



Avaya Solution & Interoperability Test Lab

Configuring Cisco VPN Concentrator to Support Avaya VPNremote Phones – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Cisco VPN 3020 Concentrator to support IPSec tunnel termination and XAUTH authentication of the Avaya VPNremote Phone.

TABLE OF CONTENTS

1. INTRODUCTION.....	3
1.1. AVAYA VPNREMOTE PHONE STARTUP EVENTS	4
2. NETWORK TOPOLOGY	4
3. EQUIPMENT AND SOFTWARE VALIDATED.....	6
4. CISCO VPN 3020 CONCENTRATOR CONFIGURATION	7
4.1. ACCESS	7
4.2. SAVE CONFIGURATION	9
4.3. ETHERNET INTERFACES.....	10
4.4. DEFAULT GATEWAY	13
4.5. AUTHENTICATION SERVER.....	16
4.6. SECURITY ASSOCIATIONS.....	17
4.7. USER GROUP	22
4.8. IP ADDRESS POOLS	29
4.9. USER ACCOUNTS.....	34
4.10. NETWORK LISTS.....	39
4.11. WELCOME BANNER SCRIPT.....	41
5. AVAYA VPNREMOTE PHONE CONFIGURATION.....	42
5.1. VPNREMOTE PHONE FIRMWARE.....	42
5.2. CONFIGURING AVAYA VPNREMOTE PHONE	42
6. AVAYA COMMUNICATION MANAGER CONFIGURATION	45
6.1. VPNREMOTE PHONE ADMINISTRATION	45
6.2. IP CODEC SETS CONFIGURATION	46
6.3. IP NETWORK MAP CONFIGURATION	47
6.4. IP NETWORK REGIONS CONFIGURATION.....	47
7. VERIFICATION.....	49
7.1. VPNREMOTE PHONE QTEST	49
7.2. VPNREMOTE PHONE IPSEC STATISTICS.....	50
7.3. VPN CONCENTRATOR LOGGING	50
7.4. VPN CONCENTRATOR ACTIVE SESSIONS.....	52
7.5. VPN CONCENTRATOR IPSEC STATISTICS	53
8. TROUBLE SHOOTING	54
8.1. INCORRECT USER NAME	54
8.2. INCORRECT USER PASSWORD.....	54
8.3. INCORRECT GROUP NAME.....	55
8.4. INCORRECT PRE-SHARED KEY	55
8.5. MISMATCHED PHASE 1 PROPOSAL	56
8.6. MISMATCHED PHASE 2 PROPOSAL	56
8.7. NO IP POOL ADDRESSES AVAILABLE.....	57
8.8. GRACEFUL REBOOT OF VPNREMOTE PHONE	58
9. CONCLUSION.....	58
10. REFERENCES	59

1. Introduction

These Application Notes describe the steps to configure the Cisco VPN 3020 Concentrator to support IPSec tunnel termination and XAUTH authentication of the Avaya VPNremote Phone.

The Avaya VPNremote Phone is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya IP 4600 Series Telephone. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. End users experience the same IP telephone features as if they were using the telephone in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Release 2 of the Avaya VPNremote Phone firmware, used in these Application Notes, extends the support of head-end VPN gateways to include Cisco security platforms. The configuration steps described in these Application Notes utilize a Cisco VPN 3020 Concentrator. However, these configuration steps can be applied to other Cisco VPN 3000 Concentrator models using the software version specified in **Table 1**.

The Avaya VPNremote Phone utilizes the Internet Key Exchange (IKE) protocol, Extended Authentication (XAUTH) and pre-shared key for IPSec tunnel establishment and authentication with the Cisco VPN Concentrator. XAUTH allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. The VPNremote Phone uses the pre-shared key to authenticate with the Cisco VPN Concentrator and create a temporary secure path to allow the VPNremote Phone end user to present credentials to the Cisco VPN Concentrator. After user authentication is successful, the VPN Concentrator sends an IP address from a pre-configured IP Address Pool, the IP address of the DNS server and the Welcome Banner.

1.1. Avaya VPNremote Phone Startup Events

The steps shown in **Figure 1** below describe the high level events that take place during the startup of a VPNremote phone. The focus of these Application Notes is on the configuration of the Avaya VPNremote Phone and the Cisco VPN 3020 Concentrator functioning as the IPSec VPN head-end.

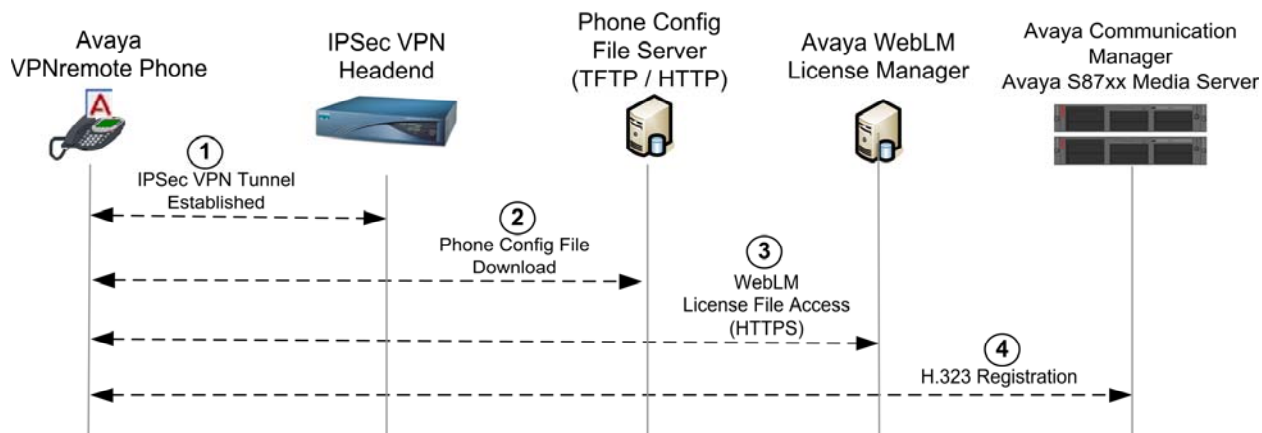


Figure 1: VPNremote Phone Startup Events

1. The VPNremote Phone establishes an IPSec VPN tunnel upon boot up with the designated IPSec VPN head-end.
2. The VPNremote Phone initiates a TFTP or HTTP session with the phone configuration file server for configuration file download. (46vpnupgade.scr, 46vpnsetting.txt, 46xxsettings.txt)
3. The VPNremote Phone initiates an HTTPS session with the WebLM server. The VPNremote Phone's WebLM client communicates with the WebLM server to request a license. The WebLM server verifies the request, confirms the license count will not be exceeded and grants a license.
4. The VPNremote Phone registers with Avaya Communication Manager and is ready for service.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 2**. The Main Campus location contains the Cisco VPN Concentrator functioning as perimeter security device and VPN head-end. The Avaya S8710 Media Server and Avaya G650 Media Gateway are also located at the Main Campus. The Main Campus is mapped to **IP Network Region 1** in Avaya Communication Manager.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the Cisco VPN Concentrator. The Cisco VPN Concentrator will assign IP addresses to the VPNremote Phones. The assigned IP addresses, also known as the inner addresses, will be used by the VPNremote Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya Communication Manager.

Avaya Communication Manager maps the VPNremote Phones to the appropriate IP Network Region using this inner IP address and applies the IP Network Region specific parameters to the VPNremote Phone. In these Application Notes, the G.729 codec with three 10ms voice samples per packet is assigned to the VPNremote Phones.

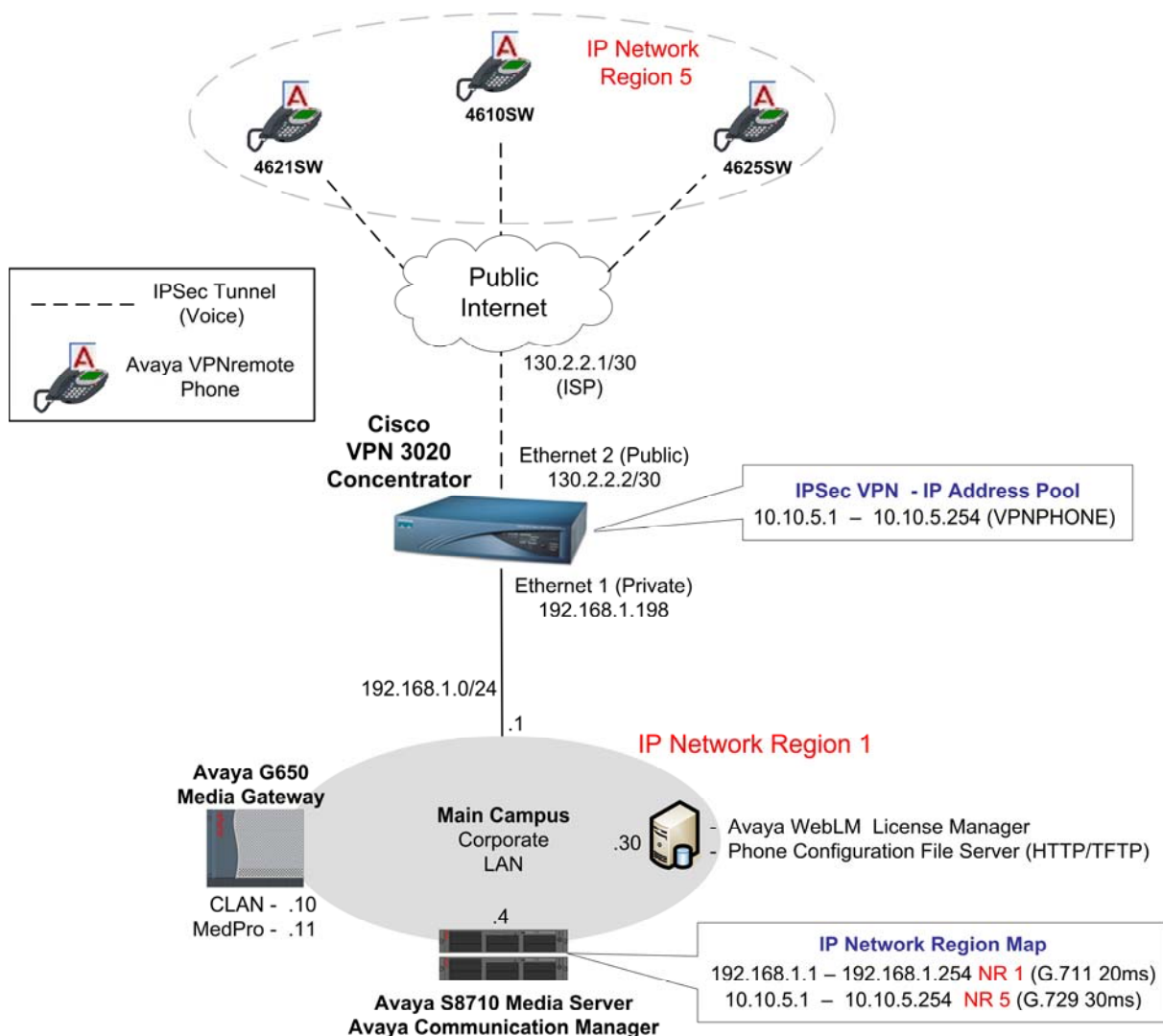


Figure 2: Network Diagram

3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Equipment	Software Version
Avaya S8710 Media Server	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway C-LAN (TN799DP) MedPro (TN2302AP)	FW 016 (HW1) FW 108 (HW12)
Avaya 4610SW IP Telephones	R2.3.2 – Release 2 (a10bVPN232_1.bin)
Avaya 4621SW IP Telephones	R2.3.2 – Release 2 (a20bVPN232_1.bin)
Avaya 4625SW IP Telephones	R2.5.2 – Release 2 (a25VPN252_1.bin)
Cisco VPN 3020 Concentrator	4.7.1 (vpn3000-4.7.1.Rel-k9.bin)

