection was just restored, to go into backup mode.
4. SIP Server 1 instructs LCA to launch the Cluster control script on its own host.
5. The Cluster control script runs on SIP Server 1, and the Virtual IP port is disabled.

## Primary Server-Disconnected Workflow 2

The following steps describe a primary server-disconnected workflow for a Windows NLB Cluster configuration in the scenario where both SIP Servers use two NICs—one NIC is used for SIP communication (NIC 2), while the second NIC (NIC 1) is used for other kinds of communication with other components on the network. The SIP traffic monitoring feature is enabled (the **HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The Ethernet cord is unplugged from NIC 2 on the SIP Server 1 host.
2. The primary SIP Server (SIP Server 1) detects that it does not receive SIP messages for a certain period of time. SIP Server 1 reports the `SERVICE_UNAVAILABLE` status to LCA/SCS.
3. Through LCA, the SCS instructs the primary SIP Server (SIP Server 1) to go into backup mode and it instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Cluster control script on its own host.
5. Because NIC 2 on SIP Server 1 is disconnected, the NLB does not react to reconfiguration commands from the Cluster control script that is used to disable the Virtual IP port on SIP Server 1, and so the port remains enabled. The Cluster control script is successfully executed on SIP Server 2 and the Virtual IP port is enabled.




HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected

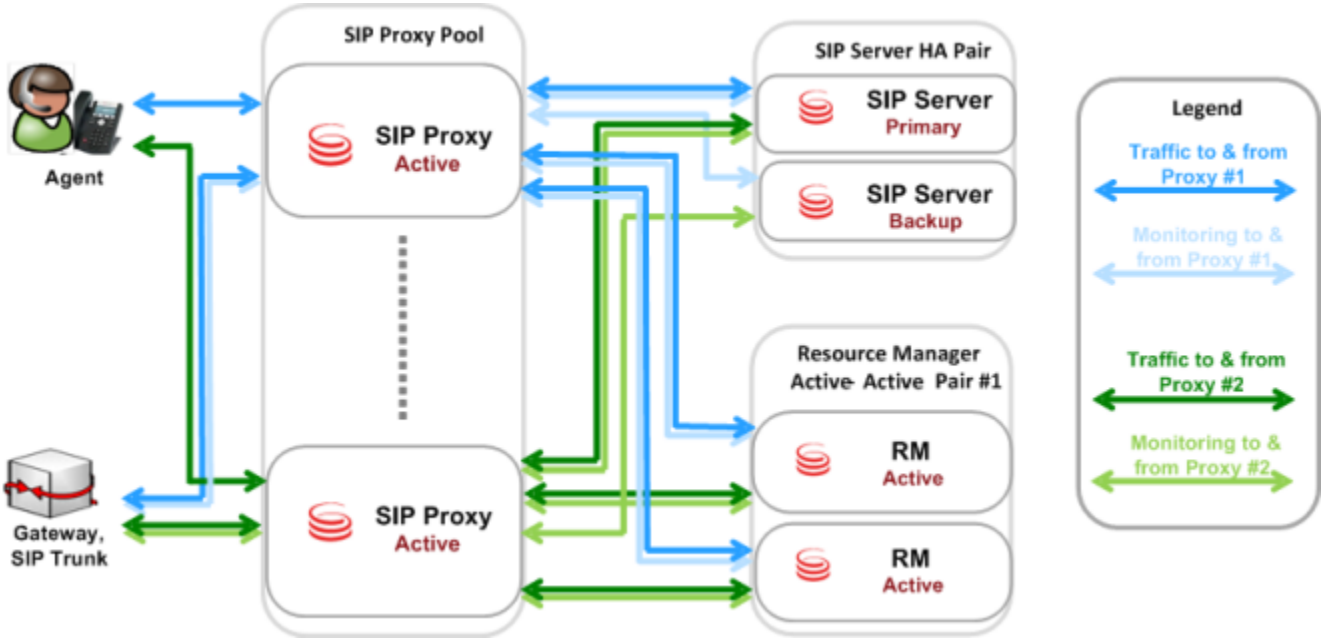
When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in the **HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected** figure):

1. Because the NLB port on SIP Server 1 remained enabled, after network connectivity is restored at NIC 2 on the SIP Server 1 host, the NLB cluster on both hosts is now incorrectly configured"SIP messages are delivered to the NLB cluster node where SIP Server is running in backup mode (SIP Server 1).
2. The primary SIP Server (SIP Server 2) detects that it had not received any SIP messages for a certain period of time. SIP Server 2 reports the `SERVICE_UNAVAILABLE` status to LCA/SCS.
3. Through LCA, the SCS instructs the primary SIP Server (SIP Server 2) to go into backup mode and instructs the backup SIP Server (SIP Server 1) to go into primary mode.
4. Each SIP Server instructs LCA to launch the Cluster control script on its own host.
5. The Cluster control scripts run NLB utilities that disable the Virtual IP port on SIP Server 2 and enable the Virtual IP port on SIP Server 1.

# SIP Proxy-based HA Workflow

The workflow of a primary-to-backup switchover proceeds as follows:

1. The primary SIP Server fails, disconnects, or a switchover is initiated manually.
2. SIP Proxy detects the primary SIP Server failure (or disconnection) if one of the following occurs:
   - The primary SIP Server stops responding to OPTIONS messages.
   - SIP Proxy receives a SIP request from the backup SIP Server.
3. SIP Proxy proxies all SIP traffic to the backup SIP Server which now runs in primary mode.




SIP Proxy: Single-Site Architecture and Traffic

**Note:** Multiple independent Active-Active RM pairs may be deployed, although this configuration is not depicted here.

# SIP Server HA Deployment

These topics describe how to deploy the SIP Server high-availability (HA) configurations:

- IP Address Takeover
- Windows NLB Cluster
- Using SIP Proxy
- TLS Configuration

> **Important**
> If you have to stop SIP Server running in HA mode, you must first promote it to a backup role. Likewise, you must do this if you have to reboot or stop the host on which the primary SIP Server is running.

# IP Address Takeover

This section describe how to deploy IP Address Takeover configurations on the following operating systems:

- IP Address Takeover HA Deployment on Windows
- IP Address Takeover HA Deployment on Linux
- IP Address Takeover HA Deployment on AIX
- IP Address Takeover HA Deployment on Solaris

# Windows

Complete these steps to set up SIP Server HA on Windows Server 2008 or 2008 R2, using the IP Address Takeover method.

> **Important**
>
> Genesys recommends using Windows 2008 R2 or later. When using the IP Address Takeover method on Windows 2008 R2, make sure you install the Microsoft Hotfix referenced in http://support.microsoft.com/kb/2811463.

1. Ensure that your system meets the deployment prerequisites
2. Configure the primary SIP Server
3. Configure the backup SIP Server
4. Create Virtual IP address control scripts for Windows 2008 R2 and later
5. Create Virtual IP address control scripts for Windows 2008
6. Test Virtual IP address control scripts
7. Create Application objects for Virtual IP address control scripts
8. Verify the HA configuration

## Ensure that your system meets the deployment prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

  > **Important**
  >
  > Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Software requirements:
  - For the Windows OS to send a gratuitous ARP packet when a new IP address is assigned on the computer, you must install the Microsoft Hotfix 2811463 for Windows 2008 R2. See

http://support.microsoft.com/kb/2811463/en-us.

- SIP Server must be installed and configured on both host computers.
- LCA release 8.1.2 or higher must be installed and configured on both host computers.
- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).

- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

## Configure the primary SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to `true`.

vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.

viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.

ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.

x. Click `Apply` to save the configuration changes.

b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP, select the **[backup-sync]** section, and configure the following options:

- **sync-reconnect-tout**
- **protocol**
- **addp-timeout**
- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tou**t option to at least two times the timeout value plus the established network latency.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. Click `Apply` to save the configuration changes.

5. Click the `Switches` tab.
   a. Ensure that the correct `Switch` object is specified. If necessary, select the correct `Switch` object by using the `Add` button.
   b. Click `Apply` to save the configuration changes.
6. Click the `Server Info` tab.
   a. Select the `Redundancy Type`. You can select either `Hot Standby` or `Warm Standby`.
   b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.
      i. In the `Ports` section, select the port to which the backup SIP Server will connect for HA data synchronization, and click `Edit Port`.
      ii. In the `Port Properties` dialog box, on the `Port Info` tab, select the `HA sync` check box.
      iii. Click `OK`.
   c. For the `Backup Server` option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
   d. Click `Apply` to save the configuration changes.
7. Click the `Start Info` tab.

a. Select `Auto-Restart`.

b. Click `Apply` to save the configuration changes.

8. Click `Apply` and then `OK` to save the configuration changes.

## Configure the backup SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. Select `Properties`.
4. Click the `Switches` tab.
   a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
   b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
   a. Select `Auto-Restart`.
   b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the same port number that you specified for the primary SIP Server.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_BACKUP_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the `sip-vip-script-down` option to the name of the Application object (`SIP_SERVER_BACKUP_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to `true`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration and have configured ADDP communication on the

primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP, select the **[backup-sync]** section, and configure the following options:

- **sync-reconnect-tout**
- **protocol**
- **addp-timeout**
- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.

c. Click Apply to save the configuration changes.

7. Click Apply and then OK to save the configuration changes.

## Create Virtual IP address control scripts for Windows 2008 R2 and later

1. On the primary SIP Server host computer, create a batch file that is named HA_IP_ON.bat, and enter the following commands into the file:
   **[+] Commands for '''HA_IP_ON.bat'''**

```
@set VirtualIP=10.10.11.103
@set vipMask=255.255.255.0
@set VirtualInterface="Local Area Connection"
@echo ********************* HA_IP_ON ********************** >> Takeover.log
@echo %time% >> Takeover.log
@rem check if Virtual IP released on Backup host
FOR /L %%A IN (1,1,6) DO (
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover1.log
@if not errorlevel 1 goto ready
)
:ready
@rem Add VirtualIP
@netsh interface ip delete arpcache
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
store=active skipassource=true >> Takeover.log
@rem check if VirtualIP added succesefully if not do it again
@cscript.exe check_ip.vbs localhost %VirtualIP% //Nologo >> Takeover.log
@if errorlevel 1 goto done
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
store=active skipassource=true >> Takeover.log
@if errorlevel 1 (
@echo %VirtualIP% not added to %VirtualInterface% >> Takeover.log
@goto done
)
:done
@echo %time% >> Takeover.log
```

**[+] Commands for '''HA_IP_ON.bat''' for IPv6**

```
@set VirtualIP=10.10.11.103
 @set VirtualIPv6=fde6:bed:c179:43f5:3:3:3:c
 @set vipMask=255.255.255.0
 @set VirtualInterface="Local Area Connection 4"
 @echo ********************* HA_IP_ON ********************** >>Takeover.log
 @if not defined VirtualIP goto done
 @echo %time% >> Takeover.log
 @rem check if Virtual IP released on Backup host
 FOR /L %%A IN (1,1,6) DO (
 @cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover1.log
 @if not errorlevel 1 goto ready
 )
 :ready
 @rem Add VirtualIP
 @netsh interface ip delete arpcache
 netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
 store=active skipassource=true >> Takeover.log
 @rem check if VirtualIP added succesefully if not do it again
 @cscript.exe check_ip.vbs localhost %VirtualIP% //Nologo >> Takeover.log
 @if errorlevel 1 goto done
 netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
 Takeover.log
 netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
 store=active skipassource=true >> Takeover.log
 @if errorlevel 1 echo %VirtualIP% not added to %VirtualInterface% >>Takeover.log
 :done
 @echo %time% >> Takeover.log
 @if not defined VirtualIPv6 goto donev6
 @echo %time% >> Takeover.log
 @rem check if Virtual IPv6 released on Backup host
 @cscript.exe ping.vbs %VirtualIPv6% //Nologo >> Takeover.log
 @if not errorlevel 1 goto readyv6
 @cscript.exe ping.vbs %VirtualIPv6% //Nologo >> Takeover.log
 @if not errorlevel 1 goto readyv6
 @cscript.exe ping.vbs %VirtualIPv6% //Nologo >> Takeover.log
 :readyv6
 @rem Add VirtualIPv6
 @netsh interface ip delete arpcache
 @netsh int ipv6 delete destinationcache
 netsh interface ipv6 add address interface=%VirtualInterface% address=%VirtualIPv6%
 store=active skipassource=true >> Takeover.log
 @rem check if VirtualIPv6 added succesefully if not do it again
 @cscript.exe check_ip.vbs localhost %VirtualIPv6% //Nologo >> Takeover.log
 @if errorlevel 1 goto donev6
 netsh interface ipv6 delete address interface=%VirtualInterface% address=%VirtualIPv6%
 >> Takeover.log
 netsh interface ipv6 add address interface=%VirtualInterface% address=%VirtualIPv6%
 store=active skipassource=true >> Takeover.log
 @if errorlevel 1 echo %VirtualIPv6% not added to %VirtualInterface% >>Takeover.log
 :donev6
 @echo %time% >> Takeover.log
```

### Important

- The `store=active` parameter of `netsh interface ip add address` is only available when you deploy the IP Address Takeover method on Windows Server 2008 R2.
- Verify that the `skipassource=true` parameter of `netsh interface ip add address`

> is available when you deploy the IP Address Takeover method on your Windows Server.

2. In the first line of the `HA_IP_ON.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
3. In the second line of the `HA_IP_ON.bat` script, replace the `vipMask` value of `255.255.255.0` with your Virtual IP mask.
4. In the third line of the `HA_IP_ON.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
5. On the primary SIP Server host computer, create a batch file that is named `HA_IP_OFF.bat`, and enter the following commands into the file:
   **[+] Commands for '''HA_IP_OFF.bat'''**

```
@set VirtualIP=10.10.11.103
@set VirtualInterface="Local Area Connection"
@echo ********** HA_IP_OFF ********** >> Takeover.log
@echo %time% >> Takeover.log
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
@netsh interface ip delete arpcache
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@echo %time% >> Takeover.log
```

   **[+] Commands for '''HA_IP_OFF.bat''' for IPv6**

```
@set VirtualIP=10.10.11.103
@set VirtualIPv6=fde6:bed:c179:43f5:3:3:3:c
@set VirtualInterface="Local Area Connection 4"

@echo ********** HA_IP_OFF ********** >>Takeover.log

@if not defined VirtualIP goto done

@echo %time% >> Takeover.log
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
@netsh interface ip delete arpcache
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
:done
@echo %time% >> Takeover.log

@if not defined VirtualIPv6 goto donev6

@echo %time% >> Takeover.log
netsh interface ipv6 delete address interface=%VirtualInterface% address=%VirtualIPv6%
>> Takeover.log
@netsh interface ip delete arpcache
@netsh int ipv6 delete destinationcache
@cscript.exe ping.vbs %VirtualIPv6% //Nologo >> Takeover.log
:donev6
@echo %time% >> Takeover.log
```

6. In the first line of the `HA_IP_OFF.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.

7. In the second line of the HA_IP_OFF.bat script, ensure that the VirtualInterface value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
8. Follow the steps in this procedure to create the same two scripts on the backup SIP Server host.
9. On the primary SIP Server host computer, create an accessory script that is named Ping.vbs, and enter the following commands into the script:
   **[+] Commands for Ping.vbs**

```
rem ping host and return 1 if ping successful 0 if not
On Error Resume Next
if WScript.Arguments.Count > 0 then
  strTarget = WScript.Arguments(0)
  Set objShell = CreateObject("WScript.Shell")
  Set objExec = objShell.Exec("ping -n 2 -w 1000 " & strTarget)
  strPingResults = LCase(objExec.StdOut.ReadAll)
  If InStr(strPingResults, "reply from") And Not CBool(InStr(strPingResults,
"unreachable")) Then
    WScript.Echo strTarget & " responded to ping."
    wscript.Quit 1
  Else
    WScript.Echo strTarget & " did not respond to ping."
    wscript.Quit 0
  End If
Else
  WScript.Echo "target is not specified."
  wscript.Quit -1
End If
```

10. On the primary SIP Server host computer, create an accessory script that is named Check_ip.vbs, and enter the following commands into the script:
    **[+] Commands for Check_ip.vbs**

```
rem check if IP address (arg0 ) can be found on host (arg1 )
On Error Resume Next
if WScript.Arguments.Count > 0 then
  strComputer = WScript.Arguments(0)
  targetIPAddress = WScript.Arguments(1)
  Set objWMIService = GetObject("winmgmts:" _
   & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
  Set colNicConfigs = objWMIService.ExecQuery _
   ("SELECT * FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled = True")
  WScript.Echo "Computer Name: " & strComputer & " ip " & targetIPAddress
  For Each objNicConfig In colNicConfigs
    For Each strIPAddress In objNicConfig.IPAddress
      If InStr(strIPAddress, targetIPAddress) Then
        WScript.Echo targetIPAddress & " is found on " & objNicConfig.Description
        wscript.Quit 1
      End If
    Next
  Next
  WScript.Echo targetIPAddress & " not found."
  wscript.Quit 0
Else
    WScript.Echo "target not specified."
    wscript.Quit -1
End If
```

11. Place accessory scripts Ping.vbs and Check_ip.vbs in the same directory as the HA_IP_ON.bat and HA_IP_OFF.bat files on both the primary and backup SIP Server hosts.

