6AOSCG0023-29B
September 2013

Configuration Guide

# Configuring SIP Trunk Failover in AOS

This configuration guide describes the configuration and implementation of Session Initiation Protocol (SIP) trunk failover in ADTRAN Operating System (AOS) voice products. This guide includes the command line interface (CLI) commands necessary for failover configuration, example configurations, and the methods used to monitor SIP failover actions.

This guide consists of the following sections:

## SIP Trunk Failover Overview

SIP technologies are used in today's communication networks to facilitate communication between endpoints in the network, whether they are local to the main enterprise site, or functioning at a remote location. SIP services provide more cost effective and scalable solutions for enterprise communication needs than traditional telephony services, and provide these services through SIP trunking and SIP networking. These configured networks often rely on some sort of redundancy to maintain VoIP connections, even when SIP servers become unreachable. SIP trunk failover configurations provide that redundancy to maintain VoIP connections and prevent loss of connectivity. *Figure 1* outlines the network topology in which SIP failover is used.

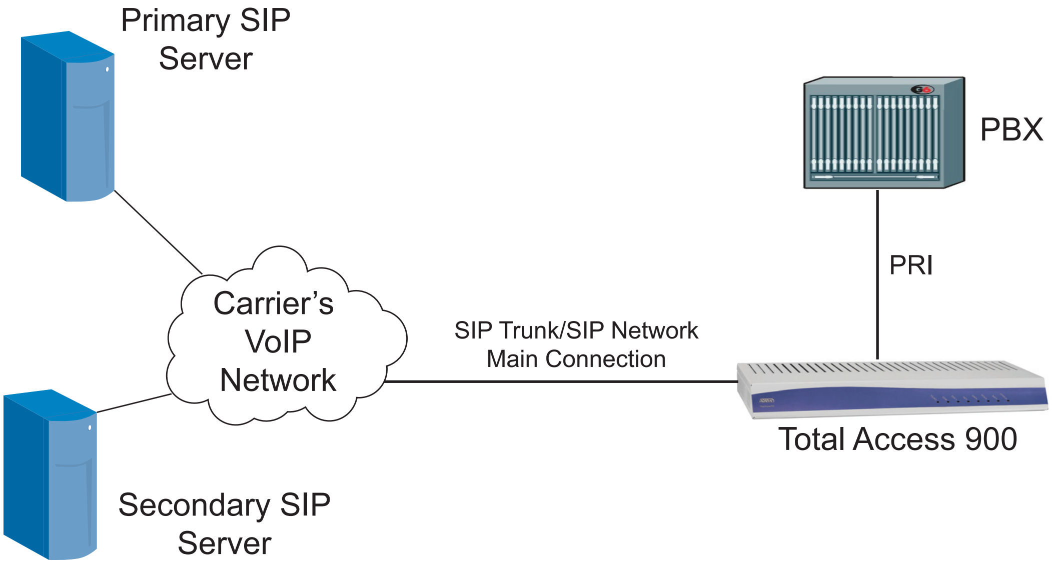

**Figure 1. SIP Trunk Failover Network Topology**

In one method of AOS SIP trunk failover, the AOS unit can be configured to communicate with SIP servers by specifying servers' fully qualified domain names (FQDNs) that are resolved using the Domain Naming System (DNS) protocol and DNS service records (SRV) included in DNS resolutions. When the AOS unit resolves the SRV records, a sorted list of SIP servers is created. The sort and order of these servers depends on the SRV priority and weight as defined in RFC 2782. Alternatively, AOS units will fall back to using A records if SRV records are not available, or the primary and redundant SIP servers can be manually configured with an IP address.

