AOS Common Application Guide
NetVanta 7100 – Remote Phone over VPN

Overview

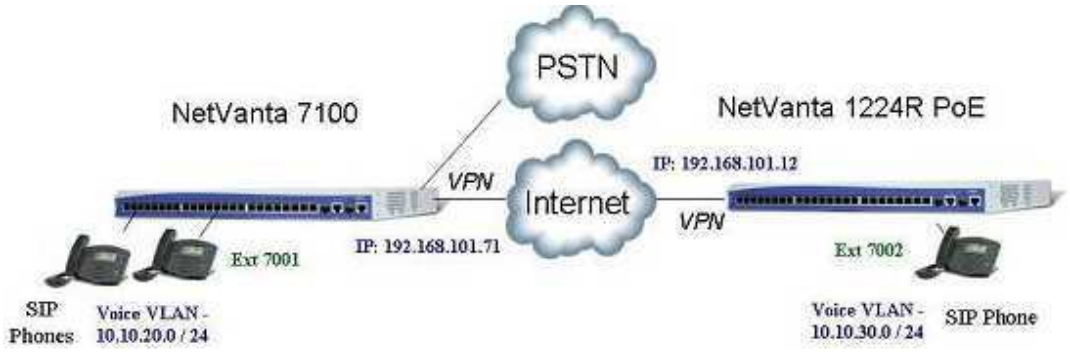
With the release of AOS 15, new configuration options have been added to the menu of the NetVanta 7100 to accommodate remote phones connected over a VPN Tunnel. This document is designed to outline this new feature and explain the configuration options. It assumes that the Internet and firewall settings have already been applied.

Hardware/Software Requirements/Limitations

A NetVanta 7100 with AOS 15.01.00 or above is required for this specific application.

Configuration

The diagram below is the example scenario that will be referenced throughout the remainder of this document. In our example, the remote device is an ADTRAN NetVanta 1224R PoE, but the same techniques and principles would apply to any VPN termination device at the remote site.



This scenario requires two VPN tunnels between the two sites. The primary LAN-to-LAN tunnel will handle RTP between phones at the main site and the remote site. A second VPN tunnel is needed to handle traffic between the NetVanta 7100 and the remote LAN. Examples of the traffic this VPN tunnel will support include SIP, FTP of configuration files, voicemail prompts and recording, and auto-attendant interaction. Lastly, steps need to be taken to ensure that the remote phone operates under a different profile than phones directly connected to the NetVanta 7100 at the main site.

Step 1 – Setup the Main VPN Tunnel between the Two Sites

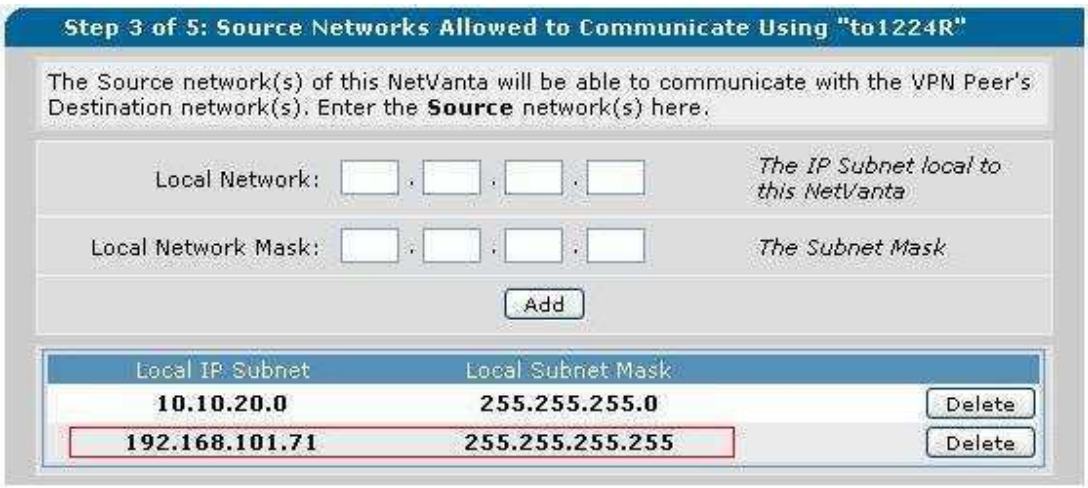
The process of setting up VPN tunnels can be done using the **VPN Wizard**, which is