# Create Virtual IP address control scripts for Windows 2008

1. On the primary SIP Server host computer, create a batch file that is named `HA_IP_ON.bat`, and enter the following commands into the file:
   **[+] Commands for '''HA_IP_ON.bat'''**

```
@set VirtualIP=10.10.11.103
@set vipMask=255.255.255.0
@set VirtualInterface="Local Area Connection"
@set GatewayIP=10.10.11.104
@set InterfaceForArping="\Device\NPF_{85FEBE1C-9EEF-4E61-974B-1158DB270F6E}"
@echo ********** HA_IP_ON ********** >> Takeover.log
@echo %time% >> Takeover.log
@rem check if Virtual IP released on Backup host
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
:ready
@rem Add VirtualIP
@netsh interface ip delete arpcache
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
>> Takeover.log
@rem check if VirtualIP added succesefully if not do it again
@cscript.exe check_ip.vbs localhost %VirtualIP% //Nologo >> Takeover.log
@if errorlevel 1 goto done
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
>> Takeover.log
@if errorlevel 1 (
@echo %VirtualIP% not added to %VirtualInterface% >> Takeover.log
@goto done
)
@rem Use arping command for windows 2008 (IPV4 only) to update ARP cache of hosts (SIP-
Server, Gateway etc)
@rem SYNOPSIS: arping [-abhpqrRd0uv] [-S host/ip] [-T host/ip] [-s MAC] [-t MAC] [-c
count] [-i interface] [ -w us ] <host|-B>
@rem Manual: http://www.habets.pp.se/synscan/docs/arping.8.html
@rem We recommend placing the SIP-Server and RM in different subnet - uncomment below to
use apring to send ARP to Gateway
@rem If multiple Gateways used (HA pair) - then you need to send for each Gateway
separately
@arping.exe -c 3 -i %InterfaceForArping% -S %VirtualIP% %GatewayIP% >> IPTakeOver.log
:done
@echo %time% >> Takeover.log
```

2. In the first line of the `HA_IP_ON.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
3. In the second line of the `HA_IP_ON.bat` script, replace the `vipMask` value of `255.255.255.0` with your Virtual IP mask.
4. In the third line of the `HA_IP_ON.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
5. In the fourth line of the `HA_IP_ON.bat` script, replace the `GatewayIP` value of `10.10.11.104` with your Gateway IP address.

6. In the fifth line of the HA_IP_ON.bat script, replace the InterfaceForArping value of \Device\NPF_{85FEBE1C-9EEF-4E61-974B-1158DB270F6E} with the value that is received by following these steps:
   a. By using Regedit, navigate to HKLM\SYSTEM\CurrentControlSet\Control\Network\.
   b. Identify the key set that has a value of {Default} and contains the Network Adapters Data.
   c. If the virtual interface is set to Local Area Connection, then search for the listed adapter with the value name that contains the Local Area Connection Data. The Key value that contains Local Area Connection is the reference to the physical device identifier.
   d. Add \Device\NPF_ to the Key, and set this value to InterfaceForArping.

   For example, from the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CEBFC1-08002BE10318}\{85FEBE1C-9EEF-4E61-974B-1158DB270F6E} key, take the {85FEBE1C-9EEF-4E61-974B-1158DB270F6E} portion, and add Device\NPF_ to the key in front. This will produce the following result: \Device\NPF_{85FEBE1C-9EEF-4E61-974B-1158DB270F6E}

> **Important**
> The value of Network Adapter ID varies on different hosts. You must complete these steps on both primary and backup hosts.

7. On the primary SIP Server host computer, create a batch file that is named HA_IP_OFF.bat, and enter the following commands into the file:
   **[+] Commands for '''HA_IP_OFF.bat'''**

```
@set VirtualIP=10.10.11.103
@set VirtualInterface="Local Area Connection"
@echo ********** HA_IP_OFF ********** >> Takeover.log
@echo %time% >> Takeover.log
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
@netsh interface ip delete arpcache
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@echo %time% >> Takeover.log
```

8. In the first line of the HA_IP_OFF.bat script, replace the VirtualIP value of 10.10.11.103 with your Virtual IP address.
9. In the second line of the HA_IP_OFF.bat script, ensure that the VirtualInterface value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
10. Follow the steps in this procedure to create the same two scripts on the backup SIP Server host.
11. On the primary SIP Server host computer, create an accessory script that is named Ping.vbs, and enter the following commands into the script:
    **[+] Commands for Ping.vbs**

```
rem ping host and return 1 if ping successful 0 if not
On Error Resume Next
if WScript.Arguments.Count > 0 then
  strTarget = WScript.Arguments(0)
  Set objShell = CreateObject("WScript.Shell")
  Set objExec = objShell.Exec("ping -n 2 -w 1000 " & strTarget)
  strPingResults = LCase(objExec.StdOut.ReadAll)
  If InStr(strPingResults, "reply from") And Not CBool(InStr(strPingResults,
```

```
"unreachable")) Then
    WScript.Echo strTarget & " responded to ping."
    wscript.Quit 1
  Else
    WScript.Echo strTarget & " did not respond to ping."
    wscript.Quit 0
  End If
Else
  WScript.Echo "target is not specified."
  wscript.Quit -1
End If
```

12. On the primary SIP Server host computer, create an accessory script that is named `Check_ip.vbs`, and enter the following commands into the script:
    **[+] Commands for Check_ip.vbs**

```
rem check if IP address (arg0 ) can be found on host (arg1 )
On Error Resume Next
if WScript.Arguments.Count > 0 then
  strComputer = WScript.Arguments(0)
  targetIPAddress = WScript.Arguments(1)
  Set objWMIService = GetObject("winmgmts:" _
   & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
  Set colNicConfigs = objWMIService.ExecQuery _
   ("SELECT * FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled = True")
  WScript.Echo "Computer Name: " & strComputer & " ip " & targetIPAddress
  For Each objNicConfig In colNicConfigs
    For Each strIPAddress In objNicConfig.IPAddress
      If InStr(strIPAddress, targetIPAddress) Then
        WScript.Echo targetIPAddress & " is found on " & objNicConfig.Description
        wscript.Quit 1
      End If
    Next
  Next
  WScript.Echo targetIPAddress & " not found."
  wscript.Quit 0
Else
    WScript.Echo "target not specified."
    wscript.Quit -1
End If
```

13. Place accessory scripts `Ping.vbs` and `Check_ip.vbs` in the same directory as the `HA_IP_ON.bat` and `HA_IP_OFF.bat` files on both the primary and backup SIP Server hosts.

## Test Virtual IP address control scripts

1. Run the `HA_IP_OFF.bat` script on the backup SIP Server host.
2. Run the `HA_IP_ON.bat` script on the primary SIP Server host.
3. Verify that the Virtual IP interface is running on the primary host by using the `ipconfig` command—for example:
   **[+] Example ipconfig command**

```
C:\GCTI\SWITCHOVER\1NIC>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
```

```
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 10.10.11.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

4. Verify that the Virtual IP interface is not running on the backup SIP Server host—for example:
   **[+] Example ipconfig command**

```
C:\GCTI\SWITCHOVER\1NIC>ipconfig
 Windows IP Configuration

 Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

5. Run the `HA_IP_OFF.bat` script on the primary SIP Server host.
6. Run the `HA_IP_ON.bat` script on the backup SIP Server host.
7. Verify that the Virtual IP interface is running on the backup SIP Server host by using the `ipconfig` command. Output should appear similar to the following:
   **[+] Example ipconfig command**

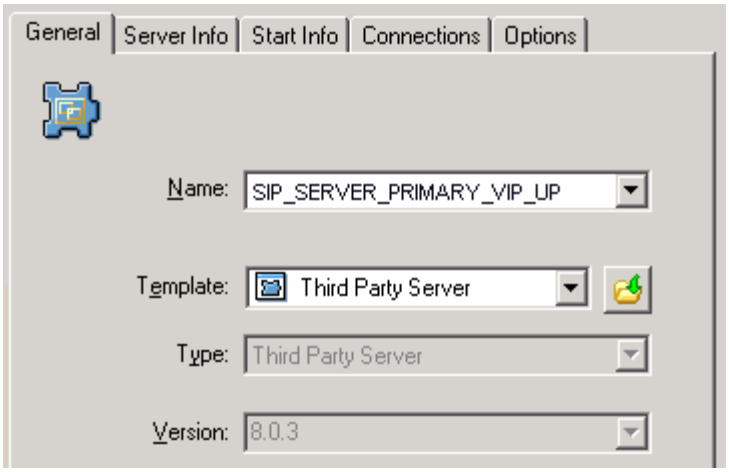
```
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 10.10.11.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

8. Verify that the Virtual IP interface is not running on the primary SIP Server host by using the `ipconfig` command. Output should appear similar to the following:
   **[+] Example ipconfig command**

```
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

## Create Application objects for Virtual IP address control scripts

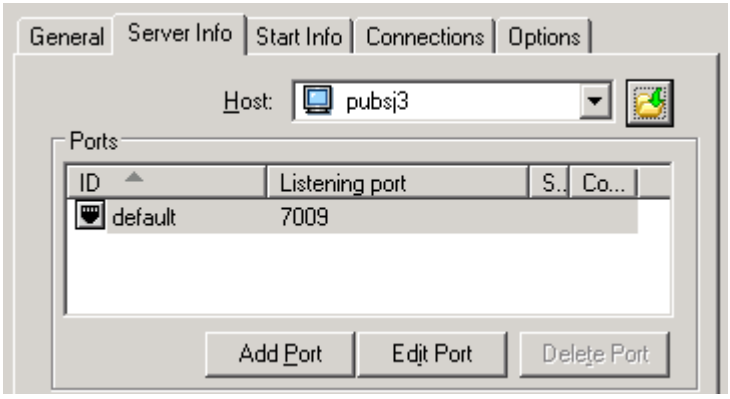
1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click `OK`.
4. On the General tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.




Configuring the Application Object for the Script, General Tab: Sample Configuration

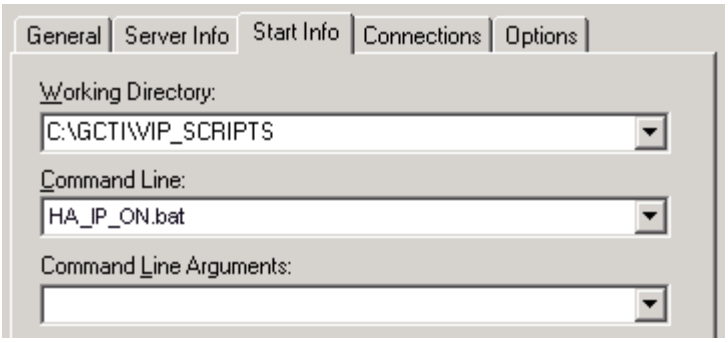
> **Important**
>
> You can use the suggested Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the Edit Port option.




Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the Virtual IP address control script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter the script name that enables the Virtual IP address (`HA_IP_ON.bat`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP address (`HA_IP_OFF.bat`).



Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

b. If you are configuring an Application object that disables the Virtual IP address (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four Virtual IP address control scripts.

## Verify the HA configuration

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 2: Manual switchback
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 3: Stop primary SIP Server
   a. Establish a call between two SIP endpoints.
   b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

# Linux

Complete these steps to set up SIP Server HA on Linux, using the IP Address Takeover method.

1. Ensure that your system meets the deployment prerequisites
2. Configure the primary SIP Server
3. Configure the backup SIP Server
4. Create a configuration file for the Virtual IP interface
5. Create Virtual IP address control scripts
6. Create Application objects for Virtual IP address control scripts
7. Verify the HA configuration

## Ensure that your system meets the deployment prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

  > **Important**
  >
  > Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - LCA release 8.1.2 or higher must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet.

A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.

- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

## Configure the primary SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to `true`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**

- **addp-timeout**
- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tou**t option to at least two times the timeout value plus the established network latency.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. Click Apply to save the configuration changes.

5. Click the Switches tab.
   a. Ensure that the correct Switch object is specified. If necessary, select the correct Switch object by using the Add button.
   b. Click Apply to save the configuration changes.
6. Click the Server Info tab.
   a. Select the Redundancy Type. You can select either Hot Standby or Warm Standby.
   b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.
      i. In the Ports section, select the port to which the backup SIP Server will connect for HA data synchronization, and click Edit Port.
      ii. In the Port Properties dialog box, on the Port Info tab, select the HA sync check box.
      iii. Click OK.
   c. For the Backup Server option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
   d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
8. Click Apply and then OK to save the configuration changes.

## Configure the backup SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.

3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. Select Properties.
4. Click the Switches tab.
   a. Click Add, and select the Switch object that you associated with the primary SIP Server Application object.
   b. Click Apply to save the configuration changes.
5. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
6. Click the Options tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the same port number that you specified for the primary SIP Server.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to true.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (SIP_SERVER_BACKUP_VIP_UP) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the sip-vip-script-down option to the name of the Application object (SIP_SERVER_BACKUP_VIP_DOWN) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to true.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to true.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to true.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to true.
      x. Click Apply to save the configuration changes.
   b. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**
      - **addp-remote-timeout**

      In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.
   c. Click Apply to save the configuration changes.
7. Click Apply and then OK to save the configuration changes.

## Create a configuration file for the Virtual IP interface

1. On each of the SIP Server host computers, locate the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.
2. Create a copy that is named `/etc/sysconfig/network-scripts/ifcfg-eth0:1`.
3. Define `IPADDR`, `NETMASK`, and `NETWORK` parameters values for the Virtual IP interface. When you are finished, the content of the file should appear similar to the following example:

```
DEVICE=eth0:1
BOOTPROTO=static
USERCTL=yes
TYPE=Ethernet
IPADDR=192.51.14.208
NETMASK=255.255.255.0
NETWORK=192.51.14.0
BROADCAST=192.51.14.255
ONPARENT=no
```

## Create Virtual IP address control scripts

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP interface and another to disable it—for example:
   - `set_ip_up.sh`—To enable the Virtual IP interface.

   **[+] Commands for ''set_ip_up.sh''**

```
#!/bin/sh
# Set the path in which log files will be stored
Logpath=<Specify the path to log files>
# For example Logpath=/home/Logs
echo -e "\n--------Bringing VIP Up----------" >> $Logpath/Takeover_On.log
date >> $Logpath/Takeover_On.log
# Set the following parameter corresponding to your machine configuration
Interface=<Interface in which VIP should be added>
# For example Interface=eth0:1
Virtual_IP=<Virtual IP of the Machine>
# For example Virtual_IP=172.24.133.254
Gateway=<Gateway of the Machine>
# For example Gateway=10.1.1.1
ping_count=1
loop_count=20
# Looping up to 20 count or till VIP disabled in the HA pair
for (( i=1; i<=$loop_count;i++ ))
do
result=$(ping -c $ping_count $Virtual_IP | grep "bytes from")
if [ "$result" ]
then
echo "$i ping reply got from the HA pair" >> $Logpath/Takeover_On.log
sleep 1
else
echo "VIP disabled in the HA pair" >> $Logpath/Takeover_On.log
# Enabling the VIP once it is disabled in paired host
break
```

```
fi
done
/sbin/ifconfig $Interface $Virtual_IP up
# Update the ARP cache of the gateway
arping -s $Virtual_IP $Gateway -f
echo -e "\n--------VIP enabled in this machine----------" >> $Logpath/Takeover_On.log
date >> $Logpath/Takeover_On.log
exit
```

- `set_ip_down.sh`—To disable the Virtual IP interface.

**[+] Commands for ''set_ip_down.sh''**

```
# Set the path in which log files will be stored
Logpath= <Specify the path to log files>
# For example Logpath=/home/Logs
echo -e "\n----------Bringing VIP down---------" >> $Logpath/Takeover_Off.log
date >> $Logpath/Takeover_Off.log
# Set the following parameter corresponding to your machine configuration
Interface=<Interface in which VIP should be added>
Virtual_IP=<Virtual IP of the Machine>
/sbin/ifconfig $Interface down
sleep 10
# Update arpcache of the local machine
ping -c 2 $Virtual_IP
echo -e "---------VIP disabled--------------" >> $Logpath/Takeover_Off.log
```

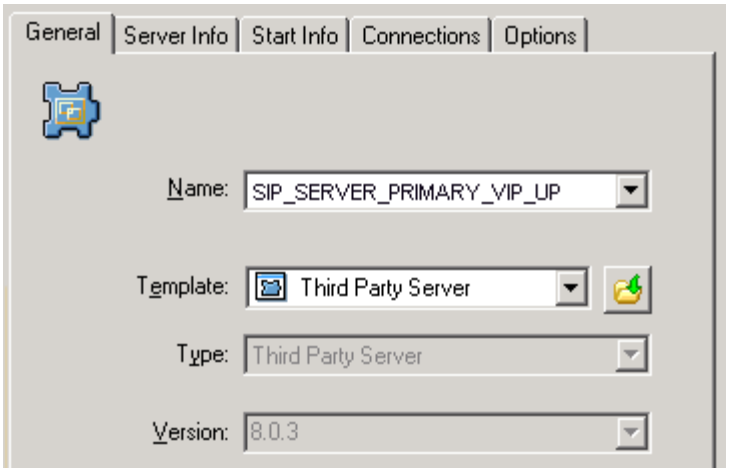
2. In the shell file, replace the variables indicated by angle brackets with appropriate values.
3. Add the `set_ip_down.sh` script as a startup script by adding the script to the current run-level of the machine.
   a. Copy `set_ip_down.sh` to the `/etc/init.d` folder.
   b. Create a symlink from your run-level directory to execute when a system starts to disable the Virtual IP. For example, if the run-level is 5, the creation of symlink is as follows:

      ```
      ln -s /etc/init.d/<scriptfile> /etc/rc.d/rc5.d/S50<scriptfile>
      ```

      The S50 tells the system to start the script when it starts.

## Create Application objects for Virtual IP address control scripts

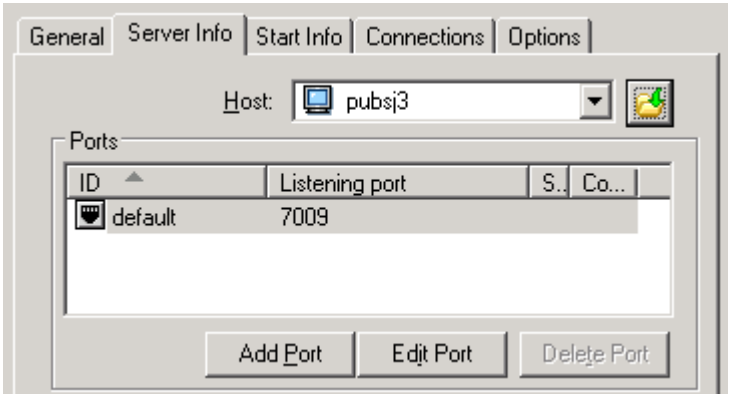
1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click `OK`.
4. On the `General` tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.




Configuring the Application Object for the Script, General Tab: Sample Configuration

> **Important**
>
> You can use the previously listed Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the `Edit Port` option.




Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter the script name that enables the Virtual IP address (`set_ip_up.sh`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP address (`set_ip_down.sh`).
   b. If you are configuring an Application object that disables the Virtual IP interface (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup`

value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

## Verify the HA configuration

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 2: Manual switchback
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 3: Stop primary SIP Server
   a. Establish a call between two SIP endpoints.
   b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

# AIX

Complete these steps to set up SIP Server HA on AIX, using the IP Address Takeover method.

1. Ensure that your system meets the deployment prerequisites
2. Configure the primary SIP Server
3. Configure the backup SIP Server
4. Create Virtual IP address control scripts
5. Create Application objects for Virtual IP address control scripts
6. Verify the HA configuration

## Ensure that your system meets the deployment prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

> **Important**
>
> Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - LCA release 8.1.2 or higher must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with

SIP Server might fail to update the ARP table during Virtual IP Address Takeover.

- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

## Configure the primary SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to `true`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**

- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tou**t option to at least two times the timeout value plus the established network latency.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. Click Apply to save the configuration changes.

5. Click the Switches tab.
   a. Ensure that the correct Switch object is specified. If necessary, select the correct Switch object by using the Add button.
   b. Click Apply to save the configuration changes.
6. Click the Server Info tab.
   a. Select the Redundancy Type. You can select either Hot Standby or Warm Standby.
   b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.
      i. In the Ports section, select the port to which the backup SIP Server will connect for HA data synchronization, and click Edit Port.
      ii. In the Port Properties dialog box, on the Port Info tab, select the HA sync check box.
      iii. Click OK.
   c. For the Backup Server option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
   d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
8. Click Apply and then OK to save the configuration changes.

## Configure the backup SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to

configure as the backup SIP Server. Select Properties.

4. Click the Switches tab.
   a. Click Add, and select the Switch object that you associated with the primary SIP Server Application object.
   b. Click Apply to save the configuration changes.
5. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
6. Click the Options tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the same port number that you specified for the primary SIP Server.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to true.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (SIP_SERVER_BACKUP_VIP_UP) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the sip-vip-script-down option to the name of the Application object (SIP_SERVER_BACKUP_VIP_DOWN) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to true.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to true.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to true.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to true.
      x. Click Apply to save the configuration changes.
   b. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**
      - **addp-remote-timeout**

      In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.
   c. Click Apply to save the configuration changes.
7. Click Apply and then OK to save the configuration changes.

## Create Virtual IP address control scripts

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP address and another to disable it—for example:
   - `set_ip_up.sh`—To enable the Virtual IP address
   - `set_ip_down.sh`—To disable the Virtual IP address
2. In the `set_ip_up.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface> <vip_address> netmask <vip_netmask> alias`
   where:
   - `<name_of_ethernet_interface>` is the name of the Virtual IP interface
   - `<vip_address>` is the Virtual IP–interface IP address
   - `<vip_netmask>` is the Virtual IP netmask
3. In the `set_ip_down.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface> <vip_address> delete`
   where:
   - `<name_of_ethernet_interface>` is the name of the Virtual IP interface
   - `<vip_address>` is the Virtual IP–interface IP address

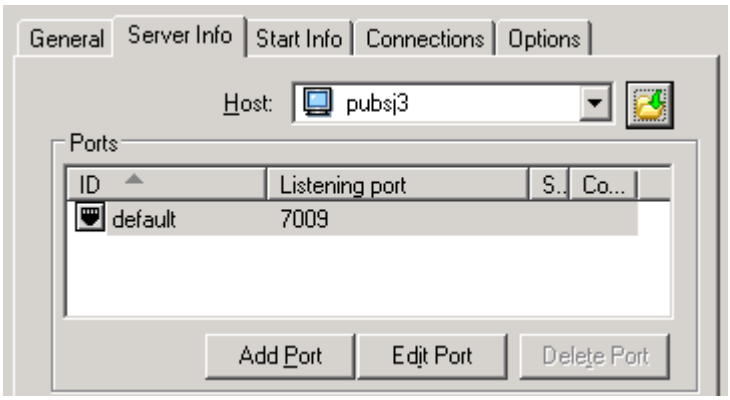
## Create Application objects for Virtual IP address control scripts

1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click `OK`.
4. On the `General` tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.


Configuring the Application Object for the Script, General Tab: Sample Configuration

> **Important**
> You can use the previously listed Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the `Edit Port` option.




Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter the script name that enables the Virtual IP address (`set_ip_up.sh`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP address (`set_ip_down.sh`).
   b. If you are configuring an Application object that disables the Virtual IP interface (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

## Verify the HA configuration

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

5. Test 2: Manual switchback
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 3: Stop primary SIP Server
   a. Establish a call between two SIP endpoints.
   b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

# Solaris

Complete these steps to set up SIP Server HA on Solaris, using the IP Address Takeover method.

1. Ensure that your system meets the deployment prerequisites
2. Configure the primary SIP Server
3. Configure the backup SIP Server
4. Create Virtual IP address control scripts
5. Create Application objects for Virtual IP address control scripts
6. Verify the HA configuration

## Ensure that your system meets the deployment prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

> **Important**
>
> Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - LCA release 8.1.2 or higher must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with

SIP Server might fail to update the ARP table during Virtual IP Address Takeover.

- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

## Configure the primary SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to `true`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**

- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tou**t option to at least two times the timeout value plus the established network latency.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. Click Apply to save the configuration changes.

5. Click the Switches tab.
   a. Ensure that the correct Switch object is specified. If necessary, select the correct Switch object by using the Add button.
   b. Click Apply to save the configuration changes.
6. Click the Server Info tab.
   a. Select the Redundancy Type. You can select either Hot Standby or Warm Standby.
   b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.
      i. In the Ports section, select the port to which the backup SIP Server will connect for HA data synchronization, and click Edit Port.
      ii. In the Port Properties dialog box, on the Port Info tab, select the HA sync check box.
      iii. Click OK.
   c. For the Backup Server option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
   d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
8. Click Apply and then OK to save the configuration changes.

## Configure the backup SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to

configure as the backup SIP Server. Select Properties.

4. Click the Switches tab.
   a. Click Add, and select the Switch object that you associated with the primary SIP Server Application object.
   b. Click Apply to save the configuration changes.
5. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
6. Click the Options tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the same port number that you specified for the primary SIP Server.
      ii. Set the **sip-address** option to the Virtual IP address.
      iii. Set the **control-vip-scripts** option to true.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (SIP_SERVER_BACKUP_VIP_UP) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the sip-vip-script-down option to the name of the Application object (SIP_SERVER_BACKUP_VIP_DOWN) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. To enable Virtual IP address monitoring, set the **sip-iptakeover-monitoring** option to true.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to true.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to true.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to true.
      x. Click Apply to save the configuration changes.
   b. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**
      - **addp-remote-timeout**

      In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.
   c. Click Apply to save the configuration changes.
7. Click Apply and then OK to save the configuration changes.

## Create Virtual IP address control scripts

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP interface and another to disable it--for example:
   - `set_ip_up.sh`—To enable the Virtual IP interface
   - `set_ip_down.sh`—To disable the Virtual IP interface
2. In the `set_ip_up.sh` file, enter the following command line:
   `ifconfig hostname.<interface_name>:<n> up`
   where `interface_name` is the name of the Virtual IP interface—for example:
   `ifconfig /etc/hostname.dmfe0:1 up`
3. In the `set_ip_down.sh` file, enter the following command line:
   `ifconfig hostname.<interface_name>:<n> down`
   where `interface_name` is the name of the Virtual IP interface—for example:
   `ifconfig /etc/hostname.dmfe0:1 down`

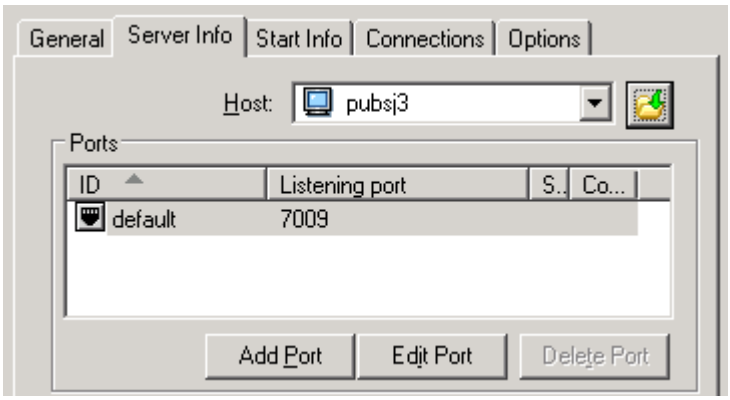
## Create Application objects for Virtual IP address control scripts

1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click `OK`.
4. On the `General` tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.


Configuring the Application Object for the Script, General Tab: Sample Configuration

> **Important**
> You can use the previously listed Application object names, or you can specify your own.

5. Select the Server Info tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the Edit Port option.




Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the Start Info tab.
   a. Set the Working Directory to the location of the script, and enter the name of the script in the Command Line field. For example, for the SIP_SERVER_PRIMARY_VIP_UP Application object, enter the script name that enables the Virtual IP address (set_ip_up.sh). For the SIP_SERVER_PRIMARY_VIP_DOWN Application object, enter the script name that disables the Virtual IP address (set_ip_down.sh).
   b. If you are configuring an Application object that disables the Virtual IP interface (SIP_SERVER_PRIMARY_VIP_DOWN and SIP_SERVER_BACKUP_VIP_DOWN), set the Timeout Startup value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

## Verify the HA configuration

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 2: Manual switchback
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles

have changed.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

5. Test 3: Stop primary SIP Server

a. Establish a call between two SIP endpoints.

b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

# Windows NLB Cluster

Complete these steps to set up SIP Server HA on Windows, using Windows Network Load Balancing (NLB) Cluster functionality.

1. Check prerequisites
2. Configure Windows NLB parameters
3. Configure the primary SIP Server
4. Configure the backup SIP Server
5. Create Cluster control scripts
6. Create Application objects for Cluster control scripts
7. Verify the HA configuration

## Check prerequisites

The following are the basic requirements and recommendations that must be complete before you can deploy a SIP Server HA configuration in a Windows NLB Cluster environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

> **Important**
>
> Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Operating-system requirement:
  - Windows Server 2008 or later with Microsoft Windows Network Load Balancing (NLB).
- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - Local Control Agent (LCA) release 8.1.2 or higher must be installed and configured on both host computers.
- Networking requirements:
  - A name-resolution method such as Domain Name System (DNS), DNS dynamic-update protocol, or Windows Internet Name Service (WINS) is required.
  - Both host computers must be members of the same domain.

- A domain-level account that is a member of the local Administrators group is required on each host computer. A dedicated account is recommended.
- Each host computer must have a unique NetBIOS name.
- A static IP address is required for each of the network interfaces on both host computers.

> **Important**
>
> Server clustering does not support IP addresses that are assigned through Dynamic Host Configuration Protocol (DHCP) servers.

- A dedicated network switch or separate virtual local-area network (VLAN) for cluster adapters is recommended to reduce switch flooding that might be caused by Windows NLB.
- Access to a domain controller is required. If the cluster service is unable to authenticate the user account that is used to start the service, the cluster might fail. It is recommended that the domain controller be on the same local-area network (LAN) as the cluster, to ensure availability.
- Each node must have at least two network adapters: one for the connection to the public network and another for the connection to the private node-to-node cluster network.
- A dedicated private-network adapter is required for HCL certification.
- All nodes must have two physically independent LANs or VLANs for public and private communication.
- If you are using fault-tolerant network cards or network-adapter teaming, verify that firmware and drivers are up to date, and check with your network-adapter manufacturer for Windows NLB cluster compatibility.
- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

## Configure Windows NLB parameters

1. Open the Microsoft Network Load Balancing Manager tool.
2. Select a cluster host, and open the `Cluster Properties` window.
3. On the `Cluster Parameters` tab, select the `Cluster operation mode`. You can choose either Unicast (default) or Multicast mode. For information about Windows NLB Unicast and Multicast modes, refer to your Microsoft Windows Server documentation.
4. Click the `Port Rules` tab.
   a. Specify a `Port range` that includes the port that you will assign as the `sip-port`. See "Configuring the primary SIP Server".
   b. In the `Protocols` section, select `Both` (both UDP and TCP).
   c. In the `Filtering mode` section, select `Multiple host`, and set `Affinity` to either `None` or `Single`.

   d. Set `Load weight` to `Equal`.

5. Click the `Host Parameters` tab. In the `Initial host state` section, set the `Default state` to `Stopped`.

For more information about Windows NLB cluster parameters, refer to your Microsoft Windows Server documentation.

## Configure the primary SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the **sip-address** option to the Windows NLB cluster IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. Disable Virtual IP address monitoring by setting the **sip-iptakeover-monitoring** option to `false`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the `sip-nic-address` option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**

- **addp-timeout**
- **addp-remote-timeout**

In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. Click Apply to save the configuration changes.

5. Click the Switches tab.
   a. Ensure that the correct Switch object is specified. If necessary, select the correct Switch object by using the Add button.
   b. Click Apply to save the configuration changes.
6. Click the Server Info tab.
   a. Select the Redundancy Type. You can select either Hot Standby or Warm Standby.
   b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.
      i. In the Ports section, select the port to which the backup SIP Server will connect for HA data synchronization, and click Edit Port.
      ii. In the Port Properties dialog box, on the Port Info tab, select the HA sync check box.
      iii. Click OK.
   d. For the Backup Server option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
   e. Click Apply to save the configuration changes.
7. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
8. Click Apply and then OK to save the configuration changes.

## Configure the backup SIP Server

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.

3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. Select Properties.
4. Click the Switches tab.
   a. Click Add, and select the Switch object that you associated with the primary SIP Server Application object.
   b. Click Apply to save the configuration changes.
5. Click the Start Info tab.
   a. Select Auto-Restart.
   b. Click Apply to save the configuration changes.
6. Click the Options tab.
   a. Select the **[TServer]** section.
      i. Set the **sip-port** option to the same port number that you specified for the primary SIP Server.
      ii. Set the **sip-address** option to the Windows NLB cluster IP address.
      iii. Set the **control-vip-scripts** option to true.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (SIP_SERVER_BACKUP_VIP_UP) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (SIP_SERVER_BACKUP_VIP_DOWN) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. Disable Virtual IP address monitoring by setting the **sip-iptakeover-monitoring** option to false.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to true.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to true.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to true.
      x. Click Apply to save the configuration changes.
   b. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**
      - **addp-remote-timeout**

      In the preceding example, the guideline that is used to configure ADDP settings is to set the **addp-timeout** and **addp-remote-timeout** options to 5 sec or at least two times the established network-latency time, and to set the **sync-reconnect-tout** option to at least two times the timeout value plus the established network latency.
   c. Click Apply to save the configuration changes.
7. Click Apply and then OK to save the configuration changes.

## Create Cluster control scripts

1. On the primary SIP Server host computer, create a batch file that is named `sip_server_primary_vip_up.bat` and enter the following commands:
   **[+] Commands for sip_server_primary_vip_up.bat**

   ```
   @title Enable Cluster Control Script
   @echo ************** Primary Virtual IP Enabled ************* >>
   vip1.log
   @echo %time% >> vip1.log
   wlbs.exe start sipcluster:host1_ip >> vip1.log
   wlbs.exe enable 5060 sipcluster:host1_ip >> vip1.log
   wlbs.exe drainstop sipcluster:host2_ip >> vip1.log
   exit
   ```

   where:

   - `host1_ip` is the dedicated cluster IP address of the primary host
   - `host2_ip` is the dedicated cluster IP address of the backup host

2. On the primary SIP Server host computer, create a batch file that is named `sip_server_primary_vip_down.bat` and enter the following commands:
   **[+] Commands for sip_server_primary_vip_down.bat**

   ```
   @title Disable Cluster Control Script
   @echo *************** Primary Virtual IP Disabled ************ >>
   vip1.log
   @echo %time% >> vip1.log
   wlbs.exe drainstop sipcluster:host1_ip >> vip1.log
   ping -n 2 127.0.0.1
   exit
   ```

3. On the backup SIP Server host computer, create a batch file that is named `sip_server_backup_vip_up.bat` and enter the following commands:
   **[+] Commands for sip_server_backup_vip_up.bat**

   ```
   @title Enable Cluster Control Script
   @echo ************** Backup Virtual IP Enabled *************** >>
   vip2.log
   @echo %time% >> vip2.log
   wlbs.exe start sipcluster:host2_ip >> vip2.log
   wlbs.exe enable 5060 sipcluster:host2_ip >> vip2.log
   wlbs.exe drainstop sipcluster:host1_ip >> vip2.log
   exit
   ```

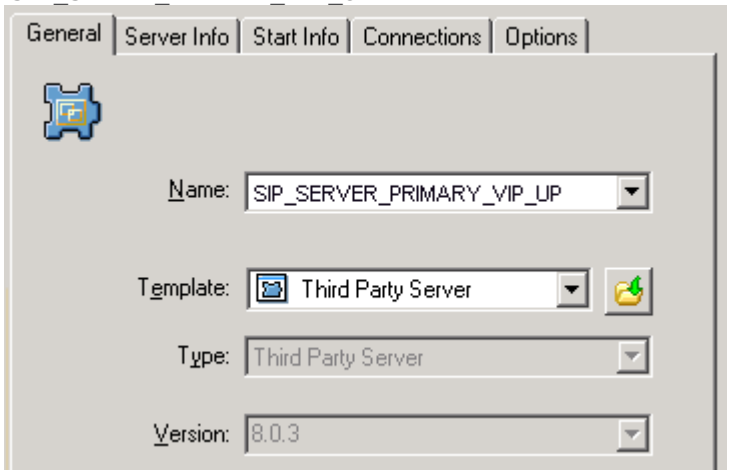
4. On the backup SIP Server host computer, create a batch file that is named `sip_server_backup_vip_down.bat` and enter the following commands:
   **[+] Commands for sip_server_backup_vip_down.bat**

   ```
   @title Disable Cluster Control Script
   @echo ***************** Backup Virtual IP Disabled ************ >>
   vip2.log
   @echo %time% >> vip2.log
   wlbs.exe drainstop sipcluster:host2_ip >> vip2.log
   ping -n 2 127.0.0.1
   exit
   ```

> **Important**
> The preceding scripts include commands for logging script execution. The logs are created in the directory in which the script is located.

