61200796L1-29.4E
July 2011

Configuration Guide

Configuring SIP Trunking and Networking for the NetVanta 7000 Series

This configuration guide describes the configuration and implementation of Session Initiation Protocol (SIP) trunking and networking in the ADTRAN Operating System (AOS) NetVanta 7000 Series products. Included in this guide is an overview of SIP trunking and networking, configuration considerations, configuration instructions using both the Web-based graphical user interface (GUI) and the command line interface (CLI), and sample SIP trunking and networking configurations.

This guide consists of the following sections:

SIP Trunking and Networking Overview

SIP technologies are used in today's communication networks to facilitate communication between endpoints in the network, whether they are local to the main enterprise site, or functioning at a remote location. SIP services provide more cost effective and scalable solutions for enterprise communication needs than traditional telephony services, and provide these services through SIP trunking and SIP networking. To fully understand the logic behind SIP trunking, it is useful to understand the traditional role of the trunk, and how SIP technologies have replaced traditional telephony for business communication.

Traditionally, telephony services were provided over a wire, also called a *trunk*, that connected the corporate private branch exchange (PBX), with the public switched telephone network (PSTN). These physical trunks provided multiple communication channels for phone service between the corporation and the telephone network. However, traditional telephony trunks become cumbersome and problematic as companies grow and their communication needs expand. Each time the company needs to add more telephone lines, they must purchase additional bundles of physical lines (T1 or E1), or additional equipment (BRI, PRIs, or PSTN gateways). SIP, on the other hand, provides a new method for providing telephony services that does not rely on additional physical trunks.

SIP trunks are virtual trunks that replace the traditional PSTN trunks of the past. These new trunks use SIP to set up communications between endpoints in the company network; whether those endpoints are all in the same building, at a neighboring location, or around the world. SIP trunking is a packet-based voice service that routes calls over an IP network to an IP-compatible PBX or voice switch using SIP signaling to place and receive calls. These calls can include all types of communication, including instant messaging, presence applications, and application sharing. SIP provides an immediate cost savings because there is no longer a need to purchase additional equipment or communication lines, and it also allows for optimal bandwidth usage as both data and voice traffic are passed in the same connection.

SIP trunks require three main parts to function: a PBX with SIP, an enterprise edge device that understands SIP, and IP phones with a SIP trunking service provider. The NetVanta 7000 Series product functions as a SIP-enabled PBX, and provides a method for creating the SIP trunks necessary to facilitate communication between multiple users and locations.

While SIP trunks provide the actual connection between enterprise sites, SIP networking is the configuration of SIP trunks between those enterprise sites. Typical SIP networking scenarios include connections between two NetVanta 7000 Series units, a NetVanta 7000 Series unit and an IP business gateway (such as a NetVanta 6355 or Total Access 900(e) Series), and a NetVanta 7000 Series unit and a NetVanta router (such as a NetVanta 3120 or NetVanta 3400 Series). *Figure 1 on page 3* illustrates SIP networking between NetVanta 7000 Series units and the SIP trunks used by each product.

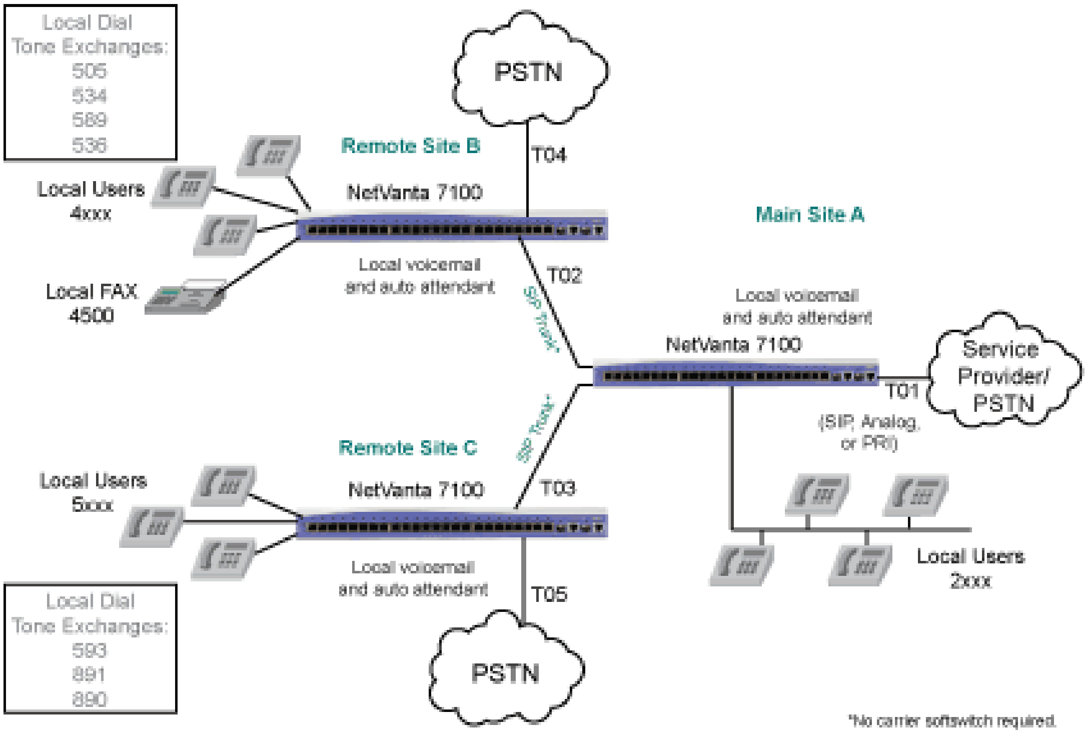


Figure 1. SIP Networking and SIP Trunks with Two NetVanta 7000 Series Products

SIP Trunking and Networking Configuration Overview

When configuring SIP trunking and networking for enterprise communications, there are generally two main areas of configuration that are necessary. The first is the configuration of the SIP trunk from an Internet service provider (ISP) to the NetVanta 7000 Series unit, and the second is the configuration of the SIP trunks between AOS products that provide the SIP networking. The following section outlines briefly the steps involved in each of these configurations.

Service Provider SIP Trunks

Service provider SIP trunks are trunks that are incoming to the NetVanta 7000 Series unit from the ISP. These trunks provide a method of receiving voice traffic through an Internet connection between the NetVanta 7000 Series and the ISP, thus removing the need for a local connection between the PSTN and the NetVanta platform. In this scenario, a gateway resides on the ISP's premises to connect to the PSTN, and the enterprise site (location of the NetVanta 7000 Series unit) uses an IP connection for voice traffic. *Figure 2 on page 4* describes the basic network topology for ISP SIP trunks.

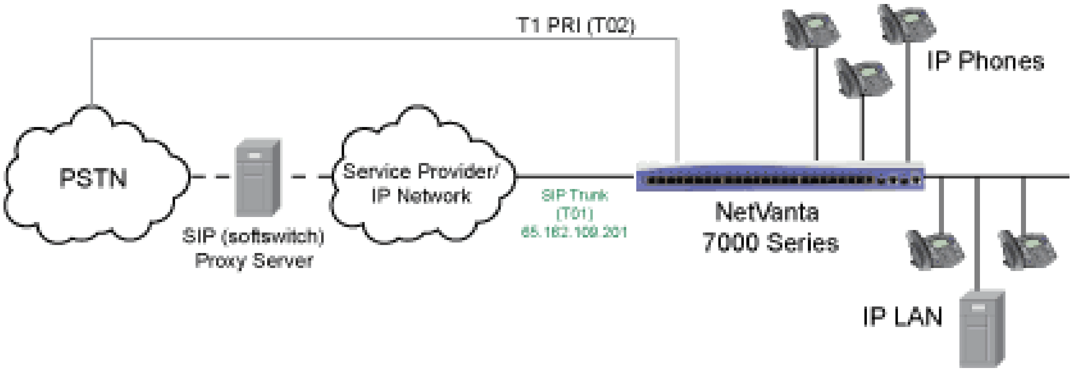

T1 PRI (T02)
IP Phones
PSTN
Service Provider/ IP Network
SIP Trunk (T01) 65.162.109.201
SIP (softswitch) Proxy Server
NetVanta 7000 Series
IP LAN

Figure 2. Service Provider SIP Trunk Network Topology

There are a few considerations you should keep in mind when configuring how your NetVanta 7000 Series product handles the service provider SIP trunk. You must consider Internet security, quality of service (QoS) parameters, failover scenarios, and SIP functionality. When you configure the service provider SIP trunk on the NetVanta platform, you will need to specify the SIP server settings, the SIP settings on the local platform, the registration of the SIP trunk or SIP identity, the automatic number identification (ANI) substitution settings, the trunk group configuration, and any SIP diversion configuration. These features, and their configuration, are discussed in more detail in *Configuring the Service Provider SIP Trunk on page 10*.

SIP Networking between NetVanta 7000 Series Products

SIP networking between NetVanta 7000 Series products generally occurs when multiple 7000 Series units are used at multiple enterprise sites. SIP trunks are configured between the NetVanta 7000 Series unit at the main site, and the NetVanta 7000 Series units at any remote office locations. *Figure 3 on page 5* illustrates a typical setup for SIP networking between NetVanta 7000 Series units. It is important to remember that in this configuration, only 10 SIP trunks can be configured per NetVanta 7000 Series unit, and that all voice features (such as auto attendant, voicemail, status groups, system directories, and paging groups) are local to each NetVanta 7000 Series unit.

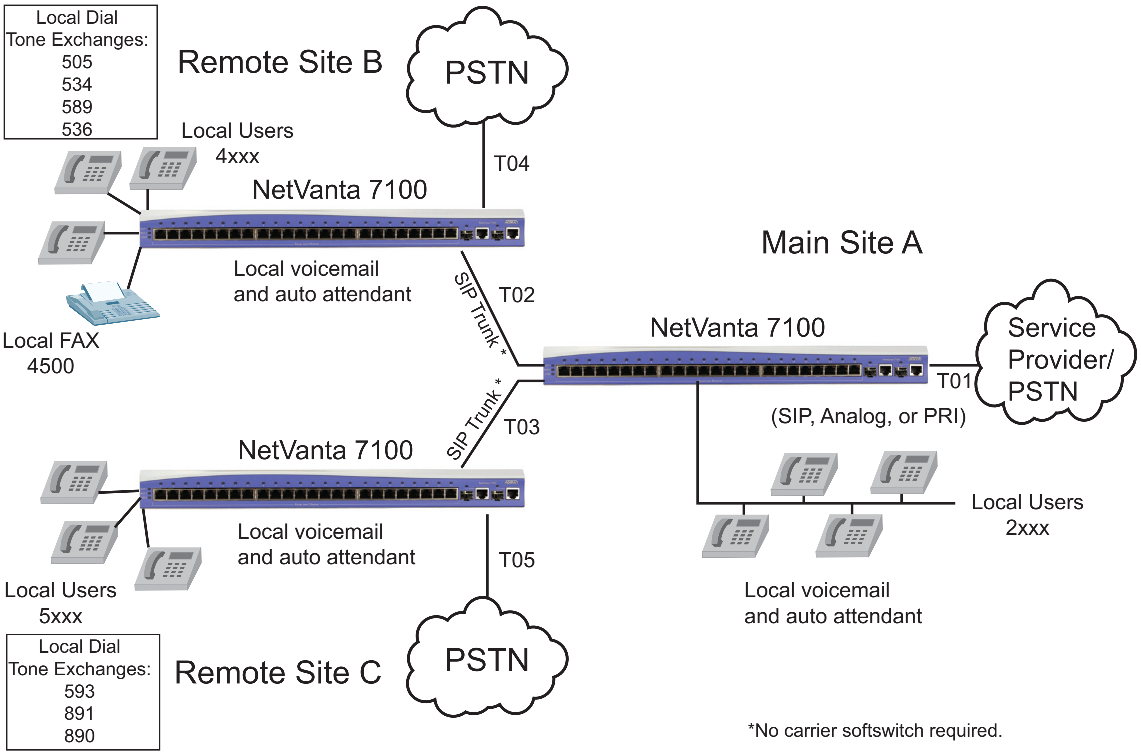


Figure 3. SIP Networking between NetVanta 7000 Series Products

In addition, when configuring SIP trunks and SIP networking between AOS platforms, you must keep in mind dial plan and call routing coordination, WAN connection parameters, and QoS between the sites. To configure SIP networking between NetVanta 7000 Series products, you will need to configure the SIP server, the SIP settings for each platform, and the necessary SIP trunks and trunk groups. This configuration is described in detail in *Configuring SIP Networking between NetVanta 7000 Series Products on page 20*.

SIP Networking Between the NetVanta 7000 Series Other AOS Products

SIP trunks and SIP networks can also be created between NetVanta 7000 Series products and either an AOS IP business gateway (such as a NetVanta 6355 or Total Access 900(e) Series), or other AOS products. This type of networking also relies on a NetVanta 7000 Series unit configured at the main site, and additional AOS products at the remote site(s). *Figure 4* below illustrates the network topology for SIP networking between a NetVanta 7000 series product and two AOS business gateways.

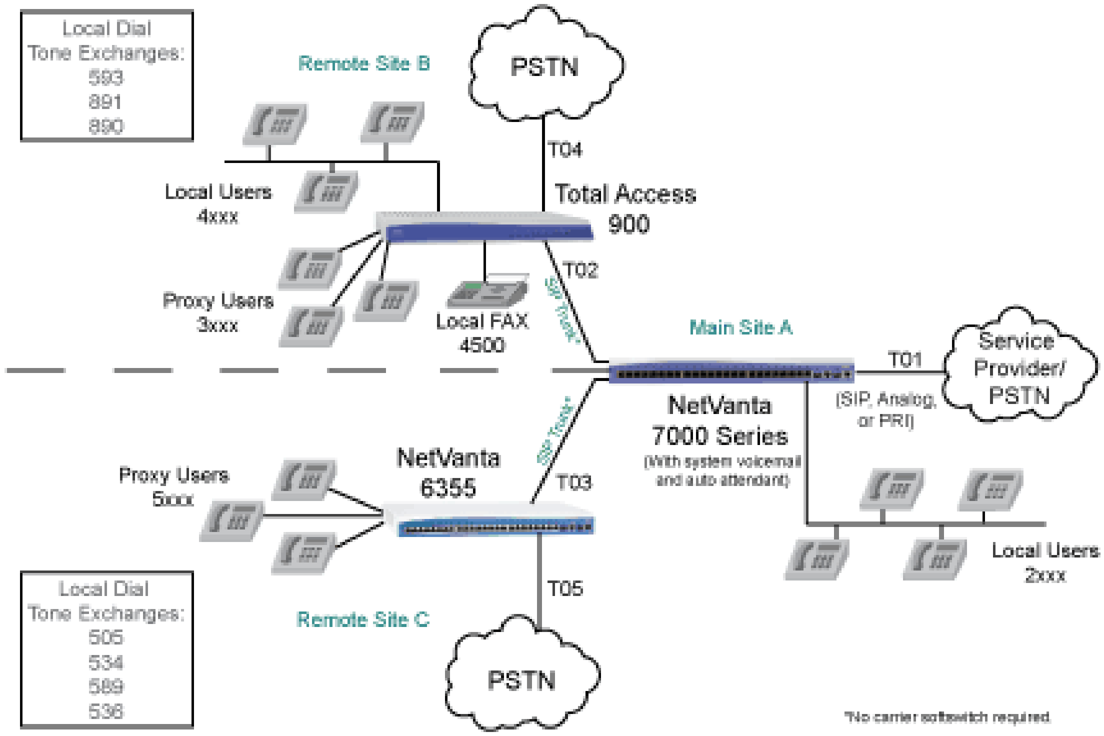


Figure 4. SIP Networking Between a NetVanta 7000 Series Product and AOS IP Business Gateways

When configuring the SIP network between the AOS products, you will also need to consider that SIP proxy is required, that Virtual Private Network (VPN) configuration is required, and that you may need to configure for any failover scenarios and least cost routing (LCR). Configuring this type of SIP network is similar to configuring SIP networks between NetVanta 7000 Series products, in that you will need to create the SIP trunk accounts for each unit, configure the SIP server, and create the necessary trunk groups. These features, and their configuration, are detailed in *Configuring a SIP Network between NetVanta 7000 and IP Gateways on page 31*.

Additional SIP Trunking and Networking Considerations

In addition to understanding which type of SIP network (and therefore the types of SIP trunks) that you are configuring, you should also take into account a few other SIP features to determine how they will fit into your SIP networking configuration. These features include SIP security, QoS, using a fully-meshed or hub-and-spoke network, ANI substitution, trunk templates, SIP diversion, and dial plan and call routing configurations. These features are discussed in the following sections.

SIP Security

Using an IP network for communication can pose many threats to the security of your network. In order to avoid attacks or other security threats, you should configure your network to take advantage of the various SIP security methods. The AOS firewall protects your network from many types of security threat, and provides an internal SIP server and SIP proxy that can rewrite SIP signaling to ensure proper routing, verify valid SIP messages, and create authentication for each SIP user on the network. In addition, when configuring SIP networking between a NetVanta 7000 Series product and another AOS product, the configured VPN provides both IP Security (IPSec) and Generic Routing Encapsulation (GRE) for additional security.

QoS in SIP Networking

QoS is used in SIP networking to ensure the quality of calls between the networked sites, based on bandwidth usage and requirements. In general, QoS is used to prioritize network traffic, and allocate bandwidth, reduce packet delay, and ensure reliability for each packet on the network.

QoS should be implemented on all devices in the SIP network, but it is only a requirement where time sensitive traffic (such as Voice over IP (VoIP)) is using the same bandwidth as data traffic. QoS should be implemented on any interface running at lower-than-Ethernet rates (such as a T1). QoS should also be used on Ethernet interfaces that connect to devices like cable or Asynchronous Data Subscriber Line (ADSL) modems. QoS configuration examples are included in *Configure QoS on page 39* and *Configuring QoS on page 62*. For more detailed information about QoS considerations and configurations, refer to the configuration guide, *Configuring Quality of Service in AOS*, available online at http://kb.adtran.com (article number 1617).

Fully-Meshed or Hub-and-Spoke SIP Networks

Before you begin to implement your SIP network, you should determine which type of SIP networking you will be using. Fully-meshed SIP networks increase redundancy between the networks using multiple SIP trunks at each location. Fully meshed networks provide multiple SIP links between locations, increase network resiliency and redundancy, and integrate voice and data between the network sites. In a fully-meshed SIP network, each NetVanta 7000 Series device can support a maximum of 10 remote SIP trunks. Voice users connected to the NetVanta 7000 Series at each site can connect to all endpoints, at all locations, and each user can have local voicemail and auto attendant services. Although fully meshed SIP networks provide more redundancy than hub-and-spoke SIP networks, they are limiting for future network growth.

Hub-and-spoke SIP networks, on the other hand, can scale up to larger, distributed enterprise solutions by using a central NetVanta 7000 Series unit to aggregate multiple SIP trunks. In a hub-and-spoke network, PSTN access is consolidated by using the NetVanta 7000 Series product as the center (hub) and the main point of access to the PSTN. All remote sites (spokes) connect back to the hub for PSTN access. In this network configuration, voice users have local voicemail and auto attendant services, and connect to the rest of the network using four-digit dialing. Hub-and-spoke networks can grow by increasing the number of NetVanta 7000 Series units that are networked together. This is the recommended method of SIP networking. It is also important to remember that when configuring hub-and-spoke SIP networks, you must have the call routing configured to allow fully meshed networking so that Realtime Protocol (RTP) traffic flows properly.

ANI Substitution

ANI is a service that provides the receiver of a telephone call with the number of the calling phone. For example, ANI is used by emergency dispatchers to quickly respond to an emergency when the caller is unable to report their location. The emergency dispatchers are able to use the two parts of ANI to locate the caller and retrieve the caller's telephone number. The two parts of ANI are its information digits and the calling party's telephone number. The information digits designate class of service (CoS) and are transmitted by dual tone multi-frequency (DTMF) tones or in-band multi-frequency (MF) signaling. This information may sound like caller ID, but it is a separate entity that is transmitted with the phone call, even if caller ID blocking is activated, allowing receivers of the information to determine the calling party's phone number and, in some cases, location.

ANI operates by causing the local switching system to send out (or outpulse) the calling customer's directory number to equipment that requires this information. This equipment could be a centralized automatic message accounting service, an operator services system, or any other office equipment that requires calling number identification. The location that receives the directory number can use it for billing or call routing purposes.

In SIP trunking and networking, ANI substitution is used to associate calls from remote locations to the correct billing number for the enterprise and to forward calls from the SIP trunk. For more information on how to configure ANI substitution, refer to the configuration guide *Enhanced ANI/DNIS Substitution* (article number 2509), or the application guide *Configuring Calling Party (ANI) Match/Substitution to Allow Forwarding of Calls out a SIP Trunk* (article number 3045), available online at http://kb.adtran.com.

Trunk Templates and Trunk Groups

Trunk templates are the accept and reject templates used by the trunk (in this case a SIP trunk), to determine which calls are accepted (and forwarded if necessary) or rejected, or which calls are allowed to be made from the trunk. These templates can be configured using the CLI or the GUI. You can choose to allow local calls, long distance calls, toll-free calls, international calls, n11 calls, 911 calls, operator-assisted calls, carrier specified calls, and 900 calls in the trunk call templates. You can also set an associated cost with each call type, and mark each call type with a low, medium, or high cost. In addition, for SIP networking applications, three-digit or four-digit extensions can be configured or added to the trunk template using an advanced option. These templates are typically configured when configuring the SIP trunk group.

SIP trunk groups combine one or more trunk accounts and assign outbound call characteristics. Individual trunk groups can be created for each trunk account, or multiple trunk accounts can be members of the same trunk group. The trunk group is assigned outbound call capabilities (local calls, long distance calls, etc.). Additionally, a cost is assigned to each attribute in the outbound call template. The cost is a preference and can be used for applications, such as LCR, where the lowest cost receives the highest priority for the specified call templates. For example, if a low cost is set for long distance calls in Trunk Group A, and a high cost is set for long distance calls in Trunk Group B, then long distance calls will go out of Trunk Group A first because it has a lower cost. If there are no available channels on the members of Trunk Group A, long distance calls will go out of Trunk Group B.

Each type of SIP networking and SIP trunk described in this document has an associated trunk group and assigned trunk templates for outbound calls.

SIP Diversion

SIP diversion headers can be modified, and used to avoid problems with redirecting numbers when an alternate identity header is needed by the service provider softswitch to authenticate the origin of the call. Adding or replacing these headers on an outbound trunk is done in a manner similar to configuring enhanced ANI and dialed number identification service (DNIS) substitution. SIP headers are added or replaced on the trunk by using templates and matching sources and targets to those templates. When adding or replacing SIP headers, you must specify the match source, the match source template, the match target, the match target template, and the match action. Each of these parameters are defined on the trunk for each SIP header you want to add or replace.

For more detailed configuration information about SIP Diversion headers, refer to the configuration guide *Modifying SIP Headers on SIP Trunks in AOS Voice Products* (article number 3506), available online at http://kb.adtran.com.

Dial Plan and Call Routing

Configuring the dial plan and call routing behavior of the SIP trunks is essential to correct SIP networking behavior. Dial plans notify the AOS voice unit when to stop collecting the digits being dialed and begin forwarding the phone call. Programmed number patterns and types govern the telephone numbers allowed by AOS voice products for inbound and outbound calls. Number-complete templates can be created and stored in the dial plan. The AOS voice unit listens for digits and looks for a match against he number-complete templates in the dial plan. As soon as the digits dialed by the user match a pattern in the dial plan, the call is routed by the switchboard. If the digits dialed do not match any of the number-complete templates, the call is eventually routed by the switchboard after a timeout period expires. In addition to number patterns, call types are defined in the dial plan, allowing the system to recognize dialed numbers as a particular type of call (local, long distance, toll free, etc.).

The switchboard in the AOS voice product ensures that inbound and outbound phone calls are routed to the proper interface (call routing). Inbound/outbound accept and reject numbers are programmed for voice trunks and referenced by the switchboard whenever a call enters or leaves the unit. For every configured SIP trunk connected to an AOS voice unit, the trunk must be placed into a trunk group. Within the trunk group, accept and reject numbers used by the switchboard to make call routing decisions are collectively assigned to the included voice trunks. Individual voice users can also be created. SIP phone users are treated as IP endpoints, a unique phone number is programmed for each user, and this number is referenced by the switchboard.

For SIP trunking and networking, particularly between two NetVanta 7000 Series products, the dial plan and call routing (switchboard) configurations must be coordinated. All users and locations must have unique extensions, and the SIP trunks between sites must allow extension to extension dialing. By default, calls cannot be routed between two voice trunks, so the trunks must be configured to allow call routing between the trunks. In addition, trunks must also be configured to allow LCR based on area code and exchange information.

For more details on dial plan and call routing configuration, refer to the configuration guide *Switchboard and Dial Plan* (article number 2130), available online at http://kb.adtran.com.

Hardware and Software Requirements and Limitations

AOS firmware version A2.01.00 or later is required on your NetVanta 7000 Series product in order to support SIP trunking. AOS firmware version A2.02.00 or later is required for GRE, VPN, and SIP networking between the NetVanta 7000 Series product and an AOS IP business gateway or NetVanta routing product.

Shared lines are not supported across SIP trunks.

The SIP trunking and networking features are available on AOS voice products as outlined in the ADTRAN knowledge base article number 2272, *AOS Product Feature Matrix*. This matrix is available online at http://kb.adtran.com.

When creating SIP networks with SIP trunks on the NetVanta 7000 Series product, note that a maximum of 10 SIP trunks can be created per NetVanta 7000 Series product.

When SIP networking between two NetVanta 7000 Series products, note that voice features are local to each 7000 Series unit. For example, auto attendants do not contain remote users, voicemail can only be forwarded to local voicemail users, status groups can only be monitored on the same 7000 Series unit as the user, system directories are not automatically synchronized between sites, and paging groups cannot have remote members (remote paging groups must be created to include remote members).

When SIP networking between a NetVanta 7000 Series product and an IP business gateway or a NetVanta router, SIP proxy must be configured and the firewall must be enabled. In addition, these types of SIP networks require a configured VPN to assure call signaling and audio pass between the sites.

Configuring the Service Provider SIP Trunk

Service provider SIP trunks are trunks that are incoming to the NetVanta 7000 Series unit from the ISP. These trunks provide a method of receiving voice traffic through an Internet connection between the NetVanta 7000 Series and the ISP, thus removing the need for a local connection between the PSTN and the NetVanta platform. The following sections provide information about configuring service provider SIP trunks.