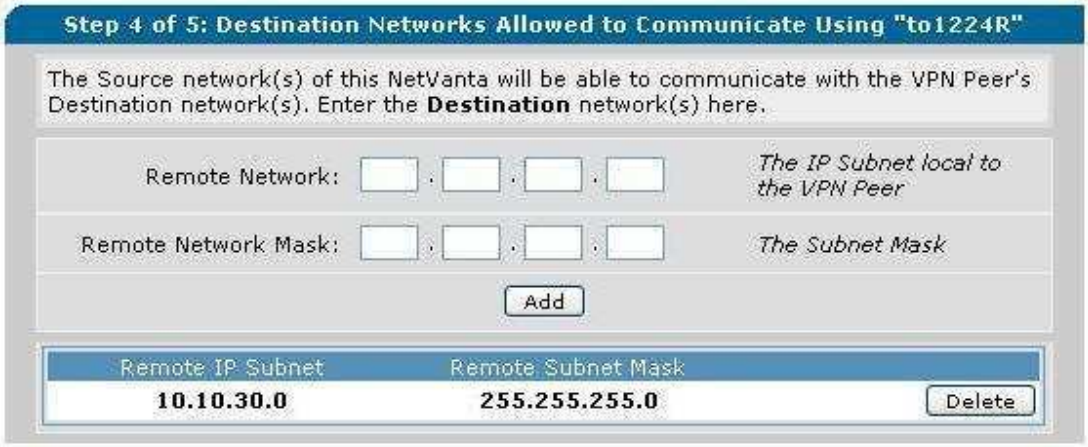
supported on all ADTRAN OS devices which have web GUI support. The first tunnel created should allow for traffic between the two voice VLANs. In this example, the first tunnel will allow for IP traffic to flow in both directions between the 10.10.20.0/24 and 10.10.30.0/24 subnets. For information about using the **VPN Wizard** to setup this tunnel, see the documents titled, "Understanding the VPN Menu in the AOS Web Interface" or "Configuring a VPN using Main Mode in AOS". Both documents are located in the knowledgebase at http://kb.adtran.com/.
The configuration can also be done via the Command Line Interface (CLI) and example configurations will be included at the end of this document for reference purposes. However, using the **VPN Wizard** for the initial VPN tunnel settings can save time by preventing setting mismatches.

Step 2 – Setup the Second VPN Tunnel Between the NetVanta 7100 WAN IP Address and the Remote LAN