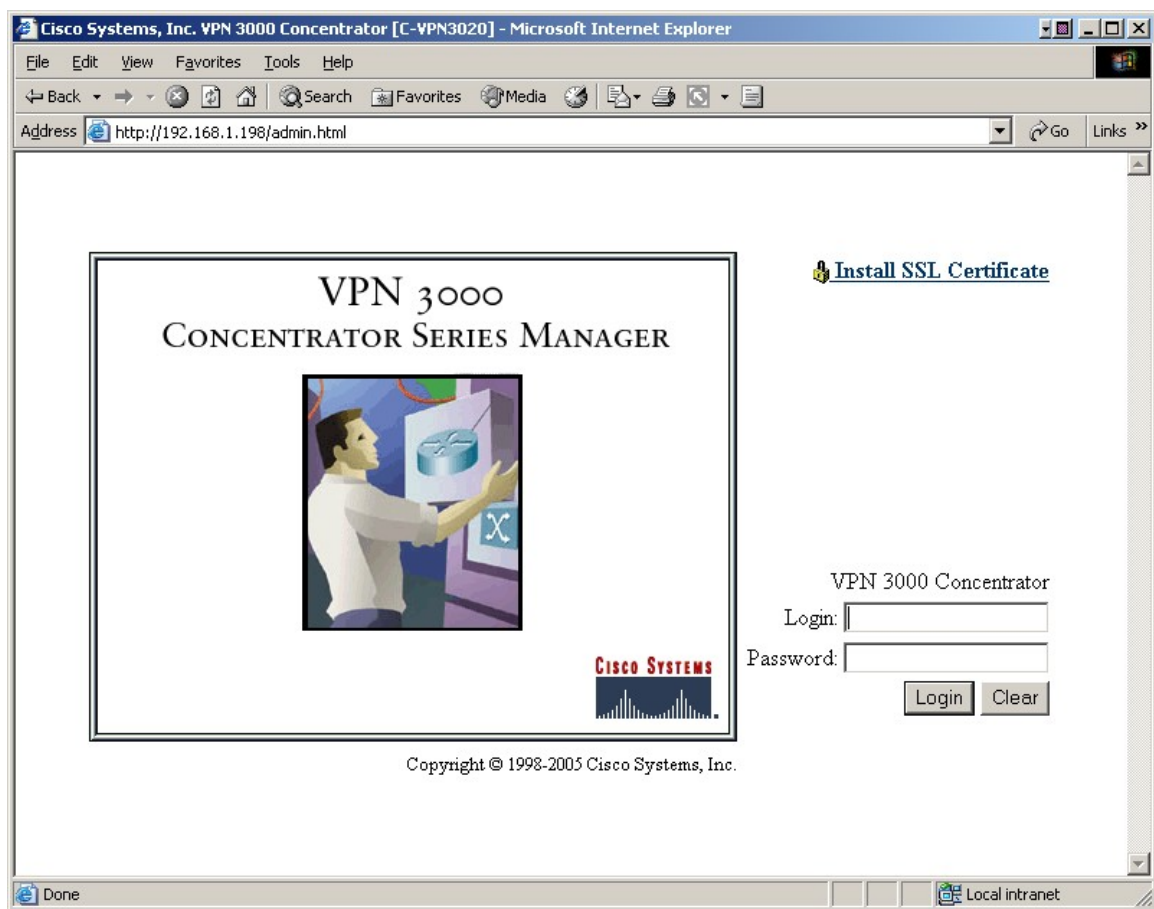
Table 1 – Equipment Version Information

4. Cisco VPN 3020 Concentrator Configuration

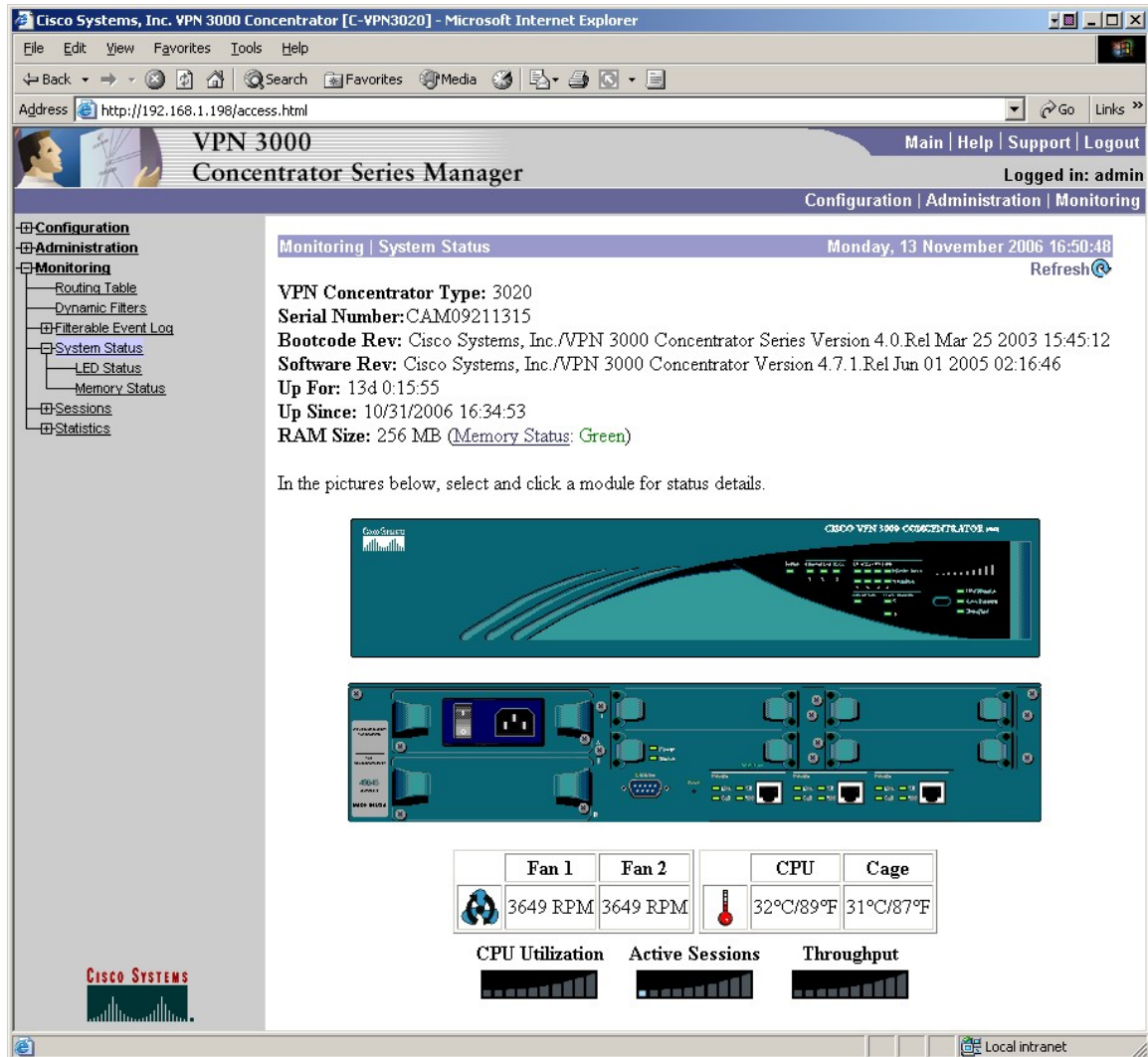
4.1. Access

These Application Notes assume the Cisco VPN 3020 Concentrator “Quick Configuration” steps have been performed to configure the Ethernet 1 (Private) network interface, as outlined in [7].

1. From a web browser, enter the URL of the Cisco VPN 3020 Concentrator Ethernet 1 (Private) interface, **http://<IP address of the 3020 Concentrator>/admin**, and the following Cisco VPN Concentrator Manager login screen appears. Log in using a user name with administrative privileges.




- The Cisco VPN Concentrator Manager main page appears upon successful login. From the left navigation menu, select **Monitoring** → **System Status**. Note the Cisco VPN Concentrator software version and compare to the version listed in **Table 1**.

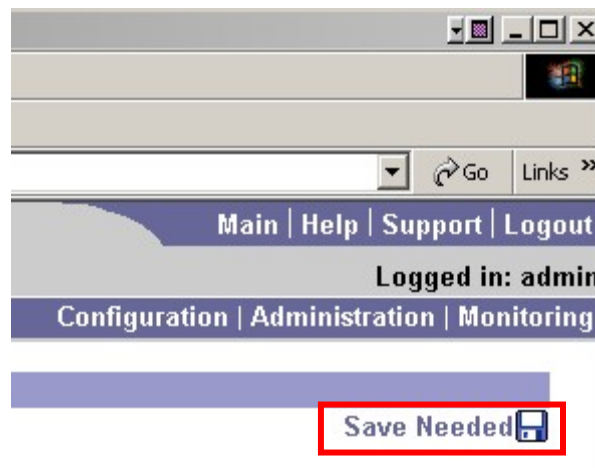


4.2. Save Configuration

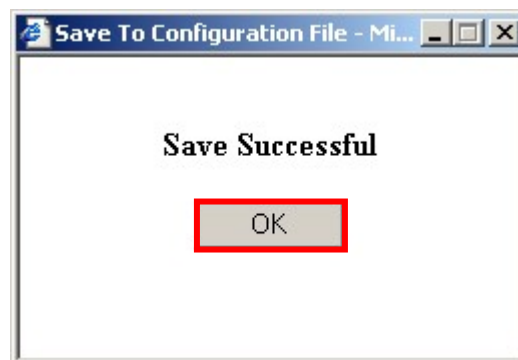
The Cisco VPN Concentrator Manager immediately applies any changes made to the running configuration of Cisco VPN Concentrator. However, these changes are NOT saved to the boot image and will NOT sustain a power cycle of the Cisco VPN Concentrator. The active running configuration must be saved to the boot configuration by executing the steps below.

Note: When the **Save Needed**  icon is displayed in the upper right corner of the Cisco VPN Concentrator Manager, these steps should be executed.

1. Select the **Save Needed** icon in the upper right corner of the Manager window.



2. Select the **OK** button from the confirmation pop-up window.



4.3. Ethernet Interfaces

The Cisco VPN 3020 Concentrator has three built-in Ethernet interfaces. These interfaces are designated as Ethernet 1 (Private), Ethernet 2 (Public) and Ethernet 3 (External). The steps below configure the Ethernet 2 (Public) interface with a public IP address facing the public Internet. Ethernet 3 (External) is not used in the sample configuration. The Avaya VPNremote Phone will interact with the Ethernet 2 (Public) interface when establishing an IPsec tunnel.

As mentioned in **Section 4.1**, these Application Notes assume the Ethernet 1 (Private) network interface has been configured using the Cisco VPN Concentrator “Quick Configuration” steps.

1. From the left navigation menu, select **Configuration → Interfaces**.

The network interfaces list page appears similar to the screen below. The Ethernet 1 (Private) interface shows a status of UP. Select **Ethernet 2 (Public)** to configure the Internet facing interface.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

Address: http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Interfaces Monday, 13 November 2006 17:30:21

Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.1.198	255.255.255.0	00.03.A0.8A.63.0E	
Ethernet 2 (Public)	Not Configured	0.0.0.0	0.0.0.0	00.03.A0.8A.63.0F	
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		

[DNS Server\(s\)](#) DNS Server Not Configured

[DNS Domain Name](#)

- [Power Supplies](#)

Cisco Systems

Filters and Access Policies Local intranet

2. Configure the highlighted fields shown below. All remaining fields can be left at the default values. Select **Apply** to save.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address http://192.168.1.198/access.html Go Links >>

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
- Administration
- Monitoring

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General RIP OSPF Bandwidth WebVPN

Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	130.2.2.2	
	Subnet Mask	255.255.255.252	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.8A.63.0F	The MAC address for this interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPSec encapsulation, fragment prior to interface transmission <input type="radio"/> Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) <input type="radio"/> Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

Apply Cancel

Ethernet Interfaces Local intranet

3. The network interface configuration page, shown below, now shows the status of both the Ethernet 1 (Private) interface and the Ethernet 2 (Public) interface as UP.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Configuration | Administration | Monitoring

Configuration | Interfaces

Monday, 13 November 2006 11:57:11


Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.1.198	255.255.255.0	00.03.A0.8A.63.0E	
Ethernet 2 (Public)	UP	130.2.2.2	255.255.255.252	00.03.A0.8A.63.0F	
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s) DNS Server Not Configured					
DNS Domain Name					

- Power Supplies



CISCO SYSTEMS

User/Group Management

Local intranet

4.4. Default Gateway

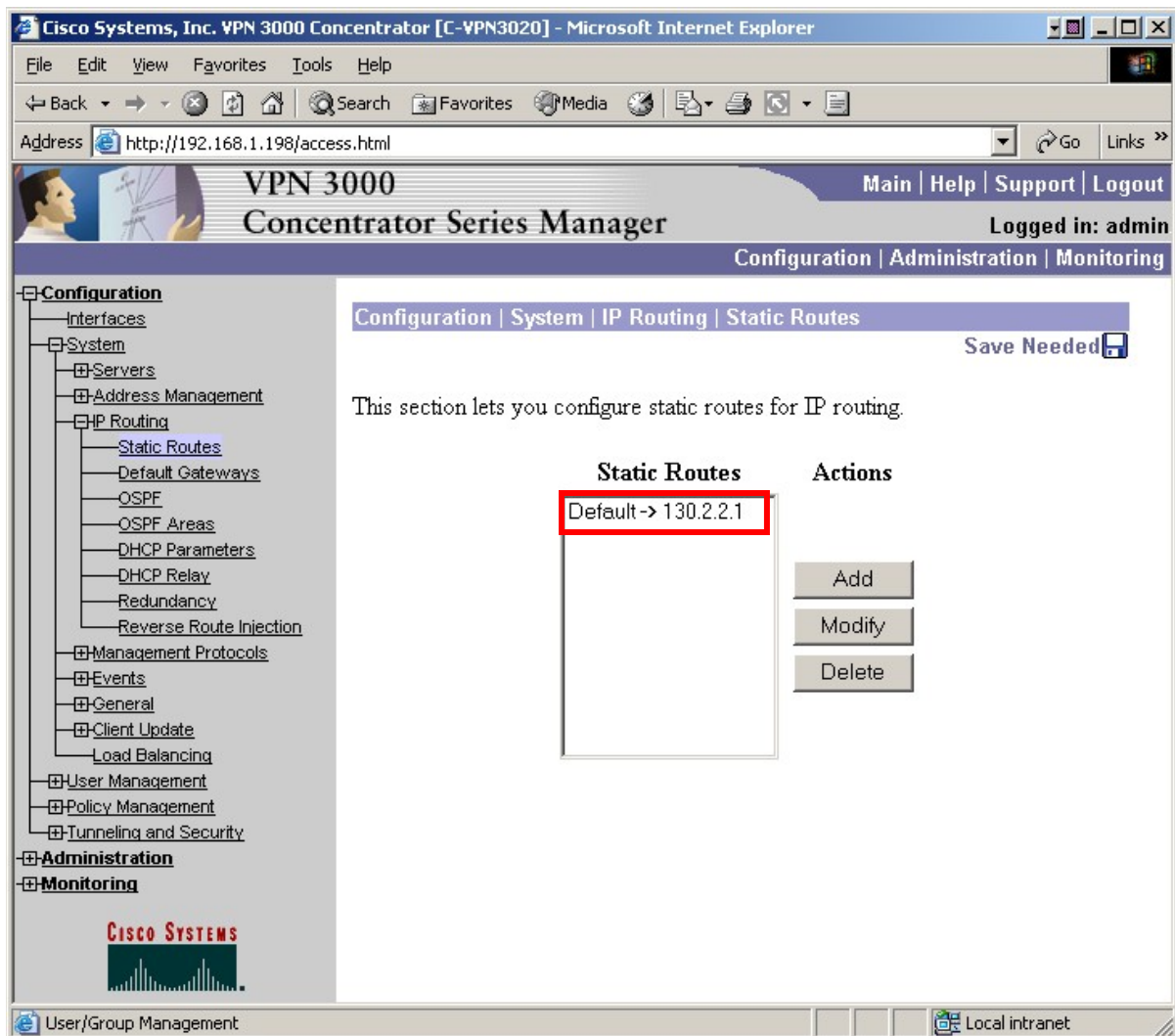
This section configures the default gateway for IP routing. The default gateway is applied to the public interface.

