Avaya Solution and Interoperability Test Lab

An Avaya IP Telephone at a Home served by an Avaya IP Office over a Virtual Private Network Implemented between an Adtran NetVanta 3305 and 2054 - Issue 1.0

Abstract

These Application Notes describes a network configuration that supports a home-based worker's use of an Avaya 5600 series IP Telephone served by an Avaya IP Office IP406v2 at the main office. An Adtran NetVanta 2054 in the home establishes a Virtual Private Network tunnel with an Adtran NetVanta 3305 in the main office over a simulated internet to provide the secure connectivity.

The Avaya 5602SW IP Telephone in the home registers with the IP Office in the main office and provides the same feature operation as if located in the main office.

Since the Internet Service Providers generally do not provide guarantees for bandwidth, delay, jitter or loss, the quality of service to the user in a real world configuration cannot be guaranteed.

1. Introduction

Figure 1 shows the tested configuration. The Main Office Avaya IP Office IP406 provides business telephony service to both the main site and the home site. The Avaya 5602SW in the home registers to the IP Office over an IPSEC Virtual Private Network implemented between the Adtran NetVanta units.

Feature operation provided to the home user was similar to feature operation for any Avaya IP Telephone user. The quality of the voice connection cannot be guaranteed, since the Internet Service Providers typically do not guarantee the performance of the underlying packet service.

These Application Notes focus on the configuration needed to support the telephony features in a given environment. Some aspects of configuration, such as the firewall configuration for non-voice traffic, are simplified.

This configuration is a modification of a customer implementation with private IP addresses substituting for the public IP addresses used with the public internet.

