

		Innovation Network App Note TPP: 10347 Date: September, 2011
Product: ShoreTel EtherSpeak with Adtran		System version: ShoreTel 11.x

Abstract

In 2008, EtherSpeak certified the SureTrunk™ for ShoreTel connection method to enable an innovative “native” SIP connectivity option for ShoreTel. SIP Trunking provides the users of ShoreTel a value-aligned alternative method for public telephone network by-pass. These connection options are enabled when a ShoreTel customer elects to use a SIP trunking provider like EtherSpeak (using the Session Initiation Protocol (SIP)) for communications beyond the customer’s IP network edge.

In the current version of EtherSpeak’s SureTrunk™ for ShoreTel offering, EtherSpeak now provides the ShoreTel administrator numerous options for connectivity of the SureTrunk™ for ShoreTel service – to virtually any version of the ShoreTel system (this application note covers only ShoreTel versions 9.x through versions 11.x).

In addition, EtherSpeak now provides options for enhancing security and quality of SIP by providing new Quality of Service (QoS) / Class of Service (COS) guarantees by broadening the EtherSpeak solution to include MPLS cross-connections to most Tier-One carrier data networks. This evolution is an improvement to how the service may be delivered, and as a result, provides the ShoreTel Administrator options for leveraging EtherSpeak SIP with seamless inter-connects to carrier networks in an unprecedented way. New carrier supported MPLS cross-connects are available currently with AT&T / ACC Business, Level 3 Communications, Qwest Communications, Windstream, Verizon Business and others. Please speak with EtherSpeak sales to verify the availability of connecting to your carrier’s network.

They include a wide array of private wide-area-network (WAN) options (MPLS T1’s), metro-Ethernet connectivity, Asynchronous Transfer Mode (ATM) and whole range of quality public network broadband and most recently, Wireless Wide Area Network (WWAN) options (including WAN (802.11n or WiMax). In two short years, EtherSpeak SIP is steadily moving to become the de-facto standard for connecting customer-premise based IP PBXs to carrier networks. With these options taking shape, it is an exciting time for ShoreTel and SIP. Although SIP connectivity is a “newer” ShoreTel connection method, it is typically regarded as less expensive, increasingly reliable, and the key driver for reducing customer monthly recurring costs when compared to “legacy” Public Switched Telephone Network (PSTN) connections. SIP is replacing Plain-Old-Telephone-Service (POTS), Basic Rate Interface (BRI), Primary Rate Interface (PRI) or T1 / E1 trunk connections. This application note provides a guide for you in selecting and implementing an EtherSpeak SureTrunk™ SIP connectivity option that is right for your customer. We will help you do this by providing an understanding of the three ShoreTel Certified methods to connect a ShoreGear system to EtherSpeak as a Communications-as-a-Service (CaaS) provider.

1. Connecting natively to EtherSpeak over an single existing Internet connection
2. Connecting natively to EtherSpeak over a redundant Internet connection
3. Connecting natively to EtherSpeak over a private network connection

This application note is for ShoreTel customers who would like encrypted (utilizing an IPSEC VPN) SIP trunking via a PRI handoff from the ShoreTel system.

Application Diagrams of the product scenarios tested with the ShoreTel ShoreGear switch appear in Figure A below.

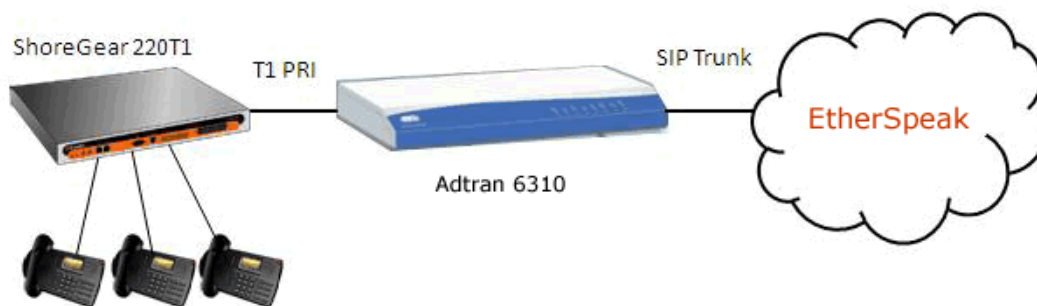


Figure A: ShoreTel's ShoreGear, Adtran's NetVanta 6310 connected with EtherSpeak

Table of Contents

Overview.....	3	Architecture Overview.....	6
Features and Benefits.....	3	Version Support.....	7
Requirements, Certification and Limitations	4	Certification Testing Results Summary	7
Problem Statement	4	Configuration Overview.....	11
Solution.....	4	ShoreTel Configuration	11
EtherSpeak Overview and Contact.....	5	Adtran Configuration.....	14
ADTRAN Product Information Product Description ...	6	Adtran Troubleshooting	39
		Document and Software Copyrights	40
		Trademarks.....	40
		Disclaimer	40
		Company Information.....	40

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.

Overview

This document provides details for connecting the ShoreTel system through the ADTRAN NetVanta® series of routing, switching and IP gateway products to EtherSpeak, for SIP Trunking, to enable audio communications. The connection to the ShoreTel system will be a T1 PRI from the NetVanta 6310 product. The document focuses on the configuration procedures needed to set up these systems to interoperate.

Features and Benefits

The EtherSpeak, ADTRAN and ShoreTel solution provides the following features and benefits:

- Inbound Calling (requires EtherSpeak extension), 800 Inbound (requires purchase or port), Long Distance Termination (includes intra-, inter-state and international), Expanded Local Calling, Outbound calling to 888, 877, 800 numbers, e911, 411 and Operator Services, Inbound Caller ID and Location, White Page Listing, Toll-Free, Domestic and International Long Distance, G.711 and G.729a Codecs.
- Benefits - Smart Reasons to Switch to SIP Trunks to Secure Your Clients and to Save Money
 - Cost Savings - Enjoy the cost savings of combining your local, long distance and broadband Internet services onto a single circuit with dynamic bandwidth allocation.
 - Save Time - Dedicated and knowledgeable EtherSpeak technicians, installation teams and customer support specialists assure rapid deployment.
 - Simplify - Experience the efficiency of managing a single network connection, receiving one bill and engaging one point of contact for all your local, long distance, and broadband Internet needs.
 - Protect your Investment - Preserve your existing capabilities via seamless integration with the ShoreTel IP PBX system while utilizing industry proven encryption technologies to assure the privacy of customer information.
 - Grow Your Business - When you grow, adding more SIP Trunks is easy, and happens within hours - not days, weeks, or months. Etherspeak SIP Trunks can be installed in about an hour and turned up remotely so you do not have to slow down.
- Affordable converged IP voice and data solution for small and medium enterprises or branch office VoIP networks
 - Lower Total Cost of Ownership and rapid return on investment
 - NetVanta's 6000 series routing series is ideal for IP Telephony, corporate connectivity and Internet access convergence
 - Enhanced routing performance, integrated firewall, VPN and robust QoS functionality
 - Ease of use features for monitoring and scoring voice quality, trending and tracking



- Web-based configuration Graphical User Interface (GUI), monitoring and remote management
- Industry-leading warranty and customer support and services
- The widest variety of standards-based , ShoreTel interoperable business networking infrastructure
- Provide ShoreTel PBX with a PRI interface, thus eliminating the feature limitations that ShoreTel has with SIP trunking

Requirements, Certification and Limitations

Problem Statement

- If ShoreTel customers wish to connect to inbound or outbound SIP trunks, a dedicated hardware device is required to establish connectivity to any ITSP.

Solution

- By leveraging advanced knowledge of Internet security protocols and voice over IP (VoIP), EtherSpeak is providing a full range of managed SIP trunking services *with* or *without* dedicated hardware prerequisites, enabling ShoreTel customers to have greater flexibility and scale SIP trunking services according to growth needs. EtherSpeak supports native connectivity options, customer provided Session Border Controller as Customer Premise Equipment, or connection as a SIP to PRI hand-off via a PRI Internet Access Device (IAD).
- Natively using EtherSpeak SureTrunk™ Service:
 - Pro: Unlimited call capacity, no capital expense with a 30 minute customer quick turn-up process.
 - Cons: Requires ShoreTel SIP Trunk License; SIP Call recording not supported on ShoreTel; No ringback generated by ShoreTel phones after call is connected through Automated Attendant.
- Utilizing a PRI to SIP hand-off:
 - Pro: No ShoreTel SIP license; ShoreTel Director thinks it is using a PRI; Fully encrypted for connections over the public Internet; All ShoreTel features supported.
 - Cons: Customer capital expenditures are significant and limited to 23 channels (PRI / T1 switch & SIP / PRI IAD); Limited to capacity of 23 concurrent calls per non-recurring equipment charge necessary for PRI hand-off; Trunks are tied to expensive hardware with limited capacity.
- Utilizing a customer-premise-based Session Border Controller
 - Pros: Provides ability to use any SIP carrier approved by ShoreTel; Normalizes SIP to carrier requirements / standards.
 - Cons: In addition to a SIP license fee, SBC requires a license fee for concurrent calls; Not all features are supported including call recording, External Assignment; Park and Pickup; Limited support for SIP Info; May become possible single point of failure on customer network.



