June 17, 2015

Data Network Best Practices for ShoreTel SKY VoIP

Description: The purpose of this document is to summarize the requirements for the ShoreTel hosted local customer network environment.

Environment: ShoreTel SKY
# Table of Contents

Introduction .................................................................................................................. 3  
Customer Site Cable Plant Requirements ................................................................. 3  
What are known issues on a data network? ............................................................... 4  
Customer Data Network Equipment Requirements .................................................. 5  
What about disaster recovery? .................................................................................. 6  
Configuring VLANs for ShoreTel IP Phones ............................................................ 7  
Automatic IP Phone VLAN Assignment – LLDP-MED ............................................ 9  
Off-Net Firewall Best Practices ............................................................................... 11  
Cisco SB switch settings – Auto Smartport & EEE ............................................... 15  
References ............................................................................................................... 16  
**Introduction**

The topics discussed below are intended to give the customer a solid understanding of how to VoIP enable their data network to support ShoreTel Sky VoIP services. Please consider the topics carefully when deciding on procuring specific data networking equipment makes and models. As long as the customer data networking equipment meets the following minimum standards and best practices, ShoreTel Sky hosted VoIP services can be configured and should function properly as designed. For any additional questions not covered in this document, please consult your ShoreTel Sky Technical Network Resource.

**Customer Site Cable Plant Requirements**

To avoid the possibility of lost packets due to corrupted electrical signals, the Ethernet wire plant and associated patch cables to each IP-phone, IAD, or network device, should be a minimum of CAT-5 UTP cable.

Ideally, each station-pull should be certified for conformance to IEEE 802.3 specifications with a commercially available CAT-5 cable tester. The tester should include conformance tests for db insertion loss, cross talk, impedance, wire mapping, and capacitance.

**Half/Full-Duplex**

Ethernet interfaces operate in either half-duplex or full-duplex mode.

In half-duplex mode, only one Ethernet frame can be transmitted across the interface at a time in either direction. If both devices should begin transmitting frames at the same time, a collision is detected and both devices abort their transmissions and retry again later. This situation adds delay, at minimum, and can cause packets to be discarded when excessive collisions occur.

In full-duplex mode, Ethernet frames can be sent in both directions simultaneously, thereby doubling the available bandwidth and eliminating the possibility of collisions and their associated delays and lost packets. With VOISS networks, it is desirable for all Ethernet interfaces carrying RTP-voice traffic to operate in full-duplex mode. This is a mandatory requirement for RTP traffic aggregation points, such as (switch-to) router, firewall, gateway, streaming server, and other-switch interfaces that carry numerous RTP flows simultaneously.

**Auto (Duplex) Negotiation Configuration**

Most Ethernet switches and station devices perform automatic duplex negotiation, and default to this mode of operation. When two auto-negotiating Ethernet devices are first connected, a set of "link code words" are transmitted by each device, advertising its own speed and duplex capabilities to the other device.

Assuming each device successfully receives and understands the link code words of its peer, the two devices will auto-configure themselves for the best duplex mode possible (e.g. full is preferred instead of half), and the highest speed possible (e.g. 10/100), that is supported by both. Full duplex via auto negotiation is the preferred mode of operation for all VOIP Ethernet devices and should be used wherever possible.

**NOTE:** If either the switch or station device should fail to receive or understand the link code words from its peer, (a rare occurrence, but one that does occur) that device will default to operating in half-duplex mode. However, if the peer should successfully receive and understand the local devices link code words and the local device has advertised full-duplex capability, the peer will configure itself to full-duplex, thus resulting in a duplex mismatch situation. This condition always results in interface errors and dropped packets!

**Forced Duplex Configuration**

Some auto-negotiating interfaces that should be running full-duplex actually fail to auto negotiate to full-duplex at both ends. The interface must be force-configured or manually configured to operate in full-duplex at both ends to work correctly.
Note: Forcing a device to operate at a particular speed or duplex mode disables transmission of the auto-negotiation code words by that device when initially connected to another device. This prevents the other device from ever being able to auto-negotiate to full-duplex. Therefore, if either device is forced to operate in full-duplex, the other device must also be forced to operate in full-duplex as well.

Half Duplex Configuration
Some low-end IP-phone and small-port IAD devices (1 or 2 analog ports) may not support full-duplex operation and can only operate in half-duplex mode. These are the only devices that should be allowed to operate half-duplex.