## Creating Application objects for Cluster control scripts

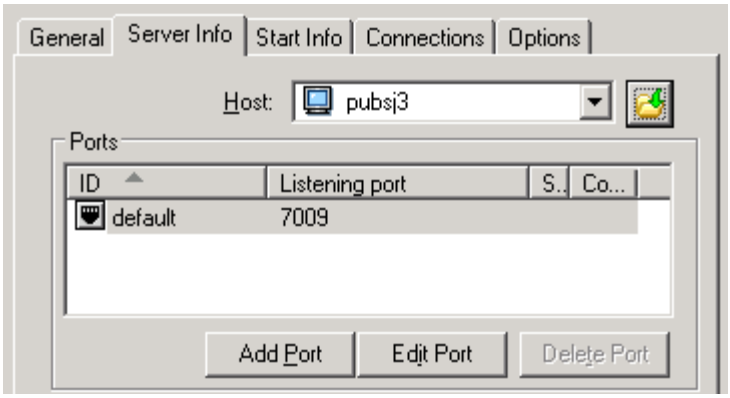
1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the Third Party Server template from the Application Templates folder, and click OK.
4. On the `General` tab, enter the name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.



Configuring the Application Object for the Script, General Tab: Sample Configuration

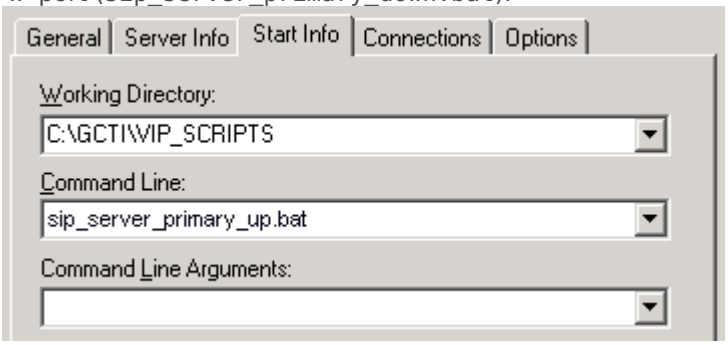
> **Important**
> You can use the suggested Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Cluster control script is located.
   b. If necessary, specify a valid communication-port number by using the `Edit Port` option.




Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the control script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter the script name that enables the Virtual IP port (`sip_server_primary_up.bat`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP port (`sip_server_primary_down.bat`).




Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

   b. If you are configuring an Application object that disables a Virtual IP port (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four Cluster control scripts.

## Verify the HA configuration

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

5. Test 2: Manual switchback

a. Establish a call between two SIP endpoints.

b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

5. Test 3: Stop primary SIP Server

a. Establish a call between two SIP endpoints.

b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

# Using SIP Proxy

Complete these steps to set up SIP Server HA using SIP Proxy. The procedure applies to both Windows and Linux deployments.

1. Configure the sip-outbound-proxy DN
2. Configure SIP Proxy
3. Configure primary and backup SIP Servers
4. Configure multi-site call handling

## Configure the sip-outbound-proxy DN

1. In the SIP Server Switch, create a DN of type `Voice over IP Service`. For a multi-site deployment, you must create several DNs of this type, one for each Switch/Site served by a SIP Server HA pair.
2. In the Options > **[TServer]** section, configure the following mandatory options:
   - **contact**—Set this option to the SIP Proxy FQDN resolved into a single or multiple SRV records.
   - **external-contact**—Set this option to the SIP Proxy address using the `host:port` format.
   - **oos-check**—Specify how often, in seconds, SIP Server checks SIP Proxy for out-of-service status.
   - **oos-force**—Specify the time interval, in seconds, that SIP Server waits before placing an unresponsive SIP Proxy in out-of-service state when the **oos-check** option is enabled.
   - **service-type**—Set this option to `sip-outbound-proxy`.

> **Important**
>
> Active Out-of-Service Detection feature (**oos-check** and **oos-force** options) must be enabled for SIP Proxy to work.

## Configure SIP Proxy

1. Create a SIP Proxy Application of the *Genesys Generic Server* type by importing the SIP Proxy Application Template `SIPProxy_811.apd` from the product installation package. A SIP Proxy Application must be created for each SIP Proxy instance.
2. On the Server Info tab, set the following parameters:

- Host—Specify the host on which this SIP Proxy is installed.
- Port IDs—Specify the following SIP Proxy ports:
  - `sip-port`, Connection Protocol: `sip`
  - `http-port`, Connection Protocol: `http` (Optional)

3. On the Options tab, create a section named `sipproxy`. In the **[sipproxy]** section, add the following options:
   - **applications**—For a multi-site environment, specify the application names of all primary SIP Servers in the environment, separated by a comma.
   - **oos-check**—Set to 5 by default.
   - **oos-force**—Set to 5 by default.
   - **serving-sipserver**—Specify the primary SIP Server application name to which all requests from endpoints and media gateways will be forwarded.
   - **sipproxy-role**—Set to `10`.
4. (Optional) On the Options tab, in the **[log]** section, you can add log options as necessary. Refer to the Framework 8.1 SIP Server Deployment Guide for detailed information about log options.
5. Install SIP Proxy by completing the following steps:
   1. On the product CD, navigate to the SIP Proxy [/media_layer/SIP_Proxy/windows_x64/] folder, and open the subdirectory windows.
   2. Double-click `Setup.exe` to start the InstallShield installation wizard.
   3. Follow the InstallShield wizard instructions to install SIP Proxy. InstallShield creates a batch file in the folder of the component it installs.
   4. Open the batch file and ensure that it includes the parameter `-app <appname>`, where `appname` is the name of the SIP Proxy application object that you have created in the Configuration Layer.

## Configure primary and backup SIP Servers

- In the Options > **[TServer]** section, configure the following options in both primary and backup SIP Server Applications:
  - **sip-address**—Set this option to the IP address of the SIP interface of SIP Server.
  - **sip-outbound-proxy**—Set this option to `true`.
  - **sip-enable-rfc3263**—Set this option to `true`.
  - **sip-enable-gdns**—Ensure this option is set to `true`.

> ### Important
> Both primary and backup SIP Servers must have the same **sip-port** setting.

## Configure multi-site call handling

In the SIP Server Switch, create DNs of type Trunk. In the Options > **[TServer]** section, configure the mandatory options depending on whether DNS resolution is used:

- ***If DNS resolution is used***, configure the following mandatory options:
  - **contact**—Set this option to the FQDN resolved into the SRV records of the primary and backup SIP Servers at the destination site.
  - **oos-check**
  - **oos-force**
  - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
  - **resolve-external-contact**—Set this option to `true` on all trunks that have **peer-proxy-contact** configured.
  - **replace-uri-contact**—Set this option to `true`.

> **Important**
> For a Business Continuity deployment, DNS resolution must be used.

- ***If DNS resolution is not used***, create one Trunk DN for each SIP Server in an HA pair.
  - In the first Trunk DN, configure the following mandatory options:
    - **contact**—Set this option to the `host:port` of the primary SIP Server at the destination site.
    - **oos-check**
    - **oos-force**
    - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
  - In the second Trunk DN, configure the following mandatory options:
    - **contact**—Set this option to the `host:port` of the backup SIP Server at the destination site.
    - **oos-check**
    - **oos-force**
    - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.

## Important

For additional configuration options that might be configured for a particular device, see the Framework 8.1 SIP Server Deployment Guide.

# Configuring TLS

Secure data transfer using TLS is now supported between SIP Server and Active-Active Resource Managers in IP Address Takeover and Windows NLB Cluster high-availability deployments. TLS is also supported between SIP Server and all SIP devices, including SBCs, Media Gateways, and SIP phones.

The integration solution described in this section makes the following assumptions:

- TLS transport is used for SIP signaling
- SIP Server performs load balancing between an Active-Active Resource Manager pair

## Configuration Steps

1. Provision SSL certificates for workstations hosting SIP Servers, RM, and MCP applications. Refer to the ''Genesys 8.1 Security Deployment Guide''.
2. Configure SIP Server to use TLS data transfer. Refer to the *Transport Layer Security for SIP Traffic* section in the ''Framework 8.1 SIP Server Deployment Guide''.
3. Configure Resource Managers in an Active-Active high-availability cluster. Refer to the *Genesys Voice Platform Integration* section in the ''Framework 8.1 SIP Server Deployment Guide''.

To configure TLS data transfer between Genesys Media Server components, refer to the ''Genesys Media Server 8.1 Deployment Guide''.

### SIP Phones

To use TLS data transfer between SIP Server (IP Address Takeover and Windows NLB HA configurations) and SIP Endpoints, complete these additional steps:

1. Create an additional certificate for a FQDN that corresponds to the IP address specified in the **sip-address** option (Virtual IP address) of the SIP Server application. Install this certificate on both hosts on which the primary and backup SIP Servers run.
2. Make sure that the following conditions exist, as appropriate:
   - On Windows, the **sip-tls-cert** option is set to the thumbprint obtained from the certificate generated in Step 1, above.
   - On UNIX, the **sip-tls-cert** option is set to the path and filename of the `.pem` encoded file that contains the host certificate created in Step 1, above.

# HA Configuration Options

This topic describes configuration options that are specific to the high availability (HA) configuration. For Business Continuity-specific options, see the BC Configuration Options topic for details.

For a complete list of configuration options, refer to the *SIP Server Deployment Guide*.

## backup-init-check

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After restart
Related Feature: Verifying Initialization Status in Backup SIP Servers

When set to `true`, SIP Server in Backup mode verifies that all internal components (T-Controller, Smart Proxy, Interaction Proxy, and Operational Information thread) are successfully initialized, and can provide the service when SIP Server switches to Primary mode. If some components fail to complete initialization, SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS. The timeout for internal components to complete initialization is defined by the **backup-init-check-timeout** option.

## backup-init-check-timeout

Setting: [TServer] section, Application level
Default Value: `60`
Valid Values: `15-3600`
Changes Take Effect: After restart
Related Feature: Verifying Initialization Status in Backup SIP Servers

Restricted option. Specifies the timeout, in seconds, during which SIP Server verifies that all internal components are successfully initialized in a scenario described by the backup-init-check option.

## backup-sip-port-check

Setting: [TServer] section, Application level
Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: After restart
Related Feature: Verifying Initialization Status in Backup SIP Servers

When set to `true`, SIP Server in Backup mode attempts to open a SIP port. If the port opens successfully, no SIP messages are processed, and SIP Server closes the port immediately. If the SIP port does not open, SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS. This functionality is enabled only when **backup-init-check** is set to `true`. The functionality is disabled in the IP Address Takeover configuration, when the **control-vip-scripts** option is set to `true`.

### control-vip-scripts

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After SIP Server restart

For the Hot Standby configuration. When set to `true`, SIP Server itself controls execution of Virtual IP address control scripts through the LCA component. The names of the Application objects representing scripts are configured using the **sip-vip-script-up** and **sip-vip-script-down** options. SIP Server instructs LCA to execute the **sip-vip-script-up** option when switching to the primary mode, or the **sip-vip-script-down** option when switching to the backup mode.

### control-remote-vip-scripts

Setting: [TServer] section, Application level
Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: After SIP Server restart

If only a single SIP Server is started out of the HA pair, the **sip-vip-script-down** option might need to be executed on the host where SIP Server is not started. When set to `true`, SIP Server connects to the remote LCA and executes the Virtual IP address control scripts on the remote host. This option applies only if the value of the **control-vip-scripts** option is set to `true`.
**Note:** This option is reserved by Genesys Engineering. Use it only when requested by Genesys Customer Care.

### ha-max-calls-sync-at-once

Setting: [TServer] section, Application level
Default Value: `500`
Valid Values: `200-1000`
Changes Take Effect: When the HA connection is established
Related Feature: Enhanced Procedure for Upgrading of SIP Server HA Pair

Specifies the maximum number of calls that can be synchronized at once between the primary SIP Server and the backup SIP Server after the HA link connection is established, before waiting for 1 second to continue with synchronization. Only calls that are missing on the backup SIP Server are synchronized.

### network-monitoring-timeout

Setting: [TServer] section, Application level
Default Value: `1`
Valid Values: `1-30`
Changes Take Effect: Immediately
Dependent Options: **sip-nic-address**, **tlib-nic-monitoring**, **sip-iptakeover-monitoring**
Related Feature: Network Status Monitoring

Defines the time interval (in seconds) for which SIP Server checks the network status of:

- The SIP NIC, if a dedicated NIC is used and the **sip-nic-address** option is configured.

- The T-Library NIC, if the value of the **tlib-nic-monitoring** option is set to `true`.
- The Virtual IP address for the IP Address Takeover configuration, if the value of the **sip-iptakeover-monitoring** option is set to `true`.

## sip-error-codes-overflow

Setting: [TServer] section, Application level
Default Value: An empty string (or 503 error code)
Valid Values: A list of patterns for numeric error codes separated by a comma (,). Letter X in a pattern represents any digit. A single pattern must start with a digit and contain all 3 digits, and a pattern containing "X" should conclude the pattern's list, if present. Examples:

- `503`
- `503,504`
- `487,50X`
- `487,5XX`
- Patterns `5X3,XXX` are invalid

Changes Take Effect: For the next call
Related Feature: Enhanced disaster recovery solution for outbound calls

When, on an initial INVITE message, SIP Server receives a negative response containing the error code that matches the option value setting, SIP Server attempts to find an alternative trunk or softswitch to initiate a call.

## sip-iptakeover-monitoring

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After SIP Server restart
Dependent Option: **sip-address**
Related Feature: Network Status Monitoring

For the Hot Standby IP Address Takeover configuration. When set to `true`, this option enables the Virtual IP address status monitoring. The Virtual IP address is taken from the **sip-address** option.

## sip-nic-address

Setting: [TServer] section, Application level
Default Value: NULL
Valid Values: Any valid IP address or FQDN
Changes Take Effect: After SIP Server restart
Dependent Option: **sip-nic-monitoring**
Related Feature: Network Status Monitoring

This option can be set in deployments with dedicated SIP NICs where the SIP traffic is separated from the T-Library network traffic. This option specifies the IP address of the NIC that belong to the host where the SIP Server runs and is used for SIP traffic. This IP address must always be present on this

host regardless of the role of SIP Server (primary or backup). For the IP Address Takeover configuration, its unique IP address is associated with the SIP NIC, not the Virtual IP address.

### sip-nic-monitoring

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After SIP Server restart
Dependent Option: **sip-nic-address**
Related Feature: Network Status Monitoring

When set to `true`, this option enables the SIP NIC IP address status monitoring. The SIP IP address is taken from the **sip-nic-address** option.

### sip-pass-check

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately
Related Feature: SIP Traffic Monitoring

When set to `true`, this option enables tracking of SIP messages that reach the primary SIP Server, including responses from SIP devices configured for Active Out-of-Service Detection.

The primary SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS when all devices configured with the Active OOS check have failed and no other SIP messages have been received for a period of time. The period of time is calculated as the maximum of the sums of the **oos-check** and **oos-force** option values configured for service DNs (if **oos-force** is less than 5, 5 is used). When SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS, SCS switches the primary SIP Server to the backup role, and SIP Server reports the SERVICE_RUNNING status to LCA/SCS. The backup SIP Server becomes the primary, and starts monitoring SIP traffic.

**Note:** If both the primary and backup servers receive no SIP traffic, a switchover would occur each time the effective out-of-service timeout expires. To prevent frequent switchovers in this case, SIP Server detects the “double switchover” condition and doubles the effective out-of-service timeout each time the double switchover happens, up to two times, or until one of the two servers detects SIP traffic. As soon as SIP traffic is detected, the server that detected the traffic remains the primary SIP Server and continues normal operation.

### sip-vip-script-down

Setting: [TServer] section, Application level
Default Value: NULL
Valid Values: Valid name of the Application object
Changes Take Effect: After SIP Server restart
Dependent Option: **control-vip-scripts**

For the Hot Standby configuration, if the **control-vip-scripts** option is set to `true`. It specifies the name of the Application object representing the scripts that is used to disable the Virtual IP address (or the port for Windows NLB Cluster) when SIP Server is switching to backup mode. The script must

be configured as an Application object of type `Third Party Server`.

For example, for a primary SIP Server, you will set the value of this option to `SIP_SERVER_PRIMARY_VIP_DOWN`, and for a backup SIP Server, you will set the value of this option to `SIP_SERVER_BACKUP_VIP_DOWN`.

### sip-vip-script-up

Setting: [TServer] section, Application level
Default Value: NULL
Valid Values: Valid name of the Application object
Changes Take Effect: After SIP Server restart
Dependent Option: **control-vip-scripts**

For the Hot Standby configuration, if the **control-vip-scripts** option is set to `true`. It specifies the name of the Application object representing the script that is used to enable the Virtual IP address (or the port for Windows NLB Cluster) when SIP Server is switching to primary mode. The script must be configured as an Application object of type `Third Party Server`.

For example, for a primary SIP Server, you will set the value of this option to `SIP_SERVER_PRIMARY_VIP_UP`, and for a backup SIP Server, you will set the value of this option to `SIP_SERVER_BACKUP_VIP_UP`.

### switchover-on-msml-oos

Setting: [TServer] section, the SIP Server Application (in standalone mode) or the VOIP Service DN with **service-type**=`sip-cluster-nodes` (SIP Cluster mode)
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: For the next call
Related Feature: Enhanced HA Resilience for Network Disruptions

Specifies the SIP Server action in case of losing connectivity with MSML VOIP Service DNs. When set to `true`, in the case of strict matching only, VOIP Service DNs with the same or alternative geo-location are considered. After detecting that those DNs are out of service, SIP Server checks one more time that MSML VOIP Service DNs are unresponsive, before reporting the SERVICE_UNAVAILABLE status to LCA/SCS in order to trigger a switchover.

### switchover-on-trunks-oos

Setting: [TServer] section, the SIP Server Application (in standalone mode) or the VOIP Service DN with **service-type**=`sip-cluster-nodes` (SIP Cluster mode)
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: For the next call
Related Feature: Enhanced HA Resilience for Network Disruptions

Specifies the SIP Server action in case of losing connectivity with Trunk DNs. When set to `true`, in the case of strict matching only, Trunk DNs with the same or alternative geo-location are considered. After detecting that those DNs are out of service, SIP Server checks one more time that Trunk DNs are unresponsive, before reporting the SERVICE_UNAVAILABLE status to LCA/SCS in order to trigger a switchover.

