61210916L1-29.6R
May 2018

ADTRAN®

Configuration Guide

Configuring the SIP Proxy in AOS

This configuration guide examines the SIP proxy feature available in ADTRAN Operating System (AOS) products. An overview of the three proxy operation modes is provided, as well as information about their features, network diagrams, advanced configuration examples, and troubleshooting tools for installation and maintenance assistance.

For a complete explanation of AOS command line interface (CLI) syntax, refer to the *AOS Command Reference Guide*, available online at https://supportforums.adtran.com.

This guide consists of the following sections:

SIP Proxy Feature Overview

ADTRAN developed its SIP proxy feature by incorporating RFC 3261-compliant stateful SIP proxy functionality to provide a way for AOS products to transport IP voice traffic. Using the SIP proxy feature allows AOS products to forward SIP messages between endpoints (phones and softswitches) without being required to interpret the messages as is done with back-to-back user agent (B2BUA) devices.

When using the SIP proxy feature, customers are not restricted to using ADTRAN-compatible (B2BUA) phone models. Unlike the B2BUA, the SIP proxy is not feature dependent. As a result, adding new phone or softswitch features does not require corresponding features in the AOS product or additional configuration to support customer endpoints. Configuration is simplified because creating voice users, voice trunks, and dial plans is not required on the AOS product. In addition to increased interoperability, the SIP proxy feature is switchboard independent and increases survivability options in the AOS products.

The three SIP proxy modes available are outbound, stateful, and transparent. The three proxy modes can be used simultaneously within an AOS product. The operation of analog and IP phones is dependent on the phone's configuration and functionality. The three modes of the SIP proxy feature are discussed in the following sections.

Stateful Proxy Mode

The stateful proxy mode is best suited for existing installations due to the ease of converting from B2BUA to IP phones without modifying the phone configurations. In this mode, phones or user agents (UAs) rely on the SIP server to act as the proxy, and the configuration is very similar to the existing B2BUA. The AOS product takes on the role of proxy. The UA is not aware of other SIP servers on the network in this mode. Each phone is configured to register to the proxy, and the phone is not aware of the softswitch(es). Either the softswitch(es) host name(s) or IP address(es) must be programmed in the system, enabling communication between the two. All phones must use the same softswitch or set of softswitches, and the phone must send all requests to the destination IP address of the AOS device. In stateful proxy mode, the softswitch address configured in the phone is the proxy (AOS device), and SIP signaling is sent to the Layer 3 destination address of the proxy (AOS device).

Outbound Proxy Mode

In the outbound proxy mode, the ADTRAN device’s duties may include numerous functions, such as establishing the service provider's boundaries, receiving and sending Voice over Internet Protocol (VoIP) traffic behind a firewall, controlling network call routing, and network quality of service (QoS). The system may not require configuration to be aware of the softswitch. The softswitch (which can be B2BUA or stateful proxy) takes on the role as the server and registrar in this mode. Requests sent from the phones are routed to the destination IP address of the softswitch. The lack of configuration is usually not an issue because the SIP messages contain the necessary routing information. The softswitch address configured in the phone is the external softswitch, and SIP signaling is sent to the Layer 3 destination address of the proxy.

Transparent Proxy Mode

The transparent proxy mode is best for new installations when the phone does not need to be aware of the device presence (transparency). In this mode, the softswitch is configured as the server and the registrar (and outbound proxy when required). The phones are not aware of the AOS device, and phones are not required to use the same softswitch. Requests sent from the phones are routed to the destination IP address of the softswitch, and the AOS device does not require configuration to be aware of the softswitch. In transparent proxy mode, the softswitch address configured in the phone is the external softswitch, and SIP signaling is sent to the Layer 3 destination address of the external softswitch.

Survivability Feature

The AOS survivability feature operates differently in the voice and data products. This section examines the functionality of the survivability feature in AOS voice and data products.

> NOTE *The survivability feature is only available in the AOS data products running the enhanced feature pack or session border controller (SBC) feature pack software.*

In AOS voice products, the survivability (failover) feature ensures that calls made by any endpoint connected to the device are completed, regardless of the state of the softswitch or proxy. All calls forwarded internally between the proxy and switchboard can be successfully completed, if the B2BUA is properly configured to route such calls over the public switched telephone network (PSTN). Under normal operation, the proxy routes calls to and from all proxy users, and the switchboard routes calls to and from all voice users and trunks. When a softswitch or proxy becomes unavailable, the AOS device enters failover mode and creates a bridge between the proxy and switchboard, ensuring that calls are routed properly.

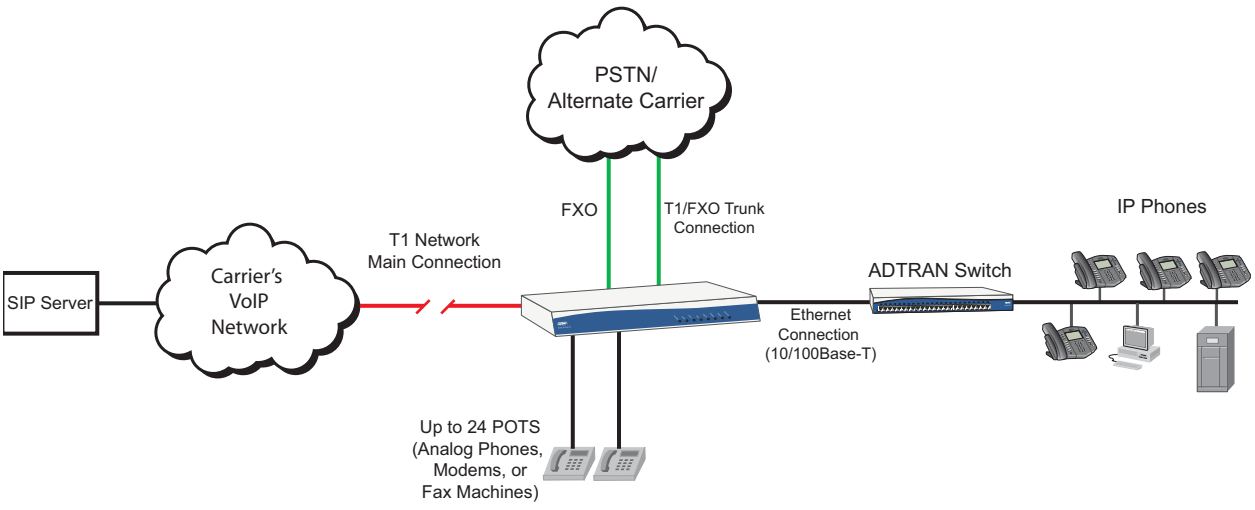

Figure 1. AOS Survivability in Voice Products

In AOS data products, the survivability (failover) feature ensures that calls made by any endpoint connected to the device are completed, regardless of the state of the softswitch or proxy. When a proxy becomes unavailable, the AOS device enters failover mode and creates a bridge between the proxy and the external gateway, ensuring that calls are routed properly. Refer to *Example 4 - Transparent Proxy Mode on an AOS Data Device on page 23* for an example configuration of the application below.

Figure 2. AOS Survivability in Data Products

Hardware and Software Requirements and Limitations

The SIP proxy feature is available on AOS data and voice products as outlined in the *AOS Feature Matrix*, available online at https://supportforums.adtran.com.

In AOS firmware release R11.9.0, the SIP proxy monitor feature and IP address spoofing capabilities were added to the SIP transparent proxy.

In AOS firmware release R13.1.0, additional security features were added to the SIP proxy functionality. These additions include the use and support of Transport Layer Security (TLS) and Secure Realtime Transport Protocol (SRTP) to secure SIP messaging between the AOS SIP proxy and the softswitch. For more information about these security features, their use with the SIP proxy, and other SIP signaling security measures, refer to the configuration guide *SIP Signaling and Media Security in AOS*, available online at https://supportforums.adtran.com.

When considering which mode of operation to use in a particular application, consider the following trade-offs:

Table 1. SIP Proxy and B2BUA Comparison

SIP Proxy Operation	B2BUA Operation
Limited local call routing	More flexible call routing
More flexible with softswitch features	Limited softswitch features
More softswitch support	Limited softswitch support
More phone support	Limited phone support
Large scale	Smaller scale
Easier migration to new SIP features	No migration to new SIP features

Getting Started with the SIP Proxy

The following configuration steps should be completed prior to implementing the SIP proxy configuration:

1. Configure the wide area network (WAN) interface.
2. Configure the local area network (LAN) interface.
3. Optional. Configure the firewall/network address translation (NAT)/virtual private network (VPN).
4. Optional. Configure QoS.
5. Optional. Configure voice trunks and trunk groups for survivability.

Configure the SIP Proxy

The following sections detail the steps required to implement SIP proxy features in AOS with an explanation and required syntax for configuration:

Step 1: Enable the SIP Stack, Protocol(s), and Port(s)

Use the **sip [tcp | udp] [**<*port*>**]** command to enable the AOS SIP stack. By default, the SIP stack is enabled on voice products and disabled on data products. When the SIP stack is enabled, memory is allocated for SIP functionality. The **no sip** command disables the SIP stack and frees memory previously allocated to the stack. To enable the SIP stack, enter the **sip** command from the Global Configuration mode as follows:

```
(config)#sip
```

By default, the SIP stack operates using the User Datagram Protocol (UDP). The optional **[tcp | udp]** parameters of this command allow you to specify which protocol you prefer to use. To change the SIP stack protocol to Transmission Control Protocol (TCP), enter the command from the Global Configuration mode prompt as follows:

```
(config)#sip tcp
```

The <*port*> parameter is also optional. By default, the TCP and UDP ports on which the SIP stack operates is **5060**. The range of available ports is **1** to **65535**. If you need to change the default SIP stack port, enter the command from the Global Configuration mode prompt as follows:

(config)#**sip udp 8900**

*If the command **sip [tcp | udp]** is entered with no port specifications, the port value will default to port **5060**.*

Step 2: Enable the SIP Proxy

Select the SIP proxy mode that is best suited for your application. To configure the SIP proxy to operate in either the stateful or outbound proxy modes, use the **sip proxy** command; to configure the SIP proxy to operate in transparent mode, use the **sip proxy transparent** command in addition to the **sip proxy** command. The **sip proxy** command enables the SIP proxy at a global level, and the **sip proxy transparent** command enables transparent proxy mode, but will only do so if the SIP proxy is globally enabled. Transparent proxy mode results in all SIP traffic being captured by the proxy. Executing the **sip proxy transparent** command automatically enables the SIP intercept application layer gateway (ALG) for the protocols and ports for which the SIP stack is configured. Realtime Transport Protocol (RTP) firewall traversal is enabled by default.

SIP Proxy on AOS Voice Products

To enable stateful or outbound proxy modes for AOS voice products, enter the command from the Global Configuration mode as follows:

(config)#**sip proxy**

To enable the SIP proxy in transparent proxy mode on AOS voice products, enter the **sip proxy** and **sip proxy transparent** commands from the Global Configuration mode as follows:

(config)#**sip proxy**
(config)#**sip proxy transparent**

SIP Proxy on AOS Data Products

The configuration for stateful, outbound, or transparent proxy modes differs on AOS data products. AOS data products include a firewall SIP ALG as well as the SIP intercept ALG. Because the **sip proxy transparent** command automatically enables the SIP intercept ALG, on data products the firewall SIP ALG must be disabled using the **no ip firewall alg sip** command to use transparent proxy mode. Even if the unit is set for transparent proxy mode, it can control which traffic is allowed to be intercepted using **stateless** or **no-alg** entries in firewall configuration.

