6AOSCG0033-29B
September 2012

ADTRAN

Configuration Guide

Configuring Remote Phones with an AOS SIP Gateway

This configuration guide outlines the steps necessary to operate a remote phone outside an ADTRAN Operating System (AOS) device serving as a Session Initiation Protocol (SIP) gateway. The guide includes an overview of the remote phone function in a network with SIP providers, outlines the steps necessary to configure the AOS device to receive and route calls to the remote phone using the command line interface (CLI), and troubleshooting information.

This guide consists of the following sections:

Remote Phone Overview

Prior to release of AOS R10.1.0, supporting a remote phone at the customer location required the remote phone to be installed behind a SIP aware firewall or virtual private network (VPN) device for service. While this solution was successful in some applications, it was not an ideal situation for every customer. With the release of AOS R10.1.0, the remote phone can now be located behind a non-SIP aware firewall.

Each remote phone is associated with a voice user configured on an ADTRAN session border controller (SBC) serving as the SIP gateway for an IP private branch exchange (PBX). Remote user support for the SIP gateway includes two key items: synchronized registering and source IP address and port routing.

First, synchronized registering means that a SIP endpoint registers to the SIP gateway and then registers to the PBX. If synchronized registering is enabled, the registration to the PBX will be initiated only when the remote endpoint is registered. The PBX needs to know when the remote endpoint is registered, so the SIP gateway's registration to the PBX must be dependent on the remote phone. The SIP gateway cannot proxy registration messages, because gateway registrar expire times will likely be significantly less than the expire times used by the PBX. When registration is not synchronized and one or more SIP identities are configured for a voice user, the system registers to the PBX whether the remote endpoint is registered or not.

Secondly, source IP address and port routing is necessary because the remote endpoint may not be located behind a SIP aware router. Typically, the system will use the IP address and port number specified in the Contact header of SIP packets to determine how to route them. However, this will not work if a remote phone is not located behind a SIP aware firewall. Rather than using the Contact IP address and port number, the back-to-back user agent (B2BUA) must send SIP messages to the Layer 3 source IP address and port number. For RTP packets, the B2BUA must anchor the media and relay packets to the Layer 3 source IP address and port number rather than using the IP address and port specified in the Session Description Protocol (SDP). When the system receives a SIP message for a voice user configured for source IP address and port routing, the system sends all subsequent SIP messages to the Layer 3 IP address and port number from which the request was received.

There is additional information available online at ADTRAN's Support Forum, https://supportforums.adtran.com. Specific resources are listed in *Additional Resources on page 13*.

Hardware and Software Requirements and Limitations

The remote phone feature is available on AOS products as outlined in the *AOS Feature Matrix*, available online at ADTRAN's Support Forum, https://supportforums.adtran.com.

Remote phones using this feature must use User Datagram Protocol (UDP) for SIP messaging.

Configuring Remote Phone Using the CLI

To configure the remote phone feature using the CLI on an AOS product, use the following steps:

1. Enable the SIP registrar and SIP call authentication.
2. Specify the default and maximum expiration periods.
3. Configure a SIP user for each remote phone.
4. Configure SABR.

5. Prefer Trunk Routing on the SIP provider trunk
6. Configure the firewall settings.

Accessing the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1.

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

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

> *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the prompt as follows:

   >enable

5. If configured, enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

   #configure terminal
   (config)#

Step 1: Enable the SIP Registrar and SIP Call Authentication

The SIP registrar server must first be configured for registering user agents (UAs) into the location database. Using the **ip sip registrar** command from the Global Configuration mode, this command enables SIP registrar on a global basis for all UDP calls.

To enable the SIP registrar, enter the command as follows from the Global Configuration mode:

(config)**#ip sip registrar**
(config)#

SIP call authentication should also be enabled to provide enhanced security. To enable SIP call authentication, enter the command as follows from the Global Configuration mode:

(config)**#ip sip authenticate**
(config)#

Step 2: Specify the Default and Maximum Expiration Period

During registration, the UA attempts to register for a specified amount of time. If the UA does not re-register before the expiration time, the registration expires. The default expiration is used if the UA does not specify an expiration period when making the request. It is important to ensure that the expire time used by the SIP gateway is less than the firewall timeout for UDP traffic on the firewall in front of the remote phones. Use the **ip sip registrar default-expires** <*value*> command to specify the default SIP registrar expiration period and the **ip sip registrar max-expires** <*value*> command to specify the SIP registrar maximum expiration period. The valid range for <*value*> is **0** to **2592000** seconds.