Summary of Valid Duplex Configurations
The following table summarizes all of the different possible duplex configuration modes between connected Ethernet devices, and their validity as applicable to VOIP applications.

<table>
<thead>
<tr>
<th>Device 1</th>
<th>Device 2</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-full</td>
<td>Auto-full</td>
<td>Preferred for all devices</td>
</tr>
<tr>
<td>Auto-full</td>
<td>Auto-half</td>
<td>Invalid—duplex mismatch produces errors—Force both ends to full-duplex; or if both ends don’t support force-full, try a different model of Ethernet switch.</td>
</tr>
<tr>
<td>Forced-full</td>
<td>Auto</td>
<td>Invalid—No code words sent by forced end, auto-end defaults to half-duplex. Mismatch produces errors.</td>
</tr>
<tr>
<td>Forced-full</td>
<td>Forced-full</td>
<td>Used as alternative when auto-auto fails to produce full-duplex.</td>
</tr>
<tr>
<td>Auto-half</td>
<td>Auto-half</td>
<td>Can be used to connect a single IP phone or low-port IAD device to a switch. Should never be used at RTP aggregation points.</td>
</tr>
</tbody>
</table>

What are known issues on a data network?

Ethernet Switch Requirements
Ethernet (repeater) hubs are strictly half-duplex devices and should therefore never be used to connect any ShoreTel devices. ShoreTel approved and managed auto-negotiating full-duplex Ethernet switches should always be used.

Ethernet switches are available in two basic forms, managed and non-managed switches. Manageable switches cost more than non-manageable ones but provide several useful features such as manual port duplex configuration and statistics reporting as well as an administrator CLI or GUI. Non-manageable switches can only perform auto-negotiation, provide no statistics or CLI/GUI.

Although non-manageable switches can possibly be used in some cases, they are NEVER recommended and void the ShoreTel managed SLA, because they don’t provide any error statistics, which are extremely valuable when troubleshooting QOS related problems.
Managed Ethernet switches should have the following features:

- Perform auto speed and duplex negotiation by default, with option to force-configure individual port speed and duplex modes when necessary.
- For those switches that support the spanning tree protocol (STP) or rapid spanning tree protocol (RSTP) should also support either disablement of spanning tree blocking or fast-enable (Cisco port-fast feature) at the individual port level.
- Provide individual-port speed and duplex mode indication, plus error & traffic statistics, which are useful in troubleshooting.

### Customer Data Network Equipment Requirements

<table>
<thead>
<tr>
<th># of Employees</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5</td>
<td>Internet: Business DSL&lt;br&gt;Router: Provided by ISP&lt;br&gt;Firewall/NAT: Approved SOHO Device&lt;br&gt;Switch: Any (no hubs)</td>
</tr>
<tr>
<td>1-20</td>
<td>Internet: Business DSL 768k&lt;br&gt;Router: Provided by ISP&lt;br&gt;Firewall/NAT: Approved SOHO Device&lt;br&gt;Switch: Any (no hubs)</td>
</tr>
<tr>
<td>1-44</td>
<td>Internet: 1 or 2 x T1 Internet&lt;br&gt;Router: Provided by ISP&lt;br&gt;Firewall/NAT: Approved SOHO Device&lt;br&gt;Switch: Switches capable of Dot1Q trunking</td>
</tr>
<tr>
<td>1-100</td>
<td>Internet: 2 x T1 Internet&lt;br&gt;Router: Provided by ISP&lt;br&gt;Firewall/NAT: Approved SOHO Device&lt;br&gt;Switch: Switches capable of Dot1Q trunking</td>
</tr>
</tbody>
</table>

- Support a minimum of 2 VLANs on all switches (1 for voice, 1 for data) and trunk to the router via dot1q.
- Managed, Layer-2 Data Switches. ShoreTel does not recommend connecting any non-managed switches or hubs to the network. In the event that a non-managed switch must be connected, only the data VLAN should be configured on the port with proper duplex settings to avoid collisions on the network.
- SNMP strings for remote monitoring capabilities.
• LLDP-MED support (ShoreTel 400 series IP Phones).
• Power over Ethernet i.e. POE to power IP Phones from the data switches.
• Enable read-only or full telnet access to all switches and routers from ShoreTel NOC.