Service Provider SIP Trunk Considerations

The following are several configuration considerations you should keep in mind when planning and implementing the service provider SIP trunk configuration on your NetVanta 7000 Series product.

- When a SIP trunk is configured on an Ethernet interface with a public IP address, it is important to correctly configure the firewall policy for that Ethernet interface. The firewall policy should be configured to only allow TCP or UDP traffic on port 5060 from the IP address of the SIP provider’s softswitch.

- During certain call flows with the NetVanta 7000 Series unit, the unit may be required to send a SIP reINVITE message. The service provider's SIP softswitch needs to support a SIP reINVITE, specifically one without Session Description Protocol (SDP).

> NOTE *In AOS firmware release A5.01, you can control where a SIP INVITE without Session Description Protocol (SDP) is sent. A SIP provider must support SIP reINVITE, and by default it must support the reINVITE without SDP.*

- When configuring the service provider SIP trunk in the SIP network, you should also consider configuring a second trunk the PSTN. You can configure a T1, analog, or PRI trunk to function as a backup should the main SIP trunk be unavailable, or the second trunk can be used for local calls by assigning a high cost to the long distance outbound call template.
- QoS should be configured on the NetVanta 7000 Series unit and applied to the Ethernet 0/0 interface to provide a priority queue of bandwidth for RTP and SIP egress packets on the interface. QoS can be configured before or after configuring SIP trunks or trunk groups.

Configuring the Service Provider SIP Trunk Using the GUI

When configuring a SIP trunk from the service provider, it is important to remember that the service provider's softswitch only has control of the call routing up to the SIP trunk interface on the NetVanta 7000 Series unit. This means the NetVanta 7000 Series unit will send and receive all basic SIP call setup messages and will accept advanced setup messages, but the SIP signals of REFER and INVITE with Replaces messages will not be sent out the trunk.

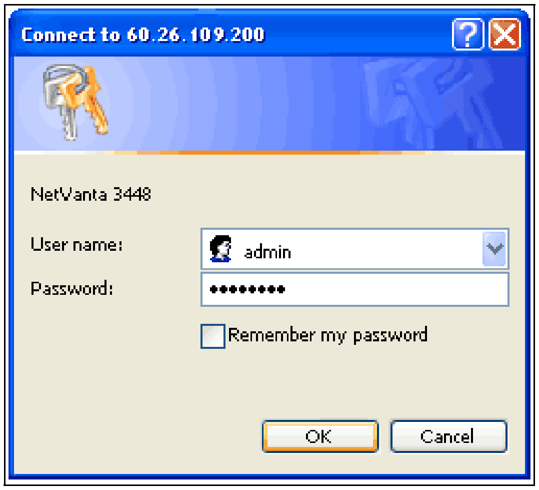
> NOTE *In AOS firmware release A5.01, you can now send SIP REFER and INVITE messages with Replaces on a per-trunk basis, but by default these messages are not sent. ADTRAN recommends that these messages not be sent to SIP providers.*

To configure the SIP trunk using the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Enter your AOS product's IP address in the Internet browser's address field in the following form: **http://**<*ip address*>/**admin**. For example:

   http://65.162.109.200/admin

3. At the prompt, enter your user name and password and select **OK**.



Connect to 60.26.109.200

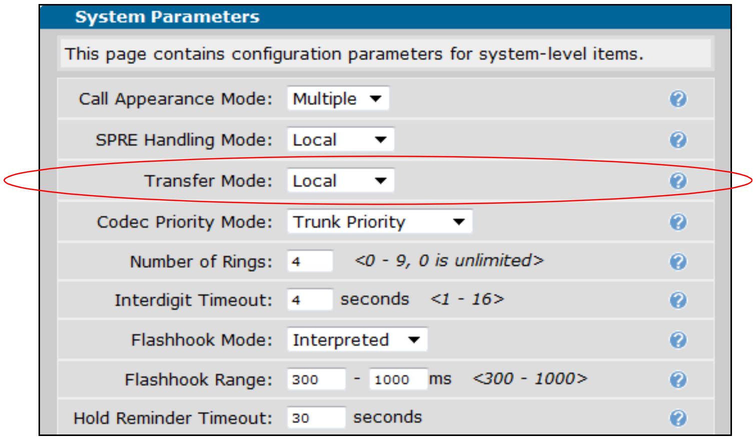
NetVanta 3448

User name:	admin
Password:	••••••••

□ Remember my password

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

4. Navigate to **Voice** > **System Setup** > **System Parameters**. Verify that the **Transfer Mode** is set to **Local**.

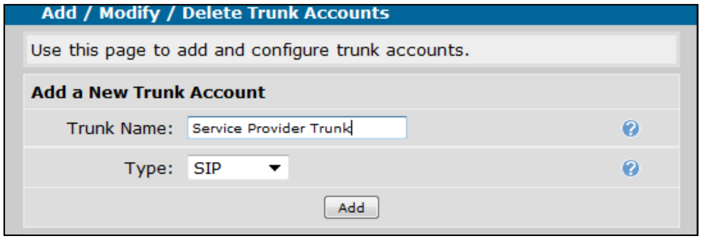


System Parameters

This page contains configuration parameters for system-level items.

Call Appearance Mode:	Multiple
SPRE Handling Mode:	Local
Transfer Mode:	Local
Codec Priority Mode:	Trunk Priority
Number of Rings:	4 <0 - 9, 0 is unlimited>
Interdigit Timeout:	4 seconds <1 - 16>
Flashhook Mode:	Interpreted
Flashhook Range:	300 - 1000 ms <300 - 1000>
Hold Reminder Timeout:	30 seconds

5. Navigate to **Voice** > **Trunks** > **Trunk Accounts**. Specify the name of the SIP trunk in the **Trunk Name** field and select **SIP** as the trunk type. Select **Add** to create the new trunk.



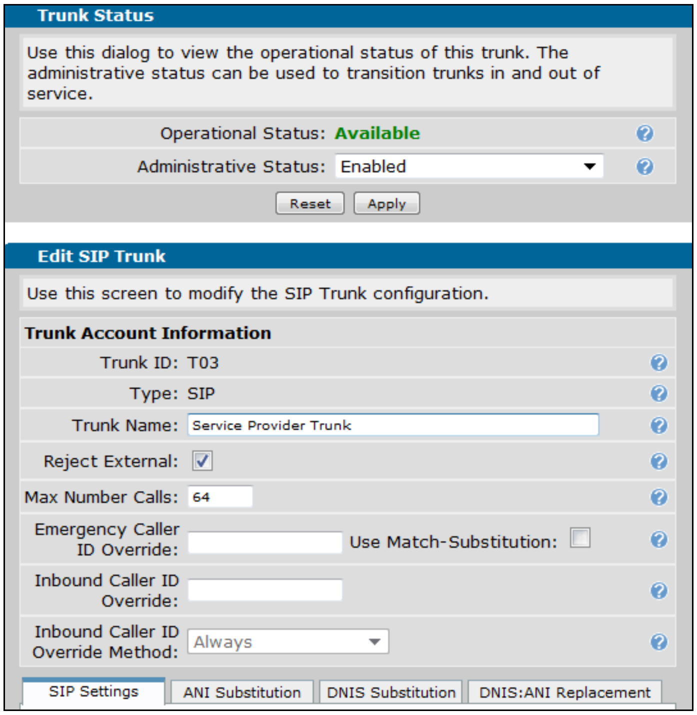
Add / Modify / Delete Trunk Accounts

Use this page to add and configure trunk accounts.

Add a New Trunk Account

Trunk Name:	Service Provider Trunk
Type:	SIP

6. Once the trunk has been created, you are directed to the **Edit SIP Trunk** menu. In this menu you can edit the trunk name, specify that external calls are (or are not) automatically rejected, specify the maximum number of active calls allowed on the trunk, and specify any caller ID override parameters. For the service provider SIP trunk, you do not typically need to change any of these settings, but you should verify these settings with your service provider.



Trunk Status

Use this dialog to view the operational status of this trunk. The administrative status can be used to transition trunks in and out of service.

Operational Status: Available

Administrative Status: Enabled

Edit SIP Trunk

Use this screen to modify the SIP Trunk configuration.

Trunk Account Information

Trunk ID: T03

Type: SIP

Trunk Name: Service Provider Trunk

Reject External: ☑

Max Number Calls: 64

Emergency Caller ID Override: Use Match-Substitution: ☐

Inbound Caller ID Override:

Inbound Caller ID Override Method: Always

The **Trunk Name** field allows you to edit the name of the trunk.

The **Reject External** option, when checked, rejects trunk-to-trunk calls. This option should be disabled for SIP networking applications.

The **Max Number Calls** field specifies the maximum number of active calls allowed on the trunk at the same time. By default, **64** active calls are allowed.

The **Emergency Caller ID Override** field configures the caller ID number on outbound emergency calls to be overridden with a specified value (on this trunk). If **Use Match-Substitution** is checked, substitution will only occur if an ANI or DNIS match substitution is found.

The **Inbound Caller ID Override** field configures the caller ID number on inbound calls to be overridden with the specified value (on this trunk).

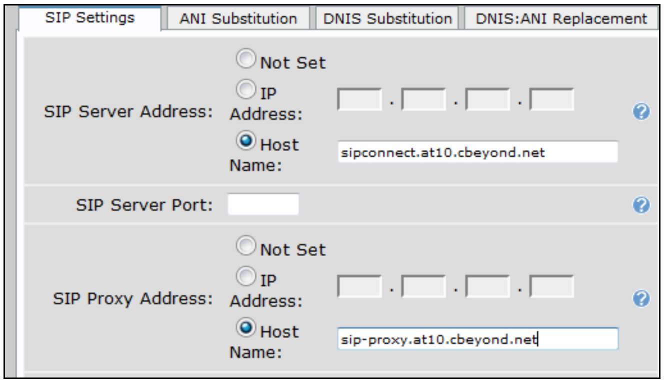
The **Inbound Caller ID Override Method** specifies the caller ID override method. You can choose **Only if Not Present** to specify that caller ID information is inserted only if no caller ID information is present in the call information, or you can choose **Always** to specify that caller ID information is always replaced with the defined caller ID value.

7. Scroll down to the **SIP Settings** tab on the **Edit SIP Trunk** menu. In this menu, you will set the SIP server address, specify the trunk's SIP settings, and configure the SIP registration. For a service provider SIP trunk, enter the **SIP Server Address** using either the specific host name with the fully qualified domain name (FQDN) or the IP address on which the trunks will terminate. This information is

provided by your service provider. For some service providers you will also need to enter the **SIP Proxy Address** using the specific IP address or FQDN on which the trunks will terminate.

NOTE *The NetVanta 7000 Series unit must be configured with a domain naming system (DNS) server address to be able to resolve any FQDN that is used here.*

In the following example, **sipconnect.at10.cbeyond.net** is used for the SIP server address, and **sip-proxy.at10.cbeyond.net** is used for the SIP proxy address.

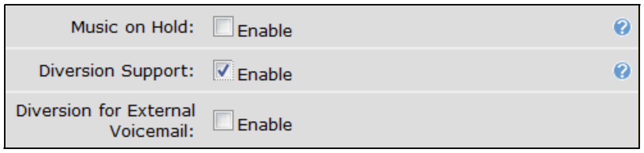


SIP Server Address: ○ Not Set ○ IP Address: . . . ● Host Name: sipconnect.at10.cbeyond.net

SIP Server Port:

SIP Proxy Address: ○ Not Set ○ IP Address: . . . ● Host Name: sip-proxy.at10.cbeyond.net

8. Enable **Diversion Support** using the check box.

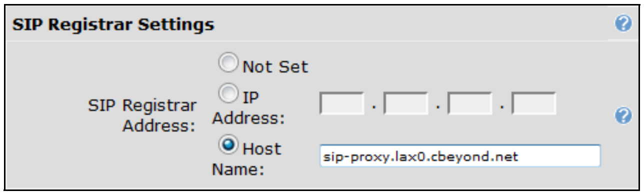


Music on Hold: □ Enable

Diversion Support: ☑ Enable

Diversion for External Voicemail: □ Enable

9. Enter the **SIP Registrar Address** using either the specific host name with the FQDN or IP address. The **SIP Registrar Address** is defined by your service provider. In the following example, **sip-proxy.lax0.cbeyond.net** is used for the **SIP Registrar Address**.

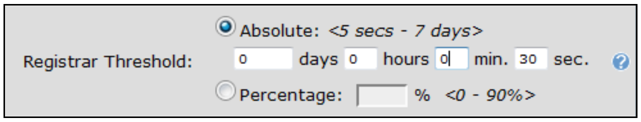


SIP Registrar Settings

SIP Registrar Address: ○ Not Set ○ IP Address: . . . ● Host Name: sip-proxy.lax0.cbeyond.net

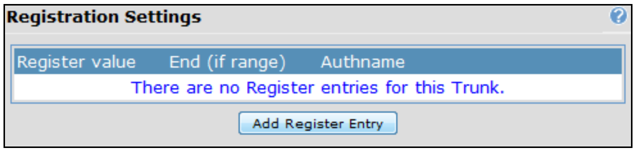
10. Change the **Registrar Threshold** setting to **30** seconds. The registrar threshold sets the remaining time for the current registration to re-register. By default, the registrar threshold is set to **5** minutes. By altering this value, it is possible to ensure that even if there is a delay in obtaining a far-end registration, the re-registration should occur before the current registration times out. Specify the registrar threshold as **absolute**, indicating the registrar threshold is a fixed amount of time. For example, if the threshold

is set for 5 minutes absolute, and the current registration is due to expire at 5:30 p.m., then re-registration begins at 5:25 p.m. You should enter the registrar threshold value supplied by your service provider.



Registrar Threshold: ● Absolute: *<5 secs - 7 days>*
0 days 0 hours 0 min. 30 sec.
○ Percentage: ____ % *<0 - 90%>*

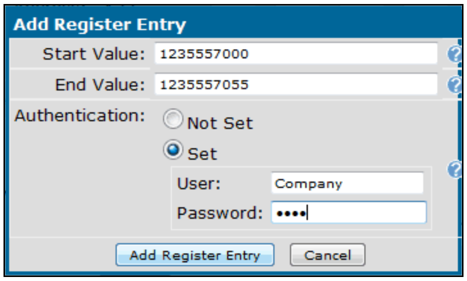
11. Configure the number(s) to be registered on this SIP trunk. To add new numbers to the register, select the **Add Register Entry** button below the **Register Settings** table.



Registration Settings

Register value	End (if range)	Authname
There are no Register entries for this Trunk.		

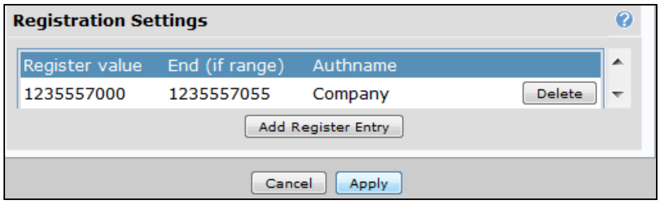
12. In the **Add Register Entry** pop-up menu, enter the **Start Value** and **End Value** numbers. These values are the beginning and ending of a range of numbers to be registered to this trunk. In addition, specify that **Authentication** is **Set**, and enter the user name and password to be used when registering users on this trunk. Select **Add Register Entry** to create the new SIP identity number registration.



Add Register Entry

Start Value: 1235557000
End Value: 1235557055
Authentication: ○ Not Set
● Set
User: Company
Password: ••••

13. Select **Apply** at the bottom of the **Edit SIP Trunk** menu to apply the new SIP trunk account settings.

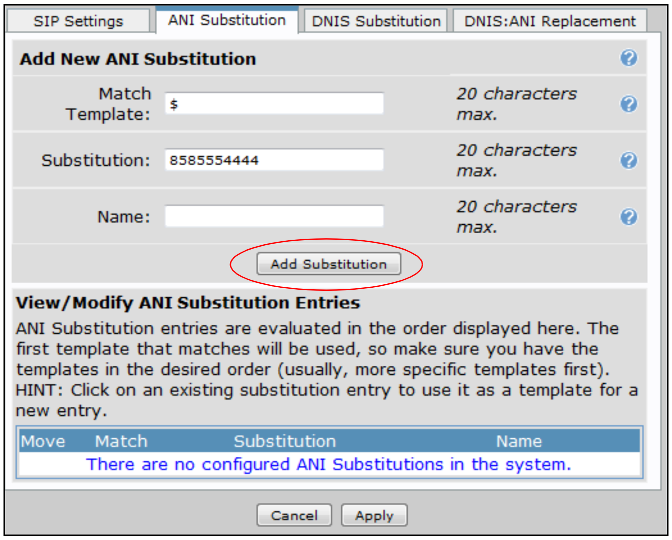


Registration Settings

Register value	End (if range)	Authname	
1235557000	1235557055	Company	Delete

14. Next, you will need to configure the service provider's SIP trunk ANI substitution settings by selecting the **ANI Substitution** tab on the **Edit SIP Trunk** menu. Configure the outgoing caller ID to match the billing number provided by your service provider. Set the **Match Template** to **$** (matches any number). Set the **Substitution** to the service provider assigned SIP trunk number registered with the softswitch.

You can optionally change the **Name** of the calling party if necessary. When you have completed the ANI substitution changes, select **Add Substitution**.



Add New ANI Substitution

Match Template:	$	20 characters max.
Substitution:	8585554444	20 characters max.
Name:		20 characters max.

View/Modify ANI Substitution Entries

ANI Substitution entries are evaluated in the order displayed here. The first template that matches will be used, so make sure you have the templates in the desired order (usually, more specific templates first). HINT: Click on an existing substitution entry to use it as a template for a new entry.

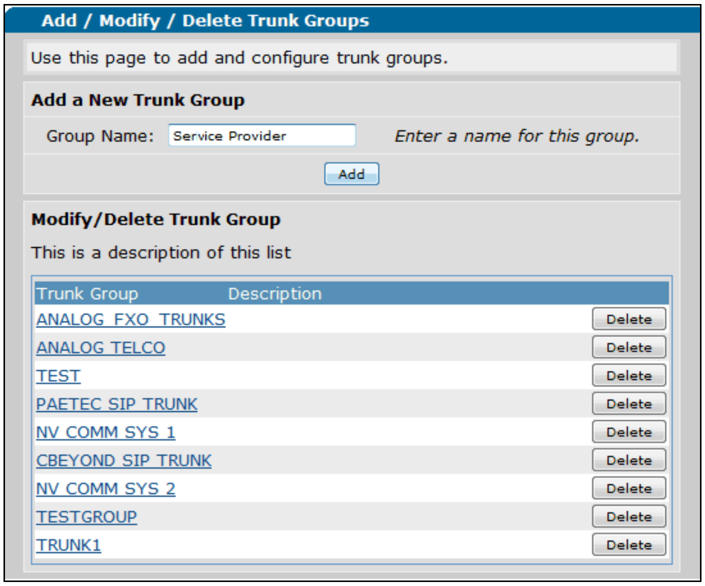
Move	Match	Substitution	Name
There are no configured ANI Substitutions in the system.			

15. After completing the ANI substitution, the service provider SIP trunk is configured. You must now configure a trunk group for the service provider SIP trunk and apply accept templates to the trunk group.

Configuring the Service Provider SIP Trunk Group using the GUI

To configure the service provider SIP trunk group, and the trunk group accept templates, follow the steps below:

1. Navigate to **Voice** > **Trunks** > **Trunk Groups**. Enter a new **Group Name** and select **Add**. In the example below, the trunk group is named **Service Provider**. If you need to edit an existing trunk, select the trunk from the list under **Modify/Delete Trunk Group**.



Add / Modify / Delete Trunk Groups

Use this page to add and configure trunk groups.

Add a New Trunk Group

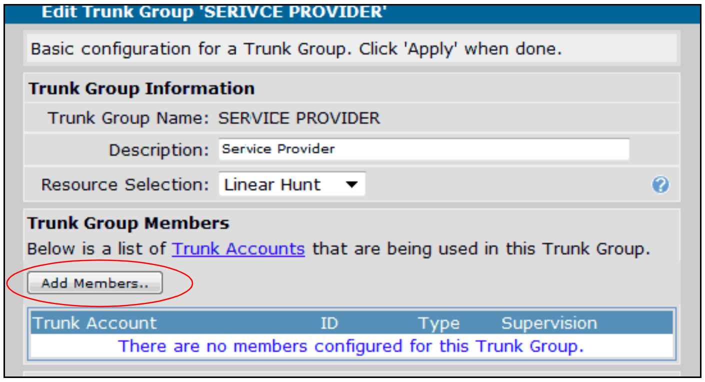
Group Name: Service Provider — *Enter a name for this group.*

Modify/Delete Trunk Group

This is a description of this list

Trunk Group	Description	
ANALOG FXO TRUNKS		Delete
ANALOG TELCO		Delete
TEST		Delete
PAETEC SIP TRUNK		Delete
NV COMM SYS 1		Delete
CBEYOND SIP TRUNK		Delete
NV COMM SYS 2		Delete
TESTGROUP		Delete
TRUNK1		Delete

2. After adding a trunk group, you are directed to the **Edit Trunk Group** menu. To add the service provider SIP trunk to this trunk group, select **Add Members**. You can optionally add a description of the trunk group in the **Description** field, or specify the method by which DS0s or ports are selected by the switchboard for call routing by selecting **Linear Hunt** or **Circular Hunt** from the **Resource Selection** drop-down menu. By default, the resource is set to **Linear Hunt**.



Edit Trunk Group 'SERIVCE PROVIDER'

Basic configuration for a Trunk Group. Click 'Apply' when done.

Trunk Group Information

Trunk Group Name: SERVICE PROVIDER

Description: Service Provider

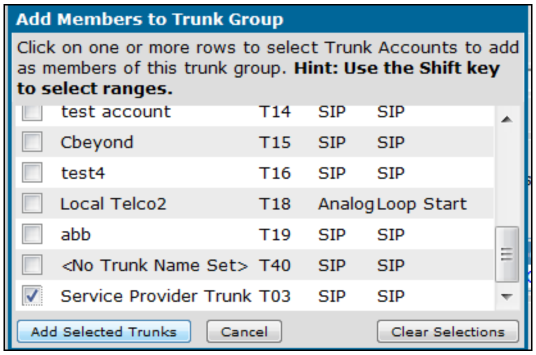
Resource Selection: Linear Hunt

Trunk Group Members

Below is a list of Trunk Accounts that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision
There are no members configured for this Trunk Group.			

3. After selecting **Add Members**, select the trunk(s) to add to the trunk group from the list in the **Add Members to Trunk Group** menu. In this example, the previously created **Service Provider Trunk** is selected to be added to the trunk group. After selecting the trunk, select **Add Selected Trunks**.



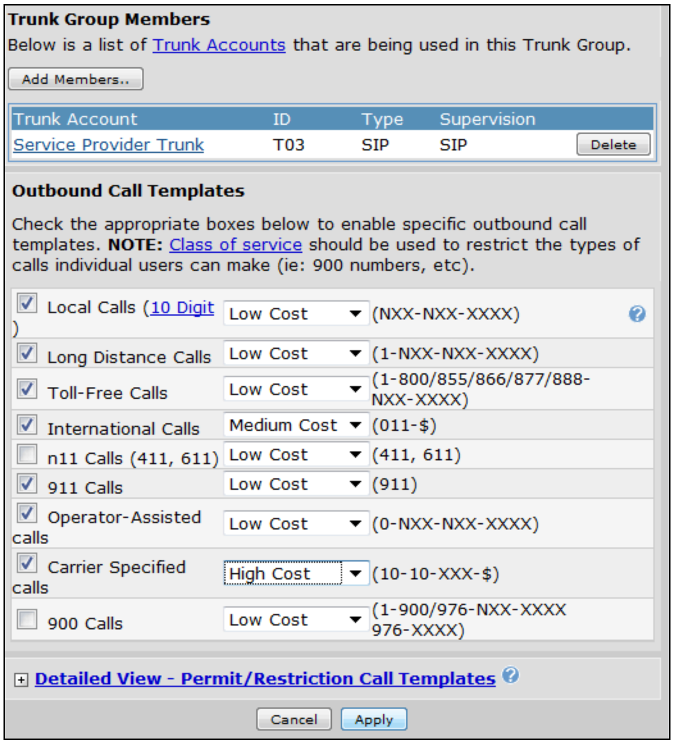
Add Members to Trunk Group

Click on one or more rows to select Trunk Accounts to add as members of this trunk group. **Hint: Use the Shift key to select ranges.**

□	test account	T14	SIP	SIP
□	Cbeyond	T15	SIP	SIP
□	test4	T16	SIP	SIP
□	Local Telco2	T18	Analog	Loop Start
□	abb	T19	SIP	SIP
□	<No Trunk Name Set>	T40	SIP	SIP
☑	Service Provider Trunk	T03	SIP	SIP

4. The new trunk group members appear in the list of trunk group members, and you can now configure the **Outbound Call Templates** for the trunk group. Outbound call templates are the types of calls to allow from this trunk. Select the appropriate boxes to enable specific outbound call capabilities for this trunk group, and select the cost for each call type from the drop-down menu. In the following example, the local calls are set to 10-digit dialing calls. To specify if local calls are 10-digit or 7-digit, specify the

local dialing type under **System Setup** > **Dial Plan**. Select **Apply** when you have configured the outbound call templates for the trunk group.



Trunk Group Members

Below is a list of Trunk Accounts that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision	
Service Provider Trunk	T03	SIP	SIP	Delete

Outbound Call Templates

Check the appropriate boxes below to enable specific outbound call templates. **NOTE:** Class of service should be used to restrict the types of calls individual users can make (ie: 900 numbers, etc).

☑ Local Calls (10 Digit)	Low Cost	(NXX-NXX-XXXX)
☑ Long Distance Calls	Low Cost	(1-NXX-NXX-XXXX)
☑ Toll-Free Calls	Low Cost	(1-800/855/866/877/888-NXX-XXXX)
☑ International Calls	Medium Cost	(011-$)
□ n11 Calls (411, 611)	Low Cost	(411, 611)
☑ 911 Calls	Low Cost	(911)
☑ Operator-Assisted calls	Low Cost	(0-NXX-NXX-XXXX)
☑ Carrier Specified calls	High Cost	(10-10-XXX-$)
□ 900 Calls	Low Cost	(1-900/976-NXX-XXXX 976-XXXX)

5. The service provider SIP trunk, and the service provider SIP trunk group are now configured. You can now continue to configure additional SIP trunks for SIP networking with other NetVanta 7000 Series or AOS devices.

Configuring the Service Provider SIP Trunk using the CLI

The following example configures the same service provider SIP trunk and trunk group as configured using the GUI, only this example is configured using the CLI. The CLI example is a sample configuration only, and does not include details of each command used in the configuration. For details about commands used to configure SIP trunks and trunk groups, refer to the *AOS Command Reference Guide* available online at http://kb.adtran.com (article number 2219).