To specify the default and maximum expiration period, enter the commands as follows from the Global Configuration mode:

(config)**#ip sip registrar default-expires 55**
(config)**#ip sip registrar max-expires 55**

Step 3: Configure a SIP User for Each Remote Phone

Voice user accounts are used to define phone users that are registered to the SIP gateway. Each remote phone must have a corresponding SIP user account. The commands in this step describe how to configure voice features for each user account. Repeat them for each remote phone you are configuring for your SIP gateway.

1. Begin by creating a SIP user and assigning an extension. This step creates the user account and enters the Voice User Account Configuration mode. To create a user, enter the **voice user** <*extension*> command from the Global Configuration mode:

   (config)**#voice user 5555**
   (config-5555)#

2. Specify that the voice user is a SIP user. Enter the **connect sip** command from the Voice User Account command mode:

   (config-5555)**#connect sip**

3. Specify that AOS use the synchronized registration method using the **no sip-register send-unsynced** command. Enter this command from the Voice User Account Configuration mode:

   (config-5555)**#no sip-register send-unsynced**

4. Configure the SIP registration options for the user using the **sip-identity** <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*> command. This command links the remote user to the PBX by specifying the station and SIP trunk. The <*station*> parameter specifies the station to be used for SIP trunk (for example, station extension). The <*Txx*> parameter specifies the SIP trunk through which to register the server. The trunk ID is specified in the format *Txx* where **xx** is the 2-digit identifier. Enter a trunk ID between **1** and **99**. Specify a user name and password for authentication by using the **auth-name** <*username*> and **password** <*password*> parameters.

   To specify the SIP registration options, enter the following command from the Voice User Account Configuration mode:

   (config-5555)**#sip-identity 5555 T11 register auth-name 5555 password 1234**

5. Use the **sip-authentication password** command to configure the SIP authentication password for the user. AOS supports passwords containing up to 16 alphanumeric characters. ADTRAN recommends a

strong password to increase user account security. Do not use typical or easy to guess passwords, such as **1234** or **abcd**. Enter this command from the Voice User Account Configuration mode:

(config-5555)**#sip-authentication password fRiaxoecrOus9lup**

6. The final step in creating a SIP user is to configure the user as a remote phone. Enter the **remote-phone** command from the Voice User Account Configuration mode:

   (config-5555)**#remote-phone**

The following is a complete example for configuring a SIP user, repeat for each user:

```
(config)#voice user 5555
(config-5555)#connect sip
(config-5555)#no sip-register send-unsynced
(config-5555)#sip-identity 5555 T11 register auth-name “5555” password “1234”
(config-5555)#sip authentication password “fRiaxoecrOus9lup”
(config-5555)#remote-phone
```

Step 4: Configure SABR

Source and automatic number identification (ANI) Based Routing (SABR) is a feature that can restrict the access of certain trunks (sources) and certain users (ANI) to a configured trunk group. You will configure SABR to force calls from remote phones to first route through the PBX instead of directly out the SIP trunk to the service provider. More detailed information about using SABR in AOS products is provided in the configuration guide *Source and ANI Based Routing in AOS Voice Products* available online at ADTRAN’s Support Forum, https://supportforums.adtran.com. Use the following steps to configure SABR.

1. Create a trunk list. Trunk lists are created by using the **voice trunk-list** <*name*> command. These lists are used to specify trunks that will be permitted or denied access on specified voice trunk groups. Use the **no** form of this command to remove the trunk list. To create a trunk list and enter the trunk list configuration mode, enter the **voice trunk-list** command as follows:

   ```
   (config)#voice trunk-list PBX
   (config-trunk-list-PBX)#
   ```

   To add a trunk to the trunk list, use the **trunk** <*Txx*> command in the trunk list configuration mode. The trunk ID is specified in the format Txx where **xx** is the 2-digit identifier. Enter a trunk ID between **1** and **99**. Use the **no** form of this command to remove the specified trunk from the trunk list.

   In the following example, **T11** is the SIP trunk to the PBX. Enter the command as follows:

   ```
   (config-trunk-list-PBX)#trunk T11
   (config-trunk-list-PBX)#
   ```


Although there are no limits on the number of trunks allowed in a trunk list or the number of ANI allowed in an ANI list, the more items that are added to a list, the more the runtime performance of call routing will be affected.

Once the necessary trunk and ANI lists have been created, enter **exit** at the trunk or ANI list configuration mode prompt to return to the Global Configuration mode. The trunk or ANI lists can now be applied to the desired voice trunk group.