1. From the left navigation menu, select **Configuration → System → IP Routing → Default Gateways**. The default gateway configuration page appears similar to the screen below.

Configure the highlighted fields shown below. All remaining fields can be left at the default values. Select **Apply** to save.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser window title is "Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer". The address bar shows "http://192.168.1.198/access.html". The page has a navigation bar with "Main | Help | Support | Logout" and "Logged in: admin". The left navigation menu is expanded to "Configuration", and the "Default Gateways" link is selected. The main content area is titled "Configuration | System | IP Routing | Default Gateways" and contains the following text: "Configure the default gateways for your system." Below this, there are three input fields: "Default Gateway" with the value "130.2.2.1", "Metric" with the value "1", and "Tunnel Default Gateway" with the value "0.0.0.0". To the right of these fields are instructions: "Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router." for the first two, and "Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router." for the third. Below the input fields is an "Override Default Gateway" checkbox, which is unchecked, with the instruction "Check to allow learned default gateways to override the configured default gateway." At the bottom of the form are "Apply" and "Cancel" buttons. The "Apply" button is highlighted with a red box. The Cisco Systems logo is visible at the bottom left of the page.

2. Once configured, the default gateway IP address appears in the Static Routes list as shown below. To display the Static Routes list, select **Configuration → System → IP Routing → Static Routes** from the left navigation menu.



- The default gateway IP address also appears in the Interfaces list as shown below. To display the Interfaces list, select **Configuration** → **Interfaces** from the left navigation menu.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Interfaces

Monday, 13 November 2006 11:52:23


Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.1.198	255.255.255.0	00.03.A0.8A.63.01	
Ethernet 2 (Public)	UP	130.2.2.2	255.255.255.252	00.03.A0.8A.63.01	130.2.2.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supplies](#)



CISCO SYSTEMS

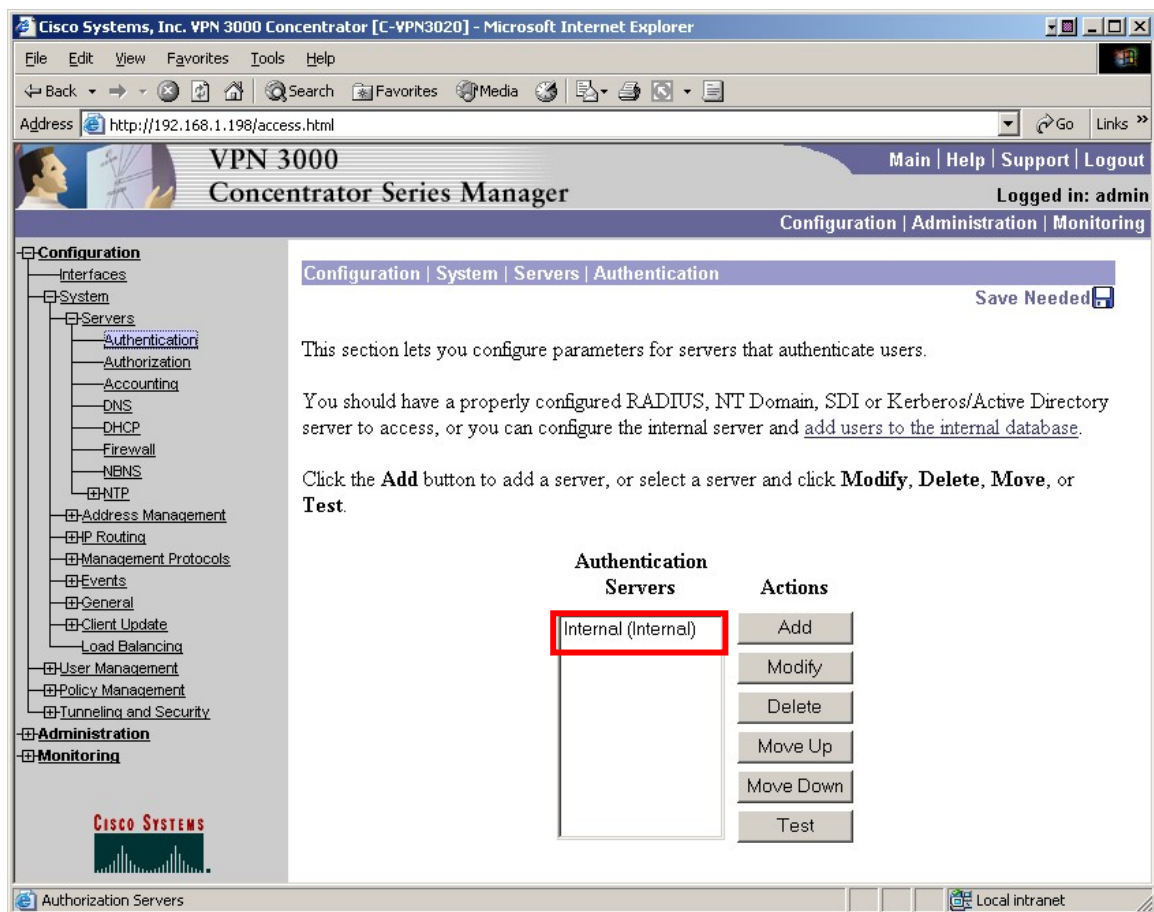
Done Local intranet

4.5. Authentication Server

The Cisco VPN 3020 Concentrator can be configured to authenticate VPNremote Phones using the internal authentication server or an external RADIUS server. For these Application Notes, the VPN 3020 Concentrator internal authentication server is used. Refer to [8] for information on configuring an external RADIUS server.

1. From the left navigation menu, select **Configuration → System → Servers → Authentication**. The authentication server configuration page appears similar to the screen below.

The Internal Authentication Server is available by default.



4.6. Security Associations

Security Associations are used by IPSec tunnels during tunnel establishment. The Security Associations are negotiated by the two tunnel endpoints, the Cisco VPN Concentrator and the Avaya VPNremote Phone in this case. IPSec tunnels consist of two Security Association phases.

- Phase 1 determines how the Avaya VPNremote Phone and the Cisco VPN Concentrator will securely negotiate and handle the building of the IPSec tunnel.
- Phase 2 determines how the data passing through the tunnel will be encrypted at one end and decrypted at the other. This process is carried out on both sides of the tunnel.

The steps below describe the creation of a Security Association on the Cisco VPN Concentrator to be used when creating IPSec tunnels with the Avaya VPNremote Phone.

Table 2 below provides the Security Association proposals used between the Avaya VPNremote Phone and the Cisco VPN Concentrator in these Application Notes.

Phase	Encryption/ Authentication Method	Diffie- Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)	VPN Concentrator Proposal Name
P1 - IKE	Pre-Shared Key	2	AES-128	SHA-1	86400	IKE-AES128- SHA
P2 - IPSec	ESP	2	AES-128	SHA-1	86400	

Table 2 –P1 /P2 Proposals

1. Verify the IKE proposal:

From the left navigation menu, select **Configuration** → **Tunneling and Security** → **IPSec** → **IKE Proposals**. Verify the IKE proposal to be used for VPNremote Phones is in the Active list. **IKE-AES128-SHA** was used for these Applications Notes. Select **IKE-AES128-SHA** and then the **Modify** button to view.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.1.198/access.html>. The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu on the left includes Configuration, Administration, and Monitoring. The Configuration menu is expanded, showing sub-menus like Interfaces, System, User Management, Policy Management, Tunneling and Security, PPTP, L2TP, IPSec, LAN-to-LAN, IKE Proposals, NAT Transparency, Alerts, SSH, SSL, and WebVPN. The IKE Proposals sub-menu is selected. The main content area shows the "Configuration | Tunneling and Security | IPSec | IKE Proposals" page. It includes a "Save Needed" button and instructions: "Add, delete, prioritize, and configure IKE Proposals." and "Select an Inactive Proposal and click Activate to make it Active, or click Modify, Copy or Delete as appropriate." and "Select an Active Proposal and click Deactivate to make it Inactive, or click Move Up or Move Down to change its priority." and "Click Add or Copy to add a new Inactive Proposal. IKE Proposals are used by Security Associations to specify IKE parameters." The page displays two lists of IKE proposals: "Active Proposals" and "Inactive Proposals". The "Active Proposals" list includes "CiscoVPNClient-3DES-MD5", "IKE-3DES-MD5", "IKE-3DES-MD5-DH1", "IKE-DES-MD5", "IKE-3DES-MD5-DH7", "IKE-3DES-MD5-RSA", "CiscoVPNClient-3DES-MD5-DH5", "CiscoVPNClient-AES128-SHA", "IKE-AES128-SHA", "CRACK-3DES-SHA-DH2", "HYBRID_AES256_SHA_RSA_DH5", "HYBRID_AES256_SHA_RSA_DH2", "HYBRID_AES192_SHA_RSA_DH2", and "HYBRID_3DES_SHA_RSA_DH5". The "Inactive Proposals" list includes "IKE-3DES-SHA-DSA", "IKE-3DES-MD5-RSA-DH1", "IKE-DES-MD5-DH7", "CiscoVPNClient-3DES-SHA-DSA", "CiscoVPNClient-3DES-MD5-RSA-DH5", "CiscoVPNClient-3DES-SHA-DSA-DH5", "CiscoVPNClient-AES256-SHA", "IKE-AES256-SHA", "HYBRID_AES128_SHA_RSA_DH2", "HYBRID_3DES_MD5_RSA_DH5", "HYBRID_3DES_MD5_RSA_DH2", "CRACK-AES256-SHA-DH5", and "CRACK-3DES-SHA1-DH5". The "Active Proposals" list is highlighted with a red box, and the "Modify" button in the "Actions" column is also highlighted with a red box.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5	<< Activate	IKE-3DES-SHA-DSA
IKE-3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5-DH1	Move Up	IKE-DES-MD5-DH7
IKE-DES-MD5	Move Down	CiscoVPNClient-3DES-SHA-DSA
IKE-3DES-MD5-DH7	Add	CiscoVPNClient-3DES-MD5-RSA-DH5
IKE-3DES-MD5-RSA	Modify	CiscoVPNClient-3DES-SHA-DSA-DH5
CiscoVPNClient-3DES-MD5-DH5	Copy	CiscoVPNClient-AES256-SHA
CiscoVPNClient-AES128-SHA	Delete	IKE-AES256-SHA
IKE-AES128-SHA		HYBRID_AES128_SHA_RSA_DH2
CRACK-3DES-SHA-DH2		HYBRID_3DES_MD5_RSA_DH5
HYBRID_AES256_SHA_RSA_DH5		HYBRID_3DES_MD5_RSA_DH2
HYBRID_AES256_SHA_RSA_DH2		CRACK-AES256-SHA-DH5
HYBRID_AES192_SHA_RSA_DH2		CRACK-3DES-SHA1-DH5
HYBRID_3DES_SHA_RSA_DH5		

- The screen below shows the default settings of the **IKE-AES128-SHA** proposal used for these Applications Notes.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.1.198/access.html`. The page title is "VPN 3000 Concentrator Series Manager". The navigation bar includes links for "Main", "Help", "Support", "Logout", and "Configuration | Administration | Monitoring". The user is logged in as "admin".

The left sidebar contains a tree view with the following categories:

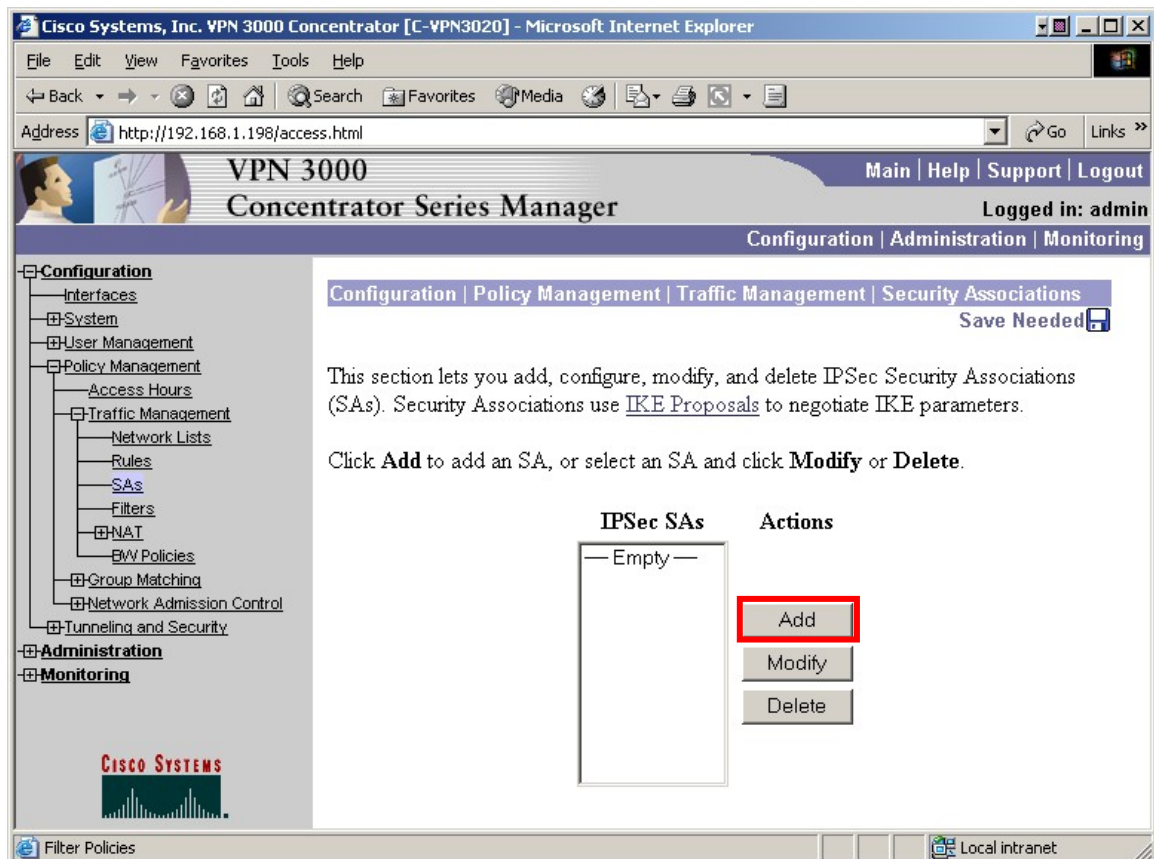
- Configuration
 - Interfaces
 - System
 - User Management
 - Policy Management
 - Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring
 - Routing Table
 - Dynamic Filters
 - Filterable Event Log
 - Live Event Log
 - WebVPN Logging
 - System Status
 - Sessions
 - Protocols
 - SEPs
 - Encryption

The main content area is titled "Configuration | Tunneling and Security | IPSec | IKE Proposals | Modify". It displays the "Modify a configured IKE Proposal" form for the "IKE-AES128-SHA" proposal.