To configure the service provider SIP trunk using the CLI, follow these steps:

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

   telnet 10.10.10.1.

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

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

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

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

   ```
   >enable
   ```

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

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

6. Create the service provider SIP trunk using the **voice trunk** command from the Global Configuration mode prompt. This command enters the trunk's configuration mode, where you can specify a description for the trunk, disable external call rejection, specify the SIP server and registrar, enable SIP diversion, specify the SIP TO and FROM header types, add registration and authentication to the trunk, and configure ANI substitution for the trunk.

   > *The following configuration is for example purposes only. These settings will vary depending on your service provider.*

   The following example configures the service provider SIP trunk:

   ```
   voice trunk T03 type sip
     description "Service Provider Trunk"
     no reject-external
     sip-server primary sipconnect.atl0.cbeyond.net
     registrar primary sip-proxy.lax0.cbeyond.net
     diversion-supported
     grammar to host domain
     grammar from host domain
     registrar threshold absolute 30
     registrar range 1235557000 1235557055 auth-name company password 1234
     match ani $ substitute 8585554444
   ```

7. Create the service provider SIP trunk group using the **voice grouped-trunk** command from the Global Configuration mode prompt. This command enters the trunk group's configuration mode, where you can specify the trunks added to the group, and the outbound call templates for the group. The following example configures the service provider SIP trunk group:

   ```
   voice grouped-trunk "Service Provider"
     trunk T03
     accept NXX-NXX-XXXX cost 0
     accept 1-NXX-NXX-XXXX cost 0
     accept 1-800-NXX-XXXX cost 0
     accept 1-888-NXX-XXXX cost 0
     accept 1-877-NXX-XXXX cost 0
     accept 1-866-NXX-XXXX cost 0
   ```

```
accept 1-855-NXX-XXXX cost 0
accept 011-$ cost 0
accept 411 cost 0
accept 611 cost 0
accept 911 cost 0
accept 0-NXX-NXX-XXXX cost 200
accept 10-10-XXX-$ cost 350
reject 976-XXXX
reject 1-900-NXX-XXXX
reject 1-976-NXX-XXXX
```

8. The service provider SIP trunk and SIP trunk group are now configured. You can now continue to configure additional SIP trunks for SIP networking with other NetVanta 7000 Series units or AOS devices.

Configuring SIP Networking between NetVanta 7000 Series Products

SIP networking between NetVanta 7000 Series products generally occurs when multiple 7000 Series platforms are used at multiple enterprise sites. SIP trunks are configured between the NetVanta 7000 Series unit at the main site, and the NetVanta 7000 Series units at any remote office locations. *Figure 5* below illustrates a typical network configuration for SIP networking between NetVanta 7000 Series products.

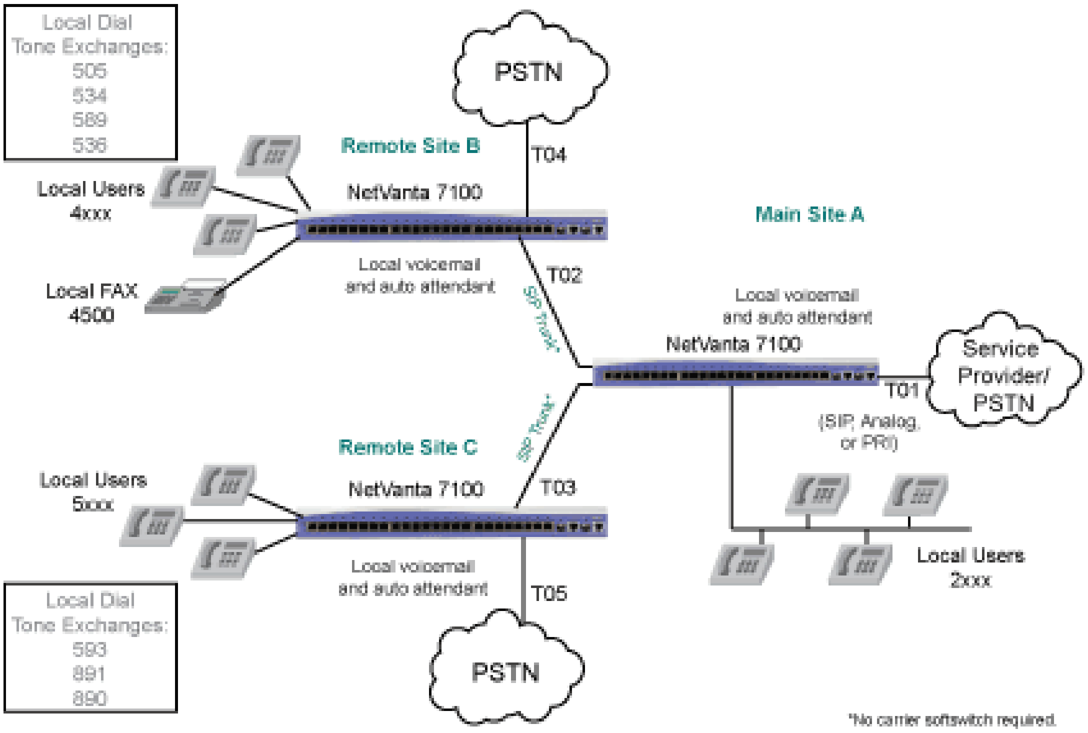


Figure 5. SIP Networking between NetVanta 7000 Series Products

There are a few things to keep in mind when configuring SIP networking between NetVanta 7000 Series units:

- There are a limit of **10** SIP trunks per NetVanta 7000 Series unit.
- Voice features are local to each NetVanta 7000 Series. Auto attendants do not contain remote users, voicemail can only be forwarded to local voicemail users, status groups can only be monitored on the same NetVanta 7000 Series as the user, system directories are not automatically synchronized between NetVanta 7000 Series products, and paging groups do not contain remote user members, rather you must create remote paging groups.
- The dial plan and call routing must be coordinated with unique extensions at each location (the previous illustration depicts 2xxx extensions at the main site, 4xxx extensions at Remote Site B, and 5xxx extensions at Remote Site C). In addition, trunks between sites need to allow for extension to extension dialing, and trunks need to allow for LCR based on area code and exchange.
- It is recommended to configure SIP networking between NetVanta 7000 Series products in a hub-and-spoke network, rather than a fully meshed network. However, call routing must allow fully meshed networking so that RTP can flow properly.
- Consider the WAN connections because they affect QoS implementation. If you are using Point-to-Point T1 or Multiprotocol Label Switching (MPLS) WAN connections, QoS is generally assured. If you are using Ethernet (Metro or from ADSL or cable modems) connections, there is no guarantee of QoS in the network.
- You must consider (and possibly configure) QoS between the NetVanta 7000 Series sites to maintain call quality.

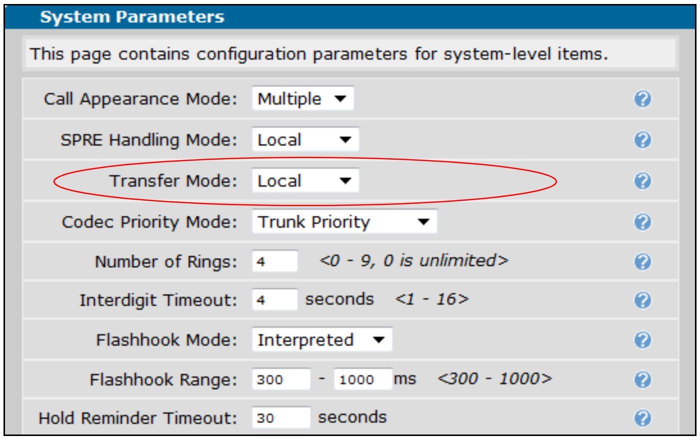
Configuring SIP Networking between NetVanta 7000 Series Products using the GUI

When configuring SIP networking between NetVanta 7000 Series products, you will configure multiple SIP trunks for communication between the NetVanta 7000 Series unit at the main site and the remote sites. This is typically done after you have configured the service provider SIP trunk to the NetVanta 7000 Series unit at the main site. In *Figure 4 on page 6*, there are two SIP trunks to be configured: trunk T02, connecting the Main Site A and Remote Site B, and trunk T03, connecting the Main Site A and Remote Site C. In addition, the trunks T04 and T05, are configured to connect to the PSTN. These trunks can be used for local calls by assigning a high cost to the long distance outbound call template for the trunk, or they can be used for survivability during possible failure of the main SIP trunk service. This configuration example focuses on the two SIP trunks between the main site and the remote sites.

Configuring SIP Trunks between Sites

To configure the SIP trunks between NetVanta 7000 Series units using the GUI, follow these steps:

1. Connect to the GUI and navigate to **Voice** > **System Setup** > **System Parameters**. Verify that the **Transfer Mode** is set to **Local**.



System Parameters

This page contains configuration parameters for system-level items.

Call Appearance Mode: Multiple

SPRE Handling Mode: Local

Transfer Mode: Local

Codec Priority Mode: Trunk Priority

Number of Rings: 4 *<0 - 9, 0 is unlimited>*

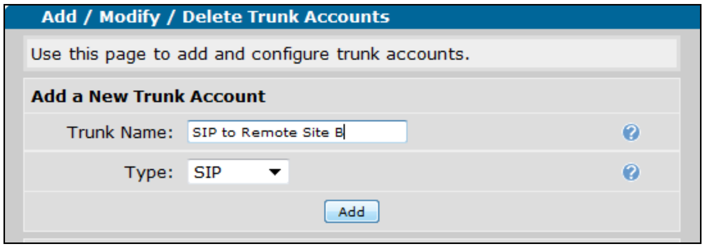
Interdigit Timeout: 4 seconds *<1 - 16>*

Flashhook Mode: Interpreted

Flashhook Range: 300 - 1000 ms *<300 - 1000>*

Hold Reminder Timeout: 30 seconds

2. Navigate to **Voice > Trunks** > **Trunk Accounts**. Specify the name of the SIP trunk in the **Trunk Name** field and select **SIP** as the trunk type. Select **Add** to create the new trunk. In the following example, the trunk is named **SIP to Remote Site B**.



Add / Modify / Delete Trunk Accounts

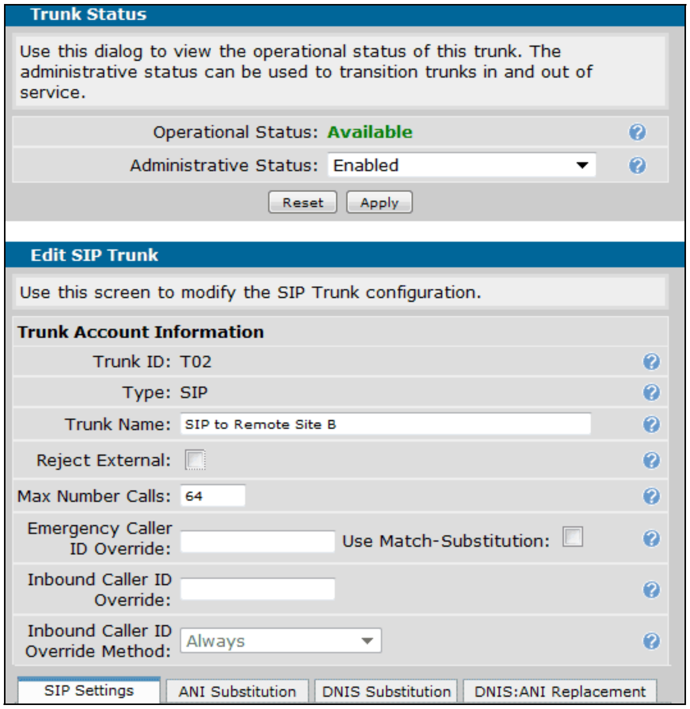
Use this page to add and configure trunk accounts.

Add a New Trunk Account

Trunk Name: SIP to Remote Site B

Type: SIP

3. Once the trunk has been created, you are directed to the **Edit SIP Trunk** menu. You do not typically need to change any of these settings for SIP trunks between NetVanta 7000 Series products.



Trunk Status

Use this dialog to view the operational status of this trunk. The administrative status can be used to transition trunks in and out of service.

Operational Status: Available

Administrative Status: Enabled

Edit SIP Trunk

Use this screen to modify the SIP Trunk configuration.

Trunk Account Information

Trunk ID: T02

Type: SIP

Trunk Name: SIP to Remote Site B

Reject External: □

Max Number Calls: 64

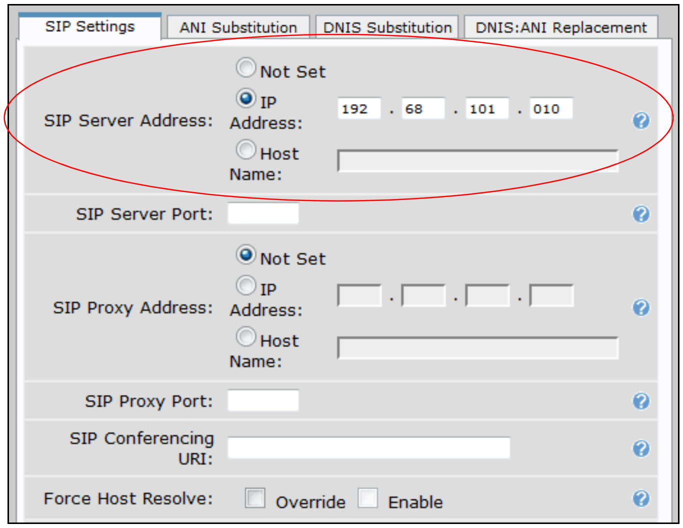
Emergency Caller ID Override: Use Match-Substitution: □

Inbound Caller ID Override:

Inbound Caller ID Override Method: Always

4. Next, set the trunk's SIP settings by selecting the **SIP Settings** tab on the **Edit SIP Trunk** menu. Here you will configure the SIP server address, the FROM SIP header, and other optional SIP parameters. For SIP networking between NetVanta 7000 Series products, enter the IP address of the remote NetVanta 7000 Series product to which the SIP trunk connects as the **SIP Server Address**.

   SIP Server Address specifies a host name or IP address of the primary SIP server. For SIP networking between NetVanta 7000 Series products, this value should be the IP address of the remote NetVanta 7000 Series product to which the SIP trunk connects. The NetVanta 7000 Series must be configured with a DNS server address if a **Host Name** is used as the **SIP Server Address**. Navigate to **System** > **Hostname/DNS** to enter a DNS server address.



SIP Server Address: ○ Not Set ● IP Address: 192 . 68 . 101 . 010 ○ Host Name:

SIP Server Port:

SIP Proxy Address: ● Not Set ○ IP Address: . . . ○ Host Name:

SIP Proxy Port:

SIP Conferencing URI:

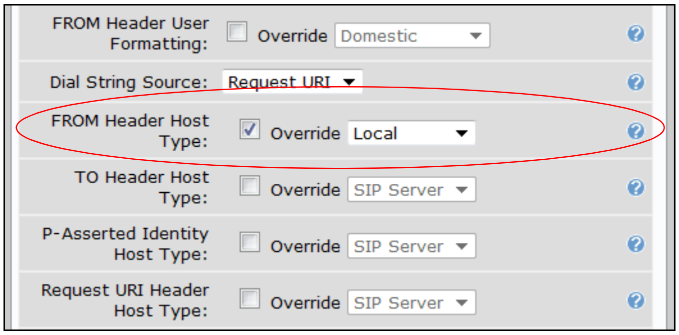
Force Host Resolve: □ Override □ Enable

FROM Header Host Type sets the FROM header host formatting type to be used on SIP trunks. This should be set to **Local** for SIP networking between NetVanta 7000 Series products. Specify the FROM header by selecting the **Override** checkbox and the appropriate parameter from the drop-down menu.

SIP Server specifies using the SIP server IP address in the host field.

Domain specifies using the **Domain Address** configured under **Trunk Accounts** (SIP Registrar Settings) menu.

Local specifies using the IP address of the local outbound interface in the host field.



FROM Header User Formatting: □ Override Domestic

Dial String Source: Request URI

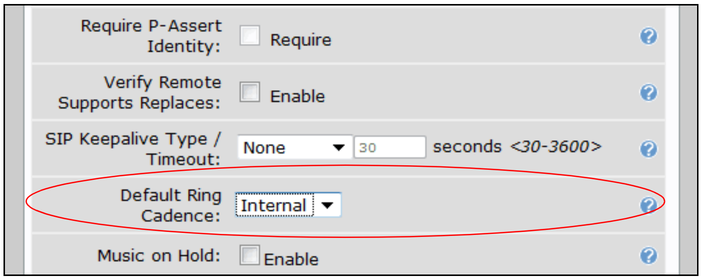
FROM Header Host Type: ☑ Override Local

TO Header Host Type: □ Override SIP Server

P-Asserted Identity Host Type: □ Override SIP Server

Request URI Header Host Type: □ Override SIP Server

Default Ring Cadence specifies the default ring cadence for incoming SIP calls that do not contain an Alert-Info header. You can select **Internal** or **External** from the drop-down menu. The ring cadence should be set to **Internal** for SIP networking between NetVanta 7000 Series products.



Require P-Assert Identity: □ Require

Verify Remote Supports Replaces: □ Enable

SIP Keepalive Type / Timeout: None 30 seconds *<30-3600>*

Default Ring Cadence: Internal

Music on Hold: □ Enable

Optional SIP Settings

SIP Server Port specifies the User Datagram Protocol (UDP) port on which the far-end server is listening for SIP messages.

SIP Proxy Address (optional) sets the host name or IP address of an outbound SIP proxy. The DNS server address is required if **Host Name** is entered.

SIP Proxy Port specifies the UDP port on which the far-end server is listening for SIP messages.

SIP Conferencing URI specifies the host name or IP address of the conferencing server. The DNS server address is required if the **Host Name** is entered.

NOTE *In most applications, the SIP Conferencing URI should not be configured.*

Force Host Resolve requires the host name in the SIP Request-URI Header be resolved to an IP address when enabled.

FROM Header User Formatting sets the SIP FROM header user formatting type. Select the formatting type to be used on the FROM header for inbound and outbound numbers on SIP trunks by selecting the **Override** checkbox and the appropriate parameter from the drop-down menu.

Global Default uses the default type set in the **VoIP Settings** tab. Access the **VoIP Settings** tab under **Voice > System Setup > VoIP Settings**.

Domestic formats numbers suitable for US domestic calls (for example, 123-555-1212).

International formats numbers using the E.164 dialing specification (for example, +1-123-555-1212).

Dial String Source specifies the dial string to use. You can select **Request URI**, which uses the Request URI user field as the dial string, or **TO Header**, which uses the TO header user field as the dial string.

TO Header Host Type sets the To header host formatting type to be used on SIP trunks. Specify the TO header by selecting the **Override** checkbox and the appropriate parameter from the drop-down menu.

SIP Server specifies using the SIP server IP address in the host field.

Domain specifies using the **Domain Address** configured under **Trunk Accounts** (SIP Registrar Settings) menu.

P-Asserted Identity Host Type sets the P-Asserted identity host formatting type to be used on SIP trunks. Specify the P-Asserted Identity host type by selecting the **Override** checkbox and the appropriate parameter from the drop-down menu.

SIP Server uses the SIP server IP address in the **Host Name** field.

Domain uses the domain address configured in the **Host Name** field.

Local uses the IP address of the local outbound interface in the **Host Name** field.

Request URI Header Host Type sets the Request URI header host formatting type to be used on SIP trunks. Specify the Request URI header by selecting the **Override** checkbox and the appropriate parameter from the drop-down menu.

SIP Server uses the SIP server IP address in the **Host Name** field.

Domain uses the domain address configured in the **Host Name** field.

Alert Info URL specifies the Alert Info URL.

Supports 100rel inserts a 100rel tag into the Supports header of all outgoing SIP messages when enabled. This indicates to the far end that the unit is capable of sending provisional acknowledgement (PRACK). Disable this setting to prevent the far end from requesting the unit to send PRACK.

Require 100rel sends a reliable provisional response to clients that supports 100rel tag when enabled. If the client to which the provisional response is being sent requires a 100rel tag, a reliable provisional response will be sent regardless of the configuration.

Dial String Source specifies the **Request URI** or **To Header** user field as the dial string.

Trust Domain enables the trunk to be a member of an RFC 3325 trust domain.

Require P-Assert Identity requires P-Asserted identities for the trust domain when enabled.

Verify Remote Supports Replaces requires verification that the remote SIP server supports SIP REPLACES, before sending REPLACES messages.

SIP Keepalive Type / Timeout specifies the type and time period of keep-alive messages that can be sent on a SIP trunk to the SIP server during a call. The purpose of a keep-alive message is to monitor the status of the connection between the SIP server and the unit. If the keepalive receives an error response or does not receive a response at all, the call will be disconnected.

NOTE *This setting should remain disabled on SIP trunks to NetVanta 7000 Series devices or IP Business Gateways.*

Type specifies the type of SIP message to be sent as a keepalive during a call on the trunk. You can select **OPTIONS**, **INFO**, or **None**. Select **None** to disable (default).

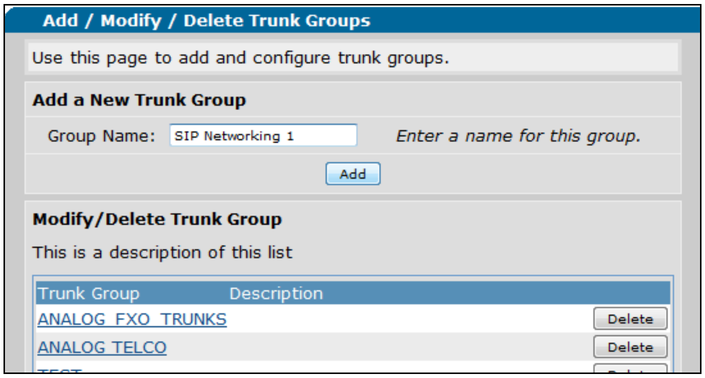
Timeout specifies time period (in seconds) between transmitting keep-alive messages. Valid range is **0** to **3600** seconds, with a default value of **30** seconds.

5. Select **Apply** once you have configured the SIP settings for the trunk. Repeat Steps 1 through 4 for each SIP trunk between the NetVanta 7000 Series products.

Configuring SIP Networking Trunk Group(s) using the GUI

Once you have configured all the necessary SIP trunks between the NetVanta 7000 Series products, you must create a trunk group for the SIP trunks. For this application, you will need to create a trunk group for each SIP trunk to the remote site(s). The trunk group allows you to configure the outbound call templates for the trunk, so you can create a trunk group for each SIP trunk with the appropriate template.

1. Create the trunk group by navigating to **Voice** > **Trunks** > **Trunk Groups**. Enter a new **Group Name** and select **Add**. In the example below, the trunk group is named **SIP Networking 1**. If you need to edit an existing trunk, select the trunk from the list under **Modify/Delete Trunk Group**.



Add / Modify / Delete Trunk Groups

Use this page to add and configure trunk groups.

Add a New Trunk Group

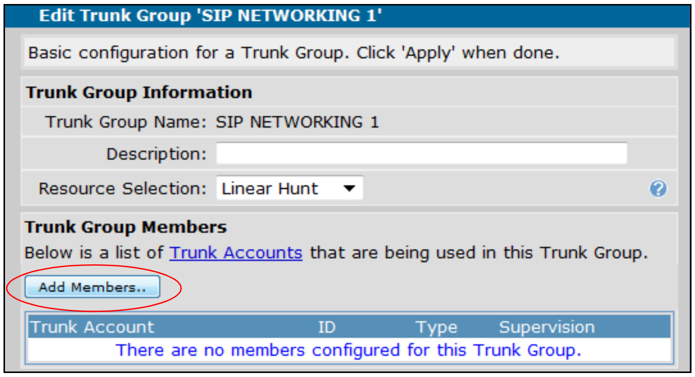
Group Name: SIP Networking 1 *Enter a name for this group.*

Modify/Delete Trunk Group

This is a description of this list

Trunk Group	Description	
ANALOG_FXO_TRUNKS		Delete
ANALOG TELCO		Delete

2. After adding a trunk group, you are directed to the **Edit Trunk Group** menu. To add the SIP networking trunk to this trunk group, select **Add Members**. You can optionally add a description of the trunk group in the **Description** field, and specify the method that DS0s or ports are selected by the switchboard for call routing by selecting **Linear Hunt** or **Circular Hunt** from the **Resource Selection** drop-down menu. By default, the resource is set to **Linear Hunt**.



Edit Trunk Group 'SIP NETWORKING 1'

Basic configuration for a Trunk Group. Click 'Apply' when done.

Trunk Group Information

Trunk Group Name: SIP NETWORKING 1

Description:

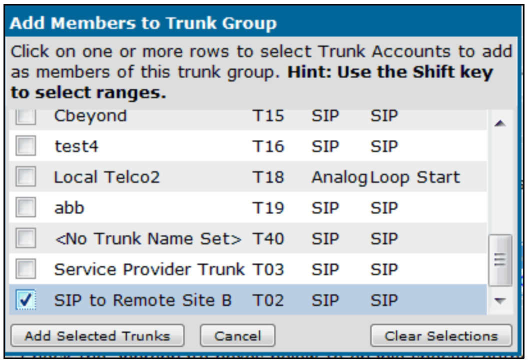
Resource Selection: Linear Hunt

Trunk Group Members

Below is a list of Trunk Accounts that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision
There are no members configured for this Trunk Group.			

3. After selecting **Add Members**, select the trunk(s) to add to the trunk group from the list in the **Add Members to Trunk Group** menu. In this example, the previously created trunk, **SIP to Remote Site B**, is selected to be added to the trunk group. After selecting all the trunks you want to add to the group, select **Add Selected Trunks**.