A VPN is required for connection of the original SureTrunk™ Native service option and the new SureTrunk™ PRI service options. Either of EtherSpeak's solutions require a VPN tunnel with access from the customer's ShoreTel switch (where trunks are configured) to a virtual IP assigned by EtherSpeak to that customer's ShoreTel SIP switch (or PRI switch). Therefore, the customer firewall device should support industry standard IPSec encryption with availability of one-tunnel VPN license. Please consult your firewall vendor to determine if your product supports industry standard IPSec and you are licensed to establish a single IPSec tunnel to enable either the Native or PRI connection options now available for utilizing the EtherSpeak SureTrunk™ service.

EtherSpeak Overview and Contact

EtherSpeak is a complete nationwide communications provider offering businesses advanced Internet, IP based voice and network service solutions. As a single source provider for business telecom needs, EtherSpeak provides its customers with unparalleled selection, savings and service. The company's unique methodology, experienced team and dedicated customer service ensures accountability and service superior to that of traditional Internet and VoIP providers.

Sales Inquiries

(866) 384-3747

sales@ietherspeak.com

Channel Inquiries

(866) 384-3747

sales@ietherspeak.com

Support Inquiries

(866) 384-3747

support@ietherspeak.com

ADTRAN offers a robust suite of IP business solutions for converged IP networking. This suite includes a variety of business trunking, hosted VoIP and premises-based VoIP solutions including IP business gateways, multiservice access routers, managed Layer 2/3, PoE and Gigabit Ethernet switches, 802.11 a/b/g Wireless Access Points and modular access routers. These products are ideal for bundled services or business networks. They address the need for branch office connectivity, Internet access, VoIP migration, bandwidth expansion, network security and voice quality monitoring.

For general sales questions regarding ADTRAN products and solutions, contact your reseller or contact ADTRAN directly at:

ADTRAN Applications Engineering

1-800-615-1176

support@adtran.com

www.adtran.com

To become an ADTRAN reseller, visit www.adtran.com/partner to find out how to join ADTRAN's award-winning partner program, or dial 1-800-9ADTRAN and asked to speak to a Customer Service Representative about the ADTRAN Advantage partner program.

For configuring joint solutions, select from the following ShoreTel-interoperable ADTRAN platforms. NetVanta 6310 part number: 1700100G1



ADTRAN Product Information Product Description

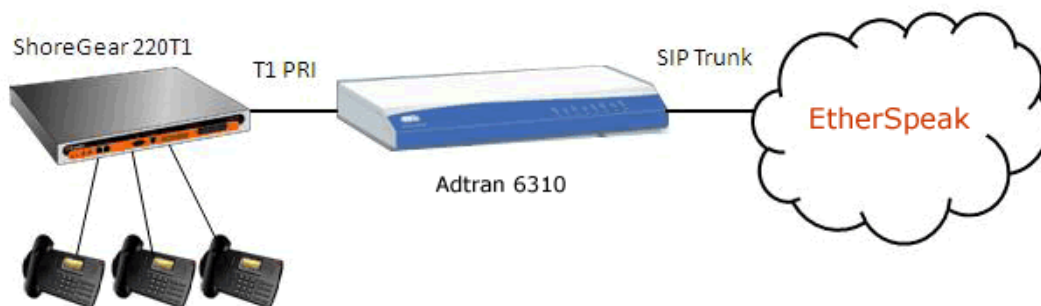
The NetVanta 6310 Modular IP Business Gateway is designed for use in integrated IP voice and data service offering to small-to-medium sized businesses, worldwide. This powerful solution combines the robust routing and voice features of ADTRAN's industry-leading NetVanta 900e Series of IP Business Gateways into a modular, multi-function chassis.

- Converged service solutions
- Combines IP Business Gateway and Ethernet access device into one chassis
- Module dual-slot chassis
- Integral SIP gateway, router, and security
- Supports a variety of network and voice interfaces
- Dual 10/100Base-T interfaces for routing, DMZ, or Ethernet-fed WAN
- Integral PRI/PRA T1/E1 for PBX connectivity
- Stateful inspection firewall for network security
- IPsec Virtual Private Network (VPN) for secure corporate connectivity across the Internet
- Compatible with industry-leading softswitches and call agents
- Up to 16 analog POTS interfaces with remote survivability
- Supports IP, analog, and digital phones/phone systems; fax machines, modems, and Wireless Access Points (WAPs)
- Dynamic bandwidth allocation enables more efficient utilization
- Standardized G.729a voice compression requires less bandwidth per voice call
- Voice Quality Monitoring (VQM) and Mean Opinion Score (MOS) prediction
- CompactFlash slot for IP phone configuration files and firmware
- Recognizable CLI eliminates retraining
- User-friendly Web-based GUI
- Feature-rich ADTRAN Operating System (AOS)
- Industry-leading warranty
- ETSI compliant

Architecture Overview

Platforms used during application testing:

- NetVanta 6310
- ShoreGear 220T1
- ShoreTel IP Phones



Version Support

The ADTRAN Products detailed in this application note are certified with the following versions of the ShoreTel system, listed below.

		Adtran NetVanta 6310
		NV6300A-A4-08-00-E.biz
ShoreTel Release	9.x	✓
	10.x	✓
	11.x	✓

Certification Testing Results Summary

Platforms Used During Testing:

- NetVanta 6310
- ShoreGear 220T1
- ShoreTel IP Phones

Features Used During Testing:

- Ethernet Interface
- SIP
- PRI Handoff

The ShoreTel system has some known limitations with SIP trunking, please refer to ShoreTel's Administration Guide, chapter 18, for the SIP trunking limitations.

1.0 Initialization and Basic Calls

ID	Name	Description	Results
1.1	Setup and initialization	Verify successful setup and initialization of the NetVanta System	Pass
1.2	Outbound Call (Domestic)	Verify calls placed outbound through NetVanta reach the external destination.	Pass
1.3	Inbound Call (Domestic)	Verify calls received by NetVanta are routed to the proper trunk group.	Pass
1.4	Device restart – Power Loss	Verify that the NetVanta system recovers after power loss.	Pass
1.5	Device restart – Network Loss	Verify that the NetVanta system recovers after loss of network link.	Pass
1.6	All Trunks Busy – Inbound Callers	Verify inbound callers hear busy tone when all channels / trunks are in use.	Conditional Pass (see Note 1)
1.7	All Trunks Busy – Outbound Callers	Verify outbound callers hear reorder tone when all channels / trunks are in use.	Pass



1.8	Incomplete Inbound Calls	Verify proper call progress tones are provided and proper call teardown for incomplete inbound calls.	Pass
-----	--------------------------	---	------

Note 1: The NetVanta system sends a 503 (Service Unavailable) message to EtherSpeak, resulting in system message: “The number you have dialed is not in service”.

2.0 Media and DTMF Support

ID	Name	Description	Results
2.1	Media Support – ShoreTel Phone to NetVanta	Verify call connection and audio path from a ShoreTel phone to an external destination through the NetVanta system using all supported tones with both sides set to a common codec.	Pass
2.2	Media Support – SIP Reference to NetVanta	Verify call connection and audio path from a SIP reference phone to an external destination through the NetVanta system using all supported tones with both sides set to a common codec.	Pass
2.3	Codec Negotiation	Verify codec negotiation between NetVanta and EtherSpeak with each side configured for a different codec.	Pass
2.4	DTMF Transmission	Verify DTMF transmission per RFC2833 for calls placed through the NetVanta System.	Pass
2.5	Auto Attendant Menu	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the desired extension.	Pass
2.6	Auto Attendant “Dial by Name”	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the desired extension using the “Dial by Name” feature.	Pass
2.7	Auto Attendant menu checking Voice Mail mailbox	Verify that inbound calls are properly terminated on the ShoreTel Auto Attendant menu and that you can transfer to the Voice Mail Login Extension.	Pass

3.0 Performance and Quality of Service

ID	Name	Description	Results
3.1	Voice Quality Service Levels	Verify the NetVanta System can provide a voice quality SLA across the WAN from the customer premises.	Pass
3.2	Capacity Test	Verify the service provider interface can sustain	Pass



		services through period of heavy outbound and inbound load.	
3.3	Post Dial Delay	Verify that post dial delay is within acceptable limits.	Pass