2. Configure the trunk group. The next step is to configure the service provider trunk group using the **voice grouped-trunk** command from the Global Configuration mode prompt. This command enters the trunk group's configuration mode. The following example enters the trunk group configuration mode on trunk group **PSTN**:

   (config)**#voice grouped-trunk PSTN**
   (config-PSTN)#

3. Apply the trunk list to a the trunk group. Each trunk list must be applied to a configured voice trunk group for the permit or deny action to take effect. A list is applied using the **permit list** and **deny list** commands from the trunk group configuration mode. Once the grouped trunk configuration mode is accessed, enter the **permit** or **deny** commands as necessary. The **list** keyword adds the trunk list to the trunk group's permit or deny policy. To add the example trunk list (**PBX)** to the voice trunk group's permit policy, enter the command as follows:

   (config-PSTN)**#permit list PBX**
   (config-PSTN)#

Although there are no limits on the number of lists applied to voice trunk groups, it is important to remember that the more lists that are applied to a trunk group, the more the runtime performance of call routing will be affected.

*The permit/deny lists are evaluated in the order they appear in the trunk group's configuration. When any permit/deny lists are applied to the trunk group, there is an implicit **deny all** added after the explicitly defined lists.*

Step 5: Prefer Trunk Routing on the SIP Provider Trunk

Configure the unit to prefer trunk routing on the SIP service provider trunk using the **prefer trunk-routing** command. This prevents having calls from the SIP service provider trunk route directly to the voice users. To prefer trunk routing on the SIP service provider trunk (**T01**), enter the following commands:

(config)**#voice trunk T01**
(config-T01)**#prefer trunk-routing**

Step 6: Configure Firewall Permissions

Some modification to the firewall settings are also necessary to ensure that the remote phones operate properly. Therefore, in the most common scenario it is necessary to configure the firewall to allow UDP SIP traffic into the public interface using the **permit udp any any eq** <*port*> command issued from within the applicable IPv4 access control list (ACL) configuration mode. The valid range for <*port*> is **0** to **65535**.

Additional configuration settings are required to fully configure the firewall and depend upon the particular needs of each customer. For additional information on firewall configuration, refer to the AOS Command Reference Guide and Configuring IPv4 Firewall in AOS, both available online at ADTRAN's Support Forum, https://supportforums.adtran.com.

For enhanced security on AOS R10.3.0 and later, use a non-standard port for SIP traffic for remote phones. To enable SIP on a non-standard port use the **ip sip udp** <*port*> command.

In the following example, SIP on UDP port 25069 is enabled:

(config)**#ip sip udp 25069**

In the following example, an extended IPv4 ACL named **REMOTE_PHONES** is configured to allow any UDP traffic that is destined for port **25069**:

(config)**#ip access-list extended REMOTE_PHONES**
(config-ext-nacl)**#remark "Remote Phone Traffic"**
(config-ext-nacl)**#permit udp any any eq 25069**

Configuration Example

The following example enables an ADTRAN SBC to receive SIP registrations from remote phones. It sets the default and maximum expiration times to allow enough time to register without timing out. Two SIP users are created, one for extension **5555** and one for extension **5777**. Both SIP users have remote phone mode enabled and require authentication to register with the SIP gateway, as well as require an authentication password to authenticate with the PBX.

In order to force the remote phone's calls to always go to the PBX, SABR is configured on the ADTRAN SBC. A voice trunk list is created and associated with a voice trunk. Two voice trunk groups are configured and each is associated with a separate voice trunk. The voice trunk list is then applied to a trunk group's permit policy.

The **eth 0/1** interface is connected to the public Internet and uses the IPv4 address of **192.0.2.2**. The firewall is configured with IPv4 ACLs to allow UDP SIP traffic.

