



Avaya Solution & Interoperability Test Lab

A Configuration of Avaya IP Office with the Westell 2200 ADSL Modem for Internet Access and Voice over IP Virtual Private Networking - Issue 1.0

Abstract

These Application Notes describe a configuration of an Avaya IP Office using a Westell 2200 Digital Subscriber Line (DSL) modem for Virtual Private Networking over the Internet. IP Office H.323 Trunking and an IP Office Virtual Private Network (VPN) were configured for inter-site voice over IP calls.

The DSL modem used the Point-to-Point Protocol (PPP) over Ethernet (PPPoE) for access and for address assignment. The Westell “IP Passthrough” feature was used to allow the IP Office to use the single “public” statically assigned IP Address.

A Paradyne GrandSLAM DSL Access Multiplexer was used to bridge the DSL and SONET protocols in the network, and a Cisco 3725 router acted as the PPPoE server.

Please Note: This configuration is based on common methods of Internet access and transport and, as such, includes no provisions for cross-network Quality of Service. Thus, packets can be lost and delayed to an extent that impacts the callers’ perception of call quality. Many acceptable calls can be made, but there can be instances of noticeable echo, gaps in speech, and even dropped calls.

1. Introduction

These Application Notes describe a configuration of IP Office Small Office Edition operating through Westell Digital Subscriber Line modems for Internet access via the Asymmetric Digital Subscriber Line (ADSL) protocol. ADSL is generally targeted to residential and small business locations.

The Network configuration was designed to be similar to current practice with:

- A single ATM PVC set to “Unspecified Bit Rate” (No Quality of Service)
 - One IP address assigned via PPPoE
 - “Static” public addresses can be purchased, but at least one must be assigned via the PPPoE mechanism.

The DSL modem in this configuration allows the IP Office to use the “public” IP address (10.8.8.100) that it was assigned via the PPPoE protocol. A Virtual Private Network (VPN) was configured from IP Office to IP Office for voice calls.

Since the IP address of the Small Office is part of the VPN configuration data, the IP address must be permanently assigned to the small office location, rather than dynamically assigned by the service provider from an IP address pool.

Figure 1 shows the configuration verified.

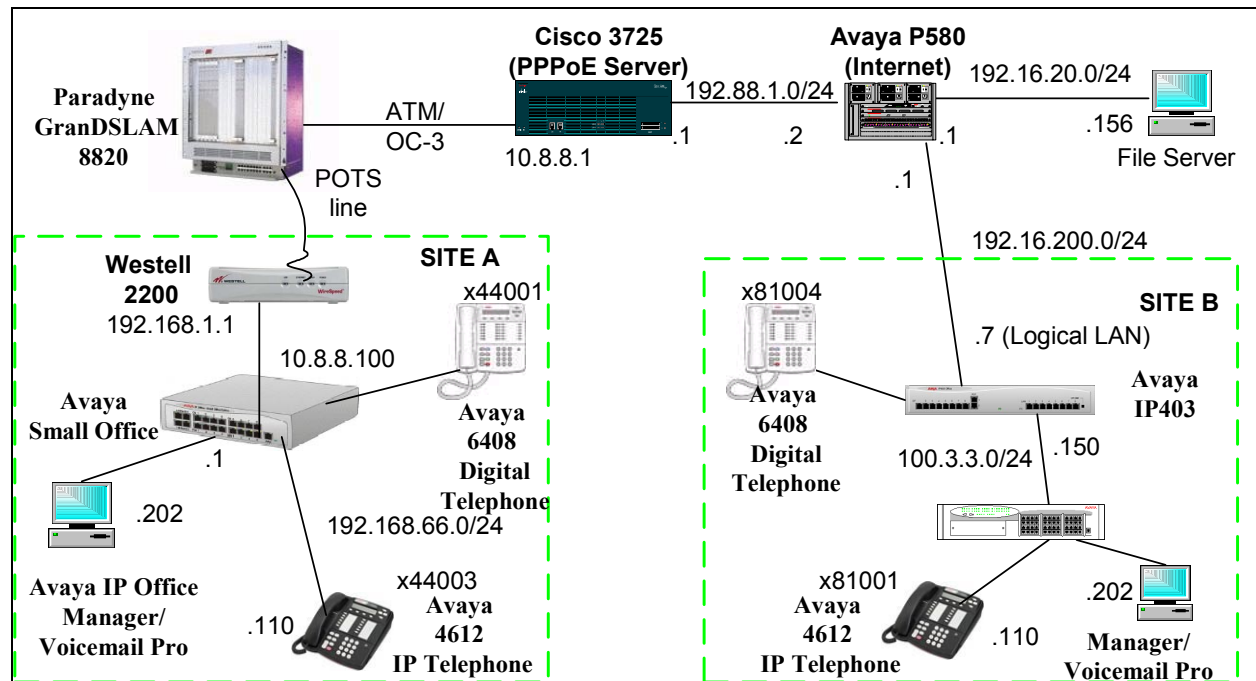


Figure 1: DSL Network Configuration

Figure 2 summarizes the protocol stack of this configuration. The Cisco 3725 acts as a PPP over Ethernet server. The DSL modem establishes a PPP over Ethernet session to the server to obtain its IP address. The modem operates in “Passthrough” mode, meaning that packets received from the network for that address were forwarded to the IP Office. Packets from the IP Office were forwarded to the network as is.

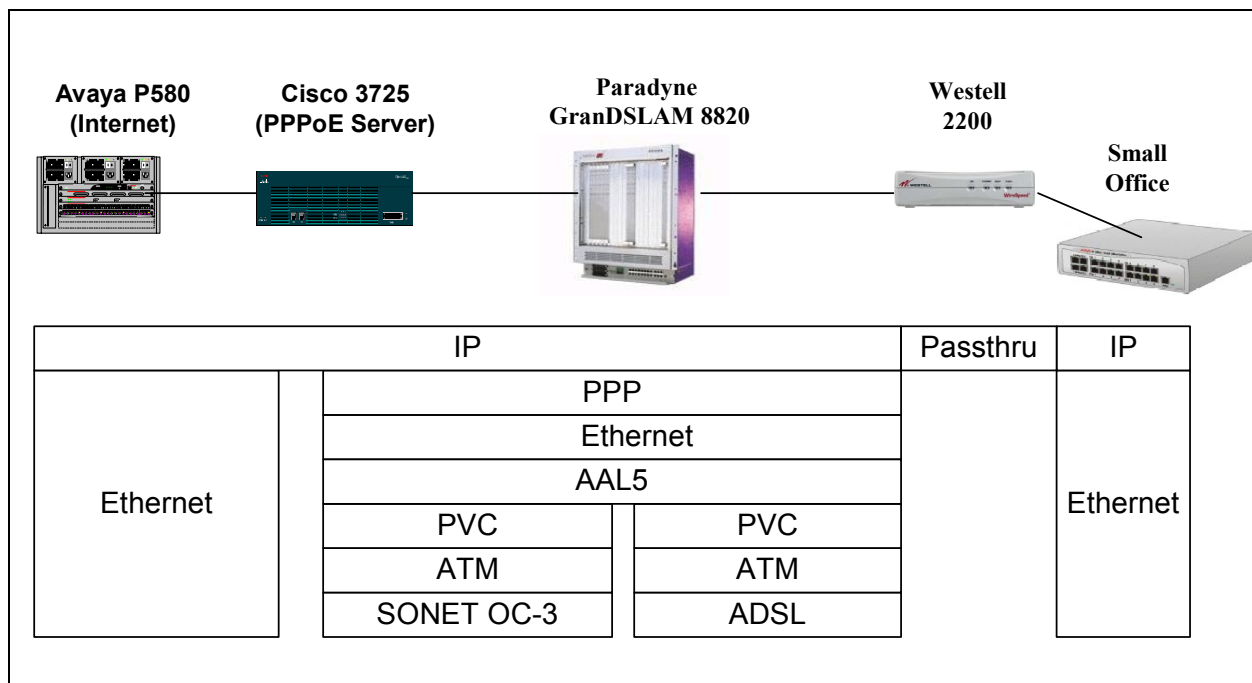


Figure 2: Protocol Stack

The Paradyne Hotwire 8820 GrandSLAM, which can be installed at the Network Service Provider (NSP), provides high-speed Internet or intranet access. The GrandSLAM is a 20-slot chassis with integral power distribution and conditioning, as well as alarm, cooling, and interface subsystems designed to accommodate 17 DSL port cards. More information can be found at www.paradyne.com.

The Westell modems reside on a customer premise or small business to provide access to the DSL network. ADSL generally will provide much higher downstream (to the customer from the network) rates than upstream over a line that can also be used for POTS traffic. For more information, visit <http://www.westell.com/>.

The Cisco 3725 router’s position in this configuration is likely to be replaced by a larger system in a production environment. There are several other adaptations that could be made to apply this configuration in a “real” environment, but the capabilities for the user would be the same.

1.1. Bandwidth and Quality of Service Considerations

The Westell 2200 ADSL modem does not prioritize packet traffic toward the upstream DSL channel. Heavy outgoing traffic will interfere with voice call quality. Also, as is typical of what is currently available from U.S. Service Providers, there is no Quality of Service configured at the DSLAM or routers for traffic from the network.

Traffic engineering for voice calls must take into account the protocol overhead as shown in **Figure 2**.

For G.729 VPN as configured in this Application Note, the following table calculates the size of each IP media packet from the IP Office, sent at 50 packets per second.

Packet Portion	Size in Bytes
Security Data Bytes	84
IP ESP Header	8
IP Header	20
Ethernet Header	14
PPPoE Headers	6
LLC encapsulation	8
AAL5 CPCS payload trailer	8
Total Packet Size	148 bytes

The ATM/DSL rate is calculated based on a 48 byte payload for each 53 byte cell.

- 148 bytes per packet / 48 bytes per cell = 4 cells per packet
- 4 cells per packet * 50 cells per second * 53 bytes per cell = **84.8 Kb/s per call**.

Considerably greater bandwidth would be required, for example, if triple Data Encryption Standard (DES) was configured for the VPN.

For a configuration using G.729 RTP without VPN, the following table calculates the size of each IP packet from the IP Office, sent at 50 packets per second.

Packet Portion	Size in Bytes
G.729 Data	20
IP/UDP/RTP Headers	40
Ethernet Header	14
PPPoE Headers	6
LLC encapsulation	8
AAL5 CPCS payload trailer	8
Total Packet Size	96 bytes

The ATM/DSL rate is calculated based on a 48 byte payload for each 53 byte cell.

- 96 bytes per packet / 48 bytes per cell = 2 cells per packet
- 2 cells per packet * 50 cells per second * 53 bytes per cell = **42.4 Kb/s per call**.

2. Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Version
Avaya IP Office - Small Office Edition	2.1(9)
Avaya IP403 Office Server	2.1(9)
Avaya 4600 Series IP Telephones	2.0
Avaya P580 Multi-service Switch	6.0
Westell 2200 ADSL Modem	1.06.53
Paradyne 8820 Hotwire DSLAM with ADSL Card 8365-B1-000	Firmware Revision: 02.03.55 Hardware Revision: 4402-83B Line Code Revision: 03.07.17 PLD Revision: 01.00.01
Cisco 3725	12.2(15)ZJ3

3. Configure the PCs

- All PCs in this configuration have the IP Office set as the default router. Otherwise, add the persistent routes as needed with the DOS prompt “route –p add” command.
- Applications that transfer data toward the network may fail due to the packet size limitation of the DSL network. An example is ftp, which can attempt to send packets up to the largest Maximum Transmission Unit (MTU). If a PC is configured to send with the MTU of its local interface, this can be greater than the size of the PPPoE protocol payload over the DSL network.

One way to address this problem is to configure the PC registry of the sending PC to use TCP Path MTU discovery to find the largest packet size. *Warning: Do not attempt this change without training in Registry procedures.*

Step 1) From the DOS prompt, type **regedit**.

Step 2) Navigate to:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP

Step 3) Ensure the following settings in the Registry.

PMTUDiscovery = 1

Step 4) Reboot.