4.0 Enhanced Services and Features

ID	Name	Description	Results
4.1	Caller ID Name and Number – Inbound	Verify that Caller ID name and number is received properly.	Pass
4.2	Caller ID Name and Number – Outbound	Verify that Caller ID name and number is sent properly.	Pass
4.3	Hold	Verify successful hold and resume of a connected call.	Pass
4.4	Call Forward	Verify outbound calls that are being forwarded are redirected and connected to the appropriate destination.	Pass
4.5	Call Transfer – Blind	Verify a call connected to the ShoreTel phone can be transferred to an alternate destination.	Pass
4.6	Call Transfer – Consultative	Verify a call connected to the ShoreTel phone can be transferred consultatively to an alternate destination.	Pass
4.7	Conference – ad hoc	Verify successful ad hoc conference of three parties.	Pass
4.8	Inbound DID / DNIS	Verify the NetVanta System provides inbound “dialed number information” and is correctly routed to the configured destination.	Pass
4.9	Outbound 911	Verify that outbound calls to 911 are routed to the correct PSAP for the calling location and that caller ID information is delivered.	Pass
4.10	Operator Assisted	Verify that 0+ calls are routed to an operator for calling assistance.	Pass
4.11	Inbound / Outbound call with Blocked Caller ID	Verify that calls with Blocked Caller ID route properly and the answering phone does not display any Caller ID information.	Pass
4.12	Inbound call to a Hunt Group	Verify that calls route to the proper Hunt Group and are answered by an available hunt group member with audio in both directions.	Pass
4.13	Inbound call to a Workgroup	Verify that calls route to the proper Workgroup and are answered successfully by an available workgroup agent with audio in both directions.	Pass
4.14	Inbound call to DNIS / DID and leave a voice mail message	Verify that inbound calls to a user, via DID / DNIS, routes to the proper user mailbox and a message can be left with proper audio.	Pass
4.15	Call Forward – “FindMe”	Verify that inbound calls are forwarded to a user’s “FindMe” destination.	Pass



4.16	Call Forward – Always	Verify that inbound calls are immediately forwarded to a user's external destination.	Pass
4.17	Inbound / Outbound Fax calls	Verify that inbound / outbound fax calls complete successfully.	Pass
4.18	ShoreTel Converged Conferencing Server	Verify that inbound calls are properly forwarded to the ShoreTel Converged Conferencing Server and it properly accepts the access code with audio to all involved parties.	Pass
4.19	Inbound call to Bridged Call Appearance (BCA) extension	Verify that inbound calls are properly presented to all of the phones that have BCA configured and that the call can be answered, placed on-hold and then transferred.	Pass
4.20	Inbound call to a Group Pickup extension	Verify that inbound calls to extensions that are part of a Group Pickup extension can be answered, placed on-hold and then transferred.	Pass

Configuration Overview

The steps included in the ADTRAN and ShoreTel Configuration sections below provide instructions on configuring a converged ADTRAN NetVanta router with a ShoreTel IP Telephony system. All ADTRAN products use a familiar command-line interface for configuration via console connection, Telnet, or a Web-based GUI is available for many features and configurations.

ShoreTel Configuration


In this implementation ShoreTel interoperates with the ADTRAN NetVanta platform via T1 PRI trunks. The connection between the two units will be via a T1 Crossover cable (if you are not familiar with what a T1 Crossover cable is, perform an Internet search for T1 crossover cable). The configuration details below are concise, for complete configuration details please refer to the ShoreTel Administration Guide.

Log into ShoreWare Director and create a new PRI Trunk Group:

Trunk Groups

Edit PRI Trunk Group

[New](#) [Copy](#) [Save](#) [Delete](#) [Reset](#) [Help](#)

Edit this record		Refresh this page
Name:	<input type="text" value="PRI"/>	
Site:	<input type="text" value="Sunnyvale TPP Lab"/>	
Language:	<input type="text" value="English(US)"/>	
Inbound:		
Number of Digits from CO:	<input type="text" value="10"/>	
<input checked="" type="checkbox"/> DNIS	Edit DNIS Map	
<input checked="" type="checkbox"/> DID	Edit DID Range	
<input type="checkbox"/> Extension		
<input checked="" type="radio"/> Translation Table:	<input type="text" value="<None>"/>	
<input type="radio"/> Prepend Dial In Prefix:	<input type="text"/>	
<input type="radio"/> Use Site Extension Prefix		
<input type="checkbox"/> Tandem Trunking		
User Group:	<input type="text" value="Anonymous Telephones"/>	
Prepend Dial In Prefix:	<input type="text"/>	
Destination:	<input type="text" value="700 : Default"/>	Search

Go to the “Inbound” parameters section and configure the “Number of Digits from CO” to 10. Configure all of the other trunk group parameters as necessary. Please refer to the ShoreTel Administration Guide for details on the configuration parameters. Once you’ve modified the trunk group parameters as needed “Save” your changes.

Note: If this is a new trunk group you will be prompted to allow access to all user groups, it is always a good practice to allow all user groups access to the newly created trunk group, but you can “Cancel” the request and provide individual user groups access to this new trunk group. Using ShoreWare Director configure the ShoreGear T1 as follows:

Switches

Edit ShoreGear T1 Switch

[New](#)
[Copy](#)
[Save](#)
[Delete](#)
[Reset](#)

[Edit this record](#)
[Refresh this page](#)

Name:

Description:

Site:

IP Address: [Find Switches](#)

Ethernet Address:

Server to Manage Switch:

Layer 3:

Protocol Type: ←

Central Office Type: ←

Call by Call Service:

☒ Enable Outbound Calling Name

Layer 1:

Clock Source: ←

Framing Format: ←

Line Code: ←

Line Build Out:

Go to the "Layer 3:" parameter section, configure the "Protocol Type" for "ISDN User" and the "Central Office Type" for "NI-2". In the "Layer 1:" parameter section configure the "Clock Source" for "Slave", the "Framing Format" for "ESF" and the "Line Code" for "B8ZS".

Scroll towards the bottom of the page to the channel parameters:

Channel	Port Type	Trunk Group	Description	Jack Number	Tx Gain (dB)	Rx Gain (dB)	
1 Edit	Trunk	PRI	Port		0	0	Fill Down
2 Edit	Trunk	PRI	Port (2)		0	0	
3 Edit	Trunk	PRI	Port (3)		0	0	
4 Edit	Trunk	PRI	Port (4)		0	0	
5 Edit	Trunk	PRI	Port (5)		0	0	
6 Edit	Trunk	PRI	Port (6)		0	0	
7 Edit	Trunk	PRI	Port (7)		0	0	
8 Edit	Trunk	PRI	Port (8)		0	0	
9 Edit	Trunk	PRI	Port (9)		0	0	
10 Edit	Trunk	PRI	Port (10)		0	0	

Begin on Channel 1 (do not click on the Edit option), configure the "Port Type" to "Trunk", then set the "Trunk Group" to match the trunk group name you created and define a "Description" (the "Description" is a label and can be anything, but you should define something that is useful and will allow you to

determine which channel is being utilized), then click on the “Fill Down” radio button. This action will automatically populate all of the remaining channels. Finally, be sure to “Save” all of the changes. This completes all the configuration modifications necessary on the ShoreTel system.

Adtran Configuration

To get started with the ADTRAN device configuration, refer to the Quick Start Guide and ADTRAN Operating System (AOS) and documentation CD included in the product box with each device. Quick Start Guides may also be downloaded from the ADTRAN support Web site at www.adtran.com/support by searching on the product device name. Once the ADTRAN device is unpacked and powered on, ADTRAN NetVanta platforms can be configured via a command-line interface accessible from a computer connect (9600 8 N 1) or via Telnet. Configuration may also be accomplished using the Web interface GUI that provides step-by-step configuration guidelines.

Initial configuration will be via the CRAFT port, where you'll define an IP address on ETH 0/1, the remaining configuration will be via the Web interface GUI. Plug your PC with a network cable and DHCP enabled into either Ethernet port (0/0; 0/1). The default IP of the system is 10.10.10.1.

If using a Com Port

- Pre-configured for 9600 8 N 1 using a straight through dB 9, RS 232 cable.
- Username and Passwords are all set to adtran.

Once you have successfully logged in, perform the following actions:

CONFIGURE THE UNIT'S IP ADDRESS

1. At the # prompt, enter config terminal.
2. At the (config)# prompt, enter interface eth 0/1 to access the configuration parameters for the ETH 0/1 Ethernet port located on the rear of the unit.
3. Enter ip address and assign an IP address to the Ethernet port using 24-bit subnet mask. This IP address and subnet mask are only examples, configure an IP address and subnet mask that are appropriate to your network environment. In addition, this IP address should be accessible from your internal network so you can complete the configuration from the Web User Interface.
4. Enter no shutdown to activate the interface to pass data.
5. Enter exit to exit the interface commands and return to the Global configuration mode.

Depending on your configuration, you may need to set a default gateway as well as using the (config)#ip default gateway command. If IP routing is enabled on the unit, do NOT set a default gateway.