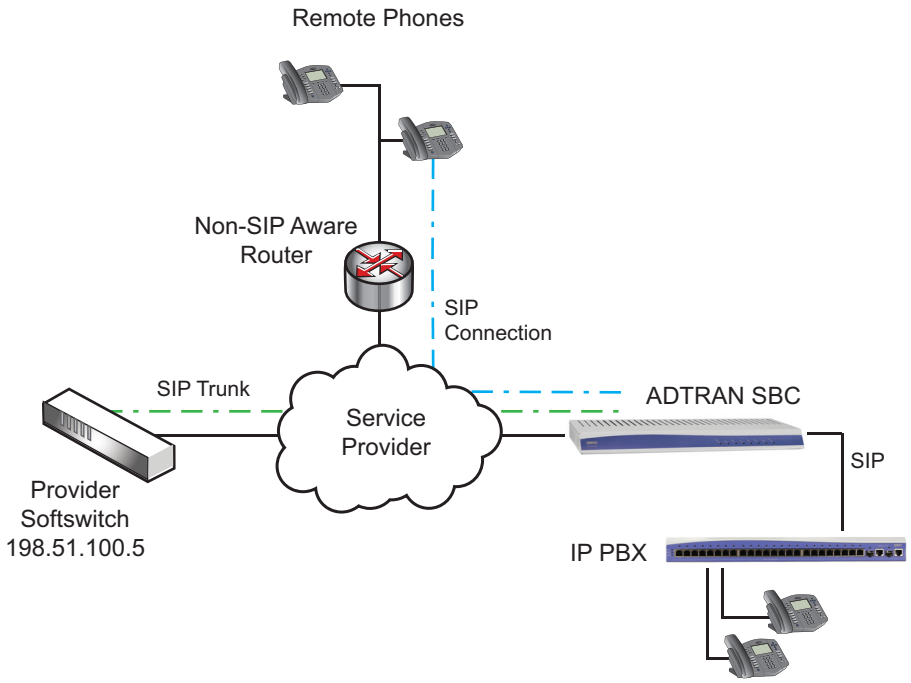

Figure 1. Remote Phones Example with AOS SIP Gateway

The configuration parameters entered in this example are sample configurations only, and only pertain to the configuration of remote phones. This application should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration example to provide a method of copying and pasting directly from this configuration guide into the CLI. This configuration should not be copied without first making the necessary adjustments to ensure it will function properly in your network.

```
!
ip sip udp 25069
!
ip sip authenticate
!
ip sip registrar
ip sip registrar default-expires 55
ip sip registrar max-expires 55
!
voice user 5555
   connect sip
   no sip-register send-unsynced
   sip-identity 5555 T11 register auth-name “5555” password “1234”
   sip authentication password “fRiaxoecrOus9Iup”
   remote-phone
!
voice user 5777
  connect sip
```



```
  no sip-register send-unsynced
  sip-identity 5777 T11 register auth-name "5777" password "4567"
  sip-authentication password "BIUT5iuSiejoaTHo"
  remote-phone
!
voice trunk-list PBX
   trunk T11
!
voice trunk T01 type sip
   description “SIP Provider”
   prefer trunk-routing
!
voice trunk T11 type sip
   description "PBX"
!
voice grouped-trunk PSTN
   trunk T01
   permit list PBX
!
voice grouped-trunk PBX
   trunk T11
!
ip access-list extended ADMIN
  remark “Admin Access”
  permit tcp any  any eq https
  permit tcp any  any eq ssh
!
ip access-list standard MATCH_ALL
  remark “All Traffic”
  permit any
!
ip access-list extended REMOTE_PHONES
  remark “Remote Phone Traffic”
  permit udp any any eq 25069
!
ip access-list extended SIP
  remark “SIP Traffic”
  permit udp host 198.51.100.5 any eq 5060
!
ip policy-class PRIVATE
  allow list MATCH_ALL self
  nat source list MATCH_ALL interface eth 0/1 overload
!
ip policy-class PUBLIC
  allow list SIP self
  allow list REMOTE_PHONES self
  allow list ADMIN self
```


Configuration Command Summary

The following table summarizes the commands used to configure remote phone in AOS products.

Step	Command	Description
Step 1	Enable the SIP registrar and SIP authentication.	
	(config)**#ip sip registrar**	Enables the SIP registrar server.
	(config)**#ip sip authenticate**	Enables SIP call authentication.
Step 2	Specify the default and maximum expire times.	
	(config)**#ip sip registrar default-expires** <*value*>	Specifies the valid range for <*value*> is **0** to **2592000** seconds.
	(config)**#ip sip registrar max-expires** <*value*>	Specifies the valid range for <*value*> is **0** to **2592000** seconds.
Step 3	Configure a SIP user for each remote phone.	
	(config)**#voice user** <*extension*>	Creates a voice user by assigning an extension and enters the voice user account configuration mode.
	(config-extension)**#connect sip**	Specifies that voice user is a SIP user account.
	(config-extension)**#no sip-register send-unsynced**	Specifies the use of the synchronized registration method.
	(config-extension)**#sip-identity** <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>	Configures the SIP registration options for the user. The <*station*> parameter specifies the station to be used for SIP trunk. The <*Txx*> parameter specifies a 2-digit identifier in the format Txx where **xx** is the trunk ID number. Enter a trunk ID between **1** and **99**. The **register** keyword registers the user to the server. The <*username*> parameter specifies the authentication name to use for registration to the SIP server. The <*password*> parameter specifies the authentication password required for registration to the SIP server.
	(config-extension)**#sip authentication password** <*password*>	Specifies the SIP authentication password for the user. The <*password*> parameter specifies the password that will be required as authentication for the phone to register to the SBC.
	(config-extension)**#remote-phone**	Configures the user as a remote phone.

