Avaya Solution & Interoperability Test Lab

Configuring Universal Port with Extreme Networks Summit X450e-48p to Support Avaya IP Telephones – 1.0

Abstract

These Application Notes describe the steps for configuring Universal Port (UP) for the Extreme Networks Summit X450e-48p switch to dynamically configure the switch to support an Avaya IP Telephone and attached PC. The UP feature provides a framework to use scripting within the Extreme Networks switch to perform many Command Line Interface (CLI) commands dynamically based on trigger events. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Universal Port (UP) feature is supported beginning with release 11.6 version of Extreme Networks XOS software. The UP feature is a flexible framework that allows the switch to take direct action based on events. The focus is on edge ports with the switch applying dynamic profiles (such as security) based on user login, and Power Over Ethernet (PoE) configuration based on Link Layer Discovery Protocol (LLDP) device discovery, and Virtual Local Area Network (VLAN) assignment.

These Application Notes describe a solution using a combination of the UP feature with LLDP to dynamically provision the X450e switch and Avaya IP Telephone. The UP feature relies on a trigger event to initiate a preconfigured script called a profile to dynamically configure the switch port. The four types of trigger events described in these Application Notes are Device-Detect, Device-Undetect, User-Authenticated, and User-Unathenticated. These trigger events can be grouped into two corresponding working pairs (Device-Detect with Device-Undetect, and User-Authenticated with User-Unauthenticated). These trigger events work as follows:

- Device-Detect – Triggered when device is connected to a switch port
- Device-Undetect – Triggered when device is disconnected from a switch port
- User-Authenticated – Triggered when device is successfully authenticated
- User-Unauthenticated – Triggered when device is unauthenticated after being successfully authenticated earlier

Figure 1 illustrates the sample network configuration used in these Application Notes. The UP feature is only enabled and configured in the X450e switch in the sample network. Each device connected to the X450e switch is dynamically assigned an IP address by the Dynamic Host Configuration Protocol (DHCP) server. For illustration purpose, Port 11 on the X450e switch is configured to use the User-Authenticated and User-Unauthenticated trigger events, and port 7 on the X450e switch is configured to use the Device-Detect and Device-Undetect trigger events. The same profile and event trigger used in the sample network can be assigned to all ports on the switch thus allowing the Avaya IP Telephone to be connected to any port with system administrator having to pre-program any of the port.

When an Avaya IP Telephone is connected into port 7, the Device-Detect event will trigger the "connect" profile associated with the Device-Detect event to be executed. This "connect" profile assigns port 7 to the voice VLAN as tagged and notifies the Avaya IP Telephone to enable 802.1Q Trunking. The Avaya IP Telephone will then save this information into NVRAM and reboot, and subsequently send traffic using an 802.1Q frame to request an IP address. This is no different than how the Avaya IP Telephone operates when DHCP option 176 is used to assigned VLAN information. During the reboot, the Device-Undetect event will be triggered due to link-down condition. The Device-Detect event will trigger the execution of the "connect" profile a second time as the Avaya IP Telephone boots up again. Using LLDP, the switch will advertise the address to be used for Avaya Communication Manager registration as well as a TFTP server address.

For port 11, the Avaya IP Telephone must be authenticated by the Internet Authentication Service (IAS) server using 802.1X authentication. Once authenticated, the User-Authenticated event will trigger the execution of the "aconnect" profile associated with the User-Authenticated event. The IAS server will also notify the switch using RADIUS Vendor Specific Attribute (VSA) as to what VLAN the switch port should be assigned. The "aconnect" profile also notifies the Avaya IP Telephone to enable 802.1Q Trunking. The Avaya IP Telephone will then save this information into NVRAM and reboot, and subsequently send traffic using an 802.1Q frame to request an IP address. During the reboot, the User-Unauthenticated event will be triggered due to un-authenticated condition. The User-Authenticated event will trigger the execution of the "aconnect" profile a second time as the Avaya IP Telephone is rebooted and re-authenticated. Using LLDP, the switch will advertise the address to be used for Avaya Communication Manager registration as well as a TFTP server address.

The PC connected to port 11 through the Avaya IP Telephone is independently authenticated by the IAS server via 802.1X. Through the use of RADIUS VSA, port 11 will be provisioned with the "data" VLAN as untagged. The PC will acquire an IP address through DHCP and connect to the network.

Through the use of the UP feature, switch port provisioning can be dynamically initiated as devices such as Avaya IP Telephones or PCs are moved from port to port or switch to switch, without requiring an administrator to be actively involved. In addition, any LLDP attribute such as model number or software version of an Avaya IP Telephone can be incorporated into the UP profile. Conditional statements (such as "IF … THEN …" statements) can be used to further refine how a switch port should be programmed or what information should be advertised to the attached device.

2. Configuration

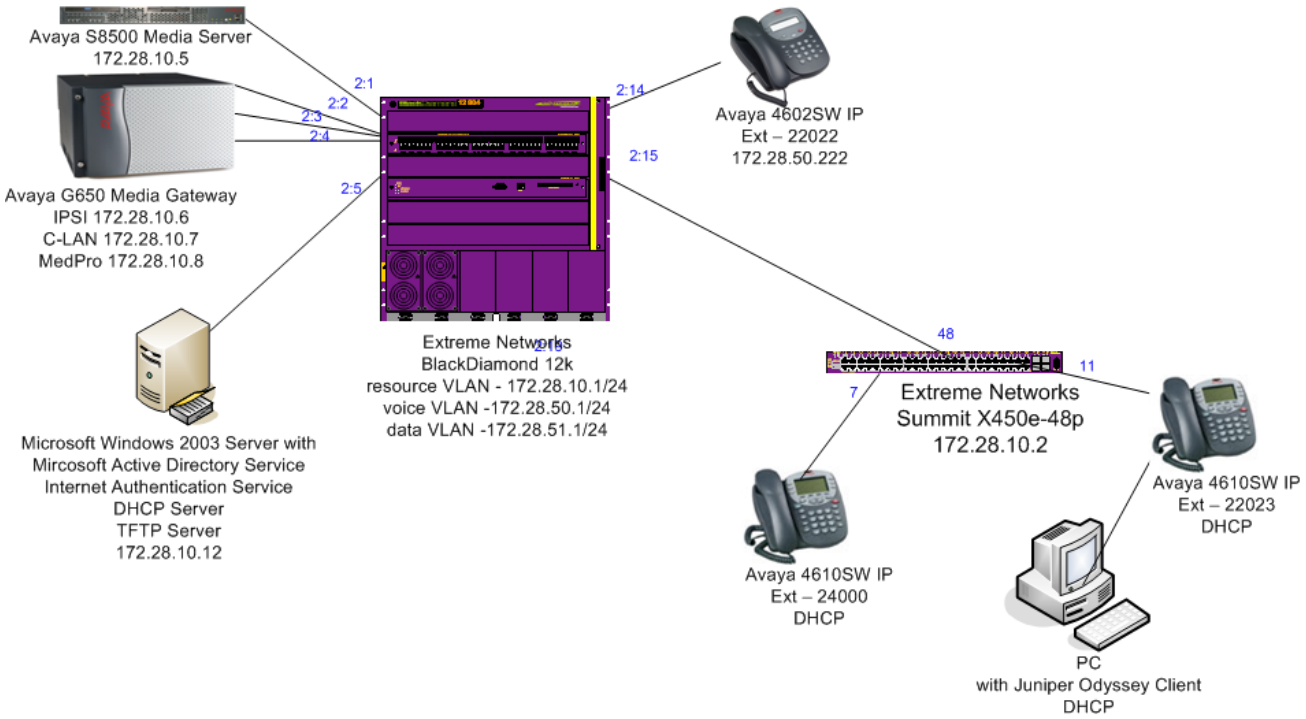


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Media Server	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway	
TN2312BP IPSI	FW 22
TN799DP C-LAN	FW 16
TN2302AP MedPro	FW 108
Avaya 4602SW IP Telephone	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone	R2.6 – Application (a10d01b2_6.bin)
Extreme Networks X450e-48p	ExtremeXOS 11.6.1.9
Extreme Networks BlackDiamond 12k	ExtremeXOS 11.4.3.4
Microsoft Windows running	2003 Server Enterprise Edition
Active Directory Users and Computers	5.2.3790.1830
Internet Authentication Service	5.2.3790.1830
DHCP Server	5.2.3790.1830
Juniper Networks Odyssey Client on PC running Microsoft Windows 2003 Server	4.50.0.2496

4. Configure the Extreme Networks Switches

This section describes the configuration for Extreme Network X450e-48p and BlackDiamond 12k as shown in **Figure 1**.

4.1. Configure the X450e-48p

This section shows the necessary steps in configuring the X450e-48p as shown in the **Figure 1**.

Step	Description

1.	Connect to the X450e-48p switch and log in using appropriate credentials.
	
	`login: ***username***`
	`password: ***xxxxxx***`

Step	Description

2.	Create the VLANs on the switch. The IP address assignment is optional. All routing is performed by the Black Diamond 12k. The VLAN name to be used by the Avaya IP Telephone must begin with the word "voice".
	
	`X450e-48p.1 # create vlan resource`
	`X450e-48p.1 # config vlan resource tag 10`
	`X450e-48p.1 # config vlan resource ipaddress 172.28.10.2/24`
	`X450e-48p.1 # create vlan voice`
	`X450e-48p.1 # config vlan voice tag 50`
	`X450e-48p.1 # config vlan voice ipaddress 172.28.50.2/24 (optional)`
	`X450e-48p.1 # create vlan data`
	`X450e-48p.1 # config vlan data tag 51`
	`X450e-48p.1 # config vlan data ipaddress 172.28.51.2/24 (optional)`

3.	Configure VLAN assignment for the ports. Port 11 will be dynamically configured via the UP feature as a device is connected to the port.
	
	`X450e-48p.1 # config vlan default add port 48 untagged`
	`X450e-48p.1 # config vlan resource add port 48 tagged`
	`X450e-48p.1 # config vlan voice add port 7,48 tagged`
	`X450e-48p.1 # config vlan data add port 7 untagged`
	`X450e-48p.1 # config vlan data add port 48 tagged`

4.	Configure the switch for RADIUS authentication and enable the switch port for netlogin. The **shared-secret** must match the one configured in Section 5.2, Step 3.
	
	`X450e-48p.1 # configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.10.2 vr VR-Default`
	`X450e-48p.1 # configure radius netlogin primary shared-secret 1234567890`
	`X450e-48p.1 # enable radius netlogin`
	`X450e-48p.1 # configure netlogin vlan temp`
	`X450e-48p.1 # enable netlogin dot1x`
	`X450e-48p.1 # enable netlogin ports 11 dot1x`

5.	By default the X450e-48p only has two priority queues, QP1 and QP8. Configure a new QoS profile QP7 on the switch and remap 802.1P priority 6 to this new profile. In the sample configuration, the Avaya IP Telephones use 802.1P value 6 for media and signaling traffic. Section 8, Step 2 configures these settings in Avaya Communication Manager. 802.1P examination is enabled by default on the X450e-48p switch; therefore, there is no need to enter any additional command to enable this feature on the port.
	