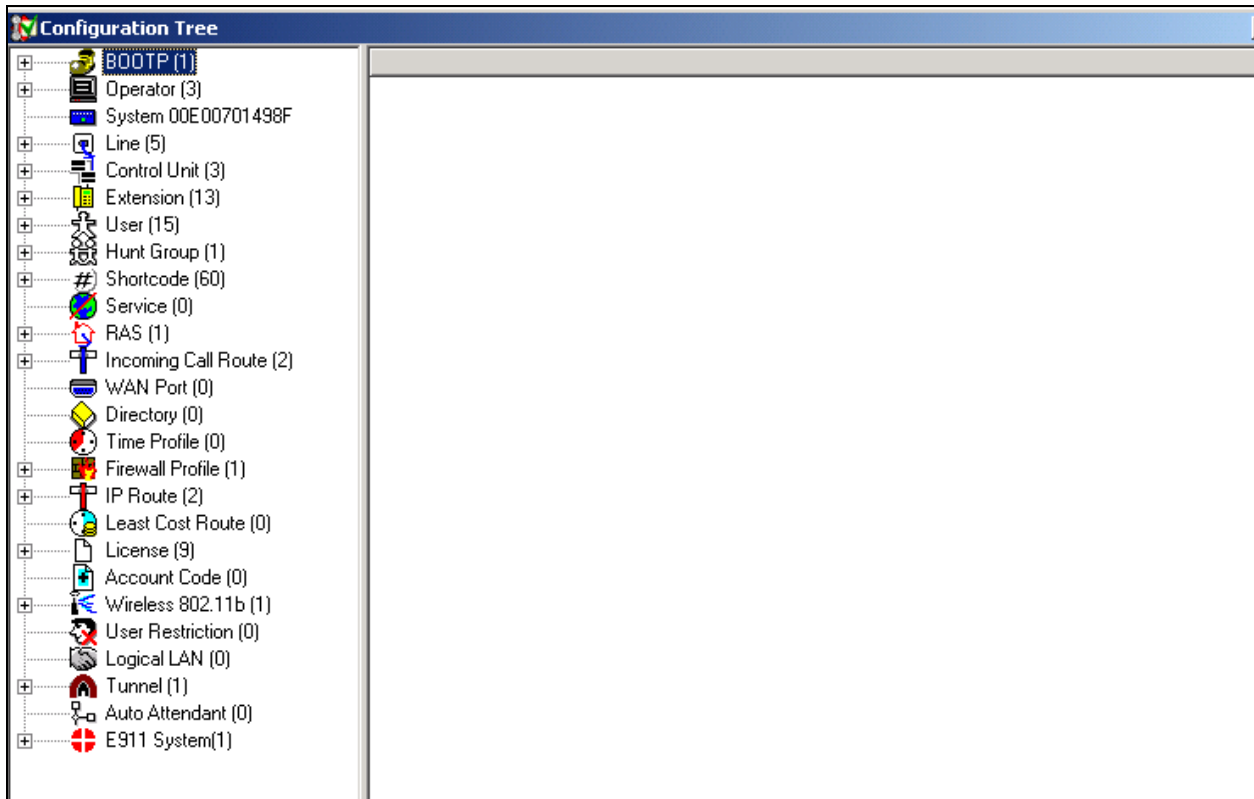
See the Microsoft Knowledge Base Article Q158474 for a more complete description.

Note that large packets can cause jitter to voice packets and increase latency by blocking upstream bandwidth during their relatively long transmission times.

4. Configure the Avaya IP Office - Small Office Edition

This section describes the configuration of the IP Office Small Office. These steps would apply also to an Avaya IP412 Office. The Hub-based models require the additional step of administering a “Logical LAN”. An example of Logical LAN configuration is described in **Section 9**.

Step 1) With the IP Office Manager, access the IP Office Configuration Menu.



Step 2) Navigate to the **System→System** tab. Ensure that the License Server IP Address and Time Server IP Address are configured with the address of the License Server PC, normally the Manager PC.

System Configuration : 00E00701498F

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Gatekeeper | LDAP | SNMP

Name	00E00701498F	Locale	enu
Password	xxxxxxxx	Confirm Password	xxxxxxxx
Monitor Password		Confirm Monitor Password	
		Licence Server IP Address	192.168.66.202
Time Offset (hours)			
TFTP Server IP Address		AVPP IP Address	
Time Server IP Address	192.168.66.202		
File Writer IP Address		☐ DSS Status	
Power Conference IP Address		☒ Beep on listen	
Power Conferencing URL	☐ Hide auto recording		
	☐ Favour RIP Routes, over static routes		

OK Cancel Help

Step 3) Configure the **System→LAN1** (Private Side) form as shown.

The screenshot shows a 'System Configuration' window for device '00E00701498F'. The 'LAN1' tab is selected. The 'IP Address' field is set to '192.168.66.1' and the 'Number Of DHCP IP Addresses' is '200'. The 'IP Mask' is '255.255.255.0'. The 'Primary Trans. IP Address' field is empty. The 'Enable NAT' checkbox is unchecked. The 'DHCP Mode' section has 'Server' selected. The 'RIP Mode' section has 'None' selected. The window has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

System	LAN1	LAN2	DNS	Voicemail	Telephony	Gatekeeper	LDAP	SNMP
IP Address: 192.168.66.1								
Number Of DHCP IP Addresses: 200								
IP Mask: 255.255.255.0								
Primary Trans. IP Address:								
☐ Enable NAT								
DHCP Mode								
☒ Server								
☐ Disabled								
☐ Dialin								
☐ Client								
RIP Mode								
☒ None								
☐ Listen Only (Passive)								
☐ RIP 1								
☐ RIP 2 Broadcast (RIP 1 Compatibility)								
☐ RIP 2 Multicast								

OK Cancel Help

Step 4) Configure the **System→LAN2** form. The IP address is the Public Address that the Service Provider will assign. NAT is enabled to allow endpoints on the private side of Small Office to address the Internet using the same public IP address. If desired, a Firewall can be configured to minimize the types of traffic that can access the private side.

Note: An alternative is to set LAN2 to be a DHCP client and the Modem to be the DHCP server. Be aware that the IP Office must be rebooted for any address change with NAT to take effect.

The screenshot shows the 'System Configuration : 00E00701498F' dialog box with the 'LAN2' tab selected. The 'IP Address' field is set to '10.8.8.100' and the 'Number Of DHCP IP Addresses' is '200'. The 'IP Mask' is '255.255.255.0'. The 'Firewall Profile' is set to 'Internet01'. The 'Primary Trans. IP Address' field is empty. The 'Enable NAT' checkbox is checked. The 'DHCP Mode' section has 'Disabled' selected. The 'RIP Mode' section has 'None' selected. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Field	Value
IP Address	10.8.8.100
Number Of DHCP IP Addresses	200
IP Mask	255.255.255.0
Firewall Profile	Internet01
Primary Trans. IP Address	
Enable NAT	☒
DHCP Mode	Disabled
RIP Mode	None

Step 5) Configure the **System→Gatekeeper** form with (RTP) DSCP and Signaling DSCP values to match any quality of service plan that may be in place in the network.

System Configuration : 00E00701498F

System | LAN1 | LAN2 | DNS | Voicemail | Telephony | **Gatekeeper** | LDAP | SNMP

☒ Gatekeeper Enable

☐ Direct Routed Signaling Enable

☒ Auto-create Extn Enable

☐ Enable RSVP

DSCP(Hex) DSCP

DSCP Mask (Hex) DSCP Mask

SIG DSCP (Hex) SIG DSCP

SSON

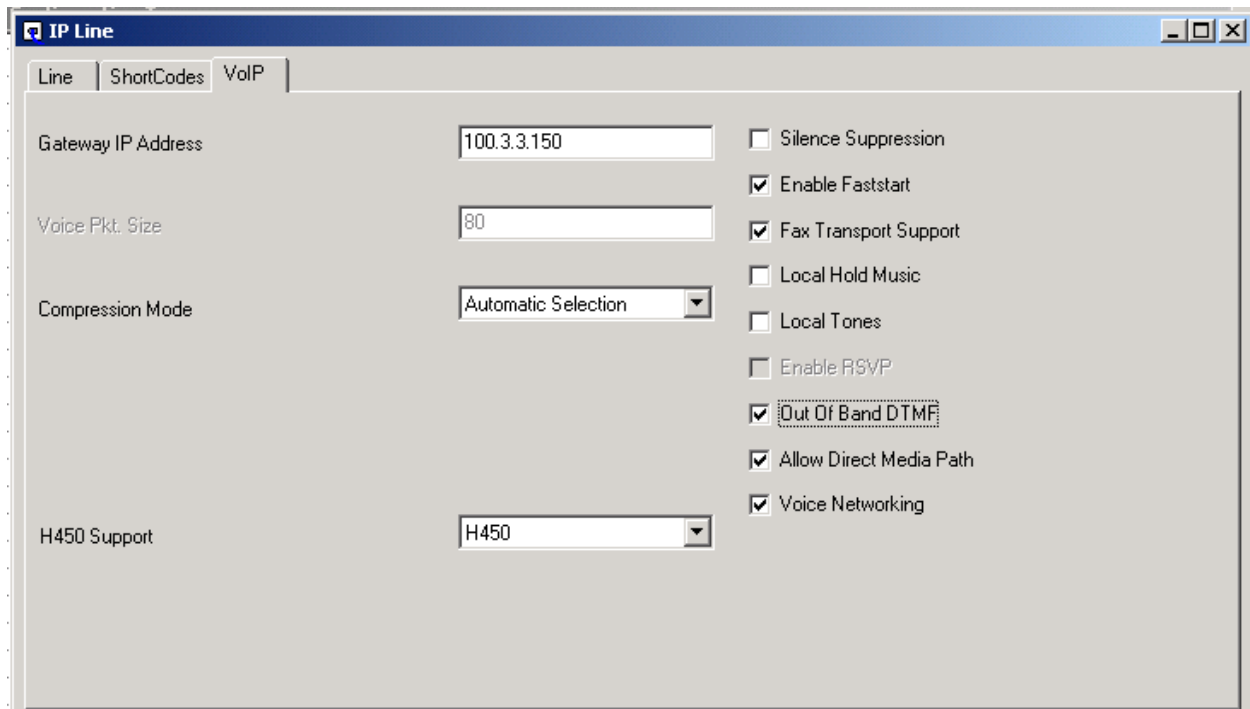
Step 6) From **Line**, create a **New** line to the IP403 Office.

Step 6 a) Enter the desired Line Number and Incoming and Outgoing Group IDs. Set the outgoing channels within the expected DSL bandwidth limitations.

The screenshot shows a window titled "IP Line" with three tabs: "Line", "ShortCodes", and "VoIP". The "Line" tab is selected. The window contains the following fields and values:

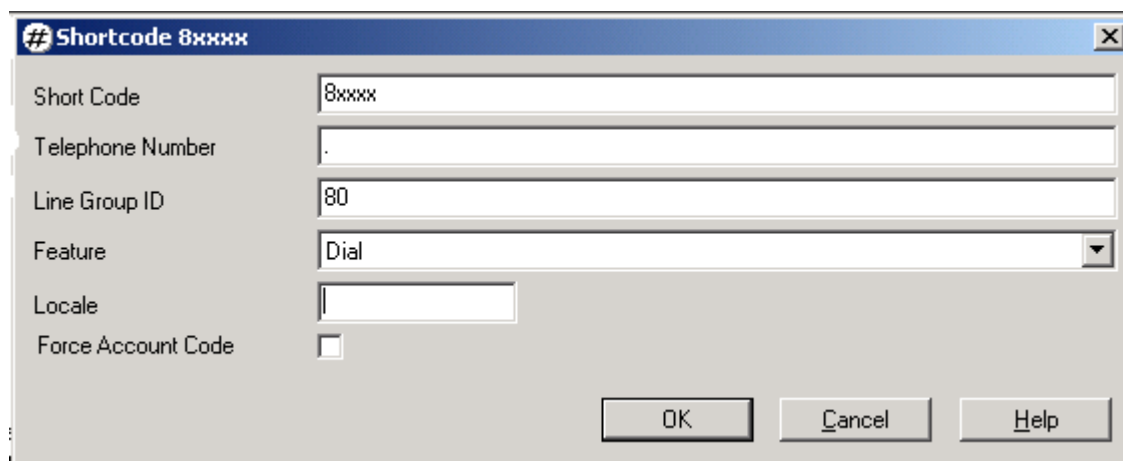
Field	Value
Line Number	80
Telephone Number	
Number Of Channels	2
Outgoing Channels	2
Data Channels	2
Voice Channels	2
TEI	0
Incoming Group ID	80
International Prefix	00
Outgoing Group ID	80
National Prefix	0
Prefix	

Step 6 b) Select the **Line VoIP** tab. Set the Gateway IP Address to the LAN1 (private side) address of the IP403 Office. “Allow Direct Media Path” should be disabled if situations of slow voice path cut-through arise for IP endpoints.