*For more information on configuring the IP firewall, the SIP ALG, and **stateless** or **no-alg** firewall configuration entries, refer to the IPv4 Firewall Protection in AOS configuration guide or to the AOS Command Reference Guide.*

To enable stateful or outbound proxy modes for AOS data products, enter the **sip proxy** command from the Global Configuration mode as follows:

(config)#**sip proxy**

To enable the SIP proxy in transparent mode on AOS data products, enter the **no ip firewall alg sip**, **sip proxy**, and **sip proxy transparent** commands from the Global Configuration mode as follows:

```
(config)#no ip firewall alg sip
(config)#sip proxy
(config)#sip proxy transparent
```

Step 3: Configure the Softswitch(es)

The guidelines for configuring the softswitch(es) depend on the proxy mode selected. Softswitch configuration is always needed for stateful proxy mode. It is only needed for outbound proxy mode when the SIP request does not contain any fields that can be resolved to the softswitch's location.

Configure Primary Softswitch

To configure the primary softswitch, enter the **sip proxy sip-server primary** <*hostname* | *ip address*> **[tcp | udp] [**<*port*>**]** command from the Global Configuration mode. The <*hostname* | *ip address*> parameter specifies the fully qualified domain name (FQDN) or IP address of the outbound proxy server. IP addresses should be expressed in dotted decimal notation, for example, **10.10.10.1**. The optional **tcp** and **udp** parameters specify the protocol used by the softswitch. The optional <*port*> parameter specifies the port used by the softswitch. Port range is **0** to **65535**. By default, the softswitch uses **udp** on port **5060**. To configure the primary softswitch, enter the command as follows:

```
(config)#sip proxy sip-server primary 198.51.100.2
```

Configure a Secondary Softswitch

To configure a secondary softswitch, enter the **sip proxy sip-server secondary** <*hostname* | *ip address*> **[tcp | udp] [**<*port*>**]** command from the Global Configuration mode. This command can be entered multiple times to configure multiple secondary softswitches. The <*hostname* | *ip address*> parameter specifies the FQDN or IP address of the outbound proxy server. IP addresses should be expressed in dotted decimal notation, for example, **10.10.10.1**. The optional **tcp** and **udp** parameters specify the protocol used by the softswitch. The optional <*port*> parameter specifies the port used by the softswitch. Port range is **0** to **65535**. By default, the softswitch uses **udp** on port **5060**. To configure a secondary softswitch, enter the command as follows:

```
(config)#sip proxy sip-server secondary 203.0.113.2
```

*If a host name is specified, a domain naming system (DNS) server must be configured on the AOS unit with the **name-server** command or be learned via a dynamic IP interface.*

Step 4: Configure SIP Proxy Emergency Call Routing (Optional)

To configure SIP proxy emergency call routing, select the method of emergency call routing to use and configure the emergency number templates.

SpecifyEmergency Call Routing Method

You can select the SIP proxy emergency call routing method by entering the **sip proxy emergency-call-routing [local | proxy]** command from the Global Configuration mode. By default, SIP proxy is set to send all emergency calls directly through the switchboard (the **local** parameter). You can change this setting by entering the command using the **proxy** keyword which specifies that all emergency calls are routed through the proxy before sending them to the switchboard. To return to the default setting, enter the command as follows:

(config)#**sip proxy emergency-call-routing local**

For the default emergency call routing method (**local**) to function on AOS data products, a local SIP gateway must be configured using the **sip proxy local-gateway** <*hostname* | *ip address*> **[tcp | udp] [**<*port*>**]** command. The <*hostname*> parameter is the name of the gateway. The <*ip address*> parameter is the IP address of the gateway. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). The optional **[tcp | udp]** parameters specify the protocol and the optional <*port*> parameter specifies the port for the local SIP gateway. By default, the gateway uses **udp** on port **5060**. The range of available ports is **1** to **65535**. To configure a local SIP gateway on an AOS data product, enter the command from the Global Configuration mode as follows:

(config)#**sip proxy local-gateway 10.19.209.55**

Configure Emergency Call Routing Template

By default, no emergency number templates or patterns are configured in the system; therefore, no calls are classified as emergency calls. To configure emergency number templates, enter the **sip proxy emergency-call-routing [accept** <*template*> **| reject** <*template*>**]** command from the Global Configuration mode. The <*template*> parameter specifies a phone number pattern for matching. Calls matching the template are either accepted or rejected based on the entered keyword.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits

3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.

2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.

3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].

4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

To specify an emergency call routing template, enter the command as follows:

(config)#**sip proxy emergency-call-routing accept 911**

Step 5: Configure Failover Settings (Optional)

SIP proxy failover occurs using an automatically created trunk contained in AOS's basic configuration. This trunk is a hidden SIP trunk with the same default settings as a regular SIP trunk. The default settings are:

- No digits or aliases are specified for matching when trying to route a surviving call.
- No coder-decoder (CODEC) lists are configured or applied.
- The dial string source is set to **request-uri**.
- No keepalive methods are specified.
- P-Asserted-Identity SIP privacy is disabled.

You can optionally change these settings to fit your network using the following commands:

- **sip proxy failover match-digits** *<number>*

  The **sip proxy failover match-digits** command specifies the number of least-significant digits of the dial string needed to match in order to route a surviving call to proxy users during failover. The valid range is **1** to **255**. This command can be entered multiple times to match different dial strings during failover. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover match-digits 10**

- **sip proxy failover match-alias** <*pattern*> **substitute** <*pattern*>

  The **sip proxy failover match-alias substitute** command configures an alias to match a dial string and its corresponding substitution value. When in failover mode, if an INVITE message is directed toward a matching alias, the substitution template is evaluated and compared to current proxy users. The first user to match the substitution value is selected to receive the SIP message. Enter the command from the Global Configuration mode prompt.

  > NOTE *The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or **?**. Using either of these characters outside of quotation marks is interpreted by the CLI as commands and not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

  Both the **match-alias** <*pattern*> and the **substitute** <*pattern*> can use traditional number matching and regular expression matching methods. Traditional number matching uses numbers and wildcard variables as described in the <*template*> explanation in the **sip proxy emergency-call-routing** command in *Step 4: Configure SIP Proxy Emergency Call Routing (Optional) on page 8*. The following example uses the traditional number matching method to match a 7-digit number beginning with 555 and replace it with 5551111:

  (config)#**sip proxy failover match-alias "555XXXX" substitute "5551111"**

  In regular expressions number matching, the match strings are encapsulated by paired / (slash) symbols. This indicates that the pattern is to be treated as a regular expression. Using regular expressions allows for greater flexibility in matching multiple number templates with fewer expressions. The following example uses the regular expression number matching method to match a 7-digit number beginning with 555 and replace it with 5551111:

  (config)#**sip proxy failover match-alias “/555\d{4}/” substitute “/5551111/”**

  > NOTE *AOS is compatible with Perl compatible regular expressions (PCRE). More information on understanding and using regular expressions is available at http://www.pcre.org.*

- **sip proxy failover group match-value** <*pattern*> **new-value** <*pattern*>

  The **sip proxy failover group match-value new-value** command enables forking of calls to users registered with unique extensions in failover mode. Enter the command from the Global Configuration mode prompt.

  > NOTE *The following configurations can lead to unexpected behavior:*
  > - *Matching a valid extension with multiple groups.*
  > - *Creating a failover group with an existing extension.*

> *The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or **?**. Using either of these characters outside of quotation marks is interpreted by the CLI as commands and not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

Both the **match-value** <*pattern*> and the **new-value** <*pattern*> can use traditional number matching and regular expression matching methods. Traditional number matching uses numbers and wildcard variables as described in the <*template*> explanation in the **sip proxy emergency-call-routing** command in *Step 4: Configure SIP Proxy Emergency Call Routing (Optional) on page 8*. The following example uses the traditional number matching method to match any 7-digit number beginning with 555 and add it to a failover group that can be dialed as 5551111:

(config)#**sip proxy failover group match-value "555XXXX" new-value "5551111"**

In regular expressions matching, the match strings are encapsulated by paired / (slash) symbols. This indicates that the pattern is to be treated as a regular expression. Using regular expressions allows for greater flexibility in matching. The following example uses the regular expression number matching method to match a dial string beginning with **5551111.sca** and create a failover group that can be dialed as **5551111**:

(config)#**sip proxy failover group match-value "/^5551111\.sca/" new-value "/5551111/"**

> *AOS is compatible with Perl compatible regular expressions (PCRE). More information on understanding and using regular expressions is available at http://www.pcre.org.*

- **sip proxy failover codec-group** <*name*>

  The **sip proxy failover codec-group** command specifies the previously configured CODEC list to use during a failover. This command is only applicable to AOS voice products. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover codec-group List1**

  > *For more information regarding CODEC list configuration, refer to the **Voice CODEC List** command set in the AOS Command Reference Guide.*

- **sip proxy failover dial-string source [request-uri | to]**

  The **sip proxy failover dial-string source** command specifies the dial string source type to use on the failover trunk. The **request-uri** setting specifies the Request-URI user field as the dial string source. The **to** setting specifies the TO header field as the dial string source. The default setting is **request-uri**. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover dial-string source request-uri**

- **sip proxy failover sip-keep-alive [info** <*value*> **| options** <*value*>**]**

  The **sip proxy failover sip-keep-alive** command specifies the SIP keepalive method (**info** or **options**). The <*value*> parameter specifies the amount of time (in seconds) between the SIP keepalive messages sent during a call. Time range is **30** to **3600** seconds. By default, no keepalive methods are specified. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover sip-keep-alive info 180**

- **sip proxy failover trust-domain** [**p-asserted-identity-required**]

  The **sip proxy failover trust-domain** command enables the AOS unit to send P-Asserted-Identity to the phones when in failover mode. The command also allows the AOS unit to look at any P-Asserted-Identity header the phones might send while the AOS device is in failover mode.

  The **p-asserted-identity-required** parameter is only used with nonstandard softswitches, and should not be used in normal configurations. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover trust-domain**

Additional commands are available to change the configuration of the SIP proxy when in failover (or survivability) mode to fit your network. You can optionally change these settings using the following commands:

- **sip proxy failover accept-registrations**

  The **sip proxy failover accept-registrations** command allows the SIP proxy to accept new registrations when in failover mode. By default, this feature is disabled and is not typically used with most network configurations. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover accept-registrations**

- **sip proxy failover direct-inbound**

  The **sip proxy failover direct-inbound** command allows direct inbound routing of calls to proxy users during failover without first routing it out a SIP trunk. This feature is used when a network configuration does not use a SIP trunk. By default, this command is disabled. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover direct-inbound**

- **sip proxy failover register-expires** <*value*>

  The **sip proxy failover register-expires** command specifies the length of time SIP phone registrations remain in the SIP proxy database while the SIP proxy is in failover. Once the **register-expires** time has elapsed, the SIP phones must re-register or they will be removed from the SIP proxy database. This setting only applies when the SIP proxy is in failover mode. The <*value*> parameter specifies the amount of time (in seconds) that the registration is valid. Time range is **30** to **86400** seconds. By default, <*value*> is **300** seconds. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy failover register-expires 120**

Step 6: Configure SIP Proxy Monitor (Optional)

The availability of SIP servers can be monitored by the SIP proxy. As of AOS firmware release R11.9.0, this feature is available in stateful or transparent proxy mode. When enabled, the SIP proxy monitor can operate in one of two modes: **continuous** or **on-failure**. In **continuous** mode, the proxy monitor always polls the SIP proxy server(s) to determine operational state. In contrast, the **on-failure** mode only polls SIP proxy servers during a detected failure state. The mode is configured using the **mode** command in the SIP Proxy Monitor Configuration mode.