	`X450e-48p.1 # create qosprofile QP7`
	`X450e-48p.1 # configure dot1p type 6 qosprofile QP7`

Step	Description
6.	Create the upm profile by using the "create upm profile <profile-name>" command at the prompt. This command will initiate a vi style editor for inputting the profile into the system. For additional information on scripting and the use of the editor, please refer to reference [6] and [7]. Steps 7-10 show the actual UP profile's scripts.

7.	The following illustrates the script for the **aconnect** profile. This profile will be used by the USER-AUTHENTICATED event.
	
	`X450e-48p.1 #` ***`create upm profile aconnect`***
	
	`#`
	`#  aconnect profile`
	`#`
	`create upm profile aconnect`
	`set var acm 172.28.10.7`
	`set var fileserver 172.28.10.12`
	`#`
	`enable lldp port $EVENT.USER_PORT`
	`#`
	`configure lldp port $EVENT.USER_PORT advertise vendor-specific dot1 vlan-name`
	`configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme call-server $acm`
	`configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme file-server $fileserver`
	`configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme dot1q-framing tag`
	`#`
	`.`

8.	The following illustrates the script for the **adisconnect** profile. This profile will be used by the USER-UNAUTHENTICATED event.
	
	`X450e-48p.1 #` ***`create upm profile adisconnect`***
	
	`#`
	`#  adisconnect profile`
	`#`
	`disable lldp port $EVENT.USER_PORT`
	`#`
	`.`

Step	Description
9.	The following illustrates the script for the **connect** profile. This profile will be used by the DEVICE-DETECT event. `X450e-48p.1 # ***create upm profile connect***  ` `#` `#  connect profile` `#` `set var voiceVlan voice` `set var dataVlan Data` `set var acm 172.28.10.7` `set var fileserver 172.28.10.12` `#` `create log entry LLDP_$EVENT.DEVICE-DETECT_on_$EVENT.USER_PORT` `#` `#  Add the port to vlan` `#` `configure $voiceVlan add port $EVENT.USER_PORT tag` `#` `#  LLDP Avaya configuration` `#` `enable lldp port $EVENT.USER_PORT` `configure lldp port $EVENT.USER_PORT advertise vendor-specific dot1 vlan-name` `configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme call-server $acm` `configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme file-server $fileserver` `configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extreme dot1q-framing tagged` `#` `.`

Step	Description

10.	The following illustrates the script for the **disconnect** profile. This profile will be used by the DEVICE-UNDETECT event.
	
	`X450e-48p.1 # create upm profile disconnect`
	
	`#`
	`#  disconnect profile`
	`#`
	`set var voicevlan voice`
	`#`
	`#`
	`#`
	`if (!$MATCH($EVENT.DEVICE_IP, 0.0.0.0)) then`
	`  enable cli scripting`
	`  create log entry "LLDP DEVICE-REMOVED, IP $(EVENT.DEVICE_IP)"`
	`else`
	`#`
	`# Remove port from VLAN and disable lldp`
	`#`
	`config $voicevlan delete port $EVENT.USER_PORT`
	`unconfig lldp port $EVENT.USER_PORT`
	`#`
	`endif`
	`#`
	`.`

11.	Assign the appropriate profile to each UPM event.
	
	`X450e-48p.1 # configure upm event user-authenticated profile aconnect ports 11`
	`X450e-48p.1 # configure upm event user-unauthenticated profile adisconnect ports 11`
	`X450e-48p.1 # configure upm event device-detect profile connect ports 7`
	`X450e-48p.1 # configure upm event device-remove profile disconnect ports 7`

4.2. Configure the BlackDiamond (BD) 12k

This section shows the necessary steps in configuring the BD12k as shown in **Figure 1**.

Step	Description

1.	Connect to the BD12k switch and log in using appropriate credentials.
	
	`login: username`
	`password: xxxxxx`

Step	Description

2.	Create the VLANs on the switch.
	
	`BD-12804.1 # create vlan resource`
	`BD-12804.1 # config vlan resource tag 10`
	`BD-12804.1 # config vlan resource ipaddress 172.28.10.1/24`
	`BD-12804.1 # enable ipforwarding resource`
	`BD-12804.1 # create vlan voice`
	`BD-12804.1 # config vlan voice tag 50`
	`BD-12804.1 # config vlan voice ipaddress 172.28.50.1/24`
	`BD-12804.1 # enable ipforwarding voice`
	`BD-12804.1 # create vlan data`
	`BD-12804.1 # config vlan data tag 51`
	`BD-12804.1 # config vlan data ipaddress 172.28.51.1/24`
	`BD-12804.1 # enable ipforwarding data`

3.	Configure VLAN assignment for the ports.
	
	`BD-12804.1 # config vlan default add port 2:15 untagged`
	`BD-12804.1 # config vlan resource add port 2:1-2:5 untagged`
	`BD-12804.1 # config vlan resource add port 2:15 tagged`
	`BD-12804.1 # config vlan voice add port 2:14,2:15 tagged`
	`BD-12804.1 # config vlan data add port 2:15 tagged`

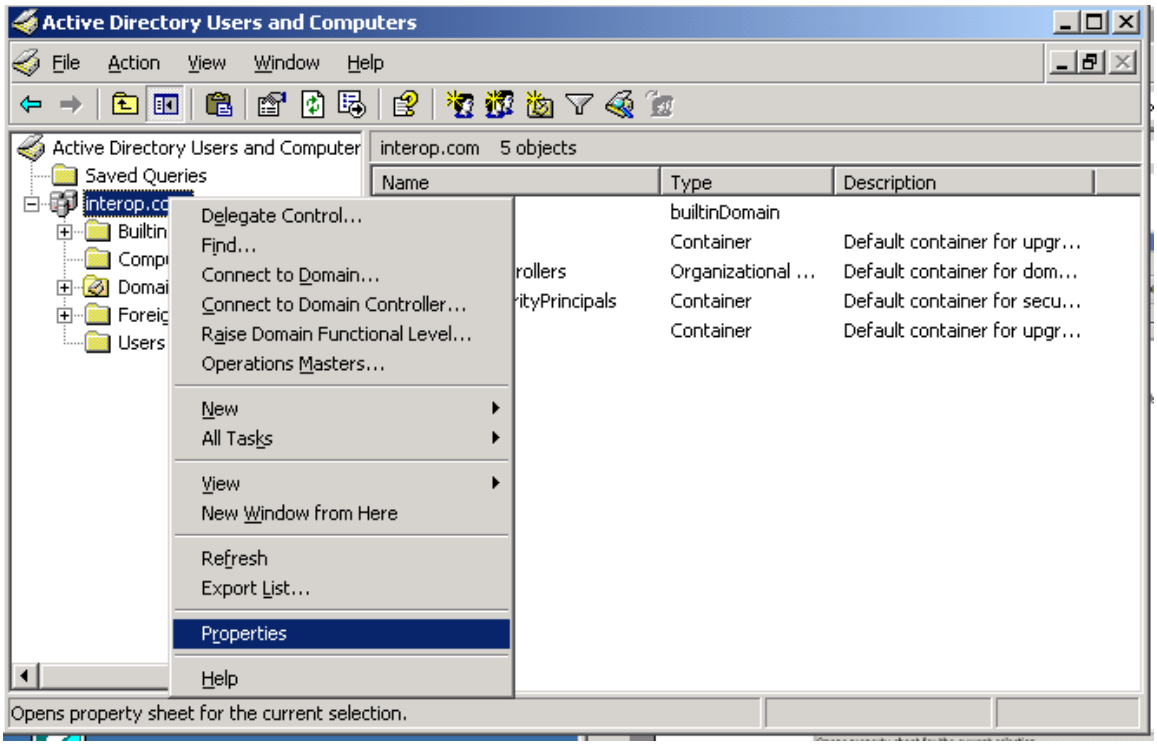
4.	Enable DiffServ Code-Point examination on the switch for ports connecting to the Avaya S8500 Media Server and G650 Media Gateway. `BD-12804.1 # enable diffserv examination ports 2:1-2:4`
5.	Configure bootprelay for DHCP request. `BD-12804.1 # configure bootprelay add 172.28.10.12 vr VR-Default`