Then enable Web interface access using the following configuration:

Web Access

```
Switch>
Switch>
Switch>en
Password:
Switch#conf t
Switch(config)#ip http server
```

Telnet configuration is not necessary but is recommended, use the following commands to enable Telnet access:

Telnet Configuration

```
Switch>
Switch>
Switch>en
Password: adtran
Switch#conf t
Switch(config)#line telnet 0 4
```



```
Switch(config-telnet0-4)#login
Switch(config-telnet0-4)#password adtran
Switch(config-telnet0-4)#
```

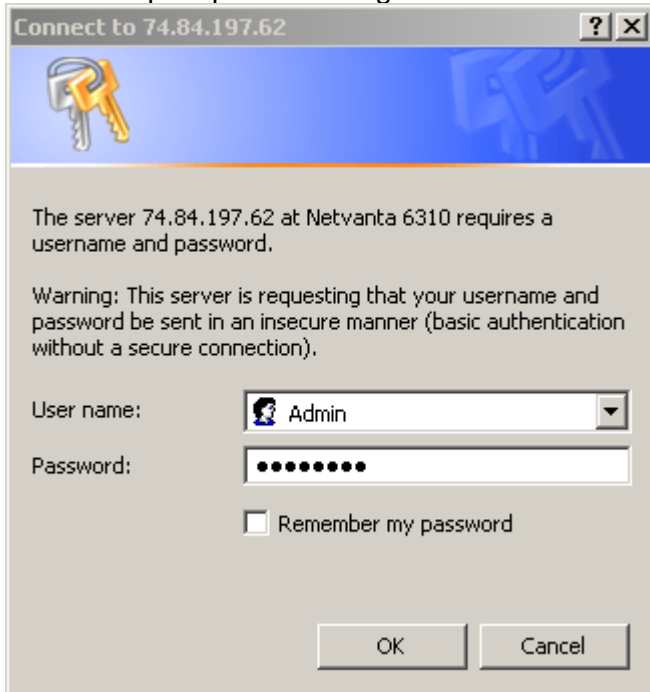
Note: Telnet and Web access require a static IP address or DHCP configured IP address. If accessing from a different subnet, routing configuration will be required.

Web User Interface

Using your preferred Web browser navigate to the Adtran NetVanta product Web interface GUI, using the IP address configured earlier via the CRAFT port, using the following syntax:

HTTP://10.10.10.1

You will be prompted with a login window:



The User name is admin and the password is also password.

Once you have successfully logged in you will get the System Summary page:

System Information

Hostname	NV6310
Firmware Version	A4.07.00.E
Part Number	1700100G1
Serial Number	LBADTN0935AJ932
System Uptime	1 weeks, 6 days, 18 hours, 36 minutes, 10 seconds
System Time	06:31:30 AM EDT
System Date	August 25, 2011
Memory	Total Heap: 85,134,320 Bytes Free Heap: 60,066,800 Bytes
CPU Utilization	System Load: 2.24% 1 Min Avg Load: 9.81% 5 Min Avg Load: 10.9% Min Load: 0% Max Load: 100% Context Switch Load: 0.11%
File System	Total: 60,455,775 Bytes Used: 26,021,460 Bytes Free: 34,434,315 Bytes
Time Server	(Not Configured)

WARNING!!! A problem has been detected with your system. Please go to the troubleshooting page for more detail.

Clear CPU Max Load

Refresh in 4 seconds...

WAN Summary

Status for the WAN interface.

We will only cover the parameters necessary to get the systems to interoperate. For other parameters please refer to Adtran's documentation.

Physical Interface Configuration

From the System Summary page scroll down to the Physical Interfaces summary page:

Physical Interfaces

This is a list of all the physical interfaces that are either physically tied to the product or connected via a plug-in module. View or edit the configuration of an interface by clicking its name.

Name	Logical Interface	Line Status	Type
eth 0/1	none	Interface Disabled	Ethernet
eth 0/2	none	100Mbps/full	Ethernet
t1 0/1	pri 1	Up	WAN-T1

Statistics Rate Interval: Statistics Rate Interval (in seconds)

Apply

Then select the available T1 0/1 interface you want to enable and configure, for connection to the ShoreGear T1.

ADTRAN **Netvanta 6310** [Save](#) [Logout](#)

Physical Interfaces > t1 0/1

Configuration for "t1 0/1"

Basic configuration for the T1 interface.

Description:	<input type="text" value="ShoreTel_PRI_Handoff"/>	Description label (optional)
Enable:	<input checked="" type="checkbox"/>	Enable or disable this interface
Clocking:	System-Wide Clock Source	Please go to the ' Clock Source ' page to set the system clock source.
Framing:	<input type="text" value="ESF"/>	Select the framing that matches the network provider framing format ?
Coding:	<input type="text" value="B8ZS"/>	Select the coding that matches the network provider line coding
FDL:	<input type="text" value="AT&T"/>	Select the format for the facility data link channel ?

This action brings up the Physical Interfaces page, in the "Configuration for "t1 0/1"" perform the following:

1. Define a "Description" for the interface (we chose ShoreTel_PRI_Handoff).
2. Click to the right of the "Enable" parameter to enable the interface, the box should now be checked.
3. Clocking will be discussed below.
4. Configure the "Framing" parameter to "ESF".
5. Configure the "Coding" parameter to "B8ZS".
6. Configure the "FDL" parameter to "AT&T".
7. Click on the "Apply" radio button. You will get the message "Settings applied successfully".

Scroll down to the "Configured DS0 Connections for "t1 0/1":

Configured DS0 Connections for "t1 0/1"

Use this dialog to connect a group of DS0's to a particular interface or service provided by this unit. To configure a connected interface's settings, click on the item in the list below. To remap a group of DS0's that are currently in use, click the delete button to remove the connections group.

Add a Connection

Connect To: *Select an interface type to map to the DS0s*

Available DS0 Range: **All DS0s in use**

DS0 Range: to *Set the range of DS0s to be mapped*

Speed: *Select the speed for the DS0s being mapped*

Connected Interface	Multilink	DS0's Used	Group Number	Speed	
pri 1	N/A	1-24	1	64kbps	<input type="button" value="Delete"/>

You will need to add the DS0s for the PRI by performing the following:

1. For the "Connect To:" parameter select "PRI".
2. For the "DS0 Range:" parameter select "1" to "24".
3. Click on the "Add" radio button.

This action brings up the "PRI Configuration" page:

Netvanta 6310

Save Logout

Physical Interfaces > PRI Config

PRI Configuration

Basic configuration for PRI interface.

Description:

SNMP Alias:

Enabled: ☒

Switch Type:

Protocol Emulation:

B-Channel Restart: ☒ Enabled

Resource Selection:

Name Delivery:

Digits Transferred:

Digit Prefix:

System

- System Summary
- Physical Interfaces
- Passwords
- IP Services
- DHCP Server
- Hostname / DNS
- LLDP
- SNMP

Voice

Data

Monitoring

Utilities

1. The “Description:” defaults to “pri 1”, leave it at default as you will need this entry later on when defining the trunk account for ISDN.
2. Enable the PRI interface by clicking the box to the right of “Enabled:”.
3. Set the “Switch Type:” to “National ISDN 2”
4. Set the “Protocol Emulation:” to “Network”.
5. Set the “B-Channel Restart:” option to “enabled”.
6. Set the “Name Delivery:” parameter to “display”.
7. Set the “Digits Transferred:” parameter to “All”.
8. Click on the “Apply” radio button. You will get the message “**PRI Interface updated successfully**”.

We will now update the system clock, under the “System” area click on the “System Summary”:

The screenshot displays the Netvanta 6310 web management interface. On the left is a navigation menu with categories: System (expanded), Voice, Data, Monitoring, and Utilities. Under 'System', 'System Summary' is selected. The main content area, titled 'System Information', shows various system metrics:

System Information	
Hostname	NV6310
Firmware Version	A4.07.00.E
Part Number	1700100G1
Serial Number	LBADTN0935AJ932
System Uptime	1 weeks, 6 days, 19 hours, 16 minutes, 23 seconds
System Time	07:11:44 AM EDT
System Date	August 25, 2011
Memory	Total Heap: 85,134,320 Bytes Free Heap: 60,066,800 Bytes
CPU Utilization	System Load: 3.28% 1 Min Avg Load: 7.65% 5 Min Avg Load: 4.36% Min Load: 0% Max Load: 100% Context Switch Load: 0.11%
File System	Total: 60,455,775 Bytes Used: 26,022,465 Bytes Free: 34,433,310 Bytes
Time Server	(Not Configured)

Below the table, a red warning message states: "WARNING!! A problem has been detected with your system. Please go to the troubleshooting page for more detail." A button labeled "Clear CPU Max Load" is present. At the bottom, it says "Refresh in 3 seconds..."

Click on the “Current System Time” link, this action will bring up the “System > Time Server” page:

Netvanta 6310 Save Logout

System > Time Server Configuration

Time Server Configuration

Configuration

Use this form to configure the time server.

Time Server:

Time: :

Date:

Auto-Correct DST: ☒

Time Zone:

Reset Apply

Set the time to the appropriate time, or use a known good NTP server in your geography. You will get the message **“Settings applied successfully”**.

Eth 0/2 Interface Configuration

We will now configure the external / WAN Ethernet interface, this will be the interface that EtherSpeak will send calls to. You will need to navigate to the “Configuration for “Ethernet 0/2”” page, you can do so either from the “System Summary” page, where you will need to scroll to the bottom of the page (Ethernet Summary) and click on the interface name “eth 0/2”. Or from the “Physical Interfaces” page, click on the interface name of “eth 0/2”, both of these pages are available under the “System” pull down menu on the left hand side of the Adtran Web UI.

Netvanta 6310 Save Logout

System > Physical Interfaces

Physical Interfaces

This is a list of all the physical interfaces that are either physically tied to the product or connected via a plug-in module. View or edit the configuration of an interface by clicking its name.

