TALKSWITCH DOCUMENTATION

TALKSWITCH VOIP NETWORK TROUBLESHOOTING GUIDE

RELEASE 3.24

CT.TS005.008001

talkswitch®

ANSWERS WITH INTELLIGENCE®

First Edition, September 2006.
CT.TS005.008001

TalkSwitch is a division of Centrepoint Technologies Inc.

TABLE OF CONTENTS

1. INTRODUCTION

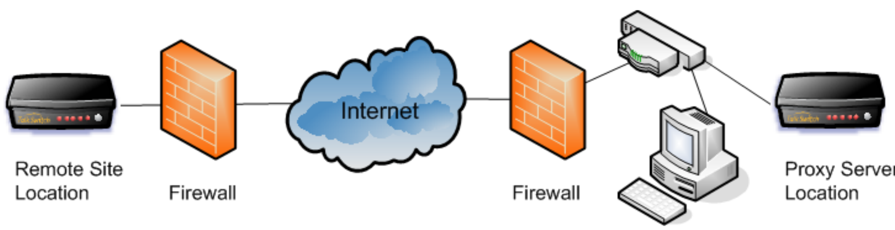
This guide assumes you are having difficulties with VoIP calls in a branch-to-branch configuration and you have already configured the following configuration settings in both the proxy server and remote site locations:

- IP addresses for private, public and proxy server network settings.
- VoIP and Line Hunt Group numbers.
- Services in the router IP mapping tables.

This guide describes the following steps:

- Verifying existing TalkSwitch configuration settings.
- Attempting a VoIP call and troubleshooting specific problems.

During the VoIP call attempt, you will be redirected to specific places in the configuration settings in order to help pinpoint the exact problem. The following figure depicts a simple branch-to-branch VoIP setup with one remote site location and the proxy server location.

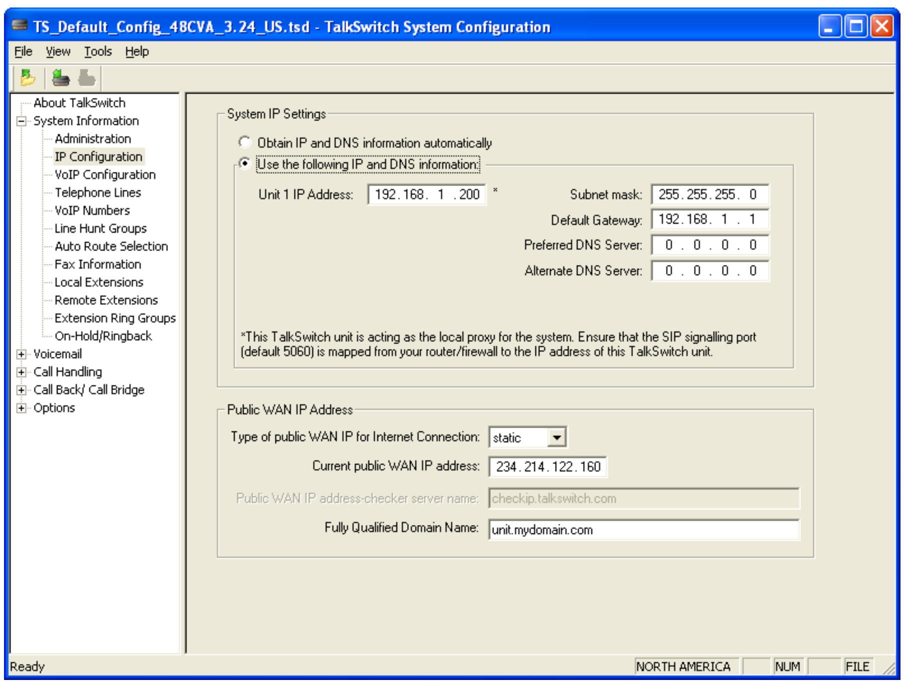


2. VERIFYING CONFIGURATION SETTINGS

Verify the TalkSwitch unit configuration settings contained in this section for the remote site and proxy server locations. This section also lists additional configuration setting information to help you determine possible errors in your TalkSwitch settings.

2.1 IP CONFIGURATION

The *System IP Settings* section displays the TalkSwitch unit private IP address. We recommend a static IP address for a TalkSwitch unit behind a firewall. The *Public WAN IP Address* section displays the IP address seen from outside the network and may be a public, or TalkSwitch unit IP address.



