Application Note

ShoreTel
Brilliantly simple™

ST AppNote 10352 (AN 10352)

October, 2011

ShoreTel VPN Concentrator and VPN Phone Deployment and Configuration Guide

Description: This application note provides detailed information on the network requirements and configuration settings for the proper deployment of the ShoreTel VPN Concentrator and its associated VPN phones.

Environment: ShoreTel IP-PBX: Versions 8 – 12
ShoreTel VPN Concentrator 4500/5300: Firmware version 8.7.2 and above
ShoreTel Gb IP Phones: IP 230g, IP 560g, IP 565g and IP 655

Overview

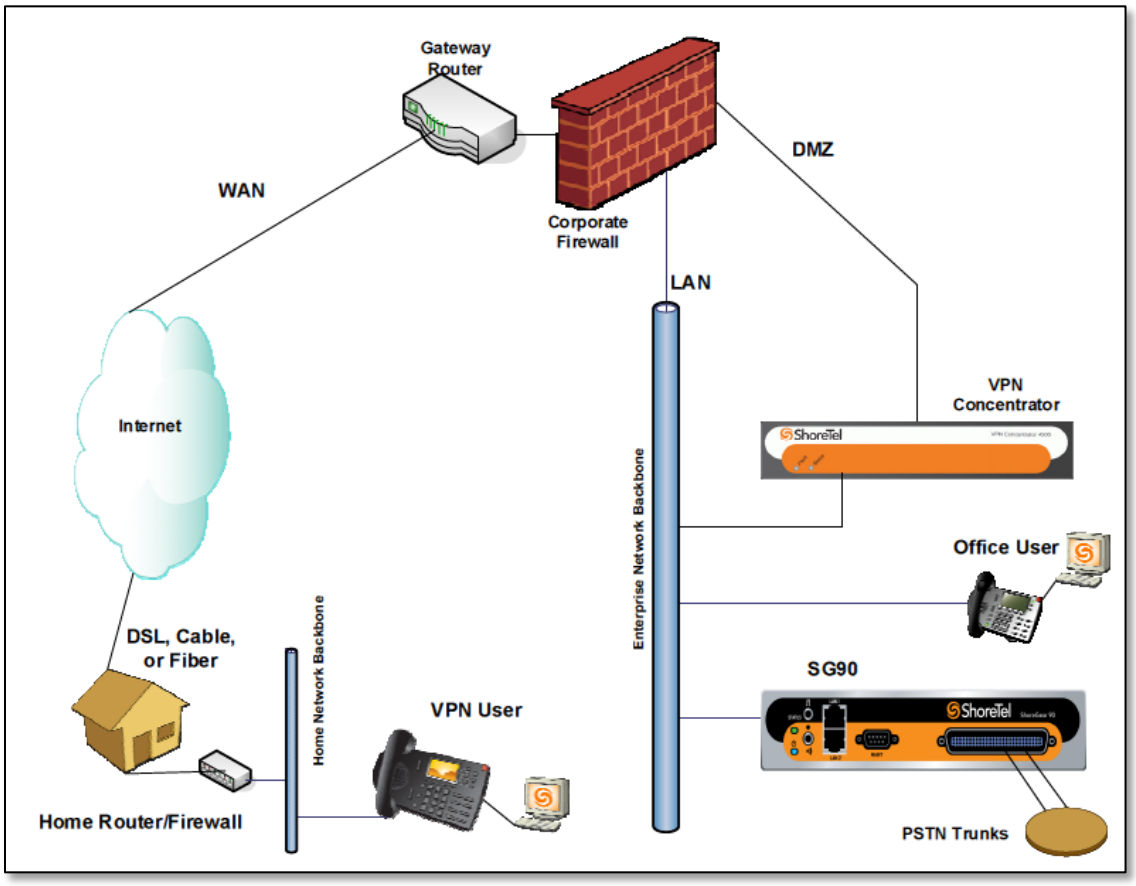
As more businesses are looking for ways to cut costs, one trend is to move workers out of leased office space and into the Small Office/Home Office (SOHO) environment. This trend is assisted by technologies such as virtual private networking (VPN) and Unified Communications (UC).

Use of a ShoreTel VPN phone permits a person working in a SOHO environment to take advantage of a physical phone at their remote office location. The phone is truly an extension on the corporate ShoreTel system and grants all of the capabilities of the system to the remote user including features like transfer, conference, directory and UC functions such as voicemail and presence. Once properly setup, the VPN phone becomes an integral part of the home office environment.

Contents

Overview 1
Contents 2
Architecture Overview 3
Internet Voice Quality Considerations 4
Configuration Steps 5
HQ Network Topology and IP addressing 5
First-time setup of the VPN Concentrator 6
Configuration of the VPN Concentrator 8
Stunnel IP Address Pool 9
Stunnel Configuration 10
Remote Site Topology 11
Configure the VPN Phone 11
Emergency (911) Calls 13
Testing VoIP Call Quality 14
Conclusion 17
Additional Resources 17

Architecture Overview



ShoreTel VPN Phone connected via the Internet through the Corporate Firewall to the ShoreTel VPN Concentrator

Internet Voice Quality Considerations

The Internet possesses several challenges that, if left unaddressed, can severely interfere with voice quality.