The image shows a software window titled "IP Line" with three tabs: "Line", "ShortCodes", and "VoIP". The "VoIP" tab is selected. The window contains several configuration fields and checkboxes. On the left, there are four fields: "Gateway IP Address" with the value "100.3.3.150", "Voice Pkt. Size" with the value "80", "Compression Mode" with a dropdown menu showing "Automatic Selection", and "H450 Support" with a dropdown menu showing "H450". On the right, there are seven checkboxes: "Silence Suppression" (unchecked), "Enable Faststart" (checked), "Fax Transport Support" (checked), "Local Hold Music" (unchecked), "Local Tones" (unchecked), "Enable RSVP" (unchecked), and "Out Of Band DTMF" (checked). Below these, there are two more checkboxes: "Allow Direct Media Path" (checked) and "Voice Networking" (checked).

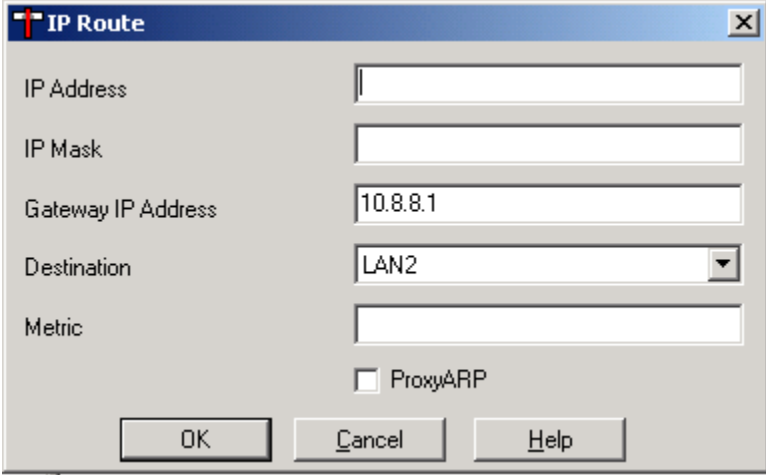
Step 7) Select the **Short Codes** tab to create a short code to direct outgoing calls to the IP403 Office based on the dialed number.



The image shows a software window titled "# Shortcode 8xxxx" with a close button in the top right corner. The window contains several configuration fields: "Short Code" with the value "8xxxx", "Telephone Number" with a single dot ".", "Line Group ID" with the value "80", "Feature" with a dropdown menu showing "Dial", "Locale" with an empty text box, and "Force Account Code" with an unchecked checkbox. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

Step 8) If a firewall was selected previously for the LAN2 port, configure as desired under **Firewall Profile**.

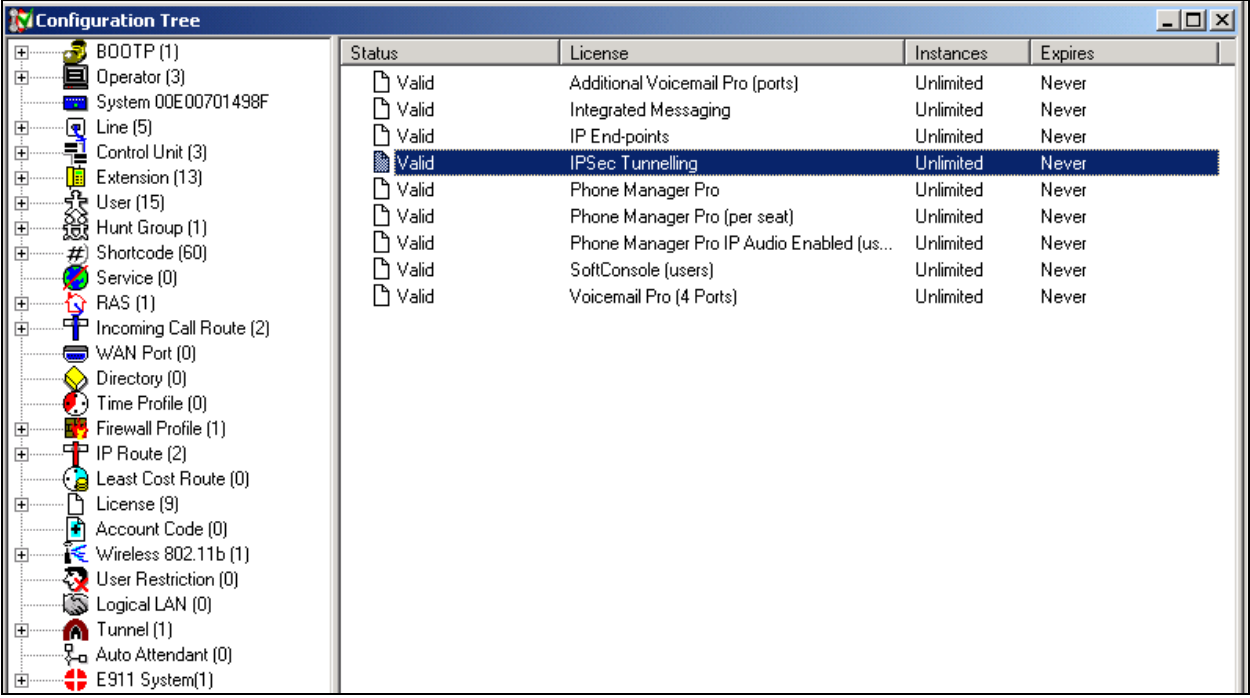
Step 9) From **IP Route** create a new default IP Route to the Service Provider Internet Gateway IP Address.



The IP Route dialog box contains the following fields and controls:

- IP Address:** An empty text input field.
- IP Mask:** An empty text input field.
- Gateway IP Address:** A text input field containing the value "10.8.8.1".
- Destination:** A dropdown menu with "LAN2" selected.
- Metric:** An empty text input field.
- ProxyARP:** An unchecked checkbox.
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom.

Step 10) Enter a license to enable IP Sec Tunneling, which is needed for IPSEC with DES3.



The Configuration Tree window displays a list of system components on the left and a detailed view of the selected 'License' component on the right. The 'License' view includes a table with the following data:

Status	License	Instances	Expires
Valid	Additional Voicemail Pro (ports)	Unlimited	Never
Valid	Integrated Messaging	Unlimited	Never
Valid	IP End-points	Unlimited	Never
Valid	IPSec Tunneling	Unlimited	Never
Valid	Phone Manager Pro	Unlimited	Never
Valid	Phone Manager Pro (per seat)	Unlimited	Never
Valid	Phone Manager Pro IP Audio Enabled (us...	Unlimited	Never
Valid	SoftConsole (users)	Unlimited	Never
Valid	Voicemail Pro (4 Ports)	Unlimited	Never

Step 11) From **Tunnel**, create an IP Sec tunnel.

Step 11 a) The Local Configuration entries correspond the Small Office LAN1 (private interface) IP Address and IP Mask entries. The Remote Configuration IP address and IP Mask correspond the IP403 Office LAN1 (private interface) entries. The Remote Configuration “Gateway” is the public side address of the IP403 Office.

IP Security to ip403

Main | IKE Policies | IPSec Policies

Name: to ip403

Local Configuration

IP Address: 192.168.66.0

IP Mask: 255.255.255.0

Gateway: <LocalInterface>

Remote Configuration

IP Address: 100.3.3.0

IP Mask: 255.255.255.0

Gateway: 192.16.200.7

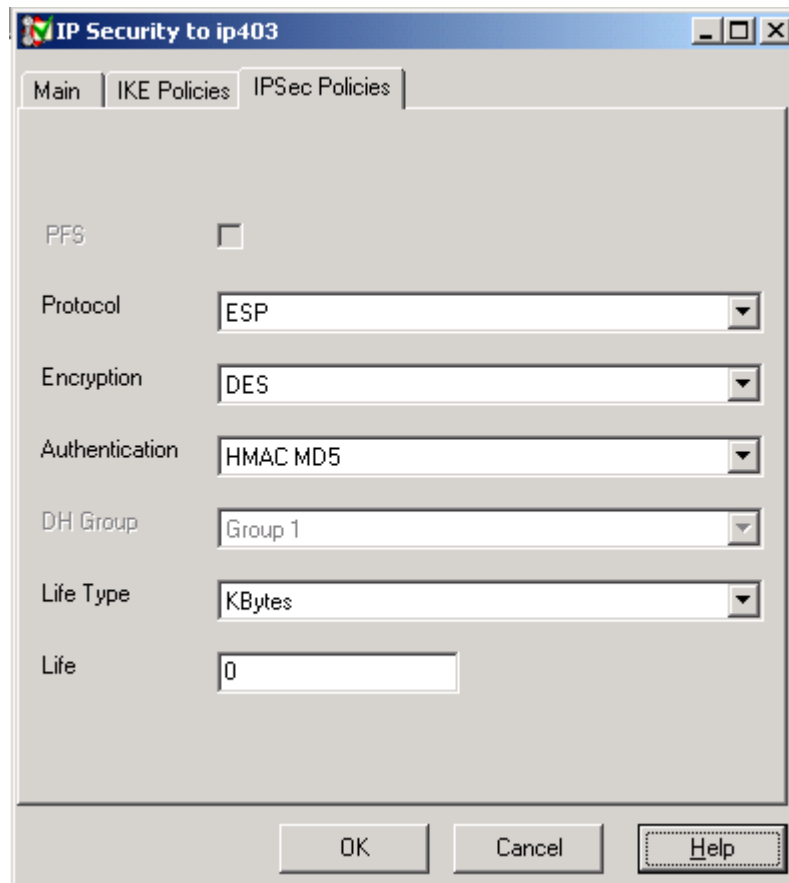
OK Cancel Help

Step 11 b) Select the **IKE Policies** tab. Ensure that all the entries, including the Shared Secret are the same as those on the corresponding IP403 Office **IKE Policies** tab.

The screenshot shows a Windows-style dialog box titled "IP Security to ip403". It has three tabs: "Main", "IKE Policies", and "IPSec Policies". The "IKE Policies" tab is selected. The dialog contains the following fields and controls:

- Shared Secret:** A text box containing "xxxxxxxx".
- Confirm Password:** A text box containing "xxxxxxxx".
- Exchange Type:** A dropdown menu with "ID Prot" selected.
- Encryption:** A dropdown menu with "DES CBC" selected.
- Authentication:** A dropdown menu with "MD5" selected.
- DH Group:** A dropdown menu with "Group 1" selected.
- Life Type:** A dropdown menu with "KBytes" selected.
- Life:** A text box containing "0".
- Buttons:** "OK", "Cancel", and "Help" buttons are located at the bottom right.

Step 11 c) Select the **IP Sec Policies** tab. Ensure that the settings are the same as the corresponding IP403 Office IP Sec Policies settings.



5. Configure the Westell 2200 ADSL Modem

Note: The Westell 2200 modem can be reset back to factory defaults, including the management address of 192.168.1.1, by pressing the square button between power input and Ethernet Jack.

This section describes the configuration of the Westell 2200 ADSL modem for Point-to-Point Protocol over Ethernet operation.