Additional monitoring behaviors can be configured to specify the poll timeout, intervals, recover response, poll request grammar, and SNMP traps. Each configuration option is explained in this section.

Enable SIP Proxy Monitor

To specify whether the SIP proxy monitor will function in both stateful and transparent, or only stateful mode, enter the **sip proxy sip-server monitor [stateful-transparent | stateful-only]** command from the Global Configuration mode. Specifying **stateful-transparent** indicates the monitor will function in both stateful and transparent proxy modes. Specifying **stateful-only** indicates the monitor will function in stateful proxy mode only (this is the default behavior). Using the **no** form of this command returns to the default setting. To enable SIP proxy monitor for both stateful and transparent proxy, enter the command as follows:

```
(config)#sip proxy sip-server monitor stateful-transparent
(config)#
```

> NOTE *In order to use the SIP proxy monitor in transparent mode, you must have entered the **sip-server primary** command. This command tells the proxy which server to monitor. Refer to Step 3: Configure the Softswitch(es) on page 7 for more information about this command.*

To enable the SIP proxy monitor, and enter the SIP Proxy Monitor Configuration mode, enter the following command from the Global Configuration mode:

```
(config)#sip proxy sip-server monitor
    Configuring New Proxy Monitor.
(config-proxy-monitor)#
```

Configure Proxy Monitor Mode

Once you have entered the SIP Proxy Monitor Configuration mode, you can configure the specific behavior of the proxy monitor feature.

The polling behavior of the proxy monitor is configured using the **mode** command. Specify **continuous** to proactively poll SIP servers regardless of their state, or **on-failure** which only polls failed servers. In **on-failure** mode, the polling will cease once the server returns to a functioning state. Use the following command to specify either **continuous** or **on-failure** polling:

```
(config-proxy-monitor)#mode continuous
(config-proxy-monitor)#mode on-failure
```


The default interval for **continuous** polling is **30** seconds. To change the interval, enter the following command where a valid range for <*value*> is **1** to **84600**.

(config-proxy-monitor)#**mode continuous interval** <*value*>

Configure the Poll Timeout and Recovery

The polling behavior can be altered to specify the timeout interval, recovery delay, recovery interval, and the number of successful responses necessary to determine if the server is available for use.

The poll request timeout specifies the number of seconds the SIP proxy monitor may wait for a response when issuing a poll request to a configured SIP server before it determines the poll request was unsuccessful. The default timeout is **32** seconds. To change from the default setting, enter the following command where a valid range for <*value*> is **1** to **600** seconds:

(config-proxy-monitor)#**poll timeout** <*value*>

*The value configured for **poll timeout** should not be greater than 64 multiplied by the configured value of **sip timer T1**.*

The **recover delay [**<*min*> **|** <*min*> <*max*>**]** configures the SIP proxy monitor recovery delay. 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 **recover delay** <*min*> command specifies the minimum length of the recovery delay period. The valid range for <*min*> is **0** to **86400** seconds.

The **recover delay** <*min*> command specifies a range for the recovery delay period. The actual value for the recovery delay period is chosen randomly within this range. The valid range for both <*min*> and <*max*> is **0** to **86400** seconds.<*max*>. The <*max*> value must be greater than the <*min*> value.

The **recover no-response interval [**<*value*> **|** <*min*> <*max*>**]** only takes effect when a SIP server is down. The proxy monitor recovery operation initiates when no response is received from the SIP server in response to a poll sent by the SIP proxy monitor.

The **recover no-response interval** <*value*> command specifies when there is no response from the SIP server, the proxy monitor will poll the SIP server at the interval specified as <*value*>. The valid range for <*value*> is **1** to **86400** seconds.

The **recover no-response interval** <*min*> <*max*> command polls the SIP server if there is no response, but at an increasing interval which begins at the minimum value (the <*min*> parameter) and doubles at each interval up to the maximum value (<*max*> parameter). This increasing range allows the system to avoid bursts of data sent at the same time. The valid range for <*min*> and <*max*> is **1** to **86400** seconds.

The default setting for the **recover no-response interval** is a range of **5** to **60** seconds. To configure the SIP proxy monitor recovery polling interval when a response is not received, enter one of the following commands:

(config-proxy-monitor)#**recover no-response interval** <*value*>
(config-proxy-monitor)#**recover no-response interval** <*min*> <*max*>

Once the SIP server responds successfully to a recovery poll (indicating the SIP server is operational) the proxy monitor continues polling the SIP server until it receives a specific number of successful responses. The **recover responses** <*value*> **interval** <*value*> command specifies the number of successful responses necessary and the interval at which to continue polling before returning service to the SIP server. The default setting is to recover after **3** successful responses which are sent at **10** second intervals. This can be changed using the following command where the valid range for **responses** <*value*> is **1** to **255** and the valid range for **interval** <*value*> is **1** to **86400** seconds:

(config-proxy-monitor)#**recover responses** <*value*> **interval** <*value*>

Configure SNMP Traps on Server Rollover

To allow a Simple Network Management Protocol (SNMP) trap to be sent when a SIP proxy monitor rollover occurs, the **trap rollover** command must be enabled. By default, the SNMP traps are disabled for SIP proxy monitor rollover. To enable this trap, enter the following command:

(config-proxy-monitor)#**trap rollover**

SNMP traps must also be enabled globally. Refer to Configuring SNMP in AOS for more information.

Configure Grammar

SIP proxy monitor poll requests contain To, From, and Request-URI headers. By default, these headers do not include a user. To change the grammar from the default setting of **none** and specify a user to format the User field, use the following commands described below:

- **grammar from user** <*username*>

  Specifies the user used to format the User field of the From header. The following example sets the User field for the From header to **2565555229**:

  (config-proxy-monitor)#**grammar from user 2565555229**
- **grammar request-uri user** <*username*>

  Specifies the user used to format the User field of the Request-URI header. The following example sets the User field for the Request-URI header to **2565555229**:

  (config-proxy-monitor)#**grammar request-uri user 2565555229**
- **grammar to user** <*username*>

  Specifies the user used to format the User field of the To header. The following example sets the User field for the To header to **2565555229**:

  (config-proxy-monitor)#**grammar to user 2565555229**

Step 7: Configure SIP REGISTER Rate Adaption (Optional)

For hosted applications using the SIP proxy, a large load on the proxy can be the periodic REGISTER requests sent by each phone into the VoIP network. This load is magnified at the session border controller (SBC), which can be the target of all of the REGISTER requests from multiple sites. Although each phone's configuration can be adjusted to spread this load out over time, that is not always feasible. SIP proxy REGISTER rate adaption allows you to reduce the rate that SIP proxy users' REGISTER requests are forwarded by the unit to the SIP server.

When rate adaption is enabled, the unit modifies the Expires header to be a greater value in outbound REGISTER requests to the SIP server. In the corresponding responses from the SIP server, the unit modifies the Expires header to be a smaller value when forwarding the REGISTER response to the phone (defined by the **user-expires** <*value*> parameter). The ratio between these two values determines how many REGISTER requests (after the first) the unit forwards to the SIP server, and how many REGISTER requests the unit will handle locally. SIP proxy user REGISTER requests are forwarded by the unit if the time remaining in the REGISTER expiration period is less than or equal to the REGISTER expiration period received from the SIP server minus the defined threshold, minus the REGISTER expiration period given to the SIP proxy user. All other REGISTER requests from SIP proxy users are handled locally by the unit. Configure SIP proxy REGISTER rate adaption using the commands explained in this section.

Enable the Default SIP Proxy Register Rate Adaption

To enable SIP proxy REGISTER rate adaption with the default **server-expires** value of **3600** seconds, default **user-expires** value of **60** seconds, and a default threshold of **threshold percentage 50**, enter the following command from the Global Configuration mode prompt:

(config)#**sip proxy register rate-adaption**

Specify an Expiration Period

Use the **sip proxy register rate-adaption server-expires** <*value*> command to specify an expiration period (in seconds) requested from the SIP server in the REGISTER request. Valid range is **30** to **86400** seconds. By default, the server expiration period requested from the SIP server is **3600** seconds. Enter the command from the Global Configuration mode prompt as follows:

(config)#**sip proxy register rate-adaption server-expires 16000**

Specify an Absolute Threshold (Optional)

Use the **sip proxy register rate-adaption threshold absolute** <*value*> command to specify a fixed amount of time that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. Threshold values indicate the desired remaining headroom in the expires window set by the server. Setting a small-value threshold results in the unit forwarding REGISTER requests from the SIP proxy users at larger time intervals, and setting a large-value threshold value results in the unit forwarding REGISTER requests at smaller time intervals. For example, if 1) the Expires period from the SIP server is 3600 seconds, 2) the threshold is set to **threshold absolute 180**, and 3) the Expires period in the REGISTER response given to the user is 60 seconds, then the first REGISTER request from the SIP proxy user that occurs after 3360 seconds (3600 - 180 - 60) will be forwarded to the SIP server. The value of this parameter must be less than the value set by the **server-expires** <*value*> **parameter.** Valid range is **5** to **604800** seconds. Enter the command from the Global Configuration mode prompt as follows:

(config)#**sip proxy register rate-adaption threshold absolute 180**

Specify a Threshold Percentage (Optional)

Use the **sip proxy register rate-adaption threshold percentage** <*value*> command to specify a percentage of the REGISTER expiration period that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. Setting a small-value threshold results in the unit forwarding REGISTER requests from the SIP proxy users at larger time intervals, and setting a large-value threshold value results in the unit forwarding REGISTER requests at smaller time intervals.

For example, if 1) the Expires period from the SIP server is 3600 seconds, 2) the threshold is set to **threshold percentage 10**, and 3) the Expires period in the REGISTER response given to the user is 60 seconds, then the first REGISTER request from the SIP proxy user that occurs after 3180 seconds (3600 - 0.10(3600) - 60) will be forwarded to the SIP server. Valid range is **10** to **90** percent. By default, the rate adaption threshold is set to **threshold percentage 50**. Enter the command from the Global Configuration mode prompt as follows:

```
(config)#sip proxy register rate-adaption threshold percentage 10
```

Specify User Expiration Period (Optional)

Use the **sip proxy register rate-adaption user-expires** <*value*> command to specify the expiration period (in seconds) given to the SIP proxy user in the REGISTER response. For effective rate adaption, the **user-expires** value should be a small fraction of the **server-expires** value. Valid range is **30** to **86400** seconds. By default, the expiration period given to the SIP proxy user is **60** seconds. Enter the command from the Global Configuration mode prompt as follows:

```
(config)#sip proxy register rate-adaption user-expires 60
```

If rate-adaption is used with proxy monitor rollover, the first REGISTER received after a monitor failure will be sent to the next available server regardless of rate-adaption state. Once a registration is successful, the rate-adaption settings will become active.