2.1.1 System IP Settings

If the unit uses a static IP address, verify that the IP addresses under *Use the following IP and DNS information* are correct and that the *Default Gateway* is within the *Subnet mask* range.

If DHCP is enabled (*Obtain IP and DNS information automatically* is selected) the unit IP addresses are grayed out and display the latest addresses retrieved by the DHCP server.

Verify that the MAC address is reserved or that the firewall supports UPnP (firewall specific information).

If the Unit IP Address is public, ensure the unit is not behind a firewall.

Test: Ping the IP address to verify that it is valid.

2.1.2 Public WAN IP Address

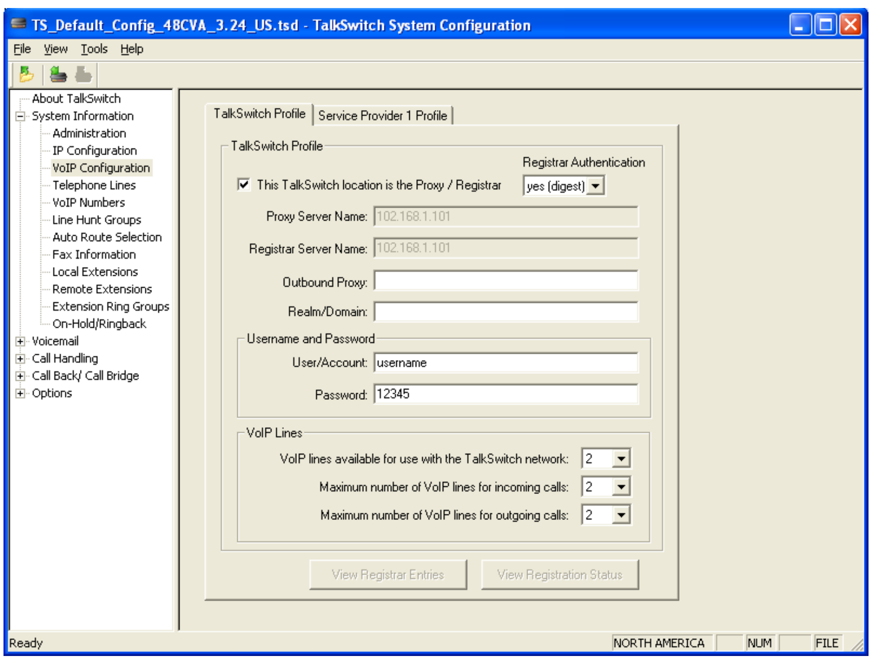
If the IP address is static, verify the address.

If the IP address is dynamic, check the address using an address-server checker (such as checkip.talkswitch.com). If FQDN is enabled, confirm the spelling of the domain name and ensure a utility exists to update the domain when it changes.

Test: Ping the FDQN name to verify that it is valid and matches the value in the *Current public WAN IP address* field.

2.2 VOIP CONFIGURATION

The *TalkSwitch Profile* section displays the Proxy and Registrar IP addresses or domain names. The *Username and Password* section contains authentication details for all TalkSwitch units making up the branch-to-branch VoIP configuration.



2.2.1 Proxy/Registrar

One unit or location must be set as the proxy server for all locations in the branch-to-branch VoIP configuration. Selecting the *This TalkSwitch is the Proxy / Registrar* box populates the server name boxes with the unit public IP address. Unchecking then rechecking this box updates the Server Names entries. The *Registrar Authentication* option turns authentication on or off.

If this location is the proxy/registrar, make sure the box is checked and verify the server name addresses and that both the proxy and the registrar entries are the same.

If FDQN is used, make sure the entries are typed correctly.

Verify that all locations have the proper proxy/registrar IP addresses.

Note: Leave the *Outbound Proxy* IP field blank, as it is not required for this type of configuration.

2.2.2 Username and Password

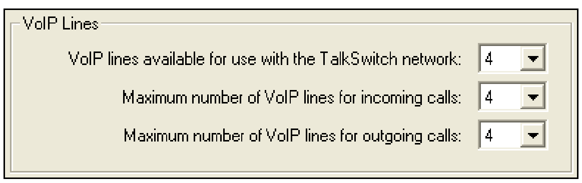
All locations must have matching username and password entries used for authentication purposes. If no Realm/Domain is entered, TalkSwitch will sub in 'norealm' for the authentication packets.

If authentication is enabled by selecting *yes(digest)* in the *Registrar Authentication* option, ensure the username and password are the same in all locations.

Note: Authentication is not required in a branch-to-branch VoIP configuration.