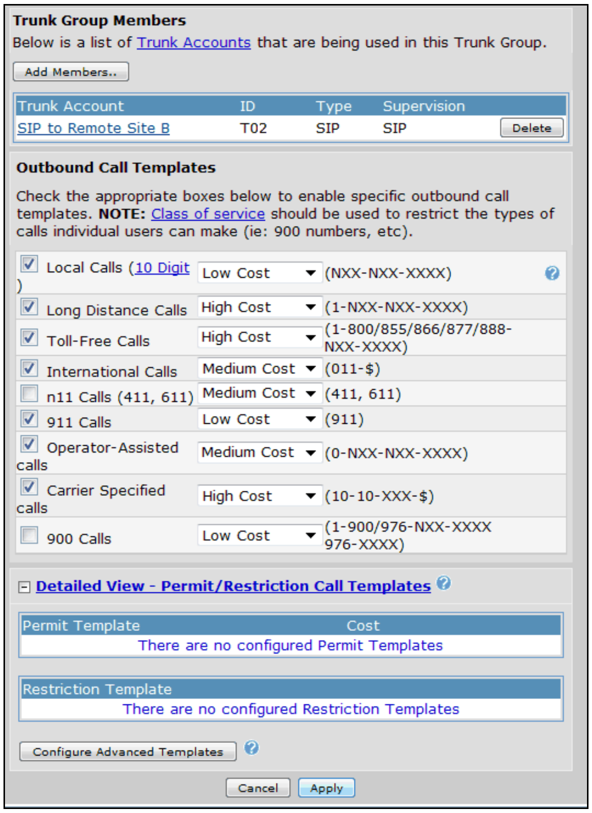


Add Members to Trunk Group

Click on one or more rows to select Trunk Accounts to add as members of this trunk group. **Hint: Use the Shift key to select ranges.**

□	Cbeyond	T15	SIP	SIP
□	test4	T16	SIP	SIP
□	Local Telco2	T18	Analog	Loop Start
□	abb	T19	SIP	SIP
□	<No Trunk Name Set>	T40	SIP	SIP
□	Service Provider Trunk	T03	SIP	SIP
☑	SIP to Remote Site B	T02	SIP	SIP

4. The new trunk group members appear in the list of trunk group members, and you can now configure the **Outbound Call Templates** for the trunk group. Outbound call templates are the types of calls to allow from this trunk. Select the appropriate boxes to enable specific outbound call capabilities for this trunk group, and select the cost for each call type from the drop-down menu. In the following example, the local calls are set to 10-digit dialing calls. To specify if local calls are 10-digit or 7-digit, specify the local dialing type under **System Setup** > **Dial Plan**. Select **Apply** when you have configured the outbound call templates for the trunk group.



Trunk Group Members

Below is a list of Trunk Accounts that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision	
SIP to Remote Site B	T02	SIP	SIP	Delete

Outbound Call Templates

Check the appropriate boxes below to enable specific outbound call templates. **NOTE:** Class of service should be used to restrict the types of calls individual users can make (ie: 900 numbers, etc).

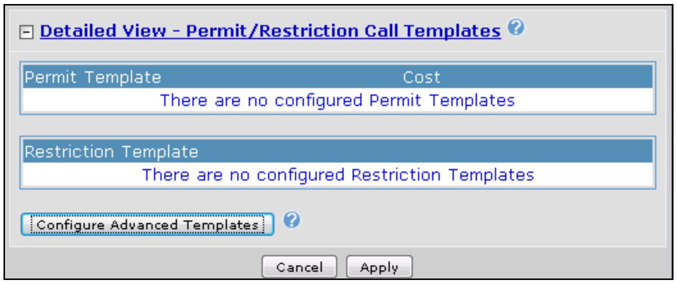
☑	Local Calls (10 Digit)	Low Cost	(NXX-NXX-XXXX)
☑	Long Distance Calls	High Cost	(1-NXX-NXX-XXXX)
☑	Toll-Free Calls	High Cost	(1-800/855/866/877/888-NXX-XXXX)
☑	International Calls	Medium Cost	(011-$)
☐	n11 Calls (411, 611)	Medium Cost	(411, 611)
☑	911 Calls	Low Cost	(911)
☑	Operator-Assisted calls	Medium Cost	(0-NXX-NXX-XXXX)
☑	Carrier Specified calls	High Cost	(10-10-XXX-$)
☐	900 Calls	Low Cost	(1-900/976-NXX-XXXX 976-XXXX)

⊟ **Detailed View - Permit/Restriction Call Templates**

Permit Template	Cost
There are no configured Permit Templates	

Restriction Template
There are no configured Restriction Templates

5. After you have applied the outbound call templates for the trunk group, you will need to configure an advanced permit template for the SIP networking trunk. The advanced permit template allows the trunk to accept calls from the extensions of the remote NetVanta 7000 Series unit. If you are configuring a trunk group for the remote unit, use the extension of the main site. In the following example, the trunk group is configured to accept calls from the 4000 extension (**4xxx**) with no cost. To create the advanced template, select **Configure Advanced Templates** from the trunk group configuration menu.

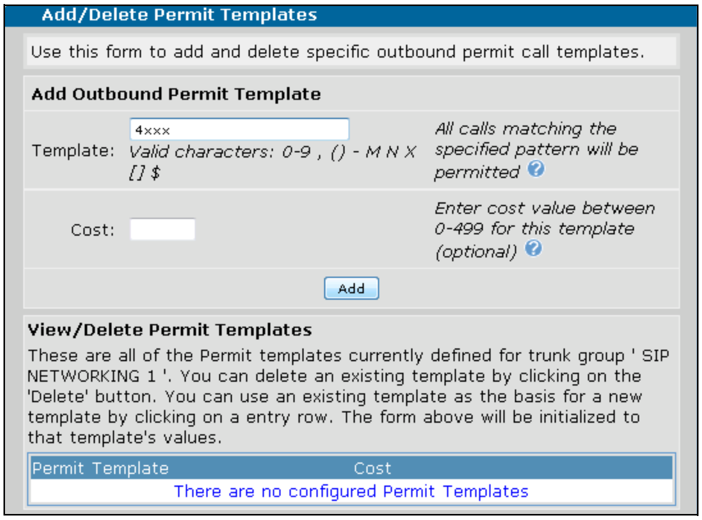


⊟ Detailed View - Permit/Restriction Call Templates

Permit Template	Cost
There are no configured Permit Templates	

Restriction Template
There are no configured Restriction Templates

6. Next, specify the call template to match in the **Template** field in the **Add/Delete Permit Templates** menu and select **Add**. The template will appear in the list at the bottom of the menu.



Add/Delete Permit Templates

Use this form to add and delete specific outbound permit call templates.

Add Outbound Permit Template

Template: 4xxx
Valid characters: 0-9 , () - M N X [] $
All calls matching the specified pattern will be permitted

Cost:
Enter cost value between 0-499 for this template (optional)

View/Delete Permit Templates

These are all of the Permit templates currently defined for trunk group ' SIP NETWORKING 1 '. You can delete an existing template by clicking on the 'Delete' button. You can use an existing template as the basis for a new template by clicking on a entry row. The form above will be initialized to that template's values.

Permit Template	Cost
There are no configured Permit Templates	

7. The SIP networking SIP trunk, and the SIP networking trunk group are now configured. You can now continue to configure additional SIP trunks for SIP networking with other AOS devices.

Configuring SIP Networking between NetVanta 7000 Series Products using the CLI

The following example configures the same SIP networking SIP trunk between two NetVanta 7000 Series products as configured using the GUI, only this example is configured using the CLI. Configuration occurs on the NetVanta 7000 Series unit at the main site, as well as the NetVanta 7000 Series unit(s) at the remote site(s). The CLI example is a sample configuration only, and does not include details of each command used in the configuration. For details about commands used to configure SIP trunks and trunk groups, refer to the *AOS Command Reference Guide* available online at http://kb.adtran.com (article number 2219).

To configure a SIP trunk between NetVanta 7000 Series products using the CLI, follow these steps:

1. Telnet to the NetVanta 7000 Series unit at the main site, and enter the Global Configuration mode.
2. Create the SIP networking SIP trunk using the **voice trunk** command from the Global Configuration mode prompt. This command enters the trunk's configuration mode, where you can specify a description for the trunk (**SIP to Remote Site B**), disable external call rejection, specify the SIP server (IP address of the unit to which the SIP trunk connects), and specify the SIP FROM header as local. The following example configures the SIP trunk between the NetVanta 7000 Series unit at the main site and the unit at the Remote Site B.

```
voice trunk T02 type sip
  description “SIP to Remote Site B”
  no reject-external
  default-ring-cadence internal
  sip-server primary 192.68.101.10
  grammar from host local
```

3. After creating the SIP trunk on the NetVanta 7000 Series unit at the main site, create the trunk group for the SIP trunk using the **voice grouped-trunk** command from the Global Configuration mode prompt. This command enters the trunk group's configuration mode, where you can specify the trunks added to the group, the outbound call templates for the group, and the advanced permit template for the group. The advanced template should allow calls from the extensions used at the site to which you are connecting. In this case, the trunk group allows all calls from the 4000 extensions (**4xxx**) used at Remote Site B. The following example configures the trunk group for the SIP trunk between the NetVanta 7000 Series unit at the main site and the unit at the Remote Site B.

```
voice grouped-trunk SIP Networking 1
  trunk T02
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
  accept 4xxx cost 0
```

4. Next you will configure the SIP trunk and SIP trunk group on the remote NetVanta 7000 Series unit using the same commands. Make sure to remember that the SIP server address will be the IP address of the NetVanta 7000 unit at the main site, and that the advanced call template for the trunk group should include the extensions used at the main site (**2xxx**). The following example is the configuration of the SIP trunk on the remote unit, and the trunk's corresponding trunk group.

```
voice trunk T03 type sip
  description “SIP to Main Site A”
  no reject-external
  sip-server primary 192.68.101.1
  grammar from host local
```

```
voice grouped-trunk SIP Networking 1
  trunk T03
  accept NXX-NXX-XXXX cost 0
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  accept 0-NXX-NXX-XXXX cost 200
  accept 10-10-XXX-$ cost 350
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
  accept 2xxx cost 0
```

5. Repeat Steps 1 through 4 for any additional SIP trunks you need to configure between NetVanta 7000 Series platforms.

Configuring a SIP Network between NetVanta 7000 and IP Gateways

SIP networking can also be used between the NetVanta 7000 Series product and IP business gateways at remote locations. IP business gateways are typically Total Access 900(e) or NetVanta 6355 products. *Figure 4 on page 6* describes the network topology for this type of SIP networking. This application functions similarly to a single PBX, in which each remote user registers back to the NetVanta 7000 Series using either SIP transparent proxy or directly using analog phones. The phones at the remote locations rely on the main site to provide voicemail and auto attendant services for incoming calls. At the remote sites, the SIP trunks facing the main site are mainly used for inbound calls. Typically, the outbound trunks configured at remote sites connect to the PSTN and are used for survivability purposes only.

There are a few things to keep in mind when configuring SIP networking between NetVanta 7000 Series products and an IP business gateway:

- The maximum number of users for each installed NetVanta 7000 Series unit is 100. All users connected directly or through SIP proxy count as part of the total sum of users.
- All remote users connected through SIP proxy to the main site have access to all the NetVanta 7000 Series features, and function as thought they are located at the main site.
- The NetVanta 7000 Series unit at the main site must have call routing and transfer modes set to **Local**, and the platforms at the remote sites must have voice feature and transfer modes set to **Network**.
- When configuring SIP networking with IP business gateways, you also will have to configure SIP proxy, a VPN tunnel, and possibly LCR.

Configuring SIP Networking with an IP Business Gateway using the GUI

To configure the SIP networking trunks between the NetVanta 7000 Series and an IP business gateway, follow these steps:

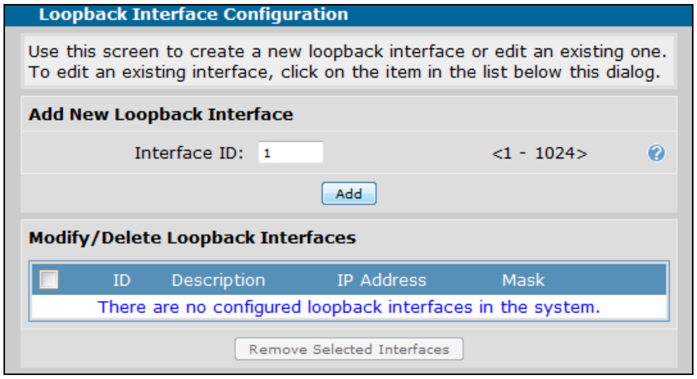
1. Plan the extensions used at each site. These extensions should use wildcards for easy matching, and each location should have their own extensions. For example, the main site can use extensions **2xxx**, Remote Site B can use extensions **3xxx**, and Remote Site C can use extensions **4xxx**.
2. Configure the media gateway for all units (remote and main).
3. Configure the IP phones and remote voice users for the remote unit(s) on the NetVanta 7000 Series unit at the main site.
4. Configure the Dynamic Host Control Protocol (DHCP) pool for the remote unit.
5. Configure QoS. The QoS configuration is done on both the NetVanta 7000 Series unit at the main site, and any AOS units at the remote sites.
6. Configure the VPN tunnels between sites.
7. Configure the SIP trunk and trunk groups for the remote unit(s).
8. Configure the PSTN trunks and trunk groups for the remote unit(s). These trunks are used for LCR and survivability.
9. Enable SIP proxy on the AOS unit(s) in the SIP network.
10. Configure the remote unit's analog users.
11. Configure the SIP trunk(s) on the NetVanta 7000 Series unit at the main site.
12. Configure the SIP trunk group(s) on the NetVanta 7000 Series unit at the main site. There are different variations for trunk group configuration, depending on the type of LCR you want to implement.

Configure Media Gateway for All Units

All units (remote and main) must have a media gateway configured. The media gateway converts digital media streams between the PSTN and the PBX (NetVanta 7000 Series unit). For this application, because inbound calls from the trunks at remote sites are routed through the NetVanta 7000 Series unit at the main site, the media gateway on all units is configured to be the loopback interface on all units.

To configure the media gateway using the GUI, connect to the GUI for each unit and follow these steps:

1. Navigate to **Data** > **Loopback Interfaces**. Create a new loopback interface by selecting **Add** on the **Loopback Interface Configuration** menu.



Loopback Interface Configuration

Use this screen to create a new loopback interface or edit an existing one. To edit an existing interface, click on the item in the list below this dialog.

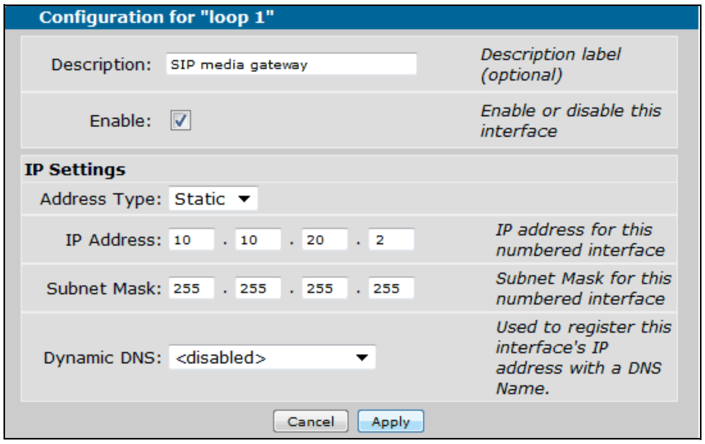
Add New Loopback Interface

Interface ID: 1 <1 - 1024>

Modify/Delete Loopback Interfaces

□	ID	Description	IP Address	Mask
There are no configured loopback interfaces in the system.				

2. In the next menu, enter a description for the interface, and enable the interface by selecting the **Enable** checkbox. Next, select **Static** from the **Address Type** drop-down menu, and enter the IP address and subnet mask of the VLAN associated with the unit you are configuring. In the example below, the IP address and subnet mask are set to the VLAN 2 (voice VLAN) settings for the NetVanta 7000 Series unit. Specify that **Dynamic DNS** is disabled, and select **Apply**.



Configuration for "loop 1"

Description: SIP media gateway — *Description label (optional)*

Enable: ☑ — *Enable or disable this interface*

IP Settings

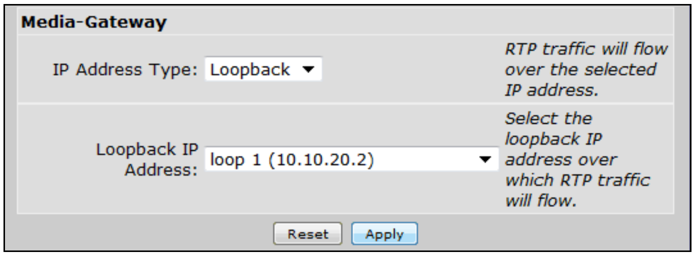
Address Type: Static

IP Address: 10 . 10 . 20 . 2 — *IP address for this numbered interface*

Subnet Mask: 255 . 255 . 255 . 255 — *Subnet Mask for this numbered interface*

Dynamic DNS: <disabled> — *Used to register this interface's IP address with a DNS Name.*

3. After creating the loopback interface, navigate to **Data** > **VLANs**. Select the appropriate VLANs for SIP networking on the unit (any IP interfaces) from the VLAN list. In the **VLAN Configuration** menu, scroll to the **Media-Gateway** section of the menu, and specify that the **IP Address Type** is **Loopback**, and then select the loopback interface you just created from the **Loopback IP Address** list. Then select **Apply**.

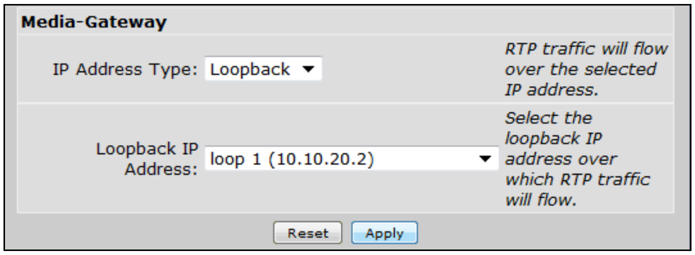


Media-Gateway

IP Address Type: Loopback — *RTP traffic will flow over the selected IP address.*

Loopback IP Address: loop 1 (10.10.20.2) — *Select the loopback IP address over which RTP traffic will flow.*

4. After assigning the loopback interface to all applicable VLANs on the unit, you must also set the Ethernet interface of the unit to use the loopback media gateway. Navigate to **System** > **Physical Interfaces**, and select the appropriate Ethernet interface from the list (in the example below, Ethernet interface **eth 0/0** with IP address **10.10.20.2** is used). In the interface configuration menu, scroll to the the **Media-Gateway** section of the menu, and specify that the **IP Address Type** is **Loopback**, and then select the loopback interface you just created from the **Loopback IP Address** list. Then select **Apply**.



Media-Gateway

IP Address Type: Loopback

RTP traffic will flow over the selected IP address.

Loopback IP Address: loop 1 (10.10.20.2)

Select the loopback IP address over which RTP traffic will flow.

NOTE *If Ethernet interface 0/0 is used for a service provider SIP trunk, then the media gateway should be set to **Primary** from the drop-down menu.*

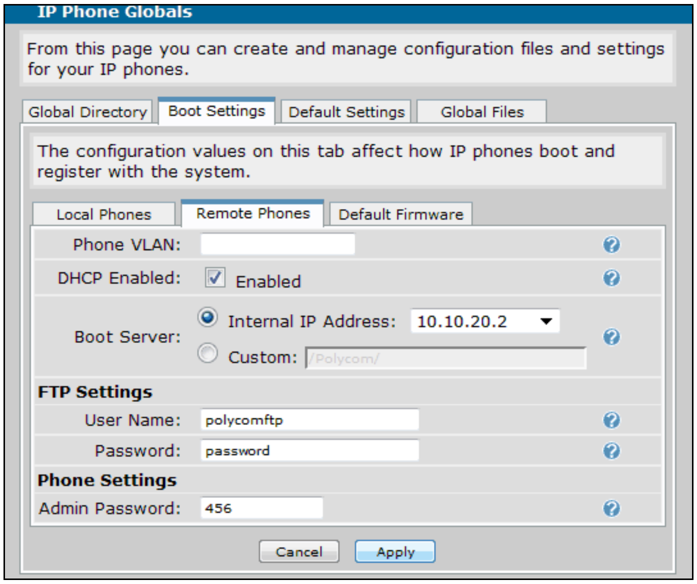
5. You have now specified that the loopback interface is used for all IP interfaces on the unit. Repeat Steps 1 through 4 for all units that will be networked.

Configure the IP Phones and Users for Remote Unit(s)

After configuring the media gateway on all units, you must configure the IP phones and the users for each of the remote units. Because the loopback interface is being used as the media gateway, the phones must be configured to use the loopback IP address as their SIP server (in this example configuration, the loopback IP address is **10.10.20.2**). To configure the remote IP phones and users, follow these steps:

1. Connect to the NetVanta 7000 Series unit GUI and navigate to **Voice** > **Stations** > **IP Phone Globals**. Then select **Boot Settings** and **Remote Phones** tabs. In this menu, you will configure the remote SIP phones to download a different configuration file than SIP phones connected locally to the NetVanta 7000 Series unit at the main site. This allows flexibility in the configuration of phones in different locations. The phones should be configured to use DHCP and contact the boot server at the NetVanta 7000 Series' loopback IP address (**10.10.20.2**). Select the **DHCP Enabled** checkbox and

select the **Internal IP Address** from the drop-down menu. After you have made these changes, select **Apply**.



From this page you can create and manage configuration files and settings for your IP phones.

The configuration values on this tab affect how IP phones boot and register with the system.

Phone VLAN:

DHCP Enabled: ☑ Enabled

Boot Server: ● Internal IP Address: 10.10.20.2 ○ Custom: /Polycom/

FTP Settings

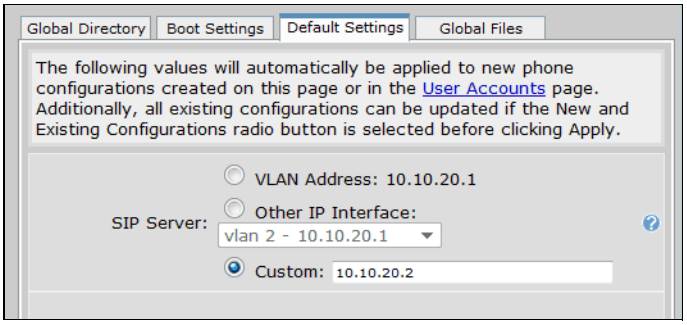
User Name: polycomftp

Password: password

Phone Settings

Admin Password: 456

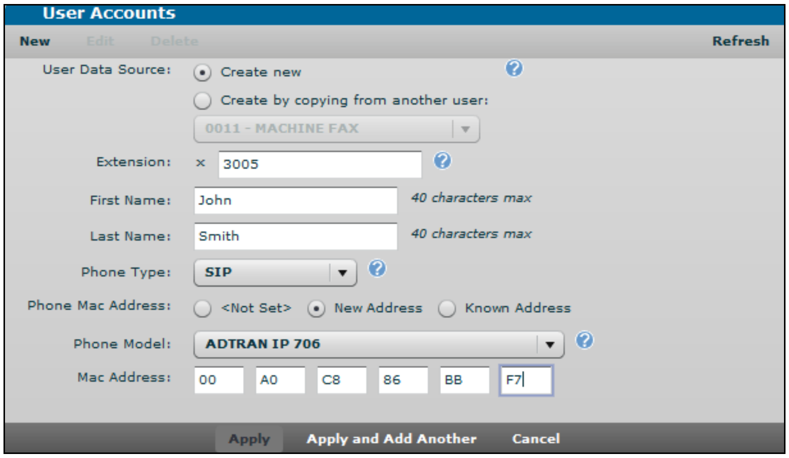
2. Next, select the **Default Settings** tab and verify that the **SIP Server** address is set to the loopback interface's IP address. Select **Apply**.



The following values will automatically be applied to new phone configurations created on this page or in the User Accounts page. Additionally, all existing configurations can be updated if the New and Existing Configurations radio button is selected before clicking Apply.

SIP Server: ○ VLAN Address: 10.10.20.1 ○ Other IP Interface: vlan 2 - 10.10.20.1 ● Custom: 10.10.20.2

3. Configure the remote voice users by navigating to **Voice** > **Stations** > **User Accounts**. Create a new user by selecting **New**, and enter the remote user's information. You will need to specify the phone's extension, the first and last name of the user, the phone type as **SIP**, and enter the phone's MAC address. Select **Apply** or **Apply and Add Another**. Repeat this step for each user that you need to add.



User Data Source: ● Create new ○ Create by copying from another user: 0011 - MACHINE FAX

Extension: × 3005

First Name: John *40 characters max*

Last Name: Smith *40 characters max*

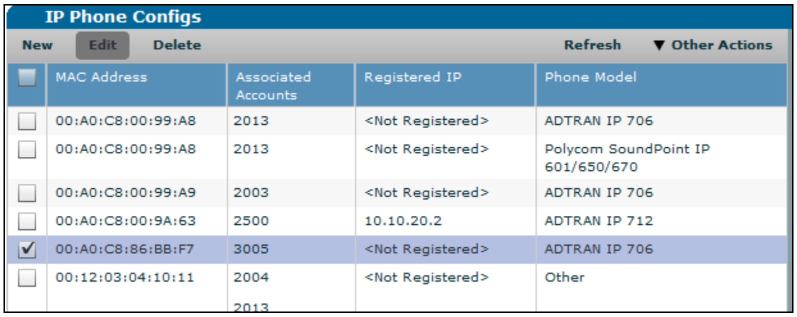
Phone Type: SIP

Phone Mac Address: ○ <Not Set> ● New Address ○ Known Address

Phone Model: ADTRAN IP 706

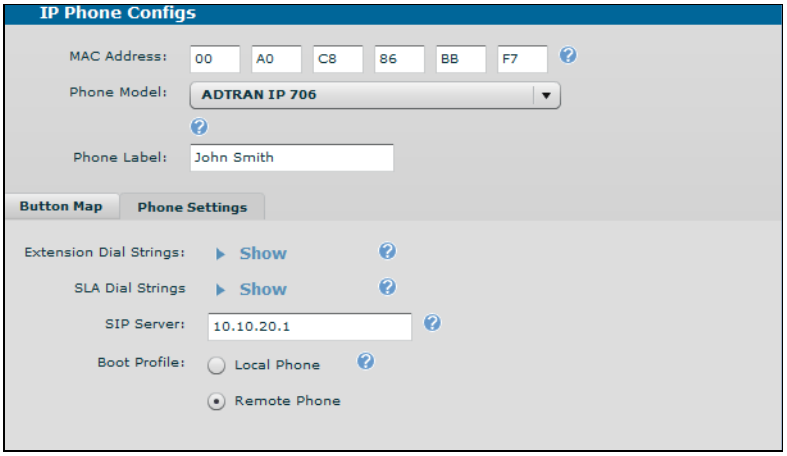
Mac Address: 00 A0 C8 86 BB F7

4. After creating the remote voice users, you must configure the remote user to use the remote user profile. Navigate to **Voice > Stations** > **IP Phone Configs** in the NetVanta 7000 Series unit. Select the checkbox next the MAC address of the remote voice user, and select **Edit**.