Bandwidth, Delay and Congestion

ShoreTel, as with any IP Telephony solution, uses a stream of IP packets (a Real-Time Protocol, or RTP, media stream) to carry voice between two different endpoints. An IP-based stream of voice packets actually consumes a very small amount of bandwidth – about 30-40 kbps in each direction, depending on the codec being used.

Most broadband Internet connections are "rated" at speeds well above what is required to adequately transport IP voice packets. For example, a typical Executive Suite environment may use a full T1 connection to the Internet and is often rated at ~1.5Mbps both up and down. A typical consumer-grade Cable Modem Internet connection might be rated at 5Mbps down and 2Mbps up. Fiber-to-the-Home connections (FTTH) are often rated at much higher speeds ranging from 5Mbps down/2Mbps up to 150Mbps down/35Mbps up.

Since voice packets only require 30-40 Kbps of bandwidth and typical Internet connections are commonly well over 1Mbps, voice problems are almost never about bandwidth; they are almost always about *delay* and *packet loss*.

> Voice problems are almost never about bandwidth; they are almost always about delay and packet loss.

Delay and packet loss are most commonly caused by congestion. Congestion occurs when more packets arrive at a device's inbound interface than can be successfully transmitted outbound in a timely fashion. Packet loss and delay are the leading causes of poor voice quality in any IP telephony system. In order to guarantee excellent quality voice between two locations you need to be able to guarantee that packet loss and delay will be kept to a minimum. This is most commonly done by implementing prioritization mechanisms on each device that could potentially be a point of congestion. Private devices and WAN connections allow for such administrative Quality of Service (QoS) settings. Public devices and connections such as Internet-based VPNs do not.

There are many effective methods for identifying and prioritizing voice packets as detailed in the ShoreTel Application Note "AN10325 - Best Practice Recommendations for VLANs and QoS with ShoreTel." The key is that the network device where congestion is occurring must be able to be programmed to identify and prioritize the voice packets for transmission ahead of other packets. In order to do this you need some degree of administrative control over those devices.

The simplest WAN networking environment might be in the form of a private, point-to-point leased line on which you connect routers that you own and administrate. You can implement any type of prioritization you choose and can guarantee perfect quality voice for every call no matter what other data is being transmitted. The most difficult case might be voice being transmitted from a home-based user to a corporate PBX over an oversubscribed, consumer-grade, broadband Internet connection with no QoS or other Service Level Agreements (SLAs) from their ISP.

Configuration Steps

The remainder of this document will prompt you through the following steps to help guide you in the proper setup and configuration of the ShoreTel VPN Concentrator.

1. Determine the best network topology at the Host (Corporate) site
2. Plan an IP address scheme to be utilized for the VPN Concentrator
3. Install and configure the VPN Concentrator
4. Program the VPN phone user's extension and privileges in the ShoreTel PBX system
5. Determine the best network topology at the Remote (Home/SOHO) site
6. Program the remote site's router to pass VPN traffic and provide traffic prioritization (if available)
7. Configure the VPN phone
8. Test the installation and VoIP call quality

HQ Network Topology and IP addressing

To secure, restrict or inhibit pass-through traffic to the VPN Concentrator, it must be deployed behind an enterprise firewall. Connect the WAN port of the VPN Concentrator to the DMZ network (or port) of the firewall. The Concentrator's WAN port should be assigned a private IP address (RFC 1918), or an appropriate IP address that can be used within the DMZ subnet.

Note: The VPN Concentrator does not act as a firewall. It should never be placed directly on the Internet. It should always be placed behind the corporate firewall.

See the Architecture Overview diagram above.

Connect the LAN port of the VPN Concentrator to the internal LAN network using an IP address from the LAN's IP subnet. A valid pool of IP addresses from the corporate LAN's internal (private) IP subnet will be assigned to and used by the VPN Concentrator to assign IP addresses to the external VPN phones via a virtual PPP connection over the SSL VPN for each phone.

An IP address pool on LAN-based IP addresses has to be preconfigured on the VPN Concentrator by the administrator so that a valid IP address can be assigned to each externally-located VPN phone connected to the VPN Concentrator.

Once positioned within the corporate firewall's DMZ and configured with a DMZ-based IP address (see below) you will need to create a port-forwarding rule on the corporate firewall. Select a valid public (routable) IP address that is routed to the external (public) interface of the firewall and create a port-forwarding rule to map any inbound traffic to that public IP on port 443 to be NATted to the IP address assigned to the ShoreTel VPN Concentrators WAN interface IP on port 443.