## tlib-nic-monitoring

Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After SIP Server restart
Related Feature: Network Status Monitoring

When set to `true`, this option enables T-Library NIC IP status monitoring. The T-Library IP address is taken from the Host object associated with the SIP Server application. The Host object name is used to resolve the T-Library NIC IP address.

## vip-state-change-timeout

Setting: [TServer] section, Application level
Default Value: `10`
Valid Values: `3-60`
Changes Take Effect: Immediately

Defines the maximum time allotted (in seconds) for the Virtual IP control script to execute. If the script fails to change the Virtual IP state during this timeout, SIP Server executes the script again. After several unsuccessful attempts, SIP Server declares that the Virtual IP script failed. The same script is not executed after the timeout expires.

# Enhanced Procedure for Upgrading SIP Server HA Pair

When a backup SIP Server is restarted or the HA connection between primary and backup was lost and then re-established, some calls would only exist on the primary SIP Server. Previously, SIP Server would not synchronize missing calls.

Starting with version 8.1.102.58, primary and backup SIP Servers, after establishing the HA connection, will exchange information about calls and trigger synchronization of missing calls to the backup SIP Server. The synchronization of new calls happens as soon as the HA connection is established.

Immediate switchover or failover after the HA connection is established (when either the primary or backup SIP Server reported readiness for a switchover equals 0) is considered as double failure.

## Readiness for Switchover or Upgrade

SIP Server reports readiness for a switchover or upgrade over its HTTP interface, as follows:
**http://<SIPSERVER_HOST>:<HTTP_PORT>/server?sipServer**

where <HTTP_PORT> is defined by the **http-port** configuration option in the SIP Server application.

The primary SIP Server reports readiness for a switchover (set to **1**) when all of the following occur:

- The HA connection is established.
- 60 seconds passed after HA link connection is established.
- All non-multisite calls are synchronized.
- All multisite calls that existed before the HA connection is established are finished.

The backup SIP Server reports readiness for a switchover (set to **1**) when all of the following occur:

- The HA connection is established.
- All calls are synchronized.

SIP Server reports readiness for an upgrade (set to **1**), when:

- The primary SIP Server is never ready. It must be switched to backup mode.
- The backup SIP Server is always ready.

Follow this procedure for upgrading the SIP Server HA pair:

1. Check the SIP Server that is running in the backup role for readiness to upgrade (set to **1**) using the SIP Server web interface.
2. Stop the backup SIP Server. Install a new SIP Server version and start the SIP Server.

3. Check the primary and backup SIP Servers for readiness to a switchover using the SIP Server web interface. If both of them are set to **1**, initiate a switchover. The upgraded SIP Server is now primary.
4. Check the SIP Server that is running in the backup role for readiness to upgrade (set to **1**) using the SIP Server web interface.
5. Stop the backup SIP Server. Install a new SIP Server version and start the SIP Server.

## Configuration Option

### ha-max-calls-sync-at-once

Section Name: **TServer**, Application level
Default Value: `500`
Valid Values: `200-1000`
Changes Take Effect: When the HA connection is established

Specifies the maximum number of calls that can be synchronized at once between the primary SIP Server and the backup SIP Server after the HA link connection is established, before waiting for 1 second to continue with synchronization. Only calls that are missing on the backup SIP Server are synchronized.

# Verifying Initialization Status in Backup SIP Servers

Starting with version 8.1.103.64, the backup SIP Server can heck the status of its internal components during startup to ensure it provides the service when it is promoted to Primary. If any internal component (T-Controller, Smart Proxy, Interaction Proxy, or Operational Information thread) fails to complete initialization, SIP Server reports the SERVICE_UNAVAILABLE status to the Management Layer (LCA/SCS).

In addition, if SIP Server fails to open a SIP port during startup, it reports the SERVICE_UNAVAILABLE status to LCA/SCS. Note that this approach does not work for the IP Address Takeover procedure or same host configuration.

To enable this functionality, configure the following options:

**backup-init-check**
Setting: [TServer] section, Application level
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After restart

When set to `true`, SIP Server in Backup mode verifies that all internal components (T-Controller, Smart Proxy, Interaction Proxy, and Operational Information thread) are successfully initialized, and can provide the service when SIP Server switches to Primary mode. If some components fail to complete initialization, SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS. The timeout for internal components to complete initialization is defined by the **backup-init-check-timeout** option.

**backup-init-check-timeout**
Setting: [TServer] section, Application level
Default Value: `60`
Valid Values: `15-3600`
Changes Take Effect: After restart

Restricted option. Specifies the timeout, in seconds, during which SIP Server verifies that all internal components are successfully initialized in a scenario described by the **backup-init-check** option.

**backup-sip-port-check**
Setting: [TServer] section, Application level
Default Value: `true`
Valid Values: `true, false`
Changes Take Effect: After restart

When set to `true`, SIP Server in Backup mode attempts to open a SIP port. If the port opens successfully, no SIP messages are processed, and SIP Server closes the port immediately. If the SIP port does not open, SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS. This functionality is enabled only when **backup-init-check** is set to `true`. The functionality is disabled in the IP Address Takeover configuration, when the **control-vip-scripts** option is set to `true`.

# Enhanced HA Resilience for Network Disruptions

Starting with version 8.1.103.61, SIP Server supports enhanced high-availability resilience for network disruptions. With this feature, switchovers can be triggered when SIP Server detects MSML VOIP Service DNs and/or Trunk DNs that are out of service. After a switchover, a backup (new primary) SIP Server can place MSML VOIP Service DNs and/or Trunk DNs back in service and proceed with calls processing, minimizing or avoiding network outages.

**switchover-on-msml-oos**
Setting: [TServer] section, the SIP Server Application (in standalone mode) or the VOIP Service DN with **service-type**=`sip-cluster-nodes` (in SIP Cluster mode)
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: For the next call

Specifies the SIP Server action in case of losing connectivity with MSML VOIP Service DNs. When set to `true`, in the case of strict matching only, VOIP Service DNs with the same or alternative geo-location are considered. After detecting that those DNs are out of service, SIP Server checks one more time that MSML VOIP Service DNs are unresponsive, before reporting the SERVICE_UNAVAILABLE status to LCA/SCS in order to trigger a switchover.

**switchover-on-trunks-oos**
Setting: [TServer] section, the SIP Server Application (in standalone mode) or the VOIP Service DN with **service-type**=`sip-cluster-nodes` (in SIP Cluster mode)
Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: For the next call

Specifies the SIP Server action in case of losing connectivity with Trunk DNs. When set to `true`, in the case of strict matching only, Trunk DNs with the same or alternative geo-location are considered. After detecting that those DNs are out of service, SIP Server checks one more time that Trunk DNs are unresponsive, before reporting the SERVICE_UNAVAILABLE status to LCA/SCS in order to trigger a switchover.

# SIP Business Continuity

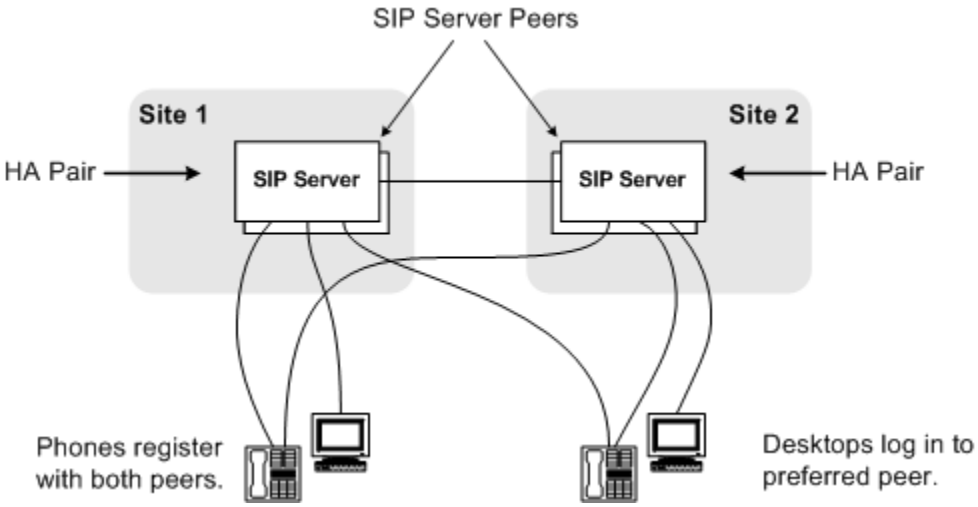
These topics contain information about SIP Business Continuity (BC), which provides the ability for a group of agents to continue offering critical business functions to customers in the event of a loss of all Genesys components running at a particular site.

- SIP Business Continuity Architecture describes the SIP Business Continuity solution, how it works, and the basic architecture.
- Deploying SIP Business Continuity describes how to deploy SIP Business Continuity in your environment.

# SIP Business Continuity Architecture

SIP Business Continuity provides the ability for a group of agents to continue offering critical business functions to customers in the event of a loss of all Genesys components running at a particular site. The SIP Business Continuity architecture uses a synchronized, two-site deployment, where Genesys switch and server components are mirrored at each site in an active-active configuration, so that any agent can log in to either switch, at any time.

The **Business Continuity Overview** figure shows the basic connections between SIP Server instances and endpoints across the redundant sites.




Business Continuity Overview

## What Does It Do

SIP Business Continuity includes (though not limited to) the following functions:

- Work area redundancy
- Disaster Recovery
- Graceful Migration

For regular call processing, agent activity can be load-balanced across the two sites, or you can configure agents to use one preferred site over the other. In the event of a failure at one site (a SIP Server HA pair or all Genesys components go down), agents connected to the failed site are re-logged in automatically to the surviving site. Although any active calls on the failed site are terminated at the moment of failure (including calls on the surviving site that include the failed SIP Server in the signaling path), the surviving site is able to process all new calls, with minimal impact to queue wait times.

> **Important**
>
> Business Continuity does not provide recovery for the local failure of particular agent endpoints or workstations. It is intended to provide redundancy for Genesys components only.

## SIP Server Peers

A pair of primary and backup SIP Server instances are deployed at each site, providing local high availability (HA). For Business Continuity, these dual HA pairs are known as *SIP Server Peers*. The SIP Server Peers rely on synchronized configuration for all agent-related objects: `Extension` DNs, `Places`, `Agent Logins` (and the references to their related `User` or `Person` object). Each agent desktop is configured with a "Preferred Site", indicating to which site it should connect if possible.

### Synchronizing Configuration Objects

Using Genesys Administrator, you can synchronize all agent-related configuration objects (DNs of certain types, Places, Agent Logins, and the reference to their associated User or Person) between the SIP Server Peers.

Synchronization applies to the following DN objects:

- `Extension` DN
- `ACD Queue` DN
- `Call Processing Port` DN

After you run the synchronization once, Genesys Administrator will automatically synchronize any further configuration changes of Places and Users between the SIP Peers—as long as the changes are made using Genesys Administrator.

> **Important**
>
> - In Business Continuity deployments only DNs of type `Extension` are supported as agent DNs.
> - The preferred Extension DN and the peer Extension DN must be assigned to the same Place.
> - Stat Server 8.1.2 or later must be used to properly support SIP Business Continuity environment.

## SIP Phones

A variety of SIP phones are approved for Business Continuity deployments (refer to the Application Note for each phone published here). Phones can be configured in single- or dual-registration modes. If the phones are in dual-registration mode, Business Continuity supports one registration for each site (Alcatel 4000-series phones are the exception). For outbound 1pcc calls, one of the sites is considered "preferred" based on either 3rd-party configuration on the phone itself, or based on DNS SRV record priority.

Alcatel-Lucent 4000-series IP Phones do not support dual registration. Instead, an active-backup registration scheme—where the phone registers to the SIP Server on the backup site only if the primary is unavailable—is used to handle disaster recovery scenarios. Special configuration for these phones is required.

Genesys recommends the active-backup registration logic for most phones.

For more information, see Using IP Phones.

## Agent Desktop

The agent desktop maintains a login to a single site at one time. Typically, the agent desktop logs into the "Preferred Site" specified in the desktop configuration, but it will log in to the other peer if both the preferred site is unavailable and the SIP endpoint switches registration to the backup site. The agent desktop maintains a basic connection (no login) to the backup peer site.

For more information, see the *Workspace Deployment Guide*.

Supported components: Workspace Desktop Edition (formerly Interaction Workspace) 8.5.x.

# Call Delivery

During regular call processing, external media gateways distribute incoming traffic between the SIP Server Peers. Or optionally, an additional SIP Server or Network SIP Server can be deployed at the network level to provide intelligent pre-routing, or for scaling SIP Server Peers.

Each SIP Server Peer delivers routed calls, internal calls, direct inbound calls, and external calls to a particular agent through the SIP Server instance to which the agent is currently logged on. The agent initiates calls through the SIP Server where they are logged in.

## About the Call Forwarding Procedure

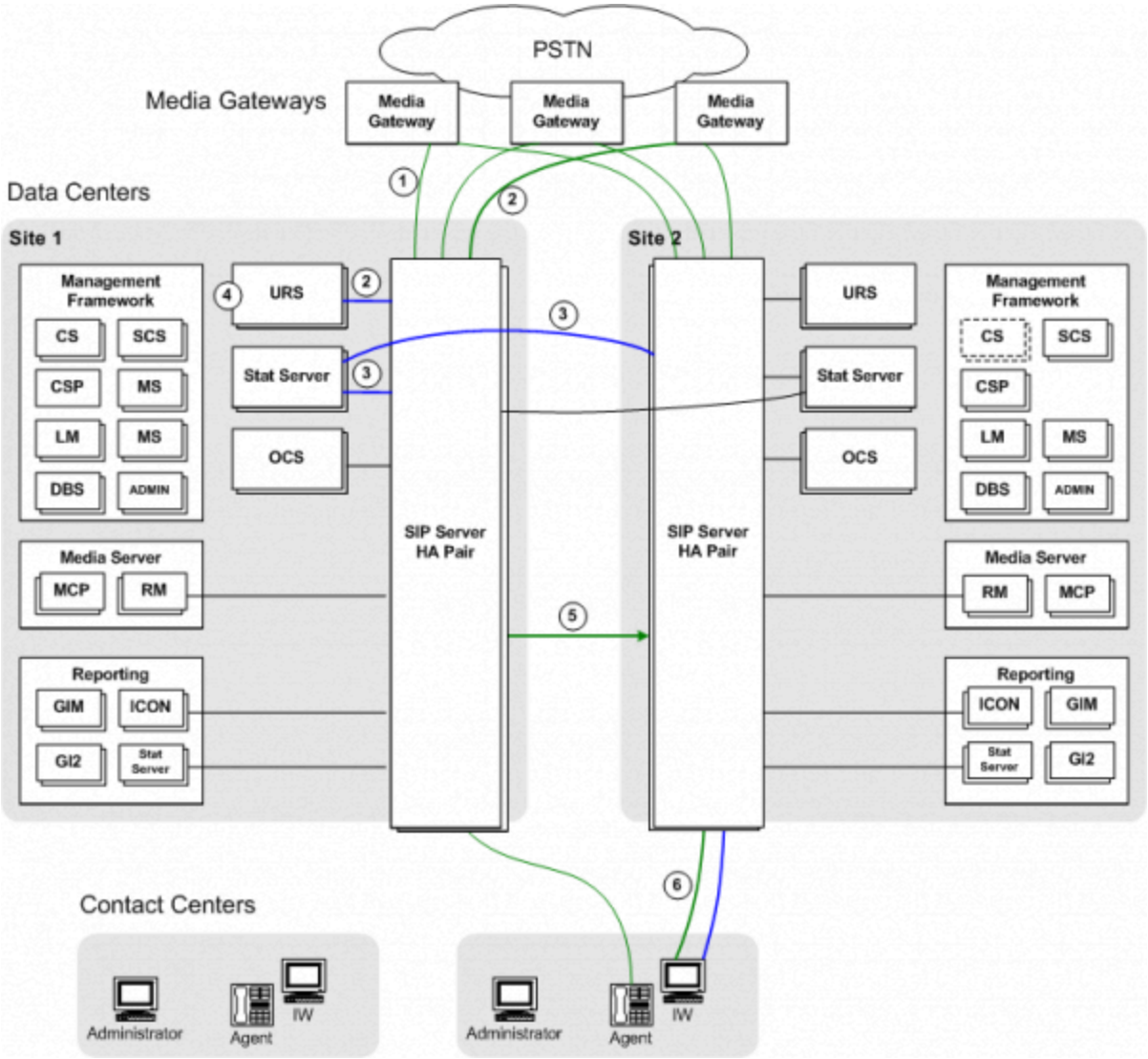
In case of a direct call to an agent phone number, Business Continuity takes special measures to make sure that the call is delivered to the DN where the agent's SIP phone is actually registered. Since agents can be registered on either SIP Server Peer site, the party that makes the call does not know the agent's current location, meaning the call can arrive at either SIP Server in the peer group. This SIP Server instance uses an internal call forwarding procedure to determine the location of the call destination (the agent phone number) and deliver the call there. This procedure ensures that the call is delivered to the site where T-Library messaging is linked to the logged in agent (identified as the `User` or `Person`), so that proper reporting takes place. The option **dr-forward** controls the rules for this call forwarding procedure.

The call forwarding procedure typically takes place as follows:

1. An inbound direct call arrives on SIP Server 1.
2. SIP Server 1 detects that the agent's phone is registered and accessible, but the agent is not logged in.
3. SIP Server 1 initiates an Out-of-Signaling-Path (OOSP) transfer—it sends a `302 Moved Temporarily` response back to the caller with the address of the DN on its SIP Server Peer.
4. The media gateway sends the secondary INVITE to SIP Server 2, targeting the same DN number.
5. SIP Server 2 processes the INVITE and tries to establish the call with the target. To prevent a forwarding loop, because the call has already been processed on SIP Server 1, SIP Server 2 will not forward the call back to that site, even if it turns out that the agent is not logged in on the SIP Server 2 site either.

## Call Delivery - SIP Server Peers

The **Call Delivery, Direct to SIP Server Peer** figure shows a typical call flow for inbound call delivery to an agent, where the call arrives directly at the SIP Server Peer (no network-level SIP Server in the flow).