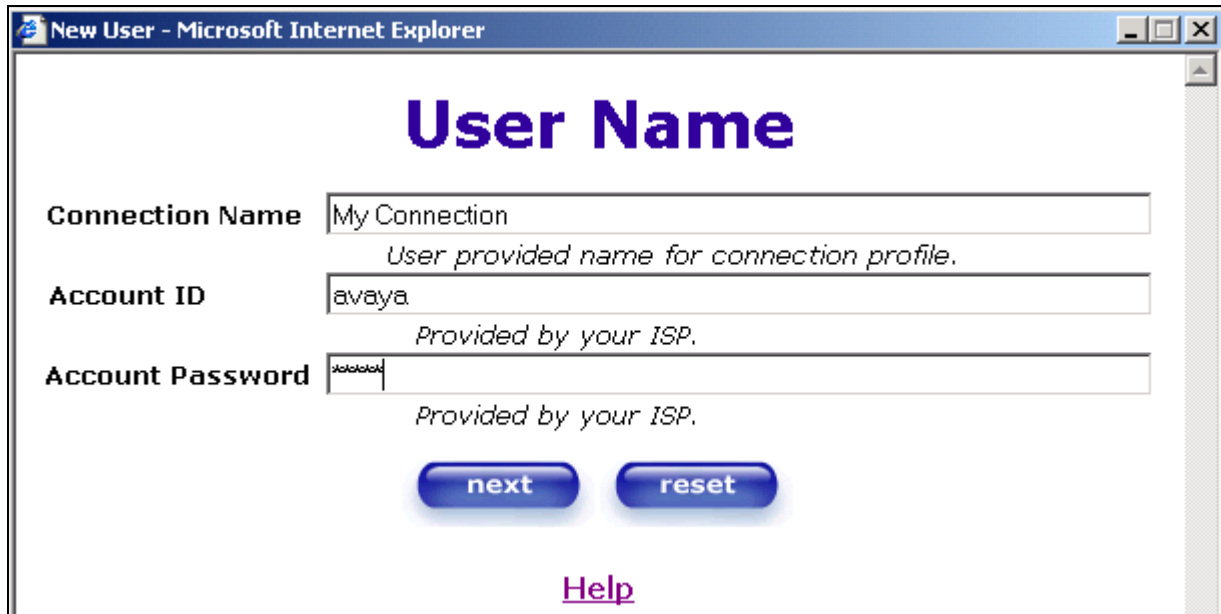
Step 1) Access the Westell interface via a Browser.

Step 1 a) To access the Westell, either connect a laptop directly to the Ethernet port via a crossover cable or use a hub.

Step 2) Update the login and password if prompted.

Step 3) If the "Getting Started" screen is presented, press **next** to use the provided wizard to install the modem basic configuration.

Step 4) Enter the **Account ID** and **Account Password** provided by the Service Provider for this PPP over Ethernet service. Press **next**.



User Name

Connection Name
User provided name for connection profile.

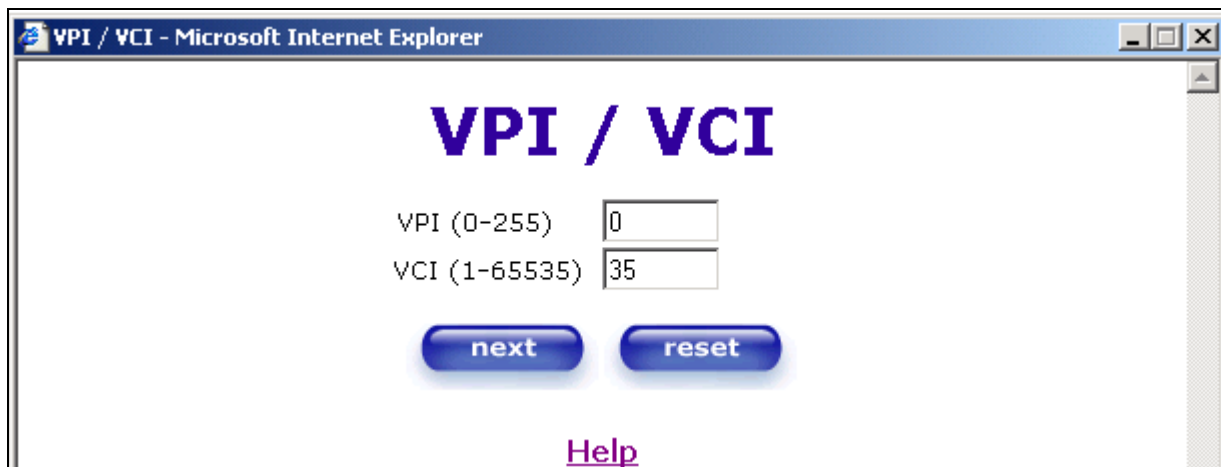
Account ID
Provided by your ISP.

Account Password
Provided by your ISP.

[next](#) [reset](#)

[Help](#)

Step 5) Enter the Service Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) provided by the Service Provider. Press **next**.



VPI / VCI

VPI (0-255)

VCI (1-65535)

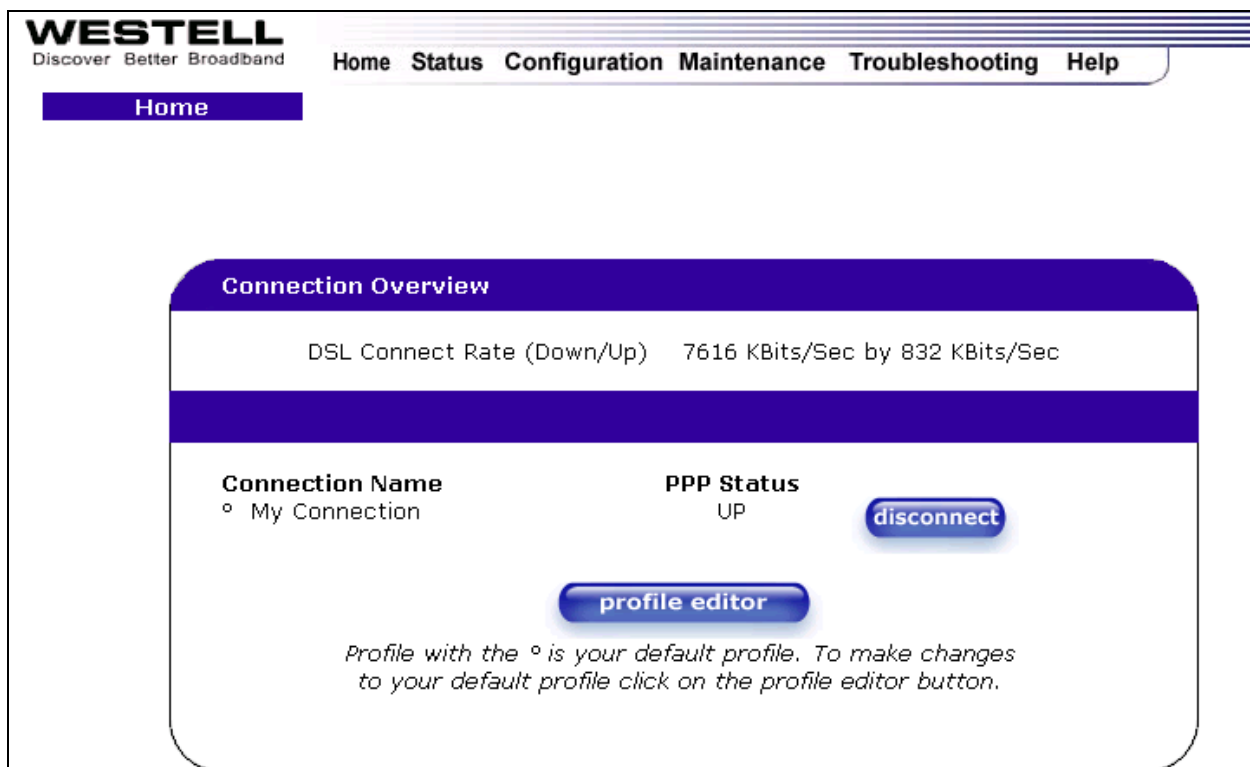
[next](#) [reset](#)

[Help](#)

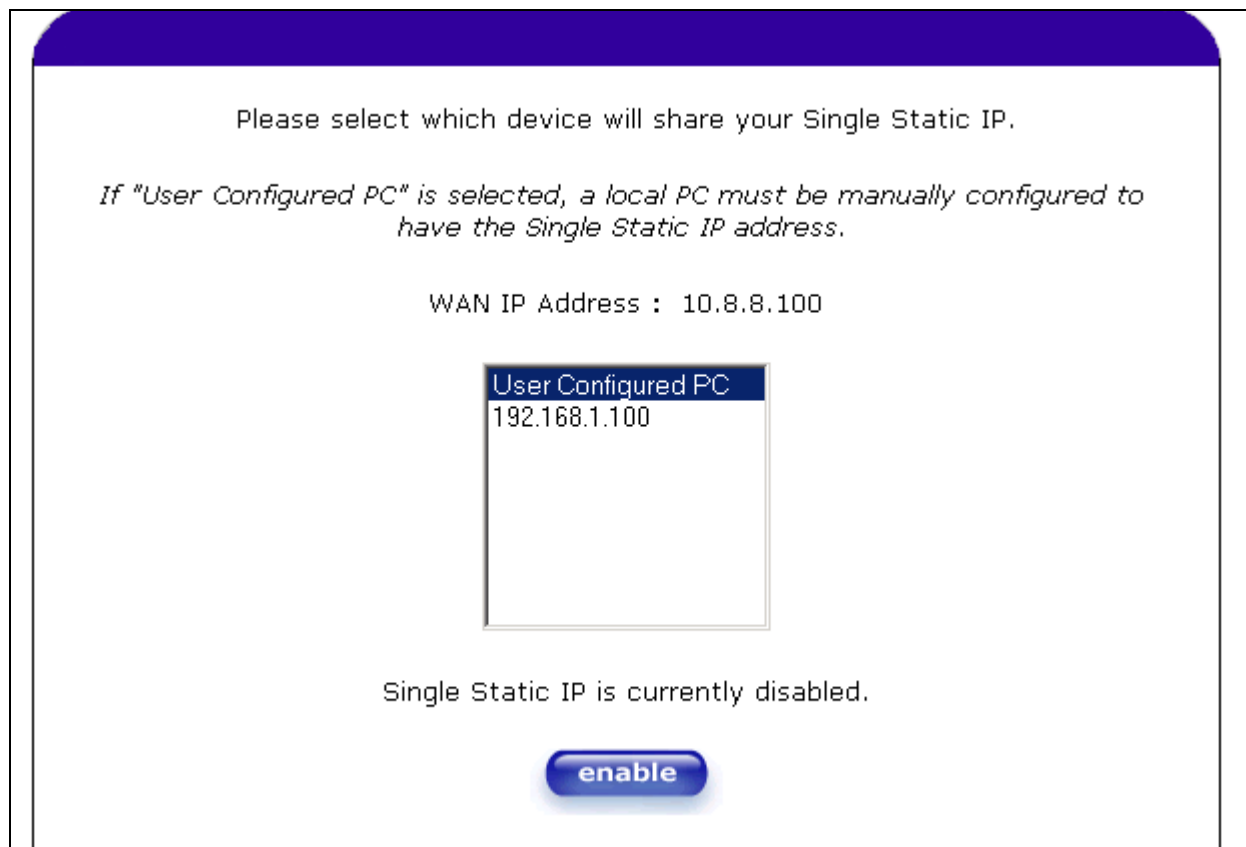
Step 6) Set the Protocol to **PPPoE**. Press **next**.



Step 7) When the Set-up Complete screen appears, press **done**. Browse again to the modem (192.168.1.1) and, if the installation has been done correctly, a screen similar to the following should appear. Note that the connect rate will likely be different than shown below.



Step 8) From the Menu, select **Configuration→Single Static IP Configuration**. Select **User Configured PC** and press **enable**. Press **OK** to confirm, and then **OK** again to reset the modem. This step configures the modem to allow the IP Office to use the “public” IP address as its IP address.



Step 9) Once the status screen shows the connection status as “UP”, the modem has been successfully configured.

6. Configure the Paradyne GrandSLAM

This section describes the Paradyne DSLAM settings needed to support this configuration. The Service Provider would typically do this portion of the configuration.

Connect to the Paradyne system either via the serial port, as described in the installation manual, or telnet to the MCP card IP address.

Step 1) Start at the Main Menu, as shown

Hotwire Chassis
A. Quick Card Select
B. Port Card Select
C. Mgmt. Card Select
D. Managed SN Select
E. Chassis Info
F. Current Users
G. Logout

Step 2) Select **Quick Card Select** to view the system configuration and link status.

Quick Card Select	<noname>
-------------------	----------

Slot	Card	Type	Status	UpLinks	ATM	-----Links-----
M1(9):	8000	MCP	- - -	U		
S1(A) :	8022	SCM	- M -	U		EEEEEE EEEEE EEUEE EEE
S2(B) :	8026	SCM	- M R	D		EEEEEE EEEEE EEUEE EEE
13:	8365	ADSL(12)	- - R		U	UXDXX XXXXX XX

Enter Slot Number to Select a Card:

Goto (M# for MCC or S# for SCM or slot# for DSL or slot#,port# for SN):
Hotwire 8820: MCP: 8000c: - - - U

Step 3) Select the ADSL card of interest (slot 13 in this configuration) by selecting the slot, then **Configuration menu** and then **Physical ports→DSL ports**. At the prompt, enter ‘e’ for edit and then enter the port number. Ensure that the speed settings match the modem settings. Ensure that the Port Status is set to **Enabled** (reset the port if necessary).