Field	Value	Description
Proposal Name	IKE-AES128-SHA	Specify the name of this IKE Proposal.
Authentication Mode	Preshared Keys	Select the authentication mode to use.
Authentication Algorithm	SHA/HMAC-160	Select the packet authentication algorithm to use.
Encryption Algorithm	AES-128	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 2 (1024-bits)	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.

Buttons: Apply, Cancel

3. From the left navigation menu, select **Configuration → Policy Management → Traffic Management → SAs**. The Security Associations list page similar to the screen below is displayed. Select **Add** to create a new Security Association for VPNremote Phones.



- The Security Associations configuration page similar to the screen below is displayed. The configuration options of this page related to the VPNremote Phone are highlighted below. All remaining fields can be left at default values. Select **Apply** when complete.

The VPNremote Phone offers an IKE Rekey time interval of 86400 seconds to the VPN head-end by default. This value is not configurable as of the firmware release used in these Application Notes. The Cisco VPN Concentrator can override this value to a lower value with the **Time Lifetime** parameter. Any **Time Lifetime** value greater than 86400 will be ignored by the VPNremote Phone and the default 86400 offered by the VPNremote Phone will be used.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

Address: http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name VPNphone SA

Inheritance From Rule

IPSec Parameters

Authentication Algorithm ESP/SHA/HMAC-160

Encryption Algorithm AES-128

Encapsulation Mode Tunnel

Perfect Forward Secrecy Group 2 (1024-bits)

Lifetime Measurement Time

Data Lifetime 10000

Time Lifetime 86400

IKE Parameters

IKE Peer 0.0.0.0

Negotiation Mode Aggressive

Digital Certificate None (Use Preshared Keys)

Certificate Transmission ☐ Entire certificate chain ☒ Identity certificate only

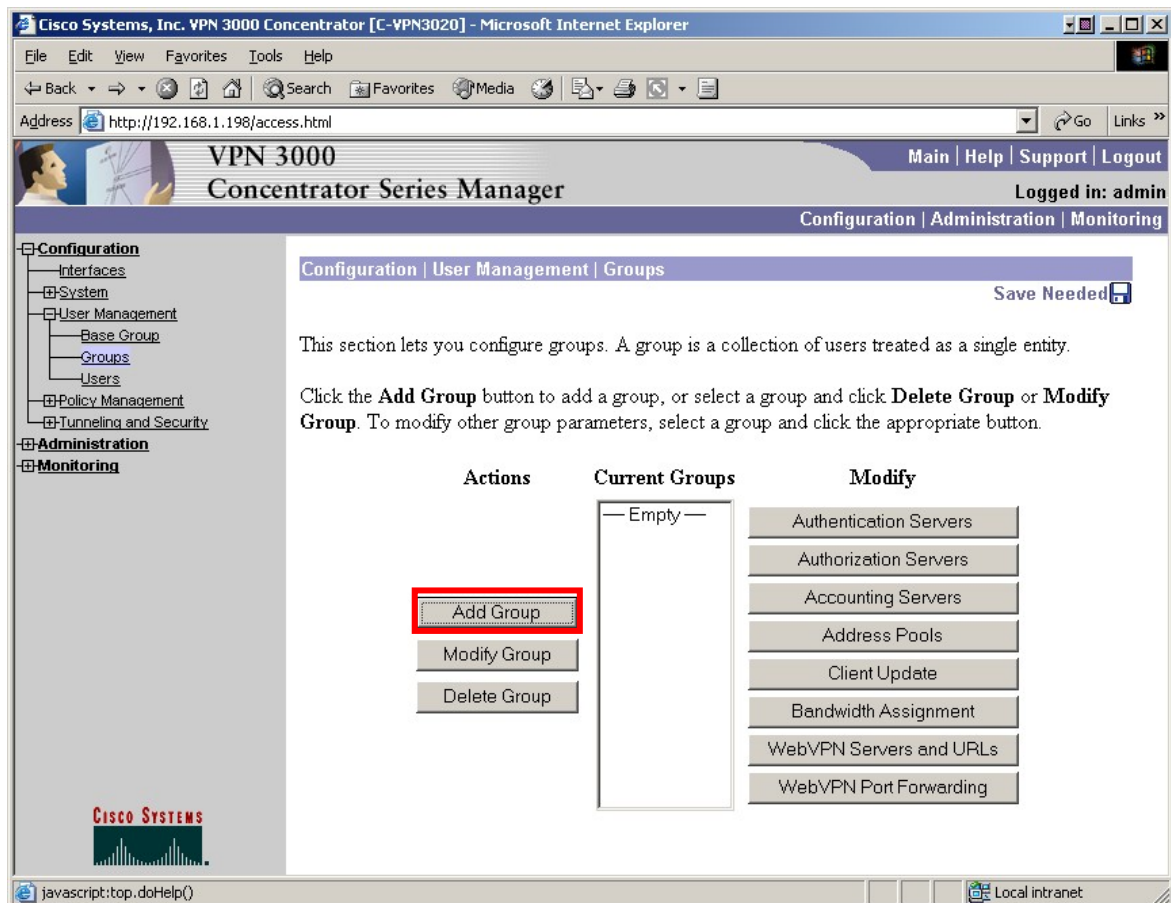
IKE Proposal IKE-AES128-SHA

Apply **Cancel**

4.7. User Group

A user group is a collection of VPN users treated as a single entity. The Cisco VPN Concentrator is able to authenticate all VPN users of the same user group with a single IKE Identity and pre-shared key. The IKE authentication of the IPSec tunnel is combined with user authentication of the VPNremote Phone user using XAUTH.

1. From the left navigation menu, select **Configuration → User Management → Groups**. The group configuration page similar to the screen below is displayed. Select **Add Group** to create a new user group for the Avaya VPNremote Phones.



2. The group **Identity Parameters** configuration page is displayed similar to the screen shown below. The configuration options of this page needed for the VPNremote phone are described and highlighted below.

Group Name: The VPNremote Phone contains a default group name of **VPNPHONE**. This default group name is used for these Application Notes.

Password: enter a group password to be used by all VPNremote Phones associated with this user group.

Type: Select the RADIUS group type if authentication is to be done with an external RADIUS server or Internal if authentication is to be done locally within the Concentrator.

Note: The **Password** entered above must match the **Group PSK** set on the VPNremote Phones. See Section 5.2 for additional information on VPNremote Phone parameters.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

Address: http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP WebVPN NAC

Attribute	Value	Description
Group Name	VPNPHONE	Enter a unique name for the group.
Password	XXXXXXXXXX	Enter the password for the group.
Verify	XXXXXXXXXX	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

3. Select the **General** tab. The group General Parameters page is displayed similar to the screen shown below. The configuration options of this page needed for the VPNremote phone are described and highlighted below. All remaining fields can be left at the default values.

Simultaneous Logins: The number entered here must be equal to or greater than the number of VPNremote Phones that could be simultaneously connected to the Cisco VPN Concentrator. The number 100 was used for these Application Notes to match the number of VPNremote Phones licensed by the Avaya WebLM License Manager.

Tunneling Protocols: Tunneling protocols enabled for this group. The VPNremote Phone supports the IPSec Tunneling protocol.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	100	<input type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group. When set to 0, WebVPN sessions use the Default Idle Timeout value specified in Configuration Tunneling and Security WebVPN HTTPS Proxy .
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.

Scroll to the bottom of the Group **General Parameters** page to display additional configuration options as shown below.

Secondary DNS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec <input type="checkbox"/> WebVPN	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

4. Select the **IPSec** tab. The group IPSec Parameters page is displayed similar to the screen shown below. The configuration options of this page needed for the VPNremote phone are described and highlighted below. All remaining fields can be left at the default values. Select **Apply** to save.

IPSec SA: Choose the IPSec security association created in **Section 4.6** to be used by VPNremote Phones when accessing the Cisco VPN Concentrator.

IKE Keepalives: If a VPNremote Phone is abruptly disconnected from the network (e.g. VPNremote Phone loses power) the Cisco VPN Concentrator is not notified and maintains the security associations for the disconnected VPNremote Phone. Enabling this option allows the Cisco VPN Concentrator to determine if an IPSec tunnel to a VPNremote Phone is active and remove security associations when no response is received to the keepalive.

Confidence Interval: Determines how often, in seconds, the Cisco VPN Concentrator sends an IKE Keepalive to the VPNremote Phone. The default is 300 seconds.

Configuration | User Management | Groups | Modify VPNPHONE

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General **IPSec** Client Config Client FW HW Client PPTP/L2TP WebVPN NAC

Attribute	Value	Inherit?	Description
IPSec SA	VPNphone SA	<input type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.

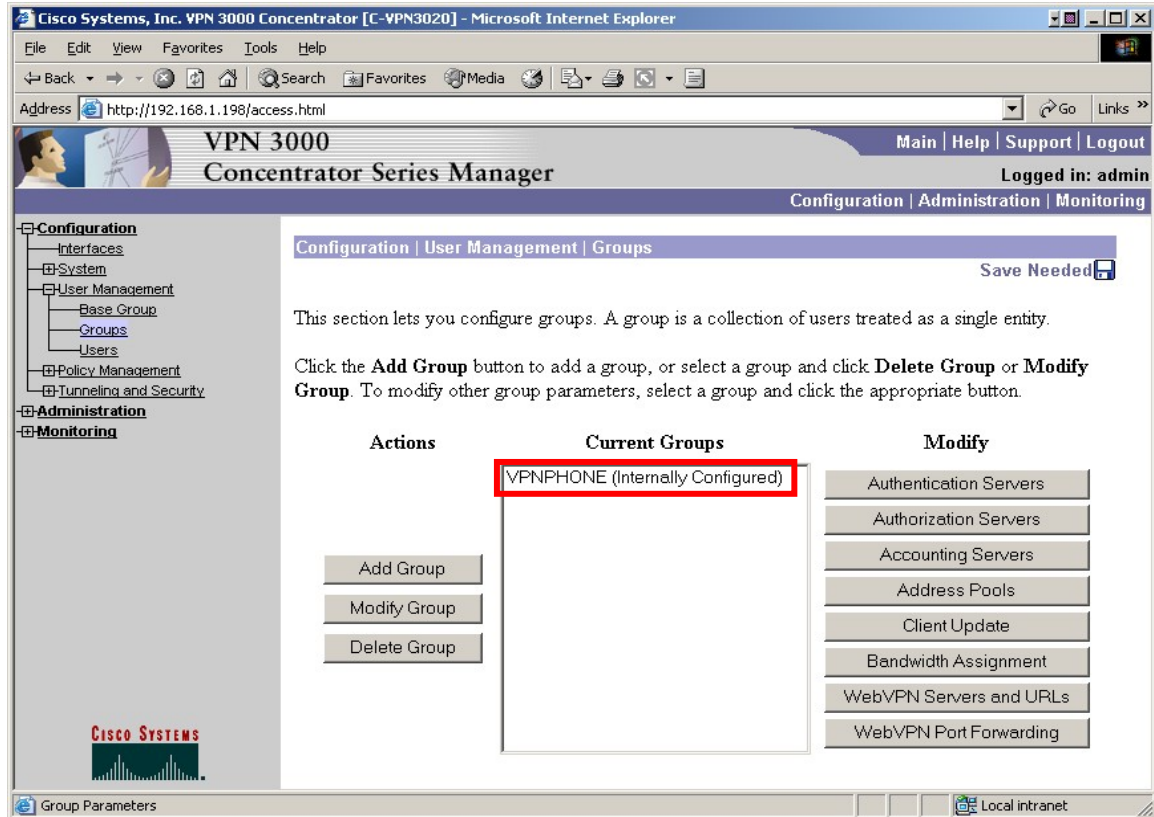
Scroll to the bottom of the **IPSec Parameters** page to display additional configuration options as shown below.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The page is divided into a left sidebar with navigation links (Configuration, System, User Management, Base Group, Groups, Users, Policy Management, Tunneling and Security, Administration, Monitoring) and a main content area. The main content area displays configuration options for a group, with a table of settings and their descriptions. The "Apply" button is highlighted with a red box.

Configuration	Value	Check	Description
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Client Type & Version Limiting		<input checked="" type="checkbox"/>	Permit or deny VPN Clients according to their type and software version. <ul style="list-style-type: none"> Construct rules in the format p[ermit]/d[eny] <type> : <version>. For example, d VPN 3002 : 3.6* The * character is a wildcard. Use a separate line for each rule. Order rules by priority. For more instructions, click here .
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiqa/Cisco client is being used by members of this group.