2.2.3 VoIP Lines

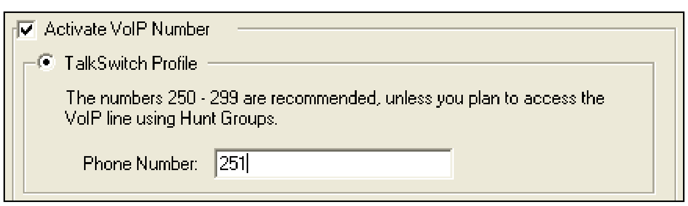
The *VoIP Lines* option is found in **System Information -> VoIP Configuration**.



Ensure the number of VoIP lines is set to a value other than zero.

2.3 VOIP NUMBERS

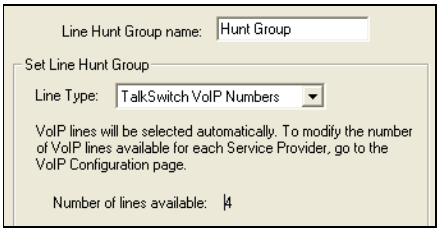
The *Activate VoIP Number* option is found in **System Information -> VoIP Numbers**.



Ensure all locations have at least one VoIP number activated and that no two locations have the same VoIP number assignment.

2.4 LINE HUNT GROUPS

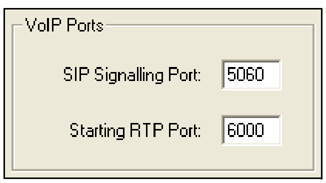
The *Set Line Hunt Group* options are found in **System Information -> Line Hunt Groups**.



Choose a hunt group and *TalkSwitch VoIP Numbers* as the *Line Type*. By default, hunt group 88 is set to use the TalkSwitch VoIP lines.

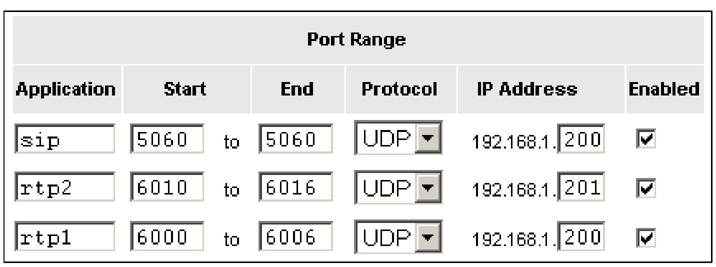
2.5 SIP AND RTP PORT ASSIGNMENTS

The *VoIP Ports* options are found in **Options -> Troubleshooting -> Advanced**.



TalkSwitch uses 5060 for SIP signalling and 6000+ for RTP packets. These values are set in the firewall routing table.

2.6 FIREWALL PORT MAPPINGS



	Port Range					
Application	Start		End	Protocol	IP Address	Enabled
sip	5060	to	5060	UDP	192.168.1.200	☑
rtp2	6010	to	6016	UDP	192.168.1.201	☑
rtp1	6000	to	6006	UDP	192.168.1.200	☑

Verify the firewall settings for services listing both SIP and RTP ports.

5060 should be forwarded to the IP address of Box 1 (UDP).

Confirm the RTP ranges for each TalkSwitch unit.

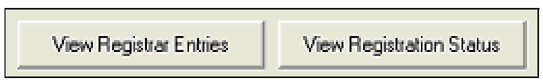
Range of RTP Ports

Unit	Start RTP	End RTP	Type
Unit 1	6000	6006	UDP
Unit 2	6010	6016	UDP
Unit 3	6020	6026	UDP
Unit 4	6030	6036	UDP

Note: Port 9393 may also need to be mapped to the TalkSwitch unit for TCP/IP access configuration.

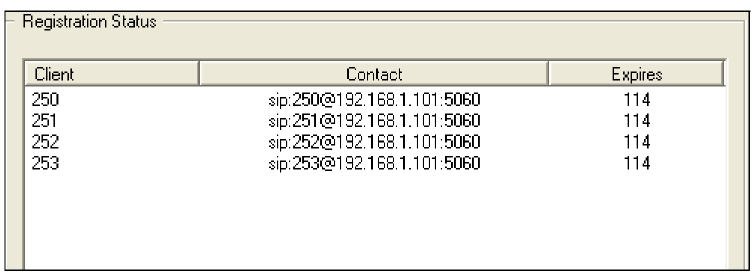
2.7 REGISTRAR

You can verify registration of the units within the TalkSwitch configuration software. On the **VoIP Configuration** software page you have the options to **View Registration Status** and in a branch-to-branch scenario you will be able to **View Registrar Entries**.