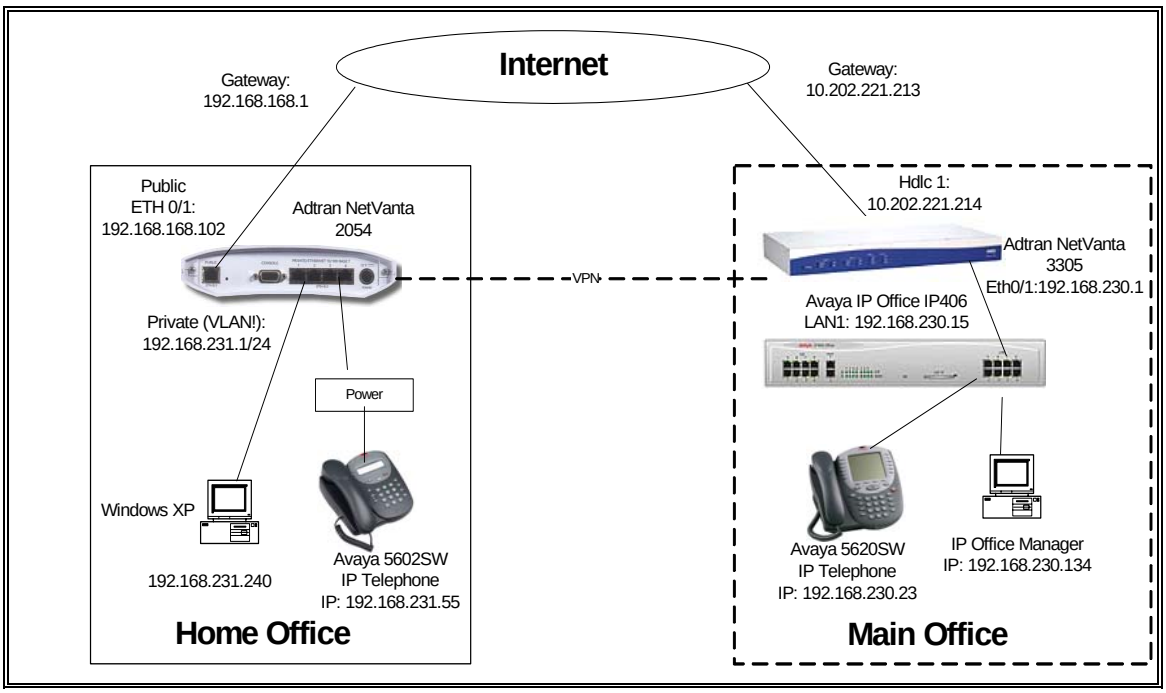


Figure 1 - Network Configuration Diagram

2. Equipment and Software Validated

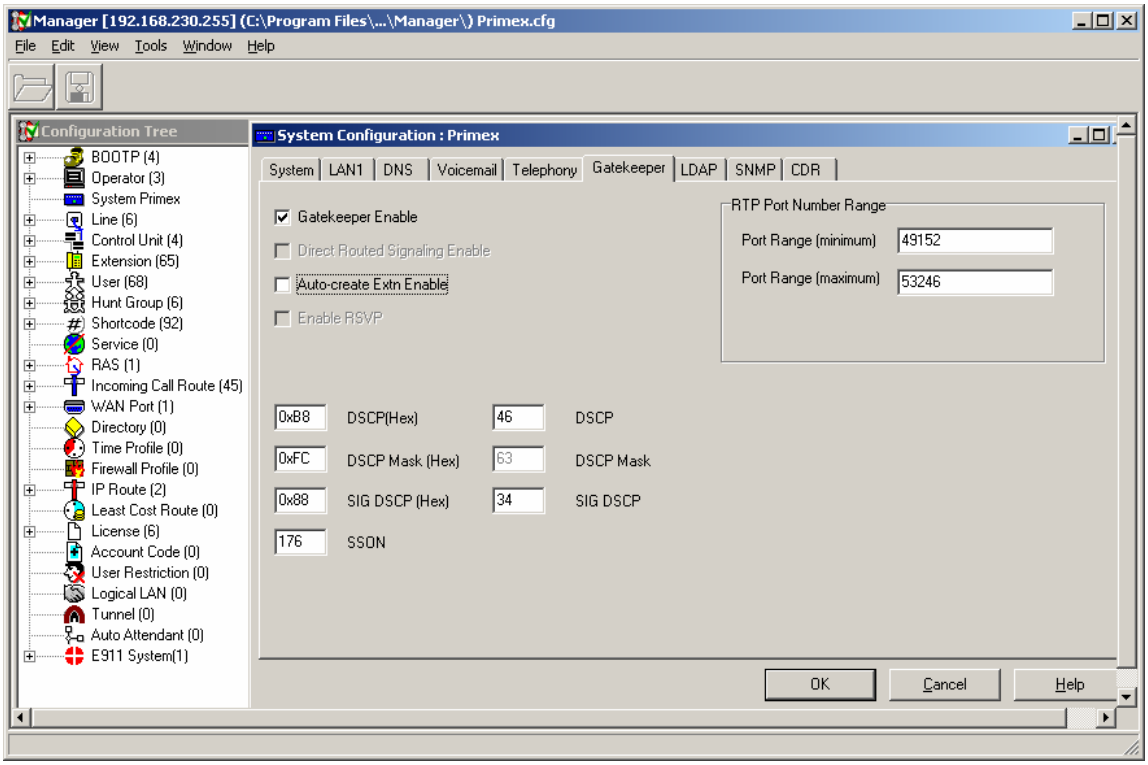
The following hardware and software versions were used for this configuration:

Equipment	Version
Avaya IP406	3.1 (56)
Avaya 5602 IP and 5620 IP Telephones	2.3
Adtran NetVanta 3305	11.02.00.E
Adtran NetVanta 2054	10.04.00.E

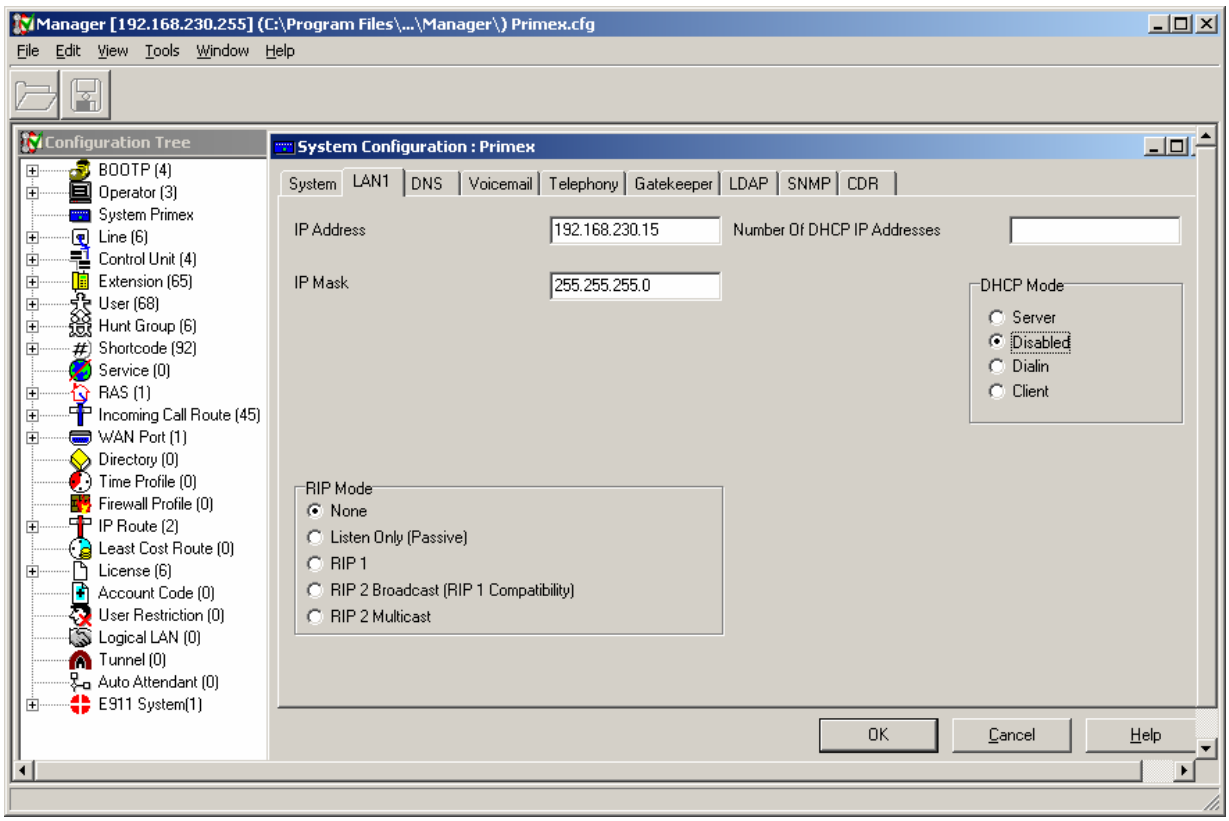
Table 1 - Equipment and Versions Validated