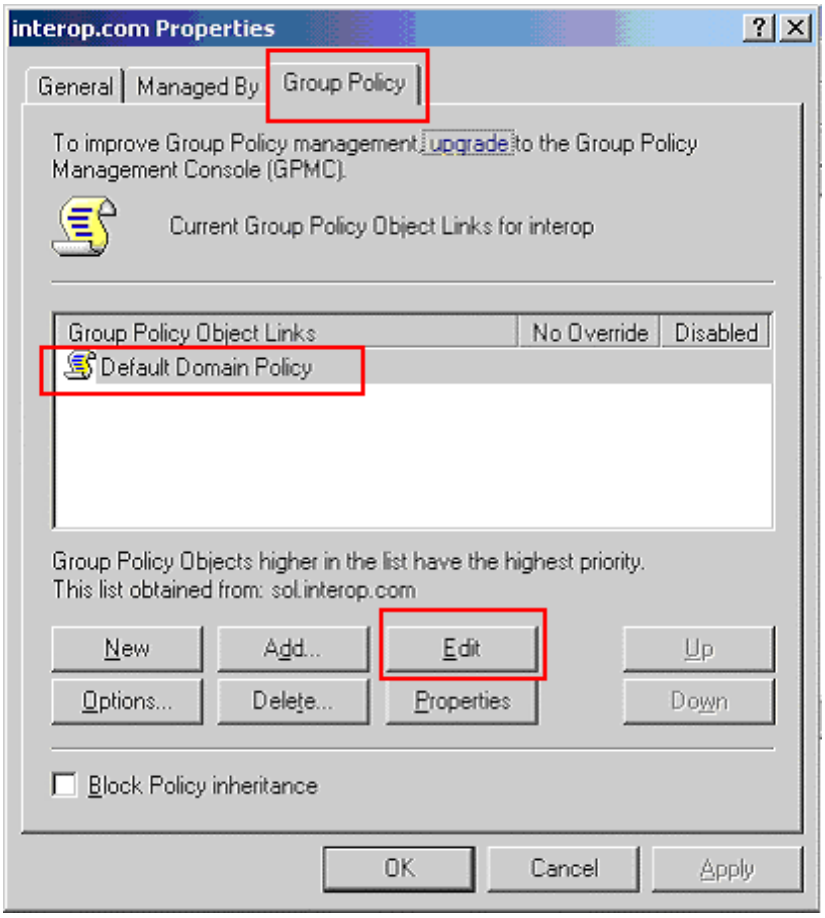
5. Configure Microsoft Services

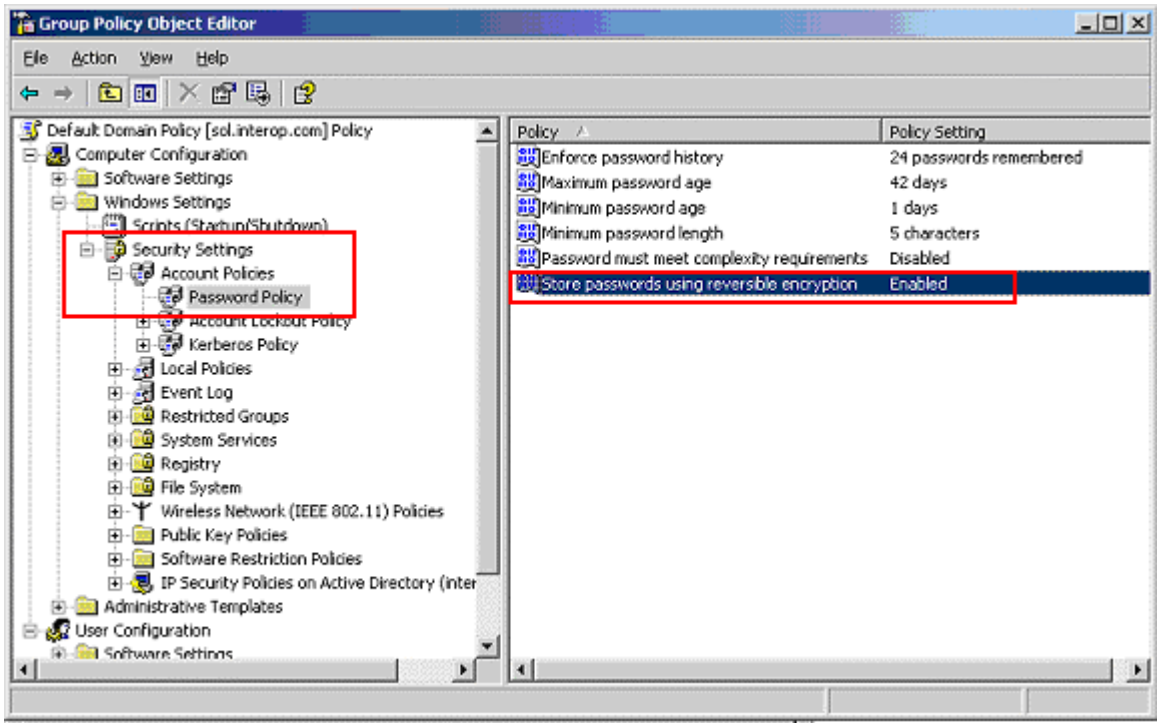
The installation of Microsoft Active Directory and Internet Authentication Services server is beyond the scope of this Application Notes and will not be covered. The configuration of the Microsoft Active Directory Service and Internet Authentication Services needed to support the sample network will be shown in the following two sections.

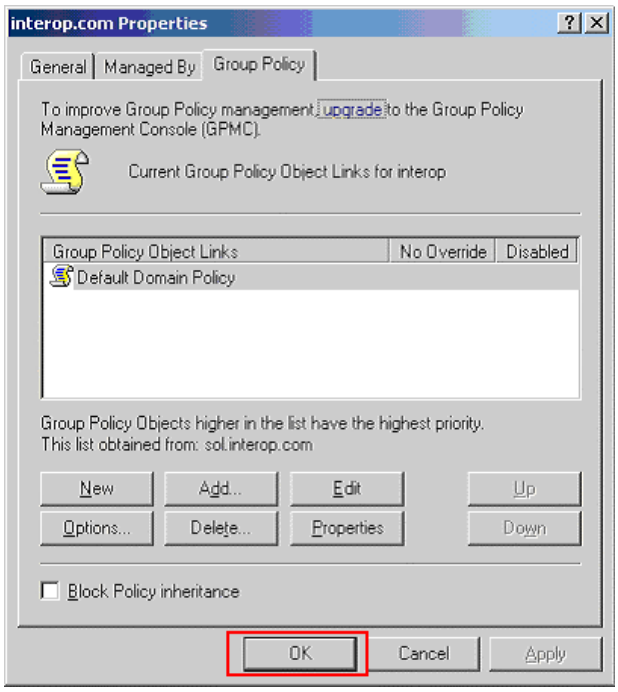
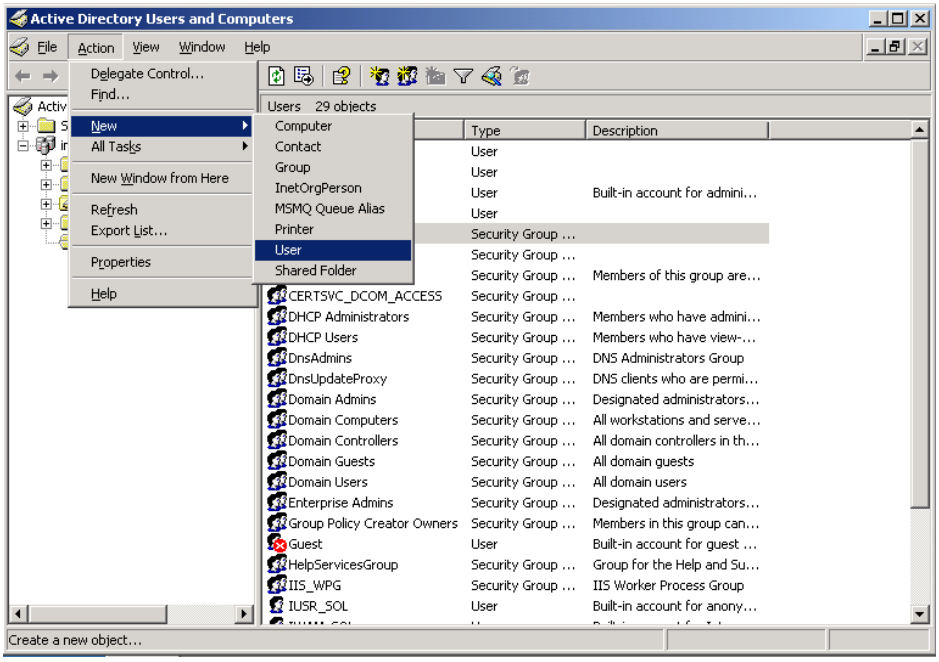
5.1. Configure the Microsoft Active Directory Service

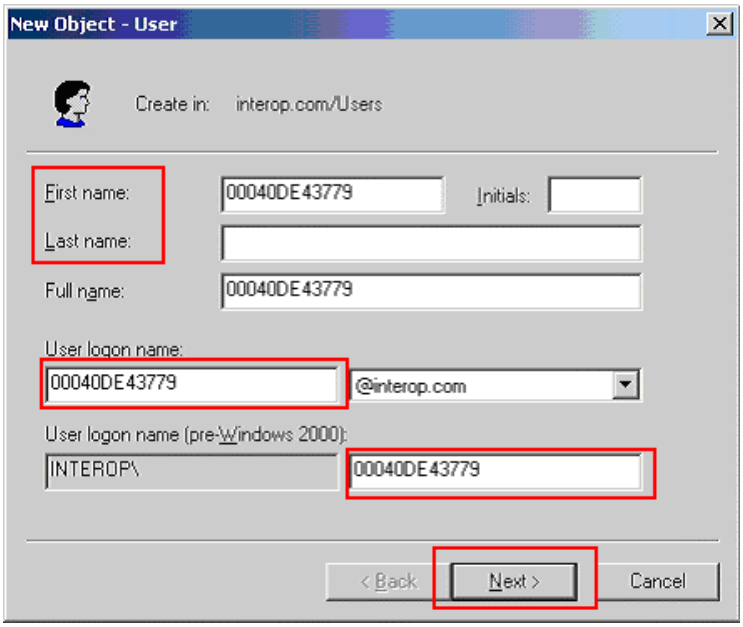
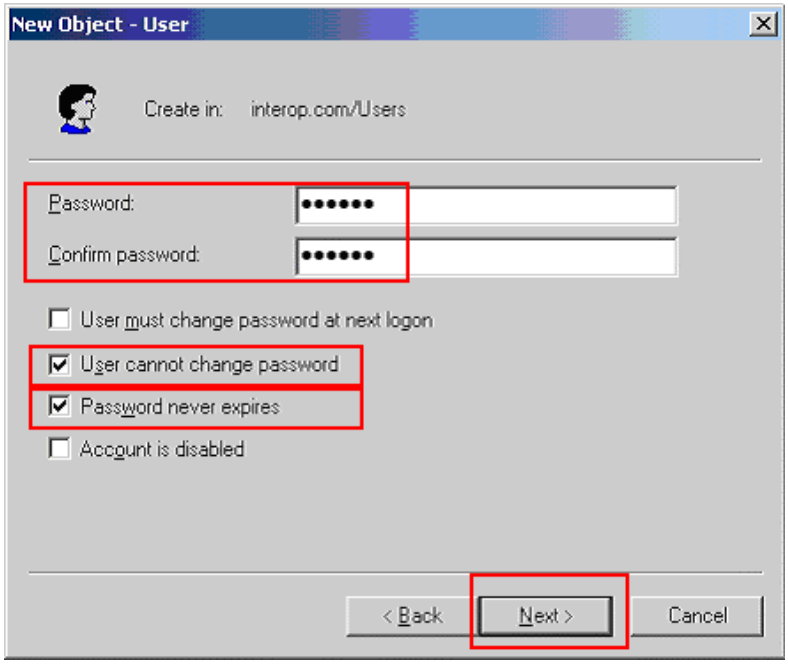
This section shows the necessary steps in configuring the Microsoft Active Directory server as shown in the **Figure 1** to support the Avaya IP Telephones and PC only.