Typically, anytime the AOS unit needs to initiate a dialog with a particular server, it tries the first server in the sorted list (**Primary SIP Server** in *Figure 1*). Subsequent servers are only used after entering a failure state with all previous servers, which means the primary SIP server is no longer responding, and the AOS unit must switch to a secondary SIP server to maintain SIP communications. However, even if the AOS unit has gone into failover mode and is communicating with the secondary server, whenever a new dialog is initiated, it is initiated with the first server in the list. This failover behavior assumes that registration information is replicated across all of the servers in the sorted list. In other words, the AOS unit will not register to the new server before it sends calls to the server. This is the default SIP trunk failover method for AOS products.

ADTRAN supports two methods of SIP trunk failover. The default method, as described above, relies on the unit's server list for connection to SIP servers, and may produce unwanted call behavior if the unit is placed in an environment where the SIP registrations are not shared across all secondary servers. The second SIP failover method relies on servers that are validated through additional configuration, and produces a more stable failover practice in which the SIP trunk failover behavior can be more predictable and controlled. Both methods are configured on the SIP trunks within the network, and each method is configured on a per-trunk basis. These methods are described in the following sections.

> NOTE *SIP trunk failover is configured on SIP trunks, on a per-trunk basis. For more information about SIP trunks, and their configuration, refer to the configuration guide Voice Traffic over SIP Trunks or the configuration guide Configuring SIP Trunking and Networking available online at https://supportforums.adtran.com.*

## AOS Default SIP Trunk Failover

In this type of SIP trunk failover, each SIP trunk provides configuration for a primary and possibly one secondary (or more) SIP servers. Each configured server is identified by either a static IP address or a host name. Each IP address (or host name) is prioritized into a list on the SIP trunk. When the SIP trunk attempts to connect to the SIP server, each INVITE or REGISTER message is sent to the first IP address in the list. If no response is received within the specified timer setting, then the request rolls over to the next IP address on the list. If the end of the list is reached without receiving a response, the request is aborted.

In this method, each SIP trunk attempts to maintain an active registration to the highest priority server that responds at the time of registration. The SIP trunk does not attempt to generate a REGISTER message to each server on its list. Rather, each trunk attempts to register to the primary server, and, if unsuccessful, attempts to failover to a secondary server. Once a successful response is received, each trunk attempts to reregister to the primary server based on the expiration value in the SIP REGISTRATION response message and the trunk's configured registrar threshold.

## AOS Validated SIP Trunk Failover

In this type of SIP trunk failover, the basic function of the failover is the same as the default method. However, extra control of the failover behavior is achieved by extra configuration in which the chosen candidate server in a failover situation is validated as operational through successful SIP registration. In this method, the SIP failover operation behaves as follows:

1. Initiated dialog to the current (typically primary) server fails.
2. The AOS unit's server selection algorithm chooses a new server candidate.
3. The originating SIP identity (OSID) is unregistered.
4. A SIP REGISTER request for the OSID is sent to the server candidate. If this request fails, the validation process begins again at Step 2.
5. Once a successful registration of the OSID occurs, the server candidate is designated as valid.
6. The validated server candidate is then used for all future dialog initiations for the given OSID and the SIP trunk, until this process is triggered again or the OSID registration expires.

The main difference between this method of SIP trunk failover and the default method is that in this method, the OSID is first unregistered from the previous server used, and then all INVITE requests are sent to the validated server candidate, rather than sending them to the primary server in the SIP server list for the trunk. The validated server is used for the SIP connections until either the server fails or the registration expires.

The triggers that begin the SIP trunk failover behavior in this method include: the SIP server registration expires, the validated server fails, or alterations to the server list result in a list that does not include the current server candidate.

### SIP Trunk Failover Recovery Delay

In AOS firmware release R10.9.0, a recovery delay feature was added to the SIP trunk failover configuration. This feature allows you to configure a delay that keeps the failover feature from selecting a higher priority server that was previously unreachable for registration for the specified amount of time. This feature is useful in failover situations where the AOS device's registration rate and the expiration of the highest ranked server's cache do not align. For example, using the recovery delay in a failover situation can cause the AOS device to refrain from connecting back to the primary server until the primary server's cache has timed out. Once it has reconnected to the primary server, it unregisters from the secondary server.