Step 8: Configure the Media Gateway

The media gateway has to be configured to specify the IP address to use for outbound RTP traffic and SIP messaging. All interfaces that will receive or initiate SIP proxy signaling must have a media gateway configured on the interface.

Specify the Outbound Interface for RTP traffic and SIP Messaging

Enter the specific interface's configuration mode using the **interface** <*interface*> command. Use only IP interfaces for configuring the media gateway for RTP traffic and SIP messaging. Specify the interface in the format *interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id* >. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**. To configure an interface's media gateway, enter the command as follows:

```
(config)#interface ppp 1
```

Specify the IP Address (Optional)

Specify the IP address for the outbound interface for RTP traffic using the **ip address** <*ip address*> <*subnet mask*> command from the interface's configuration mode. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Subnet masks correspond to a range of IP addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). Enter the command as follows:

```
(config-ppp1)#ip address 10.200.1.157 255.255.255.252
```

> *The **ip address** command is only necessary if the interface does not already have an IP address assigned. If you have already assigned an IP address to this interface, you do not need to use the **ip address** command.*

Configure Media-Gateway

Configure the media gateway on the interface using the **media-gateway ip** [**loopback** <*interface id*> | **primary | secondary** <*ip address*>] command. The **loopback** <*interface id*> parameter specifies an IP address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IP address across multiple WAN interfaces for RTP traffic. Loopback interface identifiers must be unique and cannot be used by another loopback interface. The valid range for loopback interface identifiers is **1** to **1024**.

The **primary** keyword specifies that this interface's primary IP address is used for RTP traffic. This parameter applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses. The **secondary** <*ip address*> parameter specifies that this interface's statically defined secondary IP address is used for SIP and RTP traffic. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Enter the command from the interface's configuration mode as follows:

```
(config-ppp1)#media-gateway ip primary
```

Activate the Interface (Optional)

Activate the interface using the **no shutdown** command. Enter the command from the interface's configuration mode as follows:

```
(config-ppp1)#no shutdown
```

> *The **no shutdown** command is only necessary if the interface is currently shutdown. If you have already enabled the interface, you will not need to enter this command.*

Step 9: Additional Configuration Options

The following are optional configurable parameters for the SIP proxy feature.

- **sip proxy allowed-servers** <*hostname* | *ip address*>

  The **sip proxy allowed-servers** command restricts the allowed servers in transparent and outbound proxy modes. By default, SIP traffic to any server is allowed in transparent and outbound proxy modes. This means that if no server is specified, traffic to any server is permitted, but if this command is entered, only traffic to the configured servers is allowed. This command can be entered multiple times to allow traffic to multiple servers. Enter the command from the Global Configuration mode prompt to specify which servers are allowed:

  (config)#**sip proxy allowed-servers 10.200.1.9**

- **sip access-class ip** <*name*> **in**

  The **sip access-class ip** <*name*> **in** command restricts the traffic allowed to reach the SIP stack. By default, all incoming voice traffic is allowed to reach the SIP stack. The <*name*> parameter specifies a previously configured access control list (ACL). To restrict the traffic allowed to reach the SIP stack, enter the command from the Global Configuration mode as follows:

  (config)#**sip access-class ip Trusted in**

- **sip default-call-routing [proxy | reject | switchboard]**

  The **sip default-call-routing** command specifies the method used to route a call to the internal transaction distribution unit (TDU) if the destination of a call is ambiguous. The **proxy** keyword indicates the call is routed to the proxy server, the **switchboard** keyword indicates the call is routed to the internal switchboard, and the **reject** keyword indicates the call is rejected. By default, the call routing method is **proxy**. To change the call routing method, enter the command from the Global Configuration mode as follows:

  (config)#**sip default-call-routing switchboard**

  

  *The **sip default-call-routing** command is applicable to AOS voice products only. This command is not available on AOS data products.*

- **sip timer rollover** <*value*>

  The **sip timer rollover** command specifies the time period (in seconds) that the SIP proxy is set to wait for a response to a request before attempting to find an alternate destination (the next SIP server). By default, the rollover time period is **3** seconds. The time period range is **1** to **32** seconds. To change the default rollover time period, enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip timer rollover 5**

- **sip proxy transparent ip-spoofing**

  The **sip proxy transparent ip-spoofing** command allows you to replace the source IP address (the media gateway address of the interface the phone is behind) for SIP packets traveling towards a connected phone with the softswitch IP address when using the SIP proxy in transparent mode. When enabled, this feature replaces the media gateway IP address with that of the softswitch in SIP packets egressing the AOS device towards the connected phone. By default, this feature is disabled. Enter the command from the Global Configuration mode prompt as follows:

  (config)#**sip proxy transparent ip-spoofing**

SIP Proxy Configuration Examples

The following examples describe some of the common real-world applications of the SIP proxy. All configurations are provided through the CLI. The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide you with a method of copying and pasting configurations directly from this guide into the CLI. You should not copy these configurations without first making the necessary adjustments to ensure they will function properly in your network.

Example 1 - Stateful Proxy Mode

The following example details the commands needed to use the SIP proxy in stateful mode on an AOS device. In this mode, the phones will register to the AOS device and all SIP messages received by the AOS device from the phones will be directed to the softswitch (**198.51.100.1**) in the provider's network. Configure stateful proxy mode as follows:

```
!
ip firewall
!
interface ethernet 0/2
    ip address 192.168.1.1 255.255.255.0
    ip access-policy PRIVATE
    media-gateway ip primary
    no shutdown
!
interface t1 0/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
!
interface ppp 1
    ip address 192.0.2.2  255.255.255.252
    ip access-policy PUBLIC
    media-gateway ip primary
    no shutdown
    cross-connect 1 t1 1/1 1 ppp 1
!
ip access-list standard MATCH_ALL
    permit any
!
```



```
ip access-list extended SIP
     permit udp host 198.51.100.1 any eq 5060
!
!
ip policy-class PRIVATE
     allow list MATCH_ALL self
     allow list MATCH_ALL interface ppp 1 overload
!
ip policy-class PUBLIC
     allow-list SIP self
!
!
sip
sip proxy
sip proxy sip-server primary 198.51.100.1
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
sip proxy sip-server monitor
     no shutdown
```

Several relevant portions of the AOS firewall configuration were omitted from this example because they are beyond the scope of this document. For more information on firewall configuration, refer to the IPv4 Firewall Protection in AOS configuration guide.

Example 2 - Outbound Proxy Mode

The following example details the commands needed to use the SIP proxy in outbound proxy mode on an AOS device. In this mode, the phones register with an external softswitch and all SIP messages are sent to the AOS device by the phones. The AOS device then sends the SIP messages to the softswitch listed in the Request-URI of the SIP messages. Configure outbound proxy mode as follows:

```
!
interface ethernet 0/2
     ip address 192.168.1.1 255.255.255.0
     media-gateway ip primary
     no shutdown
!
interface t1 0/1
     tdm-group 1 timeslots 1-24 speed 64
     no shutdown
!
interface ppp 1
     ip address 172.16.1.1 255.255.255.252
     media-gateway ip primary
     no shutdown
     cross-connect 1 t1 1/1 1 ppp 1
!
```



```
sip
sip proxy
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
```

Example 3 - Transparent Proxy Mode on an AOS Voice Device

The following example details the commands needed to use the SIP proxy in transparent mode on an AOS voice device. In this mode, the phone registers with an external softswitch and all SIP messages are transparently intercepted and proxied to the Layer 3 IP address to which they were originally destined. Firewall is enabled and an ACL is created to allow SIP traffic through the firewall. Configure transparent proxy mode as follows:

```
!
ip firewall
!
interface ethernet 0/2
    ip address 192.168.2.1 255.255.255.0
    ip access-policy PRIVATE
    media-gateway ip primary
    no shutdown
!
interface t1 0/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
!
interface ppp 1
    ip address 192.0.2.2  255.255.255.252
    ip access-policy PUBLIC
    media-gateway ip primary
    no shutdown
    cross-connect 1 t1 1/1 1 ppp 1
!
ip access-list standard MATCH_ALL
    permit any
!
ip access-list extended SIP
    permit udp host 198.51.100.1 any eq 5060
!
ip policy-class PRIVATE
    allow list MATCH_ALL self
    nat source list MATCH_ALL interface ppp 1 overload
!
ip policy-class PUBLIC
    allow list SIP self
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
sip
```



```
sip proxy
sip proxy transparent
```

> **NOTE** *The **ip firewall** command is optional because the firewall is automatically enabled when the **sip proxy transparent** command is issued. The **sip** command is enabled by default on AOS voice devices.*

> **NOTE** *Several relevant pieces of the AOS firewall configuration were omitted from this example because they are beyond the scope of this document. For more information on firewall configuration, refer to the IPv4 Firewall Protection in AOS configuration guide.*

Example 4 - Transparent Proxy Mode on an AOS Data Device

The following example details the commands needed to enable transparent proxy mode on an AOS data device. In this mode, the phone registers with an external softswitch and all SIP messages are transparently intercepted and proxied to the Layer 3 IP address to which they were originally destined. Firewall is enabled and an ACL is created to allow SIP traffic through the firewall. Configure transparent proxy mode as follows:

```
ip firewall
no ip firewall alg sip
!
!
interface ethernet 0/1
    ip address 192.168.2.1 255.255.255.0
    ip access-policy PRIVATE
    media-gateway ip primary
    no shutdown
!
interface t1 1/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
!
interface ppp 1
    ip address 192.0.2.2  255.255.255.252
    ip access-policy PUBLIC
    media-gateway ip primary
    no shutdown
    cross-connect 1 t1 1/1 1 ppp 1
!
ip access-list standard MATCH_ALL
    permit any
!
ip access-list extended SIP
    permit udp host 198.51.100.1 any eq 5060
!
```



```
ip policy-class PRIVATE
    allow list MATCH_ALL self
    nat source list MATCH_ALL interface ppp 1 overload
!
ip policy-class PUBLIC
    allow list SIP self
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
sip
sip proxy
sip proxy transparent
```

*The **ip firewall** command is optional because the firewall is automatically enabled when the **sip proxy transparent** command is issued.*

Several relevant pieces of the AOS firewall configuration were omitted from this example because they are beyond the scope of this document. For more information on firewall configuration, refer to the IPv4 Firewall Protection in AOS configuration guide.