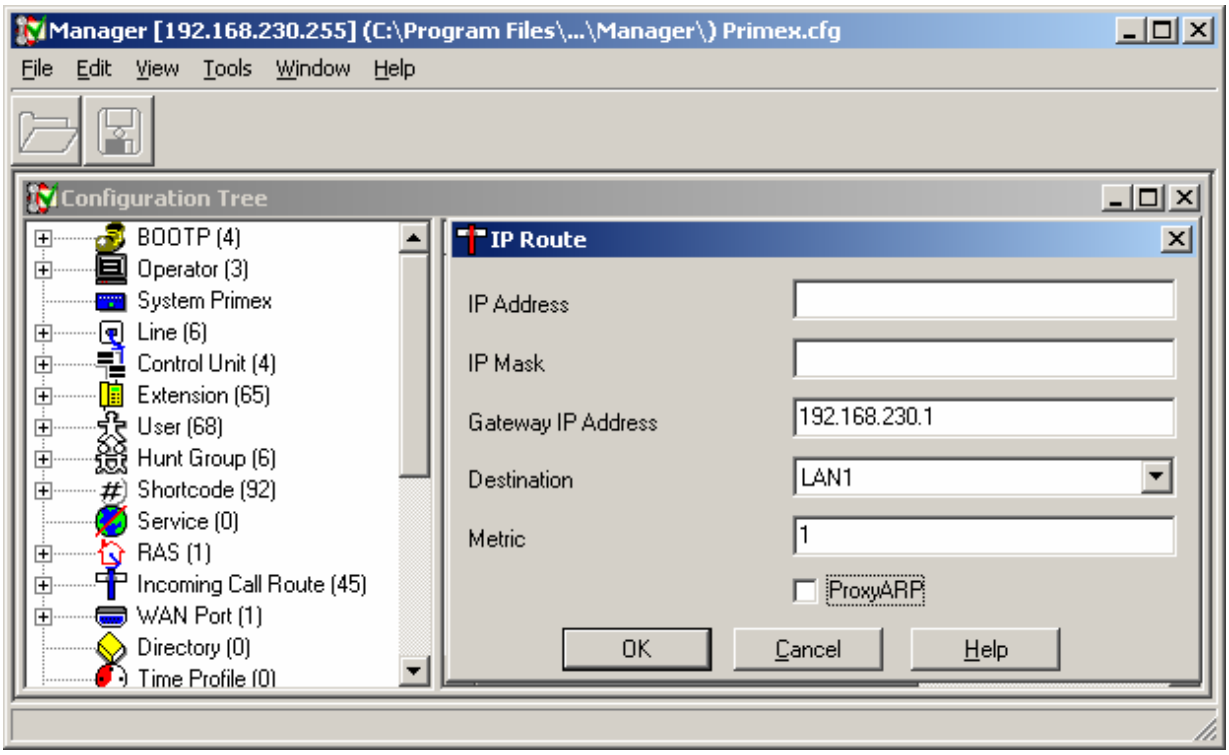
3. Configure Avaya IP Office IP 406v2 at the Main Site