Call Delivery, Direct to SIP Server Peer

The following steps describe the call flow from media gateway to the selected agent:

1. Media gateways distribute incoming traffic across both sites.
2. A call arrives at SIP Server on Site 1. SIP Server requests routing instructions from the Universal Routing Server (URS).
3. Each Stat Server monitors both SIP Server Peers. As such, the Stat Server on Site 1 is able to determine agent availability on both SIP Server Peers—agents can be logged in on either SIP Server Peer.
4. URS selects the appropriate agent to handle the call. In this example, the selected agent is logged in on the other SIP Server Peer site. URS sends a `TRouteCall` request to SIP Server, instructing it to route the call to the targeted agent.

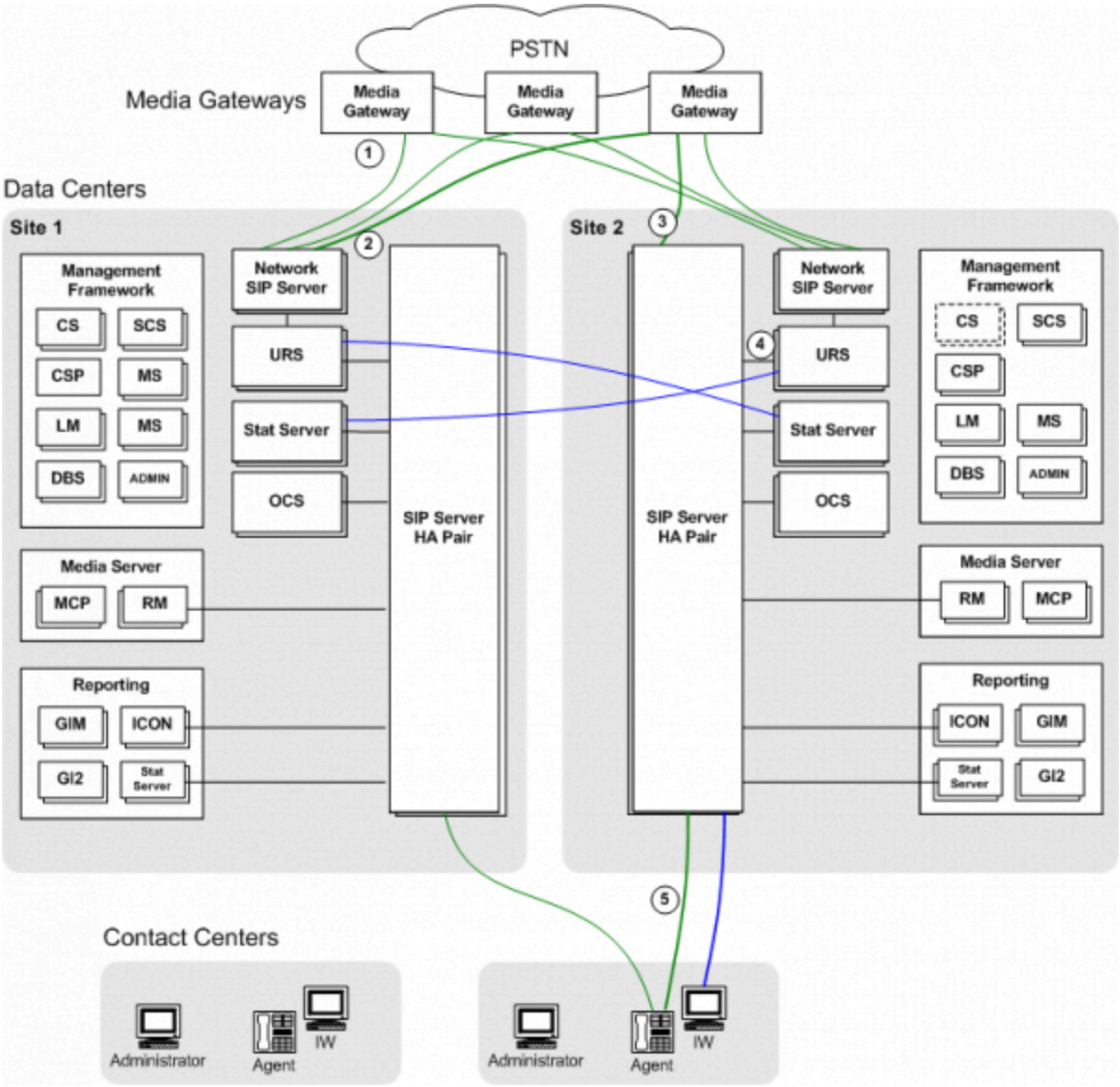
   **Note:** To route calls across sites (using Inter Server Call Control (ISCC)), Agent Reservation must be enabled. For more information, see the "Agent Reservation" section in the "T-Server Fundamentals" chapter of the Framework 8.1 SIP Server Deployment Guide. Also, see the Universal Routing 8.1 Deployment Guide.

5. As part of its internal Business Continuity Forwarding procedure, SIP Server first determines that the selected agent is not logged in locally. Based on this logic (and related option values that control the procedure), SIP Server then forwards the call to Site 2 through the specially configured inter-site Trunk DN, using ISCC routing.
6. The SIP Server Peer on Site 2 delivers the call to the agent.

**Note:** If SIP Server forwards an internal call to its DR peer, then SIP Server adjusts the call type to the Outbound value, and adds the access number of that DR peer in AttributeOtherDN of EventDialing. The access number is the prefix configured on the Trunk DN of that DR peer.

## Call Delivery - Network SIP Server

The **Call Delivery, Network SIP Server** figure shows a typical call flow for inbound call delivery to an agent, where the call first passes through a Network SIP Server.




Call Delivery, Network SIP Server

**Note:** The Network SIP Server in this architecture could be replaced with a Premise SIP Server instance, installed at the network level. In either case, Genesys recommends configuring default routing.

The following steps describe the call flow from media gateway to selected agent:

1. The media gateways distribute incoming traffic between Network SIP Server instances at the two sites. Network SIP Server, in conjunction with URS, can provide additional intelligence when deciding to which site to route the call. For example, routing can be configured to send a greater share of calls to whichever site currently has more logged in agents. Network SIP Server can also distribute calls across multiple SIP Server Peer groups, for scaled deployments.
2. The call arrives at the Network SIP Server on Site 1. URS at Site 1 determines that the call should go to Site 2, which currently has more agents logged in.

3. Network SIP Server sends a `302 Moved Temporarily` message to the media gateway. The media gateway sends a new `INVITE` to the SIP Server at Site 2.
4. URS at Site 2 selects the best agent to handle the call. In this example, the selected agent is logged in to Site 2.
5. URS sends a `TRouteCall` request to SIP Server, instructing it to route the call to the targeted agent. SIP Server establishes the call with the agent.

## Call Delivery - Multi-Site

In cases where the deployment includes an external Genesys location in addition to the SIP Server Peers, the call is delivered to one of the SIP Server Peers, based on how the targeted Trunk is resolved. For example, if the `INVITE` through `Trunk1` arrives at SIP Server on Site 1, but the targeted agent DN is not found at this site, Business Continuity Forwarding is applied, and the call is forwarded to the other SIP Server Peer at Site 2.

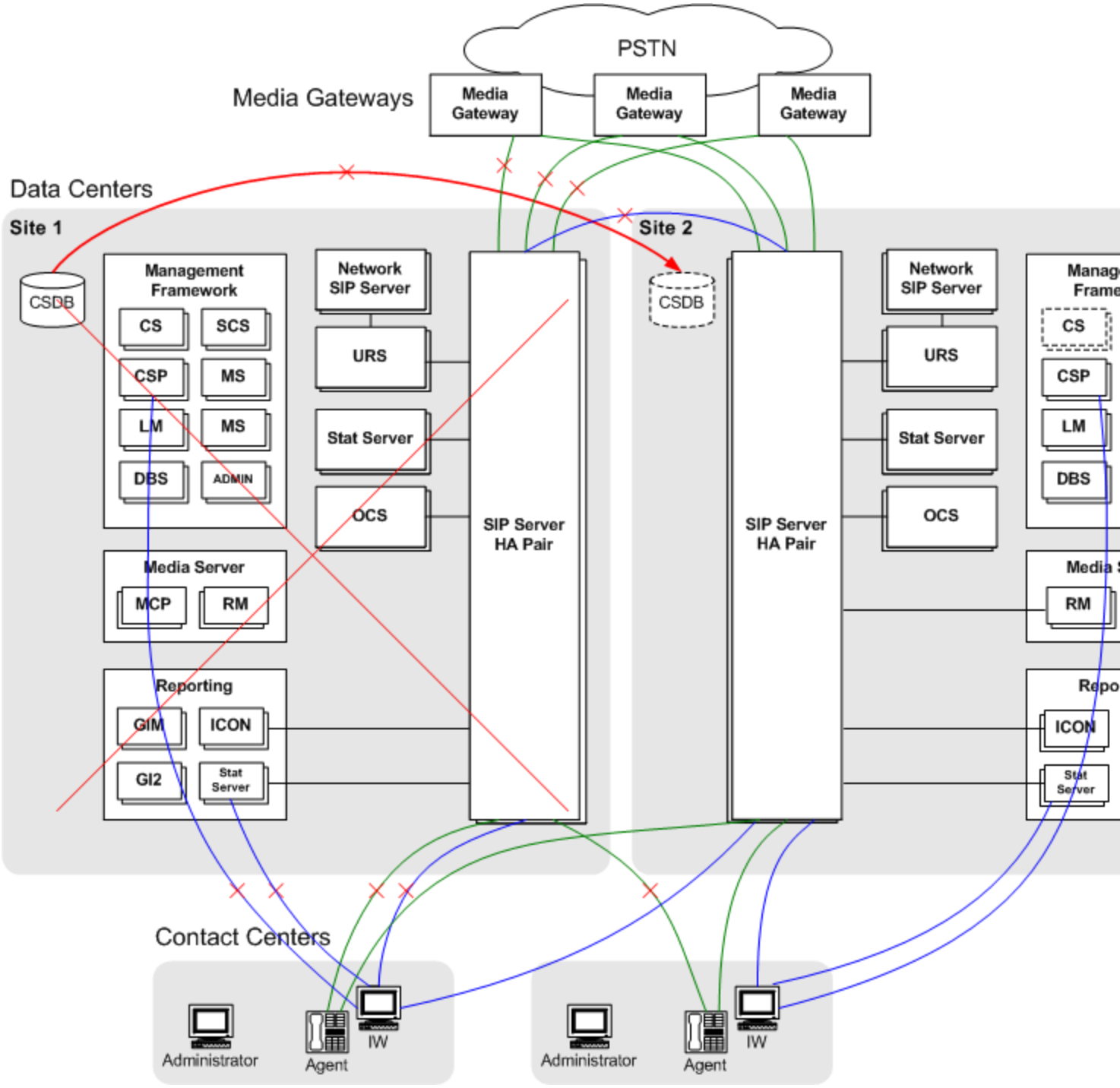
For configuration details, see Deploying SIP Business Continuity With a Remote Site.

# Disaster Recovery

In the event of the catastrophic failure of a particular site--in which all Genesys components become unavailable, including locally paired HA servers—peer site redundancy is used to provide ongoing support for all logged in agents. For those agents logged in to the surviving SIP Server Peer, their login remains unaffected and they can continue handling calls. For those agents that were logged in to the failed site, there is a temporary increase in queue wait times as these agents are logged in to the surviving site. Some loss of calls may occur at the failed site.

## Site Failure

The **Site Failure** figure illustrates what typically happens when one site in a SIP Server Peer group suffers a catastrophic failure.




Site Failure

The following steps describe how Business Continuity recovers from a catastrophic failure of a particular SIP Server Peer site:

1. Site 1 suffers a catastrophic failure. All Genesys components, including paired HA servers, are

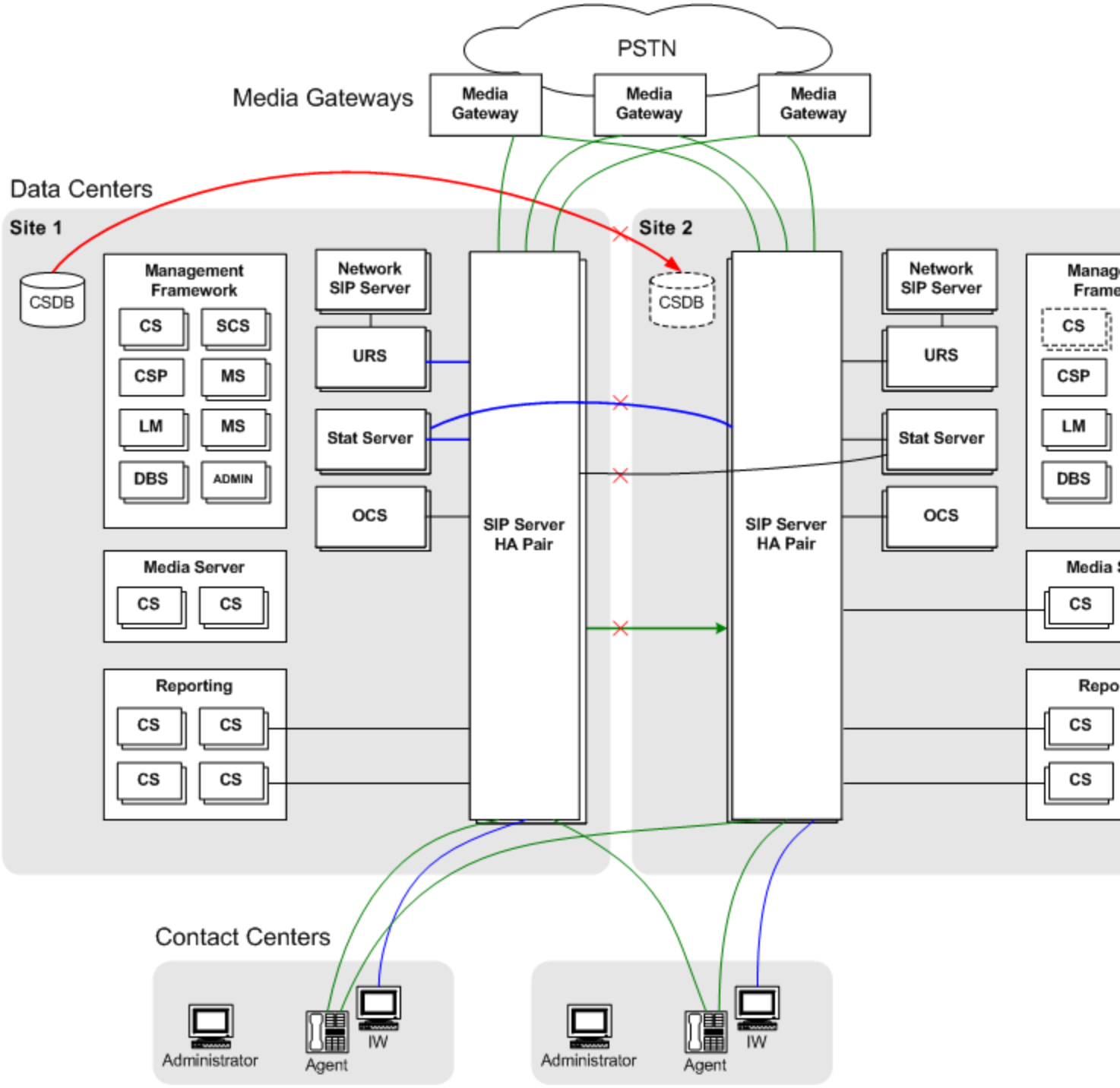
unavailable.

2. The media gateways detect a response timeout from Site 1. In response, the media gateways begin sending all new calls to Site 2.
   If the media gateway itself is affected by the disaster outage, the PSTN should detect this; load-balancing at the gateway level should redirect calls to the surviving media gateways.
3. Agents that are currently logged in to Site 2 continue to handle calls. Queue wait times increase temporarily.
4. The agent's SIP phone responds in either of the following ways:
   - If the phone is configured to register on one site only, it re-registers now on the Site 2 SIP Server.
   - If the phone is configured for dual-registration, the phone automatically switches call handling from the local site to the backup site (Site 2).

   Agent desktops detect Site 1 failure, and re-login automatically to the SIP Server on Site 2. In addition, the desktop establishes connections to the Stat Server and Configuration Server Proxy on Site 2.
5. The standby Configuration Server and Configuration Server Database as Site 2 are brought into service.
6. When the surviving SIP Server detects that its peer is failed, it continues operation in single-site mode, stopping Business Continuity functions as follows:
   - It no longer applies the call forwarding procedure to new calls.
   - It allows agents to log in independently of the status of their endpoint.
   - It does not employ the forced logout procedure

## Networking Failure Between Sites

The **Networking Failure** figure illustrates what typically happens when a networking failure occurs between SIP Server Peer sites.




Networking Failure

The following steps describe how Business Continuity recovers from a networking failure between the SIP Server Peer sites:

1. In this example, network connectivity between the two data center sites is lost. SIP Server detects this

failure through Active Out of Service detection (options `oos-check` and `oos-force`) of the inter-site `Trunk` DN. Connectivity between the media gateways and contact centers at each site are still available.

2. The SIP Server instances at each site revert to their normal non-peered operation.
3. Incoming calls at each site are routed only to agents logged in at that site--Business Continuity Forwarding does not apply.
4. In this case, the Business Continuity solution avoids any "split-brain" problems because there are no longer any inter-dependencies between the sites.
5. For short-term outages, the Configuration Server Proxy on Site 2 provides configuration data to local Site 2 applications. For longer outages, Site 2 Configuration Server and Configuration Server Database can be brought into service.
6. When the surviving SIP Server detects that its peer is failed, it continues operation in single-site mode, stopping Business Continuity functions as follows:
   - It no longer applies the call forwarding procedure to new calls.
   - It allows agents to log in independently of the status of their endpoint.
   - It does not employ the forced logout procedure

# Graceful Migration

Business Continuity supports the graceful migration of operations from two active SIP Server Peer sites to a single site, in cases where one full site needs to be taken offline or powered off—for example, to perform maintenance on an entire data center. The goal of graceful migration is to gradually move all business activity to the second site with no lost calls. Agents must migrate to the second site.