Name	Logical Interface	Line Status	Type
eth 0/1	none	Interface Disabled	Ethernet
eth 0/2	none	100Mbps/full	Ethernet
tl 0/1	pri 1	Up	WAN-T1

Statistics Rate Interval: Statistics Rate Interval (in seconds)

Apply

The “Configuration for “Eth 0/2”” page will look as follows:

Netvanta 6310

[Save](#)
[Logout](#)

System

System Summary
Physical Interfaces
Passwords
IP Services
DHCP Server
Hostname / DNS
LLDP
SNMP

Voice

Data

Monitoring

Utilities

click to toggle menu

Physical Interfaces > Ethernet 0/2

Configuration for "Ethernet 0/2"

Basic configuration for the Ethernet interface.

Description: WAN_SIP_Interface
Description label (optional)

Enable: ☒
Enable or disable this interface.

Speed/Duplex: Auto
Selection of Auto will auto-negotiate the best speed and duplex.

Factory MAC Address: 00 : A0 : C8 : 4A : 9B : 5A
The factory Media Access Control address

MAC Address Masquerade: ☐
Check to allow MAC Address Masquerade.

MAC Address: 00 : A0 : C8 : 4A : 9B : 5A
Set the masquerade Media Access Control address.

Supplicant: ☐
Enable supplicant mode.

Traffic-Shaping: ☐
Enable traffic-shaping.

Qos-policy: None
Outbound QoS-Policy map

Interface Mode: IP routing
Select an interface mode.

Wireless Control Protocol

Enable AWCP: ☒
Enable/Disable Wireless Control Protocol.

IP Settings

Address Type: Static

IP Address: 74 . 84 . 197 . 62
IP address for this numbered interface

Subnet Mask: 255 . 255 . 255 . 240
Subnet Mask for this numbered interface

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

Secondary IP Settings

To add a range of secondary IP addresses (up to 255 addresses), enter a valid start IP address, IP mask, and the number of addresses to add.

Range	Start IP Address	Mask
ADD A NEW SECONDARY IP ADDRESS		

Media-Gateway

IP Address Type: Loopback

RTP traffic will flow over the selected IP address.

Loopback IP Address: loop 1 (10.20.254.26)
Select the loopback IP address over which RTP traffic will flow.

Reset

Apply

1. Define a "Description:" for the label, we chose WAN SIP Interface.
2. Enable the interface by clicking to the right of "Enable:", making sure that the box is checked.
3. Set the "Interface Mode:" to "IP routing".
4. In the "IP Settings" area, be sure to configure the interface as appropriate, setting the "Address Type:", "IP Address:", "Subnet Mask:", and "Dynamic DNS:".
5. Click on the "Apply" radio button.

960 Stewart Drive Sunnyvale, CA 94085 USA Phone +1.408.331.3300 +1.877.80SHORE Fax +1.408.331.3333 www.ShoreTel.com

- 21 -

System Summary

Connect all of the appropriate cables (a T1 crossover cable between the ShoreGear T1 and the NetVanta T1 interface and the appropriate Ethernet cables), then click on the “System Summary” link:

1. Verify that you don’t have any warnings in the “System Information” section.
2. Verify that the “WAN Summary” section shows the T1 interface “Link” as “Up” and green.
3. Depending on your requirements – verify that Ethernet Interface 0/0 is disabled. (If you wish to enable Ethernet 0/0 with a private IP address – you may do so. However, for security reasons we prefer to have disabled the access to the internal LAN and have disabled that interface).
4. Verify that the “Ethernet Summary” section shows the “Link” for both Ethernet interfaces with the correct Ethernet link speed; and with 0/0 disabled and 0/1 enabled.

If you have any warnings, be sure to review your configuration and cabling.

Trunk Account Configuration

Click on the “Voice” link, this will expand the available options:

The screenshot shows the Netvanta 6310 web interface. On the left is a navigation menu with categories: System, Voice, Stations, Trunks, System Setup, and Reports. The 'Voice' category is expanded, showing 'Trunk Accounts' as the selected option. The main content area is titled 'Add / Modify / Delete Trunk Accounts'. It contains a form to 'Add a New Trunk Account' with fields for 'Trunk Name' and 'Type' (set to 'SIP'), and an 'Add' button. Below this is a table for 'Modify/Delete Trunk Account' with columns: Trunk Name, ID, Type, Supervision, Role, and a 'Delete' button. The table lists two entries: 'EtherSpeak_SureTrunk' (T01, SIP, SIP, User) and 'ShoreTel_PRI_Handoff' (T02, ISDN, ISDN, Network).

In the “Trunks” section click on “Trunk Accounts”, this action brings up the “Add / Modify / Delete Trunk Accounts” page. You will need to add two separate trunk accounts (one for SIP and one for ISDN).

We’ll add the SIP trunk account first:

1. Define a “Trunk Name:” that is appropriate, we chose EtherSpeak_SureTrunk
2. Set the “Type:” to “SIP”
3. Click on the “Add” radio button.

This action brings up the “Trunk Accounts > Txx” page which includes a “Trunk Status” section and “Edit SIP Trunk” section. We’ll begin with the “Trunk Status” section:

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** ?

Reset Apply

1. The "Operational Status:" may be "**Unavailable**" after you apply ALL of the settings it will become "**Available**".
2. Verify that the "Administrative Status:" is "Enabled".
3. Click on the "Apply" radio button. You will get the message "**Administrative status set successfully**".

Scroll down to the "Edit SIP Trunk Section":

Edit SIP Trunk

Use this screen to modify the SIP Trunk configuration.

Trunk Account Information

Trunk ID: T01 ?

Type: SIP ?

Trunk Name: **EtherSpeak_SureTrunk** ?

Reject External: ☐ ?

Max Number Calls: **84** ?

Emergency Caller ID Override: Use Match-Substitution: ☐ ?

Inbound Caller ID Override: ?

Inbound Caller ID Override Method: **Always** ?

SIP Settings ANI Substitution DNIS Substitution DNIS:ANI Replacement

SIP Server Address: ☐ Not Set ☒ IP Address: **172 . 26 . 1 . 90** ?

☐ Host Name:

SIP Server Port: **5060** ?

SIP Proxy Address: ☐ Not Set ☐ IP Address: ?

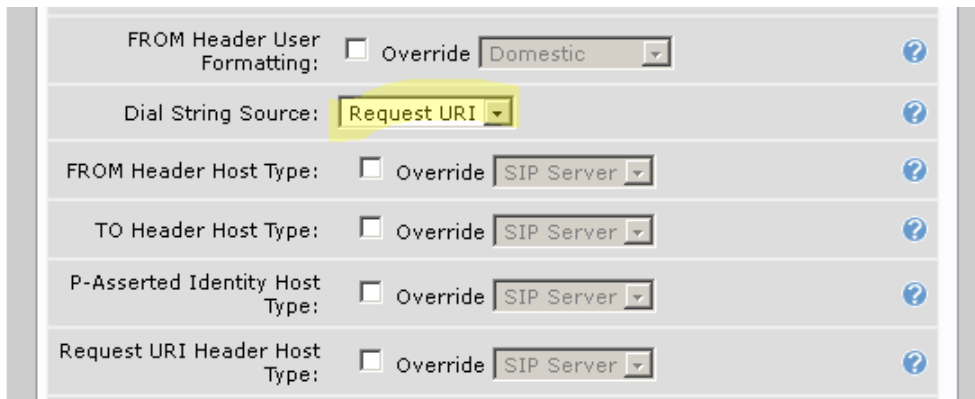
☐ Host Name:

SIP Proxy Port: ?

SIP Conferencing URI: ?

The “Trunk ID:” will be auto assigned, but in general will be “T01”, the “Type:” should be “SIP”, if it is not “SIP then you added the “Trunk Group” incorrectly, be sure to add the “Type” as “SIP” above. Define a “Trunk Name:” this can be anything you choose, we set the name as “EtherSpeak_SureTrunk”. Scroll down to SIP Settings tab and add the IP of 172.26.1.90. This IP will be accessed over a VPN.

1. Set “SIP Server Address:” parameter to “IP” and define the IP address given to you by EtherSpeak - add the IP of 172.26.1.90.
 2. Set “SIP Server Port:” parameter to “5060”.
 3. Set the “Dial String Source:” parameter to “Request URI”.
- No other parameters require adjustment, leave them at default settings. Scroll to the bottom of the “SIP Registrar Settings”:



FROM Header User Formatting:	<input type="checkbox"/> Override	Domestic	?
Dial String Source:		Request URI	?
FROM Header Host Type:	<input type="checkbox"/> Override	SIP Server	?
TO Header Host Type:	<input type="checkbox"/> Override	SIP Server	?
P-Asserted Identity Host Type:	<input type="checkbox"/> Override	SIP Server	?
Request URI Header Host Type:	<input type="checkbox"/> Override	SIP Server	?

4. Set the “Codec Group:” parameter to “711_729 (G.711 uLaw, G729)”.

No other parameter modifications are necessary in this area.

5. Click on the “Apply” radio button. This action will change the page to the main “Trunk Accounts” and you will get the message “**SIP Trunk updated successfully**”.

