IP Office Technical Tip

Tip no: **186**

Release Date: **August 14, 2007**

Region: **GLOBAL**

Configuring a VPN Remote IP Phone with an Adtran Netvanta 3305 VPN Router

The following document assumes that the user/installer is familiar with configuring both the IP Office and VPN device as well as setting manually configuring IP Hard-phones. This document is for reference purposes only when creating the VPN tunnels and does not provide any details on how to configure any other aspect of either device.

Test Systems Software Versions and Basic Phone Settings

IP Office Core Software	4.0.7
Adtran Netvanta 3305 Router Software	15.02.00.E
IP Phone Model	5610
IP Phone Firmware	2.3.252
IP Office IP Address	192.168.2.5
TFTP/File Server	192.168.2.10
IP Phone IP Address	DHCP
IP Phone CallSV	192.168.2.5
IP Phone CallSVPort	1719 [Default]
IP Phone Router	DHCP
IP Phone Mask	DHCP
IP Phone FileSv	192.168.2.10
IP Phone 802.1Q	Auto
IP Phone VLAN ID	0
Password used during testing	123456789
Remote ID (Group Name)	vpntrial10
User Name	vpn10
User Password	123456789

Notes

1. The IP Phones may require a Virtual IP Address to be configured in the VPN settings. Please take care in choosing a Virtual IP Range. Consider where the phone is most likely to be used and ensure that the Virtual IP Range selected will not conflict. For instance, many VPN IP Phones may be installed at user's homes. Typically a Home Router uses 192.168.0.x or 192.168.1.x as its internal network range therefore it is recommended that this is not used as a Virtual IP Address Range.

2. **IMPORTANT**: Many VPN Routers will not allow a direct media path to be established between two VPN Endpoints. It will be necessary to uncheck the Direct Media Path checkbox in the Extension Configuration in IP Office. Failure to do so will result in No Speech path when two VPN extensions try and establish a call.

3. Review the Sample 46vpnsetting.txt file for simplifying configuration settings on the IP Phones.

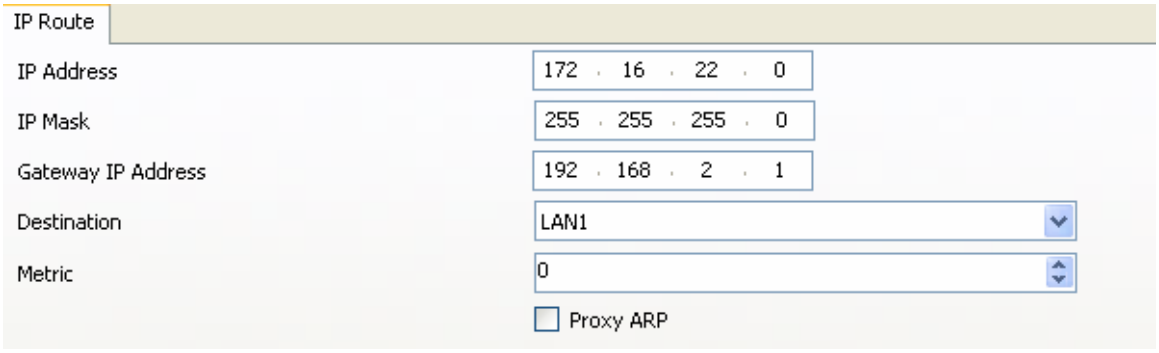
4. While the defaults for Encryption are set at 4500-4500 and these settings are preferred, there may be instances where (depending on what the Home router supports) the user may need to either disable this setting, or change to one of the other options.

5. If manually configuring a Virtual IP Address on the IP Hard-phone, ensure that accurate records are kept of IP Address allocations to avoid IP Address conflicts.

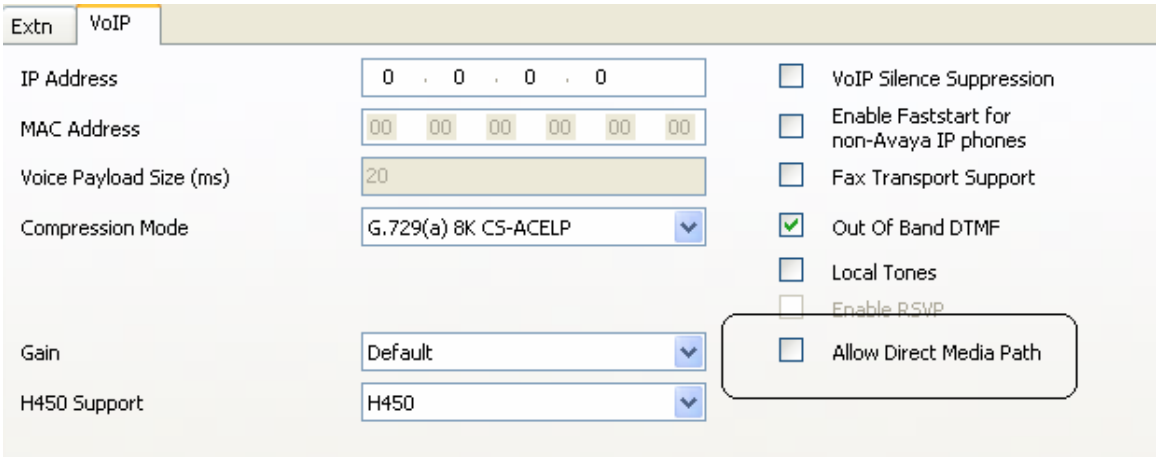
IP Office Configuration

Using IP Office Manager, Open the Configuration and Select IP Routes.

Add a New IP Route for the Virtual LAN Network to be used in the environment.