Apply Cancel

5. The new VPNPHONE group is now displayed in the Groups list page.



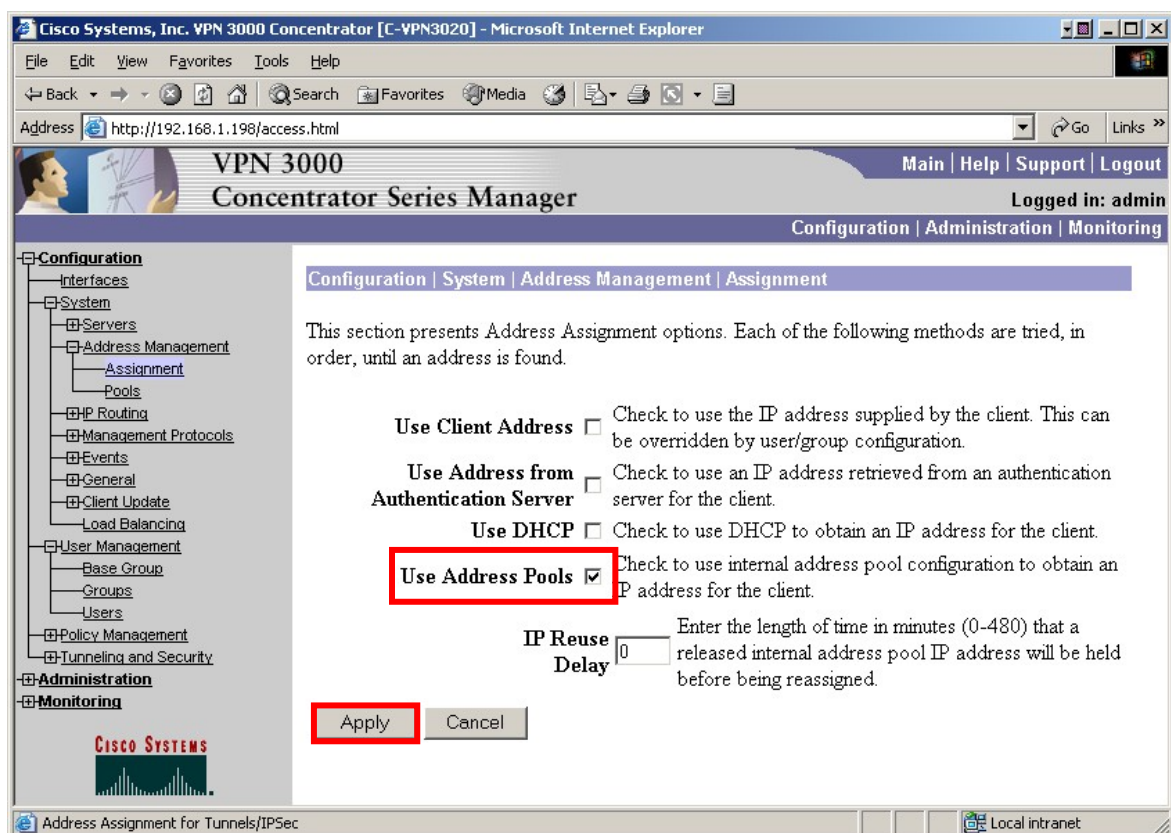
4.8. IP Address Pools

The Cisco VPN Concentrator must assign an IP address to the VPNremote Phone during the establishment of the IPSec tunnel. This IP address, referred to as the “Inner IP” by the VPNremote Phone, is used by the VPNremote Phone when communicating with the trusted corporate network via the IPSec tunnel.

Note: Ensure the IP address range assigned to the IP Address Pool does not conflict with addresses used throughout the corporate trusted network. The corporate trusted network must contain routes for the IP Address Pool network. The configuration of these routes is not within the scope of these Application Notes.

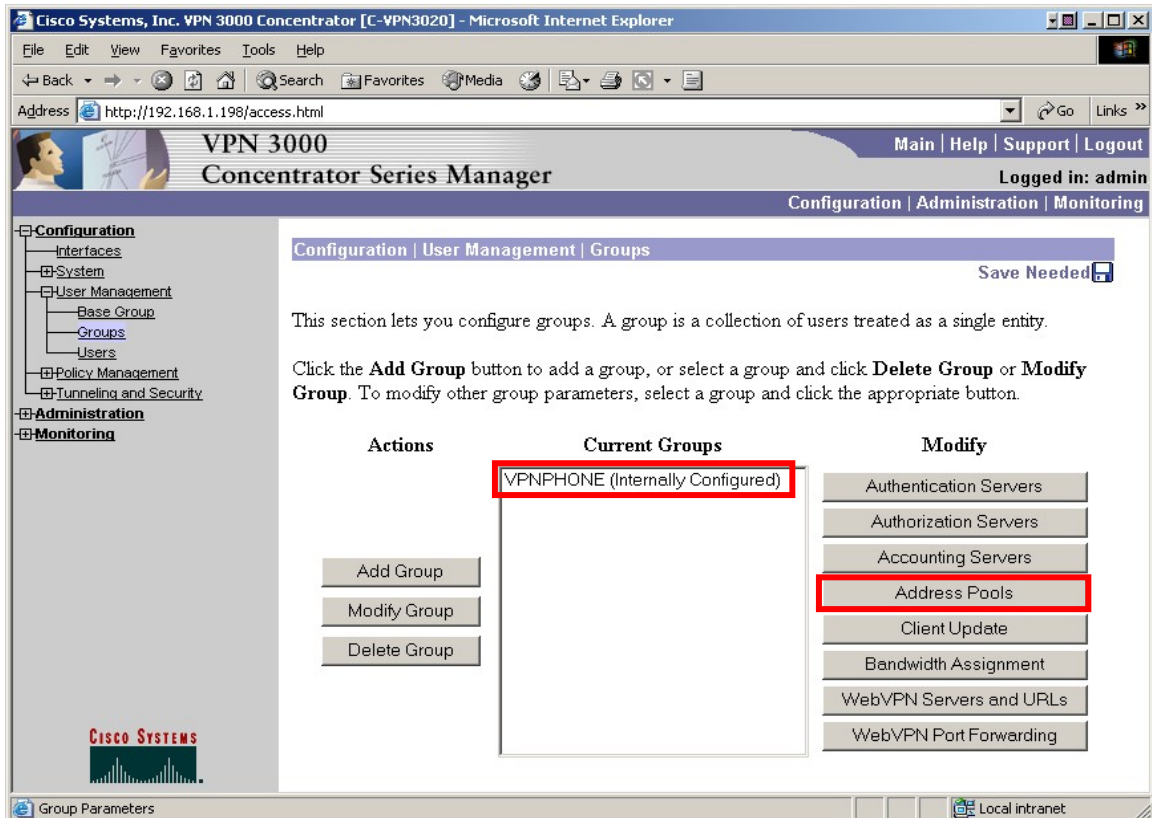
The following steps will configure the Cisco VPN Concentrator with an IP address range to be assigned to members of the VPNPHONE group created in **Section 4.7**. This range of IP Addresses is referred to as an IP Address Pool.

1. From the left navigation menu, select **Configuration → System → Address Management → Assignment**. Ensure the **Use Address Pools** option is checked. Select the **Apply** button to save.

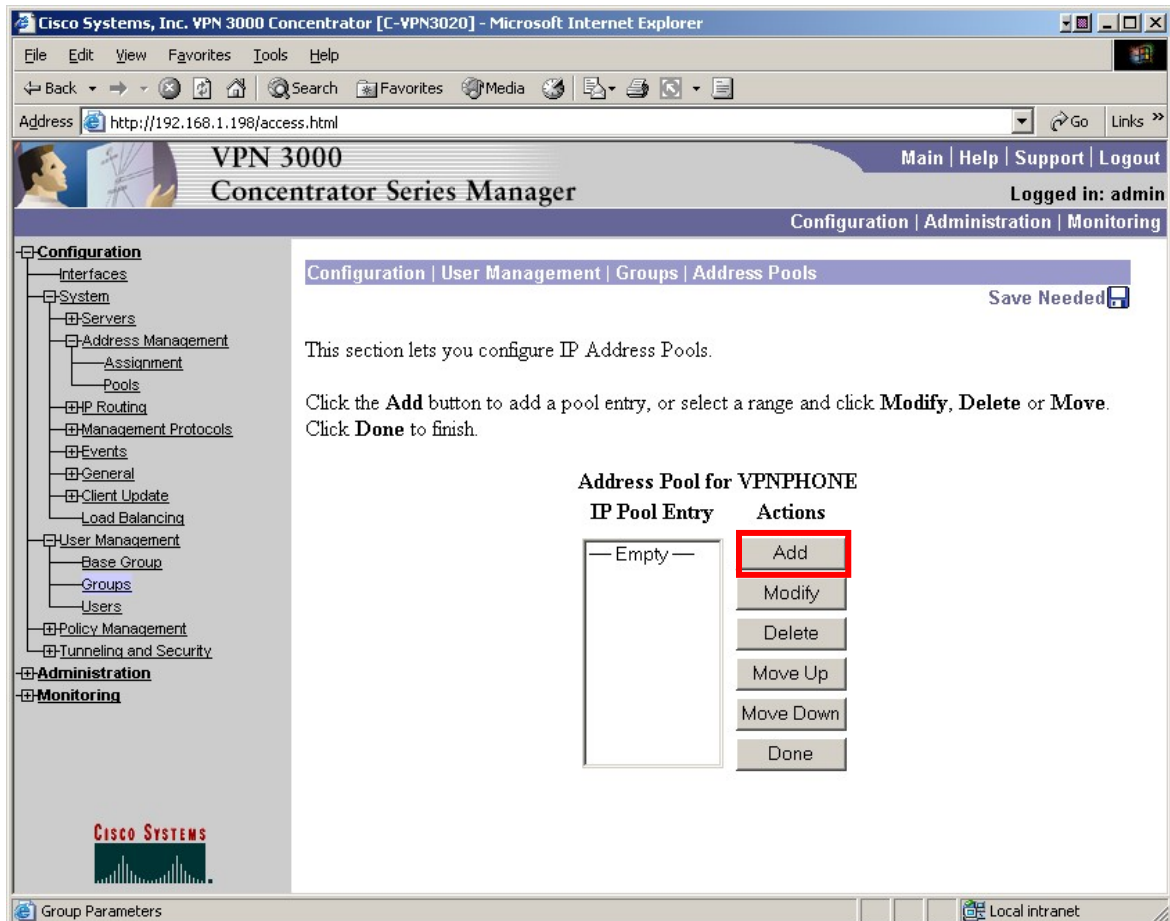


- From the left navigation menu, select **Configuration → User Management → Groups**. The group configuration page similar to the screen below is displayed. Select the **VPNPHONE** group and then the **Address Pools** button.

Note: IP Address Pools can also be created from the **Configuration → System → Address Management → Pools** menu option. IP Address Pools created using this method are available to any VPN user of any group. The method described in these configuration steps creates an IP Address Pool to be used only by the group VPNPHONE which only VPNremote Phones can authenticate against.



3. The IP Address Pool configuration page similar to the screen below is displayed. Select the **Add** button to create an IP Address Pool.

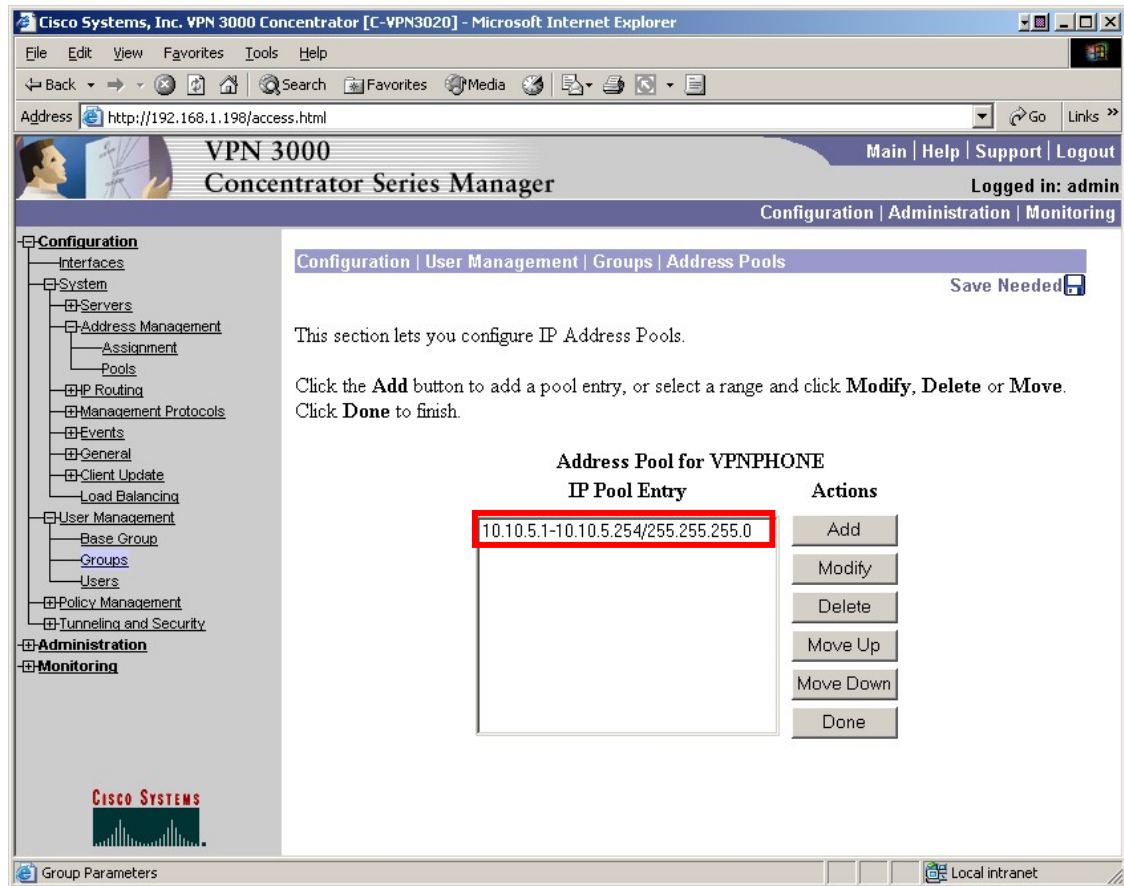


4. The IP Address Pool Add page similar to the screen below is displayed. Enter the start and end IP address range to be used for VPNremote Phones. Select **Add** to save.

Note: It is recommended to create an IP Network Region within Avaya Communication Manager for VPNremote Phones. This allows Avaya Communication Manager to have the flexibility to assign the VPNremote Phones with parameters (i.e. G.729 codec with 30ms frame size) to accommodate the network environments VPNRemote Phones are likely to be installed in. See Section 6 for additional information.