DSL Port Configuration		ADSL New	
Port Name: dsl11	Port Status: Enabled		
Line Code: Multimode	Latency: Interleaved	Behavior: Adaptive	
Downstream Speed: kbps	Maximum Downstream Speed: 8000 kbps		
Upstream Speed: kbps	Minimum Downstream Speed: 32 kbps		
	Maximum Upstream Speed: 832 kbps		
	Minimum Upstream Speed: 32 kbps		
Target Margin: 4 dB			
Minimum Margin: 0 dB			
Maximum Margin: 19 dB			
Trap Thresholds: (Upstream/Downstream)			
	Up	Down	
Error Seconds: 120	120	SN Loss of Power: 1	
Severely Error Seconds: 15	15	Link Down Count: 0	
Unavailable Seconds: 1	1		
Link Up/Down Trap: Enable			
Save Changes: no			
Edit			
Status (Enabled/Disabled):			
Slot 13: 8365: U X D X X X X X X X X X			

Step 4) Return to the **Configuration Menu** and select **ATM SWITCH→ATM Traffic Profiles**. For this system “PACKET” is the appropriate profile for Internet access.

ATM Traffic Profiles		ADSL New						
Index	Profile Name	Class	PD	POL	PCR	CDVT	SCR	MBS
0		UBR	N	N	-	-	-	-
Save Changes?: no								
1	PACKET	UBR	Y	N	-	-	-	-
2	VOICE	rt-VBR	N	T	5472	-	188	16
1	PACKET	UBR	Y	N	-	-	-	-
2	VOICE	rt-VBR	N	T	5472	-	188	16
Total Profiles: 2		UBR	Y	N	-	-	-	-
2	VOICE	rt-VBR	N	T	5472	-	188	16
Enter Index (0-Add New Profile, [Uu]-Scroll Up, [Dd]-Scroll Down) :								
Slot 13: 8365: Card Status: _ _ R WAN Status: U								

Step 5) Return to the **Configuration Menu** and select **ATM SWITCH→ATM Cross Connect**. Enter the DSL interface number of interest and ensure that there is an entry with the profile name and note the VPI, VCI and CSN for the next step.

ATM Cross Connect		ADSL New					
Interface Name: dsl1:1							
Index	VPI	VCI	Dnstream Profile	Upstream Profile	Status	CSN	
0					Enable		
Save Changes: no							
1	0	16			Up		
2	0	35	PACKET	PACKET	Up	13S01:000	
3	0	40	VOICE	VOICE	Up	13S01:001	
Total Connections For This Interface: 3							
Available Connections: 250							

Enter(index#, U/D/N, 0 for new cross connect):
Slot 13: 8365: Press ? For Help ...

Step 6) Go back to the **Quick Card Select Menu** and enter **S1** to select the SCM card. Select **Configure→Physical Ports→Uplink Parameters** to navigate to the ATM Physical Uplink. Ensure that the Mode of Operation is set to SONET STS-3c for compatibility with the Cisco 3725 configuration.

Configuration OC3 Uplink Parameters		<noname>
Uplink #: 1		
Line Width:	OC3 155 Mbps	
Line Type:	MMF-2 Km	
Mode of Operation:	SONET STS-3c	
Circuit ID (Line 1):		
(Line 2):		
(Line 3):		
(Line 4):		
(Line 5):		
Transmit Clock:	Local	
Line Status Change		
Trap Enable:	yes	
Cell Scrambling:	yes	

Mode of Operation (SONET STS-3c/SDH STM-1):
Hotwire 8820: SCM-A: 8022: _ M _ U X EEEEE EEEEE EEUEE EEE

Step 7) Return to the Hotwire-SCM Menu and select **Configure→ATM Switch→Traffic Profiles** and check that an Unspecified Bit Rate Profile that matches the needs for Internet access exists. The “PACKET” profile will be used in this configuration.

ATM Traffic Profiles		<noname>						
Index	Profile Name	Class	PD	Pol	PCR	CDVT	SCR	MBS
0		UBR	N	N	-	-	-	-
Save changes? no								
1	PACKET	UBR	Y	N	-	-	-	-
2	RESERVED1	UBR	N	N	-	-	-	-
3	RESERVED2	UBR	N	N	-	-	-	-
4	VOICE	rt-VBR	N	T	5424	-	754	0

Note: The SCM does not perform policing. Policing is performed by the port card.

Enter Index (0 Add New Profile, [Uu] Scroll Up, [Dd] Scroll Down):
Hotwire 8820: SCM-A: 8022: M U X EEEEE EEEEE EEUEE EEE

Step 8) Return to the ATM Switch Menu and select **Cross Connect**. Select **Sorted by Slot**. Enter ‘s’ to search for the slot and then the slot, port and VID corresponding to the Internet Access PVC from the DSL modem. The VID is the third portion of the CSN that was noted in **Step 6**. Set or note the VPI and VCI to be used for the uplink to the Cisco 3725.

Cross Connect Sorted by Slot										<noname>	
Index	-----CSN-----				---Uplink---			-----Profile-----		Status	
	Slot	Type	Port	VID	#	VPI	VCI	Up	Down		
0	0	Stand.	0	0	1	0	0				
Save changes? no											
1	13	Stand.	1	0	1	0	35	PACKET	PACKET	Up	
2											
3											
4											
5											
6											
7											
8											
9											
10											

Max Index: 1 Total Cross Connects: 1
Search Mode Slot: 0 Port: 0 VID: 0 Search? no

Index ('0' for Add Mode, 's' for Search Mode):
Hotwire 8820: SCM-A: 8022: M U X EEEEE EEEEE EEUEE EEE

7. Configure the Cisco 3725 Router

This section describes the configuration of the Cisco 3725 to support DSL modems configured for PPP-over-Ethernet. For reference, this table summarizes the interface configuration. Note that this is a simplified configuration. The Service Provider would typically do this portion of the configuration.

Comments	Cisco Configuration File
For this simple configuration, the user names and passwords for the modem are included in the configuration file. Normally, these would be handled in a database.	<pre> Current configuration : 2075 bytes ! version 12.2 service timestamps debug datetime msec service timestamps log uptime no service password-encryption ! hostname 3725> ! boot system flash c3725-ik9o3s-mz.122-15.ZJ3.bin logging queue-limit 100 enable password cisco ! username avaya password 0 avaya ip subnet-zero ! ! ! ip audit notify log ip audit po max-events 100 vpdn enable ! vpdn-group ipoffice accept-dialin protocol pppoe virtual-template 1 ! mta receive maximum-recipients 0 ! </pre>
The vpdn group is configured to apply virtual template 1 (defined below) to each incoming PPPoE session.	
Interface FastEthernet 0/0 is the interface to the "Internet".	<pre> interface FastEthernet0/0 description "interface to P580" ip address 192.88.1.1 255.255.255.0 duplex auto speed auto lan-name Internet ! ! ! </pre>
Interface ATM2/0 is configured as the interface to the DSLAM.	<pre> interface ATM2/0 no ip address no atm ilmi-keepalive pvc mgmt 0/1 </pre>

A single PVC is configured for each DSL Modem. The PVC VPI/VCI corresponds to the PVC settings of the DSLAM SCM card (which cross-connects from the PVC to the modem). This Virtual Template is applied to each incoming PPPoE session to create a virtual access template with these attributes. The local pool “fast1” is defined to provide the IP address for the DSL router. Simple static routes are used for this configuration to route most traffic to the Avaya P580.	<pre> ! ! interface ATM2/0.1 point-to-point pvc data 0/35 encapsulation aal5snap protocol pppoe ! ! interface Virtual-Template1 mtu 1492 ip address 10.8.8.1 255.255.255.0 no ip route-cache same-interface peer default ip address pool fast1 ppp authentication chap ! ip local pool fast1 10.8.8.100 no ip http server no ip http secure-server ip classless ip route 0.0.0.0 0.0.0.0 192.88.1.2 ip route 192.16.20.0 255.255.255.0 192.88.1.2 ip route 192.16.200.0 255.255.255.0 192.88.1.2 ! end </pre>
---	---

8. Configure the Avaya P580 Switch

This section describes the essential steps to configure the P580.

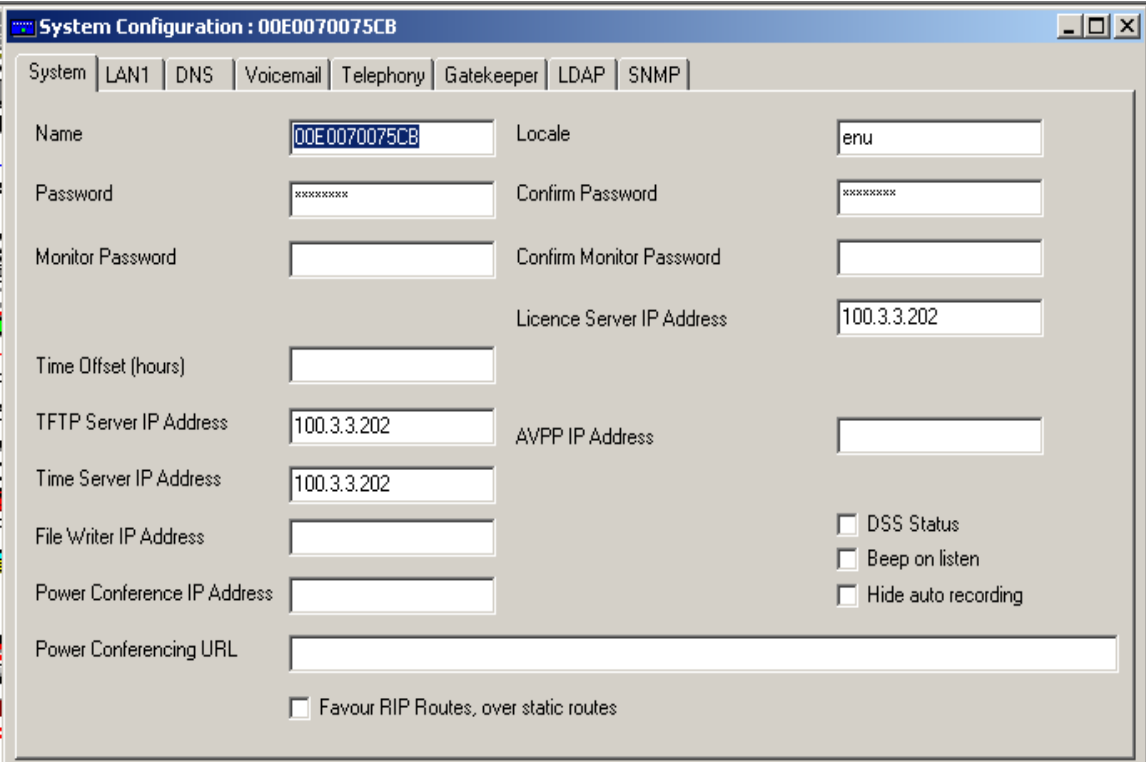
Comments	Avaya P580 Configuration File
The vlans are created for connection to the cisco 3725 (vlan 88), the pseudo-public internet (vlan 20) and the IP 403 (vlan 200). Ports are assigned to the VLANs. Router Interfaces are created for each VLAN.	<pre> ! ! Avaya Cajun Switch Agent v6.0.0 Cajun Switch ! set vlan 88 name "tocisco" set vlan 20 name "VLAN020" set vlan 200 name "VLAN0200" ! set port vlan 4/1 88 set port vlan 4/12 200 set port vlan 4/19 20 ! interface "vlan0020" ip address 192.16.20.1 255.255.255.0 ip vlan name "VLAN0020" ! </pre>

A static route is established to reach the public IP address endpoints on the cisco 3725.	<pre> interface "VLAN 88" ip address 192.88.1.2 255.255.255.0 ip vlan name "tocisco" ! interface "ip403 -192.16.200" ip address 192.16.200.1 255.255.255.0 ip vlan name "VLAN0200" ! ip route 10.8.8.0 255.255.255.0 192.88.1.1 1 low ! </pre>
--	--

9. Configure the Avaya IP403 Office Server

This section describes the configuration steps needed to configure the IP403 Office, which has only one physical LAN interface. A “Logical LAN” interface is used for communication to the next hop router.

Step 1) Access the IP Office Configuration Menu. Select **System→System** and ensure that the License and Time Server entries are set appropriately.