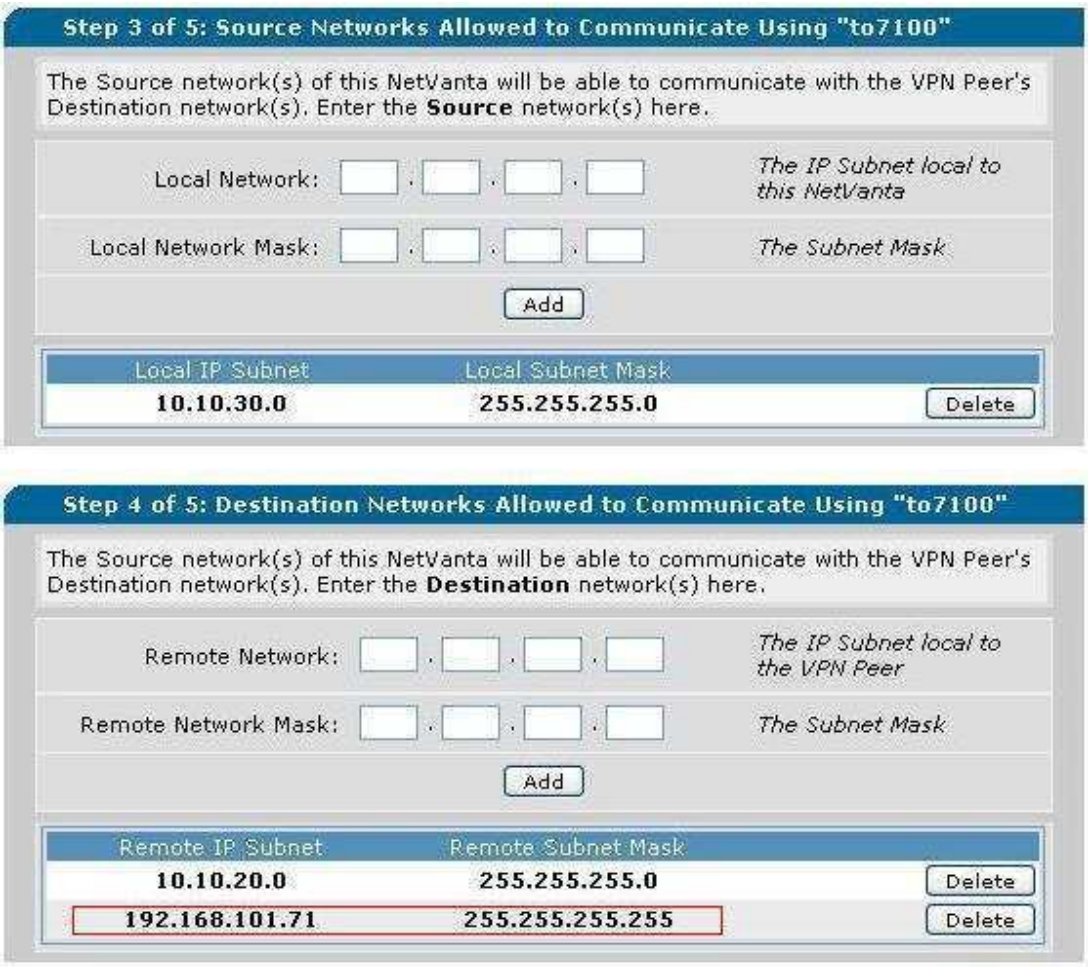
A second VPN tunnel is needed to handle traffic between the NetVanta 7100 and the remote subnet. To create this new VPN tunnel, it is only necessary to add a new VPN traffic selector to each side since it will be between the same two devices as the original VPN tunnel. The new selector is configured by clicking on the **VPN Peers** link under the Data section of the web GUI and then clicking on the name of the VPN peer.

Now the additional source network can be defined on the NetVanta 7100 as follows. Be sure to click the **Apply** button at the bottom of the page after the network has been added.