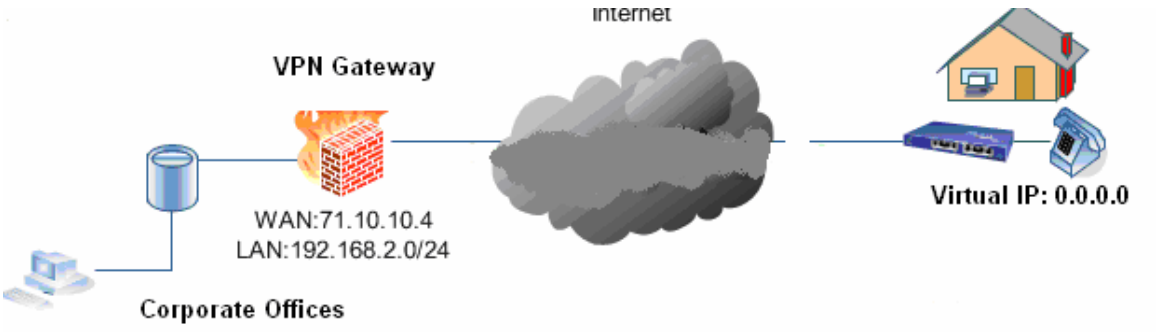


Modify the Extensions – VoIP Tab for those extensions that will be VPN Extensions, and uncheck the Direct Media Path Check Box.



Adtran Netvanta 3305 VPN Router VPN Configuration settings

Networking Scenario:



Important Requirements when using the Adtran Netvanta Router

The Following configuration settings / requirements must be configured when using an Adtran router

1. The VPN Remote phone Juniper with XAUTH profile must be used.
2. Each VPN Phone must use a unique XAUTH Username.
3. If more than one client will be connecting from the same NAT Address each device must use a different Remote ID. The Remote ID used for the phone(s) must be configured to Allow XAUTH.

[An example would be a remote user connecting VPN Software client installed on a PC, as well as a VPN IP Phone from a Home High Speed Internet connection.]

Adtran Netvant 3305 – IKE and VPN Policy Settings

To Allow XAUTH, it may be necessary to check the "AAA Mode" Checkbox on the Adtran Router. This setting is found on the Passwords page of the Adtran Management interface. By default this is not enabled.

By default the Adtran Netvanta does not have QoS enabled. Use the QoS Map Wizard and manually change parameters as needed or configure the QoS Map Manually.

QoS Map Setup	
Match Packets	DSCP (46)
Packet Marking	Disable
Priority Queue	Unlimited Bandwidth

To create usernames, select the Passwords Link in the Adtran Management interface

- TIP: Using the Serial Number of the IP Phone as the Username. Configure the 46vpnsetting.txt file and consider using the [SET NVVPNUSER

%SERIALNUM%] option. Assign a common password to all Users and use the [SET NVVPNPSWD] option.

- Note: Some phones' Serial Numbers may contain letters, while others will be all numbers. Letters must be entered in Capitals, not lower case or the Router will not accept the username and authentication will fail.

Username and Passwords	
Username	vpn10
Password	123456789

As noted above, in the event that there will be more than one VPN Device connected from the same remote network using NAT, a Remote ID must be created for each device **Tip**: Keeping the password the same, will allow for the password to be applied using the 46vpnsetting.txt script file. If only one Remote ID will be required, this may also be applied via the 46vpnsetting.txt file, however if more than one Remote ID is required, this value should not be configured in the script file and should be manually assigned on the phone.

Policy Configuration	
VPN Peer Configuration	
Name	Adtran
VPN Interface	Interface that will Terminate the VPN Tunnel
Peer Type	Mobile Peer
IKE Configuration	
XAUTH	Enabled
Respond Mode	Any
NAT Traversal	Allow V1 and Allow V2
Local ID	IP Address
	71.10.10.4
IPSEC Configuration	
PFS	Group2
Encryption / Hash	ESP:3 DES / SHA1
Encryption / Hash	No Additional Transforms
Lifetime	28800 seconds
IKE Attribute	
Encryption / Hash	3 DES
Hash	SHA
Authentication	Pre Shared Key
DH Group	2
Lifetime	28800 seconds

Remote Id's Allowed to Connect	
Remote ID Type	FQDN
Remote ID	vpntrial10
Mode Config	Enabled
Pre Shared Key	123456789
XAUTH	Enabled
NAT Traversal	Allow V1 / Allow V2
Remote Addressing	
IP Range	172.16.22.1 to 172.16.22.253
VPN Selector Entry	
Type	Permit
Protocol	Any
Source Network / Ports	192.168.2.0/24
Destination Network / Ports	172.16.22.0/24

VPN Remote Phone Settings

VPN Remote Phone Configuration	
VPN Profile	Juniper XAUTH with PSK
Server	71.10.10.4
User Name	vpn10
Password	123456789
Group Name	vpntrial10
Group PSK	123456789
VPN Start Mode	Boot
Password Type	Save in Flash
Encapsulation	4500-4500
IKE Parameters	
IKE ID Type	FQDN
Diffie Hellman Group	2
Encryption ALG	3DES
Authentication ALG	Sha1
IKE Xchg Mode	Aggressive
IKE Config Mode	Enabled
XAUTH	Enable
Cert Expiry Check	Disable
Cert DN Check	Disable
IPSEC Parameters	
Encryption ALG	3DES
Authentication ALG	Sha1
Diffie Hellman Group	2

Protected Nets	
Virtual IP	
Remote Net #1	192.168.2.0/24
Remote Net #2	
Remote Net #3	
Copy TOS	No
Connectivity Check	Always

Issued by:
Avaya SSD Tier 4 Support
Contact details:-

EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: IPOUST4ENG@Avaya.com

Internet: http://www.avaya.com