The port forwarding rule should look similar to the following:

External				NATted to DMZ	
From		To		To	
External IP	Any	Firewall IP	Public IP assigned to Firewall external interface	DMZ IP	IP Address of VPN Concentrator's WAN Interface on DMZ
		Port	443	Port	443

First-time setup of the VPN Concentrator

Note: Please refer to the Initial Configuration section of the ShoreTel VPN Concentrator 4500/5300 Installation and Configuration Guide for additional detail.

You configure the ShoreTel VPN Concentrator 4500 or 5300 using a web browser such as Internet Explorer or Firefox.

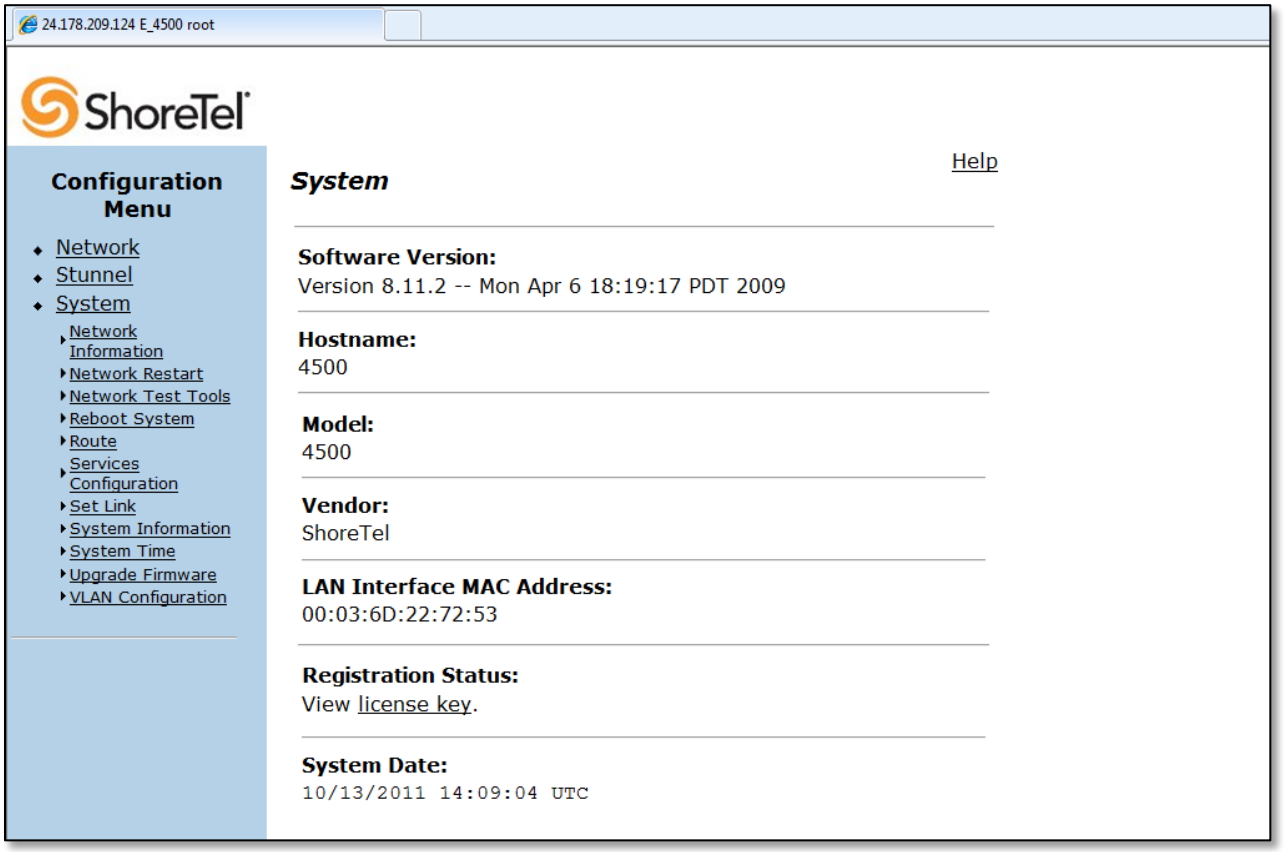
The 4500/5300 is shipped with the pre-configured IP address of 192.168.1.1 assigned to the LAN port.

To connect to the 4500/5300, follow these steps:

1. Assign a static IP address of 192.168.1.2 using a subnet mask of 255.255.255.0 to the Ethernet interface of a computer that is connected to the LAN port of the concentrator
2. Launch a web browser on the PC and enter the following URL: "http://192.168.1.1"
3. Press Return. The following login window should appear:

4. Enter the username "root" and the password "default" to log into the system

5. The "System" configuration page should appear



6. Select Network from the left-hand "Configuration Menu"
7. Perform the following steps in the "LAN Interface Settings" section:
    a. Set the "IP Address" to an IP address that can be reached from the corporate LAN network
    b. Set the proper "Subnet Mask"
8. Perform the following steps in the "WAN Interface Settings" section:
    a. Choose "Static IP Address"
    b. Set the "IP Address" to an IP address that is within the subnet of your firewall's DMZ.
        Note: The IP address can be a private IP address if desired
    c. Set the proper "Subnet Mask"
9. Perform the following steps in the "Network Settings" section:
    a. Set the "Default Gateway" to the upstream firewall's IP address on the DMZ
    b. Set the "Primary DNS Server" and "Secondary DNS Server" to the primary and secondary DNS servers, respectively
10. Click the "Submit" button to apply the above changes
11. Remove the Ethernet cable connecting the computer's Ethernet interface to the VPN Concentrator. Connect the LAN interface of the Concentrator to an Ethernet switch port on the internal Corporate LAN network