Step	Command	Description
Step 4	Configure SABR.	
	(config)#**voice trunk-list** <*name*>	Creates a trunk list and enters the voice trunk list configuration mode. The **no** form of this command removes the trunk list.
	(config-trunk-list-name)#**trunk** <*Txx*>	Adds a trunk to the trunk list. The <*Txx*> parameter specifies a 2-digit identifier in the format Txx where **xx** is the trunk ID number. Enter a trunk ID between **1** and **99**.
	(config)#**voice grouped-trunk** <*name*>	Creates a trunk group and enters the voice trunk group configuration mode.
	(config-grouped-trunk-name)#**permit list** <*name*>	Adds a trunk or ANI list to the trunk group's permit policy.
Step 5	Prefer trunk routing on the SIP provider trunk.	
	(config)#**voice trunk T01** (config-T01)#**prefer trunk-routing**	Configures the unit to prefer trunk routing on the SIP provider trunk to prevent having calls route directly to the voice users.
Step 6	Configure firewall permissions to allow UDP SIP traffic into the public interface.	
	(config)#**ip sip udp** <*port*>	Enables SIP on a non-standard UDP port.
	(config)#**ip access-list extended** <*name*>	Creates an extended IPv4 ACL and enters the Extended IPv4 ACL configuration mode.
	(config-ext-nacl)#**remark** <*"remark"*>	Associates a descriptive tag with an IPv4 ACL. Tags can be up to 80 alphanumeric characters enclosed in quotation marks.
	(config-ext-nacl)#**permit udp any any eq** <*port*>	Permits UDP packets originating from any IP address, with any destination IPv4 address and a port equal to the **eq** <*port*>. The **any** keyword matches any IP address. The <*port*> parameter specifies the port number. Range is **0** to **65535**.

Troubleshooting

The following **show** commands can be used to display and troubleshoot specific portions of the configuration. These commands are all entered from the Enable mode.

The **show run voice trunk-list [**<*name*> **| verbose]** command displays trunk list information. The optional <*name*> parameter specifies which trunk list information is displayed, and the optional **verbose** keyword indicates all information for trunk lists is displayed. The following is sample output from the **show run voice trunk-list** command:

```
#show run voice trunk-list PBX
Building configuration...
!
!
voice trunk-list PBX
  trunk T11
!
end
```

The **show run voice grouped-trunk** [<*name*> | **verbose**] command displays trunk group information. The optional <*name*> parameter specifies which trunk group information is displayed, and the optional **verbose** keyword indicates all information for trunk groups is displayed. The following is sample output from this command:

```
#show run voice grouped-trunk
Building configuration...
!
!
voice grouped-trunk PSTN
  trunk T01
  accept N11
  accept NXX-XXX-XXXX
  accept 1-NXX-XXX-XXXX
  accept 011-$
  permit list PBX
!
voice grouped-trunk PBX
  trunk T11
!
end
```

The **show run voice user** [<*number*> | **verbose**] command displays voice user information. The optional <*number*> parameter specifies which voice user information is displayed, and the optional **verbose** keyword indicates all information for voice users is displayed. The following is sample output from this command:

```
#show run voice user
Building configuration...
!
```



```
!
voice user 5555
   connect sip
   no sip-register send-unsynced
   sip-identity 5555 T11 register auth-name "5555" password "1234"
   sip authentication password "fRiaxoecrOus9Iup"
   remote-phone
!
voice user 5777
   connect sip
   no sip-register send-unsynced
   sip-identity 5777 T11 register auth-name "5777" password "1234"
   sip-authentication password "BIUT5iuSiejoaTHo"
   remote-phone
!
end
```

Additional Resources

There are additional resources available to aid in configuring your ADTRAN unit. Many of the topics discussed in this guide are complex and may require additional study, such as configuring SABR and the IPv4 firewall. The documents listed below are available online at ADTRAN's Support Forum at https://supportforums.adtran.com.

- *Configuring Media Anchoring in AOS*
- *Source and ANI Based Routing in AOS Voice Products*
- *Configuring the Firewall IPv4 in AOS*