The recovery delay is configured on a per-trunk basis when SIP trunk failover is used. The delay prevents a server from being selected for requests when the delay is in effect. When configured, the delay goes into effect for a given server when the AOS device transitions it to the failed state. The delay expires once the specified timeout period is reached, and it is cancelled if all other servers in the list are unreachable or if the delay is disabled in the trunk configuration. The delay operates based upon a specified minimum period, but can be configured with both a minimum and maximum delay value. When both values are configured, a random selection of the timeout value within the indicated range occurs. The recovery delay is disabled by default.

## Hardware and Software Requirements and Limitations

SIP trunk failover features are available on AOS voice products as outlined in the *AOS Product Feature Matrix*, available online at https://supportforums.adtran.com.

AOS firmware A5.01 or later is required on your AOS product in order to support validated SIP trunk failover and the monitoring of SIP trunks through Simple Network Management Protocol (SNMP) traps.

AOS firmware R10.9.0 or later is required to support SIP trunk failover recovery delay.

When using validated SIP trunk failover, the ability to use SRV weight fields for load balancing is forfeited. This occurs because in this failover method, the validated server is used for all future requests until it fails or the registration expires, which is incompatible with the implementation of RFC 2782 SRV weights.

Before configuring or using SIP trunk failover, you must configure the primary and secondary SIP servers for the SIP trunk on which you are configuring or using failover. These servers are configured using the commands **sip-server primary** <*ip address* | *host name*> **[tcp [**<*port*>**] | udp [**<*port*>**]]** and **sip-server secondary** <*ip address* | *host name*> **[tcp [**<*port*>**] | udp [**<*port*>**]]**, entered from the trunk's configuration mode. For more information about these commands, refer to the *AOS Command Reference Guide*, available online at https://supportforums.adtran.com.

## Configuring SIP Trunk Failover Behavior

Configuring the SIP failover behavior for the AOS voice product includes these steps:

1. Connect to the AOS unit using the CLI.
2. Configure the global SIP failover settings (optional).
3. Configure the SIP trunk failover settings (optional unless using validated failover).
4. Configure the SIP trunk failover monitoring behavior (optional).

### Connecting to the AOS Unit

SIP trunk failover configuration is only available using the CLI. To begin configuring the AOS unit's SIP trunk failover behavior, follow these steps:

1. Telnet to the unit (**telnet** <*ip address*>). For example:

   **telnet 10.10.10.1**.

   > **NOTE** *If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

2. Enter your user name and password at the prompt.

   > **NOTE** *The AOS default user name is **admin** and the default password is **password**.*

3. Enter Enable mode on your unit by entering **enable** at the prompt as follows:

   ```
   >enable
   ```

4. Enter your Enable mode password at the prompt.
5. Enter the unit's Global Configuration mode as follows:

   ```
   #configure terminal
   (config)#
   ```

## Configuring the Global Settings for SIP Trunk Failover

When configuring SIP trunk failover behavior, you can optionally first configure the SIP timer and rollover settings from the AOS unit's Global Configuration mode. If you are using either method of failover, you only have to configure these settings if your network requires it. These commands are outlined in the following section. For additional details about the commands used to configure SIP failover, refer to the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

To configure the global settings for SIP trunk failover, follow these steps:

1. Optional. Specify the initial round trip time (RTT) estimate (T1) and the maximum retransmit interval for nonINVITE requests and INVITE responses (T2) using the **ip sip timer [T1 | T2]** <*value*> command. The **T1** parameter is an estimate of network round trip time, and is used as the initial request retransmit interval. Several timers are derived from the T1 value. The **T2** parameter is the maximum retransmit interval for nonINVITE requests and INVITE responses. The <*value*> parameter is the time in milliseconds. The valid range for T1 timers is **50** to **1000** ms (**500** ms by default), and the valid range for T2 timers is **1000** to **32000** ms (**4000** ms by default). To change the T1 and T2 timers, enter the commands as follows:

   ```
   (config)#ip sip timer T1 750
   (config)#ip sip timer T2 6000
   (config)#
   ```

   Use the **no** form of this command to return to the default value.