Example 5 - Configuring an AOS Data Product for Transparent Proxy Mode with Survivability

The following example details the commands needed to enable transparent proxy mode with survivability on an AOS data device. In this mode, the phone registers to an external softswitch and all SIP messages are transparently intercepted and proxied to the Layer 3 IP address to which they were originally destined. Firewall is enabled and an ACL is created to allow SIP traffic through the firewall. 911 calls in this example are always routed to the backup gateway (**192.168.2.254**). If the WAN connection fails, all external calls are routed to the backup gateway (**192.168.2.254**). Configure transparent proxy mode and survivability as follows:

```
!
ip firewall
no ip firewall alg sip
!
interface ethernet 0/1
    ip address 192.168.2.1 255.255.255.0
    ip access-policy PRIVATE
    media-gateway ip primary
    no shutdown
!
interface t1 1/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
!
interface ppp 1
```



```
      ip address 192.0.2.2  255.255.255.252
      ip access-policy PUBLIC
      media-gateway ip primary
      no shutdown
      cross-connect 1 t1 1/1 1 ppp 1
!
ip access-list standard MATCH_ALL
      permit any
!
ip access-list extended SIP
      permit udp host 198.51.100.1 any eq 5060
!
ip policy-class PRIVATE
      allow list MATCH_ALL self
      nat source list MATCH_ALL interface ppp 1 overload
!
ip policy-class PUBLIC
      allow list SIP self
!
sip
sip proxy
sip proxy transparent
sip proxy emergency-call-routing accept 911
sip proxy local-gateway 192.168.2.254
```

Several relevant pieces of the AOS firewall configuration were omitted from this example because they are beyond the scope of this document. For more information on firewall configuration, refer to the IPv4 Firewall Protection in AOS configuration guide.

Command Summary

The following table summarizes the commands necessary for the basic configuration of the SIP proxy feature in AOS.

Table 2. Configuration Command Summary

	Command	Explanation
Step 1	Enable the SIP stack, protocol(s), and port(s).	
	(config)#**sip**	Enables the AOS SIP stack. When the SIP stack is enabled, memory is allocated for SIP functionality. By default, the SIP stack is disabled on AOS data products and enabled on AOS voice products. If the optional protocol and port parameters are not specified, the SIP stack uses **udp** on port **5060**.
	(config)#**sip [tcp | udp] [**<*port*>**]**	Optional. Specifies the protocol and port on which the SIP stack is operating. By default, the SIP stack uses **udp**. If the command **sip [tcp | udp]** is entered with no port specifications, the port value will default to **5060**. Available ports range from **1** to **65535**.
Step 2	Enable the SIP proxy.	
	(config)#**sip proxy**	Enables stateful and outbound proxy modes of operation in both AOS data and voice products at the global level.
	(config)#**sip proxy transparent**	Enables transparent proxy mode operation in both AOS data and voice products. Used in conjunction with the **sip proxy** command.
	(config)#**no ip firewall alg sip**	Disables the firewall SIP ALG. This command must be entered before the **sip proxy transparent** command on AOS data products.
Step 3	Configure the softswitches.	
	(config)#**sip proxy sip-server [primary | secondary]** <*hostname* | *ip address*> **[tcp | udp] [**<*port*>**]**	Configures the primary and secondary softswitches. The <*hostname* | *ip address*> parameter indicates the FQDN or IP address of the primary or secondary softswitch. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). The **tcp** and **udp** keywords indicate the protocol used by the softswitch. The optional <*port*> parameter indicates the port used by the softswitch. Port range is **1** to **65535**. By default, the softswitch uses **udp** on port **5060**.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 4	Configure SIP proxy emergency call routing (Optional).	
	(config)#**sip proxy emergency-call-routing [local | proxy]**	Optional. Specifies how to route emergency calls during failover. The default is **local**. However, calls cannot be routed locally on AOS data products without a configured local SIP gateway.
	(config)#**sip proxy local-gateway** <*hostname* | *ip address*> **[tcp | udp]** [<*port*>]	Optional. Enables the necessary local SIP gateway in AOS data products. Emergency calls cannot be routed locally without a configured local gateway. The <*hostname*> is the name of the gateway. The <*ip address*> is the IP address of the gateway. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). The **tcp** and **udp** keywords indicate the protocol used by the gateway. The optional <*port*> parameter specifies the port used by the gateway. Available port range is **1** to **65535**. By default, the gateway uses **udp** on port **5060**.
	(config)#**sip proxy emergency-call-routing [accept** <*template*> **| reject** <*template*>]	Optional. Specifies which types of calls are accepted or rejected for emergency call routing. Multiple accept and reject templates may be entered. By default, no templates are configured and no calls are classified as emergency calls. For valid template characters, refer to *Step 4: Configure SIP Proxy Emergency Call Routing (Optional) on page 8*.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 5	Configure failover settings (Optional).	
	(config)#**sip proxy failover match-digits** <*number*>	Optional. Specifies the number of least-significant digits of the dial string to match in order to route a surviving call to proxy users during failover. Number range is **1** to **255**. By default, no number of digits is specified. This command can be entered multiple times.
	(config)#**sip proxy failover match-alias** <*pattern*> **substitute** <*pattern*>	Optional. Configures an alias for matching a dial string to route a surviving call to proxy users during failover. Both the **match-alias** <*pattern*> and **substitute** <*pattern*> variables can be defined using traditional matching templates or regular expressions. By default, no match-alias substitution is specified.
	(config)#**sip proxy failover group match-value** <*pattern*> **new-value** <*pattern*>	Optional. Enables forking of calls to users registered with unique extensions in failover mode. Both the **match-value** <*pattern*> and **new-value** <*pattern*> variables can be defined using traditional matching templates or regular expressions. By default, no failover group patterns are defined.C
	(config)#**sip proxy failover codec-group** <*name*>	Optional. Specifies the preconfigured CODEC list to use during failover. By default, no CODEC list is configured or applied. This command is available on AOS voice products only.
	(config)#**sip proxy failover dial-string source [request-uri | to]**	Optional. Specifies the dial string source to use during failover. The **request-uri** keyword specifies the Request-URI user field as the dial string source. The **to** keyword specifies the TO header field as the dial string source. By default, the dial string source is **request-uri**.
	(config)#**sip proxy failover sip-keep-alive [info** <*value*> **| options** <*value*>**]**	Optional. Specifies the method of SIP keepalive to use during failover. The <*value*> parameter specifies the amount of time (in seconds) between the SIP keepalive messages sent during a call. Time range is **30** to **3600** seconds. By default, no keepalive method is specified.
	(config)#**sip proxy failover trust-domain [p-asserted-identity-required]**	Optional. Enables the AOS unit to send P-Asserted-Identity to the softswitch when in failover mode. The **p-asserted-identity-required** parameter is only for use with nonstandard softswitches and should not be used in normal configurations. By default, this setting is not enabled.
	(config)#**sip proxy failover accept-registrations**	Optional. Enables the SIP proxy server to accept new registrations when in failover mode.
	(config)#**sip proxy failover direct-inbound**	Optional. Enables direct inbound routing of calls to proxy users during failover. This feature is used when a network configuration does not require a SIP trunk.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 5 Cont'd	(config)#**sip proxy failover register-expires** <*value*>	Optional. Specifies the length of time SIP phone registrations remain in the SIP proxy database while the SIP proxy is in failover. Time range is **30** to **86400** seconds. The default <*value*> is **300** seconds.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 6	Configure SIP proxy monitor (Optional).	
	(config)#**sip proxy sip-server monitor [stateful-transparent | stateful-only]**	Optional. Specifies whether the SIP proxy monitor is enabled for both stateful and transparent proxy (**stateful-transparent**) or stateful only (**stateful-only**). By default, the proxy monitor is set to **stateful-only**.
	(config)#**sip proxy sip-server monitor**	Optional. Enable the SIP proxy monitor, and enter the SIP Proxy Monitor Configuration mode. By default, this feature is disabled.
	(config-proxy-monitor)#**mode [continuous [interval** <*value*>**] | on-failure]**	Optional. Specifies the polling behavior of the proxy monitor. Specify **continuous** to proactively poll the configured SIP servers regardless of their state, or **on-failure** which only polls the servers when a failed state is detected. The default setting is **mode on-failure**. If specifying **continuous**, the optional **interval** <*value*> can be used to indicate the polling interval. The valid range for <*value*> is **1** to **600** seconds. The default interval is **30** seconds.
	(config-proxy-monitor)#**poll timeout** <*value*>	Optional. Specifies the number of seconds the SIP proxy monitor may wait for a response when issuing a poll request to a configured SIP server before it determines the poll request was unsuccessful. Valid range for <*value*> is **1** to **600** seconds. The default is **32** seconds.
	(config-proxy-monitor)#**recover no-response interval [**<*value*> | <*min*> <*max*>**]**	Optional. Specifies when there is no response from the SIP server, the proxy monitor will poll the SIP server at the interval specified as <*value*>. The interval can also be configured as an increasing interval which starts at the <*min*> value and doubles with each interval to the <*max*> value. Valid range for <*value*>, <*min*>, and <*max*> is **1** to **86400** seconds. The default setting is **recover no-response interval 5 60**.
	(config-proxy-monitor)#**recover responses** <*value*> **interval** <*value*>	Optional. Specifies the number of successful responses necessary to recover service to the SIP server and the interval at which the polls are sent. Valid range for **responses** <*value*> is **1** to **255**. Valid range for **interval** <*value*> is **1** to **86400** seconds. The default setting is **recover responses 3 interval 10**.
	(config-proxy-monitor)#**trap rollover**	Optional. Allow an SNMP trap to be sent when a SIP proxy monitor rollover occurs. Use the **no** form of this command to disable the trap. By default, this trap is disabled.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 6 Cont'd	(config-proxy-monitor)#**grammar from user [**<*username*> | **none]**	Optional. Specifies the user used to format the User field of the From header. Using the **none** keyword indicates that no user is present. Default value is **none**.
	(config-proxy-monitor)#**grammar request-uri user [**<*username*> | **none]**	Optional. Specifies the user used to format the User field of the Request-URI header. Using the **none** keyword indicates that no user is present. Default value is **none**.
	(config-proxy-monitor)#**grammar to user [**<*username*> | **none]**	Optional. Specifies the user used to format the User field of the To header. Using the **none** keyword indicates that no user is present. Default value is **none**.
Step 7	Configure SIP REGISTER rate adaption (Optional).	
	(config)#**sip proxy register rate-adaption**	Enables SIP proxy REGISTER rate adaption with the default **server-expires** value of **3600** seconds, default **user-expires** value of **60** seconds, and a default threshold of **threshold percentage 50**.
	(config)#**sip proxy register rate-adaption server-expires** <*value*>	Specifies the expiration period requested from the SIP server in the REGISTER request. Valid range is **30** to **86400** seconds.
	(config)#**sip proxy register rate-adaption threshold absolute** <*value*>	Specifies a fixed amount of time that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. The value of this parameter must be less than the value set by the **server-expires** <*value*> parameter. Valid range is **5** to **604800** seconds.
	(config)#**sip proxy register rate-adaption threshold percentage** <*value*>	Specifies a percentage of the REGISTER expiration period that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. Valid range is **10** to **90** percent.
	(config)#**sip proxy register rate-adaption user-expires** <*value*>	Specifies the expiration period (in seconds) given to the SIP proxy user in the REGISTER response. Valid range is **30** to **86400** seconds.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 8	Configure the media gateway.	
	(config)#**interface** <*interface*>	Specifies an interface used for SIP and RTP traffic. Specify the interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* >. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**.
	(config)#**ip address** <*ip address*> <*subnet mask*>	Specifies the IP address for the outbound interface for RTP traffic. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Subnet masks can be expressed in decimal dotted notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). This command is needed only if the interface does not already have an IP address assigned.
	(config-<*interface*>)#**media-gateway ip [loopback** <*interface id*> **| primary | secondary** <*ip address*>**]**	Associates the IP address source to use for RTP traffic. Loopback interface identifier range is **1** to **1024**. The **primary** keyword indicates the interface's primary IP address is used for SIP and RTP traffic. The **secondary** keyword indicates using the interface's secondary IP address for SIP and RTP traffic. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
	(config-<*interface*>)#**no shutdown**	Activates the interface. By default, the interface is not active. This command is needed only if the interface has not already been enabled.