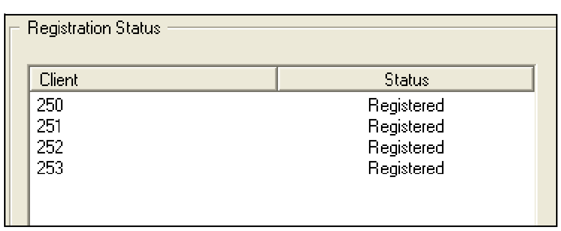
2.7.1 View Registrar Entries

This button will display all VoIP numbers registered to the CVA with their current public IP address and SIP port. Confirm all units are listed with their corresponding IP addresses.



2.7.2 View Registration Status

This button will display the unit's VoIP numbers and current registration status.



3. TESTING YOUR CONFIGURATION

This section describes using registration and placing a remote to proxy site VoIP call to pinpoint the location of possible system configuration errors which may be causing the problem.

3.1 VERIFY REGISTRATION

The steps below follow a sequence to ensure proper registration of the remote and proxy units. If the remote and proxy units are registered, then initiate a VoIP call as described in *Initiate the VoIP Call* on page 8, otherwise, follow the steps below to check the following configuration settings, in order:

- Authentication
- Proxy location SIP port mapping and remote location IP address
- Remote location SIP port mapping

If the unit's client VoIP numbers are not registered, check to see if authentication settings are causing the problem (if you are not using Registrar Authentication, skip the procedure below):

1. At the proxy registrar location, go to **System Information -> VoIP Configuration**, then set the *Registrar Authentication* field to *none*.
2. Perform a configuration save at the proxy location, followed by a configuration save at the remote location. This will attempt to register the remote location with the proxy location.
3. Check the registration status again at the proxy location.
4. If the proxy and remote locations are now registered, the authentication values at the remote location were causing the problem. You can now initiate a VoIP call.

The following steps will verify the registration status of the remote location to verify if proxy location SIP port 5060 is valid and if the remote location IP address is configured properly:

1. Go to **System Information -> IP Configuration** at the remote location and verify that the public IP address setting is correct.
2. Go to **System Information -> VoIP Configuration** at the remote location and confirm that the correct IP addresses are entered for the *Proxy* and *Registrar Server* names.
3. At the proxy registrar location, verify that the firewall port mappings for SIP have 5060 pointing to the proxy location private IP address settings.
4. Go to **System Information -> VoIP Configuration** at the proxy location, then click the **View Registrar Entries** button. If registered, go to the next section, otherwise, redo this section starting with Step 1 above.

The following steps will verify the registration status of the remote location to verify if SIP port 5060 is configured properly:

1. Go to **System Information -> VoIP Configuration** at the remote site, then click the **Registration Status** button. If registered, go to section 3.1 below and initiate a VoIP call.
2. Verify that the firewall port mappings for SIP have 5060 pointing to the proxy location private IP address settings.
3. Perform a configuration save at the proxy location, followed by a configuration save at the remote location.
4. If the proxy and remote locations are now registered, the port mapping values at the remote location were causing the problem. You can now initiate a VoIP call.

3.2 INITIATE THE VOIP CALL

From the remote site location, dial a valid VoIP number for the proxy server location that is set to ring an extension only. This will verify the remote and proxy location SIP mappings, as well as the public IP and proxy server IP addresses at the remote location. If the proxy location doesn't ring or no ringing is heard from the remote location, confirm the remote and proxy units are registered and attempt the call again.

3.3 ANSWER THE VOIP CALL

With ringing heard at the proxy and remote locations, check for audio to verify the RTP settings.

3.3.1 Audio received at proxy location

If audio is received at the proxy location, then the RTP settings in the proxy location router mapping table are correct.

3.3.2 No audio received at proxy location

If no audio is received at the proxy location, verify the following:

- Proxy location RTP settings. For more information, refer to *SIP and RTP Port Assignments* on page 5.

3.3.3 Audio received at remote location

If audio is received at the remote location, then the RTP settings in the remote location router mapping table are correct and VoIP is properly configured.

3.3.4 No audio received at remote location

If no audio is received at the remote location, verify the following:

- Proxy location RTP settings. For more information refer to *SIP and RTP Port Assignments* on page 5.

If you encounter any difficulties not covered in this guide, please contact Technical Support.