System Configuration : 00E0070075CB

System | LAN1 | DNS | Voicemail | Telephony | Gatekeeper | LDAP | SNMP

Name: 00E0070075CB Locale: enu

Password: [masked] Confirm Password: [masked]

Monitor Password: [] Confirm Monitor Password: []

Licence Server IP Address: 100.3.3.202

Time Offset (hours): []

TFTP Server IP Address: 100.3.3.202 AVPP IP Address: []

Time Server IP Address: 100.3.3.202

File Writer IP Address: []

Power Conference IP Address: []

Power Conferencing URL: []

☐ DSS Status

☐ Beep on listen

☐ Hide auto recording

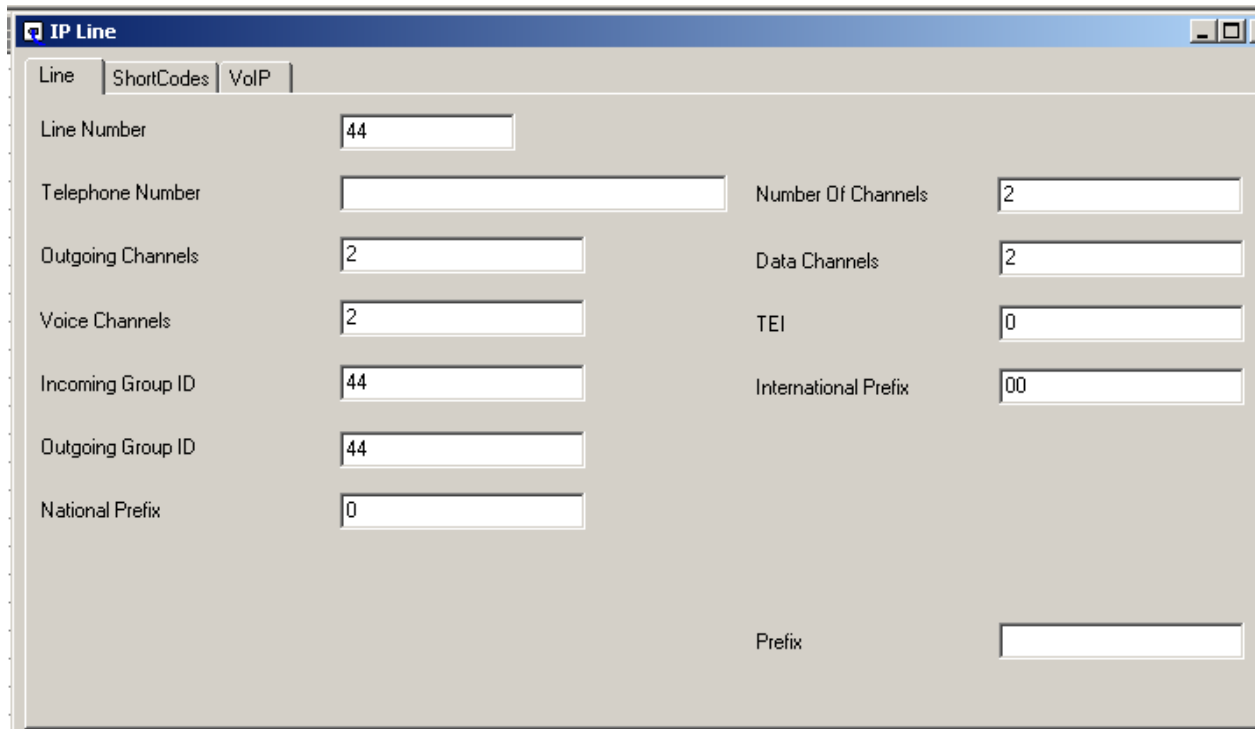
☐ Favour RIP Routes, over static routes

Step 2) Select **System** and the **LAN1** tab. Set the IP address and IP Mask of the physical LAN interface as desired.

The screenshot shows a web-based configuration interface for a device. The title bar reads "System Configuration : 00E0070075CB". Below the title bar is a tabbed menu with the following tabs: System, LAN1, DNS, Voicemail, Telephony, Gatekeeper, LDAP, and SNMP. The "LAN1" tab is currently selected. The main configuration area contains the following fields and options:

- IP Address:** A text box containing "100.3.3.150".
- IP Mask:** A text box containing "255.255.255.0".
- Number Of DHCP IP Addresses:** A text box containing "200".
- DHCP Mode:** A group box containing four radio buttons: "Server", "Disabled" (which is selected), "Dialin", and "Client".
- RIP Mode:** A group box containing five radio buttons: "None" (which is selected), "Listen Only (Passive)", "RIP 1", "RIP 2 Broadcast (RIP 1 Compatibility)", and "RIP 2 Multicast".

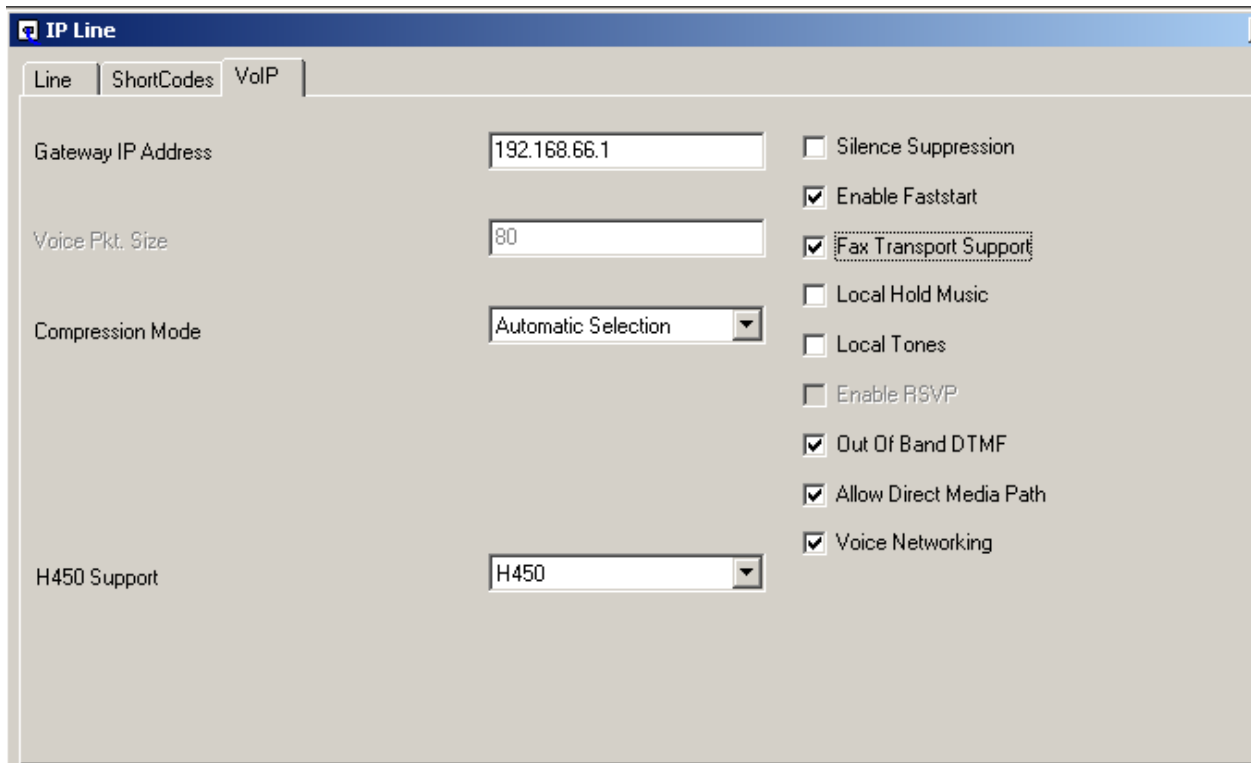
Step 3) From **Line**, create a Line for traffic to the Small Office. The number of channels should be the same as the corresponding entry on the Small Office.



The image shows a software window titled "IP Line" with three tabs: "Line", "ShortCodes", and "VoIP". The "Line" tab is selected. The window contains several input fields for configuring a line. The "Line Number" field is set to "44". The "Telephone Number" field is empty. The "Number Of Channels" field is set to "2". The "Outgoing Channels" field is set to "2". The "Data Channels" field is set to "2". The "Voice Channels" field is set to "2". The "TEI" field is set to "0". The "Incoming Group ID" field is set to "44". The "International Prefix" field is set to "00". The "Outgoing Group ID" field is set to "44". The "National Prefix" field is set to "0". There is also a "Prefix" field at the bottom right which is empty.

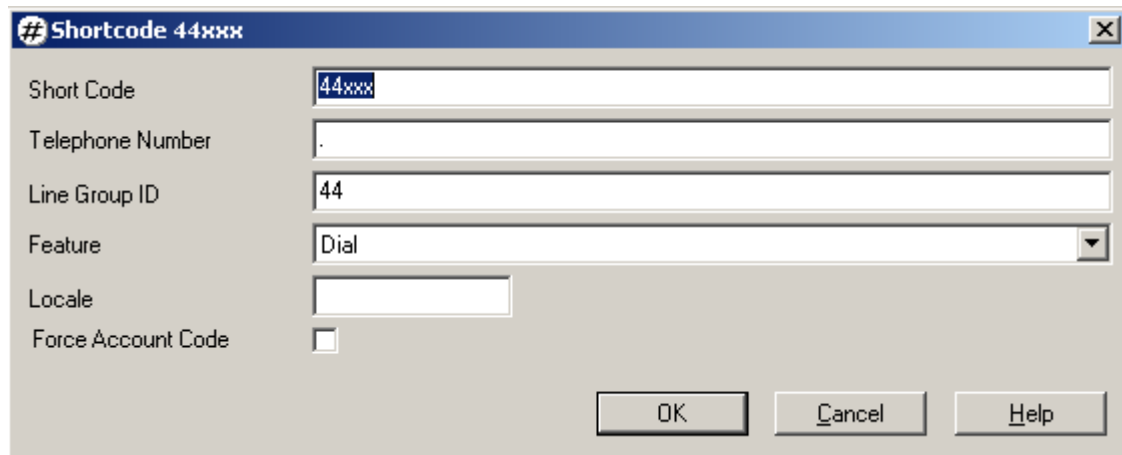
Field	Value
Line Number	44
Telephone Number	
Number Of Channels	2
Outgoing Channels	2
Data Channels	2
Voice Channels	2
TEI	0
Incoming Group ID	44
International Prefix	00
Outgoing Group ID	44
National Prefix	0
Prefix	

Step 4) Select the **Line→VoIP** tab to enter the Small Office LAN1 (Private Side) IP Address.



The image shows a software window titled "IP Line" with three tabs: "Line", "ShortCodes", and "VoIP". The "VoIP" tab is selected. The window contains several configuration fields and checkboxes. On the left, there are four fields: "Gateway IP Address" with the value "192.168.66.1", "Voice Pkt. Size" with the value "80", "Compression Mode" with a dropdown menu showing "Automatic Selection", and "H450 Support" with a dropdown menu showing "H450". On the right, there are seven checkboxes: "Silence Suppression" (unchecked), "Enable Faststart" (checked), "Fax Transport Support" (checked), "Local Hold Music" (unchecked), "Local Tones" (unchecked), "Enable RSVP" (unchecked), and "Out Of Band DTMF" (checked). Below these, there are two more checkboxes: "Allow Direct Media Path" (checked) and "Voice Networking" (checked).

Step 5) Create a Shortcode to route voice calls to the Small Office.



The image shows a software window titled "# Shortcode 44xxx" with a close button (X) in the top right corner. The window contains several configuration fields and a checkbox. On the left, there are five fields: "Short Code" with the value "44xxx", "Telephone Number" with a single dot ".", "Line Group ID" with the value "44", "Feature" with a dropdown menu showing "Dial", and "Locale" with an empty text box. Below these, there is a checkbox labeled "Force Account Code" which is unchecked. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

Step 6) Establish the **Logical LAN** as follows:

- a) From the Configuration Menu, Select **Logical LAN**, move the mouse pointer to the right hand pane, and right click to select **New**.
- b) Give the Logical LAN a unique name and enter the IP Address and IP Mask of the IP Office interface to the Router.
- c) Enter the Gateway IP Address and Gateway MAC Address. The MAC address is critical and must be the Avaya P580 MAC address in this configuration. If the IP403 Office had been connected to a DSL router, this would have been the MAC address of the DSL router. One method to get the MAC address is to “ping” the router interface from a PC, then run the PC *arp -a* command to see the MAC address that corresponds to the IP Address.

