



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# SIP Server HA Deployment Guide

Network Design Considerations

4/23/2025

# Network Design Considerations

## Contents

- **1 Network Design Considerations**
  - 1.1 General Network Design Considerations
  - 1.2 SIP Server High Availability Characteristics Essential for Network Design
  - 1.3 Dual-NIC (or multi-homed) hosts

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)

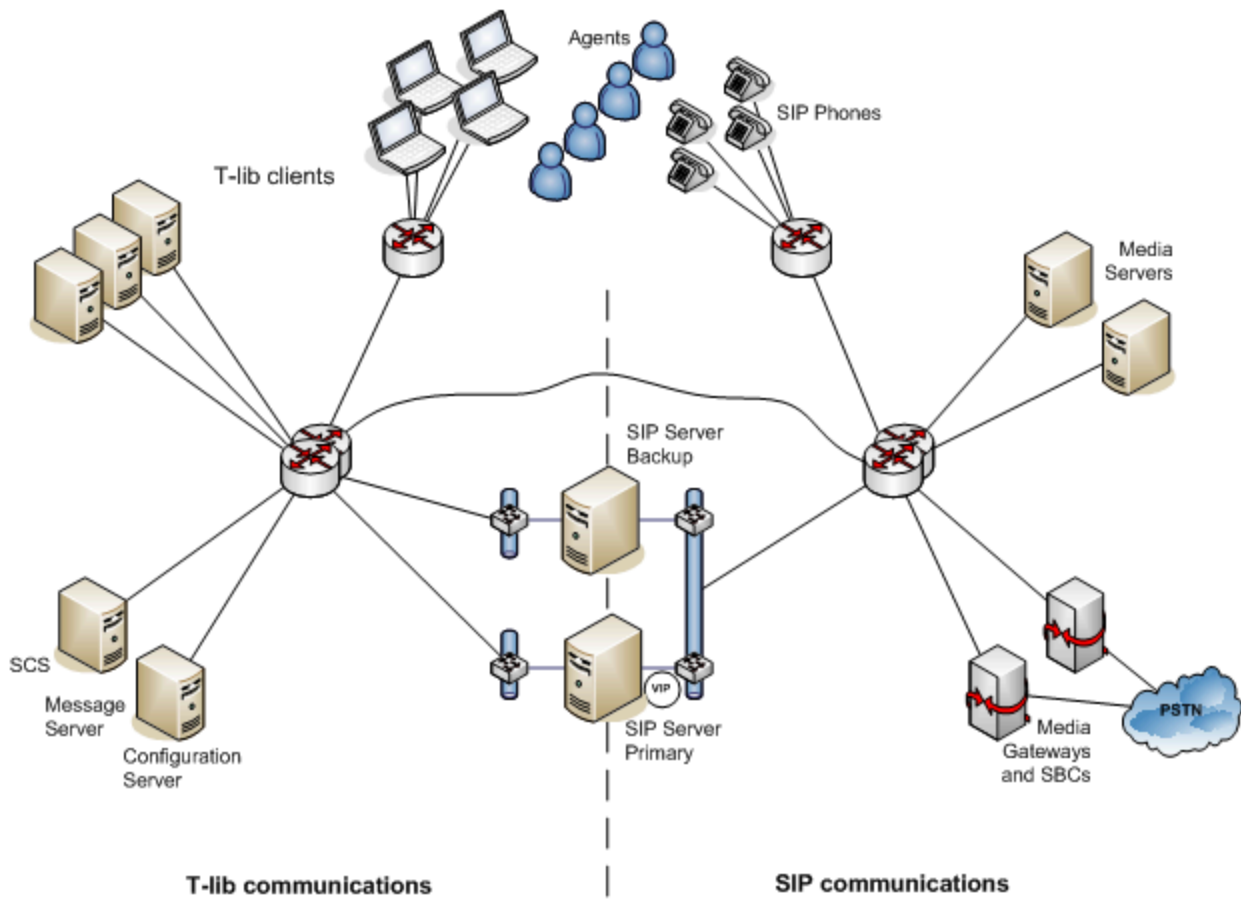
Network design must ensure that the network of VIP (VLAN) is extremely reliable.

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.