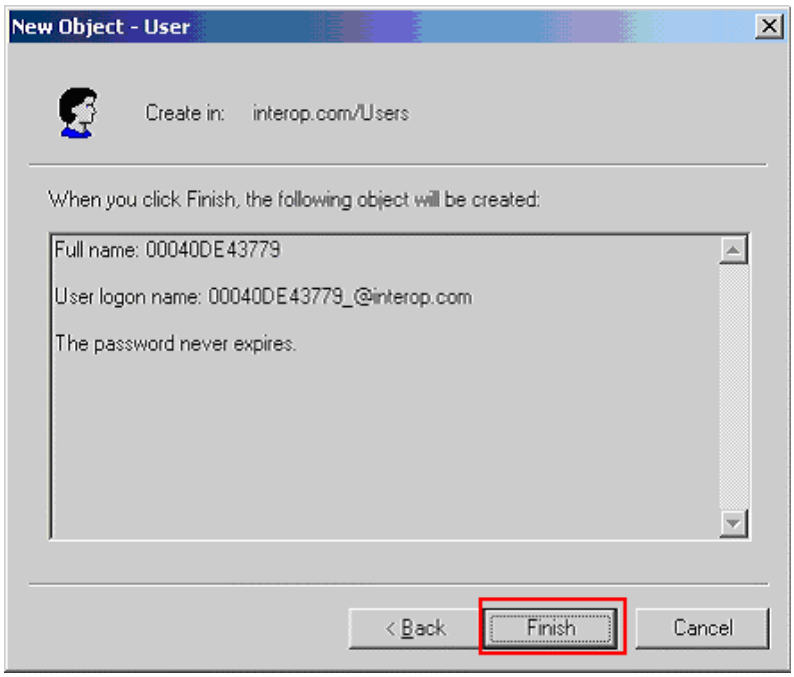
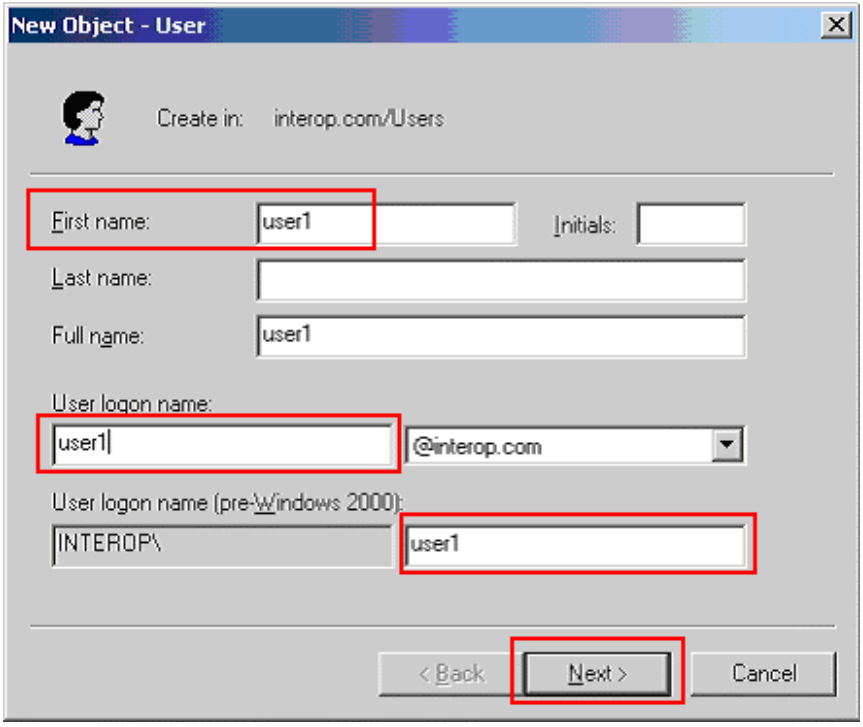
Step	Description
1.	Invoke the Active Directory Users and Computers window under Administrative Tools of a Microsoft Windows system. Configure the active directory domain properties by highlighting the Active Directory domain then right click and select **Properties**. 

Step	Description
2.	Select the **Group Policy** tab in the properties window. Highlight the **Default Domain Policy** then click **Edit** to display the Group Policy Object Editor. 

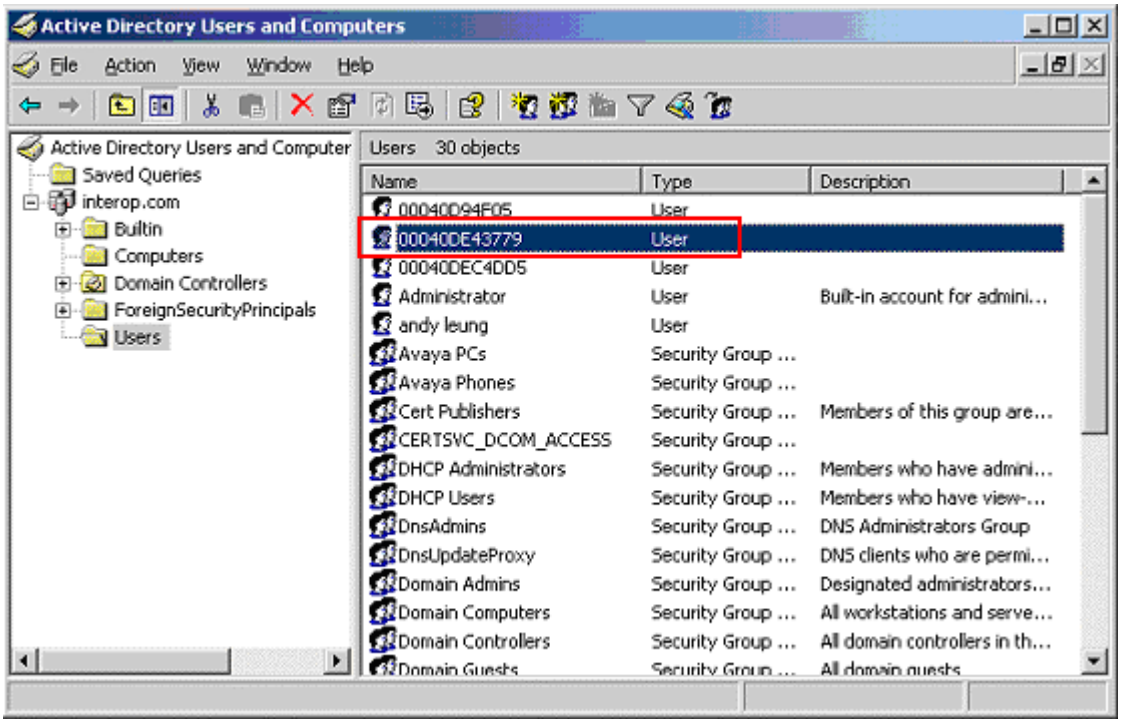
Step	Description
3.	From the Group Policy Object Editor, Navigate to **Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy** on the left panel. Double click on **Store passwords using reversible encryption policy** on the right, and change the setting to **Enabled**. 

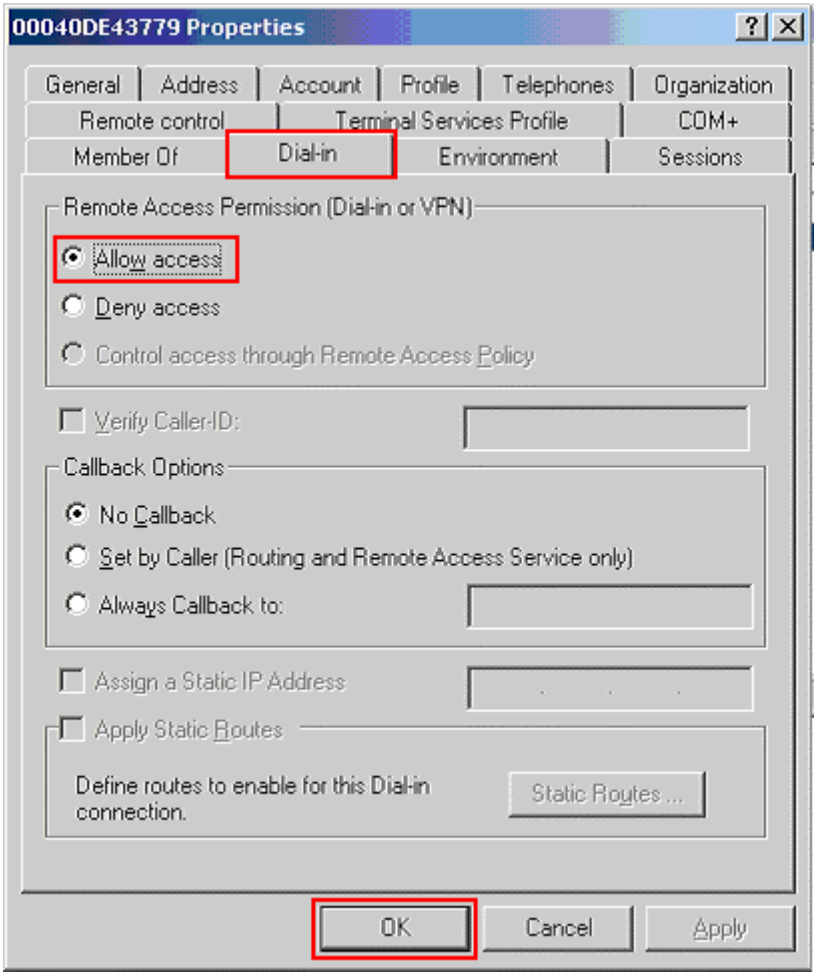
Step	Description
4.	Click **OK** on the domain properties pop-up window to complete. 
5.	Create a new user ID for an Avaya IP Telephone user and a PC user. From the Active Directory Users and Computers window menu, select **Action → New → User** to begin creating a new user ID. 

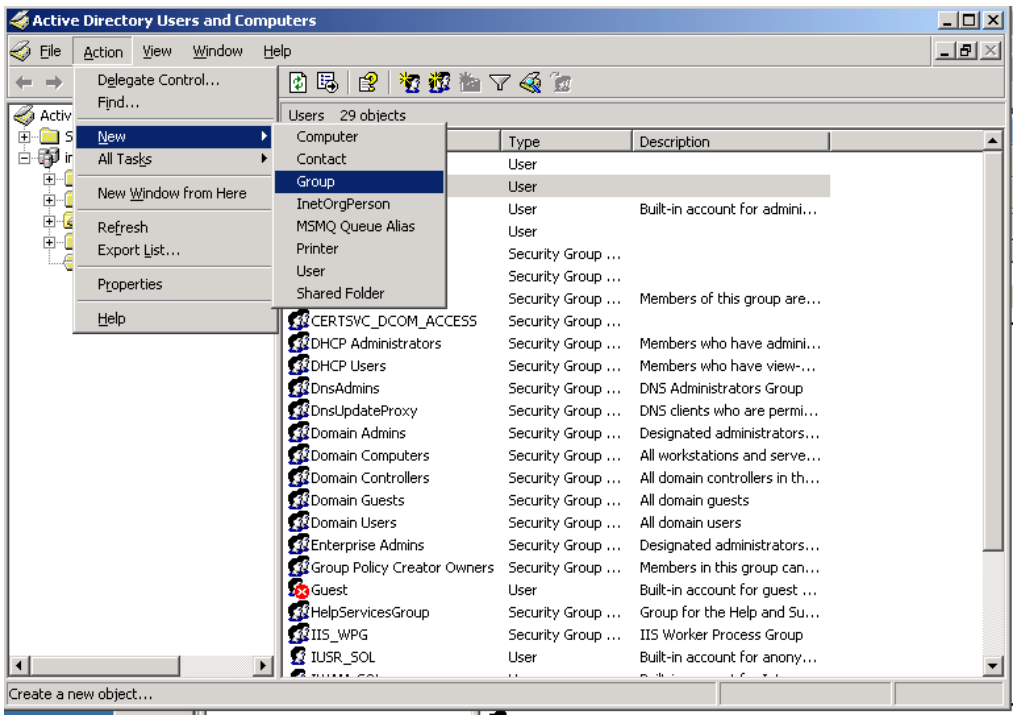
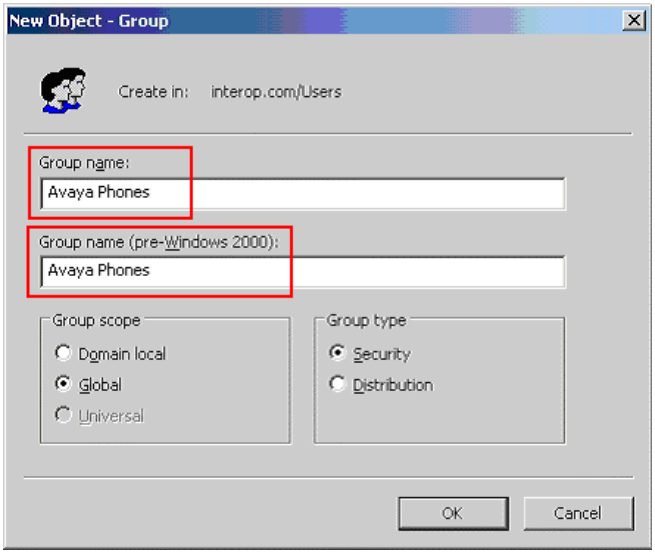
Step	Description
6.	For an Avaya IP Telephone, enter the phone's MAC address as the **User logon name**. The **First name** and **Last name** are for information only. Click **Next** to continue. 
7.	Enter a **Password** for the user ID. For an Avaya IP Telephone, enter a numeric password. Select the **User cannot change password** and **Password never expires** fields. Click **Next** to continue. 