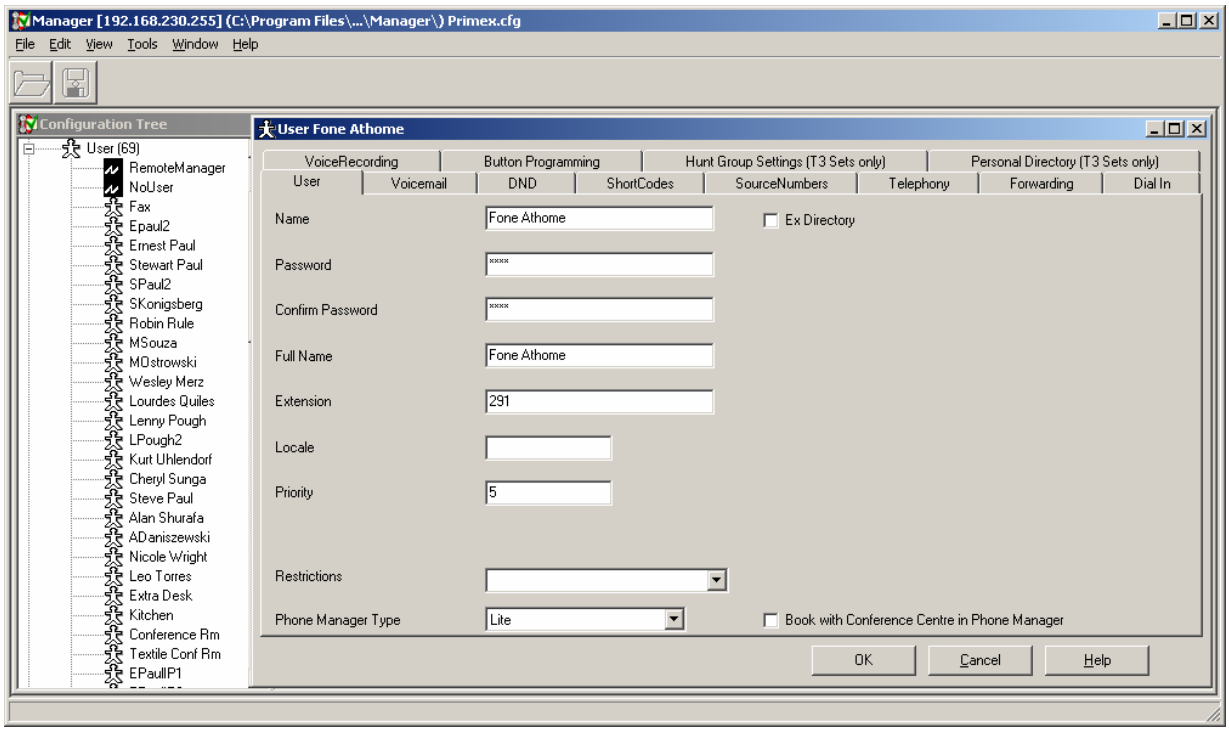
This section describes only those steps involving configuration relative to the service of the home telephone. It is assumed that the reader has run the IP Office Manager Application and logged in with the appropriate credentials.

Step	Description
1.	In the **Manager** window, double-click on **System** under the Configuration Tree. Click on the Gatekeeper tab and note the DiffServ Code Points (DSCP) value used for audio and signaling in the **DSCP** and the **SIG DSCP** fields and the **RTP Port Number Range**. This information may be needed in the configuration of the firewall access lists of sections 4 and 5 of this document. 

Step	Description
2.	Select the **System→LAN1** tab and set the **IP Address** and **IP Mask** to desired values for the local subnet. Set the **DHCP Mode** as desired. Click **OK**.



Step	Description
3.	*Add a default route*. In the **Manager** window, click on **IP Route** under the Configuration Tree. Right-click in the right pane and select **New** to add an **IP route**. Leave the **IP Address** and **IP Mask** fields blank to make this entry the default route. Enter the IP address of the Adtran NetVanta 3305 Ethernet 0/1 port in the **Gateway IP Address** field. Select LAN1 as the **Destination** interface to reach this gateway. Click **OK**. 

Step	Description
4.	*Add a User for the home IP Phone*. Select **User** from the Configuration tree, right click in the right pane and select **New**. Assign the User's **Name**, **Password** (and **Confirm Password**), **Full Name** and **Extension**. Other user configuration is not shown. Select **OK** and when prompted to create an Extension for this user, select **Yes**. 
5.	Select **File->Save** and then **OK** when prompted to save the changes.

4. Configure the Adtran NetVanta 3305 at the Main Site

The following is the annotated configuration of the Main Site Adtran NetVanta 3305. Annotations are boxed. Non-annotated entries are generally non-specific to this configuration. Otherwise, the "!" character indicates a comment or empty line.

```
!
!
hostname "Mainsite"
enable password password
!
clock timezone -5
!
ip subnet-zero
ip classless
ip routing
!
no auto-config
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
no service password-encryption
!
ip policy-timeout udp tftp 300
!
ip firewall
```

The h323 and SIP application layer gateway functionality was disabled.

```
no ip firewall alg h323
no ip firewall alg sip
!
!
!
!
!
```

The **ip crypto** command enables the VPN features.

```
ip crypto
!
```

crypto ike policy 100 accepts an Internet Key Exchange (IKE) protocol attempt from any IP address and responds with the "main" mode of protocol negotiation. Aggressive Mode was also tested in a similar configuration. The local-id address is the public IP address from the unit's interface to the Internet.
The acceptable IKE attribute set is defined to be triple DES, the MD5 hash for authentication, the use of a Pre-Shared Key (PSK, defined later in the configuration) and a lifetime of 86400 seconds.)

```
crypto ike policy 100
  no initiate
  respond main
  local-id address 10.202.221.214
  nat-traversal v1 disable
  peer any
```

```
  attribute 1
    encryption 3des
    hash md5
    authentication pre-share
    lifetime 86400
!
```