   > CAUTION *ADTRAN does not recommend changing T1 or T2 timer values. T1 and T2 timers are base timers within the unit, and any changes will affect other timers based off of these timers.*

2. Optional. Specify the rollover timer for the SIP trunk. The rollover timer allows the user to control how long to wait before trying the next server. If there is no response after the timer expires, the SIP trunk attempts to send INVITE messages to the highest priority backup SIP server obtained using the DNS SRV record, or the first configured secondary server if no additional servers are available based on the SRV record (if present). Set the time period that the SIP trunk is set to wait for a response to a request before attempting to find an alternate destination using the **ip sip timer rollover** <*value*> command. This command sets the time within which a response to an INVITE or REGISTER request must be received before the request rolls over to the next IP address in the SIP server IP address list. The <*value*> parameter specifies the time period in seconds. Range is **1** to **32** seconds (**3** seconds by default). To configure the time period for which the SIP trunk will continue to attempt a connection to the SIP server, enter the command as follows:

   ```
   (config)#ip sip timer rollover 4
   (config)#
   ```

   Use the **no** form of this command to return to the default value.

3. Optional. Specify the REGISTER rollover time period using the **ip sip timer rollover register [**<*value*> **| follow-primary]** command. This command specifies the time period (in seconds) that the SIP trunk waits for a response to a REGISTER request before attempting to find another SIP server. You can use the <*value*> parameter to specify the time period within a range of **1** to **32** seconds, or you can

use the **follow-primary** parameter to specify that the rollover timer for REGISTER requests is set to the value defined in the **ip sip timer rollover** command. By default, the rollover timer for REGISTER requests is set to **follow-primary**. To change the SIP rollover timer for REGISTER requests, enter the command as follows:

```
(config)#ip sip timer rollover register 8
(config)#
```

Use the **no** form of this command to return to the default value.

4. Optional. Specify the time between SIP endpoint registration attempts using the **ip sip timer registration-failure-retry** command. This command specifies the time (in seconds) that will elapse before a SIP endpoint retries registration with the SIP server after a registration failure has occurred. The <*value*> parameter is the time between attempts, and has a valid range of **10** to **604800** seconds. By default, the retry period is set to **60** seconds. To change the retry period for SIP endpoints, enter the command as follows:

```
(config)#ip sip timer registration-failure-retry 30
(config)#
```

Use the **no** form of this command to return to the default value.

### Global SIP Trunk Failover Settings Configuration Example

The following is a sample configuration of the AOS unit's global settings for SIP trunk failover.

```
(config)#ip sip timer T1 750
(config)#ip sip timer T2 6000
(config)#ip sip timer rollover 4
(config)#ip sip timer rollover register 8
(config)#ip sip timer registration-failure-retry 30
```

After configuring the global SIP settings, you can begin configuring the SIP trunks for SIP trunk failover.

## Configuring the SIP Trunk Failover Settings

After configuring the global settings for SIP trunk failover, you can begin configuring the SIP trunk failover settings for each SIP trunk on which it is necessary. These commands are all issued from the SIP trunk configuration mode, and it is here that you will decide if you are using the default or validated SIP trunk failover method. Both methods can have the same optional basic configuration, however, if you are using the default method, all of the trunk settings are optional because they are already configured by default. If you are using the validated SIP trunk failover method, there is one configuration step that is required (refer to *Configuring Validated SIP Trunk Failover on page 9*), while the rest are optional.