□	MAC Address	Associated Accounts	Registered IP	Phone Model
□	00:A0:C8:00:99:A8	2013	<Not Registered>	ADTRAN IP 706
□	00:A0:C8:00:99:A8	2013	<Not Registered>	Polycom SoundPoint IP 601/650/670
□	00:A0:C8:00:99:A9	2003	<Not Registered>	ADTRAN IP 706
□	00:A0:C8:00:9A:63	2500	10.10.20.2	ADTRAN IP 712
☑	00:A0:C8:86:BB:F7	3005	<Not Registered>	ADTRAN IP 706
□	00:12:03:04:10:11	2004 2013	<Not Registered>	Other

5. In the configuration menu that appears, select the **Phone Settings** tab and change the **Boot Profile** to **Remote Phone**. Then select **Apply**.



MAC Address: 00 A0 C8 86 BB F7

Phone Model: ADTRAN IP 706

Phone Label: John Smith

Extension Dial Strings: ▸ Show

SLA Dial Strings ▸ Show

SIP Server: 10.10.20.1

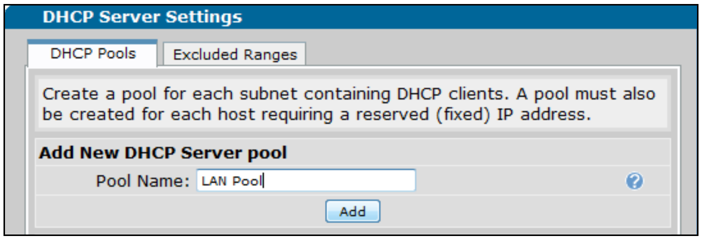
Boot Profile: ○ Local Phone ● Remote Phone

6. Repeat these steps for each remote voice user and IP phone you have at the remote locations in the SIP network.

Configure DHCP Pool for Remote Unit(s)

The DHCP pools for the IP phones on the remote unit(s) should be set up to point to the WAN interface of the NetVanta 7000 Series unit at the main site for the boot server. You will need to configure a DHCP pool for the LAN and one for VoIP, so each remote unit should have two configured DHCP pools. Configure the DHCP pools on the remote unit(s) following these steps:

1. Connect to the remote unit's GUI, and navigate to **System** > **DHCP Server**. On the **DHCP Pools** tab, enter a **Pool Name** in the appropriate field and select **Add**.

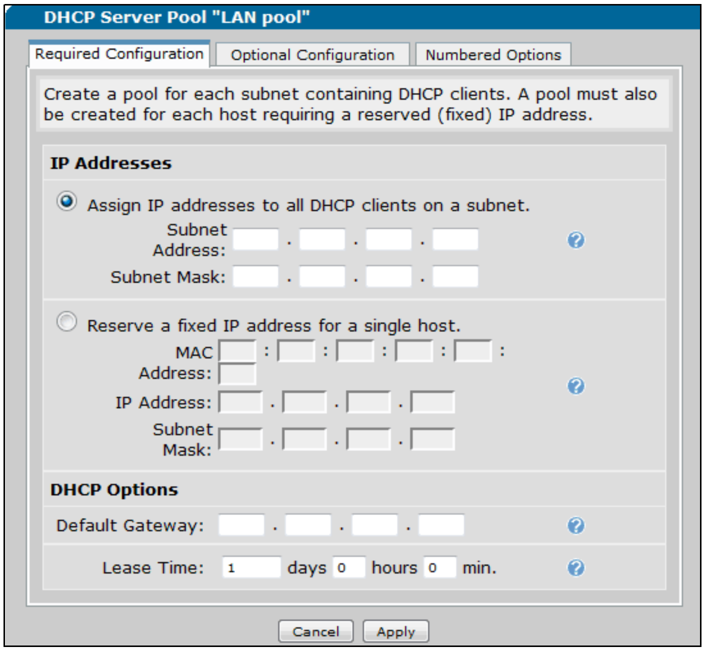


Create a pool for each subnet containing DHCP clients. A pool must also be created for each host requiring a reserved (fixed) IP address.

Add New DHCP Server pool

Pool Name: LAN Pool

2. Configure the DHCP pool settings in the **DHCP Server Pool** menu. You will need to specify that DHCP assign IP addresses for all DHCP clients on the subnet and the default gateway, using the **Required Configuration** tab.



Create a pool for each subnet containing DHCP clients. A pool must also be created for each host requiring a reserved (fixed) IP address.

IP Addresses

● Assign IP addresses to all DHCP clients on a subnet.

Subnet Address: . . .

Subnet Mask: . . .

○ Reserve a fixed IP address for a single host.

MAC Address: : : : : :

IP Address: . . .

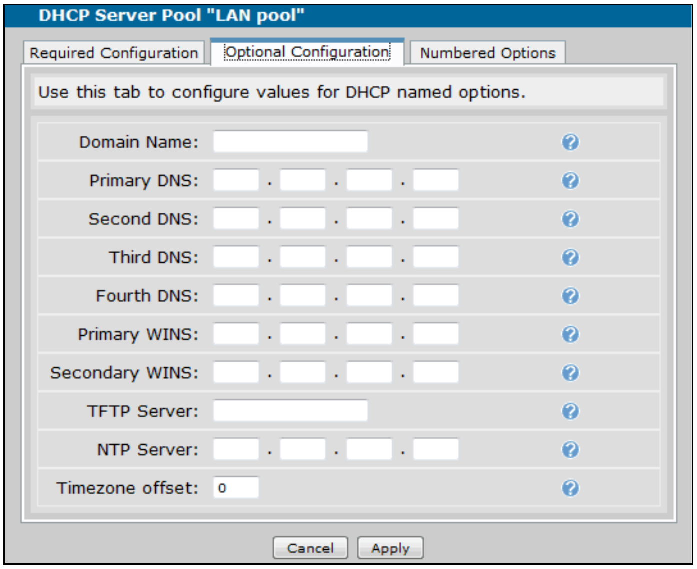
Subnet Mask: . . .

DHCP Options

Default Gateway: . . .

Lease Time: 1 days 0 hours 0 min.

3. Next, select the **Optional Configuration** tab and enter the primary DNS server, the TFTP server, NTP server, and the timezone offset.



DHCP Server Pool "LAN pool"

Required Configuration | Optional Configuration | Numbered Options

Use this tab to configure values for DHCP named options.

Domain Name:

Primary DNS: . . .

Second DNS: . . .

Third DNS: . . .

Fourth DNS: . . .

Primary WINS: . . .

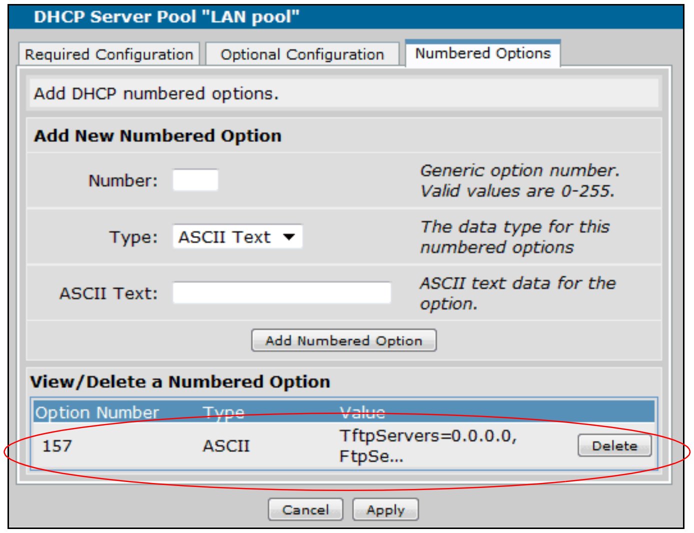
Secondary WINS: . . .

TFTP Server:

NTP Server: . . .

Timezone offset: 0

4. Finally, select the **Numbered Options** tab and enter any DHCP numbered options necessary for your network. For ADTRAN IP phones, you must configure numbered option **157**, with a **Type** of **ASCII Text**, and an **ASCII Text** value of:
TftpServers=0.0.0.0,FtpServers=10.10.20.1:/ADTRAN,FtpLogin=polycomftp,FtpPassword=password,Layer2Tagging=True,VlanID=2.
These settings are used for the ADTRAN IP phones and contains the boot server address, FTP login, and VLAN ID. For Polycom IP phones the TFTP server field must contain the boot server IP address. Select **Apply** when you have entered all the necessary DHCP pool configuration information.



DHCP Server Pool "LAN pool"

Required Configuration | Optional Configuration | Numbered Options

Add DHCP numbered options.

Add New Numbered Option

Number: — *Generic option number. Valid values are 0-255.*

Type: ASCII Text — *The data type for this numbered options*

ASCII Text: — *ASCII text data for the option.*

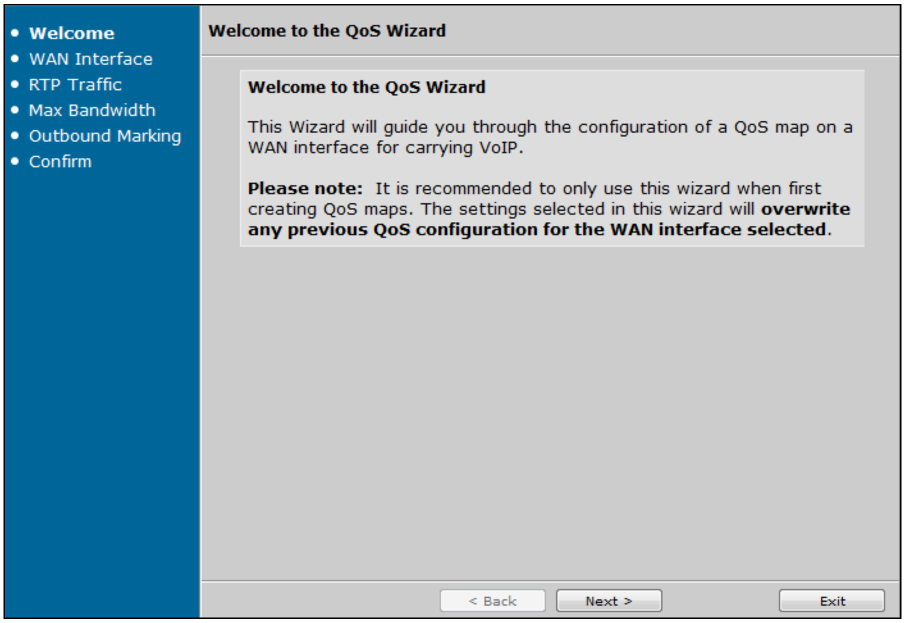
View/Delete a Numbered Option

Option Number	Type	Value	
157	ASCII	TftpServers=0.0.0.0, FtpSe...	Delete

5. Repeat Steps 1 through 4 for each DHCP pool on each remote unit.

Configure QoS

QoS is a requirement anywhere time sensitive traffic, such as VoIP, will be using the same bandwidth as a user's regular data traffic. QoS should be configured on all units (remote and main) to ensure voice quality. The QoS parameters should match between the units. Configuring QoS on the unit can be done using the **QoS Wizard**. To access the QoS wizard, connect to the AOS unit's GUI and navigate to **Data** > **Router** > **QoS Wizard**.



Welcome to the QoS Wizard

This Wizard will guide you through the configuration of a QoS map on a WAN interface for carrying VoIP.

Please note: It is recommended to only use this wizard when first creating QoS maps. The settings selected in this wizard will **overwrite any previous QoS configuration for the WAN interface selected.**

The wizard is particularly helpful if you have not previously configured any QoS maps on the unit. Using the wizard you will specify the WAN interface to which the QoS map applies, assign traffic shaping criteria, identify traffic matching criteria, configure the maximum bandwidth, and assign packet marking. Follow the prompts of the wizard to configure the QoS settings. If you already have QoS maps configured on the unit, select **QoS Maps** (rather than the wizard) to configure a new map or edit a previously configured one. Otherwise, the wizard will overwrite any existing QoS maps.

Make sure to configure the QoS parameters for all AOS units in the SIP network.

NOTE *For more information regarding QoS configurations for VoIP, refer to the training video **Configuring QoS for VoIP**, available online at http://kb.adtran.com (ADTRAN's Knowledge Base article 3091).*

Configure VPN Tunnels between SIP Networked Sites

VPN tunnels are necessary for SIP networking implementation because they assure call signaling and audio is passed between networked sites. VPN tunnel configuration is comprised of a number of configuration steps, and intermingles with the configuration steps for the SIP networking configuration between the sites. The following steps are necessary to configure the VPN tunnels:

1. Create Generic Route Encapsulation (GRE) tunnel interfaces. These are necessary so that site-to-site voice traffic has a separate media gateway IP address than SIP traffic that will not traverse a tunnel.
2. Point routes for far-end networks to the GRE tunnel interface. Routes should be created so that traffic destined for far-end networks will use the GRE tunnel.
3. Create *allow* firewall rules for physical and GRE tunnel interfaces. In order for traffic between the sites to be allowed through the ADTRAN devices, specific *allow* policies must be added for traffic that is destined for the tunnel interface. Without these policies, NAT will be performed on the site-to-site traffic introducing processing delay and unnecessary complexity without benefit.
4. Change the media gateway for each tunnel interface to the loopback interface.
5. Create SIP trunks and associated trunk groups for each remote location which will specify the remote loopback interface IP as the SIP server. The trunk group specifies the phone numbers that are to be routed to this SIP trunk.

> NOTE
>
> *These GRE tunnel SIP trunks and trunk groups are different than the SIP trunks and trunk groups created for non-tunnel SIP networking. At the end of the SIP networking configuration, you will have SIP trunks and trunk groups for both tunnel traffic (described in this section) and non-tunnel traffic (described in Configure PSTN Trunk and Trunk Groups on Remote Units on page 53). These trunks and trunk groups are configured on both the NetVanta 7000 Series unit at the main site and each remote AOS device.*

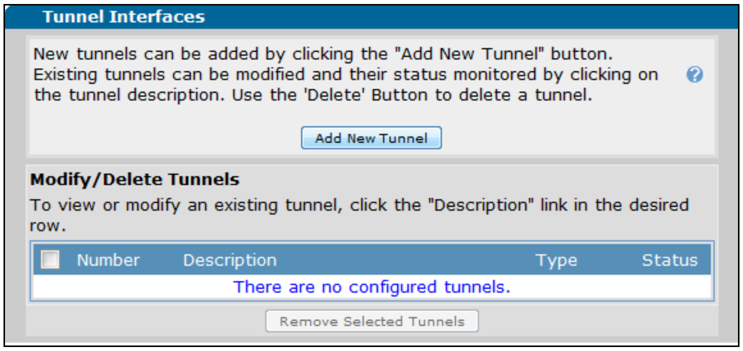
6. Configure VPN matching for GRE traffic. In order to secure the traffic routed over the GRE tunnel between sites, a VPN tunnel can be configured to encrypt the traffic. This traffic is sourced from the WAN IP address and destined for the far-end WAN IP address as protocol 47 (GRE).
7. Configure QoS for traffic matching on Differentiated Services Code Point (DSCP) values. Since the standard DSCP values are preserved through both the GRE and VPN encapsulation, these values can be matched to ensure that voice traffic is prioritized within the AOS device.
8. Create route maps for use with SIP networking. A route map can be used to make sure that RTP traffic from a remote site, and destined for a SIP server with a public IP address, is routed across the GRE tunnel rather than using the Internet connection outside the tunnel. This is necessary since the SIP server and corresponding media gateway used for PSTN access only expects SIP and RTP from the main site's public IP address.

To configure the VPN tunnel for SIP networking, follow these steps:

1. Create the GRE Tunnel Interfaces

GRE tunnel interfaces should be configured on the NetVanta 7000 Series unit at the main site, as well as any AOS devices at the remote sites. To configure the GRE tunnel interface using the GUI, follow these steps:

A. Connect to the unit's GUI and navigate to **Data** > **Router** > **Tunnels**. Select **Add New Tunnel**.



Tunnel Interfaces

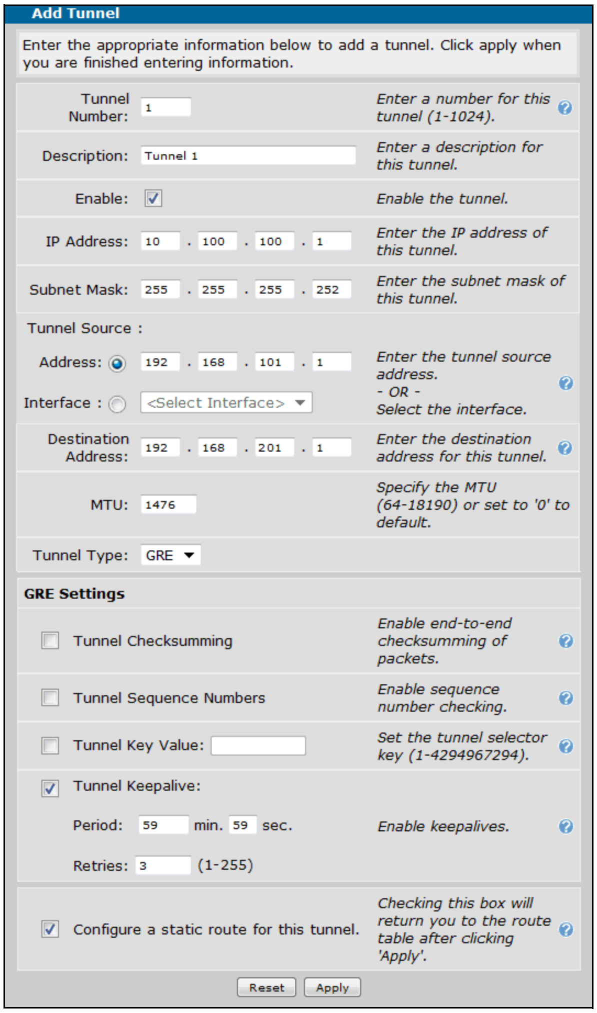
New tunnels can be added by clicking the "Add New Tunnel" button. Existing tunnels can be modified and their status monitored by clicking on the tunnel description. Use the 'Delete' Button to delete a tunnel.

Modify/Delete Tunnels

To view or modify an existing tunnel, click the "Description" link in the desired row.

□ Number	Description	Type	Status
There are no configured tunnels.			

B. In the **Add Tunnel** menu, specify the **IP address** of the tunnel (the GRE IP address for the tunnel), the **Tunnel Source** address for the tunnel (WAN IP address of the unit), the **Destination Address** for the tunnel (WAN IP address of unit to which the tunnel connects), and the tunnel type as **GRE**. You will also select the checkbox to **Configure a Static Route for this Tunnel**. This option will take you to the route table, where you can enter the route to be used (Step 2 in tunnel configuration). The following example uses an IP address of **10.100.100.1 255.255.255.252** for the GRE tunnel address, a source address of **192.168.101.1**, and a destination address of **192.168.201.1**. In addition, the the **MTU** is set to **1476** and the **Tunnel Keepalive** is set to **59** minutes and **59** seconds. Select **Apply** when you have entered the tunnel's settings.



Add Tunnel

Enter the appropriate information below to add a tunnel. Click apply when you are finished entering information.

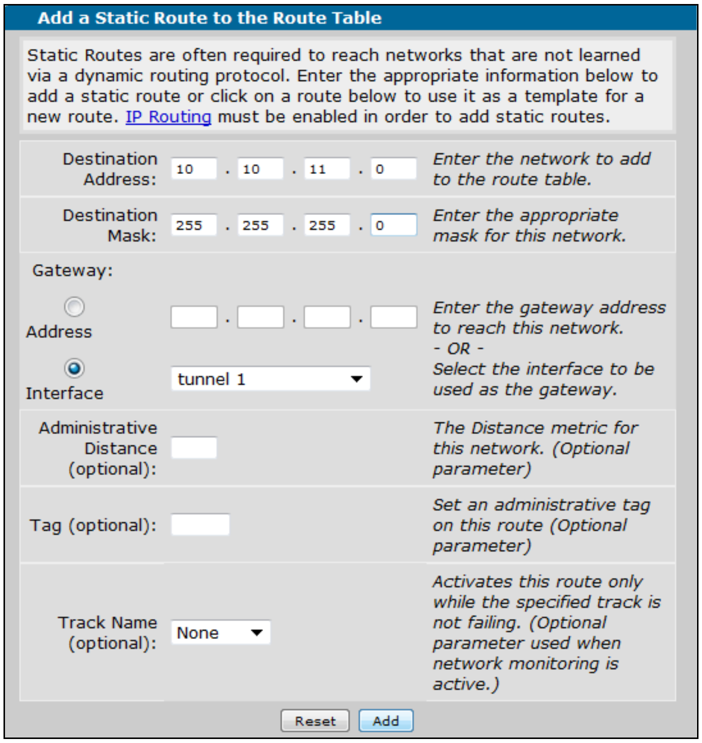
Tunnel Number:	1	*Enter a number for this tunnel (1-1024).*
Description:	Tunnel 1	*Enter a description for this tunnel.*
Enable:	☑	*Enable the tunnel.*
IP Address:	10 . 100 . 100 . 1	*Enter the IP address of this tunnel.*
Subnet Mask:	255 . 255 . 255 . 252	*Enter the subnet mask of this tunnel.*
Tunnel Source :		
Address: ●	192 . 168 . 101 . 1	*Enter the tunnel source address.*
		- OR -
Interface : ○	<Select Interface>	*Select the interface.*
Destination Address:	192 . 168 . 201 . 1	*Enter the destination address for this tunnel.*
MTU:	1476	*Specify the MTU (64-18190) or set to '0' to default.*
Tunnel Type:	GRE	

GRE Settings

□ Tunnel Checksumming		*Enable end-to-end checksumming of packets.*
□ Tunnel Sequence Numbers		*Enable sequence number checking.*
□ Tunnel Key Value:		*Set the tunnel selector key (1-4294967294).*
☑ Tunnel Keepalive:		
Period:	59 min. 59 sec.	*Enable keepalives.*
Retries:	3 (1-255)	
☑ Configure a static route for this tunnel.		*Checking this box will return you to the route table after clicking 'Apply'.*

2. Point Routes for Far-End Networks to GRE Tunnel Interface

A. Routes are created to point traffic destined for far-end networks to the GRE tunnel. If you selected **Configure a static route for this tunnel** in the **Add Tunnel** menu, you should have already been redirected to the route table. If not, navigate to **Data** > **Router** > **Route Table**. Use the **Add a Static Route to the Route Table** menu to configure the static routes for each tunnel. For the main site configuration, the route should include a separate IP route for each remote device. For the remote sites, you can use a summary tunnel route. Enter the **Destination Address** and **Destination Mask** for the route, and specify that the tunnel interface is used as the **Gateway**. Select **Add** to add the route to the route table.



Add a Static Route to the Route Table

Static Routes are often required to reach networks that are not learned via a dynamic routing protocol. Enter the appropriate information below to add a static route or click on a route below to use it as a template for a new route. IP Routing must be enabled in order to add static routes.

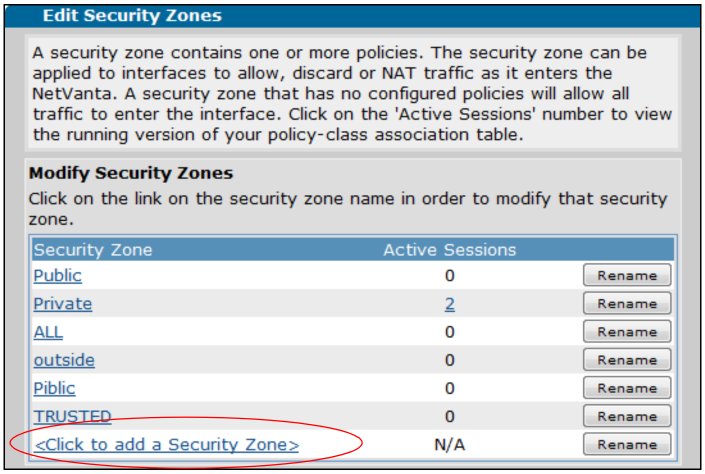
Destination Address:	10 . 10 . 11 . 0	*Enter the network to add to the route table.*
Destination Mask:	255 . 255 . 255 . 0	*Enter the appropriate mask for this network.*
Gateway:		
○ Address	. . .	*Enter the gateway address to reach this network.* *- OR -*
● Interface	tunnel 1 ▼	*Select the interface to be used as the gateway.*
Administrative Distance (optional):		*The Distance metric for this network. (Optional parameter)*
Tag (optional):		*Set an administrative tag on this route (Optional parameter)*
Track Name (optional):	None ▼	*Activates this route only while the specified track is not failing. (Optional parameter used when network monitoring is active.)*

B. Repeat Steps 1 and 2 for each device in the SIP network.

3. Configure the Firewall for the Physical and GRE Tunnel Interfaces

You must create specific *allow* policies for the traffic destined for the tunnel interface so that NAT is not performed on the site-to-site traffic. These policies must be applied to all units (remote and main) and on all VLANs used in the tunnel. To create the allow policies, follow these steps:

A. Connect to the unit's GUI and navigate to **Data** > **Router** > **Firewall** > **Security Zones**. In the **Edit Security Zones** menu, select **<Click to add a Security Zone>**.



Edit Security Zones

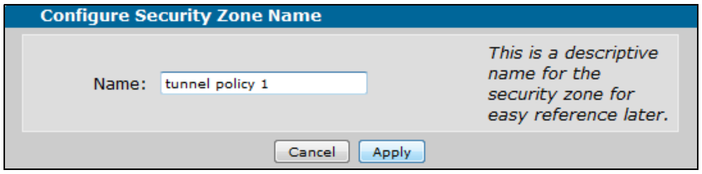
A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

Security Zone	Active Sessions	
Public	0	Rename
Private	2	Rename
ALL	0	Rename
outside	0	Rename
Piblic	0	Rename
TRUSTED	0	Rename
<Click to add a Security Zone>	N/A	Rename

B. Enter a name for the security zone in the **Configure Security Zone Name** menu and select **Apply**.

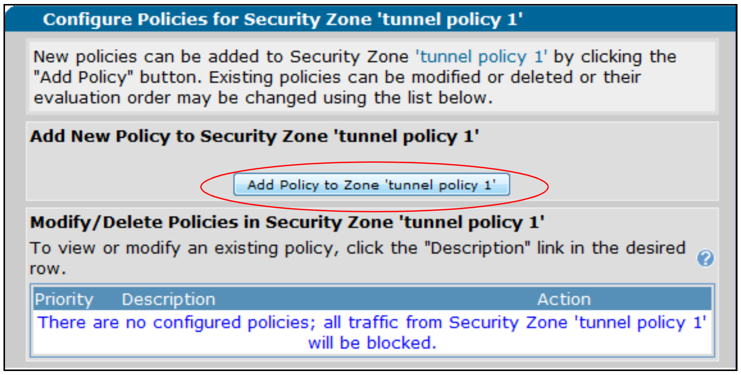


Configure Security Zone Name

Name: tunnel policy 1

This is a descriptive name for the security zone for easy reference later.