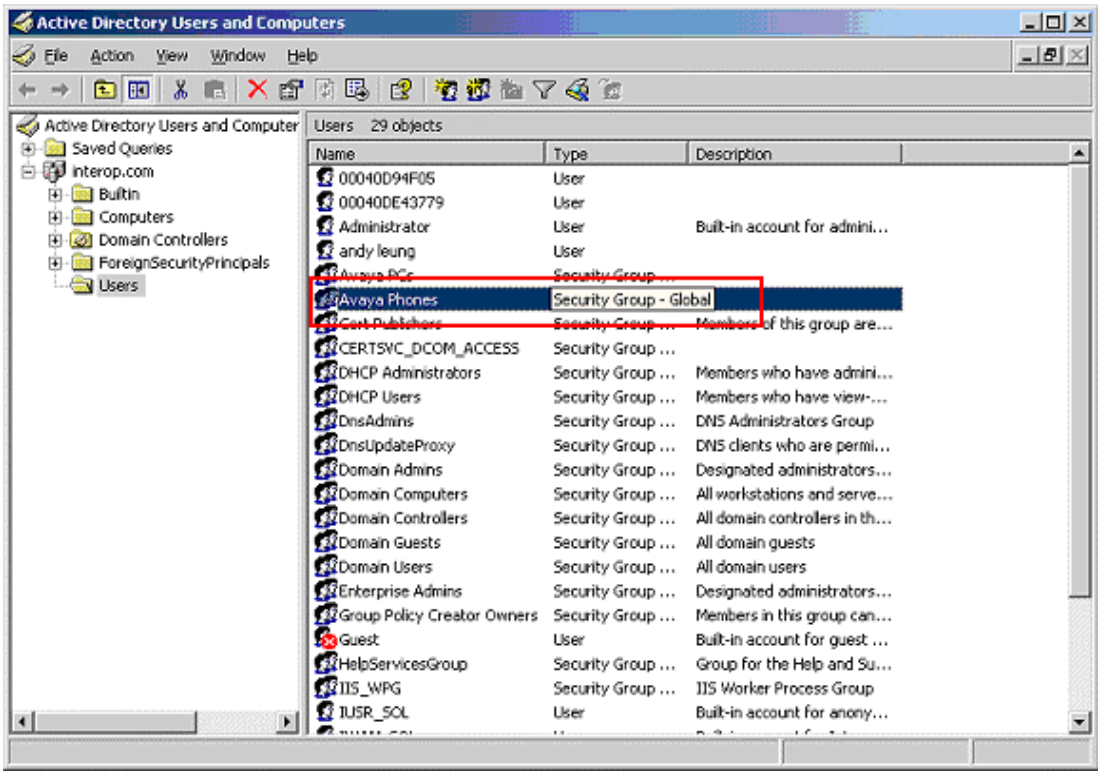
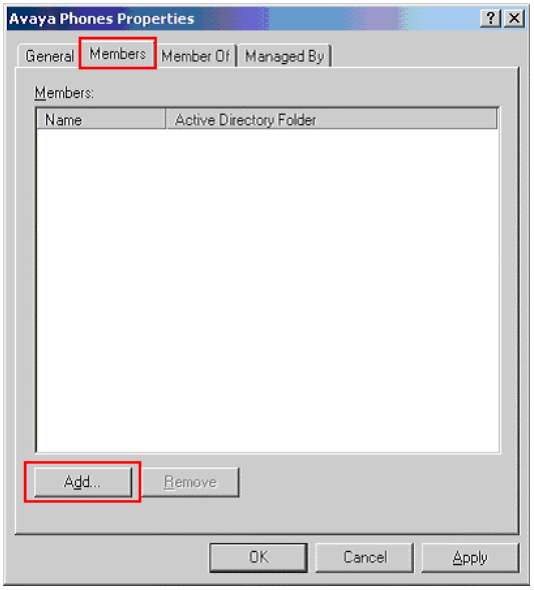
Step	Description
8.	Click **Finish** to complete. 
9.	Repeat Steps 5-8 to create a user ID for the PC. Below is a screen capture for user ID "user1" used for the PC for log in. 

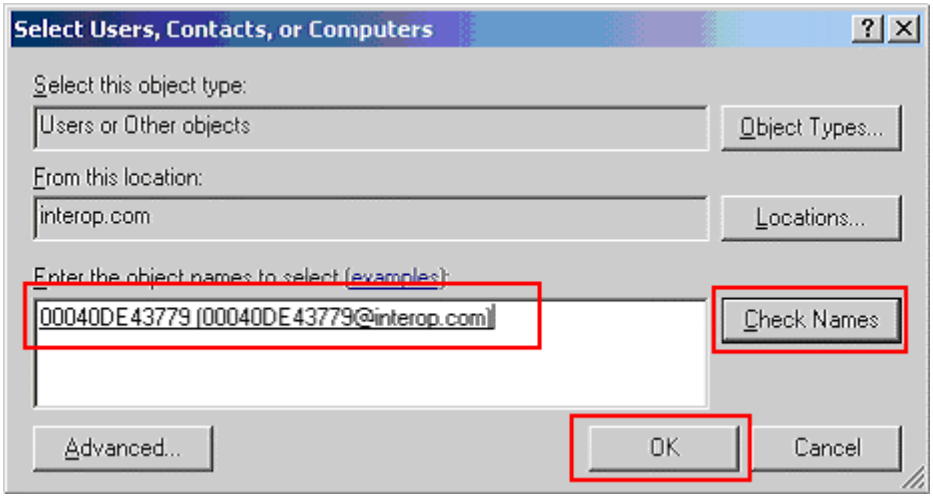
Step	Description
10.	After creating the user ID, begin editing its property by double clicking on the user ID in the Active Directory Users and Computers window.



Step	Description
11.	Select the **Dial-in** tab in the user properties window. Enable remote access by clicking on the **Allow access** radio button. Click **OK** to complete. Repeat this step for all Avaya IP Telephone and PC user IDs. 

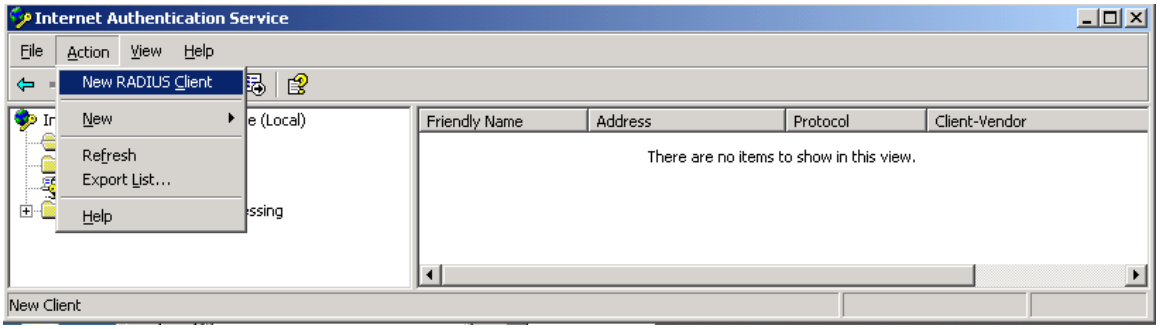
Step	Description
12.	Create a new user Group by selecting **Action → New → Group** from the drop-down menu. The use of a Group facilitates the assignment and management of additional user IDs. 
13.	Create a group for Avaya IP Telephones. The sample network uses the name Avaya Phones for this group. Click **OK** to complete. 
14.	Repeat Steps 12 and 13 to create another user Group for the PC.

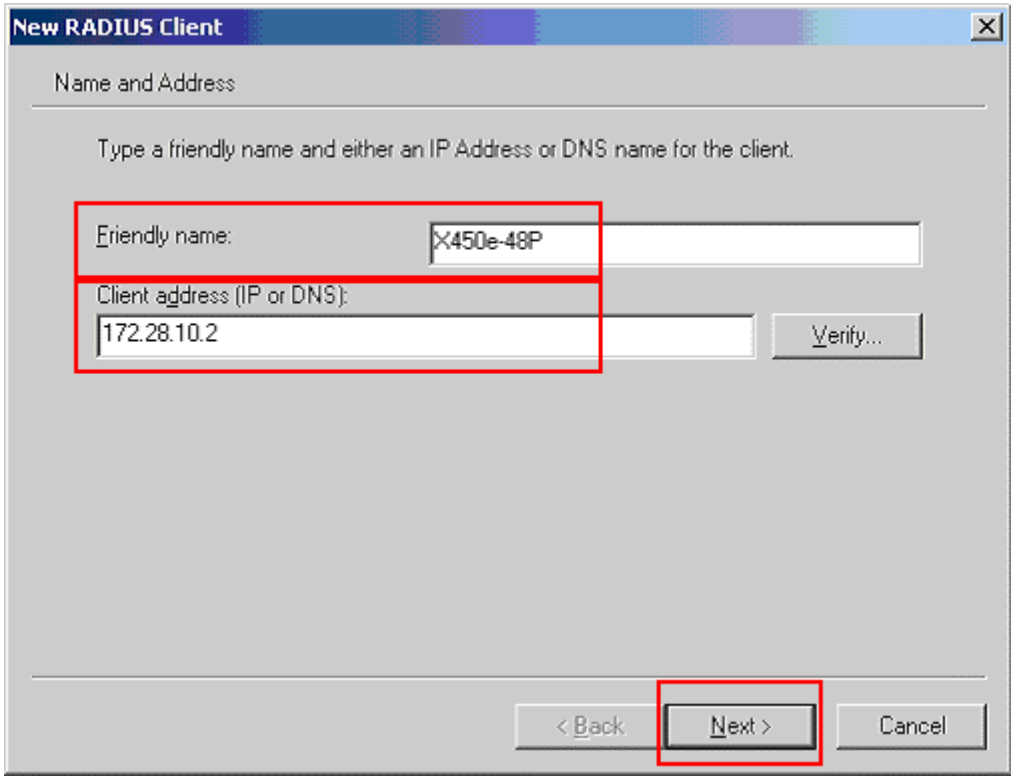
Step	Description
15.	After creating the user Group, begin editing its property by double clicking on the Group in the Active Directory Users and Computers window. 
16.	Select the **Members** tab in the group Properties window. Click **Add** to continue. 