### Specifying the SIP Registration Settings for the Trunk

The first step in configuring the SIP trunk failover settings is to configure the registration settings for the trunk. To begin configuring the registration behavior for the SIP trunk failover settings, follow these steps:

1. Optional. Configure the SIP trunk requested registration expiration time using the **registrar expire-time** <*value*> command. This command specifies the duration of the registration that is sent to the SIP server in the REGISTER request. The <*value*> range for this command depends on the

**registrar threshold** configured for the trunk (set using the **registrar threshold** command on *page 8*). If the threshold is set to **absolute**, the **expire-time** range is <*absolute threshold value*> **+ 6** to **4294967295**. If the threshold is set to **percentage**, the range is **0** to **4294967295**. By default, this value is set to **3600** seconds. To specify a registration expiration time for the trunk, enter the command from the trunk's configuration mode as follows:

```
(config)#voice trunk t01 type sip
(config-T01)#registrar expire-time 1800
```

Use the **no** form of this command to return to the default value.

2. Optional. Specify the number of concurrent registration requests allowed for the trunk using the **registrar max-concurrent-reg** <*value*> command. This command is used to control the maximum number of simultaneous registration requests that are allowed for the trunk, and can be used to help eliminate congestion caused by too many concurrent registration requests. The <*value*> parameter is the number of registrations allowed, and has a valid range of **1** to **32** registrations. By default, **32** concurrent registration requests are allowed. To change the number of concurrent registration requests, enter the command as follows:

   ```
   (config)#voice trunk t01 type sip
   (config-T01)#registrar max-concurrent-reg 2
   ```

   Use the **no** form of this command to return to the default value.

3. Optional. Specify the registration renewal threshold for the trunk using the **registrar threshold [absolute** <*value*> | **percentage** <*percent*>**]** command. The **absolute** <*value*> parameter specifies that the registration renewal occurs when the remaining amount of time on the registration coincides with this value. The <*value*> range is **5** to **604800** seconds. The **percentage** <*percent*> parameter specifies that the registration renewal occurs at a certain remaining percentage of the registration time. Valid <*percent*> range is **1** to **90** percent. By default, the registration renewal threshold is set to **absolute 300** seconds. To change the registration renewal threshold for the trunk, enter the command as follows:

   ```
   (config)#voice trunk t01 type sip
   (config-T01)#registrar threshold percentage 5
   ```

   Use the **no** form of this command to return the registration renewal threshold to the default value.

> NOTE
>
> *For SIP trunk failover, the registrar threshold value (along with the expires value in the REGISTRATION response header) determines when the trunk will attempt to reregister to the primary server in a failover situation.*

### Configuring the SIP Failover Behavior for the Trunk

After you have configured the registration settings for the trunk, you can specify the trunk's failover behavior. Whenever a new request is sent out the configured SIP trunk, the far-end servers are contacted in the prioritized list order. For example, as long as the top priority server continues to respond favorably, it will continue to be used. If the far-end server does not respond, the next server on the list is used for failover. To determine the behavior of the SIP trunk during a failover scenario, continue configuring the SIP trunk failover options by configuring the failover behavior.

To configure these settings, follow these steps:

1. Configure the failover behavior of the trunk using the **sip-server rollover [service-unavailable-or-timeout | timeout-only]** command. The **service-unavailable-or-timeout** parameter specifies that the SIP trunk rolls over to the next listed server if there is no response from the current server, or if the current server responds with a 503 Service Unavailable response. The **timeout-only** parameter specifies that the SIP trunk will rollover to the next listed server if there is no response from the current server. By default, SIP trunks only roll over to the next listed server when there is no response from the current server (**timeout-only**). To change this behavior, enter the command as follows:

   ```
   (config)#voice trunk t01 type sip
   (config-T01)#sip-server rollover service-unavailable-or-timeout
   ```

   Use the **no** form of this command to return to the default setting.