Logical LAN- ISP

Logical LAN

Name: ISP

IP Address: 192.16.200.7

IP Mask: 255.255.255.0

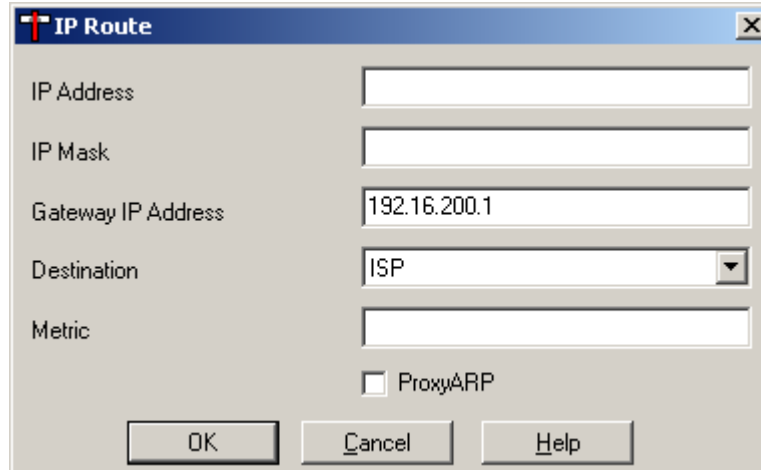
Gateway IP Address: 192.16.200.1

Gateway MAC Address: 00306db0fcc7

Firewall Profile: [Dropdown Menu]

Enable NAT: ☒

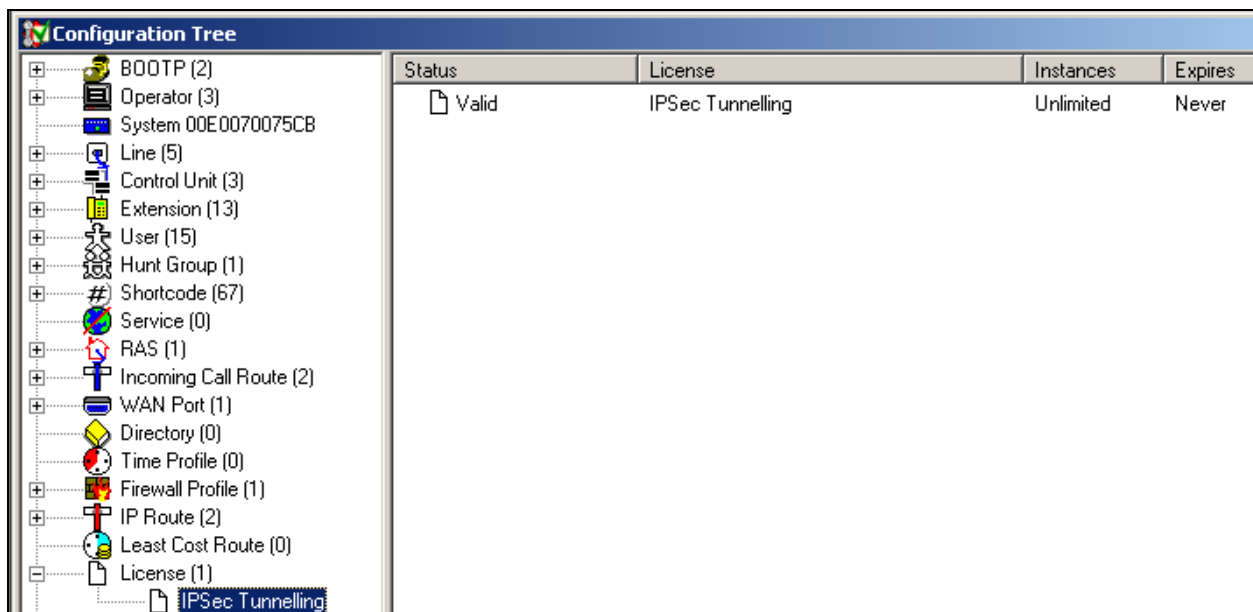
Step 7) Create a route to forward packets to the Avaya P580 switch.



The IP Route configuration dialog box contains the following fields and controls:

- IP Address: [Empty text box]
- IP Mask: [Empty text box]
- Gateway IP Address: 192.16.200.1
- Destination: ISP (dropdown menu)
- Metric: [Empty text box]
- ☐ ProxyARP
- Buttons: OK, Cancel, Help

Step 8) From **License**, ensure that a valid license is entered for the IPSec Tunnel.

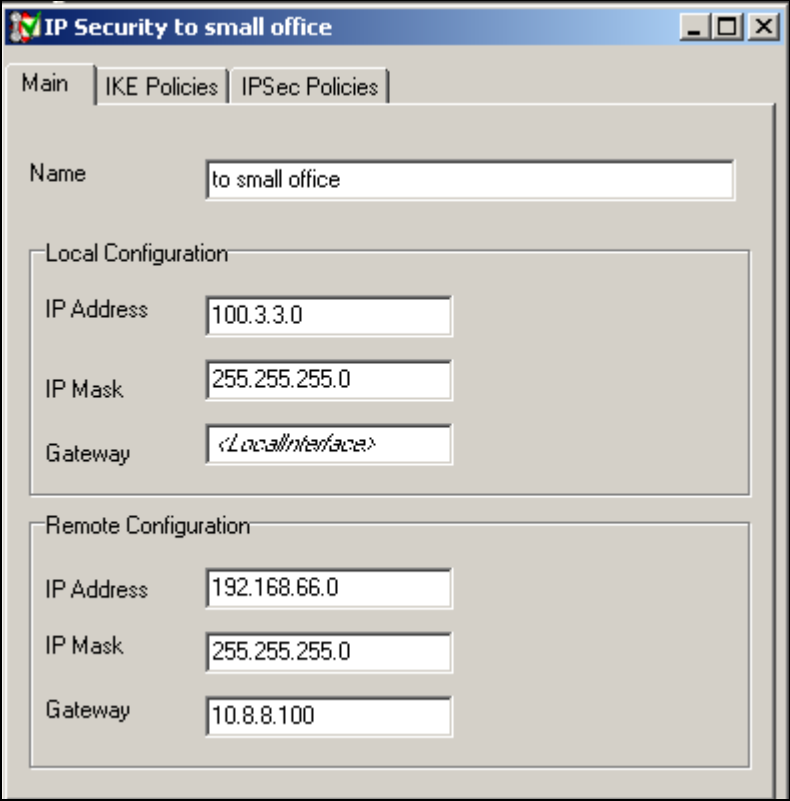


The Configuration Tree on the left lists various system components. The table on the right displays the license information for the selected 'IPSec Tunnelling' component.

Status	License	Instances	Expires
Valid	IPSec Tunnelling	Unlimited	Never

Step 9) From **Tunnel**, create an IP Sec Tunnel.

- a) Enter the IP403 Office LAN1 IP address and mask as the Local Configuration **IP Address** and **IP mask**. Enter the Small Office LAN1 address and mask as the remote configuration **IP Address** and **IP mask**. Enter the Small Office public IP address (LAN2) as the Remote Configuration **Gateway**.



IP Security to small office

Main | IKE Policies | IPSec Policies

Name: to small office

Local Configuration

IP Address: 100.3.3.0

IP Mask: 255.255.255.0

Gateway: <LocalInterface>

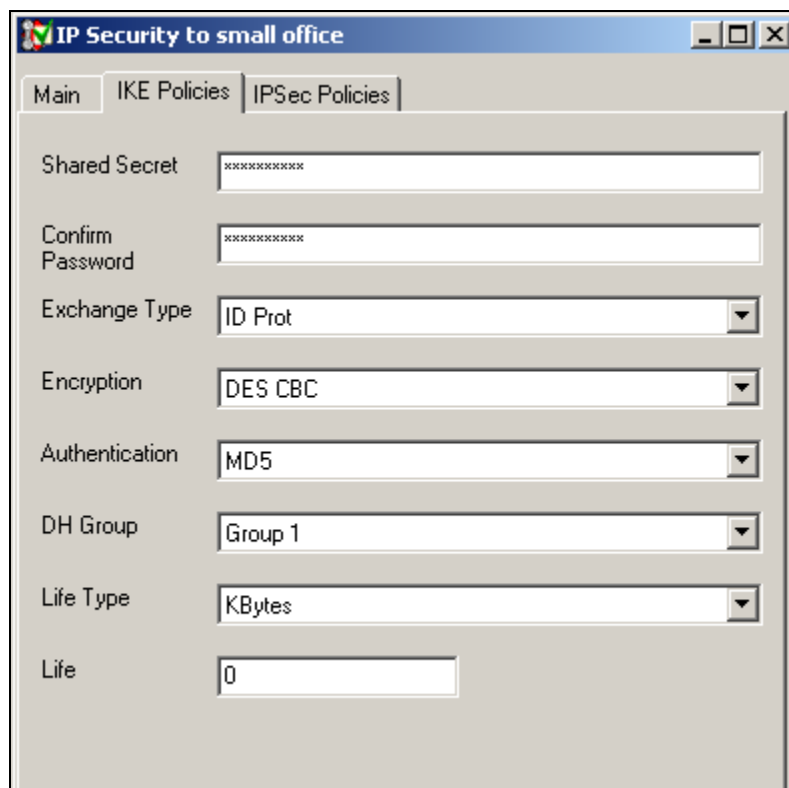
Remote Configuration

IP Address: 192.168.66.0

IP Mask: 255.255.255.0

Gateway: 10.8.8.100

- b) Select the **IKE Policies** tab and ensure that the settings, particularly the shared secrets, are the same as administered for the Small Office.



The screenshot shows a window titled "IP Security to small office" with three tabs: "Main", "IKE Policies", and "IPSec Policies". The "IKE Policies" tab is selected. The settings are as follows:

Field	Value
Shared Secret	xxxxxxxx
Confirm Password	xxxxxxxx
Exchange Type	ID Prot
Encryption	DES CBC
Authentication	MD5
DH Group	Group 1
Life Type	KBytes
Life	0

- c) Select the **IPSec Policies** tab and ensure that the settings are the same as for the Small Office.

IP Security to small office

Main | IKE Policies | **IPSec Policies**

PFS ☐

Protocol ESP

Encryption DES

Authentication HMAC MD5

DH Group Group 1

Life Type KBytes

Life 0

Step 10) Save this configuration to the IP403 Office.

10. Verification Steps

This section describes steps that can be taken to verify that the configuration has been done correctly.

Verification 1 - ADSL status

To verify the DSL Modem ADSL status, navigate to **Status→Connection Summary**. Verify that the IP Network Address is the public address that has been assigned to the IP Office. If the connection is not in the “UP” state, proceed to Verification 2, then Verification 4.

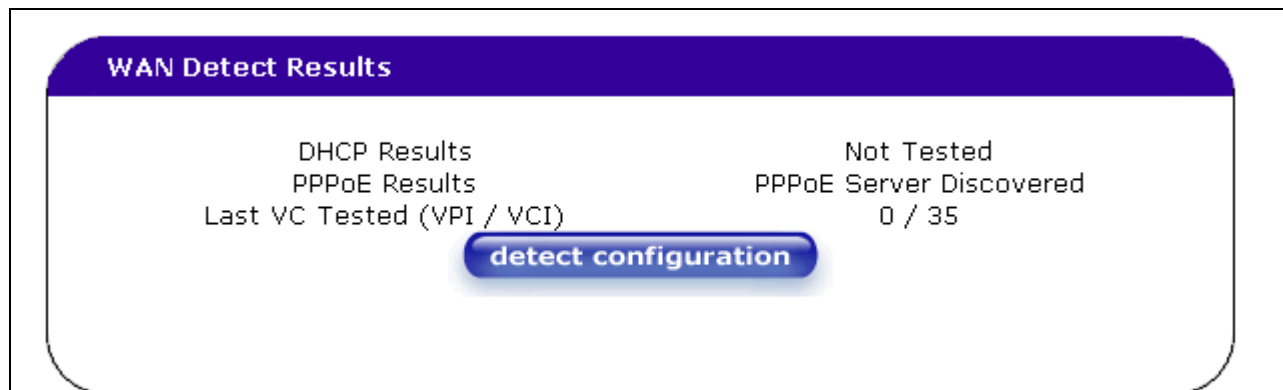
DSL Connection Information				
Connection Rate	(Down/Up):	7616 KBits/Sec by 832 KBits/Sec		
Connection Status	In Packets	2908		
	Out Packets	6625		
IP Network Address	PPP	10.8.8.100		
	Primary DNS	Unavailable		
	Secondary DNS	Unavailable		
Ethernet Status	In Packets	7123		
	Out Packets	3278		
ATM NetworkAddress	VPI	0		
	VCI	35		
Firewall Status	Passed	In: 0	Out: 0	
	Dropped	In: 0	Out: 0	
Connection Information				
Connection Name	Connection Duration	Status	Number of Reconnects	
My Connection	14:53:46	UP	0	

Verification 2 – Modem Training State

If the ADSL Modem DSL light is not on steady, the modem has not “trained” with the Network DSLAM. This is most likely an installation issue (e.g., wiring) and must be resolved before the ATM and PPPoE protocols will become operational.