What about disaster recovery?
Every enterprise, whether large or small, places a heavy reliance on their communication infrastructure to conduct and grow their business. It is imperative that your Unified Communication (UC) system provide extremely high levels of reliability, survivability and functionality, even when faced with outages, faults and unforeseen disasters.

The cloud based architecture of the ShoreTel Sky solution is uniquely tailored to exceed these expectations and is built with reliability, resiliency, survivability and fault tolerance in mind. Like any advanced system, proper planning, deployment strategies and best practice configurations are necessary keys to installing and maintaining a fully survivable and highly-available ShoreTel Sky UC system.

NOTE: that your backup connection may NOT be on a private network. The speed of the network may be slower and voice calls could be affected compared to the primary network connectivity.

Without redundancy, if you lose power to the Shoretel provided router, all incoming calls will go to voicemail or any other predetermined find-me-follow-me settings. You will NOT lose any incoming calls since it is a hosted service.

Take into account the following redundancy considerations when considering how best to mitigate issues in your data network converged with ShoreTel Sky:

Redundant Services – Which services need High Availability?
• Voice
• Internal Data (i.e. site to site)
• Internet

Redundant Links – Which connectivity options are possible based on their HA services?
• ShoreTel provided backup MPLS circuit (e.g. into a CUG) - Will support current voice, data and backhauled Internet.
• GRE VPN Tunnel - Will support voice but not data or backhauled Internet.
• NAT (i.e. Network Address Translation) over local Internet (i.e. assumes a local Internet connection) - Will support voice and Internet but not internal site to site data.

Redundant Hardware – What hardware is needed for more redundancy and security based on above selections?
• Backup ShoreTel provided router for backup MPLS circuit into carrier CUG.
• Local Internet connection(s) per site.
• Local firewall with a Layer-3 switch per site.
Once the customer decides on the necessary redundancy requirements, a ShoreTel data network engineer will help design the specific network topology per the HA requirements. Redundant configurations and designs are additional cost from the typical deployment and will be quoted per the customer requirements and environment designed.

**Configuring VLANs for ShoreTel IP Phones**

IP phones are a specialized device on the data network and have capabilities and requirements which need to be considered when designing the data network. For example, to help better utilize port capacity on data switches, a PC is allowed to piggy-back on an IP phone and share a single data switch port, utilizing VLAN trunking or tagging the Voice and Data VLANs for each device respectively.

ShoreTel IP phones have an internal 2-port switch on the back of the IP phone to connect it to the data network through the network port as well as a PC through the access port. ShoreTel IP Phones prioritize voice so the connected PC is unable to disrupt outbound voice quality.

Most data network equipment manufacturers have a voice VLAN feature either at the data switch access port or VLAN level that supports various VoIP capabilities (i.e. to mitigate deteriorating IP phone sound quality of a call if the data is unevenly sent due to lack of layer-2 output switch interface buffer prioritization). The Voice VLAN feature helps QoS use classification and scheduling to send network traffic from the switch in a predictable manner for IP phones. By default, the voice VLAN feature is disabled but when the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port and all 802.1P or 802.1Q tagged VLAN traffic’s CoS is trusted.

For further discussion how an IP phone is automatically assigned to the Voice VLAN when the Voice and Data VLANs are both assigned to the data switch port, refer to the sections below, *Automatic IP Phone VLAN Assignment - DHCP and Automatic IP Phone VLAN Assignment - LLDP-MED*.

The phone connected PC or laptop only has access to the local data network for normal Internet access so Voice and Data are still on separate virtual networks. While piggy-packed to the phone, the PC or laptop can start its own VPN client to connect separately to the corporate data network without any conflict or issue with the phone.
Figure 3 above demonstrates the physical connection of a PC connected to a ShoreTel IP phone in turn connected to the network connection on a single data switch access port.

Figure 4 below demonstrates a Cisco example of how to configure the voice VLAN feature on the data switch access port to support both Voice and Data VLANs for each ShoreTel IP phone. Figure 4 also shows the access port configuration when the Voice VLAN is the only VLAN (i.e. untagged VLAN) applied to the port for each dedicated ShoreTel IP phone.
The different port configuration examples above include the following two commands on each Fast Ethernet port when ShoreTel devices are present:

```
spanning-tree portfast
no cdp enable
```

Although these statements are not required, it is recommended that CDP (Cisco Discovery Protocol) be disabled on Ethernet ports not connected to Cisco devices to reduce unnecessary traffic. In addition, Spanning Tree should be set to either “portfast” or “rapid spanning tree” mode for Cisco switches or “edge” for Juniper switches. This will allow faster boot times and fewer network issues when connecting to ShoreTel phones.