12. Re-IP address your PC to an appropriate IP address on the corporate LAN
13. Launch a web browser on any computer on the LAN network and enter the new LAN IP address of the 4500/5300. Press Return and log into the system as explained above
14. Start general configuring of the system

Configuration of the VPN Concentrator

The network deployment options of the ShoreTel VPN concentrator have several non-changeable requirements:

- The ShoreTel VPN Concentrator does NOT have a built-in firewall.
- Therefore it MUST be deployed behind, and protected by, your corporate firewall, preferably in a DMZ.
- The ShoreTel VPN Concentrator is REQUIRED to have each interface (internal & external) on a different IP subnet.
- Therefore, you CANNOT configure both interfaces to be connected to the internal LAN's IP subnet.
- When behind a corporate firewall, deployment in a DMZ is a requirement.

The following three authentication modes are supported on the VPN Concentrator:

- User name and password validation – The SSL VPN client on the remote phone is expected to provide a username and password to be matched against either of the following databases:
  - Local database (default) – A list of valid usernames and their associated passwords configured for the authentication in the local database on the VPN Concentrator itself, set by the administrator.
  - LDAP server database (optional) – This option requires an external LDAP server, such as Microsoft Active Directory, containing the username and password information for authentication. LDAP needs to be enabled in the VPN Concentrator before this database can be used instead of the local database.
- MAC Address Whitelist Validation (optional) – When enabled, a local database of MAC addresses is used to validate the MAC address of a remote VPN phone. If the MAC address of a remote VPN phone is not found in this database, the SSL VPN connection request is rejected.
- MAC Address Blacklist Rejection (optional) – When enabled, a local database of MAC addresses is used to identify remote phones that should be *denied* access to the network. If the MAC address of a remote phone is found in this database, then the SSL VPN connection request is rejected. This option is useful to 'disable' remote VPN phones for users, such as contractors, who are no longer employed by the company.

Stunnel IP Address Pool

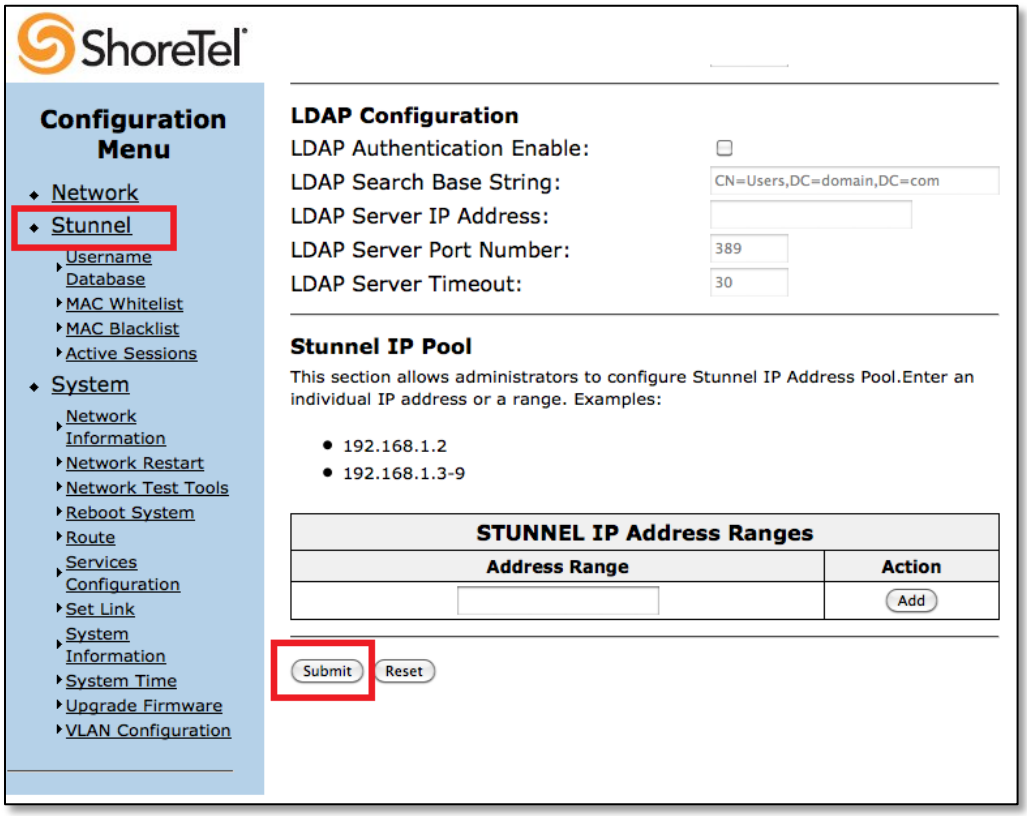
The Stunnel IP address pool specifies the specific IP addresses to be assigned to each external SSL VPN phone. The permissible format is to specify a valid IP address, or a range of IP addresses. For example: "10.10.10.2", or "10.10.10.2 - 100".