C. Select **Add Policy to Zone 'tunnel policy 1'** in the **Configure Policies** menu. If you do not create a new policy, all traffic from this security zone is blocked.



Configure Policies for Security Zone 'tunnel policy 1'

New policies can be added to Security Zone 'tunnel policy 1' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

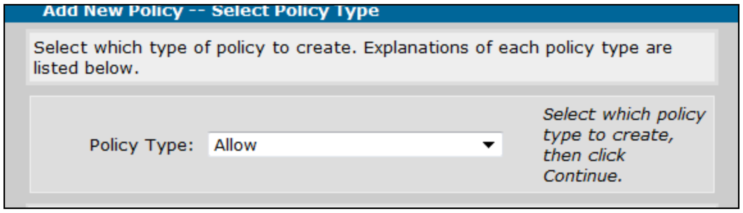
Add New Policy to Security Zone 'tunnel policy 1'

Modify/Delete Policies in Security Zone 'tunnel policy 1'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action
There are no configured policies; all traffic from Security Zone 'tunnel policy 1' will be blocked.		

D. Select **Allow** as the **Policy Type** in the **Add New Policy** menu and select **Continue**.



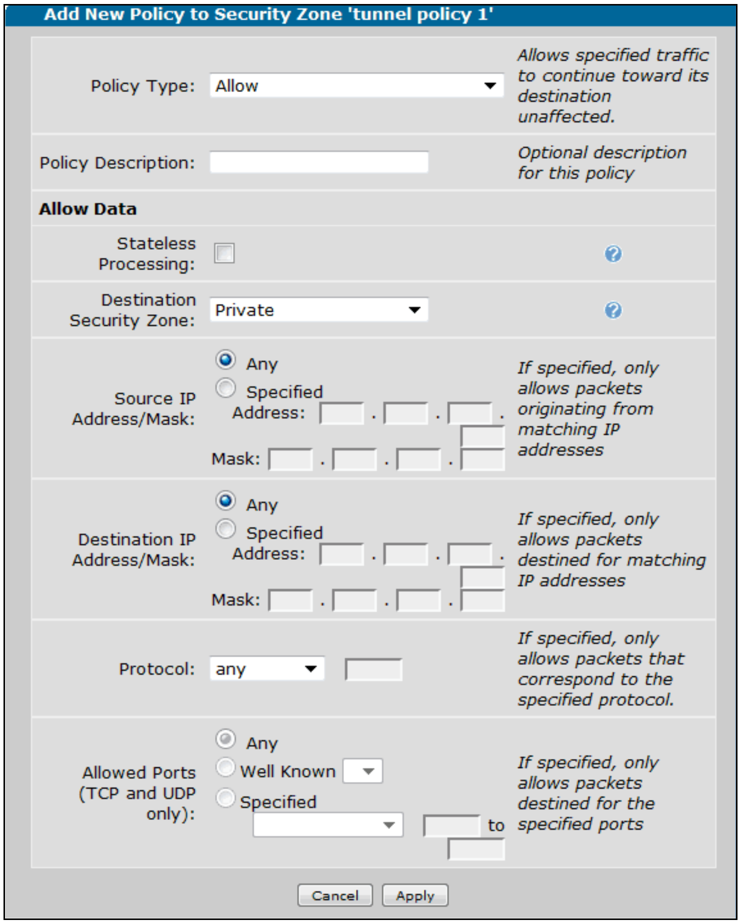
Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Allow

Select which policy type to create, then click Continue.

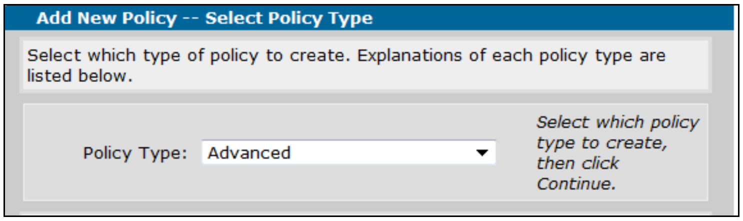
E. In the next menu, you will specify the particulars of the new allow policy. You can specify a policy description, enable stateless processing, specify the destination security zone, enter a source and destination IP address and subnet mask, specify a particular protocol, and specify the allowed ports. The information entered in this menu is used to match traffic; any traffic matching this criteria is allowed to traverse the tunnel. In the example below, the policy's **Destination Security Zone** is specified as **Private**, and the source and destination IP addresses, as well as the protocol type, are left as the default value of **any**. This means that all traffic destined for the **Private** security zone is allowed, and can be routed to the local VLANs. Select **Apply** once you have entered the match criteria for the policy.



Add New Policy to Security Zone 'tunnel policy 1'

Policy Type:	Allow	*Allows specified traffic to continue toward its destination unaffected.*
Policy Description:		*Optional description for this policy*
Allow Data		
Stateless Processing:	□	
Destination Security Zone:	Private	
Source IP Address/Mask:	● Any ○ Specified Address: . . . Mask: . . .	*If specified, only allows packets originating from matching IP addresses*
Destination IP Address/Mask:	● Any ○ Specified Address: . . . Mask: . . .	*If specified, only allows packets destined for matching IP addresses*
Protocol:	any	*If specified, only allows packets that correspond to the specified protocol.*
Allowed Ports (TCP and UDP only):	● Any ○ Well Known ○ Specified to	*If specified, only allows packets destined for the specified ports*

F. Next, create a second policy to add to the **tunnel policy 1** security zone. To do this, select **Add Policy to Zone 'tunnel policy 1'** after selecting **Apply** from creating the first policy (Step E). Specify the **Policy Type** as **Advanced** from the drop-down menu, and select **Continue**.



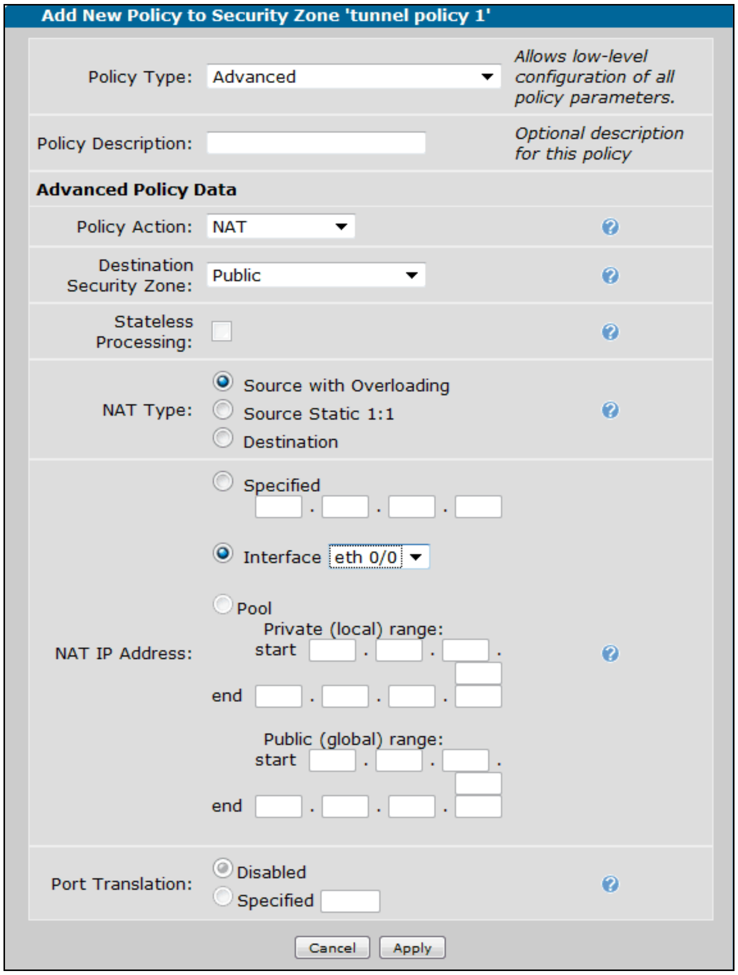
Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Advanced

Select which policy type to create, then click Continue.

G. In the policy configuration menu, specify this **Policy Action** as **NAT** from the drop-down menu. The **Destination Security Zone** for this policy is the WAN interface (**Public** in this example). The remaining settings should stay as the default value. This configured policy is used for voice traffic from remote phones sent out a service provider SIP trunk. Select **Apply** when the new security policy is configured.



Add New Policy to Security Zone 'tunnel policy 1'

Policy Type: Advanced — *Allows low-level configuration of all policy parameters.*

Policy Description: — *Optional description for this policy*

Advanced Policy Data

Policy Action: NAT

Destination Security Zone: Public

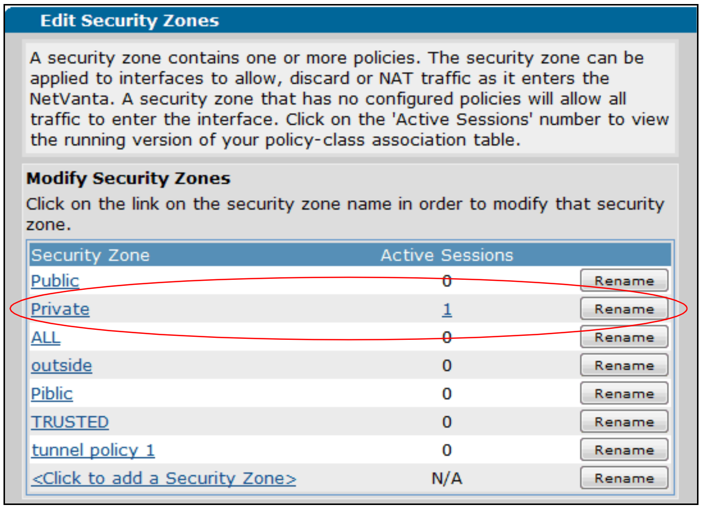
Stateless Processing: □

NAT Type: ● Source with Overloading ○ Source Static 1:1 ○ Destination

NAT IP Address:
○ Specified
● Interface eth 0/0
○ Pool
Private (local) range: start / end
Public (global) range: start / end

Port Translation: ● Disabled ○ Specified

H. After configuring the security policies for the **tunnel policy 1** security zone, you will need to add another policy to the **Private** security zone. This new policy will permit traffic out the tunnel interface. To do this, navigate to **Data** > **Firewall** > **Security Zones** and select the **Private** security zone from the list on the **Edit Security Zones** menu.



Edit Security Zones

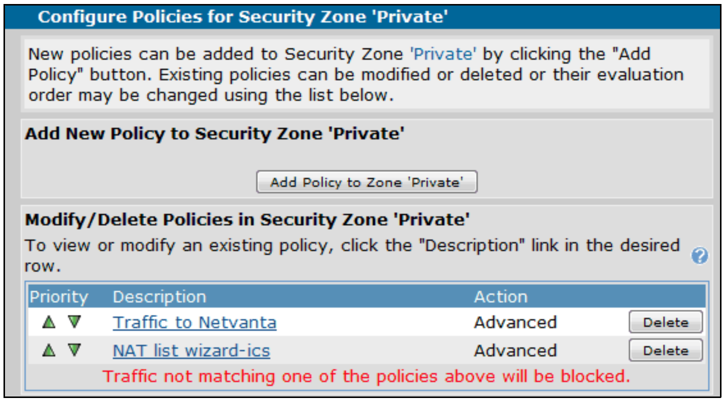
A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

Security Zone	Active Sessions	
Public	0	Rename
Private	1	Rename
ALL	0	Rename
outside	0	Rename
Piblic	0	Rename
TRUSTED	0	Rename
tunnel policy 1	0	Rename
<Click to add a Security Zone>	N/A	Rename

I. Next, select **Add Policy to Zone 'Private'**.



Configure Policies for Security Zone 'Private'

New policies can be added to Security Zone 'Private' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Private'

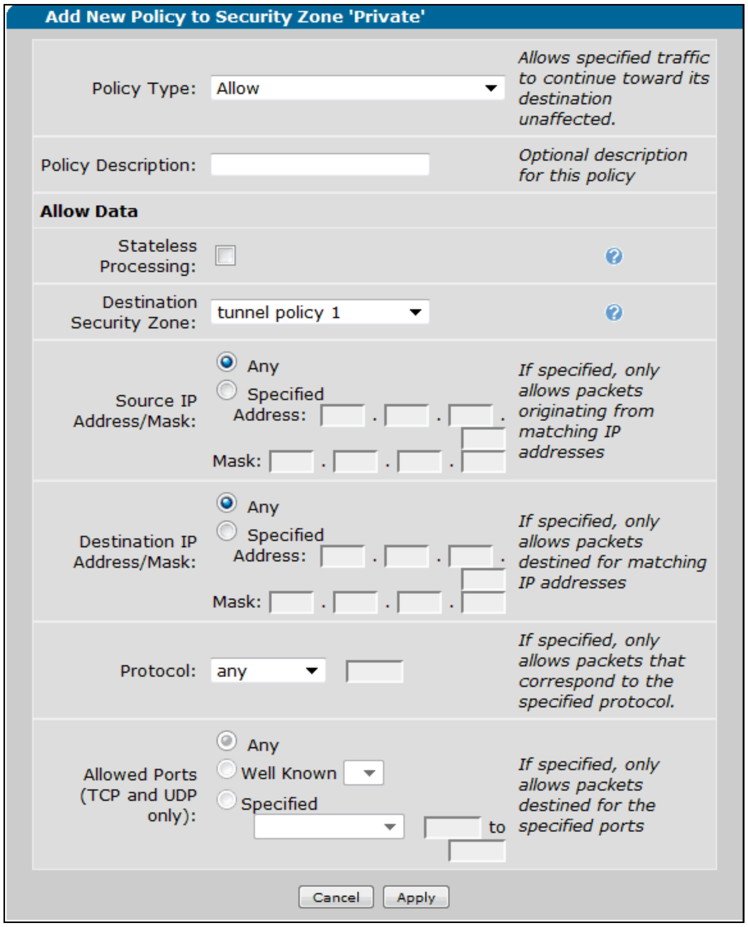
Modify/Delete Policies in Security Zone 'Private'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action	
▲ ▼	Traffic to Netvanta	Advanced	Delete
▲ ▼	NAT list wizard-ics	Advanced	Delete

Traffic not matching one of the policies above will be blocked.

J. Specify the **Policy Type** as **Allow**, and select **Continue**. In the **Add New Policy to Security Zone 'Private'** menu, specify the **Destination Security Zone** as **tunnel policy 1** (or the security zone created for the tunnel in Step B *on page 44*). The remaining policy settings can stay as the default values. Select **Apply** to create the policy.



Add New Policy to Security Zone 'Private'

Policy Type: Allow — *Allows specified traffic to continue toward its destination unaffected.*

Policy Description: — *Optional description for this policy*

Allow Data

Stateless Processing: □

Destination Security Zone: tunnel policy 1

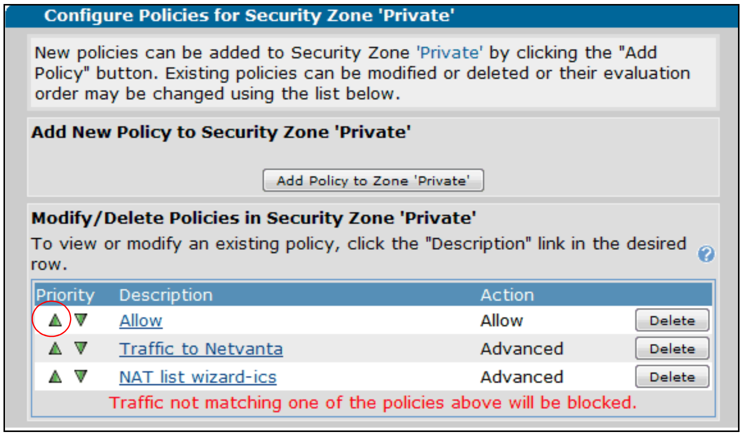
Source IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — *If specified, only allows packets originating from matching IP addresses*

Destination IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — *If specified, only allows packets destined for matching IP addresses*

Protocol: any — *If specified, only allows packets that correspond to the specified protocol.*

Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ○ Specified to — *If specified, only allows packets destined for the specified ports*

K. After creating the **Allow** policy for the security zone **Private**, you will need to move that policy to the top of the policy list for the the **Private** security zone. In the **Configure Policies for Security Zone 'Private'** menu, use the green up arrows to move the **Allow** policy to the top of the list.



Configure Policies for Security Zone 'Private'

New policies can be added to Security Zone 'Private' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

Add New Policy to Security Zone 'Private'

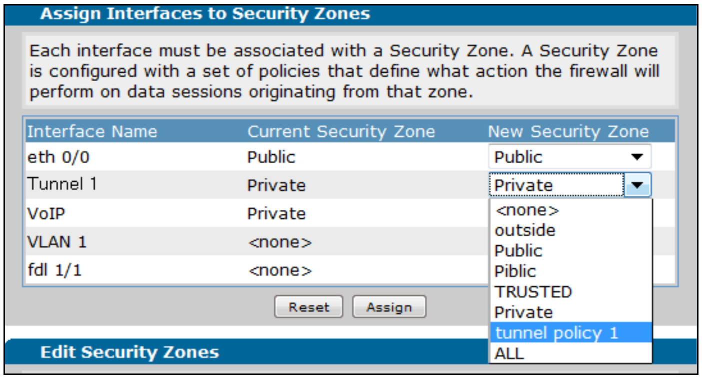
Modify/Delete Policies in Security Zone 'Private'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action	
▲ ▼	Allow	Allow	Delete
▲ ▼	Traffic to Netvanta	Advanced	Delete
▲ ▼	NAT list wizard-ics	Advanced	Delete

Traffic not matching one of the policies above will be blocked.

L. After configuring the security zones and the appropriate policies, you will need to add the **tunnel policy 1** to the tunnel interface. To do this, navigate to **Data** > **Firewall** > **Security Zones**. In the **Assign Interfaces to Security Zones** menu, select **tunnel policy 1** from the drop-down menu for the tunnel interface and select **Assign**.



Assign Interfaces to Security Zones

Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone.

Interface Name	Current Security Zone	New Security Zone
eth 0/0	Public	Public
Tunnel 1	Private	Private
VoIP	Private	
VLAN 1	<none>	
fdl 1/1	<none>	

M. Repeat these steps to create firewall rules for all units in the SIP network.

4. Create SIP Trunks and Associated Trunk Groups for Each Remote Location

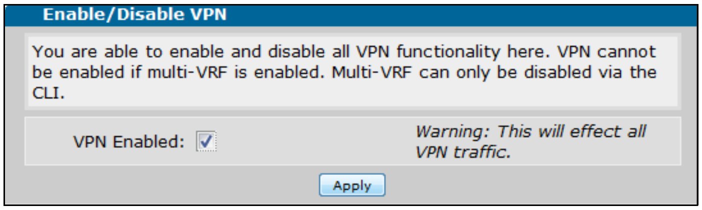
A. After creating the firewall rules for the GRE tunnels, you must configure the SIP trunks and associated trunk groups for each remote location that will have SIP traffic traversing the tunnel. These trunks are different than the SIP trunks and trunk groups created for the Service Provider SIP trunk, and are only used for the tunnel traffic. To configure the GRE tunnel SIP trunks, navigate to **Voice** > **Trunk Accounts** and follow the steps outlined in *Configuring SIP Networking between NetVanta 7000 Series Products using the GUI on page 21*. Make sure that you specify the SIP server as the remote unit's loopback interface IP address, that the FROM header is set to **Local**, and that you create a call template for the trunk group that includes all extensions at the remote site.

B. Repeat these steps for each remote unit.

5. Configure VPN Matching for GRE Traffic

After configuring the SIP trunks and trunk groups for the GRE tunnel, you should configure a VPN tunnel for the GRE tunnel in order to encapsulate traffic. Since the decision to build a VPN tunnel and encrypt traffic is made as the traffic is prepared to leave the egress interface of the unit, the VPN traffic selector must specify the GRE header being used. This traffic is sourced from the WAN IP address and destined for the far-end WAN IP address as protocol 47 (GRE). VPN matching should be configured on all units (both remote and main). To configure the VPN traffic selector, follow these steps:

A. Connect to the unit's GUI and navigate to **Data** > **VPN** > **VPN Peers**. Enable VPN by selecting the **VPN Enabled** checkbox and select **Apply**.



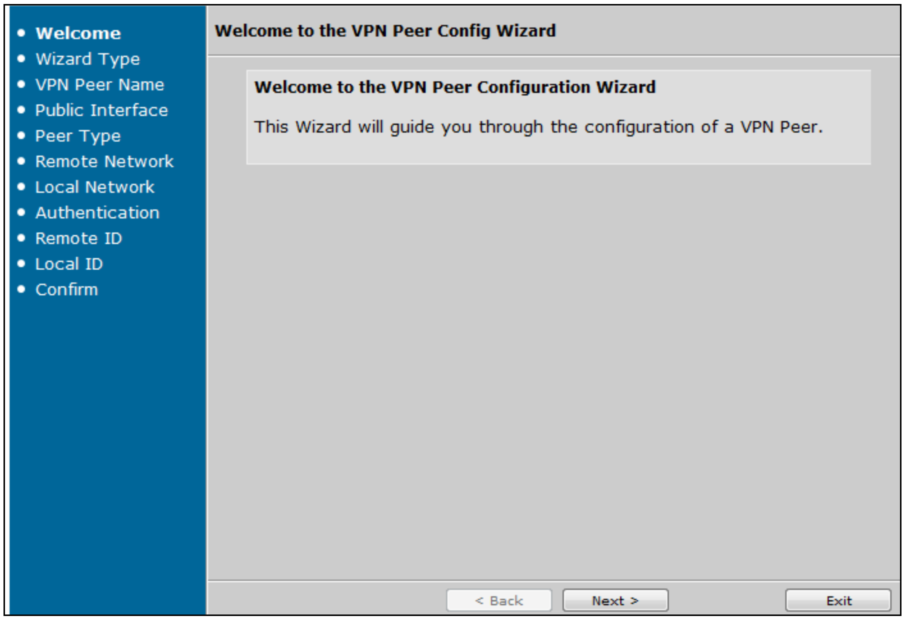
Enable/Disable VPN

You are able to enable and disable all VPN functionality here. VPN cannot be enabled if multi-VRF is enabled. Multi-VRF can only be disabled via the CLI.

VPN Enabled: ☑

Warning: This will effect all VPN traffic.

B. Next, navigate to **Data** > **VPN > VPN Wizard** and follow the **VPN Wizard** prompts to configure the VPN parameters and its traffic selectors.



Welcome to the VPN Peer Config Wizard

Welcome to the VPN Peer Configuration Wizard

This Wizard will guide you through the configuration of a VPN Peer.

NOTE *The VPN wizard can be used to set up the VPN tunnel; however, the VPN traffic selector cannot be configured to match the GRE traffic using the VPN wizard. Once you have completed the wizard, navigate to **VPN** > **VPN Peers** > **Advanced VPN Policies** > **IPsec Policy**. Here you can correctly match the GRE tunnel traffic.*

C. Repeat these steps to configure the VPN criteria for each AOS unit.

6. Configure QoS for Traffic Matching on DSCP Values

After configuring the VPN matching criteria for each unit, you must configure the QoS parameters for each unit in the SIP network (remote and main). The QoS matching criteria for the VPN tunnel is based on the DSCP values because using these values as the traffic matching basis ensures that voice traffic is prioritized. Configure the QoS parameters on each unit for the VPN tunnel by following the steps outlined in *Configure QoS on page 39*. When configuring the QoS map, make sure to check the **DSCP** box in the **Packet Matching** tab of the **QoS Map Setup** menu. When you have configured the QoS map, apply it to the interface used for the VPN tunnel.

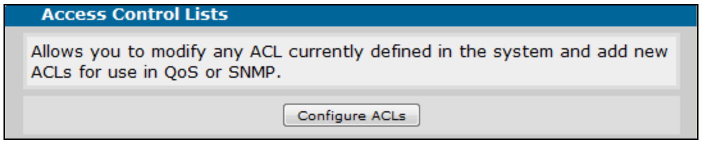
NOTE *It is important to note that by default, voice RTP packets are tagged with a DSCP value of **46**, and voice signaling packets are tagged with a DSCP value of **26**.*

7. Create Route Maps to Route RTP Traffic Through the Tunnel

The last step in creating the VPN tunnel for SIP networking is to create route maps that route RTP traffic through the GRE tunnel. These route maps are necessary in complex SIP networking configurations because they keep the RTP traffic from remote sites from using the Internet connection outside the GRE tunnel, and route the traffic instead through the secure tunnel. Without a route map, the outbound RTP traffic from the remote sites is improperly sent outside the GRE tunnel.

To create a route map for the SIP traffic from remote sites, enter the unit's GUI and follow these steps:

A. On the unit at the remote site, create an extended ACL that permits any traffic from the voice VLAN IP subnet to any destination. To do this, navigate to **Data** > **Firewall** > **General Firewall**. Scroll to the bottom of the menu and select **Configure ACLs**.



Allows you to modify any ACL currently defined in the system and add new ACLs for use in QoS or SNMP.

B. Enter the name and ACL type, and select **Add New ACL**. Next, create a traffic selector by selecting **Add New Traffic Selector**, specify the **Source Host/Network** as the IP subnet of the voice VLAN, and leave the ACL parameters at the default values. Select **Apply**.

C. After configuring the ACL for the remote unit, you must create route maps for each of the remote units. Traffic should be routed to the NetVanta 7000 Series at the main site. To create the route maps, connect to the unit's CLI, and follow these steps:

- Create a route map from the Global Configuration mode using the **route-map** command.
- Assign the ACL created to match the voice VLAN IP subnet using the **match ip** command.
- Set the tunnel interface as the gateway for the route map using the **set interface** command.
- Apply the route map to the VLAN interface used for the remote phones using the **ip policy route-map** command from the VLAN interface's configuration mode.
- Your configuration should follow this example:

```
(config)#route-map VOIP 10
(config-route-map)#match ip address VOICE
(config-route-map)#set interface tunnel 1
(config-route-map)#interface vlan 2
(config-intf-vlan 2)#ip policy route-map VOIP
```

D. Repeat Steps A through C for each of the remote units, making sure to deny any traffic that does not need to be routed over the GRE tunnel.

After configuring the route maps for the GRE tunnel, you have completed the VPN portion of the SIP networking configuration. The next step is to configure the SIP trunks and trunk groups for all AOS units. These SIP trunks are for the SIP traffic not routed through the VPN tunnel.