In summary, ShoreTel leverages the use of VLANs to integrate into the network topology that you, the network administrator, have decided is most appropriate for your LAN topology. ShoreTel does not require nor dictate that you use a specific vendor’s equipment for your LAN edge, core, WAN, switches, routers, operating systems, etc. as long as your data hardware supports the minimum recommended requirements presented in this document.

**Automatic IP Phone VLAN Assignment – LLDP-MED**

LLDP (IEEE 802.1AB) is a vendor agnostic Layer 2 protocol designed to be used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 Ethernet LAN. LLDP performs similar functions as several proprietary protocols such as the Cisco Discovery Protocol (CDP), Extreme Discovery Protocol, Nortel Discovery Protocol and Microsoft’s Link Layer Topology Discovery. An enhancement to LLDP is LLDP-MED, Link Layer Discovery Protocol-Media Endpoint Discovery. LLDP eliminates the phone from using the untagged Data VLAN and allows only one DHCP request directly on the Voice VLAN.
The Automatic VLAN Assignment using LLDP-MED during the ShoreTel IP Phone standard boot process is as follows:

1. As the Phone powers up, the Ethernet switch sends LLDP Data Units defined as LLDP_Multicast packets to the Phone.

2. The Phone responds in kind adding TIA Organizationally Specific LLDP-MED TLV’s such as “TIA – Network Policy” with “VLAN Id: 0” among many other TLV extensions. “VLAN Id: 0” is the request from the phone asking the Ethernet switch for the Voice VLAN ID as well as L2 Priority, DSCP value, and etc.

3. The Ethernet switch in turn responds to the phone with the same TIA LLDP-MED TLV extensions and in the “TIA – Network Policy” TLV, the designated VLAN Id of the Voice VLAN is offered to the phone (e.g. VLAN Id: 50. See Figure 5 below).

4. The Phone performs a typical DHCP sequence of Discover, Offer, Request, Ack to get an IP address plus available DHCP Options from the Voice VLAN.

5. The Phone via FTP downloads its configuration file, upgrades the Boot Image if needed as well as other required files and finally reboots.

6. The Phone registers successfully and is ready for service.

LLDP is enabled by default on all supported ShoreTel IP phones starting with build version “SEV.3.3.0”. All Ethernet switches in the data network intended to support IP phones should be configured for LLDP if not enabled by default with the appropriate TLVs enabled and configured per the Ethernet switch manufacturer’s documentation and with the appropriate LLDP supported Ethernet switch firmware releases.

ShoreTel 400-series IP Phones

LLDP-MED can also send a default DSCP value assignment to the IP phone for application type voice. To better understand the IP phone’s inheritance behavior, in general, the last setting assigned wins unless some other logic prevails.

**LLDP OFF:** ShoreTel DSCP used for RTP and Signaling

**LLDP-MED TLV ON with a default of 0:** ShoreTel DSCP used for RTP and Signaling

**LLDP-MED TLV ON with a non-zero value:** LLDP Value used for RTP. ShoreTel DSCP used for Signaling
**Off-Net Firewall Best Practices**

A firewall is an information technology (IT) security device which is configured to permit, deny or proxy data connections set and configured by the organization’s security policy. Firewalls can either be hardware and/or software based. ShoreTel does not support customer firewalls, nor do we make recommendations on what firewalls to use other than what capabilities are required.

*Firewalls can be combination devices, and can include the following features:*

- Stateful Inspection
- NAT
- DHCP server
- AV Antivirus Enforcement
- Spam filter
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)

**Troubleshooting**

A public IP address is generally not assigned directly to a user’s computer. Computers are generally located on a private network behind a router or firewall providing network address translation (i.e. NAT) or a dedicated NAT device. In these cases, the firewall configuration needs to be considered for ShoreTel Sky services and features.