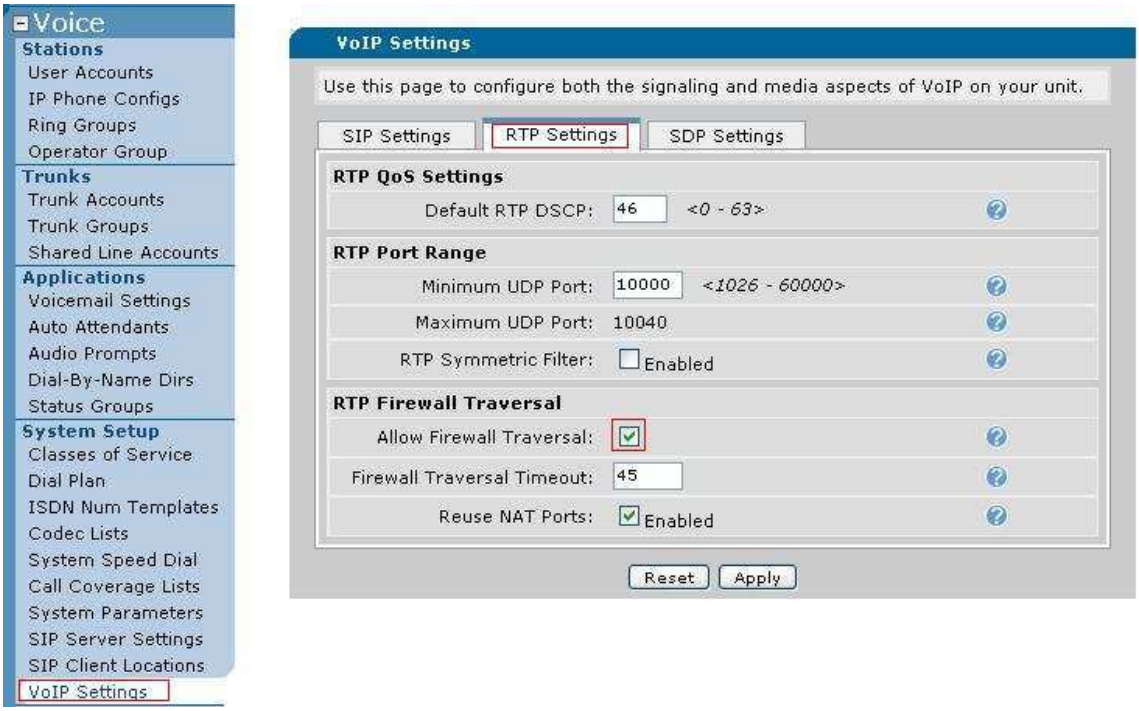


Similarly, a corresponding Destination network needs to be defined on the remote side unit. Below is an example of the selectors that would be defined on the NetVanta 1224R PoE.



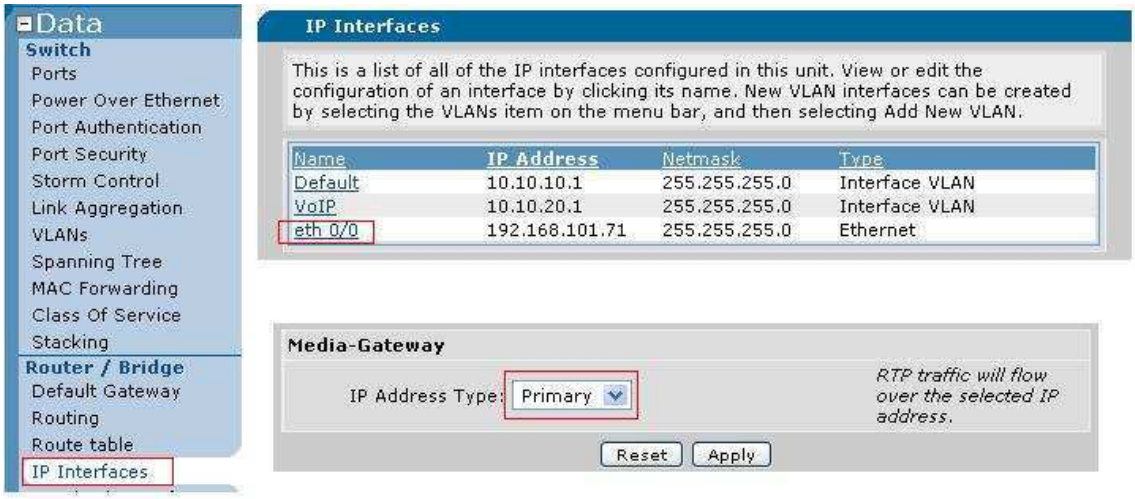
Step 3 – Enable RTP Firewall Traversal in the NetVanta 7100

Click on the **VoIP Settings** link in the Voice section of the GUI. Then click the **RTP Settings** tab to verify that RTP Firewall Traversal is enabled. This enables the firewall in the NetVanta 7100 to dynamically allow RTP streams through as calls come up.