Overlapping IP Address ranges are not supported.

The IP address ranges configured in the Stunnel IP address pool must not be used by any other device. Be sure that the IP address ranges added to the Stunnel IP address pool do not include any IP address used by any other device on the LAN, including the VPN Concentrator itself.

It is important to remember that every incoming VPN phone session requires a unique IP Address to be assigned from the Stunnel IP address pool. If the number of addresses in the pool is not adequate, it imposes a limitation on the max simultaneous Stunnel connections, irrespective of the configured "Max Clients" parameter value. By default, this IP address pool list is empty.

Newly added values in the Stunnel IP pool will not become effective until after the next restart of the Stunnel service on the VPN Concentrator. To restart the Stunnel service, choose the "Stunnel" submenu from the left-hand "Configuration Menu." *Click "submit" on this page to restart network services and the Stunnel service.*



Note: *Restarting the Stunnel service will terminate all active SSL VPN sessions. Perform this during a designated maintenance window.*

Important: The IP addresses in the Stunnel IP address pool must be part of the internal LAN subnet, and must not overlap with the pool used by any DHCP server(s) on the same internal LAN subnet.

All IP addresses configured in the VPN Concentrator's address pool should be removed from any DHCP server(s) scopes on the internal LAN.

Stunnel Configuration

Select the "Stunnel" submenu from the left-hand "Configuration Menu." Enter and edit the following parameters:

1. Stunnel Enable: Check this box to enable Stunnel on the ShoreTel VPN Concentrator
2. Stunnel Server IP Address: This must be same IP address as the VPN Concentrator's LAN interface.
3. Stunnel Server Port Number: Keep the default value of "443"
4. Enable Stunnel Server Timeout: Enable this option if you want to enable Stunnel session timeout. This will cause IP phones to be disconnected and reconnected from Stunnel session after a definable period of time. Network security policies and security best-practices may require a VPN session timeout and re-authentication process to avoid network attacks. Check with the network administrator during deployment of the VPN Concentrator to determine if this setting should be enabled.
5. Stunnel Server Tunnel Timeout: If enabled in accordance with 4 (above), enter the desired Stunnel timeout value. The unit is in seconds.
6. Enable TCP No Delay: Leave this option enabled. When enabled (checked), the Stunnel server will send packets to remote clients without any delay, rather than combining packets to save overhead. This is important for voice traffic since it is very sensitive to delay. This parameter is enabled by default.
7. MAC Whitelist Validation: Select this option only if you want to enable Whitelist checking.

   Note: Only phone MAC addresses listed on the Whitelist will be allowed to establish Stunnel sessions. Other VPN phones will be blocked.
8. MAC Blacklist Validation: Select this option only if you want to enable Blacklist checking. All the blacklisted users' MAC addresses in the Blacklist table will be blocked.

   Note: The Blacklist supersedes the Whitelist. If a phone's MAC is defined in the both the Whitelist and the Blacklist tables the phone will be blocked.
9. Max Clients: This value corresponds to your Stunnel Session user license. To check your license, click "View license key" under Registration Status on the "System" page.
10. Stunnel IP Pool: In the last section on the Stunnel page, you will see the Stunnel IP pool where you need to define the Stunnel IP pool range. This range corresponds to the

maximum number of clients. For example, if Max Client=20, the IP Pool range must have at least 20 IP addresses.

To define the range, use the following format: 10.23.106.20-39 and click ADD.

Note: The Stunnel IP Pool range must include valid and unique IP addresses from the internal LAN. Verify that the Stunnel Server IP address is not in this range and that none of the IP addresses are in use or configured to be assigned by a DHCP server.

Remote Site Topology

Review the remote location's network to determine what other devices and associated traffic flows may exist on the SOHO network. As cited earlier, the most common problems are packet loss and delay due to congestion.

It is important to understand whether the SOHO-based router provides a business-class level of capabilities. If a traffic flow prioritization setting is available on the SOHO router, set it to specify the packets from the ShoreTel VPN phone to be given priority over other, non-real-time traffic.

Other methods to consider are cited in the Testing VoIP Call Quality section of this document.

Configure the VPN Phone

Follow this procedure to configure a VPN-enabled phone:

1. Connect the VPN-enabled phone to an Ethernet network that has access to the Internet. The phone boots up.

   Note: The Phone must be powered by a Power over Ethernet (PoE, 802.3af) port or by a local power injector (power brick).

2. At the password prompt enter the IP Phone password provided by your ShoreTel or network administrator. The default password is 1234 #.