**Remote Phone**

For ShoreTel Sky phones to work over a broadband internet connection, firewalls must be configured to allow outbound traffic from the following ports:

**General to Call Manager/VSBC/Pat Server IP**

- 2000 TCP and UDP (SCCP - Cisco 79XX series phones)
- 69 TCP/UDP (TFTP)
- 5060 TCP (SIP)
- 10000 thru 14500 & 16384 thru 32767 UDP (RTP streaming ports)
- 80 TCP (http services)

**General to portal.shoretelsky.com**

- 80 http access to webportal redirect
- 443 SSL access to webportal redirect
Call Manager specific

- 80 HTTP access to webportal
- 443 SSL access to webportal
- 2001 CM HTTP Services
- 12000 (PAT SCCP Cisco 79XX phones)
- 12001 (PAT HTTP services)
- 15061 TCP (SIP Phones - Off ShoreTel's Network)
- proxy.m5net.com:8081 TCP
- proxy.m5net.com:8082 TCP
- proxy.m5net.com:8085 TCP
- proxy.m5net.com:8086 TCP

Console Assistant

- console.m5net.com:4XXX
- 32769 Console assistant port.
- admin.m5net.com:80 (services button)
- 80 HTTP access to webportal

ShoreTel Sky Call Conductor SIP Phones: General Firewall Configuration

Symptoms such as failed registration, inability to receive and/or make calls, inability to receive and/or send audio (i.e. "one-way talk paths") or calls failing to ring inbound after the connection is idle for some time might all be attributed to firewall or NAT issues.

- The following ports must not be blocked by the firewall or ISP:
  - TCP port 15061
  - UDP ports 27000 through 29047

  NOTE: ShoreTel uses non-standard SIP signaling and RTP ports.

Stateful firewall/NAT configuration - connection-timeout-adjusting method

This method can be used by single users, but it must be used on LANs where multiple SIP devices are traversing the same NAT.

- Stateful firewalls recognize inbound traffic that is part of an established connection and send it to the correct IP and ports on the client. With such a configuration, the NAT/firewall device handles port mapping, as long as the connection does not time out.

- ShoreTel requires that SIP softphones re-register (i.e., let the server know they are still available and connected) at least every 3600 seconds (6 minutes), so configuring the firewall/NAT device with TCP timeouts greater than 6 minutes will maintain the connection.
• Note that ShoreTel uses this relatively long registration interval because the client SIP softphone is temporarily unavailable during the re-register process. Many NAT devices by default forget port mappings after 30 seconds, so this is an important area to troubleshoot.

• Stateless firewall/NAT configuration - port forwarding method

• This method works for single users on SOHO networks, as it eliminates the need to adjust the port timeout settings for their NAT/firewall device.

• It is required for users using less common stateless firewalls (firewalls that do not automatically map inbound ports based on outbound connections).

• In these cases, one can configure the NAT device (e.g., home router) to forward connections from the SIP signaling port (TCP port 15061) and real-time (RTP) audio port range (UDP ports 27000 - 29047) to the computer on the user's local area network.

Troubleshooting Connectivity

The eyeBeam application can be configured to generate a diagnostic log of varying detail. This can be used in combination with packet sniffing to isolate a problem. GUI software such as Ethereal/Wireshark or CLI programs such as tcpdump on Unix or Unix-like OS's (e.g. Mac OS X) can be helpful. EyeBeam does not provide a meaningful error, though errors identified with a packet dump are likely caused by the client computer typically.

In Summary:

• A lack of sent packets in a packet dump indicates a local computer problem outside of ShoreTel's control, for example, in the TCP stack.

• A lack of RECEIVED SIP messages in the X-Lite diagnostic log from "Catch 9 Communications" indicates a problem connecting to ShoreTel that may be caused by local computer, NAT, or Internet routing problems outside of ShoreTel's control.

• Other symptoms can be diagnosed in the eyeBeam client display or diagnostic log based on the type of RECEIVED SIP messages from "Catch 9 Communications."

• A "service unavailable" message on the client, accompanied by errors in the diagnostic log without any packets sent or received by the client indicate a problem with the client PC's network configuration or a bug in the SIP softphone client, e.g., a WINSOCK error. ShoreTel may not be able to resolve this issue; the client may have to reinstall the networking components of his or her operating system or perform a full re-installation.