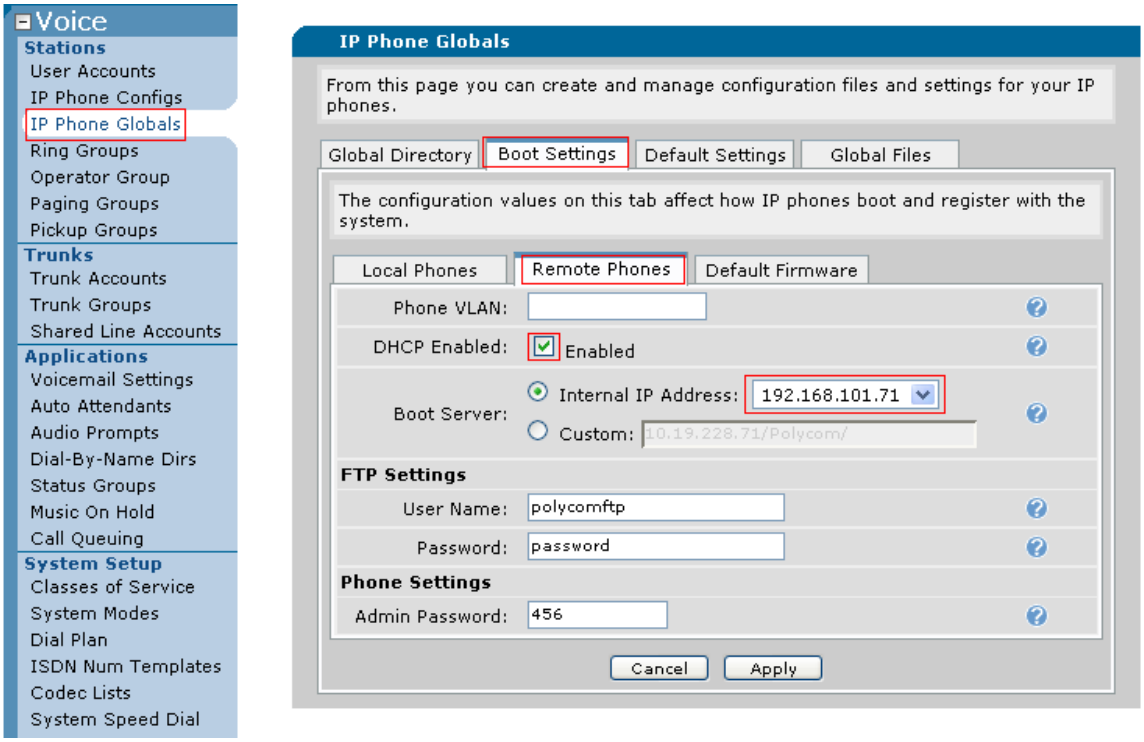
Step 4 – Define the Media-Gateway on the WAN Interface of the NetVanta 7100

The Media-Gateway will need to be defined as primary on the WAN interface. In this example, the WAN interface is Ethernet 0/0. The WAN Interface on some installations may require this setting be applied on a virtual (PPP, HDLC, etc.) or VLAN interface. The Media-Gateway setting can be reached by clicking the **IP Interfaces** link under the Data section of the NetVanta 7100. Then click on the specific WAN interface.