The **crypto ike** command defines the Pre-Shared Key for the IKE policy defined above ("simplekey") and associates the policy to "VPN 10" for which further attributes are defined in this configuration. The key "simplekey" must match the same setting in the "home" device.

```
crypto ike remote-id any preshared-key simplekey ike-policy 100 crypto map
VPN 10 no-mode-config no-xauth
!
```

The **crypto ipsec** command defines a transform set with the attributes of the IPSEC association for which the data will be passed in this VPN. The Encrypted Security Protocol of triple DES with the Message Digest 5 hash for authentication will be used.

```
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
  mode tunnel
!
```

The **crypto map VPN 10 ipsec-ike** construct ties together the ipsec transform set and the ike-policy defined above with the "selectors". Traffic matching the given address list will be encrypted into the tunnel. In this configuration, it will not initiate the tunnel as the tunnel policy is configured earlier as "no initiate". (Since the "home" device obtains its public address via dhcp, there is not a sure way to know ahead of time what address to establish a tunnel to.).

```
crypto map VPN 10 ipsec-ike
  match address VPN-10-vpn-selectors
  set transform-set esp-3des-esp-md5-hmac
  set security-association lifetime seconds 86400
  ike-policy 100
!
```

The **qos map VOICE** commands define the "VOICE" Quality of Service map, which is intended to give priority to the voice signaling and media in any contention for the outgoing bandwidth. The DiffServ CodePoint values must match the settings of the IP Office System Gatekeeper form.
The following lines define the "VOICE" QoS map, where the device will attempt to match each packet first against the criteria of "VOICE 10" and then against the match criteria of "VOICE 20". The Voice Media (DSCP 46) is thus given priority for up to 200 kb/s and the Voice signaling (DSCP 34) for up to 10 kb/s. The amount of bandwidth required is dependant on the number of simultaneous voice calls, the level of encryption used and the codec selection.

```
qos map VOICE 10
  match dscp 46
  priority 200
qos map VOICE 20
  match dscp 34
  priority 10
```

```
!
```

Interface Ethernet 0/1 is the default router for the IP Office at the main site. The "private" side access policy is defined later in the configuration.

```
interface eth 0/1
  description voice interface
  ip address  192.168.230.1  255.255.255.0
  access-policy private
  no shutdown
!
interface eth 0/2
  description data interface
  ip address  192.166.230.1  255.255.255.0
  no shutdown
!
!
!
interface t1 1/1
  shutdown
!
interface t1 1/2
  shutdown
!
```

Interface t1 2/1 defines a 24 channel (1.536 kb/s) T1 interface to the internet.

```
interface t1 2/1
  tdm-group 2 timeslots 1-24 speed 64
  no shutdown
!
interface t1 2/2
  shutdown
```

Interface hdlc 1 is a logical interface to the Internet provider using the HDLC protocol. The access-policy "Public" is defined later in the configuration. The crypto map VPN command will cause "VPN 10" as defined earlier in this configuration to terminate at this interface.
The "VOICE" Quality of Service policy, defined earlier in the configuration, is applied to give voice packets higher priority to the internet.
The "cross-connect" command applies this interface to the T1 of interface 2/1 defined earlier.

```
!
interface hdlc 1
  ip address  10.202.221.214  255.255.255.252
  no ip route-cache
  access-policy Public
  crypto map VPN
  qos-policy out VOICE
  no shutdown
  cross-connect 2 t1 2/1 2 hdlc 1
!
!
!
```

```
!
!
!
!
ip access-list standard liberal
  permit any
!
!
ip access-list extended cangoto
  remark limited
  permit ip 192.168.230.0 0.0.0.255  192.168.168.0 0.0.0.255
!
ip access-list extended NAT
  remark internet Connection sharing
  permit ip any  any    log
  permit icmp any  any    log
!
```

The **VPN-10-vpn-selectors** access list was applied to the IPSEC Security associated in the previous command (crypto map VPN 10 ipsec-ike) and the private side interface policy (ip policy-class private) to define the traffic that is eligible for the tunnel. This configuration allows traffic intiated from the Main site subnet (192.168.230.0) to each of two Home sites. (Only the configuration of one Home site is otherwise shown in these Application Notes).

```
ip access-list extended VPN-10-vpn-selectors
  permit ip 192.168.230.0 0.0.0.255  192.168.231.0 0.0.0.255
  permit ip 192.168.230.0 0.0.0.255  192.168.232.0 0.0.0.255
!
```

The **ip policy-class private** allows traffic from the Main site private side to the “home” private side. NAT is applied to general internet traffic using the Public side IP address.

```
ip policy-class private
  allow list VPN-10-vpn-selectors
  allow list self self
  nat source list cangoto interface hdlc 1 overload policy Public
!
```

The **ip policy-class Public** configuration included the complement of the private policy to allow traffic from the Home Site to the Main Site private subnet.

```
ip policy-class Public
  allow reverse list VPN-10-vpn-selectors
  allow list self self
!
!
!
```