3. The phone is now ready for you to enter the following configuration parameters:

VALUE / MESSAGE	OPTIONS	COMMENT
CLEAR ALL VALUES	YES/NO	Press '#' for Yes and '*' for No For first time configuration, select 'Yes'
DHCP	ON/OFF	ON
IP ADDRESS	–	This information will be automatically obtained via DHCP
MASK	–	This information will be automatically obtained via DHCP

GATEWAY	–	This information will be automatically obtained via DHCP
FTP	IP Address	Enter the internal (private) IP Address of the HQ Server
MGC	–	Leave blank. It will obtain this parameter automatically
SNTP	IP Address	Enter the NTP Server's IP address
802.1Q TAGGING	ON/OFF	OFF
VLAN ID	–	N/A
DNS	–	Leave at the default of 0.0.0.0
VPN GATEWAY	–	Enter the public IP address used on the corporate firewall that is mapped to the VPN Concentrator's DMZ (WAN) interface
VPN PORT		Use the default of "443" (unless changed under the Stunnel page in ShoreTel VPN Concentrator GUI)
VPN	ON/OFF	ON
VPN USER PROMPT	ON/OFF	ON – The user will be prompted for their VPN Phone User ID
VPN PASSWORD PROMPT	ON/OFF	ON – The user will be prompted for their VPN phone password
ETHERNET 1	AUTO/FD/HD	ShoreTel recommends leaving this parameter at a default setting of "Auto," unless your network environment requires modification.
ETHERNET 2	AUTO/FD/HD	ShoreTel recommends leaving this parameter at a default setting of "Auto," unless your network environment requires modification.
COUNTRY	–	Leave at the default value
LANGUAGE	–	Leave at the default value
SAVE CHANGES	YES/NO	Yes

After saving this configuration, the phone should reboot and the VPN Authentication Prompt should appear. Input the appropriate user information and your phone will successfully login.

Gigabit Phones

No special build or firmware of the ShoreTel system is needed in order to support VPN-based IP Phones. All versions of ShoreTel 8.1 and higher have native VPN phone support. All that is required is the ShoreTel VPN Concentrator and Concentrator licenses.

Any ShoreTel IP phone with a built-in Gigabit (Gb)-speed Ethernet switch will automatically be upgraded with the firmware to support the VPN features when attached to a ShoreTel 8.1 or higher PBX. Only ShoreTel IP phones with internal Ethernet switches supporting Gb speeds have enough extra processing power to support the encryption used by the VPN process.

Therefore, only those phones with Gb ports will contain the necessary firmware and configuration settings for supporting VPN use.

The current line of ShoreTel IP Phone that support GB-speed, and therefore VPN use, are:

- IP 230g, IP 560g, IP 565g and IP 655

Emergency (911) Calls

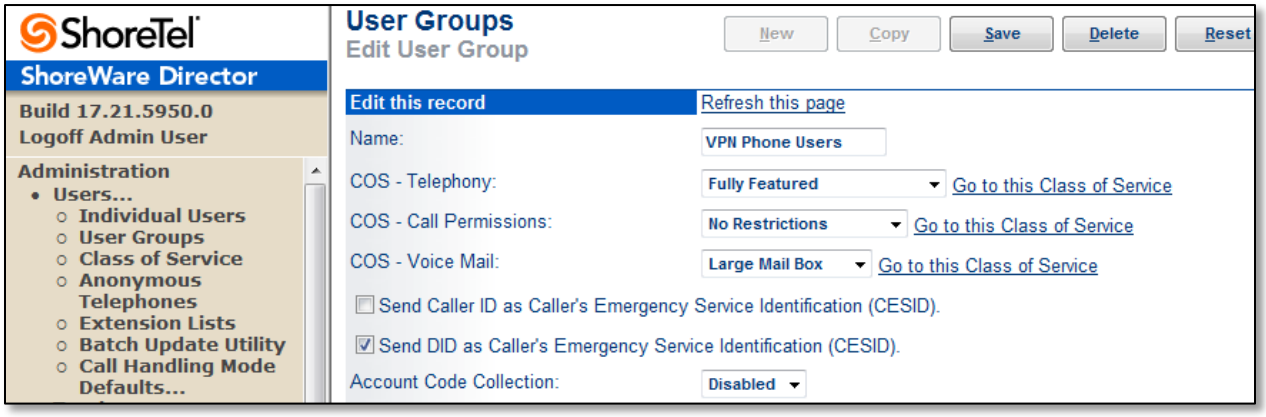
If ShoreTel VPN phones will be deployed at remote locations, emergency calls placed from these phones will be routed to the Public Safety Answering Point (PSAP) servicing the site that hosts the ShoreGear voice appliances that the VPN phones are connecting to. This is commonly the same site that the VPN concentrator is located at.

Note: For complete details on proper emergency settings please see the ShoreTel documentation.

For emergency (e.g. 911) calls, there are settings within the user's User Group which control what number gets sent to the PSAP as the "Caller's Emergency Service ID", or CESID, number.