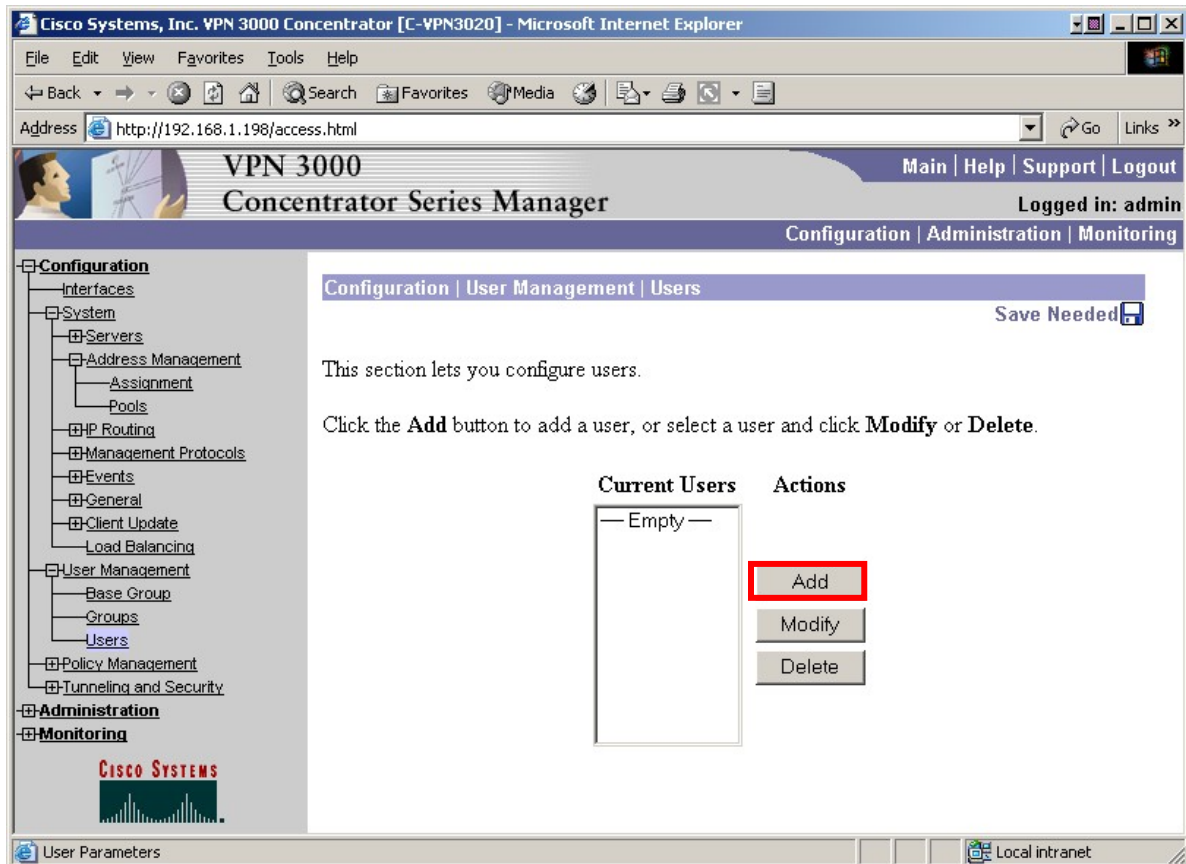
The screenshot shows a web browser window titled "Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer". The address bar shows "http://192.168.1.198/access.html". The page header includes "VPN 3000 Concentrator Series Manager" and navigation links: "Main | Help | Support | Logout". A status bar indicates "Logged in: admin". Below the header is a navigation menu with "Configuration | Administration | Monitoring". The left sidebar contains a tree view with categories: "Configuration" (expanded), "Administration", and "Monitoring". Under "Configuration", sub-items include "Interfaces", "System", "Servers", "Address Management" (expanded), "Management Protocols", "Events", "General", "Client Update", "Load Balancing", "User Management", "Base Group", "Groups", "Users", "Policy Management", and "Tunneling and Security". The main content area is titled "Configuration | User Management | Groups | Address Pools | Add". It contains the text "Add an address pool." followed by three input fields: "Range Start" with value "10.10.5.1", "Range End" with value "10.10.5.254", and "Subnet Mask" with value "255.255.255.0". Each field has a descriptive text to its right: "Enter the start of the IP pool address range.", "Enter the end of the IP pool address range.", and "Enter the subnet mask of the IP pool address range. Enter 0.0.0.0 to use default behavior." At the bottom of the form are "Add" and "Cancel" buttons. The Cisco Systems logo is visible in the bottom left corner of the page.

5. The new IP Address Pool for the VPNPHONE group is now displayed in the Address Pools list page.



4.9. User Accounts

1. From the left navigation menu, select **Configuration → User Management → Users**.
The user configuration page similar to the screen below is displayed. Select **Add** to create a new user account for each user of a VPNremote Phone.



2. The user **Identity Parameters** configuration page is displayed similar to the screen shown below. The configuration options of this page needed for the VPNremote phone are described and highlighted below.

User Name: The unique username of the VPNremote Phone user.

Password: This password must be shared with the user. The VPNremote Phone will prompt the user for a password during the XAUTH authentication phase of establishing the IPsec tunnel. This password can optionally be stored in the flash memory of the VPNremote Phone to avoid prompting on subsequent reboots.

Group: Select the user group created in **Section 4.7**. The VPNremote Phone default group name of **VPNPHONE** is used in these Application Notes.

IP Address: This field is left blank because an IP Address will be assigned to the VPNremote Phone from the IP Address Pool created in **Section 4.8**.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

Address: http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Attribute	Value	Description
Username	ehope	Enter a unique username.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	VPNPHONE	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

User Parameters

Local intranet

3. Select the **General** tab. The user General Parameters page is displayed similar to the screen shown below. The configuration options of this page needed for the VPNremote phone are described and highlighted below. All remaining fields can be left at the default values. The default values are inherited from the group with which the user is associated, VPNPHONE in this case.

Simultaneous Logins: The number entered here must be equal to the number of simultaneous active login sessions allowed for this user. A value of 1 was used for these Application Notes allowing only one VPNremote Phone to be used under this account. Optionally, a value of 2 would allow a user to use the same user account for both a VPNremote Phone and remote computer access to the corporate network.

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

Address: http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Users | Modify ehope

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identis **General** PSec PPTP/L2TP

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	1	<input type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	0	<input type="checkbox"/>	(minutes) Enter the idle timeout for this user. Note: A value of zero will not apply to WebVPN users. It will be overridden by the value set for Default Idle Timeout for the HTTPS Proxy.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this user can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec <input type="checkbox"/> WebVPN	<input type="checkbox"/>	Select the tunneling protocols this user can connect with.

Apply Cancel

System Monitoring Local intranet

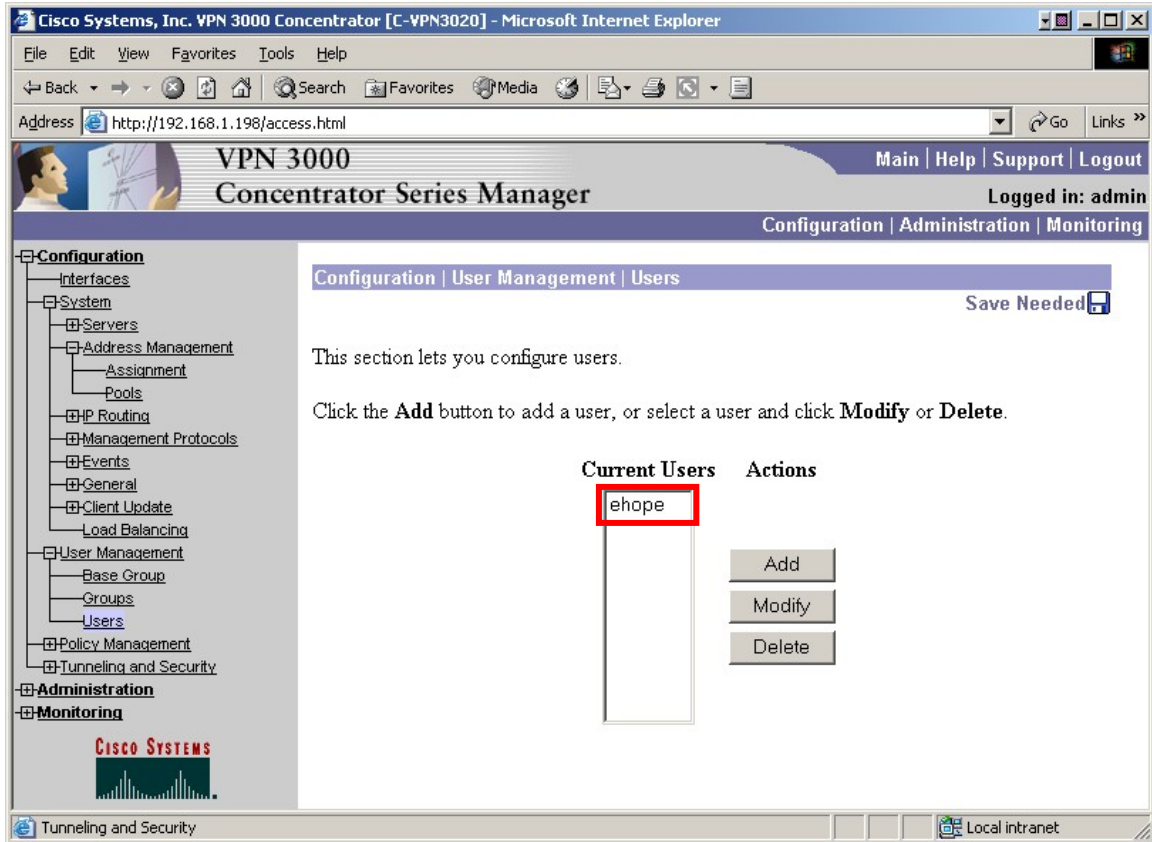
4. Select the **IPSec** tab. The user IPSec Parameters page is displayed similar to the screen shown below. The default values are inherited from the group with which the user is associated, VPNPHONE in this case. Verify the correct security association is selected for this user. Select **Apply** to save.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.1.198/access.html`. The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu on the left includes Configuration, System, User Management, Policy Management, Tunneling and Security, Administration, and Monitoring. The main content area shows the "Configuration | User Management | Users | Modify ehope" path. Below this, there is a table with the following data:

Attribute	Value	Inherit?	Description
IPSec SA	VPNphone SA	<input checked="" type="checkbox"/>	Select the IPSec Security Association assigned to this user.
Store Password on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.

Below the table are "Apply" and "Cancel" buttons. The "Apply" button is highlighted with a red box. The "IPSec" tab is also highlighted with a red box.

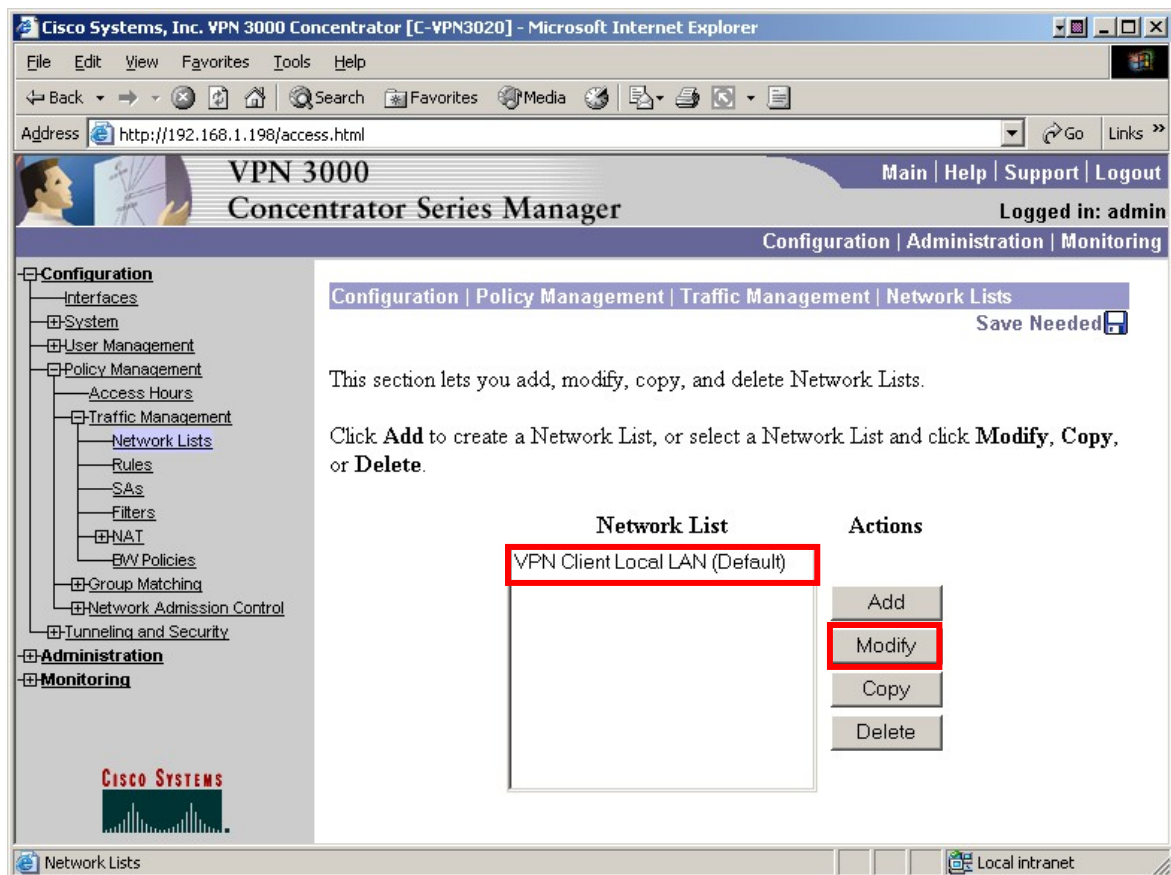
5. The new user account is now displayed in the user list page.