The **ip route** applied is the default route through the internet gateway.

```
ip route 0.0.0.0 0.0.0.0 10.202.221.213
!
no ip tftp server
no ip http server
no ip http secure-server
ip snmp agent
no ip ftp agent
!
```

```
!
!
!
snmp-server enable traps
snmp-server source-interface ethernet 0/1
snmp-server community simplesnmp RO
!
!
!
line con 0
  no login
  line-timeout 0
!
line telnet 0 4
  login
  password password
  line-timeout 0
  no shutdown
line ssh 0 4
  login local-userlist
  no shutdown
!
!
end
```

5. Configure the (Home) Adtran NetVanta 2054

The following is the annotated configuration of the Home Adtran NetVanta 2054.

```
!
!
hostname "home"
enable password password
!
clock timezone -5
clock no-auto-correct-DST
!
ip subnet-zero
ip classless
ip domain-proxy
ip routing
!
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
logging email priority-level info
!
ip policy-timeout udp all-ports 120
ip policy-timeout tcp telnet 28800
ip policy-timeout tcp 1720 200
!
ip firewall
```

The h323 and SIP application layer gateway functionality was disabled.

```
no ip firewall alg h323
no ip firewall alg sip
!
!
!
!
!
!
```

The **ip crypto** command enables the VPN features.

```
ip crypto
!
```

The **crypto ike policy 100** will intiate an Internet Key Exchange (IKE) protocol attempt to the Main Site Public IP address. Aggressive Mode was also tested in a similar configuration. The acceptable IKE attribute set is defined to be triple DES, the MD5 hash for authentication, the use of a Pre-Shared Key (PSK, defined later in the configuration) and a lifetime of 86400 seconds.)

```
crypto ike policy 100
  initiate main
  no respond
  peer 10.202.221.214
  attribute 1
    encryption 3des
    hash md5
    authentication pre-share
!
```

The **crypto ike policy 100** line defines the Pre-Shared Key for the IKE policy defined above ("simplekey") and associates the policy to "VPN 10" for which further attributes are defined in this configuration. The key "simplekey" must match the same setting in the Main Site device.

```
crypto ike remote-id address 10.202.221.214 preshared-key simplekey ike-policy 100 no-mode-config no-xauth
!
```

The **crypto ipsec** command defines a transform set the attributes of the IPSEC association for which the data will be passed in this VPN. The Encrypted Security Protocol uses triple DES with the Message Digest 5 hash for authentication.

```
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
  mode tunnel
!
```

The **crypto map VPN 10 ipsec-ike** construct ties together the ipsec transform set and the ike-policy defined above with the "selectors". Traffic matching the access list will be encrypted into the tunnel.

```
crypto map VPN 10 ipsec-ike
  description to main site
  match address VPN-10-vpn-selectors
  set peer 10.202.221.214
  set transform-set esp-3des-esp-md5-hmac
  set security-association lifetime seconds 86400
  ike-policy 100
!
```

The **qos map VOICE** commands define the "VOICE" Quality of Service map, which is intended to give priority to the voice signaling and media in any contention for the outgoing bandwidth. The DiffServ CodePoint Values must match the settings of the IP Office System Gatekeeper form.
The Voice Media is given priority for up to 170 kb/s and the voice signaling for up to 10 kb/s. The amount of bandwidth required is dependant on the number of simultaneous voice calls, the level of encryption used and the codec selection.
Activating this capability may not be effective, if the size of the bandwidth "bottleneck" upstream (e.g., in a DSL router or cable modem) is not administered into the configuration. See the "interface eth 0/1" configuration below for further detail.

```
qos map VOICE 10
  match dscp 46
  priority 170
qos map VOICE 20
  match dscp 34
  priority 10
qos map VOICE 30
!
!
vlan 1
  name "Default"
!
```

Interface eth 0/1 connects to the "internet" (e.g., a DSL router or Cable Modem). The configuration shows a fixed IP Address, but a DHCP configuration was also tested.
The access-policy **Public** is defined later in the configuration. The **crypto map VPN** command will cause VPN 10 as defined earlier in this configuration to originate at this interface.
The **VOICE** Quality of service policy, defined earlier in the configuration, is applied to give voice packets higher priority to the internet.
The **cross-connect** command applies this interface to the T1 of interface 2/1 defined earlier.

The **traffic-shape rate** command allows the device to manage outgoing traffic to the anticipated upstream "bottleneck" (e.g., the DSL service upstream rate). Increasing the **max-reserved-bandwidth** to 90% allows the use of a **qos map** where most of this bandwidth can be used for voice packets as a priority.

```
interface eth 0/1
  ip address  192.168.168.102  255.255.255.0
  access-policy Public
  crypto map VPN
  traffic-shape rate 200000
  qos-policy out VOICE
  max-reserved-bandwidth 90
  no shutdown
  no lldp send-and-receive
```

```
!
interface eth 0/2
  no shutdown
!
interface eth 0/3
  no shutdown
!
interface eth 0/4
  no shutdown
!
interface eth 0/5
  no shutdown
!
!
```