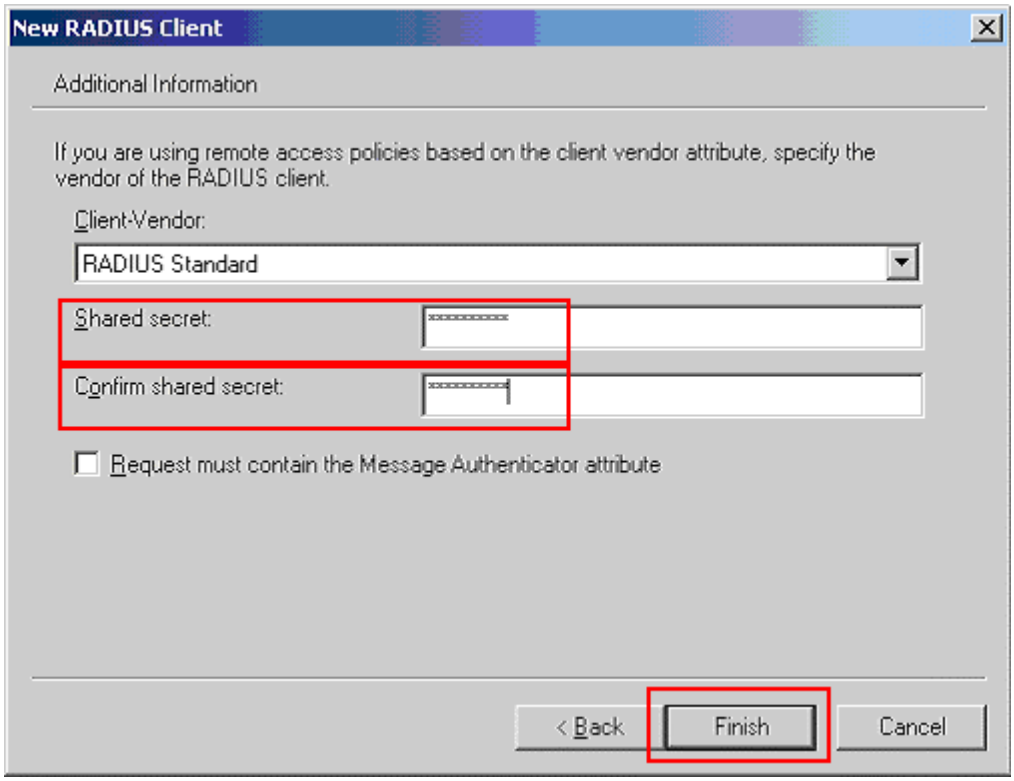
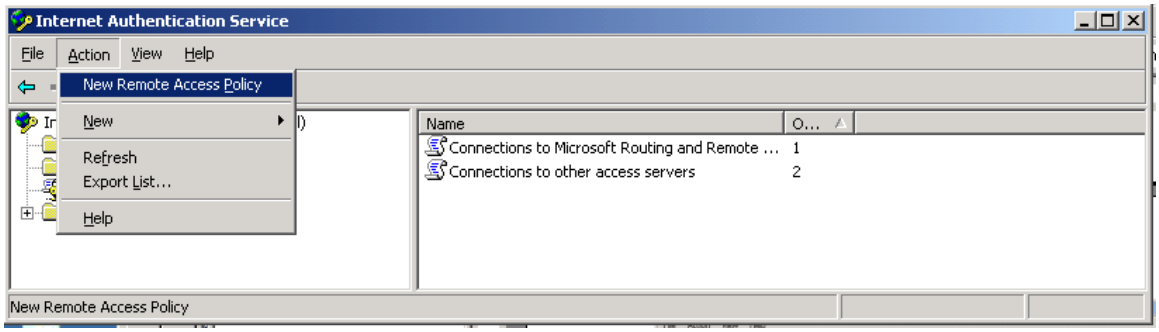
Step	Description
17.	Enter the user ID that should be assigned to the Avaya Phones group. This should be the user ID for the Avaya IP Telephone. Use **Check Names** to assist in searching for the user ID. Click **OK** to complete. 
18.	Repeat Steps 15-17 to add members to the PCs user group.

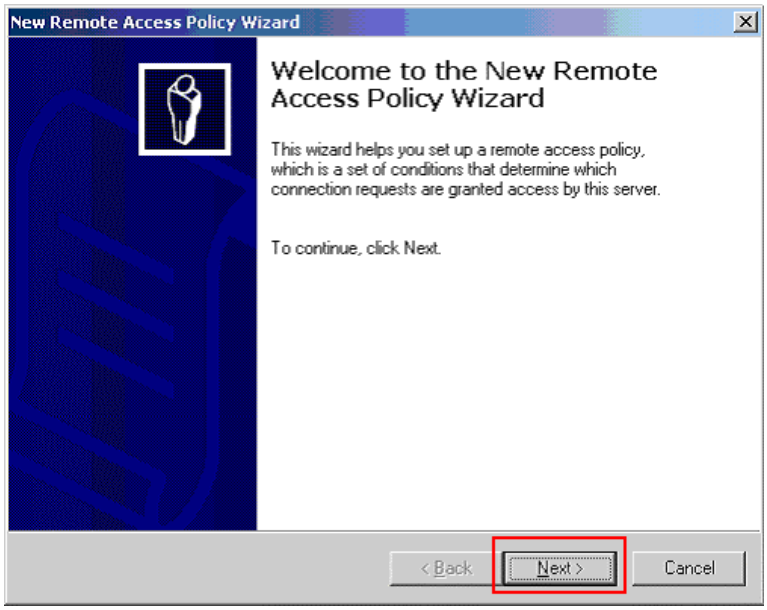
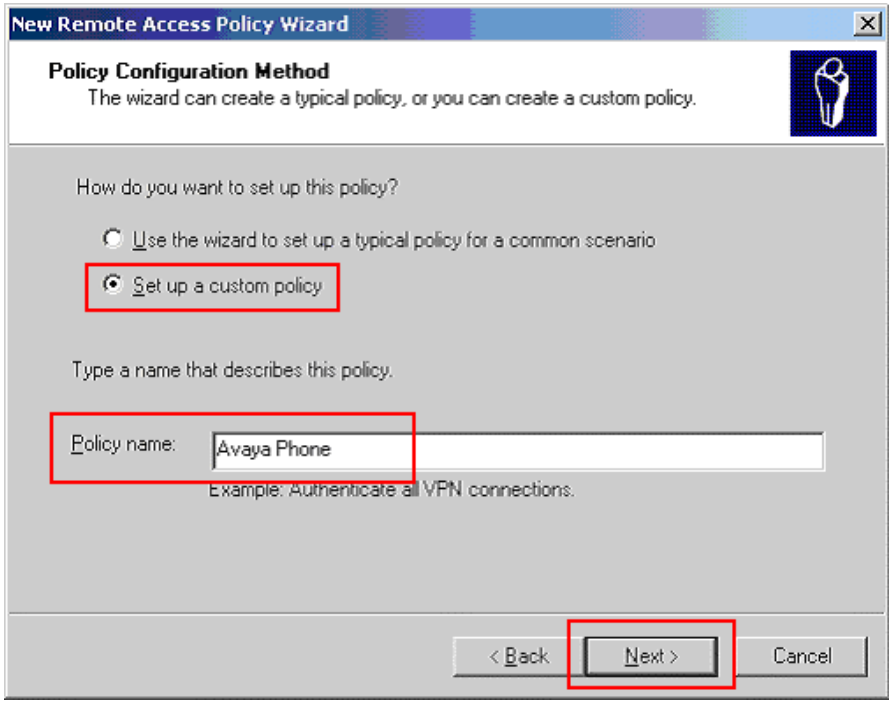
5.2. Configure Microsoft Internet Authentication Services (IAS) Server

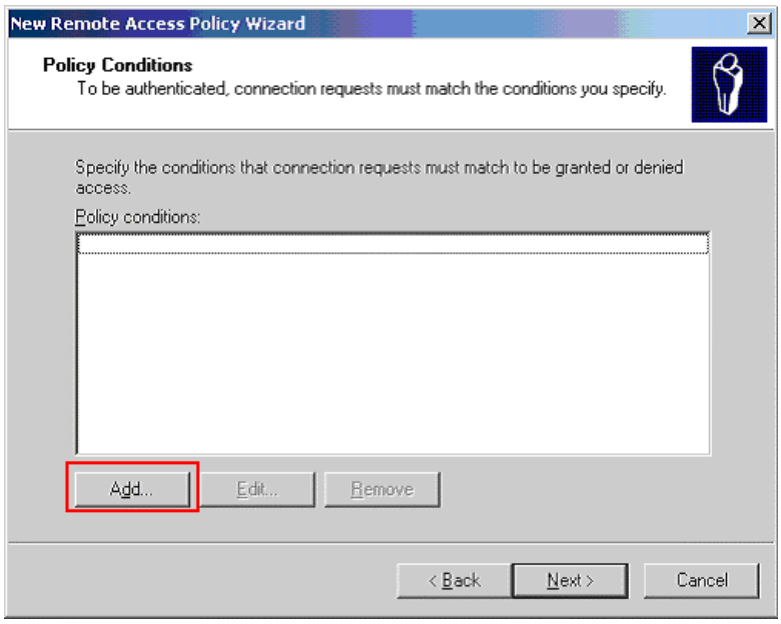
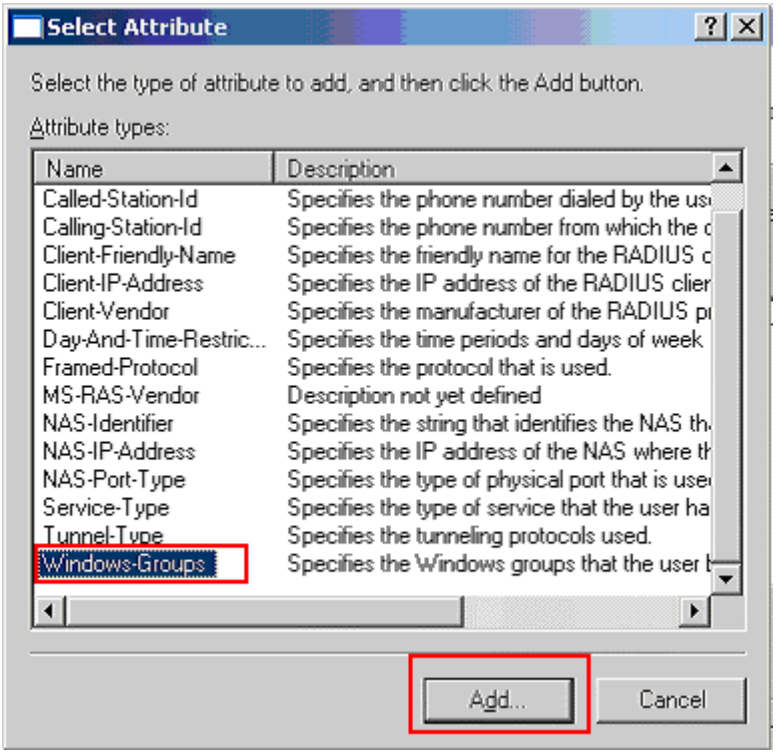
This section shows the steps for configuring the IAS server to support 802.1X authentication for an Avaya IP Telephone and a PC.