Table 2. Configuration Command Summary *(Continued)*

	Command	Explanation
Step 9	Additional configuration options.	
	(config)#**sip proxy allowed-servers** <*hostname* | *ip address*>	Optional. Specifies a server to which devices behind the proxy are allowed to send SIP traffic. This command can be entered multiple times to allow a list of servers. IP addresses should be specified in dotted decimal notation (for example, **10.10.10.1**). By default, traffic from any server is allowed.
	(config)#**sip access-class ip** <*name*> **in**	Optional. Applies a preconfigured ACL to the incoming connections and limits the traffic allowed to reach the SIP stack. By default, no ACL is configured or applied, and all traffic reaches the SIP stack.
	(config)#**sip default-call-routing [proxy | reject | switchboard]**	Optional. Specifies the method used to route a call to the internal TDU if the destination of a call is ambiguous. The **proxy** keyword indicates the call is routed to a proxy server. The **switchboard** keyword indicates the call is routed to an internal switchboard. The **reject** keyword indicates the call is rejected. By default, the routing method is **proxy**. This command is available on AOS voice products only.
	(config)#**sip timer rollover** <*value*>	Optional. Specifies the time period (in seconds) that the SIP proxy is set to wait for a response to a request before attempting to find an alternate destination. The <*value*> range is **1** to **32** seconds. By default, the rollover time period is **3** seconds.
	(config)#**sip transparent proxy ip-spoofing**	Optional. Specifies that the source IP address of SIP packets traveling towards a connected phone is replaced by the IP address of the softswitch. By default, this feature is disabled.

Troubleshooting

After configuring the SIP proxy feature, several different commands can be issued from the Enable mode prompt in the CLI to assist in troubleshooting. The recommended method for troubleshooting the SIP proxy is to run the following debug commands simultaneously: **debug sip stack messages**, **debug sip proxy routing**, and **debug sip proxy database**. It is important to keep in mind that these debug messages provide the most benefit when run together rather than when run individually. *Table 3* describes these commands, as well as other available debug options.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Table 3. SIP Proxy Troubleshooting Commands

Command	Explanation
debug sip proxy database	Displays SIP proxy user database events.
debug sip proxy routing	Displays SIP proxy message routing events, as well as general errors or other failure information.
debug sip proxy register rate-adaption	Displays SIP proxy REGISTER rate adaption debug messages.
debug sip stack messages	Displays SIP stack messaging events.
debug sip proxy dialogs	Displays debugging information related to SIP dialog objects. A dialog object is created to track SIP dialogs whose messages traverse the proxy. This debug command can be useful in specific circumstances, but is not necessary for most normal debugging situations.
debug sip proxy transactions	Displays information about the interactions between the SIP proxy and the SIP stack. This debug command can be useful in specific circumstances, but is not necessary for most normal debugging situations.
debug sip proxy verbose	Displays all SIP proxy debug message events. This debug command displays an extensive amount of information, and should not be run unless specifically requested.
show sip proxy monitor	Displays the current status of the SIP proxy monitor.

Table 3. SIP Proxy Troubleshooting Commands *(Continued)*

Command	Explanation
show sip proxy registration [range <*range*> **| user** <*user*>**] [extended | realtime | verbose]**	Displays the SIP proxy registration status for SIP proxy users. A range of users can be displayed using the **range** <*range*> parameter, and a single user can be displayed using the **user** <*user*> parameter.
show sip proxy resources	Displays a list of SIP proxy resources since the last system reload. When the SIP proxy forwards a SIP message, one or more SIP resources are temporarily allocated for the operation.
show sip proxy user [extended | realtime | verbose]	Displays a list of SIP proxy users, the outbound server, when the registration was created, and when it will expire.
test template match <*string*> **to** <*pattern*> **[substitute-using** <*pattern*>**]**	Evaluates dial numbers and regular expressions for template matching and substitution.

Debug Command Sample Output

The following is sample output from the recommended transparent proxy debug procedure, using the **debug sip stack messages**, **debug sip proxy database**, and **debug sip proxy routing** commands simultaneously. This output records the events from call inception to termination.

The output below is not presented exactly as it will appear on your terminal session. Due to their extensive length, some lines in the following example are wrapped to fit within the margins of this document.