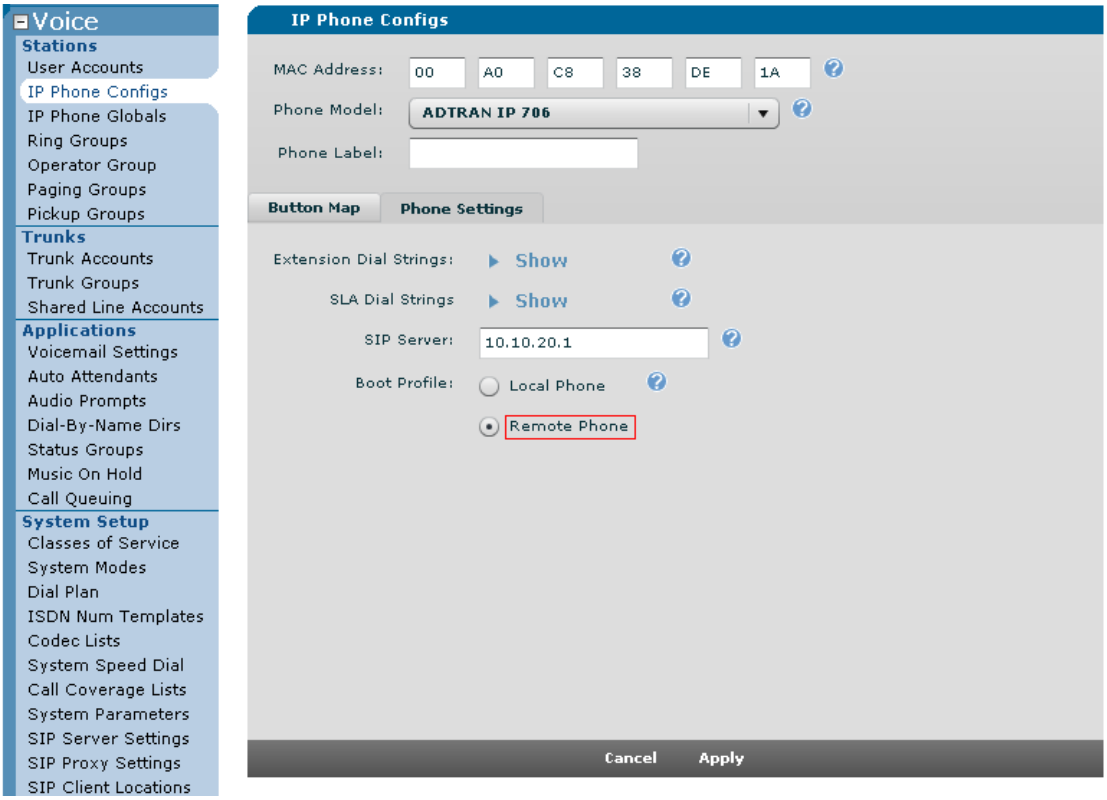
Step 5 – Setup the Remote User Profile

Remote SIP phones need to be able to download a different configuration file than SIP phones connected locally to the NetVanta 7100. This allows for flexibility in the configuration of phones in different locations. In this example, the Remote Phone profile will be defined to use DHCP and will contact the boot server at the NetVanta 7100's WAN IP address of 192.168.101.71. The administrator should select **IP Phone Globals** and then the **Boot Settings** tab to make these changes.



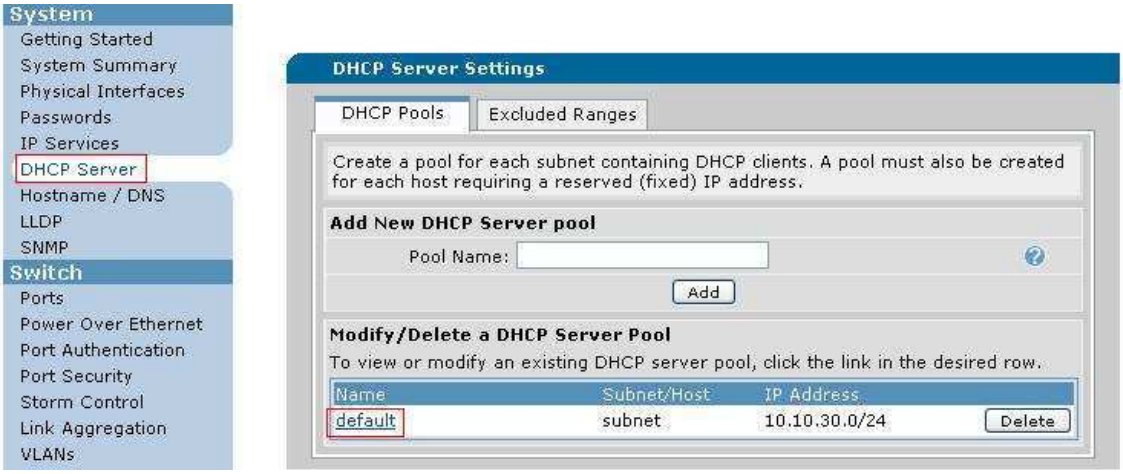
Step 6 – Define a Remote Voice User

Setup the remote voice user as described in the NetVanta 7100 Administrator Guide and dealer certification training material. Once the remote voice user has been created, it will need to be configured to use the remote user profile. This is done by clicking on the **IP phone Configs** link in the Voice section of the NetVanta 7100. Then click on the MAC address of the remote phone followed by the **Phone Settings** tab. At the bottom of this screen the **Boot Profile** should be changed to Remote Phone.