Interface vlan 1 defines the home side private subnet. Access-policy **Private**, defined later in the configuration, filters the incoming packets to those with the allowed characteristics.

```
interface vlan 1
  ip address  192.168.231.1  255.255.255.0
  access-policy Private
  no shutdown
!
!
!
!
!
ip access-list extended cangoto
  permit icmp any  any
!
ip access-list extended NAT
  remark Internet Connection Sharing
  permit ip any  any log
!
```

The access list **VPN-10-vpn-selectors** defines a minimal set of policies to support Avaya IP Telephone operation, although it could be further narrowed. For example, only traffic from the IP address of the Avaya IP Telephone could be allowed to the main site telephony systems, rather than allowing traffic from the whole private subnet.
The lines below allow, respectively:

- H.323 Registration (to the IP Office IP address, port 1719)
- H.3233 signaling (to the IP Office IP address, port 1720)
- Voice Media (to the Main Site subnet and a subnet another home site, to the range of ports specified on the IP Office gatekeeper form)
- TFTP download of firmware from the Management PC.

Alternatives include:

- simply allowing all traffic between the private subnets (as in the Main Site configuration)
- Support for the Phone Manager Pro PC Softphone as described in the note at the end of this section.

```
ip access-list extended VPN-10-vpn-selectors
  permit udp 192.168.231.0 0.0.0.255  host 192.168.230.15 eq 1719
  permit tcp 192.168.231.0 0.0.0.255  host 192.168.230.15 eq 1720
  permit udp 192.168.231.0 0.0.0.255  192.168.232.0 0.0.0.255 range 49152 53246
  permit udp 192.168.231.0 0.0.0.255  192.168.230.0 0.0.0.255 range 49152 53246
  permit udp 192.168.231.0 0.0.0.255  host 192.168.230.134
!
```

The **ip policy-class Private** allows traffic from the home site private side to the Main private side. NAT is applied to general internet traffic using the Public side IP address.

```
ip policy-class Private
  allow list self self
  allow list VPN-10-vpn-selectors
  nat source list NAT interface eth 0/1 overload
!
```

The **ip policy-class Public** configuration included the complement of the private policy to allow traffic from the Main site to the Home Site private subnet.

```
ip policy-class Public
  allow reverse list VPN-10-vpn-selectors
  allow list cangoto
!
!
!
```

The **ip route** applied is the default route through the internet gateway.

```
ip route 0.0.0.0 0.0.0.0 192.168.168.1
!
no ip tftp server
no ip http server
```

```
no ip http secure-server
no ip snmp agent
no ip ftp agent
!
!
!
!
!
line con 0
  no login
  line-timeout 0
!
line telnet 0 4
  login local-userlist
!
!
!
end
```

Note: For PhoneManager Pro PC Softphone support, additional UDP ports must be opened beyond what is allowed in this configuration and UDP sessions initiated from the IP Office at the Main site must be allowed. The following lines were configured in the “VPN-10-vpn-selectors” access list to test this configuration:

```
permit udp 192.168.231.0 0.0.0.255  host 192.168.230.15
permit udp host 192.168.230.15  192.168.231.0 0.0.0.255
```

For security purposes, the access list can be further refined. See IP Office documentation relative to the ports that are required to be open for PC Softphone operation.

6. Home Avaya 5602SW IP Telephone

The Avaya IP Telephone manual configuration mode can be entered by either:

- Pressing "*" at the appropriate time during power up.
- At an idle registered phone, pressing:
  i. "HOLD"
  ii. A D D R # (2 3 3 7 #).

At the prompts, enter the following data to repeat this configuration:

Prompt	Data	Meaning
Phone=	192.168.231.55	The IP Telephone's IP Address
CallSv=	192.168.230.15	The IP Office LAN1 address
CallSvPort=	1719	The registration port
Router=	192.168.231.1	The Home 2054 VLAN 1 address
Mask=	255.255.255.0	The Home private subnet mask
FileSv=	192.168.230.134	The File Server for IP Telephone firmware updates (typically the IP Office Manager PC)
802.1Q=	Off	Activates VLAN/Layer 2 priority tagging
	#	OK to accept values (and restart the phone if necessary.

Alternatively, if the home device can be configured to use VLAN tagging, the 802.1Q= entry can be set to "On" and the appropriate VLAN tag entered.

7. Verification and Troubleshooting

Ultimately, the quality of experience provided to the end user will be dependent on the performance of the underlying packet network. The nature of most Internet service is that there are no service level guarantees that can be measured and assumed stable over time.

Still, a basic evaluation might include:

- What is the subscribed upstream/downstream bandwidth to the home?
- What is the expected non-voice use?
- How does the above compare to the expected encrypted voice bandwidth needs.
- What is the end to end delay and loss (e.g., as measured by a ping) by time of day and day of week?

The following are some of the tests that were run in the lab, and can be used to verify an installation:

- The idle phone screen should show as it does when locally connected to an IP Office.
- Dial an extension on another telephone and verify talk path. In particular, call an IP telephone to verify that IP Direct Media ("shuffling") works as expected.

- Features of interest, such as hunt group operation, bridging, conferencing and should be verified to show that the features work similar to local operation.
- Resetting or re-powering the phone should show that it checks for a needed firmware upgrade and then reregisters.