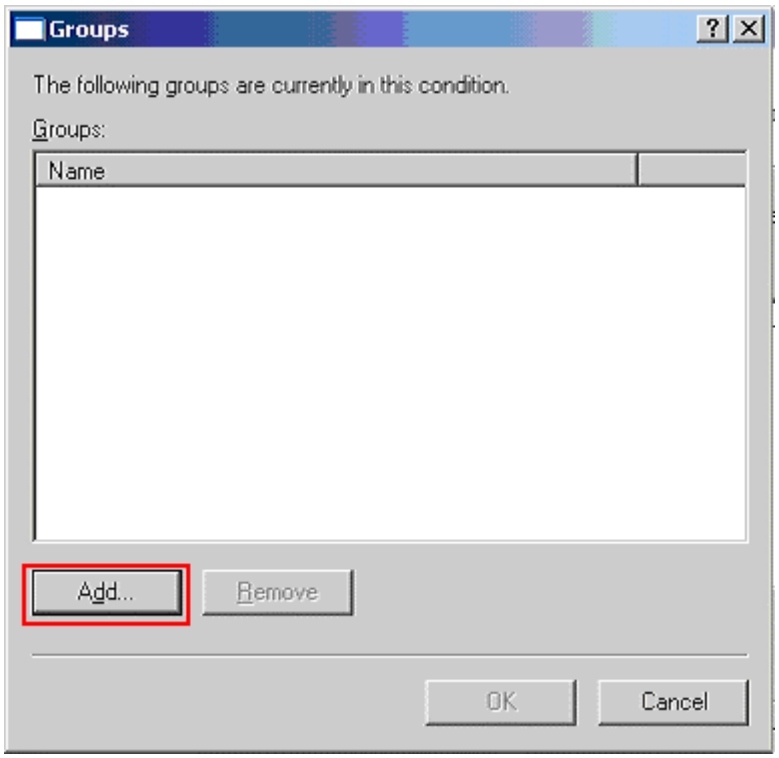
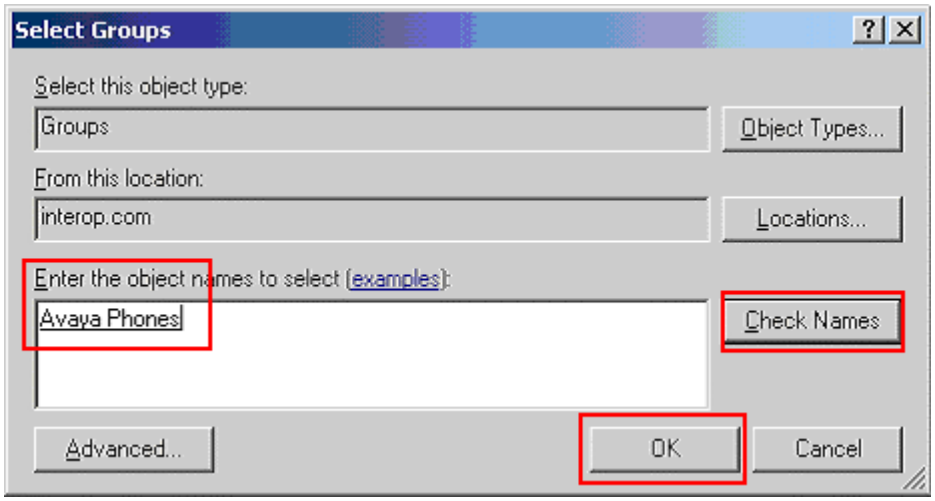
Step	Description
1.	Invoke the Internet Authentication Service window under Administrative Tools of the Microsoft Windows system. Create a new RADIUS client by selecting **Action → New RADIUS Client** from the drop down menu in Internet Authentication Service window. 

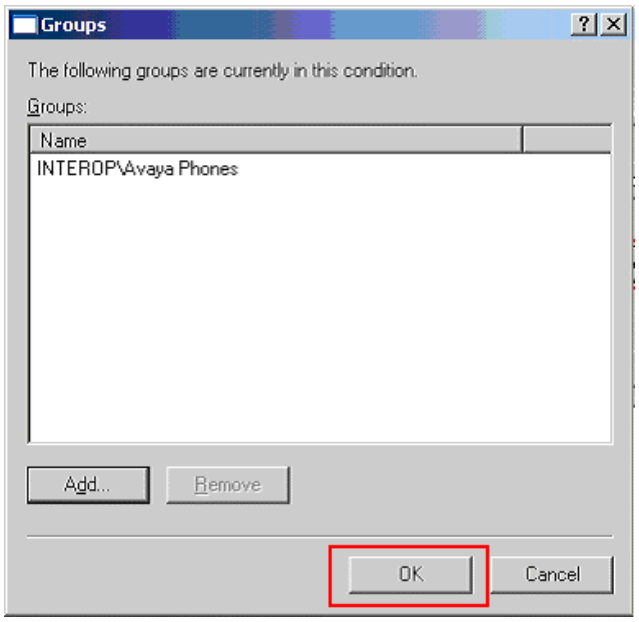
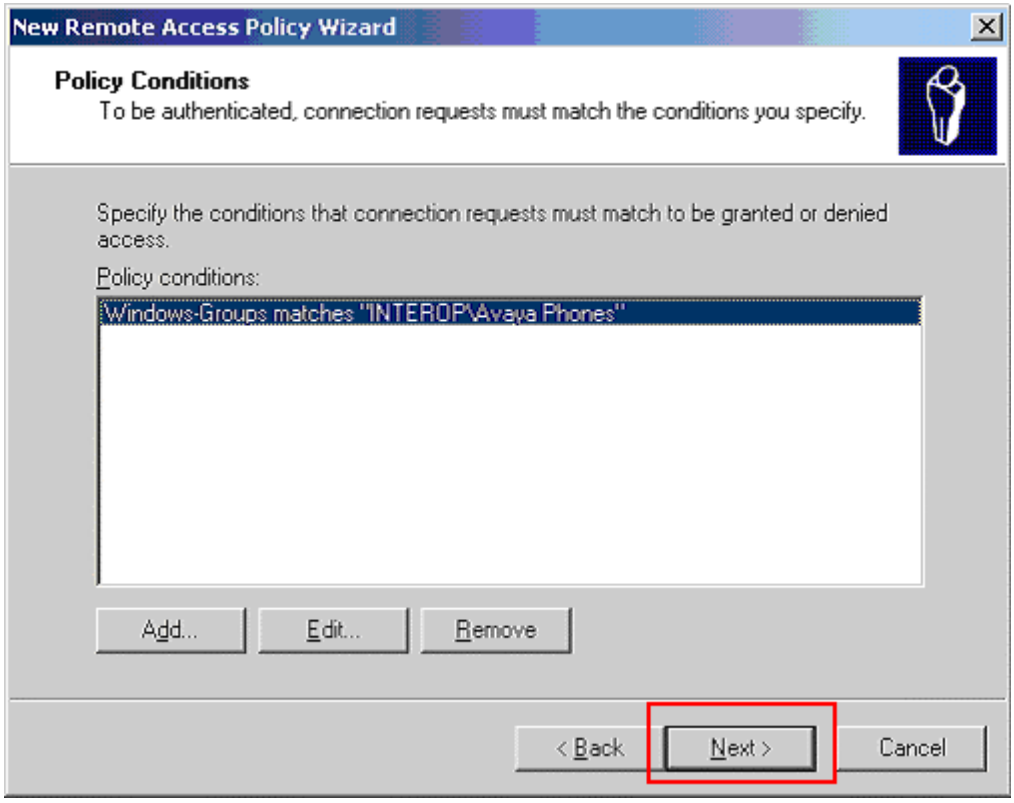
Step	Description
2.	Enter the name and IP address of the X450e-48p switch to create a new RADIUS client. This must match the IP address configured in Section 4.1, Step 4. Click **Next** to continue. 

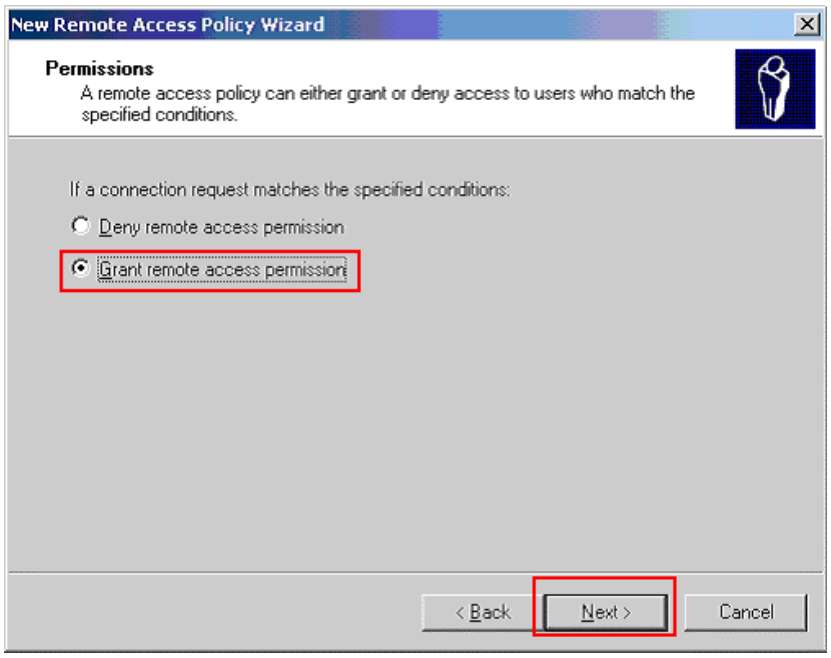
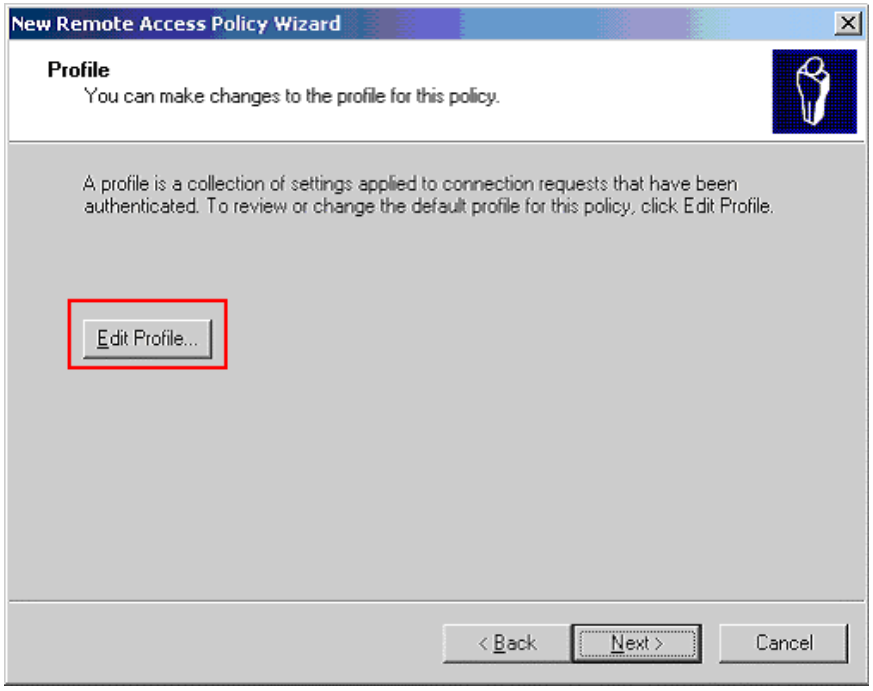
Step	Description
3.	Enter the Shared secret that will be used for this client. This shared secret must match the information configured in the switch in Section 4.1, Step 4. Click **Finish** to complete. 
4.	Create a new access policy for the Avaya IP Telephones by clicking on **Action → New Remote Access Policy**. 