We will now add the “ISDN” trunk account:

Netvanta 6310

[Save](#) [Logout](#)

System

Voice

Stations

User Accounts

Ring Groups

Trunks

Trunk Accounts

Trunk Groups

System Setup

Classes of Service

Dial Plan

ISDN Num Templates

Codec Lists

Call Coverage Lists

System Parameters

Local SIP Server

Local SIP Proxy

SIP Client Locations

VoIP Settings

Email Alerts

Add / Modify / Delete Trunk Accounts

Use this page to add and configure trunk accounts.

Add a New Trunk Account

Trunk Name:

Type: SIP

Modify/Delete Trunk Account

Click on a name to edit that trunk's settings.

Trunk Name	ID	Type	Supervision	Role	
EtherSpeak_SureTrunk	T01	SIP	SIP	User	<input type="button" value="Delete"/>
ShoreTel_PRI_Handoff	T02	ISDN	ISDN	Network	<input type="button" value="Delete"/>

1. Define a "Trunk Name:" that is appropriate, we chose ShoreTel_PRI_Handoff.
2. Set the "Type:" to "ISDN".
3. Click on the "Add" radio button.

This action brings up the "Trunk Accounts > Txx" page which includes a "Trunk Status" section and "Edit Trunk" section. We'll begin with the "Trunk Status" section:

Voice

Stations

User Accounts

Ring Groups

Trunks

Trunk Accounts

Trunk Groups

System Setup

Classes of Service

Dial Plan

ISDN Num Templates

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

1. The "Operational Status:" may be "**Unavailable**" after you apply ALL of the settings it will become "**Available**".
2. Verify that the "Administrative Status:" is "Enabled".
3. Click on the "Apply" radio button. You will get the message "**Administrative status set successfully**".

Scroll down to the "Edit Trunk Section":

Edit Trunk

Use this dialog to modify the Trunk Account configuration.

Trunk Account Information	
Trunk ID: T02	?
Type: ISDN	?
Supervision: ISDN	?
Trunk Name: ShoreTel_PRI_Handoff	?
Reject External: <input type="checkbox"/>	?
Resource Selection: Circular Hunt Descending	?
Emergency Caller ID Override: <input type="text"/> Use Match-Substitution: <input type="checkbox"/>	?
Inbound Caller ID Override: <input type="text"/>	?
Inbound Caller ID Override Method: Always	?
ISDN Settings	
ISDN Interface: pri 1	?
Min Needed B Channels: <input checked="" type="radio"/> Not specified <input type="radio"/> Specified: <input type="text"/>	?
Max Needed B Channels: <input checked="" type="radio"/> Not specified <input type="radio"/> Specified: <input type="text"/>	?

The “Trunk ID:” will be automatically assigned, if it s a new installation it will most likely be “T02. Verify that the “Type:” and “Supervision:” are set to “ISDN”, if they are not, then you added the incorrect “Type” for the “Trunk Account” above. The “Trunk Name:” will be what you defined when adding the trunk account, you may modify it here (if necessary).

1. Set the “Resource Selection:” to “Circular Hunt Descending”.
2. Set the “ISDN Interface:” to the entry you created above (PRI Configuration), should be named “pri 1”.

No additional modifications are necessary; the default settings should not be adjuste, scroll to the bottom of the page and click on the “Apply” radio button. This action will change the page to the main “Trunk Accounts” and you will get the message **“Trunk updated successfully”**.

Trunk Group Configuration

On the left of the Web UI, below the “Trunks” section, click on the “Trunk Groups” link:

Add / Modify / Delete Trunk Groups

Use this page to add and configure trunk groups.

Add a New Trunk Group

Group Name: *Enter a name for this group.*

Modify/Delete Trunk Group

This is a description of this list

Trunk Group	Description
SIP	<input type="button" value="Delete"/>
ISDN	<input type="button" value="Delete"/>

You will need to define two trunk groups, one for SIP and one for PRI, we will add SIP first. In the "Group Name:" section type SIP and click on the "Add" radio button. This action brings up the "Edit Trunk Group 'SIP'" page:

Voice

Stations

User Accounts

Ring Groups

Trunks

Trunk Accounts

Trunk Groups

System Setup

Classes of Service

Dial Plan

ISDN Num Templates

Codec Lists

Call Coverage Lists

System Parameters

Local SIP Server

Local SIP Proxy

SIP Client Locations

VoIP Settings

Email Alerts

Reports

Extensions List

SIP Registrations

Call Quality Stats

RTP Channel Stats

RTP Session Stats

Trunk Statistics

Data

Monitoring

Utilities

Edit Trunk Group 'SIP'

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

Trunk Group Information

Trunk Group Name: SIP

Description:

Resource Selection:

Trunk Group Members

Below is a list of [Trunk Accounts](#) that are being used in this Trunk Group.

Trunk Account	ID	Type	Supervision
EtherSpeak SureTrunk	T01	SIP	SIP <input type="button" value="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).

<input type="checkbox"/> Local Calls (10 Digit)	Low Cost	(NXX-NXX-XXXX)
<input type="checkbox"/> Long Distance Calls	Low Cost	(1-NXX-NXX-XXXX)
<input type="checkbox"/> Toll-Free Calls	Low Cost	(1-800/855/866/877/888-NXX-XXXX)
<input type="checkbox"/> International Calls	Low Cost	(011-\$)
<input type="checkbox"/> n11 Calls (411, 611)	Low Cost	(411, 611)
<input type="checkbox"/> 911 Calls	Low Cost	(911)
<input type="checkbox"/> Operator-Assisted calls	Low Cost	(0-NXX-NXX-XXXX)
<input type="checkbox"/> Carrier Specified calls	Low Cost	(10-10-XXX-\$)
<input type="checkbox"/> 900 Calls	Low Cost	(1-900/976-NXX-XXXX 976-XXXX)

Verify that the “Resource Selection:” parameter is set to “Linear Hunt” (this is the default setting), then click on the “Add Members...” radio button, this action brings up the “Add Members to Trunk Group” pop-up window:

Set the “Outbound Call Templates” parameters as needed and click on the “Apply” radio button. This action takes you back to the main “Trunk Group” page (Add / Modify / Delete Trunk Groups) and you will get the message “**Settings applied successfully**”.

The screenshot shows the Netvanta 6310 web interface. The left sidebar contains a navigation menu with categories: System, Voice, Trunks, System Setup, Reports, Data, Monitoring, and Utilities. The main content area is titled 'Edit Trunk Group 'ISDN'' and includes a 'Save' and 'Logout' link. The page content is organized into sections: 'Trunk Group Information' (with fields for Name, Description, and Resource Selection set to 'Linear Hunt'), 'Trunk Group Members' (with an 'Add Members..' button and a table of existing members), and 'Outbound Call Templates' (with checkboxes and dropdowns for various call types like Local, Long Distance, Toll-Free, etc.).

Trunk Account	ID	Type	Supervision	
ShoreTel PRI Handoff	T02	ISDN	ISDN	Delete

We will now add the PRI trunk group. In the “Group Name:” section type PRI and click on the “Add” radio button. This action brings up the “Edit Trunk Group ‘PRI’ ” page:

System

Voice

Stations

User Accounts

Ring Groups

Trunks

Trunk Accounts

Trunk Groups

System Setup

Classes of Service

Dial Plan

ISDN Num Templates

Codec Lists

Call Coverage Lists

System Parameters

Local SIP Server

Local SIP Proxy

SIP Client Locations

VoIP Settings

Email Alerts

Reports

Extensions List

SIP Registrations

Call Quality Stats

RTP Channel Stats

RTP Session Stats

Trunk Statistics

Data

Monitoring

Utilities

Trunk Accounts > 'ShoreTel PRI Handoff'

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

Reset

Apply

Edit Trunk

Use this dialog to modify the Trunk Account configuration.

Trunk Account Information

Trunk ID: T02

Type: ISDN

Supervision: ISDN

Trunk Name: ShoreTel_PRI_Handoff

Reject External: ☐

Resource Selection: Circular Hunt Descending

Emergency Caller ID Override:

Use Match-Substitution: ☐

Inbound Caller ID Override:

Inbound Caller ID Override Method: Always

ISDN Settings

ISDN Interface: pri 1

Min Needed B Channels: ☒ Not specified ☐ Specified:

Verify that the “Resource Selection:” parameter is set to “Circular Hunt Descending”. Click to the left of the “ISDN” trunk account (which was created earlier) to select the ISDN trunk account. Then click on the “Add Selected Trunks” radio button. This action takes you back to the “Edit Trunk Group ‘PRI ’” page, but now you’ll have the “ShoreTel” account listed in the “Trunk Group Members” section and you will get the message “**Account(s) added successfully**”.