Some trouble-shooting scenarios include:

- If the IP Telephone Display shows "Discover 192.168.230.15":
  - The IP Phone trying to initiate H.323 registration (to the IP Office IP address and UDP port 1719) and is not receiving a response.
  - Possible issues include:
    - The Phone CallSv parameter is incorrect.
    - The VPN tunnel is not "up" between the sites
    - The Adtran NetVanta access list does not allow the traffic

- The following shows that the VPN tunnel is operational. Note that there are inbound and outbound associations associated with each direction of the registration to UDP port 1719 and the signaling over TCP port 1720.

```
Mainsite#show crypto ipsec sa
IPSec Security Associations: Total IPSec SAs: 4

  Peer IP Address: 10.202.221.214
  Direction: Inbound
  SPI: 0xE2F0D787 (3807434631)
  Encapsulation: ESP
  RX Bytes: 37204
  Selectors: Src:192.168.231.0/255.255.255.0  Port:ANY  Proto:17
             Dst:192.168.230.15/255.255.255.255  Port:1719  Proto:17
  Hard Lifetime: 70630
  Soft Lifetime: 0
  Crypto Map: VPN 10

  Peer IP Address: 10.202.221.214
  Direction: Inbound
  SPI: 0xE3C05275 (3821032053)
  Encapsulation: ESP
  RX Bytes: 20920
  Selectors: Src:192.168.231.0/255.255.255.0  Port:ANY  Proto:6
             Dst:192.168.230.15/255.255.255.255  Port:1720  Proto:6
  Hard Lifetime: 70620
  Soft Lifetime: 0
  Crypto Map: VPN 10

  Peer IP Address: 192.168.168.1
  Direction: Outbound
```

```
  SPI: 0xE377C8F7 (3816278263)
  Encapsulation: ESP
  TX Bytes: 20960
  Selectors: Src:192.168.230.15/255.255.255.255  Port:1720  Proto:6
          Dst:192.168.231.0/255.255.255.0  Port:ANY  Proto:6
  Hard Lifetime: 70620
  Soft Lifetime: 70560
  Crypto Map: VPN 10

  Peer IP Address: 192.168.168.1
  Direction: Outbound
  SPI: 0xFFAC5C81 (4289485953)
  Encapsulation: ESP
  TX Bytes: 31808
  Selectors: Src:192.168.230.15/255.255.255.255  Port:1719  Proto:17
          Dst:192.168.231.0/255.255.255.0  Port:ANY  Proto:17
  Hard Lifetime: 70630
  Soft Lifetime: 70540
  Crypto Map: VPN 10

Mainsite#
```

- The following command, run from the Home site, can used to see if the packets being sent are matching as expected the applied access list:

home# **show access VPN-10-vpn-selectors**

```
Extended IP access list VPN-10-vpn-selectors
   permit udp 192.168.231.0 0.0.0.255  host 192.168.230.15 eq 1719   (52 matches)
   permit tcp 192.168.231.0 0.0.0.255  host 192.168.230.15 eq 1720  (25 matches)
   permit udp 192.168.231.0 0.0.0.255  192.168.232.0 0.0.0.255 range 49152 53246   (0
matches)
   permit udp 192.168.231.0 0.0.0.255  192.168.230.0 0.0.0.255 range 49152 53246   (29
matches)
   permit udp 192.168.231.0 0.0.0.255  host 192.168.230.134    (8 matches)
```

- If the previous command shows that the packets are matching, but the VPN tunnel is not becoming operational, consider using the “debug” commands from the NetVanta systems. Be careful not to impact the performance of real time users. The “debug crypto ike” and “debug crypto ipsec” commands can be used to see if the home device is attempting to initiate the tunnel, if the main sites is receiving the initiation and if so, is there a problem with mis-matched transform sets.

- A sniffer can be used to verify whether traffic is traversing the tunnel as expected.

- The IP Office System Monitor, with the H.323 RAS traces enabled, can be used to verify whether Registration requests are being received and, if so, if there are replies.

- If the phone is operational, but there are issues with sound quality, consider bandwidth limitations. A sniffer measurement of traffic between the Adtran 2054 and 3305 showed 134 byte packets at 50 packets per second (= ~54 kb/s) for a G.729 codec. Check that the total packet traffic delivered to a bandwidth bottleneck (e.g., a DSL Modem or a Cable Modem) does not exceed its capacity since there is no priority given for voice packets at that bottleneck. Also, consider whether there are issues in the customer's home network, such as the use of hubs or possible looping conditions that might affect the user's perceived voice quality.

8. Conclusion

These Application Notes describe the configuration of a remote Avaya IP Telephone served by an Avaya IP Office over a Virtual Private Network implemented with an Adtran NetVanta 3305 and an Adtran NetVanta 2054. The configuration was tested successfully.

9. References

Avaya product documentation can be found at http://support.avaya.com.

Adtran product documentation can be found at http://support.adtran.com.

.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com