> NOTE *Remember that no matter the failover behavior established with this command, every time the AOS device needs to send a new request it will* ***always*** *try the highest priority IP address in the server list, regardless of previous failover behavior.*

### Configuring Validated SIP Trunk Failover

After configuring the basic SIP trunk failover behavior, you can optionally configure the SIP trunk to only use validated servers when in failover mode. When this feature is enabled, new requests are only sent to valid servers, or the highest priority server to which the SIP trunk can register. This method of SIP trunk failover works in the following manner:

When the AOS unit first boots, it establishes a prioritized list of SIP server addresses, using DNS as necessary. It uses the highest priority server as the destination of outbound trunk registrations. As long as these registrations are successful, the unit continues to use that server. If a failover condition occurs (if a request times out or there is no response from the server), the unit unregisters the specific registration to that server. The unit then iterates through the prioritized list of servers to find a valid one. A server is valid if it accepts the trunk registration request. All other trunk registrations remain unchanged. When the registration expires, the new REGISTER request is always sent to the highest priority server address in the list. You can optionally configure the failover on the trunk to delay communication with the highest priority server for a specified amount of time (see *page 10*).

To add the validation feature to the SIP trunk failover configuration, enter the **sip-server validation register** command from the SIP trunk's configuration mode. This command enables registration for SIP server validation on the SIP trunk.

> NOTE *SIP registration validation cannot be configured in conjunction with registrar servers. You cannot configure registrar servers on the trunk and also use the validation method of SIP failover.*

To enable SIP server validation, enter the command as follows:

```
(config)#voice trunk t01 type sip
(config-T01)#sip-server validation register
```

Use the **no** form of this command to disable the validation feature.

In addition, a SIP trunk failover recovery delay can be configured on the trunk using the SIP server monitor. This delay allows the AOS device to delay communication attempts to a higher priority server for a specified amount of time. By default, this delay feature is disabled. To enable the SIP trunk failover recovery delay, enter the SIP Server Monitor's Configuration mode (using the the **sip-server monitor** command from the SIP trunk's configuration mode), and then enter the **recover delay** <*minimum*> **[**<*maximum*>**]** command. The <*minimum*> parameter is the minimum delay period in seconds. The optional <*maximum*> parameter is the maximum delay period. When a maximum delay period is specified, a randomly selected delay period is selected from within the indicated range. Valid delay minimum and maximum ranges are **0** to **86400** seconds. Using the **no** form of this command disables the delay. By default, the SIP server monitor is disabled and the recovery delay is disabled. Enter the command as follows:

```
(config)#voice trunk t01 type sip
(config-T01)#sip-server monitor
(config-T01-monitor)#recover delay 1800
(config-T01-monitor)#no shutdown
```

The **no shutdown** command must be used on the SIP server monitor to activate the delay process on the trunk.

### SIP Trunk Failover Configuration Examples

The following examples show all the configuration for the SIP trunk in SIP trunk failover, and also includes the validated SIP trunk failover configuration. The first example is the default failover configuration, and the second example is the validation failover configuration.

```
(config)#voice trunk t01 type sip
    (config-T01)#registrar expire-time 1800
    (config-T01)#registrar max-concurrent-reg 2
    (config-T01)#registrar threshold percentage 5
    (config-T01)#sip-server primary as1.adtran.com
    (config-T01)#sip-server secondary as2.adtran.com
    (config-T01)#sip-server rollover service-unavailable-or-timeout

config)#voice trunk t01 type sip
    (config-T01)#registrar expire-time 1800
    (config-T01)#registrar max-concurrent-reg 2
    (config-T01)#registrar threshold percentage 5
    (config-T01)#sip-server primary as1.adtran.com
    (config-T01)#sip-server secondary as2.adtran.com
    (config-T01)#sip-server rollover service-unavailable-or-timeout
    (config-T01)#sip-server validation register
    (config-T01)#sip-server monitor
        (config-T01-monitor)#recover delay 1800
        (config-T01-monitor)#no shutdown
```

Once you have configured the SIP trunk failover settings, the SIP trunk failover configuration is complete. You can optionally choose to monitor the status of your SIP trunks, which is discussed in the following section.