To enable a graceful migration, you first configure your environment to stop sending calls to the SIP Server Peer site that you intend to shutdown. Using Genesys Administrator, you then initiate a graceful shutdown of the SIP Server itself, in which SIP Server stops accepting new calls while still allowing any ongoing calls to finish, ensuring that no calls are dropped when this SIP Server instance is finally stopped.

Assuming that Site 2 is going to be taken offline, the general procedure for graceful migration as follows:

1. Configure the media gateways to stop sending new calls to Site 2.
2. Configure the routing strategy to stop sending new calls to Site 2.
3. Initiate the graceful shutdown procedure for SIP Server. You can initiate this in one of two ways:
   - Using Genesys Administrator, initiate the graceful shutdown procedure from the SIP Server `Application` object.
   - Sending a `TPrivateRequest` with `serviceid=3019` from a T-Library client.

   Either of these actions starts the SIP Server graceful shutdown process.

During the graceful shutdown, SIP Server does the following:

- Rejects all new `INVITE` requests with a configurable error response (the **shutdown-sip-reject-code** option).
- Rejects all new calls initiated by T-Library requests.
- Terminates all nailed-up SIP connections automatically.
- Handles the agents depending on their state, as follows:
  - If agents are not on calls or not in the AfterCallWork (ACW) state, SIP Server forcibly logs them out. While graceful shutdown is in progress, new calls can no longer be distributed to the agents.
  - If agents are not on calls and are in the `NotReady` state with the ACW workmode, SIP Server waits for agents to complete the ACW and for the ACW timeout to expire, then sets the agents to Ready and logs them out.
  - If agents are on calls and have the ACW workmode, SIP Server waits for the end of their calls, sets the agents to `NotReady` and waits for the ACW timeout to expire, then sets agents to Ready and logs them out.
  - If agents are on calls and do not have the ACW workmode, SIP Server waits for the end of their calls and then logs them out.

- If agents have the untimed ACW period, SIP Server logs them out immediately.

  **Note:** When SIP Server logs agents out, it reports the ReasonCode `graceful_shutdown_logout` in AttributeExtensions of EventAgentLogout messages.

- If the agents use Genesys Interaction Workspace, they are logged in automatically at Site 1.
- When no calls remain, SIP Server starts the timeout (the **graceful-shutdown-sip-timeout** option) to retransmit BYE requests that were not confirmed with 200 OK responses.
- After the timeout expires and all agents are logged out, SIP Server (at Site 2) shuts down. SIP Server at Site 1 now handles all calls.

# Deploying SIP Business Continuity

These topics describe how to deploy SIP Business Continuity in different scenarios, environments, and modes.

### Basic Deployment

Use these procedures to set up basic SIP Business Continuity.

Deploying basic SIP Continuity

Configuration options

### DR Peer and Remote Site Deployment

Use these additional procedures to include a remote site in the continuity setup.

Deploying SIP Continuity with a remote site

### Additional Features

Feature-specific configuration that might be required for your SIP Business Continuity deployment.

Hunt Groups

Instant Messaging

Nailed-up connections

Shared Call Appearance

Enhanced disaster recovery solution for outbound calls

# Basic Deployment

The following tasks are required to deploy basic SIP Business Continuity in your environment. Unless otherwise stated, refer to the Framework 8.1 SIP Server Deployment Guide for information about the configuration options.

## Deploying Basic SIP Business Continuity

### 1. Create the peer switch.

For each DR pair required, use the Sync Switch Wizard in Genesys Administrator to create a new peer switch or use an existing switch as the peer. Each switch in the DR pair must be located at a separate site. The Wizard sets up the switches as peers, synchronizes switch-related elements between them, and then keeps them synchronized.

For remote agents, before using the Sync Switch Wizard in Genesys Administrator to create a new peer switch:

1. Configure the **contact** option with the value equal the FQDN of the media gateway for all remote agent DNs or a softswitch.
2. Configure local DNS servers for each peer to resolve this FQDN to respective gateway addresses.

> **Important**
>
> The switches are not synchronized automatically for changes made outside of Genesys Administrator. However, you can re-synchronize these switches at any time by using the Sync Switch Wizard. For more information about the Sync Switch Wizard, refer to *Genesys Administrator 8.1 Help*.

### 2. Interconnect the DR peers.

On each DR peer:

1. Configure the **contact** option on a Trunk DN pointing to the other peer.
2. Assign to each DN a unique prefix (by setting the option named **prefix**) that does not match a possible dialed number to avoid the DN being mistaken for use by an outbound call. The options **oos-check** and **oos-force** must be configured to enable Active Out Of Service Detection.
   **Note:** Use the names of these DNs when configuring the Application option **dr-peer-trunk**.

3. Set the **dr-peer-location** option to the name of the Switch object of the other SIP Server in the DR pair.
4. Do not configure the **auto-redirect-enabled** option.
5. (Optional) Consider configuring the **replace-prefix** option to replace initial characters of the call's destination name.

## 3. Configure ISCC COF between the DR peer switches.

Refer to the Framework 8.1 SIP Server Deployment Guide for instructions. Set the following options in the **[extrouter]** section on each SIP Server:

- **cof-feature**=`true`
- **default-network-call-id-matching**=`sip`

## 4. Set up default routing.

Do one or both of the following, as appropriate:

- If you are using premise SIP Servers at the network level, use the configuration options **router-timeout** and **default-dn**.
- If you are using Network SIP Servers, use the configuration option **default-route-destination**.

## 5. Configure routing from premise to peer.

On each premise SIP Server, use the configuration option **dr-peer-trunk** to identify that the SIP Server is a part of a DR pair, and to identify the Trunk DN that points to the other SIP Server in the pair. Genesys also recommends the following:

- Add the addresses of a DR peer to the list of addresses in the option **enforce-external-domains**, to ensure that the call parties are properly recognized based on the Host element of the contacts. This configuration should apply to both SIP Servers in a DR pair.
- Use the option **dr-forward** at the Application or DN level to define the mode of forwarding inbound and internal calls when SIP Server is operating in Business Continuity mode. Set this option to one of the following values, as appropriate:
  - `no-agent`—for call center deployments or for an agent's DNs
  - `oos`—for Alcatel-Lucent and Bria IP phones that do not support simultaneous registrations on two sites
  - `off`—for office (that is, non-agent) deployments of endpoints

## 6. Configure ADDP.

Advanced Disconnect Detection Protocol (ADDP) must be configured in the Stat Server application on the connection to SIP Server. It is also recommended to configure ADDP in other components on the connection to SIP Server.

## 7. Configure Places.

When you configure Place objects for agents, assign the preferred Extension DN and the peer Extension DN to the same Place.

**Note:** Stat Server 8.1.2 or later must be used to properly support SIP Business Continuity environment.

## 8. (Optional) Configure the preferred site for agents.

Workspace Desktop Edition (formerly, Interaction Workspace) supports preferred-site connections for agents. Other agent desktops must use the same mechanism as used by Workspace for configuring preferred-site connections. For configuration details, see the Workspace Deployment Guide.

# DR Peer and Remote Site Deployment

The following tasks describe the steps necessary to deploy SIP Business Continuity in the following scenario:

- Two sites, S1 and S2, are configured as a DR peer. You want to call the agents in the DR peer from a third site S3.

Unless otherwise stated, refer to the Framework 8.1 SIP Server Deployment Guide for information about the configuration options.

### Deploying SIP Business Continuity With a Remote Site

## 1. Configure sites S1 and S2 as DR peers.

See Basic Deployment.

## 2. Configure two trunks on the third switch, one each to the other switches in the DR pair.

1. On the third switch, configure two Trunk DNs, and configure the **contact** option on each DN as follows:
   - First DN: **contact**=<FQDN of DR peer>
   - Second DN: **contact**=<FQDN of DR peer>
2. On both DNs, do no configure the **auto-redirect-enabled** option.

All other options can remain the same. However, if you want, you can use the options **priority** and **capacity** to indicate the preference of one trunk over the other.

## 3. Configure ISCC COF between DR peer switches.

Configure ISCC COF access between the following sites:

- The remote site and the first DR pair site.
- The remote site and the second DR pair site.

Refer to the Framework 8.1 SIP Server Deployment Guide for instructions. Set the following options in the `extrouter` section on each SIP Server:

- **cof-feature**=`true`
- **default-network-call-id-matching**=`sip`

# Nailed-Up Connections in Business Continuity

SIP Server supports a persistent “nailed-up connection” for agents, where it maintains an extended telephone call between SIP Server and the agent. During this time, the agent can handle multiple customer interactions without dropping the telephone connection to SIP Server.

Nailed-up connections offer a few key benefits, including:

- Minimal delay between the time an agent is selected and the audio path to the customer is established
- Improved overall reliability—the connection is already established when delivering a customer “call”, and the agent is less likely to take non-contact center calls

One typical use of nailed-up connections is for agents who use a legacy PSTN phone. These agents could be working from their home, or in a branch office that has simple PSTN connectivity. Another typical use of nailed-up connections is for agents behind a 3rd party PBX, when the PBX is connected to SIP Server through a gateway or simple SIP trunk.

SIP Server supports virtually all agent functionality in conjunction with nailed-up connections. The agent can make calls, receive calls, transfer calls, consult with other agents, use call supervision, and more. In addition, SIP Server’s call recording functionality is fully compatible with nailed-up connections.

Inbound calls to an agent with a nailed-up connection are delivered by default with “auto answer”—meaning the audio connects immediately. If this “auto answer” experience is not desired, then Preview Interactions should be used to provide the agent the opportunity to see call information in their agent desktop and accept or reject the call.

Nailed-up connections can be established or disconnected either by SIP Server or by the agent.

> **Important**
>
> In Business Continuity deployments, any DN with a statically configured contact must use `dr-forward` set to `no-agent`. In practical terms, such a DN is commonly used for a “remote agent”, often in conjunction with the nailed-up connection.

## Establishing the Nailed-Up Connection

Nailed-up connections can be established by three different methods:

- SIP Server establishes the nailed-up connection on agent login or when an agent is in Ready state.
- SIP Server establishes the nailed-up connection on the first customer call.
- Agent establishes the nailed-up connection by calling into a contact center Route Point.

### SIP Server Establishes the Nailed-up Connection on Agent Login or Ready state

SIP Server can establish the persistent nailed-up connection with an agent when the agent logs in, depending on the configuration:

- When **connect-nailedup-on-login**=<Routing Point number>, SIP Server connects the agent's endpoint with the specified Routing Point and then, after processing the TRouteCall to the predefined gcti::park device, SIP Server parks the agent on the gcti::park device establishing the persistent nailed-up connection with the agent's endpoint.
- When **connect-nailedup-on-login**=gcti::park, SIP Server directly parks the agent on the gcti::park device, establishing the persistent nailed-up connection with the agent's endpoint while processing TAgentLogin.

If a nailed-up connection is terminated for any reason, SIP Server places the agent in the NotReady state. If an agent is in the NotReady state and a nailed-up connection is not yet established, SIP Server, while processing the TAgentSetReady request, initiates a SIP call to the agent's phone with further parking on the gcti::park device. If the call fails, SIP generates EventError in response to TAgentSetReady; the agent remains in the NotReady state.

If the agent logs out, the nailed-up connection is dropped.

### SIP Server Establishes the Nailed-up Connection on First Customer Call

SIP Server calls the agent to start a session—SIP Server sends the call to a remote TDM agent configured for the nailed-up feature. This applies to the first transfer to the agent, where the initial nailed-up session starts. When the caller releases the call or the agent releases the call using 3pcc, SIP Server parks the agent on Media Server, keeping the connection for the call leg to the nailed-up connection.

The basic call flow when SIP Server first calls an agent who is configured for the nailed-up feature is as follows:

1. SIP Server receives a customer call, which the Universal Routing Server then processes.
2. After qualification and queuing, the routing strategy selects the agent who will handle the call.
3. SIP Server contacts the agent as it would for any remote TDM extension (SIP Server does not yet consider the agent to be nailed-up).
4. At the end of the call, when the agent requests to release the call through the Agent Desktop (a 3pcc TReleaseCall), SIP Server does not disconnect the call leg to the nailed-up connection but, instead, parks the agent on the predefined gcti::park device. At this point, the agent is considered to be nailed-up. Media Server applies a silent treatment while the nailed-up connection is maintained.

In Business Continuity deployments, SIP Server applies the following “Call Delivery” logic when establishing the initial call to a DN with a statically configured contact:

1. If the first SIP Server to handle the call determines an agent is locally logged in and using the DN, this SIP Server delivers the call directly to the DN.
2. Otherwise, the first SIP Server forwards the call to the second SIP Server on the alternate site, using the inter-site Trunk DN and ISCC. The second SIP Server delivers the call to the DN, regardless of whether any agent is logged in and using the DN or not.

> **Important**
> Carefully consider this behavior. This could result in high telephone connection charges, if, for example, DNs and data centers are distributed across different countries.

### Agent Establishes the Nailed-Up Connection by Calling into a Contact Center Route Point

The agent calls the contact center to start a session—The remote TDM agent (configured for the nailed-up feature) initiates a call (1pcc) to the contact center.

The basic call flow when a remote TDM agent who is configured for the nailed-up feature is as follows:

1. A call from the remote agent arrives at the contact center on a Routing Point DN.
2. A short treatment is applied, and URS issues a TRouteCall to the predefined `gcti::park` device (RouteType=Unknown; OtherDN='gcti::park').
3. SIP Server parks the agent on the `gcti::park` device, keeping the call leg to the agent connected. At this point, the agent is considered to be nailed-up. Media Server applies a silent treatment while the nailed-up connection is maintained.

In Business Continuity deployments, each data center should have a unique routing point, which allows an agent to connect to their preferred data center based on which routing point they contact.

### Disconnecting the Nailed-Up Connection

Nailed-up connections can be disconnected for several reasons:

- The agent hangs up the phone.
- A network problem between SIP Server and the phone causes the call to be dropped.
- The agent logs out (applies when SIP Server established the connection on login, or if the **drop-nailedup-on-logout** option is set to `true`).
- The agent is inactive (no changes in agent state or incoming/outgoing calls at the DN) for the specified period of time (**disconnect-nailedup-timeout**).

## Feature Configuration

## 1. Configure the gateway.

On the `Trunk` DN that represents the gateway that is used to contact the remote agent, specify the following option in the **[TServer]** section:

- **refer-enabled**—Set to this option `false`.

## 2. Configure the agent DN.

On the `ACD Position` or `Extension` DN for the agent, specify the following options in the **[TServer]** section:

- **contact**—Set this option to the contact URI of the PSTN gateway/SBC or third-party PBX, depending on the agent location.
- **line-type**—Set this option to 1.
- **refer-enabled**—Set this option to `false`.
- **dual-dialog-enabled**—Set this to `false`.
- **reject-call-notready**—Set this option to `true` (recommended, not mandatory).
- **sip-cti-control**—Ensure that this option is not configured.

## 3. Configure the SIP Server Application.

### Connection on Agent Login

To enable the persistent nailed-up connection on agent login, in the **[TServer]** section of the SIP Server Application, configure the following option:

- **connect-nailedup-on-login**

**Note:** If the agent logs out, the nailed-up connection will be dropped; the same behavior as if the **drop-nailedup-on-logout** is set to `true`.

### Disconnection on Inactivity

To terminate the agent's nailed-up connection because of agent's inactivity, in the **[TServer]** section of the SIP Server Application, configure the following option:

- **disconnect-nailedup-timeout**

### Disconnection on Agent Logout

To enable automatic disconnection of the agent from the nailed-up connection on agent logout, in the **[TServer]** section of the SIP Server Application, configure the following option:

- **drop-nailedup-on-logout**—Set this option to `true`.

**Note:** If enabled, SIP Server can only establish the nailed-up connection if the agent is logged in.

# 4. (Optional) Configure Business Continuity.

For Business Continuity deployments, set **dr-forward** to `no-agent`. See Basic Deployment for details.

## Configuration Options

### connect-nailedup-on-login

Setting: Application and DN levels
Default Value: An empty string
Valid Values: Routing Point number, `gcti::park`
Changes Take Effect: At the next agent login session

Specifies SIP Server actions when receiving a TAgentLogin request from a DN with the configured nailed-up connection, as follows:

- When this option is set to a DN of type Routing Point, SIP Server immediately establishes a nailed-up connection between an agent's endpoint and the specified Routing Point. After processing the TRouteCall request to the `gcti:park` device, SIP Server parks the agent on `gcti::park`, establishing the persistent SIP connection with the agent's endpoint.
- When this option is set to `gcti::park`, SIP Server parks the agent on the `gcti::park` device directly, establishing the persistent SIP connection with the agent's endpoint.
- When the value for this option is not specified (the default), SIP Server does not take any action.

At a DN level, this option must be set on agent Extension DN, or, if this DN is located behind the softswitch on the respective softswitch DN.

### disconnect-nailedup-timeout

Setting: Application and DN levels
Default Value: `0`
Valid Values: Any positive integer
Changes Take Effect: At the next nailed-up connection

Specifies whether SIP Server terminates an agent's nailed-up connection because of the agent's inactivity. When set to a non-zero value, SIP Server waits this time interval, in seconds, before terminating the agent's nailed-up connection. When set to `0` (the default), SIP Server does not terminate the agent connection.

## AttributeExtensions

The **connect-nailedup-on-login** key supports this feature. It overrides the **connect-nailedup-on-login** option setting but only for a current login session.

Key: **connect-nailedup-on-login**
Type: String
Values: Routing Point number, `gcti::park`
Requests: TAgentLogin

Specifies SIP Server actions when receiving a TAgentLogin request from a DN with the configured

nailed-up connection, as follows:

- When this key is set to a Routing Point number, SIP Server immediately establishes a nailed-up connection between an agent's endpoint and the specified Routing Point. After processing the TRouteCall request to the `gcti:park` device, SIP Server parks the agent on `gcti::park`, establishing the persistent SIP connection with the agent's endpoint.
- When this key is set to `gcti::park`, SIP Server parks the agent on the `gcti::park` device directly, establishing the persistent SIP connection with the agent's endpoint.
- When this key is set to an empty value, SIP Server disables this feature for a particular agent in a current login session.