Verification 3 - WAN Setting Detection

If the DSL light is steady but there is doubt as to the required WAN settings, select **Configuration→Detect WAN Configuration** to detect the WAN parameters.



Verification 4 – Virtual Circuit settings

Verify the configuration settings by navigating first to **Configuration→VC Configuration**. Ensure that the Status is set to **Enable** and the VPI/VCI settings are correct.

Status	VPI	VCI	Protocol	
Enable	0	35	PPPoE	edit
Disable	0	36	Bridge	edit
Disable	0	37	Bridge	edit
Disable	0	38	Bridge	edit
Disable	0	39	Bridge	edit
Disable	0	40	Bridge	edit
Disable	0	41	Bridge	edit

Bridge Broadcast

☒

Bridge Multicast

☒

Spanning Tree Protocol

☐

Select **edit** to view or change the PVC parameters.

VC 1 Configuration

VPI

0

VCI

35

PCR

100

QoS

UBR

Protocol

PPPoE

Status

Enabled

VC 1 - PPPoE Settings

IP Address

0.0.0.0

Gateway

0.0.0.0

DNS Primary

0.0.0.0

DNS Secondary

0.0.0.0

Subnet Mask

MRU Negotiation

☐

LCP Echo Disable

☐

LCP Echo Failures

6

"Must be between 1 and 30 inclusive."

LCP Echo Duration

60

"Must be between 5 and 300 seconds inclusive"

LCP Echo Duration

60

"Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration."

LCP Echo Retry Duration

10

"Must be between 5 and 300 seconds inclusive."

Tunneling

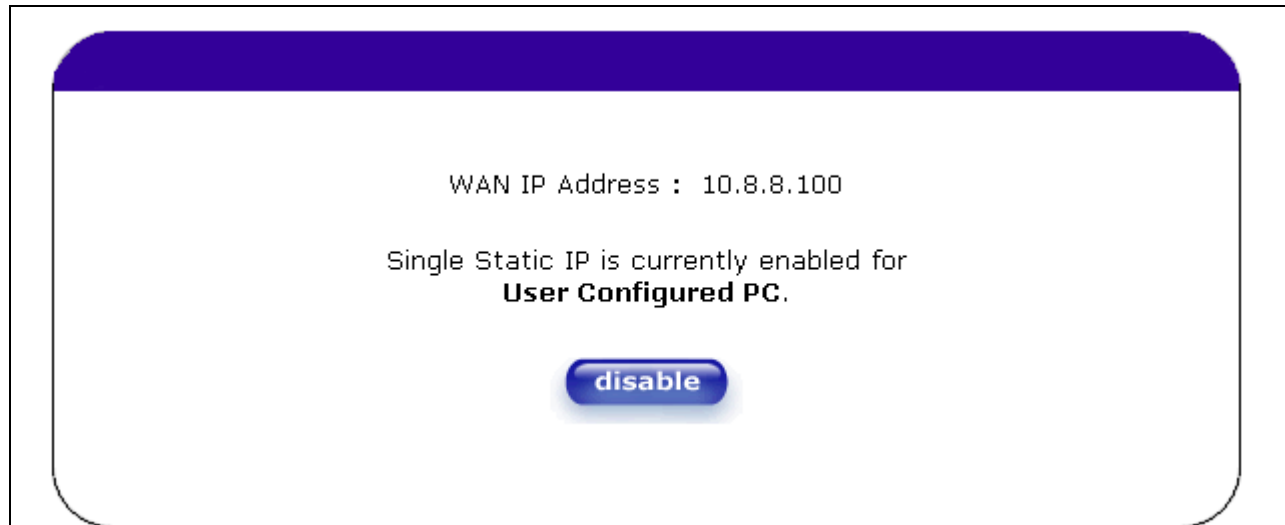
☒ Enable ☐ Disable

set VC

cancel

Verification 5– Single Static IP status

Check that the Single Static IP address that has been assigned to the Modem is set to be shared with the IP office by selecting **Configuration→Single Static IP Configuration**.



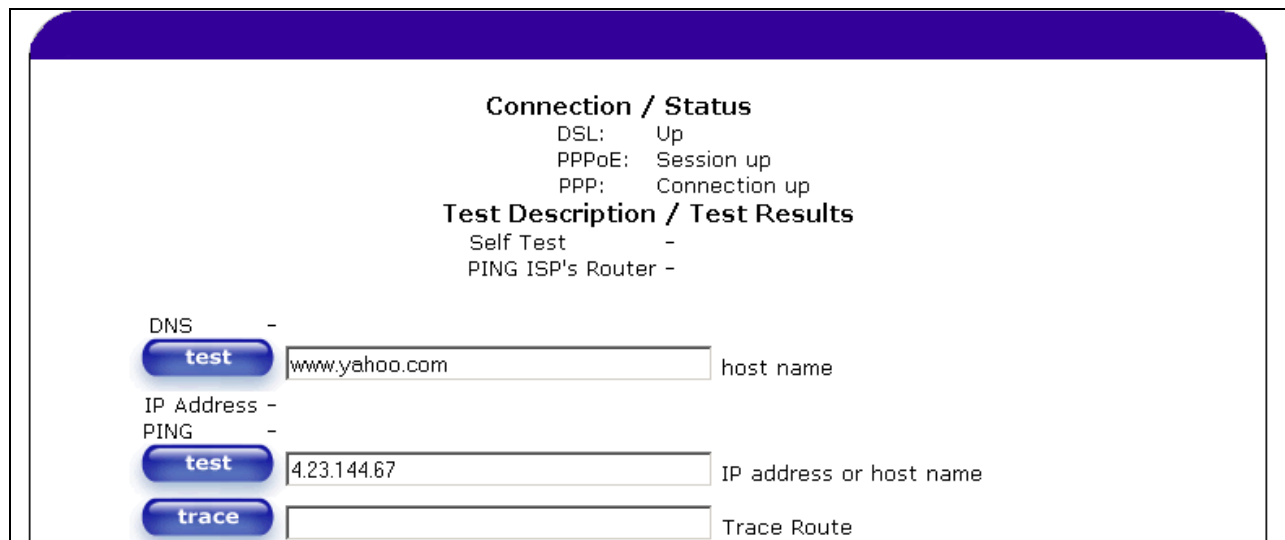
WAN IP Address : 10.8.8.100

Single Static IP is currently enabled for
User Configured PC.

disable

Verification 6– modem ping

Select **Troubleshooting→System Self Tests** to view the overall status and execute ping tests.



Connection / Status
DSL: Up
PPPoE: Session up
PPP: Connection up

Test Description / Test Results
Self Test -
PING ISP's Router -

DNS -
test host name

IP Address -
PING -
test IP address or host name

trace Trace Route

Verification 7 - ADSL verification from the DSLAM side

From the “Hotwire-DSL” menu for the card in question, select **Monitoring→Physical Ports→Active List**. The port should show “In-use”. If the port is in the Training/Dormant state and configuration is otherwise complete, there may be a break in the wiring.

Active Ports List			ADSL New	
Num	Name	Status		
1	dsl1	In-use		
2	dsl2	Training/Dormant		
3	dsl3	Disconnected		
4	dsl4	Training/Dormant		
5	dsl5	Training/Dormant		
6	dsl6	Training/Dormant		
7	dsl7	Training/Dormant		
8	dsl8	Training/Dormant		
9	dsl9	Training/Dormant		
10	dsl10	Training/Dormant		
11	dsl11	Training/Dormant		
12	dsl12	Training/Dormant		
Top Entry#:			Total Entries: 12	
Select top entry (#, U, D):				
Slot 13: 8365: Press ? For Help ...				

Verification 8 - PPP “callers” from the Cisco 3725.

To see which IP addresses have been assigned or to see which Virtual Interface is associated with a user, use the **show caller** command.

3725>#show caller				
Line	User	Service	Active Time	Idle Time
vtty 106	-	VTY	00:04:01	00:00:00
Vi1.1	avaya	PPPoE	00:37:03	00:00:00

Verification 9 - Virtual Interface Status

The status of the Cisco Virtual Interfaces associated with the ATM PVCs can be seen with the **show vpdn** and **show interface** commands.

```
3725>#show vpdn

%No active L2TP tunnels

%No active L2F tunnels

%No active PPTP tunnels

PPPoE Tunnel and Session Information Total tunnels 1 sessions 1

PPPoE Session Information
UID  SID  RemMAC      OIntf      Intf  Session
      LocMAC      VASt      state
16   16   0060.0fed.9098 ATM2/0.1    Vi1.1  CNCT_PTA
      000e.38b6.6d20 VP/VC: 0/35  UP
3725>#
```

The show interface command provides more detail, including the PPP protocol state.

```
3725>#show interface vi1.1
Virtual-Access1.1 is up, line protocol is up
Hardware is Virtual Access interface
Internet address is 10.8.8.1/24
MTU 1492 bytes, BW 100000 Kbit, DLY 100000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP
PPPoE vaccess, cloned from Virtual-Template1
PPPoE Bound to ATM2/0.1 VCD: 2, VPI: 0, VCI: 35
  301 packets input, 19639 bytes
  155 packets output, 3965 bytes
Last clearing of "show interface" counters never
```

Verification 10 – IP Office VPN Verifications

Basic steps for verifying IP Office include:

- Ping the public IP address of each IP Office from a PC on the private side of each IP Office.
 - The pings must succeed before higher-level protocols (e.g., VPNs) can work. If there is difficulty, check the IP Office “IP route” and LAN interface

- configurations. Use the verification steps to verify the ADSL modem operation (e.g., can a ping from the ADSL modem succeed to the far end?)
- Run ping with the “-t” option. If the reply times vary or there are many timeouts, voice quality may suffer.
 - Ping the private IP address of each IP Office from a PC on the private side of each IP Office.
 - These pings must succeed before the H.323 calls will succeed. Check all VPN settings including that the Licenses are valid in each IP Office.
 - If the pings succeed, place voice calls between the sites. Use the System Monitor with the H.323 trace settings enabled to see if the H.323 setup message makes it from one site to the other. If not, check the VPN line and short code configurations.

11. Conclusion

By following the steps of these Application Notes, a user will have successfully configured IP Office for Internet access and VPN operations across a DSL network.

Please Note: This configuration is based on common methods of Internet access and transport and, as such, includes no provisions for cross-network Quality of Service. Thus, packets can be lost and delayed to an extent that impacts callers’ perception of call quality. Many acceptable calls can be made, but there can be instances of noticeable echo, gaps in speech fidelity and even dropped calls.

12. Additional References

Avaya product information and similar Application Notes can be found at www.avaya.com

For Paradyne product information, visit www.paradyne.com:

“Hotwire ATM Line Cards Models 8335, 8365 and 8385” Users Guide”, Document No:8335-A2-GB20-80, January 2004.

“Hotwire Shelf Concentration Module (SCM) Card User’s Guide”, Document No. 8021-A2-GB20-40

For Westell product information, visit www.westell.com.

Many DSL resource documents are available from www.dslforum.org,

12.1. Glossary

AAL5	ATM Adaptation Layer 5
ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
DSL	Digital Subscriber Line Access Multiplexer
DSLAM	Digital Subscriber Line
LAN	Local Area Network
LLC	Logical Link Control
NAT	Network Address Translation
OC	Optical Carrier
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PVC	Permanent Virtual Circuit
SONET	Synchronous Optical Network
UBR	Unspecified Bit Rate
VCI	Virtual Circuit Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network

©2004 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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