• A login timeout when placing an outbound call, accompanied by repeated SENT SIP messages without any RECEIVED SIP messages in the diagnostic log and packets sent to (e.g. 66.11.207.75, pat1.212803.m5net.net) via UDP or TCP with a response from e.g. pat1212803.m5net.net, indicating that the port is "unavailable for IP" suggests a misconfigured SIP softphone (e.g., one that is trying to register or communicate on the wrong port). Note that ShoreTel does not use registered SIP ports.

• A busy signal when attempting to place an outgoing call accompanied by a RECEIVED SIP message in the diagnostic log stating "Proxy Authentication Required" indicates that the softphone is misconfigured and is not set to register. Incoming calls will fail to ring in this scenario. Set the softphone to register.
An "unauthorized" message on the client accompanied by a RECEIVED SIP message in the diagnostic log stating "Unauthorized" when attempting to register indicates that the password or authorization name is incorrect. Incoming calls will fail to ring in this scenario.

SCCP Phones: Cisco Pix Firewall
When running a SCCP phone behind a Cisco PIX Firewall or routers configured for NAT can cause SCCP (Skinny) IP phones to freeze or not work.

SCCP phone behind a Cisco PIX Firewall
By default, a PIX firewall inspects the content of TCP-SCCP packets and will discard any packet it doesn't understand. If a SCCP message becomes segmented into two separate TCP packets, the 2nd packet won't be understood by the PIX and will be discarded. Subsequent re-transmissions of the packet are likewise discarded, causing the phone to freeze. It must then be power-cycled to recover.

The solution is to add the following line to the PIX configuration and then reset all SCCP phones to make them open a new SCCP session.

no fixup protocol skinny 2000

SCCP phone behind a router configured for NAT
A Cisco router at a customer site configured for NAT will detect TCP-SCCP messages and translate the network address information inside the SCCP messages. Although this process is necessary for operation with Cisco Call Manager, it interferes with translations performed by ShoreTel's Call Manager and can also cause the phone to 'freeze'.

The solution is to add the following line to the NAT router configuration and then reset all SCCP phones to make them open a new SCCP session.

no ip nat service skinny tcp port 2000
Cisco SB switch settings – Auto Smartport & EEE
When using ShoreTel 400-series IP Phones with Cisco Small Business switches (i.e. SG series), 2 port management features, Administrative Auto Smartport and Energy Efficient Ethernet (i.e. EEE), need to be disabled. This will ensure that the phone service will not be inadvertently interrupted due to the features’ behavior. Issues with these features enabled typically experience IP Phone service recycling at a regular interval such as every 15 minutes or so.

To disable the features, follow the appropriate marked fields shown below.
References
IEEE 802.1Q Tagging:
http://www.ieee802.org/1/pages/802.1Q.html
http://ieeexplore.ieee.org/xpl/standardstoc.jsp?isnumber=27089&isYear=2003
Cisco Configuration Guides and References:
Troubleshooting Output Drops with Priority Queueing
Document and Software Copyrights
Copyright © 2013 by ShoreTel, Inc., Sunnyvale, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of ShoreTel Communications, Inc.

ShoreTel, Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to typographical, arithmetic or listing errors.

Trademarks
The ShoreTel logo, ShoreTel, ShoreCare, ShoreGear, ShoreWare and ControlPoint are registered trademarks of ShoreTel, Inc. in the United States and/or other countries. ShorePhone is a trademark of ShoreTel, Inc. in the United States and/or other countries. All other copyrights and trademarks herein are the property of their respective owners.

Disclaimer
ShoreTel tests and validates the interoperability of the Member's solution with ShoreTel's published software interfaces. ShoreTel does not test, nor vouch for the Member's development and/or quality assurance process, nor the overall feature functionality of the Member's solution(s). ShoreTel does not test the Member's solution under load or assess the scalability of the Member's solution. It is the responsibility of the Member to ensure their solution is current with ShoreTel's published interfaces.

The ShoreTel Technical Support organization will provide Customers with support of ShoreTel's published software interfaces. This does not imply any support for the Member's solution directly. Customers or reseller partners will need to work directly with the Member to obtain support for their solution.

Company Information
ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085 USA
+1.408.331.3300
+1.408.331.3333 fax

Author
CHAD HORTON
Manager, Innovation and Network Services
chorton@ShoreTel.com
+1 (512) 551-7185 Tel/Fax/Cell