>**enable**
#**debug sip stack messages**
#**debug sip proxy database**
#**debug sip proxy routing**

```
12:09:50 SIP.STACK MSG     Rx: UDP src=10.19.209.66:5060 dst=0.0.0.0:5060
12:09:50 SIP.STACK MSG         INVITE SIP:9030@bw2.pq.adtran.com;user=phone SIP/2.0
12:09:50 SIP.STACK MSG         Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG         From: "TA 924e IP 501"
    <SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG         To: <SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG         CSeq: 1 INVITE
12:09:50 SIP.STACK MSG         Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG         Contact: <SIP:9034@10.19.209.66>
12:09:50 SIP.STACK MSG         Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE,
    SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER
12:09:50 SIP.STACK MSG         User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:09:50 SIP.STACK MSG         Supported: 100rel,replaces
12:09:50 SIP.STACK MSG         Allow-Events: talk,hold,conference
12:09:50 SIP.STACK MSG         Max-Forwards: 70
12:09:50 SIP.STACK MSG         Content-Type: application/sdp
12:09:50 SIP.STACK MSG         Content-Length: 213
12:09:50 SIP.STACK MSG
12:09:50 SIP.STACK MSG         v=0
12:09:50 SIP.STACK MSG         o=- 1241629785 1241629785 IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG         s=Polycom IP Phone
12:09:50 SIP.STACK MSG         c=IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG         t=0 0
12:09:50 SIP.STACK MSG         m=audio 2222 RTP/AVP 18 0 101
12:09:50 SIP.STACK MSG         a=rtpmap:18 G729/8000
12:09:50 SIP.STACK MSG         a=rtpmap:0 PCMU/8000
12:09:50 SIP.STACK MSG         a=rtpmap:101 telephone-event/8000
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY DB PUD entry lookup: contact = original contact
12:09:50 SIP.PROXY ROUTING Transc 0x2b5f2c0: SIP Request Method = INVITE.
12:09:50 SIP.PROXY ROUTING Using ALG Info to forward transparent outbound INVITE to 10.1.4.5:5060
```

```
    via UDP.
12:09:50 SIP.PROXY ROUTING Found SDP in Request.
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.239:5060 dst=10.1.4.5:5060
12:09:50 SIP.STACK MSG        INVITE SIP:9030@bw2.pq.adtran.com;user=phone SIP/2.0
12:09:50 SIP.STACK MSG        From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG        To: <SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG        Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG        CSeq: 1 INVITE
12:09:50 SIP.STACK MSG        Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG        Contact: <SIP:9034-adtnpxyid-1i31gd5h-153id9k@10.19.209.66>
12:09:50 SIP.STACK MSG        Allow:
    INVITE,ACK,BYE,CANCEL,OPTIONS,INFO,MESSAGE,SUBSCRIBE,NOTIFY,PRACK,
    UPDATE,REFER
12:09:50 SIP.STACK MSG        User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:09:50 SIP.STACK MSG        Supported: 100rel
12:09:50 SIP.STACK MSG        Supported: replaces
12:09:50 SIP.STACK MSG        Max-Forwards: 70
12:09:50 SIP.STACK MSG        Allow-Events: talk,hold,conference
12:09:50 SIP.STACK MSG        Content-Type: application/SDP
12:09:50 SIP.STACK MSG        Content-Length: 213
12:09:50 SIP.STACK MSG
12:09:50 SIP.STACK MSG        v=0
12:09:50 SIP.STACK MSG        o=- 1241629785 1241629785 IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG        s=Polycom IP Phone
12:09:50 SIP.STACK MSG        c=IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG        t=0 0
12:09:50 SIP.STACK MSG        m=audio 2222 RTP/AVP 18 0 101
12:09:50 SIP.STACK MSG        a=rtpmap:18 G729/8000
12:09:50 SIP.STACK MSG        a=rtpmap:0 PCMU/8000
12:09:50 SIP.STACK MSG        a=rtpmap:101 telephone-event/8000
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b5a9b8: Request forwarded.
12:09:50 SIP.STACK MSG    Rx: UDP src=10.1.4.5:33175 dst=10.19.209.239:5060
12:09:50 SIP.STACK MSG        SIP/2.0 401 Unauthorized
12:09:50 SIP.STACK MSG        Via:SIP/2.0/UDP
    10.19.209.66;received=10.19.209.239;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG        From:"TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG
    To:<SIP:9030@bw2.pq.adtran.com;user=phone>;tag=157480839-1241629790354
12:09:50 SIP.STACK MSG        Call-ID:7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG        CSeq:1 INVITE
12:09:50 SIP.STACK MSG        WWW-Authenticate:DIGEST
    qop="auth",nonce="BroadWorksXfueabhqqT5u2rpiBW", algorithm=MD5,
    realm="bw2.pq.adtran.com"12:09:50 SIP.STACK MSGContent-Length:0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b5a9b8: SIP Response Code = 401 to INVITE.
12:09:50 SIP.PROXY ROUTING Sending ACK for received final response to INVITE.
```

```
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.239:5060 dst=10.1.4.5:5060
12:09:50 SIP.STACK MSG        ACK SIP:9030@bw2.pq.adtran.com;user=phone SIP/2.0
12:09:50 SIP.STACK MSG        From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG        To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=157480839-1241629790354
12:09:50 SIP.STACK MSG        Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG        CSeq: 1 ACK
12:09:50 SIP.STACK MSG        Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG        Content-Length: 0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Using server transaction to forward 401 to 10.19.209.66:5060 via UDP.
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.65:5060 dst=10.19.209.66:5060
12:09:50 SIP.STACK MSG        SIP/2.0 401 Unauthorized
12:09:50 SIP.STACK MSG        From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG        To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=157480839-1241629790354
12:09:50 SIP.STACK MSG        Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG        CSeq: 1 INVITE
12:09:50 SIP.STACK MSG        Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG        WWW-Authenticate: Digest realm="bw2.pq.adtran.com",
    nonce="BroadWorksXfueabhqqT5u2rpiBW", algorithm=MD5,qop="auth"
12:09:50 SIP.STACK MSG        Content-Length: 0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b5f2c0: Response forwarded.
12:09:50 SIP.PROXY ROUTING Call Failed.
12:09:50 SIP.STACK MSG    Rx: UDP src=10.19.209.66:5060 dst=0.0.0.0:5060
12:09:50 SIP.STACK MSG        ACK SIP:9030@bw2.pq.adtran.com SIP/2.0
12:09:50 SIP.STACK MSG        Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK4dfb7d644C780971
12:09:50 SIP.STACK MSG        From: "TA 924e IP 501"
    <SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG        To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=157480839-1241629790354
12:09:50 SIP.STACK MSG        CSeq: 1 ACK
12:09:50 SIP.STACK MSG        Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG        Contact: <SIP:9034@10.19.209.66>
12:09:50 SIP.STACK MSG        Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE,
    SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER
12:09:50 SIP.STACK MSG        User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:09:50 SIP.STACK MSG        Max-Forwards: 70
12:09:50 SIP.STACK MSG        Content-Length: 0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY DB PUD entry lookup (associated): from user = contact user
12:09:50 SIP.PROXY ROUTING Transc 0x2b5f2c0: SIP Request Method = ACK.
12:09:50 SIP.PROXY ROUTING No need to proxy ACK.
12:09:50 SIP.STACK MSG    Rx: UDP src=10.19.209.66:5060 dst=0.0.0.0:5060
12:09:50 SIP.STACK MSG        INVITE SIP:9030@bw2.pq.adtran.com;user=phone SIP/2.0
12:09:50 SIP.STACK MSG        Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK30fa103f32D9DBCC
```

```
12:09:50 SIP.STACK MSG      From: "TA 924e IP 501"
    <SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG      To: <SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG      CSeq: 2 INVITE
12:09:50 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      Contact: <SIP:9034@10.19.209.66>
12:09:50 SIP.STACK MSG      Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE,
    SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER
12:09:50 SIP.STACK MSG      User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:09:50 SIP.STACK MSG      Supported: 100rel,replaces
12:09:50 SIP.STACK MSG      Allow-Events: talk,hold,conference
12:09:50 SIP.STACK MSG      Authorization: Digest username="9034", realm="bw2.pq.adtran.com",
    nonce="BroadWorksXfueabhqqT5u2rpiBW", qop=auth, cnonce="wnoHppBUW9iCSkz",
    nc=00000001,uri="SIP:9030@bw2.pq.adtran.com; user=phone",
    response="84714de0322a3e946b10d9d899bc9dfa", algorithm=MD5
12:09:50 SIP.STACK MSG      Max-Forwards: 70
12:09:50 SIP.STACK MSG      Content-Type: application/sdp
12:09:50 SIP.STACK MSG      Content-Length: 213
12:09:50 SIP.STACK MSG
12:09:50 SIP.STACK MSG      v=0
12:09:50 SIP.STACK MSG      o=- 1241629785 1241629785 IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG      s=Polycom IP Phone
12:09:50 SIP.STACK MSG      c=IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG      t=0 0
12:09:50 SIP.STACK MSG      m=audio 2222 RTP/AVP 18 0 101
12:09:50 SIP.STACK MSG      a=rtpmap:18 G729/8000
12:09:50 SIP.STACK MSG      a=rtpmap:0 PCMU/8000
12:09:50 SIP.STACK MSG      a=rtpmap:101 telephone-event/8000
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY DB PUD entry lookup: contact = original contact
12:09:50 SIP.PROXY ROUTING Transc 0x2b59b78: SIP Request Method = INVITE.
12:09:50 SIP.PROXY ROUTING Using ALG Info to forward transparent outbound INVITE to 10.1.4.5:5060
    via UDP.
12:09:50 SIP.PROXY ROUTING Found SDP in Request.
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.239:5060 dst=10.1.4.5:5060
12:09:50 SIP.STACK MSG      INVITE SIP:9030@bw2.pq.adtran.com;user=phone SIP/2.0
12:09:50 SIP.STACK MSG      From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG      To: <SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      CSeq: 2 INVITE
12:09:50 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK30fa103f32D9DBCC
12:09:50 SIP.STACK MSG      Contact: <SIP:9034-adtnpxyid-1i31gd5h-153id9k@10.19.209.66>
12:09:50 SIP.STACK MSG      Allow:
    INVITE,ACK,BYE,CANCEL,OPTIONS,INFO,MESSAGE,SUBSCRIBE,NOTIFY,PRACK,
    UPDATE,REFER
12:09:50 SIP.STACK MSG      User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:09:50 SIP.STACK MSG      Supported: 100rel
12:09:50 SIP.STACK MSG      Supported: replaces
```

```
12:09:50 SIP.STACK MSG      Max-Forwards: 70
12:09:50 SIP.STACK MSG      Allow-Events: talk,hold,conference
12:09:50 SIP.STACK MSG      Authorization: Digest username="9034",realm="bw2.pq.adtran.com",
    nonce="BroadWorksXfueabhqqT5u2rpiBW",uri="SIP:9030@bw2.pq.adtran.com;user=phone",
    response="84714de0322a3e946b10d9d899bc9dfa",algorithm=MD5,cnonce="wnoHppBUW9iCSkz",q
    op=auth,nc=00000001
12:09:50 SIP.STACK MSG      Content-Type: application/SDP
12:09:50 SIP.STACK MSG      Content-Length: 213
12:09:50 SIP.STACK MSG
12:09:50 SIP.STACK MSG      v=0
12:09:50 SIP.STACK MSG      o=- 1241629785 1241629785 IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG      s=Polycom IP Phone
12:09:50 SIP.STACK MSG      c=IN IP4 10.19.209.66
12:09:50 SIP.STACK MSG      t=0 0
12:09:50 SIP.STACK MSG      m=audio 2222 RTP/AVP 18 0 101
12:09:50 SIP.STACK MSG      a=rtpmap:18 G729/8000
12:09:50 SIP.STACK MSG      a=rtpmap:0 PCMU/8000
12:09:50 SIP.STACK MSG      a=rtpmap:101 telephone-event/8000
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b55ee8: Request forwarded.
12:09:50 SIP.STACK MSG    Rx: UDP src=10.1.4.5:33175 dst=10.19.209.239:5060
12:09:50 SIP.STACK MSG      SIP/2.0 100 Trying
12:09:50 SIP.STACK MSG      Via:SIP/2.0/UDP
    10.19.209.66;received=10.19.209.239;branch=z9hG4bK30fa103f32D9DBCC
12:09:50 SIP.STACK MSG      From:"TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG      To:<SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG      Call-ID:7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      CSeq:2 INVITE
12:09:50 SIP.STACK MSG      Content-Length:0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b55ee8: SIP Response Code = 100 to INVITE.
12:09:50 SIP.PROXY ROUTING Using server transaction to forward 100 to 10.19.209.66:5060 via UDP.
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.65:5060 dst=10.19.209.66:5060
12:09:50 SIP.STACK MSG      SIP/2.0 100 Trying
12:09:50 SIP.STACK MSG      From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG      To: <SIP:9030@bw2.pq.adtran.com;user=phone>
12:09:50 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      CSeq: 2 INVITE
12:09:50 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK30fa103f32D9DBCC
12:09:50 SIP.STACK MSG      Content-Length: 0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b59b78: Response forwarded.
12:09:50 SIP.STACK MSG    Rx: UDP src=10.1.4.5:33175 dst=10.19.209.239:5060
12:09:50 SIP.STACK MSG      SIP/2.0 180 Ringing
12:09:50 SIP.STACK MSG      Via:SIP/2.0/UDP
    10.19.209.66;received=10.19.209.239;branch=z9hG4bK30fa103f32D9DBCC
12:09:50 SIP.STACK MSG      From:"TA 924e IP
```

```
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG
    To:<SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:09:50 SIP.STACK MSG      Call-ID:7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      CSeq:2 INVITE
12:09:50 SIP.STACK MSG      Supported:
12:09:50 SIP.STACK MSG      Contact:<SIP:10.1.4.5:5060>
12:09:50 SIP.STACK MSG      Remote-Party-ID:"IP
    712"<SIP:9030@10.1.4.5;user=phone>;screen=yes;party=called;privacy=off; id-type=subscriber
12:09:50 SIP.STACK MSG      Call-Info:<SIP:10.1.4.5>;appearance-index=1
12:09:50 SIP.STACK MSG
    Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
12:09:50 SIP.STACK MSG      Content-Length:0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b55ee8: SIP Response Code = 180 to INVITE.
12:09:50 SIP.PROXY ROUTING Using server transaction to forward 180 to 10.19.209.66:5060 via UDP.
12:09:50 SIP.STACK MSG    Tx: UDP src=10.19.209.65:5060 dst=10.19.209.66:5060
12:09:50 SIP.STACK MSG      SIP/2.0 180 Ringing
12:09:50 SIP.STACK MSG      From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:09:50 SIP.STACK MSG      To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:09:50 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:09:50 SIP.STACK MSG      CSeq: 2 INVITE
12:09:50 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK30fa103f32D9DBCC
12:09:50 SIP.STACK MSG      Supported:
12:09:50 SIP.STACK MSG      Remote-Party-ID: "IP
    712"<SIP:9030@10.1.4.5;user=phone>;screen=yes;party=called;privacy=off;id-type=subscriber
12:09:50 SIP.STACK MSG      Call-Info: <SIP:10.1.4.5>;appearance-index=1
12:09:50 SIP.STACK MSG      Contact: <SIP:10.1.4.5:5060>
12:09:50 SIP.STACK MSG      Allow:
    ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
12:09:50 SIP.STACK MSG      Content-Length: 0
12:09:50 SIP.STACK MSG
12:09:50 SIP.PROXY ROUTING Transc 0x2b59b78: Response forwarded.
12:10:00 SIP.STACK MSG    Rx: UDP src=10.1.4.5:33175 dst=10.19.209.239:5060
12:10:00 SIP.STACK MSG      SIP/2.0 200 OK
12:10:00 SIP.STACK MSG      Via:SIP/2.0/UDP
    10.19.209.66;received=10.19.209.239;branch=z9hG4bK30fa103f32D9DBCC
12:10:00 SIP.STACK MSG      From:"TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:10:00 SIP.STACK MSG
    To:<SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:10:00 SIP.STACK MSG      Call-ID:7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:10:00 SIP.STACK MSG      CSeq:2 INVITE
12:10:00 SIP.STACK MSG      Supported:
12:10:00 SIP.STACK MSG      Contact:<SIP:10.1.4.5:5060>
12:10:00 SIP.STACK MSG      Remote-Party-ID:"IP
    712"<SIP:9030@10.1.4.5;user=phone>;screen=yes;party=called;privacy=off ;id-type=subscriber
```

```
12:10:00 SIP.STACK MSG      Call-Info:<SIP:10.1.4.5>;appearance-index=1
12:10:00 SIP.STACK MSG
    Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
12:10:00 SIP.STACK MSG      Accept:multipart/mixed,application/media_control+xml,application/sdp
12:10:00 SIP.STACK MSG      Content-Type:application/sdp
12:10:00 SIP.STACK MSG      Content-Length:236
12:10:00 SIP.STACK MSG
12:10:00 SIP.STACK MSG      v=0
12:10:00 SIP.STACK MSG      o=BroadWorks 202498 1 IN IP4 10.19.209.55
12:10:00 SIP.STACK MSG      s=-
12:10:00 SIP.STACK MSG      c=IN IP4 10.19.209.55
12:10:00 SIP.STACK MSG      t=0 0
12:10:00 SIP.STACK MSG      m=audio 3004 RTP/AVP 0 101
12:10:00 SIP.STACK MSG      a=rtpmap:0 PCMU/8000
12:10:00 SIP.STACK MSG      a=rtpmap:101 telephone-event/8000
12:10:00 SIP.STACK MSG      a=fmtp:101 0-15
12:10:00 SIP.STACK MSG      a=ptime:20
12:10:00 SIP.STACK MSG      a=sendrecv
12:10:00 SIP.STACK MSG      a=silenceSupp:off - - - -
12:10:00 SIP.STACK MSG
12:10:00 SIP.PROXY ROUTING Transc 0x2b55ee8: SIP Response Code = 200 to INVITE.
12:10:00 SIP.PROXY DB PUD entry lookup failed.
12:10:00 SIP.PROXY ROUTING WARNING Unable to find PUD entry on 2xx response to INVITE.
12:10:00 SIP.PROXY ROUTING Using server transaction to forward 200 to 10.19.209.66:5060 via UDP.
12:10:00 SIP.PROXY ROUTING Checking for internal Media Gateway IP Address
12:10:00 SIP.PROXY ROUTING Given RTP Channel is null, checking for hairpinned RTP Channel
12:10:00 SIP.PROXY ROUTING Unable to find hairpinned RTP Channel
12:10:00 SIP.PROXY ROUTING RTP Channel is NULL, Media Gateway must not be involved in call
12:10:00 SIP.PROXY ROUTING Checking need for firewall traversal
12:10:00 SIP.PROXY ROUTING Testing firewall policies
12:10:00 SIP.PROXY ROUTING NAT not required, no need for firewall traversal here
12:10:00 SIP.PROXY ROUTING Found SDP in Response.
12:10:00 SIP.PROXY ROUTING Inserting new CCMID entry _pxyCCM_7bb0b9fe-914b8898-f95acf0b
    [0x4].
12:10:00 SIP.PROXY ROUTING Connecting SDP through firewall.
12:10:00 SIP.PROXY ROUTING firewallConnectCall: Testing firewall policies
12:10:00 SIP.PROXY ROUTING Call matches VQM user, access list, or sampling criteria.
12:10:00 SIP.STACK MSG    Tx: UDP src=10.19.209.65:5060 dst=10.19.209.66:5060
12:10:00 SIP.STACK MSG      SIP/2.0 200 OK
12:10:00 SIP.STACK MSG      From: "TA 924e IP
    501"<SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:10:00 SIP.STACK MSG      To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:10:00 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:10:00 SIP.STACK MSG      CSeq: 2 INVITE
12:10:00 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK30fa103f32D9DBCC
12:10:00 SIP.STACK MSG      Supported:
12:10:00 SIP.STACK MSG      Remote-Party-ID: "IP712"<SIP:9030@10.1.4.5;user=phone>
    screen=yes;party=called;privacy=off; id-type=subscriber
```

```
12:10:00 SIP.STACK MSG      Call-Info: <SIP:10.1.4.5>;appearance-index=1
12:10:00 SIP.STACK MSG      Accept: multipart/mixed,application/media_control+xml,application/sdp
12:10:00 SIP.STACK MSG      Contact: <SIP:10.1.4.5:5060>
12:10:00 SIP.STACK MSG      Allow:
    ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
12:10:00 SIP.STACK MSG      Content-Type: application/SDP
12:10:00 SIP.STACK MSG      Content-Length: 236
12:10:00 SIP.STACK MSG
12:10:00 SIP.STACK MSG      v=0
12:10:00 SIP.STACK MSG      o=BroadWorks 202498 1 IN IP4 10.19.209.55
12:10:00 SIP.STACK MSG      s=-
12:10:00 SIP.STACK MSG      c=IN IP4 10.19.209.55
12:10:00 SIP.STACK MSG      t=0 0
12:10:00 SIP.STACK MSG      m=audio 3004 RTP/AVP 0 101
12:10:00 SIP.STACK MSG      a=rtpmap:0 PCMU/8000
12:10:00 SIP.STACK MSG      a=rtpmap:101 telephone-event/8000
12:10:00 SIP.STACK MSG      a=fmtp:101 0-15
12:10:00 SIP.STACK MSG      a=ptime:20
12:10:00 SIP.STACK MSG      a=sendrecv
12:10:00 SIP.STACK MSG      a=silenceSupp:off - - - -
12:10:00 SIP.STACK MSG
12:10:00 SIP.PROXY ROUTING Transc 0x2b59b78: Response forwarded.
12:10:00 SIP.STACK MSG    Rx: UDP src=10.19.209.66:5060 dst=0.0.0.0:5060
12:10:00 SIP.STACK MSG      ACK SIP:10.1.4.5:5060 SIP/2.0
12:10:00 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK83f67700477F390D
12:10:00 SIP.STACK MSG      From: "TA 924e IP 501"
    <SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:10:00 SIP.STACK MSG      To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:10:00 SIP.STACK MSG      CSeq: 2 ACK
12:10:00 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
12:10:00 SIP.STACK MSG      Contact: <SIP:9034@10.19.209.66>
12:10:00 SIP.STACK MSG      Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, INFO, MESSAGE,
    SUBSCRIBE, NOTIFY, PRACK, UPDATE, REFER
12:10:00 SIP.STACK MSG      User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:10:00 SIP.STACK MSG      Max-Forwards: 70
12:10:00 SIP.STACK MSG      Content-Length: 0
12:10:00 SIP.STACK MSG
12:10:00 SIP.PROXY DB PUD entry lookup (associated): from user = contact user
12:10:00 SIP.PROXY ROUTING OOC Msg 0x3388890: Proxy Request Method = ACK.
12:10:00 SIP.PROXY ROUTING Using ALG Info to forward transparent outbound ACK to 10.1.4.5:5060
    via UDP.
12:10:00 SIP.STACK MSG    Tx: UDP src=10.19.209.239:5060 dst=10.1.4.5:5060
12:10:00 SIP.STACK MSG      ACK SIP:10.1.4.5:5060 SIP/2.0
12:10:00 SIP.STACK MSG      From: "TA 924e IP
    <SIP:9034@bw2.pq.adtran.com>;tag=85F5E932-8D7826A5
12:10:00 SIP.STACK MSG      To:
    <SIP:9030@bw2.pq.adtran.com;user=phone>;tag=1924834008-1241629790780
12:10:00 SIP.STACK MSG      Call-ID: 7bb0b9fe-914b8898-f95acf0b@10.19.209.66
```

```
12:10:00 SIP.STACK MSG      CSeq: 2 ACK
12:10:00 SIP.STACK MSG      Via: SIP/2.0/UDP 10.19.209.66;branch=z9hG4bK83f67700477F390D
12:10:00 SIP.STACK MSG      Contact: <SIP:9034-adtnpxyid-1i31gd5h-153id9k@10.19.209.66>
12:10:00 SIP.STACK MSG      Allow:
    INVITE,ACK,BYE,CANCEL,OPTIONS,INFO,MESSAGE,SUBSCRIBE,NOTIFY,PRACK,
    UPDATE,REFER
12:10:00 SIP.STACK MSG      User-Agent: PolycomSoundPointIP-SPIP_501-UA/2.2.2.0084
12:10:00 SIP.STACK MSG      Max-Forwards: 70
12:10:00 SIP.STACK MSG      Content-Length: 0
12:10:00 SIP.STACK MSG
12:10:00 SIP.PROXY ROUTING Trx 0x2aff760, OOC Msg 0x3388890: Request forwarded.
```