VoIP Settings	ANI Substitution	DNIS Substitution	DNIS:ANI Replacement
Codec Group: PCMU_G729 (G.711 uLaw, G.729) ?			
Modem Passthrough: <input type="checkbox"/> Enabled ? Detection Timespan: 8 secs <0-8>			
T38: <input checked="" type="checkbox"/> Enabled ?			
VAD: <input type="checkbox"/> Enabled ?			
PLC: <input type="checkbox"/> Enabled ?			
NLS: <input checked="" type="checkbox"/> Enabled ?			
ALC: <input type="checkbox"/> Enabled ?			
Echo Cancellation: <input checked="" type="checkbox"/> Enabled ?			
RTP Settings			
Frame Packetization: 20 ms ?			
Packet Delay Mode: Adaptive ?			
Packet Delay:			
	Nominal:	50 ms	<10 - 240, incr of 10>
	Maximum:	100 ms	<40 - 320, incr of 10>
	Fax:	50 ms	<0 - 500>
<input type="button" value="Set to Defaults"/>			
DTMF Relay:			
	<input type="radio"/> Inband		
	<input checked="" type="radio"/> NTE Value: 101 <96 - 127>		
RTP DSCP Value:			
	<input checked="" type="radio"/> Use Global Default : 46		
	<input type="radio"/> Specified: -1 <0 - 63>		
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>			

Set the “Codec Group” selection parameters as needed and click on the “Apply” radio button. Then click the Apply button at the bottom of the page.

Configuration of Loopback Interface

What differentiates this solution over previous methods for SIP connection is that this solution provides the highest level of security available for ShoreTel customers wanting to use SIP trunks with ShoreTel over the public Internet.

To that end, the solution requires the configuration of a VPN tunnel from the NetVanta device to the EtherSpeak edge.

Physical Connections required:

1. Ethernet 0/1 needs to be plugged into the customer router and the customer needs to provide an available public IP address
2. Ethernet 0/0 is disabled to ensure the highest level of security. At the customer’s option, this interface may be enabled for LAN access to the NetVanta router
3. PRI port is connected to ShoreTel PRI switch (e.g. 220T1) with a T1 cross-over cable

4. The loopback interface is configured for a virtual private IP address to use for the IP SEC encryption

To configure the loop back address, go to DATA / Loopback Interfaces.

The screenshot shows the Netvanta 6310 web interface. On the left is a navigation menu with categories: System, Voice, Data, and Firewall. Under 'Data', there is a sub-menu for 'Loopback Interfaces'. The main content area is titled 'Configuration for "loop 2"'. It contains fields for 'Description' (with a placeholder 'Description label (optional)'), an 'Enable' checkbox which is checked, and 'IP Settings'. Under 'IP Settings', 'Address Type' is set to 'None' and 'Dynamic DNS' is set to '<disabled>' (with a note 'Used to register this interface's IP address with a DNS Name.'). At the bottom are 'Cancel' and 'Apply' buttons.

Then select enable (if not by default), select address to type “static” and then enter a unique private IP address. This IP has to be unique to EtherSpeak – and should also be unique from your LAN network of IP addresses. Please consult with EtherSpeak about which loopback address you would like to use as each address has to be unique to EtherSpeak. Ensure Dynamic DNS is disabled, then click apply.

The screenshot shows the 'Configuration for "loop 1"' page. It has a 'Description' field (placeholder: 'Description label (optional)'), an 'Enable' checkbox which is checked, and 'IP Settings'. Under 'IP Settings', 'Address Type' is set to 'Static'. The 'IP Address' field is filled with '10', '20', '254', and '27'. The 'Subnet Mask' field is filled with '255', '255', '255', and '255'. The 'Dynamic DNS' field is set to '<disabled>' (with a note 'Used to register this interface's IP address with a DNS Name.'). At the bottom are 'Cancel' and 'Apply' buttons.

After the physical connections and the loopback address is established, go to Data / VPN / VPN Peers and type a name for the tunnel. In this example, we typed “EtherSpeak” and assigned the VPN to the Untrust interface and the statically assigned IP address.

ADTRAN **Netvanta 6310** Save Logout

VPN Peers > Creating a New VPN Peer...

System
Voice
Data
 Router / Bridge
 Default Gateway
 Routing
 Route Table
 IP Interfaces
 Loopback Interfaces
 GRE Tunnels
 QoS Wizard
 QoS Maps
 Bridging
 UDP Relay
 Spanning Tree
Firewall
 Firewall Wizard
 General Firewall
 Security Zones
Network Monitor
 Wizard
 Probes / Tracks
 Probe Responder
URL Filtering
 URL Filters
 Top Websites
Wireless
 AC / AP Discovery
 APs / Radios / VAPs
 Clients
 MAC Access List
 AP Firmware
VPN
 VPN Wizard
VPN Peers
 Certificates

Step 1: Please enter information about what type of peer you are wanting to configure

Before you can start to configure your new VPN Peer, I need some information about your configuration.

VPN Peer Configuration

Name: *Set a name for this VPN Peer.*

VPN Interface: *Select the Interface that will Terminate the VPN Tunnel.*

Peer Type: ☒ Static Addressed *If the VPN Peer's address is static (assigned by the Service Provider).*

☐ Dynamically Addressed *If the VPN Peer's address is dynamic (DHCP, PPPoE, etc.)*

☐ Mobile Peer *This is used for VPN client software peers.*

Once that is complete, you need to make sure the loop back is enabled to pass the SIP traffic to the PRI on the NetVanta. To do so, select the Public Interface, Eth 0/2.

ADTRAN **Netvanta 6310** Save Logout

System
Voice
Data
 Router / Bridge
 Default Gateway
 Routing
 Route Table
IP Interfaces
 Loopback Interfaces
 GRE Tunnels
 QoS Wizard
 QoS Maps

IP Interfaces

This is a list of all of the IP interfaces configured in this unit. View or edit the configuration of an interface by clicking its name.

Name	IP Address	Netmask	Type	
loop 1	10.20.254.27	255.255.255.255	Loopback	<input type="button" value="Delete"/>
eth 0/2	75.151.110.195	255.255.255.240	Ethernet	
eth 0/1	192.168.66.231	255.255.255.0	Ethernet	

Once you select the Eth 0/2, scroll to the bottom until you see the Media Gateway setting. This setting instructs the NetVanta to bridge the SIP media packets (RTP) to the PRI interface on the NetVanta and then to the ShoreTel.

Media-Gateway

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

Loopback IP Address: *Select the loopback IP address over which RTP traffic will flow.*

Configuration of VPN Tunnel Settings to Connect to EtherSpeak



We then click into “EtherSpeak” from the VPN Peers main screen and enter the VPN connection information including IKE information, IPSEC information and information regarding the two hosts that will connect the networks together to permit encrypted SIP communications.

The screenshot shows the Netvanta 6310 web interface. The left sidebar contains a navigation menu with categories: System, Voice, Data, Firewall, Network Monitor, URL Filtering, and Wireless. The 'Data' category is expanded, showing options like Router / Bridge, Default Gateway, Routing, Route Table, IP Interfaces, Loopback Interfaces, GRE Tunnels, QoS Wizard, QoS Maps, Bridging, UDP Relay, and Spanning Tree. The 'VPN' category is also visible at the bottom. The main content area is titled 'Step 1 of 5: VPN Peer Configuration for "EtherSpeak"'. It includes a 'VPN Peer Configuration' section with fields for Name (EtherSpeak), VPN Interface (eth 0/2), and Peer Type (Static Addressed). Below this is an 'IKE Configuration' section with fields for XAUTH Enabled (Disabled), Initiate Mode (Main), and Respond Mode (Main). Each field has a corresponding help text on the right.

Netvanta 6310 Save Logout

VPN Peers > EtherSpeak

Step 1 of 5: VPN Peer Configuration for "EtherSpeak"

You are able to base a VPN Peer off of another VPN peer or create a new Peer from scratch.

VPN Peer Configuration

Name: *Set a name for this VPN Peer.*

VPN Interface: *Interface that will Terminate the VPN Tunnel.*

Peer Type: ☒ Static Addressed *If the VPN Peer's address is static (assigned by the Service Provider).*

☐ Dynamically Addressed *If the VPN Peer's address is dynamic (DHCP, PPPoE, etc.)*

☐ Mobile Peer *This is used for VPN client software peers.*

IKE Configuration

XAUTH Enabled: *You must enable AAA to do XAUTH.*

Initiate Mode: *Select the mode of IKE you would like to initiate VPN tunnels with the VPN Peer.*

Respond Mode: *Select the mode of IKE that you will allow the VPN Peer to use when initiating tunnels with us.*

There are two main configuration components with establishing an IPSEC tunnel between two endpoints over the Internet. The first is IKE settings and the second is IPSEC settings. They are also commonly referred to as “Phase 1 settings” and “Phase 2 settings”.

For the IKE Settings – you will need to provide information that will be supplied by EtherSpeak. For this example, we have illustrated some settings.