Configure PSTN Trunk and Trunk Groups on Remote Units

After configuring the SIP trunks and trunk groups on the remote units, you must configure the remote site PSTN trunks and trunk groups. These trunks are necessary to send calls from the remote unit to the PSTN for LCR. This trunk is also used for sending calls to the PSTN directly when the NetVanta 7000 Series unit is unreachable.

> NOTE *An analog, ISDN, or T1 RBS trunk can be configured on the remote units. Configuring these trunks is different than configuring SIP trunks. Refer to the configuration guide **NetVanta 7000 Series Trunk Accounts** for more information on how to configure these types of trunks. This guide is available online at http://kb.adtran.com, article number 1541.*

When configuring the PSTN trunks, you must specify the trunk type. In addition, make sure that **prefer trunk-routing** is enabled.

The PSTN trunk groups accept numbers dialed both with and without a leading 9. Outbound calls that go through the NetVanta 7000 Series unit at the main site will have the leading 9 stripped before the call reaches the remote unit. However, the leading 9 is not stripped when the NetVanta 7000 Series unit is unreachable. When the leading 9 is present, such as in a failover, the leading 9 is stripped on the voice trunk by using DNIS substitution. DNIS substitution is configured by using the **DNIS Substitution** tab in the **Edit Trunk** menu. Enter the wildcard templates with a leading 9 as the match number (for example, **9-NXX-NXX-XXXX**) and enter the wildcard templates without the leading 9 as the substitution number (for example, **NXX-NXX-XXXX**).

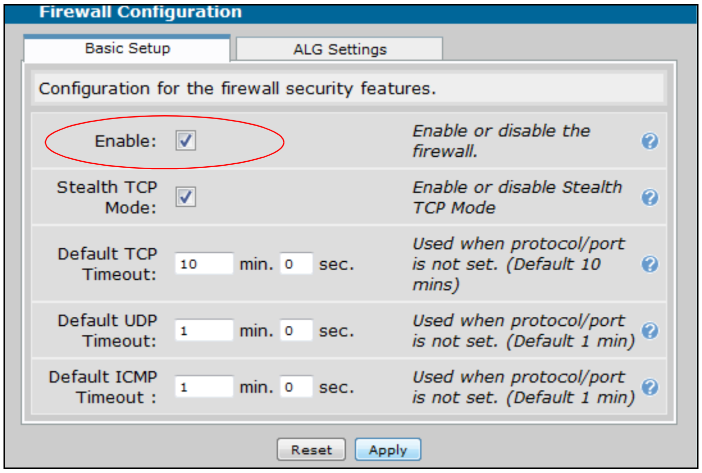
When specifying the cost associated with the outbound call templates in the trunk group's configuration, set a lower cost so that analog phones on the remote unit first attempt to route their calls to the NetVanta 7000 Series unit at the main site instead of directly out the PSTN trunks. This is beneficial because the AOS units at the remote sites do not provide voice features locally.

Enable SIP Proxy

After configuring the PSTN trunks, the next step in configuring SIP networking is to enable SIP proxy on all AOS units in the SIP network. SIP proxy must be enabled for local survivability and failover on an IP business gateway. SIP proxy must be enabled on both the unit at the main site and any units at remote sites. The following configuration information is basic configuration for this application. For more information about SIP proxy, refer to the configuration guide *Configuring the SIP Proxy in AOS* available online at http://kb.adtran.com (article number 2183). To configure SIP proxy on the remote unit, using the GUI, follow these steps:

1. Connect to the GUI and navigate to **Data** > **Firewall**. Select **General Firewall**, and in the **Basic Setup** tab of the **Firewall Configuration** menu, check the **Enable** box to enable the firewall. The firewall must be enabled for SIP proxy to function properly. If you also need to configure your firewall, you can use the **Firewall Wizard** or continue the configuration through the **General Firewall** settings. For more information about firewall configuration, refer to the configuration guide *IPv4 Firewall Protection*

available online at http://kb.adtran.com (article number 1543). Select **Apply** once you have enabled the firewall.

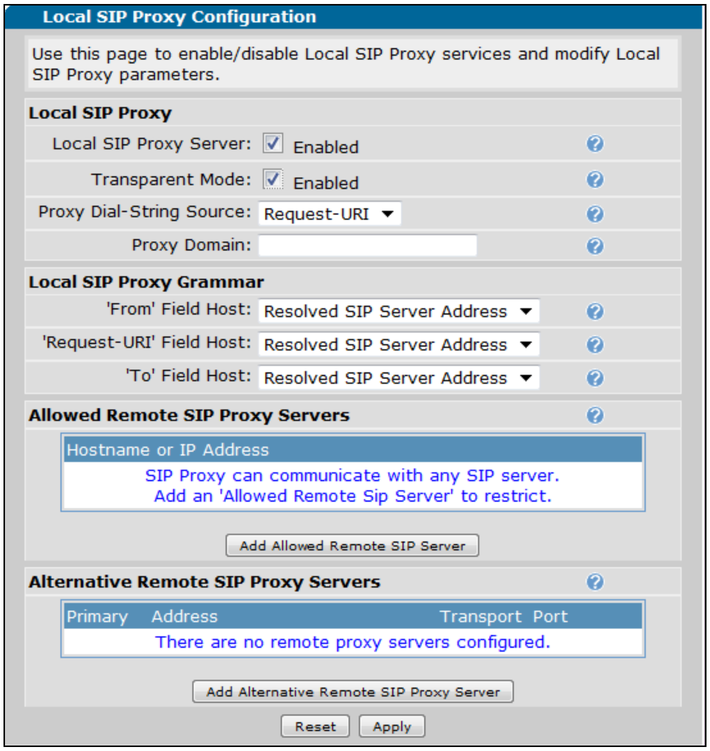


Firewall Configuration

Configuration for the firewall security features.

Enable:	☑	*Enable or disable the firewall.*
Stealth TCP Mode:	☑	*Enable or disable Stealth TCP Mode*
Default TCP Timeout:	10 min. 0 sec.	*Used when protocol/port is not set. (Default 10 mins)*
Default UDP Timeout:	1 min. 0 sec.	*Used when protocol/port is not set. (Default 1 min)*
Default ICMP Timeout :	1 min. 0 sec.	*Used when protocol/port is not set. (Default 1 min)*

2. After enabling the firewall, navigate to **Voice** > **System Setup** > **SIP Proxy Settings**. Enable the **Local SIP Proxy Server** and **Transparent Mode** by selecting the appropriate checkboxes, then select **Apply**.



Local SIP Proxy Configuration

Use this page to enable/disable Local SIP Proxy services and modify Local SIP Proxy parameters.

Local SIP Proxy

Local SIP Proxy Server:	☑ Enabled
Transparent Mode:	☑ Enabled
Proxy Dial-String Source:	Request-URI ▼
Proxy Domain:	

Local SIP Proxy Grammar

'From' Field Host:	Resolved SIP Server Address ▼
'Request-URI' Field Host:	Resolved SIP Server Address ▼
'To' Field Host:	Resolved SIP Server Address ▼

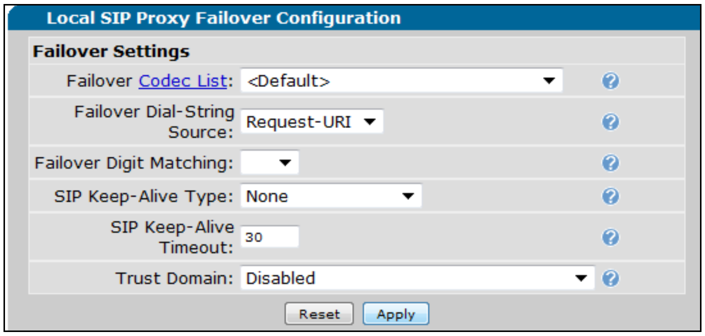
Allowed Remote SIP Proxy Servers

Hostname or IP Address
SIP Proxy can communicate with any SIP server. Add an 'Allowed Remote Sip Server' to restrict.

Alternative Remote SIP Proxy Servers

Primary	Address	Transport	Port
There are no remote proxy servers configured.			

3. Configure the SIP proxy failover settings. In the **SIP Proxy Settings** menu, scroll to the **Local SIP Proxy Failover Configuration** menu. In this menu you can specify the coder-decoder (CODEC) used for failover, the failover dial string source, the digits to match, the SIP keepalive type and timeout, and whether you will use a trusted domain.



Local SIP Proxy Failover Configuration

Failover Settings

Failover Codec List: <Default>

Failover Dial-String Source: Request-URI

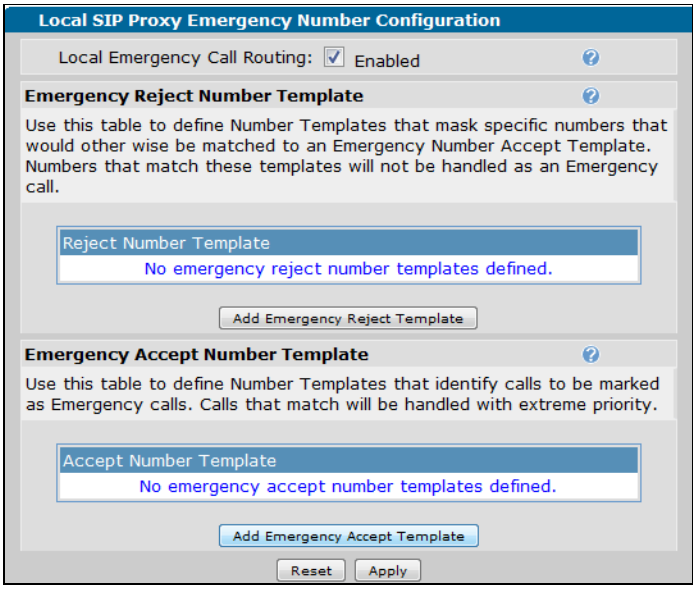
Failover Digit Matching:

SIP Keep-Alive Type: None

SIP Keep-Alive Timeout: 30

Trust Domain: Disabled

4. Configure the emergency call routing parameters. To force 911 calls to be immediately routed to the PSTN trunks on the remote unit without having to first go through the NetVanta 7000 Series unit, enable **Local Emergency Call Routing** and specify the emergency numbers by selecting **Add Emergency Accept Templates**.



Local SIP Proxy Emergency Number Configuration

Local Emergency Call Routing: ☑ Enabled

Emergency Reject Number Template

Use this table to define Number Templates that mask specific numbers that would other wise be matched to an Emergency Number Accept Template. Numbers that match these templates will not be handled as an Emergency call.

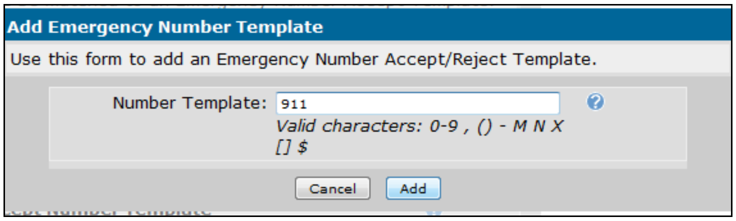
Reject Number Template
No emergency reject number templates defined.

Emergency Accept Number Template

Use this table to define Number Templates that identify calls to be marked as Emergency calls. Calls that match will be handled with extreme priority.

Accept Number Template
No emergency accept number templates defined.

Enter the phone number to be treated as an emergency number in the dialog box, and select **Add**.



Add Emergency Number Template

Use this form to add an Emergency Number Accept/Reject Template.

Number Template: 911

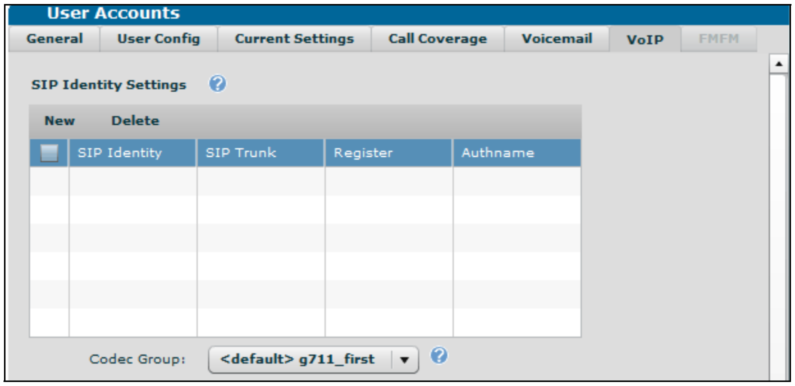
Valid characters: 0-9 , () - M N X [] $

5. Repeat Steps 1 through 4 for all remote AOS units in the SIP network.

Configure the Remote Unit's Analog Users

Analog users on the remote unit(s) should be configured to register to the NetVanta 7000 Series unit using the SIP trunk. For this registration, the analog user should be given a SIP identity with an authorization name and password. Follow these steps for each analog user at each remote site:

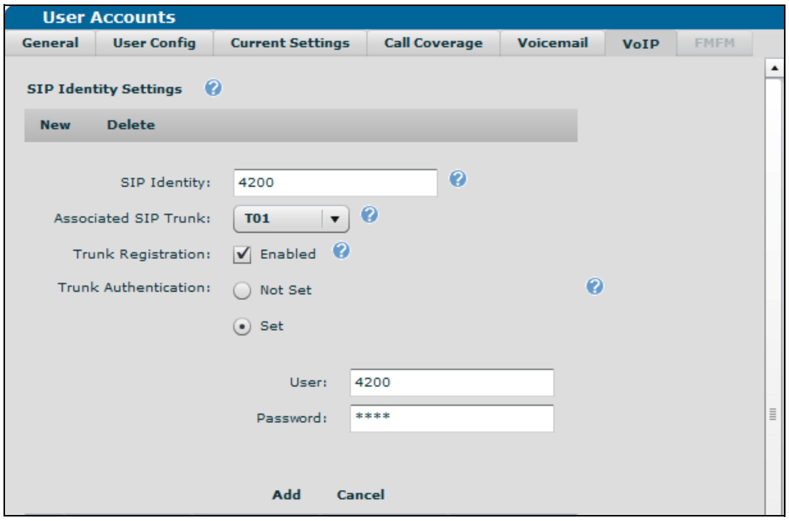
1. Connect to the remote unit's GUI and navigate to **Voice** > **Stations** > **User Accounts**. Select the analog user from the user list, and select **Edit**. In the **User Accounts** configuration menu, select the **VoIP** tab.



	SIP Identity	SIP Trunk	Register	Authname

Codec Group: <default> g711_first

2. Create a SIP identity for this user by selecting **New** under **SIP Identity Settings**. Specify the user's SIP identity in the appropriate field (you can use the user's extension to keep it simple). In addition, you need to specify the associated SIP trunk from the drop-down menu, enable trunk registrations, and specify the user's trunk authentication by setting a user name and a password. Select **Add** when you have created the SIP identity, and select **Apply** at the bottom of the menu to apply the settings.



SIP Identity: 4200
Associated SIP Trunk: T01
Trunk Registration: ☑ Enabled
Trunk Authentication: ○ Not Set
● Set
User: 4200
Password: ****

NOTE *The user name must be the extension number configured for the analog user. On the NetVanta 7000 Series unit, a SIP user account must be created for the remote analog extension and this is used for the SIP registration of that analog user.*

3. Repeat Steps 1 and 2 for all analog users on each of the remote AOS units.

Configuring NetVanta 7000 Series Trunk Groups Using the GUI

After you have configured the trunks on the NetVanta 7000 Series unit at the main site, you must configure the unit's trunk groups. There are three main variations for the trunk group configuration, and each variation determines which users can use which PSTN trunks. The first option is to allow users from all sites to use all trunks in a true LCR scenario. The second option is to allow the remote site users to use their local trunks for local calls, but force all long distance calls out the PRI or service provider SIP trunk at the main site. The final option is to only allow users to use their local trunks for all calls. The following sections describe the configuration of these three scenarios, providing you with three LCR configuration options.

For these configurations, ANI and trunk lists are used to force 7- or 10-digit local dialing out of the correct trunk. The trunk lists are needed because when a phone is forwarded, the call is considered to have originated from the trunk on which it was received. ANI lists must be configured and applied to the appropriate trunk group using the CLI. After configuring the trunk groups using the GUI, refer to *Configuring Trunks on the NetVanta 7000 Series Using the CLI on page 70* for information on how to add the trunk and ANI lists to the trunk groups using the CLI.

Trunk Groups for True LCR Configuration

The first trunk group configuration option provides a method for configuring true LCR. In a true LCR scenario, the trunks on the remote sites are used for calls that are local to those sites, and the PRI or service provider SIP trunk off the NetVanta 7000 Series unit at the main site is used for all other calls.

To configure these trunk groups using the GUI, follow the steps outlined in *Configuring SIP Networking Trunk Group(s) using the GUI on page 26*. The configuration parameters for this scenario are as follows:

1. Create a trunk group, and add the PSTN trunk created when configuring the trunks on the NetVanta 7000 Series unit. Specify that this trunk group accepts local, long distance, toll-free, and international calls (or others as your network demands) in the **Outbound Call Templates** GUI menu. Set the cost for these calls as **Low Cost**.
2. Create a local dialing trunk group, and also add the PSTN trunk created when configuring the trunks on the NetVanta 7000 Series unit. Specify that this trunk group accepts local, emergency, and informational calls (411, 611) with a **Low Cost**. Configure and add ANI lists as described in *Configuring Trunks on the NetVanta 7000 Series Using the CLI on page 70*.
3. Create a trunk group for local calls at the first remote location (for example, **Remote Site B Local Dialing**), and add the PSTN trunk at the remote site to this trunk group. Specify that the trunk group accepts local, emergency, and informational calls with a **Low Cost**.
4. Create a SIP trunk group for remote calls at the first remote location (for example, **Remote Site B Remote Dialing**), and add the SIP trunk at the remote site to this trunk group. Specify that this trunk group accepts long distance calls with a **Low Cost**.
5. Repeat Steps 3 and 4 for each remote unit.
6. The trunk groups for true LCR configuration are now complete.

Trunk Groups Configured for Remote Sites to Use Local Trunks for Local Calls

The second trunk group configuration option provides a method for configuring the remote sites to use local trunks for local calls. In this scenario, users at the remote sites are permitted to use their trunks for local calls, but long distance calls are routed out the PRI or service provider SIP trunk at the main site.

To configure these trunk groups using the GUI, follow the steps outlined in *Configuring SIP Networking Trunk Group(s) using the GUI on page 26*. The configuration parameters for this scenario are as follows:

1. Create a trunk group, and add the PSTN trunk created when configuring the trunks on the NetVanta 7000 Series unit. Specify that this trunk group accepts local, long distance, toll-free, and international calls (or others as your network demands) in the **Outbound Call Templates** GUI menu. Set the cost for these calls as **Low Cost**.
2. Create a local dialing trunk group, and also add the PSTN trunk created when configuring the trunks on the NetVanta 7000 Series unit. Specify that this trunk group accepts local, emergency, and informational calls (411, 611) with a **Low Cost**. Configure and add ANI and trunk lists as described in *Configuring Trunks on the NetVanta 7000 Series Using the CLI on page 70*.
3. Create a trunk group for local calls at the first remote location (for example, **Remote Site B Local**), and add the SIP trunk at the remote site to this trunk group. Specify that the trunk group accepts local, emergency, and informational calls with a **Low Cost**. Configure and add ANI and trunk lists as described in *Configuring NetVanta 7000 Series Trunk Groups using the CLI on page 70*.
4. Repeat Step 3 for each remote unit.
5. The trunks groups for configuring remote sites to use local trunks for local calls are now complete.

Trunk Groups Configured for Remote Sites to Use Local Trunks for All Calls

The third trunk group configuration option provides a method for configuring the remote sites to use local trunks for all calls. In this scenario, users from each site only use the trunks that are local to their site.

To configure these trunk groups using the GUI, follow the steps outlined in *Configuring SIP Networking Trunk Group(s) using the GUI on page 26*. The configuration parameters for this scenario are as follows:

1. Create a trunk group, and add the PSTN trunk created when configuring the trunks on the NetVanta 7000 Series unit. Specify that this trunk group accepts local, long distance, toll-free, and international calls (or others as your network demands) in the **Outbound Call Templates** GUI menu. Set the cost for these calls as **Low Cost**. Configure and add ANI and trunk lists as described in *Configuring Trunks on the NetVanta 7000 Series Using the CLI on page 70*.
2. Create a trunk group for all calls at the first remote location (for example, **Remote Site B Trunks**), and add the SIP trunk at the remote site to this trunk group. Specify that the trunk group accepts local, emergency, and informational calls (or others as your network demands) with a **Low Cost**. Configure

and add ANI and trunk lists as described in *Configuring Trunks on the NetVanta 7000 Series Using the CLI on page 70*.

3. Repeat Step 2 for each remote unit.
4. The trunks groups for configuring remote sites to use local trunks for all calls are now complete.

Configuring SIP Networking with IP Business Gateways using the CLI

SIP networking can also be used between the NetVanta 7000 Series product and IP business gateways at remote locations. IP business gateways are typically Total Access 900(e) or NetVanta 6355 products. *Figure 5 on page 20* describes the network topology for this type of SIP networking. This application functions similarly to a single PBX, in which each remote user registers back to the NetVanta 7000 Series using either SIP transparent proxy, or directly using analog phones. The phones at the remote locations rely on the main site to provide voicemail and auto attendant services for incoming calls. At the remote sites, the SIP trunks facing the main site are mainly used for inbound calls. Typically, the outbound trunks configured at remote sites connect to the PSTN and are used for survivability purposes only.

There are a few things to keep in mind when configuring SIP networking between NetVanta 7000 Series products and an IP business gateway:

- The maximum number of users per installed NetVanta 7000 Series product is 100. All users connected directly or through SIP proxy count as part of the total sum of users.
- All remote users connected through SIP proxy to the main site have access to all the NetVanta 7000 Series features, and function as thought they are located at the main site.
- Users that do not register using SIP proxy, over a VPN connection or through the SIP trunk, are not supported.
- The NetVanta 7000 Series unit at the main site must have call routing and transfer modes set to **Local**, and the platforms at the remote sites must have voice feature and transfer modes set to **Network**.
- When configuring SIP networking with IP business gateways, you will have to also configure SIP proxy, a VPN tunnel, and possibly LCR.

To configure the SIP networking trunks between the NetVanta 7000 Series and an IP business gateway, follow these steps:

1. Plan the extensions used at each site. Each location should have their own extensions. For example, the main site can use extensions **2xxx**, remote site B can use extensions **3xxx**, and remote site C can use extensions **4xxx**.
2. Configure the media gateway for all units (remote and main).
3. Configure the IP phones and remote voice users for the remote unit(s) on the NetVanta 7000 Series unit at the main site.
4. Configure the Dynamic Host Control Protocol (DHCP) pool for the remote unit.
5. Configure QoS. The QoS configuration is done on both the NetVanta 7000 Series unit at the main site, and any AOS units at the remote sites.
6. Configure the VPN tunnels between sites.
7. Configure the SIP trunk and trunk groups for the remote unit(s).

8. Configure the PSTN trunks and trunk groups for the remote unit(s). These trunks are used for LCR and survivability.
9. Enable SIP proxy on the AOS unit(s) in the SIP network.
10. Configure the remote unit's analog users.
11. Configure the SIP trunk(s) on the NetVanta 7000 Series unit at the main site.
12. Configure the SIP trunk group(s) on the NetVanta 7000 Series unit at the main site. There are different variations for trunk group configuration, depending on the type of LCR you want to implement.

Configuring the Media Gateway for All Units

All units (remote and main) must have a media gateway configured. The media gateway converts digital media streams between the PSTN and the PBX (NetVanta 7000 Series unit). For this application, because inbound calls from the trunks at remote sites are routed through the NetVanta 7000 Series unit at the main site, the media gateway on all units is configured to be the loopback interface on all units. To configure the media gateway using the CLI, connect to the CLI for each unit and follow these steps:

1. Configure the media gateway on the NetVanta 7000 Series unit at the main site. The example below enables the loopback interface and configures its IP address, as well as specifies that all IP interfaces use the loopback interface as the media gateway. Begin this configuration from the Global Configuration mode.

```
interface loopback 1
   ip address 10.10.20.2 255.255.255.255
   no shutdown
   !
interface vlan 1
  media-gateway ip loopback 1
  !
interface vlan 2
  media-gateway ip loopback 1
  !
interface eth 0/0
  media-gateway ip loopback 1
```

2. Configure the media gateway on the remote unit(s). The example below enables and configures the loopback interface, as well as specifies that all IP interfaces use the loopback interface as the media gateway. Begin this configuration from the Global Configuration mode.

```
interface loopback 1
   ip address 10.20.20.2 255.255.255.255
   no shutdown
   !
interface vlan 1
  media-gateway ip loopback 1
  !
interface vlan 2
  media-gateway ip loopback 1
  !
interface eth 0/0
  media-gateway ip loopback 1
```

3. Repeat Step 2 for each remote unit.

Configuring the IP Phones and Users for the Remote Unit(s)

After configuring the media gateway on all units, you must configure the IP phones and the users for each of the remote units. IP phone and remote user configuration should only be done using the GUI. Refer to *Configure the IP Phones and Users for Remote Unit(s) on page 34* for instructions.

Configuring the DHCP Pool for the Remote Unit(s)

The DHCP pools for the IP phones on the remote unit(s) should be configured to point to the WAN interface of the NetVanta 7000 Series unit at the main site for the boot server. You will need to configure a DHCP pool for the LAN and one for VoIP, so each remote unit should have two configured DHCP pools. For more specific information about DHCP configuration and commands, refer to the troubleshooting guide *Configuring DHCP in AOS* (article number 2149) or the *AOS Command Reference Guide* (article number 2219) available online at http://kb.adtran.com. The following steps provide sample CLI configuration for the DHCP pools on the remote unit(s):

1. Configure the DHCP pool for the LAN on the remote unit. Specify the network address, the DNS server address, the Netbios type, default router address, NTP server address, timezone offset, DHCP options, and TFTP and FTP server information. Begin this configuration from the Global Configuration mode.

```
ip dhcp-server pool “LAN_pool”
    network 10.20.10.0 255.255.255.0
    dns-server 10.20.10.1
    netbois-node-type h-node
    default-router 10.20.10.1
    ntp-server 10.20.10.1
    timezone-offset -6:00
    option 66 ascii ftp://polycomftp:password@192.0.2.2/Polycom
    option 157 ascii
    TftpServers=0.0.0.0, FtpServers=192.0.2.2:/ADTRAN, FtpLogin=polycomftp,
    FtpPassword=password, Layer2TAgging=True, VlanID=2
```

2. Configure the DHCP pool for VoIP on the remote unit. Specify the network address, the DNS server address, the Netbios type, default router address, NTP server address, timezone offset, DHCP options, and TFTP and FTP server information. Begin this configuration from the Global Configuration mode.

```
ip dhcp-server pool “LAN_pool”
    network 10.20.20.0 255.255.255.0
    dns-server 10.20.20.1
    netbois-node-type h-node
    default-router 10.20.20.1
    ntp-server 10.20.20.1
    timezone-offset -6:00
    option 66 ascii ftp://polycomftp:password@192.0.2.2/Polycom
    option 157 ascii
    TftpServers=0.0.0.0, FtpServers=192.0.2.2:/ADTRAN, FtpLogin=polycomftp,
    FtpPassword=password, Layer2TAgging=True, VlanID=2
```

3. Repeat Steps 1 and 2 for each remote unit, making sure to make the necessary adjustments to the network, DNS server, default router, and NTP server addresses.