4.10. Network Lists

The Cisco VPN Concentrator Network Lists page consists of a list of the private networks on the Ethernet 1 (Private) side of the Cisco VPN Concentrator which VPN remote clients can access once a tunnel is established. The default network list VPN Client Local LAN (Default) was used for these Application Notes with a network and mask of 0.0.0.0/0.0.0.0 which gives the VPNremote Phones access to all private networks.

1. From the left navigation menu, select **Configuration → Policy Management → Traffic Management → Network Lists**. The Network List configuration page similar to the screen below is displayed. Select **VPN Client Local LAN (Default)** followed by the **Modify** button.



2. Enter the network and wildcard mask of networks the VPNremote Phone need access in the Network List field. Select the **Apply** button when done.

Note: Optionally the **Generate Local List** button can be selected to automatically generate a list of private networks from the routing table if the RIP or OSPF routing protocols are being used

Cisco Systems, Inc. VPN 3000 Concentrator [C-VPN3020] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.1.198/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name VPN Client Local LAN (Default)

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format:
n.n.n.n/n.n.n.n (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

0.0.0.0/0.0.0.0

Apply Cancel Generate Local List

Network Lists Local intranet

4.11. Welcome Banner Script

An Avaya 46xxsettings script file contains optional settings which enable Avaya IP Telephones to be customized for each enterprise environment. The 46xxsettings file is downloaded from a TFTP or HTTP server by the Avaya IP Telephone as the telephone boots up.

Optionally, the Welcome Banner of the Cisco VPN Concentrator can be used to deliver script text to the VPNremote Phone as the IPsec tunnel is established. This script text will be treated as content of a 46xxsettings script file by the VPNremote Phone.

The script portion of the banner message is indicated by the **<SCRIPT_START>** and **<SCRIPT_END>** tags. These tags are case sensitive. Any text after the **<SCRIPT_END>** tag is delivered as a welcome banner. Everything between the script tags will be treated as the content of a 46xxsettings script file by the VPNremote Phone.

The script text shown below sets the TFTP server IP address on the VPNremote Phone using the Welcome Banner. This avoids having to manually enter this IP address into the VPNremote Phone. The script also sets the WebLM License Manager URL.

```
<SCRIPT_START>
set TFTP SRVR 192.168.1.30
set NVWEBLMURL http://192.168.1.30:8080/weblm/LicenseServer
<SCRIPT_END>
```

From the left navigation menu, select **Configuration → User Management → Groups**. Select the **VPNPHONE** group and the **Modify Group** button. Select the **Client Config** tab and scroll down to the **Banner** option. Enter the script text and save the configuration. The Cisco VPN Concentrator will now download all entered text to the VPNremote Phone as the IPsec tunnel is established. The VPNremote Phone will recognize the **<SCRIPT_START>** tag and display **Executing Scripts**. Verify the TFTP server is accessed by the VPNremote Phone to confirm the script execution.

Banner	<div><div><SCRIPT_START> set TFTP SRVR 192.168.1.30 set NVWEBLMURL http://192.168.1.30:8080/weblm /LicenseServer <SCRIPT_END></div></div>	<input type="checkbox"/>	Enter the banner for this group.
---------------	---	--------------------------	----------------------------------

5. Avaya VPNremote Phone Configuration

5.1. VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. Refer to [1] and [2] for details on installing VPNremote Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the **Options** hard button → **View IP Settings** soft button → **Miscellaneous** soft button → **Right arrow** hard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1**, VPNremote Phone firmware includes the letters **VPN** in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

5.2. Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from an HTTP/TFTP server or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to [1] and [2] for details on a centralized configuration.

Note: The WebLM Server URL can not be set from the local phone configuration menu as of the firmware release used in these Application Notes. A centralized HTTP/TFTP server must be used to set this value (NVWEBLMURL) from the phone configuration scripts.

1. There are two methods available to access the **VPN Configuration Options** menu from the VPNremote Phone.

a. During Telephone Boot:

During the VPNremote Phone boot up, the option to press the * key to enter the local configuration mode is displayed on the telephone screen as shown below.

```
DHCP
* to program
```

When the * key is pressed, several configuration parameters are presented such as the phone's IP Address, the Call Servers IP Address, etc. Press # to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode option shown below. Press the * key to enter the VPN Options menu.

```
VPN Start Mode: Boot
*=Modify  #=OK
```

b. During Telephone Operation:

While the VPNremote Phone is in an operational state, e.g. registered with Avaya Communication Manager, press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The follow is displayed:

```
VPN Start Mode: Boot
*=Modify  #=OK
```

Press the * key to enter the VPN Options menu.

2. The VPN configuration options menu is displayed. For detailed description of each VPN configuration option, refer to [1] and [2].

The configuration values of one of the VPNremote Phones used in the sample configuration are shown in **Table 3** below.

Note: The values entered below are case sensitive.

Press the ► hard button on the telephone to access the next screen of configuration options. Phone models with larger displays (e.g. 4621) will present more configuration options per page.

Configuration Options	Value	Description
Server:	130.2.2.2	IP address of the Cisco VPN Concentrator Ethernet 2 (Public) interface
User Name:	ehope	User created in Section 4.9
Password:	*****	Must match user password entered in Section 4.9
Group Name:	VPNPHONE	Group name created in Section 4.7
Group PSK:	*****	Must match Group password entered in Section 4.7
VPN Start Mode:	BOOT	IPSec tunnel dynamically starts on Phone power up.
Password Type:	Save in Flash	User is not prompted at phone boot up.
Encapsulation	4500-4500	This default value enables NAT Traversal
Syslog Server:	-	

Configuration Options	Value	Description
IKE Parameters:	(DH2-AES128-SHA1)	Must match SA proposals from Section 4.6
IKE ID Type:	KEY-ID	
Diffie-Hellman Grp	2	Can be set to “Detect” to accept VPN Concentrator settings
Encryption Alg:	AES-128	Can be set to “Any” to accept VPN Concentrator settings
Authentication Alg:	SHA1	Can be set to “Any” to accept VPN Concentrator settings
IKE Xchg Mode:	Aggressive	
IKE Config Mode:	Enable	
IPSec Parameters:	DH2-AES128-SHA1	Must match SA proposals from Section 4.6
Encryption Alg:	AES-128	Can be set to “Any” to accept VPN Concentrator settings
Authentication Alg:	SHA1	Can be set to “Any” to accept VPN Concentrator settings
Diffie-Hellman Grp	2	Can be set to “Detect” to accept VPN Concentrator settings
Protected Net:		
Remote Net #1:	0.0.0.0/0	Access to all private nets
Copy TOS:	Yes	Maintain phone TOS setting on Corp Network for QoS
File Srvr:	192.168.1.30	TFTP/HTTP Phone File Srv
Connectivity Check:	First Time	Test initial IPSec connectivity

Table 3 – VPNremote Phone Configuration

3. The VPNremote Phone can interoperate with several VPN head-end vendors. The VPNremote Phone must be told which VPN head-end vendor will be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** on the VPNremote Phone.

Press the **Profile** soft button at the bottom of the VPNremote Phones display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. If a Profile other than Cisco is already chosen, press the Modify soft button to display the following list:

- **Avaya Security Gateway**
- **Cisco Xauth with PSK**
- **Juniper Xauth with PSK**
- **Generic PSK**

Press the button aligned with the **Cisco Xauth with PSK** profile option then press the **Done** soft button.

When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press # to save the configuration and reboot the phone.

```
Save new values ?
*=no  #=yes
```

6. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has already been completed.

As shown in **Figure 2**, the VPNremote Phones are assigned to IP Network Region 5 using the IP address range of the VPN Concentrator IP Address Pool. IP Network Region 5 is then assigned to a codec set configured with the G.729 codec. The Main Campus is assigned to IP Network Region 1 using the G.711 codec.

6.1. VPNremote Phone Administration

An Avaya VPNremote Phone is administered the same as other IP telephones within Avaya Communication Manager. Even though the Avaya VPNremote Phone is physically located outside of the corporate network, the AvayaVPNremote Phone will behave the same as other Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established.

For additional information regarding the administration of Avaya Communication Manager, refer to [3].

6.2. IP Codec Sets Configuration

Use the **change ip-codec-set n** command to configure IP Codec Set parameters where n is the IP Codec Set number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

1. Use the **change ip-codec-set 1** command to define a codec set for the G.711 codec as shown below.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1: G.711MU	n	2	20			
2:						
3:						

2. Use the **change ip-codec-set 2** command to define a codec set for the G.729 (30ms) codec as shown below.

change ip-codec-set 2				Page	1 of	2
IP Codec Set						
Codec Set: 2						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1: G.729	n	3	30			
2:						
3:						

3. Use the **list ip-codec-set** command to verify the codec assignments.

list ip-codec-set					
IP CODEC SETS					
Codec Set	Codec 1	Codec 2	Codec 3	Codec 4	Codec 5
1	G.711MU				
2	G.729				
3					
4					

6.3. IP Network Map Configuration

Use the **change ip-network-map** command to define the IP address to Network Region mapping for VPNremote Phones.

change ip-network-map						Page	1 of	32
IP ADDRESS MAPPING								
From IP Address	(To IP Address	Subnet	Region	VLAN	Emergency			
		or Mask)			Location			
					Extension			
10 .10 .5 .1	.	24	5	n				
.	.	.	.	n				
.	.	.	.	n				
.	.	.	.	n				

6.4. IP Network Regions Configuration

Use the **change ip-network-region n** command to configure IP Network Region parameters where n is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

Intra-region and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to “yes” enables the most efficient audio path to be taken. **Codec Set 1** is used for IP Network Region 1 as described in **Section 6.2**.

change ip-network-region 1		Page	1 of	19
IP NETWORK REGION				
Region: 1				
Location: 1 Authoritative Domain: avaya.com				
Name: Main Campus				
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes		
Codec Set: 1		Inter-region IP-IP Direct Audio: yes		
UDP Port Min: 2048		IP Audio Hairpinning? y		
UDP Port Max: 3327				
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y		
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS		
Audio PHB Value: 46		Use Default Server Parameters? y		
Video PHB Value: 26				
802.1P/Q PARAMETERS		AUDIO RESOURCE RESERVATION PARAMETERS		
Call Control 802.1p Priority: 6		RSVP Enabled? n		
Audio 802.1p Priority: 6				
Video 802.1p Priority: 5				
H.323 IP ENDPOINTS				
H.323 Link Bounce Recovery? y				
Idle Traffic Interval (sec): 20				
Keep-Alive Interval (sec): 5				
Keep-Alive Count: 5				

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls between IP Network Region 1 and IP Network Region 5 use Codec Set 2 (G.729).

change ip-network-region 1										Page 3 of 19
Inter Network Region Connection Management										
src rgn	dst rgn	codec set	direct WAN	WAN-BW-limits	Intervening-regions	Dynamic CAC Gateway	CAC IGAR			
1	1	1								
1	5	2	y	:NoLimit					n	
1	3									
1	4									

Use the **change ip-network-region 5** command to configure IP Network Region 5 parameters. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

change ip-network-region 5										Page 1 of 19
IP NETWORK REGION										
Region: 5										
Location: Authoritative Domain:										
Name: VPNphones-Cisco 3020										
MEDIA PARAMETERS										
Codec Set: 2										
UDP Port Min: 2048										
UDP Port Max: 3028										
Intra-region IP-IP Direct Audio: yes										
Inter-region IP-IP Direct Audio: yes										
IP Audio Hairpinning? y										

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 5, i.e. a VPNremote Phone calling another VPNremote Phone, use Codec Set 2 (G.729). Calls between IP Network Region 5 and IP Network Region 1 will also use Codec Set 2 (G.729).

change ip-network-region 5										Page 3 of 19
Inter Network Region Connection Management										
src rgn	dst rgn	codec set	direct WAN	WAN-BW-limits	Intervening-regions	Dynamic CAC Gateway	CAC IGAR			
5	1	2	y	:NoLimit					n	
5	2									
5	3									
5	4									
5	5	2								

7. Verification

7.1. VPNremote Phone QTest

The Avaya VPNremote Phone **Quality Test** feature can be used to predict the quality of voice to be expected with the current IP network(s) the VPNremote Phone has established an IPSec tunnel across.

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, enter the Avaya VPNremote Phone VPN configuration mode as described in **Section 5.2**. Select the **QTest** soft button at the bottom of the VPNremote Phones display to enter the QTest menu similar to the display shown below. Select the **Start** soft button to start QTest. Note the reported statistics to determine the network connection quality.

VPNremote Phone QTest display:

Time Elapsed x Secs	
Packets Lost:	0%
Round Trip Delay:	0ms
Packets Late:	0%
Packets Sent:	0
Packets Received:	0
Average Delay:	0ms
Maximum Delay:	0ms
Packets Lost	0
Maximum Burst Lost:	0
Packets out of seq:	0
Interruptions:	0

7.2. VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, from the telephone keypad, press the **OPTIONS** hard button (with √ icon). From the telephone keypad, press the ► hard button until the **VPN Status...** option appears. Select **VPN Status...** The VPN statistics of the active IPSec tunnel will be displayed. Use the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

The list below shows the statistics from the VPNremote phone used in the sample configuration.

VPN Status...	
PKT S/R	448/419
FRAG RCVD	0
Comp/Decomp	0/0
Auth Failures	0
Recv Errors	0
Send Errors	0
Gateway	130.2.2.2
Outer IP	100.2.2.232
Inner IP	10.10.5.1
Gateway Version	0.0.0
Inactivity Timeout	0
DH2-AES128-SHA-1 days	

7.3. VPN Concentrator Logging

The VPN Concentrator **Live Event Log** displays the current event log contents of the VPN Concentrator to the Manager GUI with updates every 5 seconds. The Live Event Log snapshot shown below contains the IKE Phase1, IKE Phase2 and XAUTH events logged as a single Avaya VPNremote Phone successfully authenticates and establishes an IPSec tunnel. Key events are highlighted in bold.