When the VPN phone user places an emergency call:

- If "Send Caller ID as CESID" is checked, and a value has been entered in the user's Caller ID field, that information will be sent as the CESID on the outbound call to the PSAP
- Otherwise, if "Send DID as CESID" is checked, and a value has been entered in the user's DID field, that information will be sent as the CESID on the outbound call to the PSAP



- Otherwise, if a CESID has been set for the IP Phone Address Map used by the VPN IP phones, that information will be sent as the CESID on the outbound call to the PSAP
- Otherwise, if a CESID has been set for the site the phone is assigned to, that information will be sent as the CESID on the outbound call to the PSAP

It is strongly recommended that, for VPN phone users who are located at a fixed location (such as a home-based worker), you work with your local trunk provider and PSAP to enter the user's actual location & address for each user's DID in the Public Safety Automatic Location Identification (PS-ALI) database that is used for display on the screens of dispatchers at the PSAP.

By doing so, any emergency call placed by a VPN phone user will display the actual address of the caller on the screen of the dispatcher that fields the call at the PSAP.

Testing VoIP Call Quality

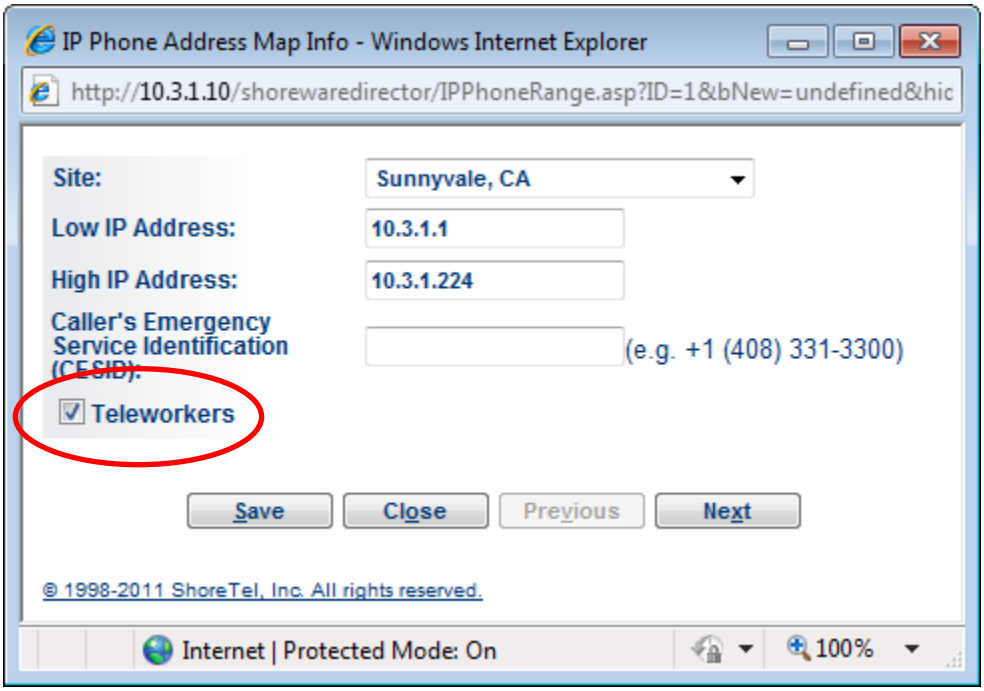
Be sure that test calls are performed using several scenarios. If the remote user also uses a PC during their workday, be sure to make test calls while using the PC at the same time. Evaluate the call quality during various times and during various data traffic loads.

In the event that call quality is not up to the expected level, consider the suggestions below.

1) Codec Selection

Configure your IP Phone Address Map in the ShoreTel PBX to use the "Teleworkers" checkbox.

Create an IP Phone address map that matches the Stunnel IP Pool Address range, assigned to the same site that hosts the VPN Concentrator. Check the Teleworker box to instruct all remote VPN phones to use the "Inter-site Codec List" thereby using a smaller, tighter codec.



2) The amount of traffic that is being sent by your computer when connected behind an IP/VPN phone and the ability of the IP Phone to prioritize outbound traffic

Each ShoreTel IP Phone has a built-in, two-port Ethernet switch. Connecting your computer's Network Interface Card (NIC) into the IP Phone's Ethernet switch means that all traffic sent to and from your PC will pass through the IP phone. Each ShoreTel IP phone has a built-in QoS/prioritization mechanism so that all voice packets that are being sent out from the phone will always be queued ahead of any data packets that are being received from the PC for re-

transmission. This built-in QoS means that large amounts of outbound traffic from the PC will not affect the ability of the phone to transmit its voice packets to the LAN in a timely fashion.

Consider placing your computer (or all computers) behind the IP phone. Doing so will ensure that your outbound voice traffic will be prioritized ahead of your outbound data traffic.

3) The amount of traffic being sent by other PCs on your cabled LAN

The amount of traffic being sent and received by other devices on your Ethernet network will affect the total amount of traffic that is being sent to and from your shared Internet connection. Some "consumer grade" Ethernet switches are not able to re-transmit packets fast enough to keep up with heavy network usage.