### Configuring the SIP Trunk Failover Monitoring Behavior

You can optionally choose to monitor the registration status of the SIP trunks in your network by using SNMP traps. The details of SNMP operation, use, and configuration are covered in the configuration guide, *SNMP in AOS*, available online at https:supportforums.adtran.com. You should follow the instructions outlined in that document to ensure that SNMP is configured properly on your AOS unit. Once you have configured SNMP on the unit, you can enable SNMP traps on the SIP trunk using the **snmp trap registration failures** <*value*> **interval** <*value*> command from the SIP trunk's configuration mode.

The **snmp trap registration** command specifies that SNMP traps are enabled for the trunk, and that these traps are sent for registration events. In addition, this command specifies how many registration failures can occur before an SNMP trap is sent and at what interval (in seconds) the traps are sent. The **failures** <*value*> parameter specifies the number of failures that occur before a trap is sent. The valid range is **1** to **128** failures. The **interval** <*value*> parameter specifies how many seconds elapse between traps. Valid range is **30** to **86400** seconds. By default, SNMP traps are disabled on the SIP trunk. To enable SNMP traps for registration failures, enter the command as follows:

```
(config)#voice trunk t01 type sip
(config-T01)#snmp trap registration failures 3 interval 3600
```

## SIP Trunk Failover Configuration Example

In the following examples, both the default and validation methods of SIP trunk failover are shown. In the default SIP trunk failover example, the SIP trunk is configured with a primary SIP server at **as1.adtran.com** and a secondary SIP server at **as2.adtran.com**. SNMP traps are configured to report registration events after **3** failed registrations.

The validated SIP trunk failover configuration is the same as the default configuration example, except that the configuration includes enabling the validation feature and the recovery delay.

### Default SIP Trunk Failover Configuration Example

```
voice trunk t01 type sip
    sip-server primary as1.adtran.com
    sip-server secondary as2.adtran.com
    sip-server rollover service-unavailable-or-timeout
    snmp trap registration failures 3 interval 3600
```

### Validated SIP Trunk Failover Configuration Example

```
voice trunk t01 type sip
    sip-server primary as1.adtran.com
    sip-server secondary as2.adtran.com
    sip-server rollover service-unavailable-or-timeout
    sip-server validation register
    snmp trap registration failures 3 interval 3600
    sip-server monitor
        recover delay 1800
        no shutdown
```

## SIP Trunk Failover Command Summary

The following tables outline the commands used in configuring SIP trunk failover. *Table 1* outlines the global failover settings, *Table 2* outlines the SIP trunk settings, and *Table 3* outlines the SNMP settings.

### Table 1. Global Failover Commands

| Prompt | Command | Description |
|---|---|---|
| (config)# | **[no] ip sip timer [T1 \| T2]** <*value*> | Specifies the round trip time (RTT) (**T1**) and the maximum retransmit interval for nonINVITE requests and INVITE responses (**T2**). The <*value*> parameter specifies the time in milliseconds. Valid range for T1 timers is **50** to **1000** ms (**500** ms by default), and the valid range for T2 timers is **1000** to **32000** ms (**4000** ms by default). |
| (config)# | **[no] ip sip timer rollover** <*value*> | Specifies how long to wait before trying the next server in the server address list when in a failover situation. The <*value*> parameter specifies the time period in seconds. Valid range is **1** to **32** seconds. Default value is **3** seconds. |
| (config)# | **[no] ip sip timer rollover register [**<*value*> **\| follow-primary]** | Specifies the time period (in seconds) that SIP trunks wait for a response to a REGISTER request before attempting to find another SIP server. The <*value*> parameter specifies the time period within a range of **1** to **32** seconds. The **follow-primary** parameter specifies that the rollover timer for REGISTER requests is set to the value defined in the **ip sip timer rollover** command. By default, the rollover timer for REGISTER requests is set to **follow-primary**. |