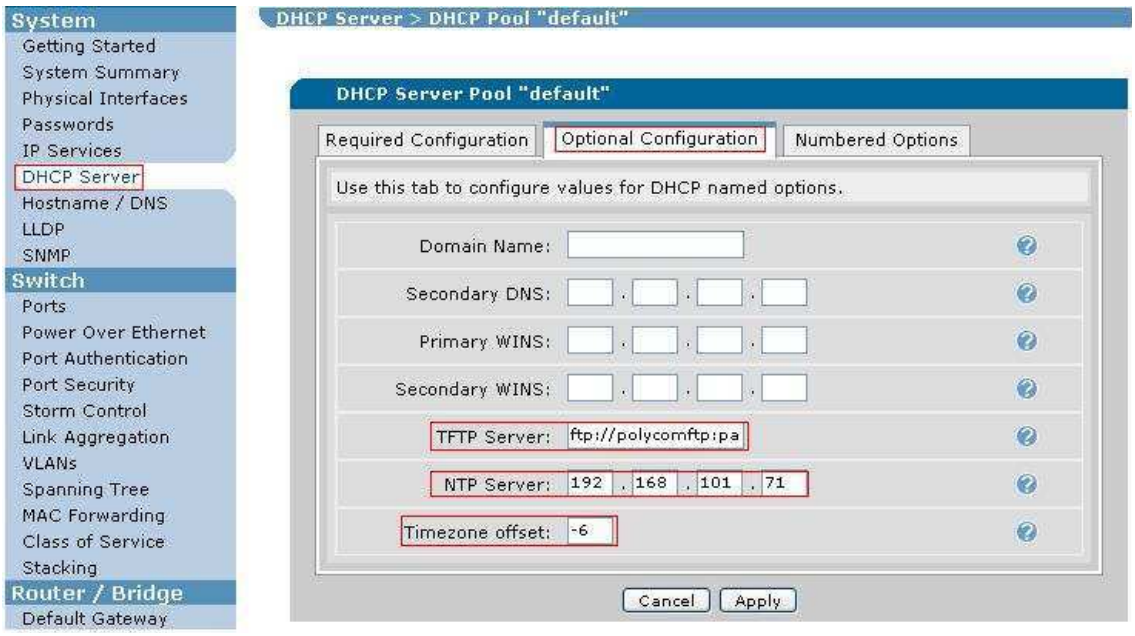
Step 7 – Configure DHCP on the NetVanta 1224R PoE for the Remote Phone

The remote phone will need to learn its IP address and boot server options via DHCP or be statically configured with this information. In this example, the remote phone will be using DHCP. In the NetVanta 1224R PoE, the administrator should click on **DHCP Server** and then click on an existing DHCP pool or **Add** a new pool.



After configuring the required network settings to be handed out via DHCP, click on the

Optional Configuration tab to enter the important phone specific options. The TFTP Server has been defined as ftp://polycomftp:password@192.168.101.71/Polycom/ and the NTP Server has been defined as 192.168.101.71. Lastly, the Timezone offset will need to be configured before clicking Apply at the bottom of the page.



Step 8 – Implement Quality of Service on all Devices between the Two VoIP Endpoints

Quality of Service (QoS) is a requirement anywhere time sensitive traffic, such as VoIP, will be using the same bandwidth as a user's regular data traffic. The NetVanta 7100 administrator should implement QoS on any interface that runs at lower than Ethernet rates, such as a T-1 interface. Also, traffic shaping and QoS should be used on Ethernet interfaces that will connect to devices such as cable or ADSL modems that may not have the feature set to implement QoS or prioritization or voice traffic. The guide titled "Configuring QoS Priority Queuing in AOS" available at http://kb.adtran.com can be used as a resource when configuring QoS.

Step 9 – Verify Operation of Remote Phone

Install and deliver power to the Remote Phone. After the phone has had an opportunity to download its configuration files and register its extension, the administrator should verify that it is possible to call voice users at the main site, access voicemail, and utilize any auto attendants that may be configured.

Troubleshooting

The following can be used as a basic guideline to help isolate any problem that is

preventing the remote phone from working properly.

- Verify that both sites have access to the Internet using a computer on the LAN.
- Check that the remote phone is getting DHCP from the remote side router by using the **debug ip dhcp-server** command and then power-cycling the phone.
- Ensure that the VPN tunnel is coming up by using the **show crypto ipsec sa** command. If not, use the **debug crypto ike** command to view the negotiation of the VPN tunnel. A VPN tunnel can be triggered by issuing a ping from one LAN to the other or by utilizing the **source** keyword in a ping from within a NetVanta. For the example discussed in this guide, using **ping 10.10.30.1 source 10.10.20.1** while logged into the NetVanta 7100 would trigger an attempt to negotiate a VPN tunnel since this traffic matches the VPN selectors.
- Confirm that the remote phone is attempting to establish communications with the NetVanta 7100 by using the **show ip policy-sessions** command on the NetVanta 7100 and the remote router to view firewall sessions. Verify that no NAT is taking place on these sessions.
- Check that the NetVanta 7100 is receiving FTP requests from the remote side phone and successfully transferring configuration files by using the **debug ip ftpserver** command on the NetVanta 7100. Reference the guide titled "Polycom Phone Operation", document #2049, which can be found in the knowledgebase at http://kb.adtran.com for detailed information and sample debug output.
- Ensure that the remote phone is registering properly and able to pass SIP messaging to bring up a phone call by using the **debug sip stack messages** command.
- Utilize **debug voice summary** on the NetVanta 7100 to track down common configuration problems.