Consider using an Ethernet switch that is capable of "near line-rate" packet forwarding and is as close to "non-blocking" as possible to reduce the possibility of added delay or packet loss on a heavily trafficked LAN.

4) The amount of traffic being sent & received by Wi-Fi devices.

Many consumer-grade, multi-function devices perform the task of router, wireless access point (WAP), firewall, and Ethernet switch – all in one, single device. These devices must split their processing power between each of these multiple functions. Be careful not to use a device that can be overloaded by requests to do too many tasks as once.

Consider using a business-grade, multi-function device with more processing power. Or consider splitting up the functions so that you have a dedicated device for each purpose: wireless access point, Ethernet switch, router, and dedicated firewall.

5) The ability of the Ethernet switch/router to identify and prioritize traffic

Inbound traffic from the Internet, through the LAN to the IP Phone, passes through the Ethernet switch on your LAN. The Ethernet switch/router/firewall device needs to be able to receive large amounts of inbound traffic from the Internet and successfully re-transmit 100% of those packets towards the phone and connected PC without adding any delay or packet loss.

Many consumer-grade firewall devices can identify different types of traffic in order to allow or disallow the traffic but do not have any mechanism to prioritize one type of traffic over another. Also, many firewall-oriented devices are built primarily to inspect and block traffic and may not be as capable, or as fast at forwarding, the allowed traffic. This can be especially true of consumer-grade firewalls.

Some newer firewalls allow you to specify a single port, IP address, or MAC address on the internal LAN to be considered "high priority." Sometimes this is called a "Game" port or "Game Device" and is intended to allow the prioritization of traffic from this "real-time" device over regular traffic. If your device has such a port, consider assigning the IP/MAC address of the VPN phone for this purpose.

Consider using a business-grade firewall that can inspect and forward traffic with minimal delay.

Consider using a business-grade firewall that has the ability to prioritize voice traffic over other types of traffic.

Consider using a business-grade firewall that has QoS tools to rate-shape and adjust transmission speeds of both inbound and outbound traffic.

6) The congestion and buffering capabilities of the Internet border device (e.g. cable or DSL modem)

Often you are limited in the choice of edge routers/modem devices when connecting to a broadband Internet connection. This device can be a congestion point between the high speed LAN (100Mb+) and the relatively slow speed WAN (1-15 Mb). Therefore, any delay or packet loss introduced by this device often needs to be compensated for via other mechanisms.

Consider upgrading your device to a newer, faster device that supports faster speeds, introduces less delay and has QoS features.

7) The Internet Service Provider's QoS, SLA, peering, and oversubscription characteristics

If your Internet Service Provider (ISP) is heavily oversubscribed then you will experience greater congestion. If your ISP is peered to other upstream ISPs in a fashion that routes your corporate/VPN/Voice traffic in a slower, more circuitous route, your packet latency will be longer. If your ISP does not offer any method of identifying and prioritizing your voice traffic then all your packets are at the mercy of their "best effort" queuing mechanisms.

Consider using an ISP that is as minimally oversubscribed at their aggregation points as possible.

Consider using an ISP whose Internet peering creates fewer "hops" to your corporate headquarters.

Consider using a "Tier 1" ISP that has better connection speeds, less oversubscription, less congestion and better peering than the "mom and pop" ISP (i.e. "you get what you pay for").

Consider using an ISP that offers some degree of Service Level Agreements (SLAs) for classifying and prioritizing traffic. Be wary of so-called "business-grade" broadband connection as these are commonly only the same consumer services with more bandwidth.

Remember: Bandwidth plays effectively no role in delivering high-quality voice.

Remember: There is no way to guarantee quality voice over the Internet. These recommendations can help improve connection quality but cannot guarantee voice quality over the Internet.

Conclusion

Successful VPN phone use depends upon a careful review of the deployment environment and business processes along with consideration of multiple network parameters.

A review of network policies and practices implemented within the enterprise is also highly advised. Prior to configuration of the VPN Concentrator, discussions must take place with respect to IP address schemes, corporate firewall settings, traffic prioritization, and link utilization. Remote environments should also be reviewed and proper expectations set with the VPN phone user community.

ShoreTel VPN phones and VPN Concentrators provide an option for those SOHO workers who desire a physical instrument at their remote location. Once setup and deployed, this solution makes it simple for remote workers to take advantage of the benefits and features of the ShoreTel IP phone system.

Additional Resources

- KB11826 – VPN Concentrator/Phone Configuration Guides
- AN10112 – Optimizing the ShoreTel VPN Phone Solution
- AN10119 – VPN Phone Solution: Configuration Examples
- ShoreTel VPN Concentrator 4500/5300 Installation & Configuration Guide

Special thanks to Resilient Intelligent Networks, Argyle, TX for their assistance in testing and documenting this Application Note.

Version	Date	Contributor	Content
1.0	October, 2011	D. Cristofano	Original App Note