Show Command Sample Output

show sip proxy user [extended | realtime | verbose]

This command shows the contents of the SIP proxy user database. The SIP proxy user database maintains information about SIP endpoints whose messages have traversed the proxy. Using the **extended** or **verbose** keywords displays more detailed output. Using the **realtime** keyword displays full-screen output in real time.

> NOTE *Using the **realtime** argument for this command can adversely affect the performance of your unit.*

#**show sip proxy user extended**

```
User          Outbound Server      Flg      Created           Expires
-------------------------------------------------------------------------------------------------------------
9034          bw2.pq.adtran.com    -RT      May 6  11:30:11  May 6  12:30:25
  IP 10.19.209.66    OIP 10.19.209.66   Key 153id9k  From 9034
```

User Displays SIP user field that was present in the REGISTER request that created this entry.

Outbound Server Displays the server to which the request was directed.

Flg Displays status flags in three fields, starting from left:

First Field

- `-` Indicates the last known proxied REGISTER request succeeded.
- `U` Indicates the last attempt to proxy a REGISTER request failed because the outbound server was unreachable.

Second Field

- `-` Indicates the endpoint has initiated a REGISTER request, but no 2xx final response has been received.
- `R` Indicates the endpoint has successfully registered through the proxy.

Third Field

- `T` Indicates the endpoint is operating in transparent proxy mode.

	O Indicates the endpoint is operating in outbound proxy mode. S Indicates the endpoint is operating in stateful proxy mode.
Created	Displays the date and time when the entry was created.
Expires	Displays the date and time when the entry will automatically expire.
IP	Displays the IP address of the endpoint.
OIP	Displays the offered IP address of the interface used to proxy the request.
Key	Displays the internal SIP messaging key used for endpoint identification.
From	Displays the source of the entry.

The following is sample output from the **show sip proxy monitor** command:

#**show sip proxy monitor**

```
Proxy Server Monitor:              Admin UP
Polling mode:                      On failure
Recovery no-response interval:     5 - 60
Recovery responses needed:         3  Interval 10

Servers:
Address                                  Port        Status      Poll
---------------------------------------  ----------  ----------  --------------------
10.255.3.2                               5060        DOWN        Next poll 12 seconds
10.17.233.254                            5060        UP*
10.17.1.254                              5060        UP
```

Additional Troubleshooting Commands

test template match <*string*> **to** <*pattern*> **[substitute-using** <*pattern*>**]**

This command evaluates matching number patterns. Once the command is entered from the Global Configuration mode prompt, a response is provided indicating if the match was successful. If the **substitute-using** parameter is entered, AOS responds with the resulting substitute.

The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or **?***. Using either of these characters outside of quotation marks is interpreted by the CLI as commands and not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

The following is a sample response using the **test template match** command with traditional number matching:

#**test template match “5551234” to “555XXXX”**

Match Result -> Match

The following is a sample response using the **test template match** command with regular expression matching:

#**test template match “5551234” to “/555\d{4}/”**

Match Result -> Match

The following is a sample response using the **test template match** <*string*> **to** <*pattern*> **substitute-using** <*pattern*> command with traditional number matching:

#**test template match “5551234” to “555XXXX” substitute-using “1359555XXXX”**

Substitute Result -> 13595551234

The following is a sample response using the **test template match** <*string*> **to** <*pattern*> **substitute-using** <*pattern*> command with regular expression matching:

#**test template match “5552121DE” to “/(\d+).*/” substitute-using “/\1/”**

Substitute Result -> 5552121

AOS is compatible with PCRE. More information on understanding and using regular expressions is available at http://www.pcre.org.

Additional Resources

There are additional resources available to aid in configuring your AOS device. The documents listed below are available online on ADTRAN’s Support Forum at https://supportforums.adtran.com.

- *AOS Command Reference Guide*
- *Configuring SNMP in AOS*
- *IPv4 Firewall Protection in AOS*
- *SIP Signaling and Media Security in AOS*