Configuration Samples

The relevant portion of the NetVanta 7100 configuration discussed in this guide is included below.

```
!
hostname "NV7100"
!
username "polycomftp" password "password"
!
ip firewall
ip rtp firewall-traversal
ip rtp firewall-traversal reuse-nat-ports
!
!
ip crypto
!
crypto ike policy 100
initiate main
respond main
local-id address 192.168.101.71
peer 192.168.101.12
attribute 1
encryption 3des
hash md5
authentication pre-share
```

```
!
crypto ike remote-id address 192.168.101.12 preshared-key adtranadtran
ike-policy 100 crypto map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
mode tunnel
!
crypto map VPN 10 ipsec-ike
description to1224R
match address VPN-10-vpn-selectors
set peer 192.168.101.12
set transform-set esp-3des-esp-md5-hmac
ike-policy 100
!
!
interface eth 0/0
ip address 192.168.101.71 255.255.255.0
access-policy Public
crypto map VPN
media-gateway ip primary
no shutdown
no lldp send-and-receive
!
interface vlan 1
ip address 10.10.10.1 255.255.255.0
access-policy Private
media-gateway ip primary
no shutdown
interface vlan 2
ip address 10.10.20.1 255.255.255.0
access-policy Private
media-gateway ip primary
no shutdown
!
ip access-list standard wizard-ics
remark Internet Connection Sharing
permit any
!
ip access-list extended VPN-10-vpn-selectors
permit ip 10.10.20.0 0.0.0.255 10.10.30.0 0.0.0.255
permit ip host 192.168.101.71 10.10.30.0 0.0.0.255
!
!
ip policy-class Private
allow list VPN-10-vpn-selectors stateless
nat source list wizard-ics interface eth 0/0 overload
!
ip policy-class Public
allow reverse list VPN-10-vpn-selectors stateless
!
ip route 0.0.0.0 0.0.0.0 192.168.101.254
!
```

Below is the relevant portion of the NetVanta 1224R PoE configuration.

```
!
hostname "NV1224R"
!
ip firewall
!
ip dhcp-server pool "default"
network 10.10.30.0 255.255.255.0
dns-server 10.10.30.1
```

```
netbios-node-type h-node
default-router 10.10.30.1
tftp-server ftp://192.168.101.71/Polycom/
ntp-server 192.168.101.71
timezone-offset -6
!
ip crypto
!
crypto ike policy 100
initiate main
respond main
local-id address 192.168.101.12
peer 192.168.101.71
attribute 1
encryption 3des
hash md5
authentication pre-share
!
crypto ike remote-id address 192.168.101.71 preshared-key adtranadtran
ike-policy 100 crypto map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
mode tunnel
!
crypto map VPN 10 ipsec-ike
description to7100
match address VPN-10-vpn-selectors
set peer 192.168.101.71
set transform-set esp-3des-esp-md5-hmac
ike-policy 100
!
!
interface vlan 1
ip address 10.10.30.1 255.255.255.0
access-policy Private
no shutdown
interface vlan 100
ip address 192.168.101.12 255.255.255.0
access-policy Public
crypto map VPN
no shutdown
!
ip access-list standard wizard-ics
remark Internet Connection Sharing
permit any
!
ip access-list extended VPN-10-vpn-selectors
permit ip 10.10.30.0 0.0.0.255 10.10.20.0 0.0.0.255
permit ip 10.10.30.0 0.0.0.255 host 192.168.101.71
!
ip policy-class Private
allow list VPN-10-vpn-selectors stateless
nat source list wizard-ics interface vlan 100 overload
!
ip policy-class Public
allow reverse list VPN-10-vpn-selectors stateless
!
ip route 0.0.0.0 0.0.0.0 192.168.101.254
!
```