Initiate Mode: MAIN

Respond Mode: MAIN

NAT Traversal: Allow both V1 and allow V2

Peer Address: 4.28.51.x (ask EtherSpeak for correct connection info)

Remote ID: Optional

Preshared Key: Is a unique passphrase that will be issued by EtherSpeak. For this illustration we entered “password”

Local ID: Optional

IKE Configuration	
XAUTH Enabled: <input type="button" value="Disabled"/>	You must enable AAA to do XAUTH. ?
Initiate Mode: <input type="button" value="Main"/>	Select the mode of IKE you would like to initiate VPN tunnels with the VPN Peer.
Respond Mode: <input type="button" value="Main"/>	Select the mode of IKE that you will allow the VPN Peer to use when initiating tunnels with us.
NAT Traversal: <input type="button" value="Allow V1"/> <input type="button" value="Allow V2"/>	Enable/Disable/Force NAT-T for this VPN Peer. ?
Peer Address: <input type="text" value="4.28.51.55"/>	Enter a valid IP Address or a hostname of the peer.
Remote ID: <input type="button" value="IP Address"/> <input type="text" value="4.28.51.55"/>	This uniquely identifies the Peer from other Peers.
Preshared Key: <input type="text" value="password"/>	This is used to authenticate the IKE negotiations with the peer.
Also, add Peer Address as Remote ID: <input type="checkbox"/>	You are required to have an IP Address Remote ID when using main mode.
Local ID: <input type="button" value="IP Address"/> <input type="text" value="75.151.110.122"/>	This uniquely identifies us to the Peer.

For the IPSEC settings, you need to specify the following:

Perfect Forward Secrecy or PFS: Group 2

Reverse Route: check Enable

Encryption Hash: ESP: AES 128bit / SHA1

IPSec Configuration		
PFS:	Group 2 ▼	Select the PFS Group.
Reverse Route:	<div>Enable: <input checked="" type="checkbox"/></div> <div>Administrative Distance (optional): <input type="text" value="1"/></div> <div>Tag (optional): <input type="text" value="0"/></div>	Check to insert peer's network into the route table. You can also enter the distance metric (1-255) and an administrative tag (1-65535) for this network.
Encryption / Hash:	ESP: AES 128bit / SHA1 ▼	Select an Encryption scheme and hash.
Encryption / Hash:	No additional Transforms. ▼	Select an additional Encryption scheme and hash.
Lifetime:	3600 seconds <input type="text"/> KB	Specify the Lifetime in seconds and/or kB of traffic.
Voice Quality Monitoring		
Monitor RTP Streams:	<input type="checkbox"/>	Check this box if monitoring RTP streams passing over this VPN tunnel. VQM will need to be enabled on the RTP Monitoring page.
<div>Cancel</div> <div>Apply</div>		

You then must select the IKE attributes for connection "EtherSpeak".

Encryption / Hash: 3 DES / SHA1

Diffey Helman: Group 2

Lifetime: 288000

Click Apply

Step 2 of 5: Add/Delete IKE Attributes for "EtherSpeak"

Create new IKE attributes here. To modify an existing attribute, delete the original and replace it with a new one.

Add/Delete IKE Attributes for IKE Priority ID 100

Encryption / Hash: /

Set encryption/hash algorithm for protection suite.

Authentication:

Set authentication method for protection suite.

DH Group:

Set the Diffie-Hellman group.

Lifetime: seconds

Set lifetime for IKE security association.

IKE Attribute List

Click on an attribute grouping to configure the above panel with its settings. Click on the arrows to change the order in which the attributes are processed.

	Encryption	Hash	Authentication	DH Group	Lifetime	
▲▼	3des	sha	pre-share	2	28800	<input type="button" value="Delete"/>

The next step is to identify which networks (or hosts in this case) are permitted to communicate on the VPN. The local network is the customer network / premise and the remote network is EtherSpeak's network.

For Local Network: Loopback with a 255.255.255.255 or /32 subnet mask. Recall that the Loopback address is a virtual address that is only on this device and only necessary to enable the encrypted communications. Click Add.

Step 3 of 5: Source Networks Allowed to Communicate Using "EtherSpeak"

The Source network(s) of this Netvanta will be able to communicate with the VPN Peer's Destination network(s). Enter the **Source** network(s) here.

Local Network: . . .

The IP Subnet local to this Netvanta

Local Network Mask: . . .

The Subnet Mask

Local IP Subnet	Local Subnet Mask	
10.20.254.27	255.255.255.255	<input type="button" value="Delete"/>

For the Destination (or remote) network setting, enter 172.26.1.90 with a subnet mask of 255.255.255.255 or a subnet mask of /32. This identifies the only host that may speak with the Adtran. Click Add.

Step 4 of 5: Destination Networks Allowed to Communicate Using "EtherSpeak"

The Source network(s) of this Netvanta will be able to communicate with the VPN Peer's Destination network(s). Enter the **Destination** network(s) here.

Remote Network:	172 . 26 . 1 . 90	The IP Subnet local to the VPN Peer
Remote Network Mask:	255 . 255 . 255 . 255	The Subnet Mask
Add		

Remote IP Subnet	Remote Subnet Mask	
172.26.1.90	255.255.255.255	Delete

Lastly, make sure VPN Interface Security Zone Public and Private are both enabled to permit VPN traffic. Click Apply and then click SAVE at the top of the screen to save your running config to memory.

Step 5 of 5: Select the Security Zone for Local Traffic for "EtherSpeak"

The VPN Interface Security Zone allows traffic from the remote end of the VPN Peer on to the VPN tunnel, and eventually through to your local peer(s). Unchecking this box prevents any VPN traffic on this peer from reaching this Netvanta. Additionally, traffic must match an enabled Outbound Security Zone to pass from the local side of the VPN peer to the remote.

VPN Interface Security Zone	Allow Incoming VPN Traffic
Public	<input checked="" type="checkbox"/>

Local Traffic Security Zones	Allow Outgoing VPN Traffic
Private	<input checked="" type="checkbox"/>

Cancel Apply

For the security zones, you have to define which traffic is permitted to speak over the VPN. To get to the settings for security zones, got to Firewall / Security Zones and click "Public". Then click "Allow List SIP" to see the access control list in the NetVanta GUI.

Netvanta 6310

Save Log

- System
- Voice
- Data
 - Router / Bridge
 - Default Gateway
 - Routing
 - Route Table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Spanning Tree
 - Firewall
 - Firewall Wizard
 - General Firewall
 - Security Zones
 - Network Monitor
 - Wizard
 - Probes / Tracks
 - Probe Responder
 - URL Filtering
 - URL Filters
 - Top Websites
 - Wireless

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
loop 1	<none>	<none>
eth 0/1	Private	Private
eth 0/2	Public	Public

Reset Assign

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	
Private	0	Rename
Public	5	Rename
<Click to add a Security Zone>	N/A	Rename

Netvanta 6310

Save Logout

- System
- Voice
- Data
 - Router / Bridge
 - Default Gateway
 - Routing
 - Route Table
 - IP Interfaces
 - Loopback Interfaces
 - GRE Tunnels
 - QoS Wizard
 - QoS Maps
 - Bridging
 - UDP Relay
 - Spanning Tree
 - Firewall
 - Firewall Wizard
 - General Firewall
 - Security Zones

Security Zones > Security Zone 'Public'

Configure Policies for Security Zone 'Public'

New policies can be added to Security Zone 'Public' 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 'Public'

Add Policy to Zone 'Public'

Modify/Delete Policies in Security Zone 'Public'

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

Priority	Description	Action	
1	EtherSpeak	VPN Selector	
2	Allow list ADMIN ACCESS	Advanced	Delete
3	Allow list sip	Advanced	Delete

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

Make sure you permit access to the following:

- EtherSpeak Public VPN IP
- EtherSpeak's Session Border Controller public IP address
- EtherSpeak's Session Border Controller private IP address

This information will be supplied by EtherSpeak with your order confirmation.

Add / Modify / Delete Policy Traffic Selectors

Configure one or more traffic selectors that define the data sessions this policy will Allow.

Add New Traffic Selector

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports	
▲ ▼	Permit	any	205.129.10.90/32	any	<input type="button" value="Delete"/>
▲ ▼	Permit	any	4.28.51.70/32	any	<input type="button" value="Delete"/>
▲ ▼	Permit	any	172.26.200.13/32	any	<input type="button" value="Delete"/>
▲ ▼	Permit	any	172.26.1.90/32	any	<input type="button" value="Delete"/>

With this step completed, please make sure you click “SAVE” on the top of the NetVanta screen and you should have a working config. EtherSpeak engineers will be available to assist with this process and with your configuration.

However, for a detailed explanation of how to configure the units along with frequently asked questions, please see configuration guides online at www.adtran.com or in the included “ADTRAN OS System Documentation” CD.

Adtran Troubleshooting

ADTRAN Technical Support is available toll-free for the life of the product during business hours. To speak with an ADTRAN Technical Support Specialist or Network Engineer, contact ADTRAN support at the following number or via the support Web site listed below:

Post-Sales Technical Support

888-423-8726

support@adtran.com

www.adtran.com/support

Registering your ADTRAN product entitles you to streamlined access to ADTRAN technical phone support and online knowledge base. You also receive free firmware updates, free access to pre-sales design assistance, trial access to the n-Command suite of network productivity tools for remote configuration and firmware management, as well as e-mail notification of product and firmware updates. For specific warranty details on an ADTRAN product, please visit www.adtran.com/warranty.

Pre-Sales Technical Support

800-615-1176

application.engineer@adtran.com

www.adtran.com/support

Installation and Maintenance Services

888-874-2237

aces@adtran.com

www.adtran.com/support

Training

800-615-1176



Document and Software Copyrights

Copyright © 2011 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