### Table 1. Global Failover Commands *(Continued)*

| Prompt | Command | Description |
|---|---|---|
| (config)# | **[no] ip sip timer registration-failure-retry** <*value*> | Specifies the time between SIP endpoint registration attempts. The <*value*> parameter is the time between attempts, with a valid range of **10** to **604800** seconds. By default, the retry period is set to **60** seconds. |

### Table 2. SIP Trunk Failover Commands

| Prompt | Command | Description |
|---|---|---|
| (config-T01)# | **[no] registrar expire-time** <*value*> | Specifies the duration of the registration that is requested in the REGISTER sent to the SIP server. Valid range depends on the **registrar threshold** setting. If the threshold is set to **percentage**, the **expire-time** range is **0** to **4294967295**. If the threshold is set to **absolute**, the range is **6+**<*absolute threshold value*> to **4294967295**. By default, this value is set to **3600** seconds. |
| (config-T01)# | **[no] registrar max-concurrent-reg** <*value*> | Specifies the maximum number of simultaneous registration requests allowed for the trunk. Valid range is **1** to **32**. By default, **32** concurrent registration requests are allowed. |
| (config-T01)# | **[no] registrar threshold [absolute** <*value*> **\| percentage** <*percent*>**]** | Specifies the registration renewal threshold for the SIP trunk. For SIP trunk failover, the registrar threshold value (along with the expires value in the REGISTRATION response header) determines when the trunk will attempt to reregister to the primary server in a failover situation. The **absolute** <*value*> parameter specifies that the registration renewal occurs when the remaining time on the registration reaches the specified number of seconds; valid range is **30** to **604800** seconds. The **percentage** <*percent*> parameter specifies that the registration renewal occurs at a certain remaining percentage of the registration time; valid range is **1** to **90** percent. By default, the registration renewal threshold is set to **absolute 300** seconds. |

## Table 2. SIP Trunk Failover Commands *(Continued)*

| Prompt | Command | Description |
|---|---|---|
| (config-T01)# | **[no] sip-server rollover [service-unavailable-or-timeout \| timeout-only]** | Configures the failover behavior of the trunk. The **service-unavailable-or-timeout** parameter specifies that the SIP trunk will rollover to the next listed server if there is no response from the current server, or if the server responds with a 503 Service Unavailable response. The **timeout-only** parameter specifies that the SIP trunk will rollover to the next listed server if there is no response from the current server. By default, failover behavior is set to **timeout-only**. |
| (config-T01)# | **[no] sip-server validation register** | Enables validated SIP trunk failover. By default, this feature is disabled. This feature cannot be configured in conjunction with registrar and outbound-proxy servers. |
| (config-T01)# | **[no] sip-server monitor** | Enables the SIP server monitor and enters the monitor's configuration mode. |
| (config-T01-monitor)# | **[no] recover delay** *<minimum>* **[***<maximum>***]** | Enables the SIP trunk failover recovery delay. The *<minimum>* parameter specifies a minimum delay in seconds. The optional *<maximum>* parameter specifies a maximum delay. Valid range is **0** to **86400** seconds. When both a minimum and maximum value are specified, the delay is randomly selected within the range. This feature is disabled by default. |
| (config-T01-monitor)# | **no shutdown** | Enables the SIP server monitor and the recovery delay on the trunk. By default, this feature is disabled. |

## Table 3. SIP Trunk SNMP Commands

| Prompt | Command | Description |
|---|---|---|
| (config-T01)# | **[no] snmp trap registration failures** *<value>* **interval** *<value>* | Enables SNMP traps for registration events on the trunk. The **failures** *<value>* parameter specifies how many failures are allowed before an SNMP event is created. Valid range is **1** to **128** failures. The **interval** *<value>* parameter specifies how many seconds elapse between trap events. Valid range is **30** to **86400** seconds. By default, SNMP traps are disabled on the trunk. |