Key: **ReasonCode**
Type: String
Values: `NailedUpConnectionTerminated`
Event: EventAgentNotReady

Specifies that the nailed-up connection is terminated.

## Feature Limitations

- Consultation calls for nailed-up DNs are supported in single dialog mode only.
- If an agent with the nailed-up connection is participating in the first call before it was ever parked, SIP Server cannot park this agent if the call is released before it is established. For example, if the agent with the nailed-up connection initiates a call and releases it while the call is ringing, or if the agent with the nailed-up connection completes a two-step transfer in ringing state. To avoid this, the agent should call the call center to get parked first.

# Hunt Groups in Business Continuity

A Hunt Group is a set of extension numbers that are grouped as a single logical unit. Depending on the Hunt Group call distribution strategy (sequential or parallel), an incoming call is propagated to one or all extensions within the group. Hunt Groups with the parallel distribution strategy (simultaneous ringing) are now supported in Business Continuity deployments.

## Hunt Group Preferred Site

In DR mode (when both DR peers are running and connected to each other), one DR peer is considered a preferred site for a Hunt Group. The preferred site is configured by the `hg-preferred-site` option of the corresponding Hunt Group DN. When an inbound call arrives at a Hunt Group, SIP Server checks if the current site is the Hunt Group preferred site. If it is, the call is processed as usual and distributed to Hunt Group members. If it is not, the call is redirected to the preferred site using the DR call forwarding procedure. So, the outgoing calls to Hunt Group members are always distributed from the Hunt Group preferred site. The DR call forwarding procedure is not used for calls distributed from the Hunt Group. Instead, outgoing calls are distributed only to Hunt Group members on a local DN, regardless of the agent presence on this DN.

If a DR peer fails, the remaining DR peer switches to the standalone HA mode and distributes all inbound Hunt Group calls to Hunt Group members; no preferred site check is performed. The same happens if a connection between DR peers is lost—each site tries to distribute all inbound Hunt Group calls locally. This distribution can be successful if on the site where an inbound call arrives, at least one DN belonging to a Hunt Group member is in service. Otherwise, the default routing destination applies.

## Agent Desktop Considerations

To have a call visible on an agent desktop, the desktop must be connected to the Hunt Group preferred site. The agent desktop preferred site must be set to the same value as the Hunt Group preferred site. If the agent desktop connects to the non-preferred site and tries to log in an agent, SIP Server allows this login but notifies the agent desktop through a special EventPrivateInfo containing the name of the SIP Server DR peer.

In case of preferred site failure and recovery from the failure, SIP Server notifies agent desktops about Hunt Group members through EventPrivateInfo recommending them to log in to the Hunt Group preferred site.

## SIP Phone Connections

In Business Continuity deployments, SIP phones must be connected to both DR peers simultaneously, where dual registration is strongly recommended. For single-registration SIP phones, some limitations apply. Based on its configuration, the phone chooses the preferred site to send outgoing calls and handle outgoing SIP traffic.

## Feature Configuration

On a DN of type ACD Queue, specify the following configuration option in the **[TServer]** section:

- **hg-preferred-site**

For Business Continuity deployments, see Basic Deployment for details.

### hg-preferred-site

Default Value: No default value
Valid Values: Any string value
Changes Take Effect: For next call distribution

Specifies the name of the SIP Server DR Peer application corresponding to the preferred Hunt Group site. If not set or set to an invalid application name, the preferred Hunt Group site cannot be determined, and inbound Hunt Group calls are processed at the site where they are received.

## Feature Limitations

- If a preferred site fails, calls can be delivered to an agent phone when an agent desktop is not yet logged in to the non-preferred site.
- If a connection between DR peers is lost, Hunt Group members might receive calls even if they are already on calls at the other peer.
- If an agent desktop does not comply with the recommendation to reconnect to the preferred Hunt Group site, or a connection to the DR peer is unavailable for the desktop and SIP phone is still connected to both sites, there is a risk of non-monitored calls arriving at the agent phone. This situation can also occur if different preferred sites are configured for the desktop and for the Hunt Group.
- During preferred site startup, inbound Hunt Group calls are routed to a default destination on the preferred site until agents/phones become available at this site.
- For single registration SIP phones, the following limitations apply:
  - If inter-site connection is lost, only the preferred site distributes Hunt Group calls to the phones.
  - An alternate site will not distribute Hunt Group calls to phones until they REGISTER with the alternate site.

See other limitations common for Hunt Groups.

# Shared Call Appearance in Business Continuity

Starting with SIP Server version 8.1.101.75, Shared Call Appearance (SCA) is supported in Business Continuity deployments.

In Business Continuity mode (when both BC/DR peers are running and connected to each other), one DR peer is considered a preferred site for SCA. The preferred site is configured by the **sca-preferred-site** option of the corresponding SCA DN. When an inbound call arrives at an SCA, SIP Server checks if the current site is the SCA-preferred site. If it is, the call is processed as usual and distributed to SCA members. If it is not, the call is redirected to the preferred site using the BC call forwarding procedure. So, the outgoing calls to SCA members are always distributed from the SCA-preferred site.

The DR call forwarding procedure is not used for calls distributed from the SCA. Instead, outgoing calls are distributed only to SCA members on a local DN, regardless of the agent presence on this DN.

If a DR peer fails, the remaining DR peer switches to the standalone HA mode and distributes all inbound SCA calls to SCA members; no preferred site check is performed. The same happens if a connection between DR peers is lost—each site tries to distribute all inbound SCA calls locally. This distribution can be successful if, on the site where an inbound call arrives, at least one DN belonging to an SCA member is in service.

## Feature Configuration

1. On the Primary shared-line DN, specify the following configuration option in the **[TServer]** section:
   - **sca-preferred-site**
2. In the SIP Server Application, specify the following configuration option in the **[TServer]** section:
   - **dr-peer-location**

For Business Continuity deployments, see Basic Deployment for details.

### sca-preferred-site

Default Value: No default value
Valid Values: Any string value
Changes Take Effect: For the next call

Specifies the name of the SIP Server DR Peer application corresponding to the preferred SCA site. If not set or set to an invalid application name, the preferred SCA site cannot be determined, and inbound SCA calls are processed at the site where they are received. The option can be configured only for the Primary shared line DN, where the **shared-line** option is set to `true`.

## Feature Limitations

- Phones of SCA members must be SIP registered at the same preferred site.
- If a preferred site fails and an inbound call comes to SCA at a non-preferred site, calls will be delivered to those SCA members' phones which have already determined the preferred site failure and have SIP registered at the non-preferred site.
- If a preferred site recovers after failure and an inbound call comes to SCA at a preferred or non-preferred site, calls will be delivered to those SCA members' phones which have already determined the preferred site recovery and have SIP registered at the preferred site.
- If a connection between DR peers is lost, calls arriving at a non-preferred site will not be delivered to SCA members phones.

# Instant Messaging in Business Continuity

Starting with release 8.1.101.97, Instant Messaging (IM) functionality is supported in multi-site and Business Continuity deployments. The IM functionality is performed through a T-Library client (Workspace Desktop). When an agent at the desktop makes an IM input, SIP Server receives a TPrivateService request. The IM is delivered to the desktop via EventPrivateInfo messages. A SIP INVITE dialog establishes the IM session between SIP Servers, and a SIP MESSAGE message delivers the IM sentence.

### Supported Call Operations

The following call operations are supported within an IM session for multi-site calls:

- Direct calls between agents using TMakeCall
- Routing
- Treatments
- Supervision

## Feature Configuration

- On the Instant Messaging DN, in the **[TServer]** section, set the **sip-signaling-chat** option to none, so no SIP session with an agent endpoint is created for the IM call.
- For the IM solution to work, make sure the following configuration options are enabled (set to `true`) in the Workspace Desktop and Stat Server applications:
  - **multimedia**
  - **voice**

**Note:** If a URS/ORS application (a strategy) dedicated to serve IM calls uses CollectDigits or PlayAnouncementAndDigits treatments, the processing of these treatments should be started after the first EventPrivateInfo is received in the application's session. The SuspendForEvent URS function will suspend the strategy execution until URS receives the specified event. The Type parameter of the SuspendForEvent function must be set to the integer value 150 for EventPrivateInfo.

## Feature Limitations

- In multi-site deployments, the `route` or `direct-uui` ISCC transaction types are required.
- Instant Messaging transfers are not supported in multi-site deployments.
- Instant Messaging conferences are not supported in multi-site deployments.

- When an IM call is routed across sites, SIP Server will pass the IM transcript to the remote site if an ISCC transaction precedes the actual routing (`route` or `direct-uui`), but it will not pass the IM transcript to the remote site if an ISCC transaction follows the actual routing (such as Call Overflow (COF)).

# Enhanced disaster recovery solution for outbound calls

Introduced in SIP Server version 8.1.103.78. After receiving a negative response, SIP Server can now select an alternative trunk for outbound calls. In addition, SIP Server can now attempt to connect to a DN via an alternative softswitch (found in the DN configuration) if the first attempt to connect to a DN via a softswitch resulted in a negative response from that softswitch.

The following Application-level option supports this feature:

**sip-error-codes-overflow**
Setting: [TServer] section, SIP Server Application
Default Value: An empty string (or 503 error code)
Valid Values: A list of patterns for numeric error codes separated by a comma (,). Letter X in a pattern represents any digit. A single pattern must start with a digit and contain all 3 digits, and a pattern containing "X" should conclude the pattern's list, if present. Examples:

- `503`
- `503,504`
- `487,50X`
- `487,5XX`
- Patterns `5X3,XXX` are invalid

Changes Take Effect: For the next call

When, on an initial INVITE message, SIP Server receives a negative response containing the error code that matches the option value setting, SIP Server attempts to find an alternative trunk or softswitch to initiate a call.

# BC Configuration Options

This topic describes configuration options that are used in the deployment of SIP Business Continuity. For high-availability-specific options, see the HA Configuration Options topic for details.

For a complete list of configuration options, refer to the *SIP Server Deployment Guide*.

## Application-Level Options

### connect-nailedup-on-login

Setting: [TServer] section, Application and DN levels
Default Value: An empty string
Valid Values: Routing Point number, `gcti::park`
Changes Take Effect: At the next agent login session
Related Feature: Nailed-Up Connections

Specifies SIP Server actions when receiving a TAgentLogin request from a DN with the configured nailed-up connection, as follows:

- When this option is set to a DN of type Routing Point, SIP Server immediately establishes a nailed-up connection between an agent's endpoint and the specified Routing Point. After processing the TRouteCall request to the `gcti:park` device, SIP Server parks the agent on `gcti::park`, establishing the persistent SIP connection with the agent's endpoint.
- When this option is set to `gcti::park`, SIP Server parks the agent on the `gcti::park` device directly, establishing the persistent SIP connection with the agent's endpoint.
- When the value for this option is not specified (the default), SIP Server does not take any action.

At a DN level, this option must be set on agent Extension DN, or, if this DN is located behind the softswitch on the respective softswitch DN.

### disconnect-nailedup-timeout

Setting: [TServer] section, Application and DN levels
Default Value: `0`
Valid Values: Any positive integer
Changes Take Effect: At the next nailed-up connection
Related Feature: Nailed-Up Connections

Specifies whether SIP Server terminates an agent's nailed-up connection because of the agent's inactivity. When set to a non-zero value, SIP Server waits this time interval, in seconds, before terminating the agent's nailed-up connection. When set to `0` (the default), SIP Server does not terminate the agent connection.

## dr-forward

Setting: [TServer] section, Application level
Default Value: `off`
Valid Values:

- `off`—DR forwarding to the peer switch is disabled. SIP Server delivers calls to a DN on the local switch.
- `no-agent`—SIP Server delivers a call to a DN on the local switch when there is an agent logged in on this DN; if there is no agent logged in, SIP Server forwards the call to the peer switch. This setting applies only to DNs on "dual-registered" SIP endpoints that simultaneously register to both peers, or for DNs without any registered endpoints, such as for "remote agents".
- `oos`—SIP Server delivers a call to a DN on the local switch when the DN is in service; if the DN is out of service, SIP Server forwards the call to the peer switch. This setting applies only to DNs on "single-registered" SIP endpoints that register only to the preferred peer unless there is an error, in which case they register to the alternate peer.

Changes Take Effect: Immediately

Defines a system-wide mode of forwarding inbound and internal calls when SIP Server is operating in Business Continuity mode. This option can also be set at the DN level, in which case the setting overrides that set at the Application level.

**Notes:**

- The registration timing of endpoints must be carefully considered when using the `oos` setting. For maximum responsiveness in a disaster scenario, a short registration interval must be used so the phone can quickly detect when a peer is unavailable. The deployment should be properly planned to account for the corresponding load of REGISTER messages.
- For both the `no-agent` and `oos` settings, SIP Server only forwards calls targeting an Extension DN, and it will only forward each call a single time; if the other peer is unable to deliver the call, an error is generated.
- With the `oos` setting, if a desktop is unable to connect to the site where a SIP phone is registered, it might result in a phone registering a DN on one peer while the agent desktop connects to the other peer. Calls would be delivered to the phone, but the agent desktop would be unaware of these calls.

## dr-peer-location

Setting: [TServer] section, Application level
Default Value: `NULL`
Valid Values: A valid name of the DR peer Switch
Changes Take Effect: on the next target detection

Specifies the location of the other SIP Server in the DR pair. If set to `NULL` (the default), SIP Server is unable to support the Dial Plan feature.

## dr-peer-trunk

Setting: [TServer] section, Application level
Default Value: `NULL`
Valid Values: A valid name of a `Trunk` DN that points to the DR peer site
Changes Take Effect: Immediately

Specifies that this SIP Server is a part of a DR pair, and identifies the Trunk DN that points to the other SIP Server in the DR pair. If set to NULL (the default), SIP Server operates in the traditional single mode.

### graceful-shutdown-sip-timeout

Setting: [TServer] section, Application level
Default Value: 4
Valid Values: 0–32
Changes Take Effect: Immediately

Specifies the timeout, in seconds, during which SIP Server re-transmits the BYE requests that were not confirmed with 200 OK responses. The timeout starts as soon as the last call is ended. If set to 0 (zero), no BYE requests are re-transmitted. The timeout applies only when SIP Server processes the graceful shutdown.

### shutdown-sip-reject-code

Setting: [TServer] section, Application level
Default Value: 603
Valid Values: 300–603
Changes Take Effect: Immediately

Specifies the error response used for rejecting new INVITE messages received by the system that is in shutdown mode. If set to 300, 301, or 302, SIP Server first checks to see if **dr-peer-trunk** is configured, and if so, sends the contact of that Trunk DN in the 302 response.

## DN-Level Options

### dr-oosp-transfer-enabled

Setting: [TServer] section, DN level
Default Value: true
Valid Values: true, false
Changes Take Effect: For the next call

In Business Continuity deployments, for special circumstances where an inbound call remains on the same site where it arrives and SIP Server puts itself Out of Signaling Path. This option is supported only for Trunk DNs pointing to external destinations. It must not be configured on the trunks between SIP Servers.

If set to false on the Trunk DN from where an inbound INVITE is received, SIP Server stays in the signaling path if the call, after being processed on the Routing Point DN, is sent to the local Extension DN where the DR call forwarding procedure is applied to deliver the call to the corresponding DN on the peer SIP Server. If set to true (the default), SIP Server puts itself Out Of Signaling Path.

### hg-preferred-site

Setting: [TServer] section, DN level

Default Value: No default value
Valid Values: Any string value
Changes Take Effect: For the next call
Related Feature: Hunt Groups in Business Continuity

Specifies the name of the SIP Server DR Peer application corresponding to the preferred Hunt Group site. If not set or set to an invalid application name, the preferred Hunt Group site cannot be determined, and inbound Hunt Group calls are processed at the site where they are received.

## sca-preferred-site

Setting: [TServer] section, DN level
Default Value: No default value
Valid Values: Any string value
Changes Take Effect: For the next call
Related Feature: Shared Call Appearance in Business Continuity

Specifies the name of the SIP Server DR Peer application corresponding to the preferred SCA site. If not set or set to an invalid application name, the preferred SCA site cannot be determined, and inbound SCA calls are processed at the site where they are received. The option can be configured only for the Primary shared line DN, where the **shared-line** option is set to `true`.

# Using IP Phones

This section describes how SIP endpoints, such as IP phones, work with SIP Server in Business Continuity mode.

## Supported IP Phones

See the Genesys Supported Media Interface Guide (SMI) document for information on supported SIP phones, including in SIP Business Continuity mode.

**Note:** Advanced IP phone features, such as Presence and MWI, are not available in SIP Business Continuity mode.

Refer to device-specific documentation for detailed information and instructions for configuring the phone.

## Registration Requirements

In a standalone SIP Server configuration with Business Continuity mode activated, agents' phones must be able to register on two sites in one of the following ways:

- Simultaneously (dual registration)—Register on both peer SIP Servers at the same time.
- Sequentially (single registration)—Register on the main peer SIP Server first; if that peer SIP Server is down, then register on the secondary peer SIP Server.

There are also specific configuration requirements for SIP endpoints. In the following situations, the **dr-forward** must be set to `oos`:

- When SIP endpoints are configured to register sequentially.
- When Bria or ALU IP phones are configured.

# Using Siemens OSV

SIP Server integrated with Siemens OpenScape Voice version 5 can be configured in Business Continuity mode. You must configure the option **dr-forward**=`no-agent` on the Application or DN (`Voice over IP Service` DN with **service type**=`softswitch`) when you configure SIP Server.

See the SIP Server Integration Reference for information and instructions about configuring the Siemens OpenScape Voice PBX.

# Known Issues and Recommendations

- Agent Desktops are not able to issue T-Requests (TMakeCall, TInitiateTransfer, and so on) with `AttributeLocation` to reach a destination in a DR pair, because:
  - The origination site does not know the real destination location for the agent.
  - One of the DR peers can be down.

    **Note:** The above restrictions are not applicable to the URS as it always knows exactly the location of the call destination.
- Stat Server 8.1.2 or later must be used to properly support SIP Business Continuity environment.
- Advanced Disconnect Detection Protocol (ADDP) must be configured in the Stat Server application on the connection to SIP Server. It is also recommended to configure ADDP in other components on the connection to SIP Server.