To access to the VPN Contractor Live Event Log, select **Monitoring → Filterable Event Log → Live Event Log**.

```
17081 11/15/2006 16:06:31.410 SEV=4 IKE/52 RPT=533 100.2.2.232
Group [VPNPHONE] User [ehope]
User (ehope) authenticated.

17082 11/15/2006 16:06:31.510 SEV=5 IKE/184 RPT=533 100.2.2.232
Group [VPNPHONE] User [ehope]
Client Type:
Client Application Version:
```

17083 11/15/2006 16:06:31.510 SEV=4 IKE/131 RPT=533 100.2.2.232
Group [VPNPHONE] User [ehope]
Received unknown transaction mode attribute: 14

17084 11/15/2006 16:06:31.660 SEV=4 AUTH/22 RPT=524 100.2.2.232
User [ehope] Group [VPNPHONE] connected, Session Type: IPSec

17085 11/15/2006 16:06:31.660 SEV=4 IKE/119 RPT=560 100.2.2.232
Group [VPNPHONE] User [ehope]
PHASE 1 COMPLETED

17086 11/15/2006 16:06:31.660 SEV=5 IKE/25 RPT=798 100.2.2.232
Group [VPNPHONE] User [ehope]
Received remote Proxy Host data in ID Payload:
Address 10.10.5.1, Protocol 0, Port 0

17089 11/15/2006 16:06:31.660 SEV=5 IKE/34 RPT=798 100.2.2.232
Group [VPNPHONE] User [ehope]
Received local IP Proxy Subnet data in ID Payload:
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

17092 11/15/2006 16:06:31.660 SEV=5 IKE/66 RPT=733 100.2.2.232
Group [VPNPHONE] User [ehope]
IKE Remote Peer configured for SA: VPNphone SA

17093 11/15/2006 16:06:31.660 SEV=5 IKE/75 RPT=616 100.2.2.232
Group [VPNPHONE] User [ehope]
Overriding Initiator's IPSec rekeying duration from 86400 to 28800 seconds

17095 11/15/2006 16:06:31.750 SEV=4 IKE/49 RPT=616 100.2.2.232
Group [VPNPHONE] User [ehope]
Security negotiation complete for User (ehope)
Responder, Inbound SPI = 0x573ade19, Outbound SPI = 0xa161c17f

17098 11/15/2006 16:06:31.750 SEV=4 IKE/120 RPT=616 100.2.2.232
Group [VPNPHONE] User [ehope]
PHASE 2 COMPLETED (msgid=0d357733)

17099 11/15/2006 16:06:31.750 SEV=4 NAC/27 RPT=616
NAC is disabled for peer - PUB_IP:100.2.2.232, PRV_IP:10.10.5.1

7.4. VPN Concentrator Active Sessions

The active VPN sessions to the VPN Concentrator can be viewed by selecting **Monitoring** → **Sessions** from the left navigation menu of the VPN Concentrator Manager.

Active IPSec tunnels are shown in the **Remote Access Sessions** category of the display. The screen shot below shows the **Remote Access Sessions** of four VPNremote Phones with active tunnels to the VPN Concentrator.

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

<u>Username</u>	<u>Assigned IP Address</u> <u>Public IP Address</u>	<u>Group</u>	<u>Protocol</u> <u>Encryption</u>	<u>Login Time</u> <u>Duration</u>	<u>Client Type</u> <u>Version</u>	<u>Bytes Tx</u> <u>Bytes Rx</u>	<u>NAC Result</u> <u>Posture Token</u>
owen	10.10.5.2 100.2.2.34	VPNPHONE	IPSec 3DES-168	Nov 17 7:59:49 0:06:13	N/A N/A	49072 11520	N/A
ehope	10.10.5.1 100.2.2.232	VPNPHONE	IPSec 3DES-168	Nov 17 8:00:44 0:05:18	N/A N/A	48880 11424	N/A
evan	10.10.5.3 100.2.2.234	VPNPHONE	IPSec 3DES-168	Nov 17 8:05:37 0:00:25	N/A N/A	48224 10512	N/A
garrett	10.10.5.4 100.2.2.231	VPNPHONE	IPSec 3DES-168	Nov 17 8:05:58 0:00:04	N/A N/A	288 288	N/A

7.5. VPN Concentrator IPSec Statistics

The VPN Concentrator IPSec statistics can be viewed by selecting **Monitoring** → **Statistics** → **IPSec** from the left navigation menu of the VPN Concentrator Manager.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address is <http://192.168.1.198/access.html>. The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu on the left includes Configuration, Administration, Monitoring, and Statistics. The Monitoring section is expanded, showing Routing Table, Dynamic Filters, Filterable Event Log, System Status, Sessions, and Statistics. The Statistics section is further expanded, showing Accounting, Address Pools, Administrative AAA, Authentication, Authorization, Bandwidth Mgmt, Compression, DHCP, DNS, Events, Filtering, HTTP, IPSec, L2TP, Load Balancing, NAT, PPTP, SSH, SSL, Telnet, VRRP, and MIB-II Stats. The IPSec section is selected, displaying two tables: IKE (Phase 1) Statistics and IPSec (Phase 2) Statistics. The date and time are Friday, 17 November 2006 13:56:46. The status bar at the bottom shows "IPSec/IKE Statistics" and "Local intranet".

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	4	Active Tunnels	4
Total Tunnels	956	Total Tunnels	430
Received Bytes	2306921	Received Bytes	32699864
Sent Bytes	980968	Sent Bytes	52729112
Received Packets	8275	Received Packets	419652
Sent Packets	6111	Sent Packets	398934
Received Packets Dropped	272	Received Packets Dropped	273
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	631	Sent Packets Dropped	0
Sent Notifies	81	Inbound Authentications	419379
Received Phase-2 Exchanges	1243	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	3	Outbound Authentications	398934
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	419379
Rejected Received Phase-2 Exchanges	528	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	398934
Phase-2 SA Delete Requests Received	401	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	250	System Capability Failures	0
Initiated Tunnels	0	No-SA Failures	0
Failed Initiated Tunnels	0	Protocol Use Failures	0
Failed Remote Tunnels	535		
Authentication Failures	14		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	56		

8. Trouble Shooting

This section offers some common configuration mismatches between the VPNremote Phone and the VPN Concentrator to assist in troubleshooting. The key events of the logs are highlighted in bold.

8.1. Incorrect User Name

- **VPNremote Phone display:**

Initial display shows the following:

Enter Username and Password

Password:

After a short period of time with no input (5 minutes) the display shows the following:

Invalid password OR user name

Press the **More** soft button to display the following:

Error Code: 3997700:0

Module: IKECFG:340

- **VPN Concentrator Log:**

```
23926 11/17/2006 11:22:37.730 SEV=3 AUTH/5 RPT=13 100.2.2.232
```

```
Authentication rejected: Reason = User was not found
```

```
handle = 350, server = Internal, user = ehop, domain = <not specified>
```

8.2. Incorrect User Password

- **VPNremote Phone display:**

Initial display shows the following:

Enter Username and Password

Password:

After a short period of time with no input (5 minutes) the display shows the following:

Invalid password OR user name

Press the **More** soft button to display the following:

Error Code: 3997700:0

Module: IKECFG:340

- **VPN Concentrator Log:**

```
23898 11/17/2006 11:19:20.650 SEV=3 AUTH/5 RPT=12 100.2.2.232
```

```
Authentication rejected: Reason = Invalid password
```

```
handle = 346, server = Internal, user = ehope, domain = <not specified>
```

8.3. Incorrect Group Name

- **VPNremote Phone display:**

IKE Phase 1 No Response

Press the **More** soft button to display the following:

Error Code: 3997700:0

Module: IKEMPD:164

Press the **Next** soft button to display the following:

Module: IKECFG:321

- **VPN Concentrator Log:**

```
23974 11/17/2006 11:26:34.650 SEV=4 IKE/165 RPT=449 100.2.2.232
Group [VPNC_Base_Group]
Client IKE Auth mode differs from the group's configured Auth mode

23976 11/17/2006 11:26:35.650 SEV=4 IKE/165 RPT=450 100.2.2.232
Group [VPNC_Base_Group]
Client IKE Auth mode differs from the group's configured Auth mode

23978 11/17/2006 11:26:37.650 SEV=4 IKE/165 RPT=451 100.2.2.232
Group [VPNC_Base_Group]
Client IKE Auth mode differs from the group's configured Auth mode

23980 11/17/2006 11:26:39.650 SEV=4 IKE/165 RPT=452 100.2.2.232
Group [VPNC_Base_Group]
Client IKE Auth mode differs from the group's configured Auth mode
```

8.4. Incorrect Pre-Shared Key

- **VPNremote Phone display:**

Invalid PSK or Group Password

Press the **More** soft button to display the following:

IKE PSK mismatch

Error Code: 3997698:0

Module: HASH:227

Press the **Next** soft button to display the following:

Error Code: 3997700:0

Module: IKECFG:316

- **VPN Concentrator Log:**

No events are logged on the VPN Concentrator when PSK is incorrect.

8.5. Mismatched Phase 1 Proposal

- **VPNremote Phone display:**

IKE Pase 1 no response

Press the **More** soft button to display the following:

Error Code: 3997700:0

Module: IKMPD:164

Press the **Next** soft button to display the following:

Error Code: 3997700:0

Module: IKECFG:321

- **VPN Concentrator Log:**

```
24219 11/17/2006 13:20:37.150 SEV=5 IKE/226 RPT=6 100.2.2.232
All IKE SA proposals found unacceptable!
```

```
24220 11/17/2006 13:20:39.180 SEV=5 IKE/226 RPT=7 100.2.2.232
All IKE SA proposals found unacceptable!
```

8.6. Mismatched Phase 2 Proposal

- **VPNremote Phone display:**

IKE Pase 2 no response

Press the **More** soft button to display the following:

Error Code: 3997700:0

- **VPN Concentrator Log:** (some non-relevant log entries removed for brevity)

```
24343 11/17/2006 13:42:29.700 SEV=4 IKE/119 RPT=982 100.2.2.232
Group [VPNPHONE] User [ehope]
PHASE 1 COMPLETED
```

```
24351 11/17/2006 13:42:29.700 SEV=4 IKE/227 RPT=515 100.2.2.232
Group [VPNPHONE] User [ehope]
All IPsec SA proposals found unacceptable!
```

```
24352 11/17/2006 13:42:29.700 SEV=4 IKEDBG/97 RPT=583 100.2.2.232
Group [VPNPHONE] User [ehope]
QM FSM error (P2 struct &0xbb45548, mess id 0xeald942)!
```

```
24354 11/17/2006 13:42:29.710 SEV=4 AUTH/23 RPT=515 100.2.2.232
User [ehope] Group [VPNPHONE] disconnected: duration: 0:00:00
```

8.7. No IP Pool Addresses Available

- **VPNremote Phone display:**

Missing ike configuration

Press the **More** soft button to display the following:

Error Code: 3997700:0

Module: IKECFG:498

- **VPN Concentrator Log:**

24634 11/17/2006 14:04:26.640 SEV=5 IKE/132 RPT=7 100.2.2.34

Group [VPNPHONE] User [owen]

Cannot obtain an IP address for remote peer - exhausted all available addresses

(held address count = 0)

The VPN Concentrator IP Address Pools status can be viewed by selecting **Monitoring** → **Statistics** → **Address Pools** from the left navigation menu of the VPN Concentrator Manager.

The screen shot below shows the **IP Address Pool** for the VPNPHONE group created in **Section 4.8**. To demonstrate IP Address depletion, the available IP addresses were modified to offer only three IP addresses.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.1.198/access.html>. The page title is "VPN 3000 Concentrator Series Manager". The user is logged in as "admin". The navigation menu on the left includes Configuration, Administration, and Monitoring. The Monitoring section is expanded, showing Routing Table, Dynamic Filters, Filterable Event Log, System Status, Sessions, Statistics, Accounting, Address Pools, and Administrative AAA. The Address Pools link is selected. The main content area shows the "Monitoring | Statistics | Address Pools" view for the "VPNPHONE" group. The IP Address Range is 10.10.5.1 to 10.10.5.3. The table shows the status of the IP address pool.

Group	IP Address Range		Addresses				
	Start	End	Total	Available	Allocated	Held	Max Allocated
VPNPHONE	10.10.5.1	10.10.5.3	3	0	3	0	3

8.8. Graceful Reboot of VPNremote Phone

- **VPNremote Phone display:**

```
Rebooting...
```

- **VPN Concentrator Log:**

```
23892 11/17/2006 11:18:36.340 SEV=5 IKE/50 RPT=400 100.2.2.232
Group [VPNPHONE] User [ehope]
Connection terminated for peer ehope.
Reason: Peer Terminate
Remote Proxy 10.10.5.1, Local Proxy 0.0.0.0

23895 11/17/2006 11:18:36.350 SEV=4 AUTH/28 RPT=413 100.2.2.34
User [owen] Group [VPNPHONE] disconnected:
  Session Type: IPSec
  Duration: 0:18:47
  Bytes xmt: 56176
  Bytes rcv: 17776
Reason: User Requested
```

9. Conclusion

The Avaya VPNremote Phone combined with Cisco VPN Concentrator security appliance provides a secure solution for remote worker telephony over any broadband Internet connection. The Avaya VPNremote Phone XAUTH implementation for Cisco security appliances (utilizing the **Cisco Xauth with PSK** profile) demonstrated successful interoperability with the Cisco VPN Concentrator.

10. References

- [1] *Avaya VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide*,
Doc ID: 19-600753
- [2] *VPNremote for 46xx Series IP Telephone Installation and Deployment Guide*,
Doc ID: 1022006
- [3] *Administrators Guide for Avaya Communication Manager*,
Doc ID: 03-300509
- [4] *Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote™ Phone Release 2 – Issue 1.0*, Avaya Application Note
- [5] **Avaya Application Notes and Resources Web Site:**
<http://www.avaya.com/gcm/master-usa/en-us/resource/>
- [6] **Avaya Product Support Web Site:**
<http://support.avaya.com/japple/css/japple?PAGE=Home>
- [7] *Cisco VPN 3000 Series Concentrator Getting Started, Release 4.7*
- [8] *Cisco VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7*

©2006 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