Configuring QoS

QoS is a requirement anywhere time sensitive traffic, such as VoIP, will be using the same bandwidth as a user's regular data traffic. QoS should be configured on all units (remote and main) to ensure voice quality. The QoS parameters should match between units, and should be applied to each unit at the egress interface for the traffic between sites. The following steps present a sample QoS configuration. When implementing QoS, make sure the parameters fit with your network. For more specific information about QoS configuration, refer to the configuration guide *Configuring QoS in AOS* (article number 1617) or the *AOS Command Reference Guide* (article number 2219) available online at http://kb.adtran.com.

1. Configure the QoS maps, specifying the match criteria and the traffic priority. Begin this configuration from the Global Configuration mode.

```
qos map VOIP 10
  match dscp 46
  priority percent 50
qos map VOIP 20
  match dscp 26
  bandwidth percent 25
```

2. Apply the QoS maps to a QoS policy, and apply the policy to the egress interface of the unit (**eth 0/0**). Begin this configuration from the Global Configuration mode.

```
interface eth 0/0
  qos-policy out VOIP
```

3. Repeat Steps 1 and 2 for each unit in the SIP network (both remote and main).

Configuring the VPN Tunnels between SIP Networked Sites

VPN tunnels are necessary for SIP networking implementations because they assure call signaling and audio is passed between networked sites. VPN tunnel configuration is comprised of a number of configuration steps, and intermingles with the configuration steps for the SIP networking configuration between the sites. The following steps are necessary to configure the VPN tunnels:

1. Create Generic Route Encapsulation (GRE) tunnel interfaces. These are necessary so that site-to-site voice traffic has a separate media gateway IP address than SIP traffic that will not traverse a tunnel.
2. Point routes for far-end networks to the GRE tunnel interface. Routes should be created so that traffic destined for far-end networks will use the GRE tunnel.
3. Create allow firewall rules for physical and GRE tunnel interfaces. In order for traffic between the sites to be allowed through the ADTRAN devices, specific allow policies must be added for traffic which is destined for the tunnel interface. Without these policies, NAT will be performed on the site-to-site traffic introducing processing delay and unnecessary complexity without benefit.

4. Configure VPN matching for GRE traffic. In order to secure the traffic routed over the GRE tunnel between sites, a VPN tunnel can be configured to encrypt the traffic. This traffic is sourced from the WAN IP address and destined for the far-end WAN IP address as protocol 47 (GRE).
5. Create route maps for use with SIP networking. A route map can be used to make sure that RTP traffic from a remote site, and destined for a SIP server with a public IP address, is routed across the GRE tunnel rather than using the internet connection outside the tunnel. This is necessary since the SIP server and corresponding media gateway used for PSTN access only expects SIP and RTP from the main site's public IP address.

To configure the VPN tunnel for SIP networking, follow the steps below:

1. Create the GRE Tunnel Interfaces

GRE tunnel interfaces should be configured on the NetVanta 7000 Series unit at the main site, as well as any AOS devices at the remote sites. For more information about GRE configuration or tunnel interface commands, refer to the configuration guide *GRE* (article number 1619) or the *AOS Command Reference Guide* (article number 2219) online at http://kb.adtran.com. The following steps provide sample configuration of the GRE tunnel interface:

A. Configure the tunnel interface on the AOS unit. Enter a description for the tunnel, the IP address of the tunnel, specify the tunnel's media gateway, the tunnel mode, source, and destination, and the keepalive time, the MTU size, and the bandwidth. Enter the configuration from the Global Configuration mode. The following is an example configuration for the tunnel interface:

```
interface tunnel 1
  description Tunnel 1
  ip address 10.100.100.1 255.255.255.252
  access-policy Tunnel
  media-gateway ip loopback 1
  tunnel mode gre
  tunnel source 192.168.1.1
  tunnel destination 192.168.101.1
  keepalive 60 5
  mtu 1476
  bandwidth 100000
  no shutdown
```

B. Repeat Step A for each unit (remote and main) in the SIP network.

2. Point Routes for Far-End Networks to the GRE Tunnel Interface

Routes are created to point traffic destined for far-end networks to the GRE tunnel. For the main site configuration, the route should include a separate IP route for each remote device. For the remote sites, you can use a summary tunnel route. For more information about GRE configuration or routing configuration interface commands, refer to the configuration guide *GRE* (article number 1619) or the *AOS Command*

Reference Guide (article number 2219) online at http://kb.adtran.com. The following steps provide sample configuration of the tunnel routes:

A. Specify the IP routes on the NetVanta 7000 Series unit at the main site. Create one or more routes for each remote unit. Begin this configuration in the Global Configuration mode.

```
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 10.10.11.0 255.255.255.0 tunnel 1
ip route 10.10.21.0 255.255.255.0 tunnel 1
```

B. Specify the IP routes on the remote units. If you are using a hub-and-spoke network configuration, a summary tunnel route can be used for multisite installations (however, the main site should always include specific routes for each site). The summary tunnel route is shown below. Begin this configuration in the Global Configuration mode.

```
ip route 10.10.0.0 255.255.0.0 tunnel 1
```

C. Repeat Step B for each remote unit.

3. Configure the Firewall for the Physical and GRE Tunnel Interfaces

You must create specific “allow” policies for the traffic which is destined for the tunnel interface so that NAT is not performed on the site-to-site traffic. These policies will need to be applied to all units (remote and main) and on all VLANs used to route traffic over the tunnel. For more specific information about firewall configuration or firewall commands, refer to the configuration guide *IPv4 Firewall Protection in AOS* (article number 1543) or the *AOS Command Reference Guide* (article number 2219) available online at http://kb.adtran.com. The following steps provide sample configuration of the firewall policies for the tunnels:

A. Create an access control list (ACL) for the tunnel that permits any traffic.

```
ip access-list extended tunnel
  permit ip any any
```

B. Create an access control policy (ACP) for the networked traffic. The **allow list tunnel policy Tunnel** command allows all traffic that matches the ACL **tunnel** (all traffic) as long as the traffic is destined for the interface to which the **Tunnel** ACP (Step 4) is applied. Therefore, only traffic destined for the tunnel interface is allowed with this rule.

```
ip policy-class Private
  allow list self self
  allow list tunnel policy Tunnel
  nat source list NAT interface eth 0/0 overload
```

C. Configure the VLAN interface, and add the ACP for networked traffic.

```
interface vlan 2
  ip address 10.10.20.1 255.255.255.0
  access-policy Private
  media-gateway ip primary
  no shutdown
```

D. Configure an ACP for the tunnel traffic.

```
ip policy-class Tunnel
  allow list self self
  allow list tunnel policy Private
```

E. Configure the tunnel interface, and apply the ACP for tunnel traffic.

```
interface tunnel 1
  description Tunnel 1
  ip address 10.100.100.1 255.255.255.252
  access-policy Tunnel
```

F. Repeat Steps A through E for each unit in the SIP network (remote and main).

4. Configure VPN Matching for GRE Traffic

After configuring the SIP trunks and trunk groups for the GRE tunnel, you should configure a VPN tunnel for the GRE tunnel in order to encapsulate traffic. Since the decision to build a VPN tunnel and encrypt traffic is made as the traffic is prepared to leave the egress interface of the unit, the VPN traffic selector will need to specify the GRE header being used. This traffic is sourced from the WAN IP address and destined for the far-end WAN IP address as protocol 47 (GRE). VPN matching should be configured on all units (both remote and main). For more specific information about the commands used to configure the VPN matching, refer to the *AOS Command Reference Guide* available online at http://kb.adtran.com (article number 2219).

> NOTE *For more information about VPN configuration, refer to the common application guide, Configuring a VPN using Main Mode in AOS, available online at http://kb.adtran.com (article number 1925).*

The following steps provide sample configuration for the VPN traffic selector:

A. Create an ACL for the VPN, and specify the permitted traffic.

```
ip access-list extended VPN-10-vpn-selectors
  permit gre host 192.168.1.12 host 192.168.101.1
```

> NOTE *If you used the VPN wizard to create the tunnel, the VPN selector ACL will already be applied to the ACP. This step creates an ACL if the VPN wizard was not used.*

B. Configure the crypto map, and specify the VPN to which the map is assigned, a description of the map, and the match criteria (by applying the VPN ACL).

```
crypto map VPN 10 ipsec-ike
  description to-Site-B
  match address VPN-10-vpn-selectors
```

C. Repeat Steps A and B for all units in the SIP network.

5. Create Route Maps to Route RTP Traffic Through the Tunnel

The last step in creating the VPN tunnel for SIP networking is to create route maps that route RTP traffic through the GRE tunnel. These route maps are necessary in complex SIP networking configurations because they keep the RTP traffic from remote sites from using the Internet connection outside the GRE tunnel, and rather route the traffic through the secure tunnel. Without a route map, the outbound RTP traffic from the remote sites is improperly sent outside the GRE tunnel.

The following is an example of the additional configuration needed in order to ensure the proper flow RTP from the remote sites through the main site. In this example, all calls from the remote site B are routed to the main site A. Site A just needs to be configured to perform NAT on traffic not destined for the local Private interfaces or other remote sites through the tunnel interface. The remote site B needs additional accept templates and the route map to ensure that all traffic from the remote voice VLAN is properly routed across the GRE tunnel if not destined for the local NetVanta 7000 Series unit.

A. Configure the route maps on the NetVanta 7000 Series unit at the main site. Create an ACL for the VoIP traffic (**VoIPRouteMap**), create a route map (**VoIP**) with the ACL, and apply the route map to the voice VLAN interface.

```
ip access-list extended VoIPRouteMap
  deny ip 10.10.21.0 0.0.0.255 host 10.10.21.1
  deny ip 10.10.21.0 0.0.0.255 10.10.11.0 0.0.0.255
  permit ip 10.10.21.0 0.0.0.255 any
!
route-map VoIP permit 10
  match ip address VoIPRouteMap
  set interface tunnel 1
!
interface vlan 2
  ip policy route-map VoIP
```

B. Repeat Step A for each remote unit.

Configuring PSTN Trunk and Trunk Groups on the Remote Units

After configuring the SIP trunks and trunk groups on the remote units, you must configure the remote site PSTN trunks and trunk groups. These trunks are necessary to send calls from the remote unit to the PSTN for LCR. This trunk is also used for sending calls to the PSTN directly when the NetVanta 7000 Series unit is unreachable.

> NOTE *An analog, ISDN, or T1 RBS trunk can be configured on the remote units. Configuring these trunks is different than configuring SIP trunks. Refer to the configuration guide NetVanta 7000 Series Trunk Accounts for more information on how to configure these types of trunks. This guide is available online at http://kb.adtran.com, article number 1541.*

When configuring the PSTN trunks, you will need to specify the trunk type. In addition, make sure that **prefer trunk-routing** is enabled.

The PSTN trunk groups accept numbers dialed both with and without a leading 9. Outbound calls that go through the NetVanta 7000 Series unit at the main site will have the leading 9 stripped before the call reaches the remote unit. However, the leading 9 is not stripped when the NetVanta 7000 Series unit is unreachable. When the leading 9 is present, such as in a failover, the leading 9 is stripped on the voice trunk by using DNIS substitution. Enter the wildcard templates with a leading 9 as the match number (for example, **9-NXX-NXX-XXXX**) and enter the wildcard templates without the leading 9 as the substitution number (for example, **NXX-NXX-XXXX**).

When specifying the cost associated with the outbound call templates in the trunk group's configuration, set a lower cost so that analog phones on the remote unit first attempt to route their calls to the NetVanta 7000 Series unit at the main site instead of directly out the PSTN trunks. This is beneficial because the AOS units at the remote sites do not provide voice features locally.

The following steps provide sample configuration of the PSTN trunks at the remote site(s). For more specific information about ISDN trunk and trunk group configuration commands, refer to the *AOS Command Reference Guide* available online at http://kb.adtran.com (article number 2219).

1. Configure the ISDN trunk on the remote unit. This trunk is used to connect to the PSTN at the remote site.

```
voice trunk T02 type isdn
  description "PSTN"
  resource-selection linear descending
  connect isdn-group 1
  match dnis "9-NXX-XXXX" substitute "NXX-XXXX"
  match dnis "9-NXX-NXX-XXXX" substitute "NXX-NXX-XXXX"
  match dnis "9-1-NXX-NXX_XXXX" substitute "1-NXX-NXX-XXXX"
  match dnis "9-NXX" substitute "NXX"
  match dnis "9-011-$" substitute "011-$"
  rtp delay-mode adaptive
  prefer trunk-routing
```

2. Configure the PSTN trunk group on the remote unit.

```
voice grouped-trunk PRI
  no description
  trunk T02
  accept NXX-XXXX cost 200
  accept 1-NXX-NXX-XXXX cost 200
  accept 011-$ cost 200
  accept 411 cost 200
  accept 611 cost 200
  accept 911 cost 200
  accept 0-NXX-NXX-XXXX cost 200
  accept 10-10-XXX-$ cost 200
  accept 9-NXX-XXXX cost 200
  accept 9-1-NXXX-NXXX-XXXX cost 200
  accept 9-1-800-NXX-XXXX cost 200
  accept 9-1-888-NXX-XXXX cost 200
  accept 9-1-877-NXX-XXXX cost 200
  accept 9-1-866-NXX-XXXX cost 200
  accept 9-1-855-NXX-XXXX cost 200
  accept 9-011-$ cost 200
  accept 9-411 cost 200
```

```
   accept 9-611 cost 200
   accept 9-911 cost 200
   accept 9-0-NXX-NXXX-XXXX cost 200
   accept 9-10-10-XXX-$ cost 200
   reject 976-XXXX
   reject 1-900-NXX-XXXX
   reject 1-976-NXX-XXXX
   reject 9-976-XXXX
   reject 9-1-900-NXX-XXXX
   reject 9-1-976-NXX-XXXX
```

3. Configure an analog trunk at the remote site.

```
voice trunk T02 type analog supervision loop-start
  description “PSTN”
  caller-id
  trunk-number 4300
  connect fxo 0/1
  connect fxo 0/2
  match dnis “9-NXX-XXXX” substitute “NXX-XXXX”
  match dnis “9-NXX-NXX-XXXX” substitute “NXX-NXX-XXXX”
  match dnis “9-1-NXX-NXX_XXXX” substitute “1-NXX-NXX-XXXX”
  match dnis “9-NXX” substitute “NXX”
  match dnis “9-011-$” substitute “011-$”
  rtp delay-mode adaptive
  prefer trunk-routing
```

4. Configure a trunk group for the analog trunk at the remote site.

```
voice grouped-trunk ANALOG_TRUNKS
  no description
  trunk T02
   accept NXX-XXXX cost 200
   accept 1-NXX-NXX-XXXX cost 200
   accept 1-800-NXX-XXXX cost 200
   accept 1-888-NXX-XXXX cost 200
   accept 1-877-NXX-XXXX cost 200
   accept 1-866-NXX-XXXX cost 200
   accept 1-855-NXX-XXXX cost 200
   accept 011-$ cost 200
   accept 411 cost 200
   accept 611 cost 200
   accept 911 cost 200
   accept 0-NXX-NXX-XXXX cost 200
   accept 10-10-XXX-$ cost 200
   accept 9-NXX-XXXX cost 200
   accept 9-1-NXXX-NXXX-XXXX cost 200
   accept 9-1-800-NXX-XXXX cost 200
   accept 9-1-888-NXX-XXXX cost 200
   accept 9-1-877-NXX-XXXX cost 200
   accept 9-1-866-NXX-XXXX cost 200
   accept 9-1-855-NXX-XXXX cost 200
   accept 9-011-$ cost 200
   accept 9-411 cost 200
   accept 9-611 cost 200
   accept 9-911 cost 200
   accept 9-0-NXX-NXXX-XXXX cost 200
   accept 9-10-10-XXX-$ cost 200
   reject 976-XXXX
   reject 1-900-NXX-XXXX
   reject 1-976-NXX-XXXX
   reject 9-976-XXXX
   reject 9-1-900-NXX-XXXX
   reject 9-1-976-NXX-XXXX
```

5. Repeat Steps 1 through 4 for each unit at the remote site.

Enabling SIP Proxy

After configuring the PSTN trunks, the next step in configuring SIP networking is to enable SIP proxy on all remote units in the SIP network. SIP proxy must be enabled for SIP networking to function properly between the NetVanta 7000 Series product and an IP business gateway. SIP proxy must be enabled on any units at remote sites. The following configuration information is basic configuration for this application. For information about SIP proxy, refer to the configuration guide *Configuring the SIP Proxy in AOS* available online at http://kb.adtran.com (article number 2183). To configure SIP proxy on the NetVanta 7000 Series unit or the remote unit, using the CLI, follow these steps:

1. Make sure the firewall is enabled on the unit.

```
ip firewall
```

2. Enable SIP proxy in transparent mode on the unit.

```
ip sip proxy
ip sip proxy transparent
```

3. Configure SIP proxy emergency call routing. This feature forces 911 calls to immediately be routed to the PSTN trunks on the remote unit without first passing through the NetVanta 7000 Series unit at the main site.

```
ip sip proxy emergency-call-routing accept 911
ip sip proxy emergency-call-routing accept 9-911
```

4. Repeat Steps 1 through 3 on all units in the SIP network.

Configure the Remote Unit’s Analog Users

Analog users on the remote unit(s) should be configured to register to the NetVanta 7000 Series unit using the SIP trunk. For this registration, the analog user should be given a SIP identity with an authorization name and password. Follow these steps for each analog user at each remote site:

1. Configure the analog user and the user’s SIP identity.

```
voice user 4200
  connect fxs 0/1
  sip-identity 4200 T01 register auth-name 4200 password 1234
```

2. Repeat Step 1 for all analog users on each of the remote units.

Configuring Trunks on the NetVanta 7000 Series Using the CLI

After configuring the remote units, remote users, and remote phones, you must configure the necessary trunks on the NetVanta 7000 Series unit at the main site. These trunks are used for sending calls out the PSTN trunks on the remote AOS units, and for receiving calls from the PSTN trunks on the remote devices. SIP keepalives are used to make sure all units maintain the correct call state in case of network connectivity issues. When configuring these trunks, you will configure one trunk for the PSTN, and a SIP trunk for each remote AOS unit to which the NetVanta 7000 Series unit connects. The following steps provide sample configuration for the ISDN and SIP trunks on the NetVanta 7000 Series unit:

1. Configure the PSTN trunk on the NetVanta 7000 Series unit.

```
voice trunk T01 type isdn
  description “PSTN”
  resource-selection linear descending
  connect isdn-group 1
  rtp delay-mode adaptive
```

2. Configure the SIP trunk(s) on the NetVanta 7000 Series unit for the remote sites. Repeat this step to create a SIP trunk for each remote unit that communicates with the NetVanta 7000 Series unit.

```
voice trunk JT02 type sip
  description “Remote A”
  sip-server primary 10.20.20.2
  grammar from host local
  sip-keep-alive info 60
  default-ring-cadence internal
```

Configuring NetVanta 7000 Series Trunk Groups using the CLI

After you have configured the trunks on the NetVanta 7000 Series unit at the main site, you must configure the unit’s trunk groups. There are three main variations for the trunk group configuration, and each variation determines which users can use which PSTN trunks. The first option is to allow users from all sites to use all trunks in a true LCR scenario. The second option is to allow the remote site users to use their local trunks for local calls, but force all long distance calls out the PRI at the main site. The final option is to only allow users to use their local trunks for all calls. The following sections describe the configuration of these three scenarios, providing you with three LCR configuration options.

For these configurations, ANI and trunk lists are used to force 7-digit local dialing out of the correct trunk. The trunk lists are needed because when a phone is forwarded, the call is considered to have originated form the trunk on which it was received. ANI and trunk lists must be configured and applied to the appropriate trunk group using the CLI.

Trunk Groups for True LCR Configuration

The first trunk group configuration option provides a method for configuring true LCR. In a true LCR scenario, the trunks on the remote sites are used for calls that are local to those sites, and the PRI off the NetVanta 7000 Series unit at the main site is used for all other calls.

The sample configuration for this scenario is as follows:

```
voice ani-list Local_ANI
  ani 2XXX
!
voice ani-list Remote_A_ANI
   ani 3XXX
!
voice ani-list Remote_B_ANI
   ani 4XXX
!
voice trunk T04 type sip
  description "Remote A"
  match dnis 1-615-NXX-XXXX sub NXX-XXXX
  sip-server primary 10.20.20.2
  grammar from host local
  default-ring-cadence internal
!
voice trunk T05 type sip
  description "Remote B"
  match dnis 1-205-NXX-XXXX sub NXX-XXXX
  sip-server primary 10.30.20.2
  grammar from host local
  default-ring-cadence internal
  !
voice grouped-trunk PRI
  no description
  trunk T01
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 0-NXX-NXX-XXXX cost 0
  accept 10-10-XXX-$ cost 0
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
!
voice grouped-trunk PRI_LOCAL_DIALING
  no description
  trunk T01
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  reject 976-XXXX
  permit list Local_ANI
!
voice grouped-trunk REMOTE_A_LOCAL_DIALING
  no description
  trunk T024
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  permit list Remote_A_ANI
!
voice grouped-trunk REMOTE_A_REMOTE_DIALING
  no description
  trunk T04
  accept 1-615-NXX-XXXX cost 0
  permit list Local_ANI
  permit list Remote_B_ANI
!
voice grouped-trunk REMOTE_B_LOCAL_DIALING
  no description
  trunk T05
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  permit list Remote_B_ANI
!
voice grouped-trunk REMOTE_B_REMOTE_DIALING
  no description
  trunk T05
  accept 1-205-NXX-XXXX cost 0
  permit list Local_ANI
  permit list Remote_A_ANI
```

Trunk Groups Configured for Remote Sites to Use Local Trunks for Local Calls

The second trunk group configuration option provides a method for configuring the remote sites to use local trunks for local calls. In this scenario, users at the remote sites are permitted to use their trunks for local calls, but long distance calls are routed out the PRI at the main site.

The sample configuration for this scenario is as follows:

```
trunk T01
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 0-NXX-NXX-XXXX cost 0
  accept 10-10-XXX-$ cost 0
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
!
```

```
voice grouped-trunk PRI_LOCAL_DIALING
  no description
  trunk T01
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  reject 976-XXXX
  permit list Local_ANI
!
voice grouped-trunk REMOTE_A_LOCAL_DIALING
  no description
  trunk T04
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  permit list Remote_A_ANI
!
voice grouped-trunk REMOTE_B_LOCAL_DIALING
  no description
  trunk T05
  accept NXX-XXXX cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  permit list Remote_B_ANI
```

Trunk Groups Configured for Remote Sites to Use Local Trunks for All Calls

The third trunk group configuration option provides a method for configuring the remote sites to use local trunks for all calls. In this scenario, users from each site only use the trunks that are local to their site.

The sample configuration for this scenario is as follows:

```
voice ani-list Local_ANI
  ani 2XXX
!
voice ani-list Remote_A_ANI
  ani 3XXX
!
voice ani-list Remote_B_ANI
  ani 4XXX
!
voice grouped-trunk PRI
  no description
  trunk T01
  accept NXX-XXXX cost 0
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  accept 0-NXX-NXX-XXXX cost 0
  accept 10-10-XXX-$ cost 0
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
  permit list Local_ANI
!
voice grouped-trunk REMOTE_A_TRUNKS
  no description
  trunk T04
  accept NXX-XXXX cost 0
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  accept 0-NXX-NXX-XXXX cost 0
  accept 10-10-XXX-$ cost 0
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
  permit list Remote_A_ANI
  permit list Remote_A_Trunks
!
voice grouped-trunk REMOTE_B_LOCAL_DIALING
  no description
  trunk T05
  accept NXX-XXXX cost 0
  accept 1-NXX-NXX-XXXX cost 0
  accept 1-800-NXX-XXXX cost 0
  accept 1-888-NXX-XXXX cost 0
  accept 1-877-NXX-XXXX cost 0
  accept 1-866-NXX-XXXX cost 0
  accept 1-855-NXX-XXXX cost 0
  accept 011-$ cost 0
  accept 411 cost 0
  accept 611 cost 0
  accept 911 cost 0
  accept 0-NXX-NXX-XXXX cost 0
  accept 10-10-XXX-$ cost 0
  reject 976-XXXX
  reject 1-900-NXX-XXXX
  reject 1-976-NXX-XXXX
```

permit list Remote_B_ANI
permit list Remote_B_Trunks

Configuring a SIP Network Between NetVanta 7000 Series and Routers

SIP networking between a NetVanta 7000 Series unit and a NetVanta router generally occurs when the NetVanta 7000 Series platform is used at the main enterprise site, and NetVanta routers are used at remote enterprise locations. The configuration of this type of SIP networking is very similar to SIP networking between NetVanta 7000 Series units and an IP business gateway. However, when configuring a SIP network with a NetVanta router, you must consider which router is best for your application. If a SIP trunk exists on the NetVanta 7000 Series unit, policy based routing (PBR) could be required if you are networking with a NetVanta 3120. PBR in this case ensures that call signaling and audio pass between the sites. Product selection also depends on the number of phones at the remote location. If there are only one or two phones at the remote location, the NetVanta 3120 can be used. If there are more than two phones, however, you should use the NetVanta 3400 for SIP networking.

To configure SIP networking between a NetVanta 7000 Series product and a NetVanta router using the GUI, follow the steps outlined in *Configuring a SIP Network between NetVanta 7000 and IP Gateways on page 31*.

To configure SIP networking between a NetVanta 7000 Series product and a NetVanta router using the CLI, follow the steps outlined in *Configuring SIP Networking with IP Business Gateways using the CLI on page 59*.

NOTE *Only the VPN, QoS, and SIP proxy configurations are necessary on the NetVanta routers. The configuration for the NetVanta 7000 Series unit is, however, the same.*