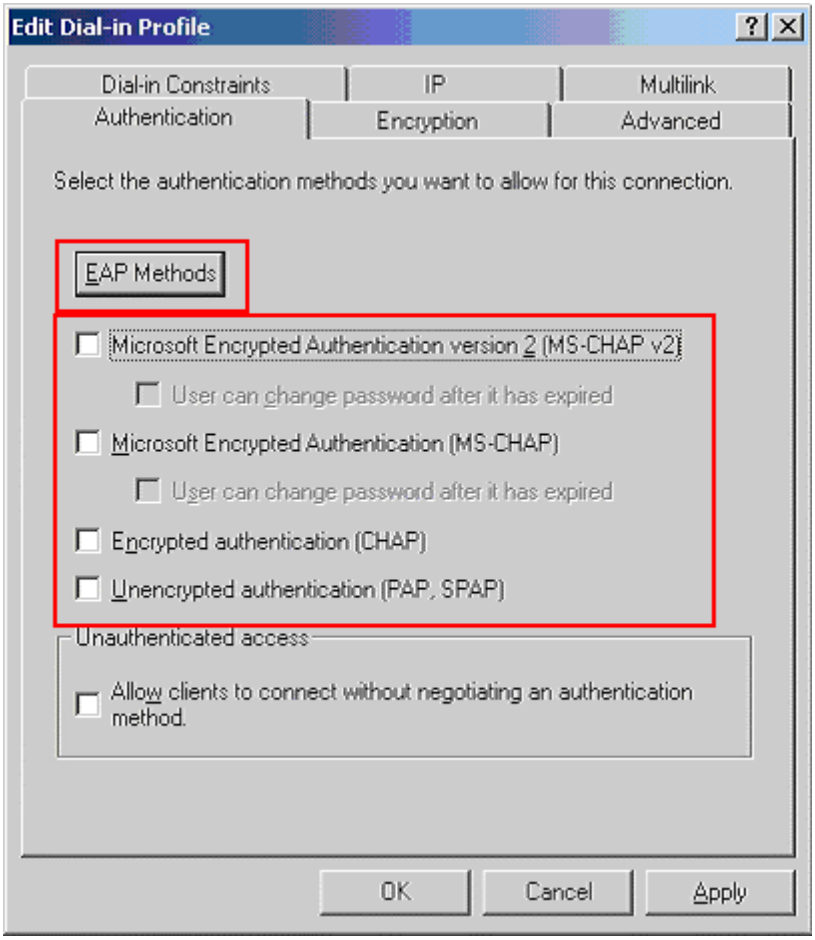
Step	Description
5.	Click **Next** in the **New Remote Access Policy Wizard**. 
6.	Select **Set up a custom policy** radio button and enter a **Policy name**. The sample network uses the name Avaya Phone. Click Next to continue. 

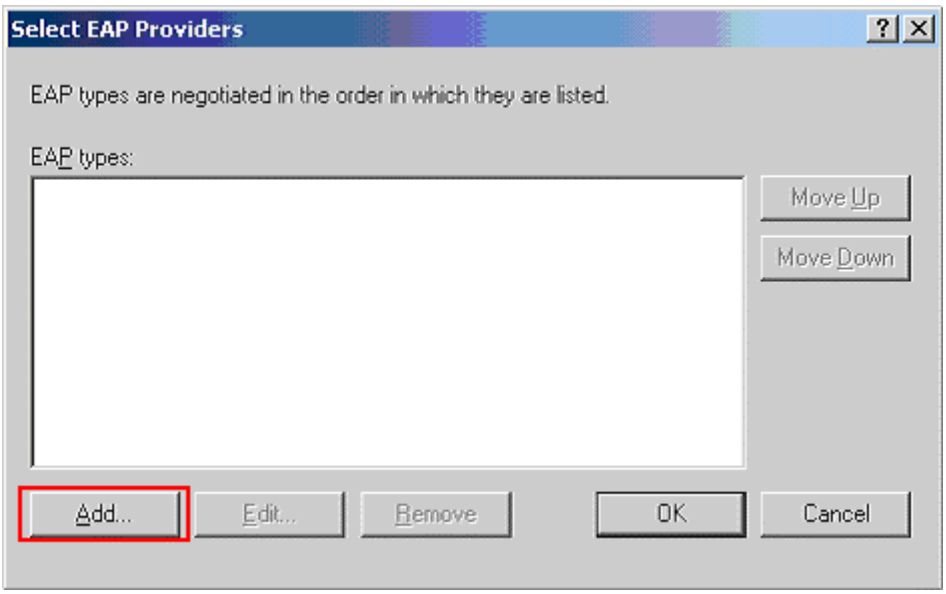
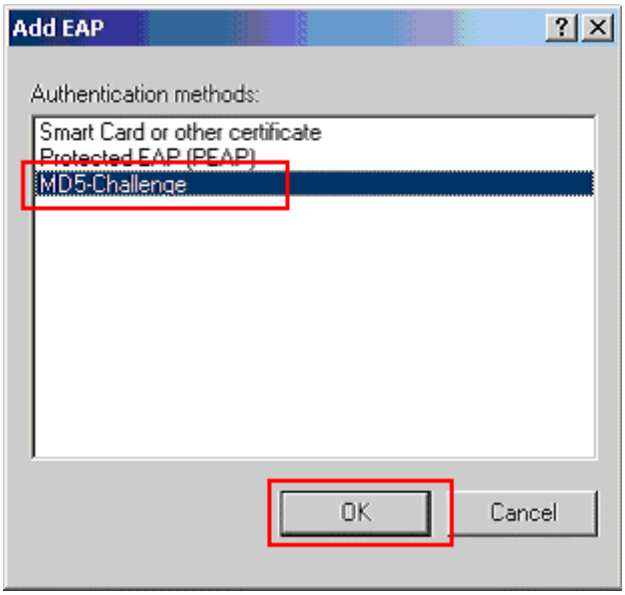
Step	Description
7.	Click the Add button to add a new policy condition. 
8.	Highlight **Windows-Groups** from the Select Attribute pop-up window. Click **Add** to continue. 

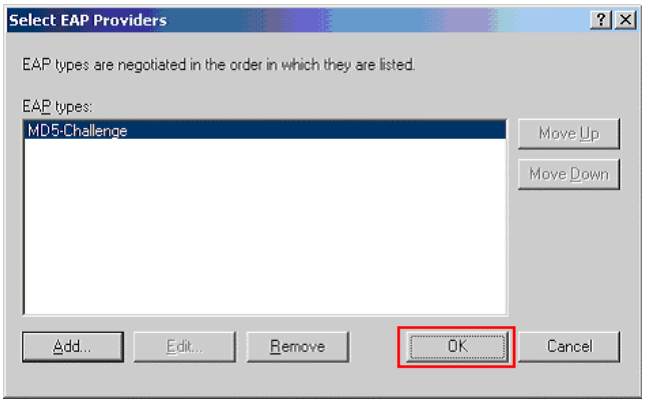
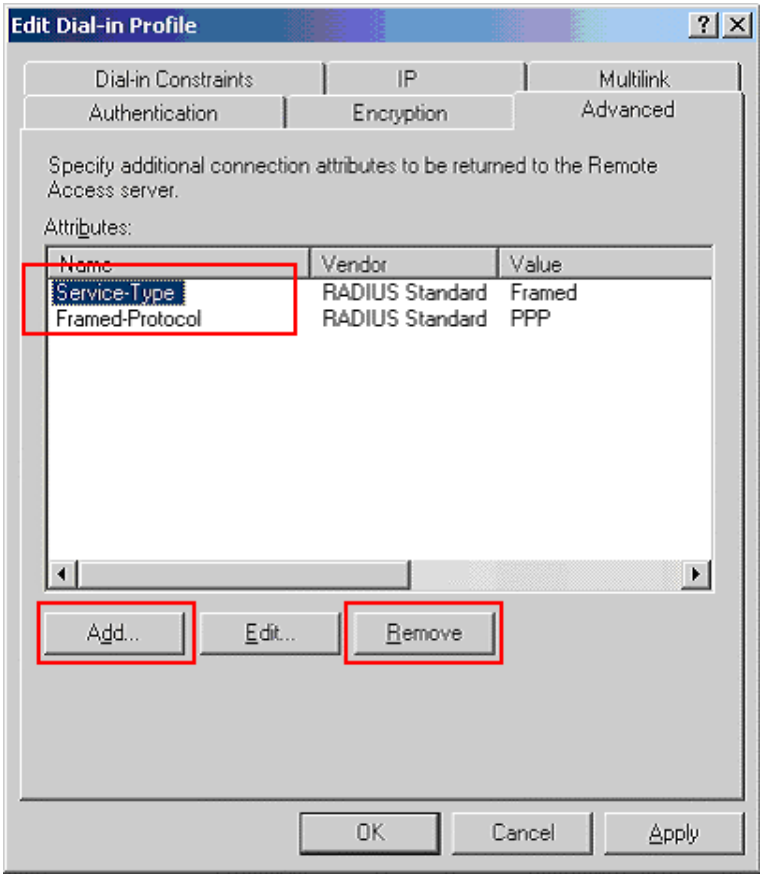
Step	Description
9.	Click **Add** in the Groups pop-up window to add a windows group. 
10.	Enter the Active Directory user group created in Section 5.1, Steps 12-13. Use **Check Names** to assist in searching for the user group. Click **OK** to complete. 

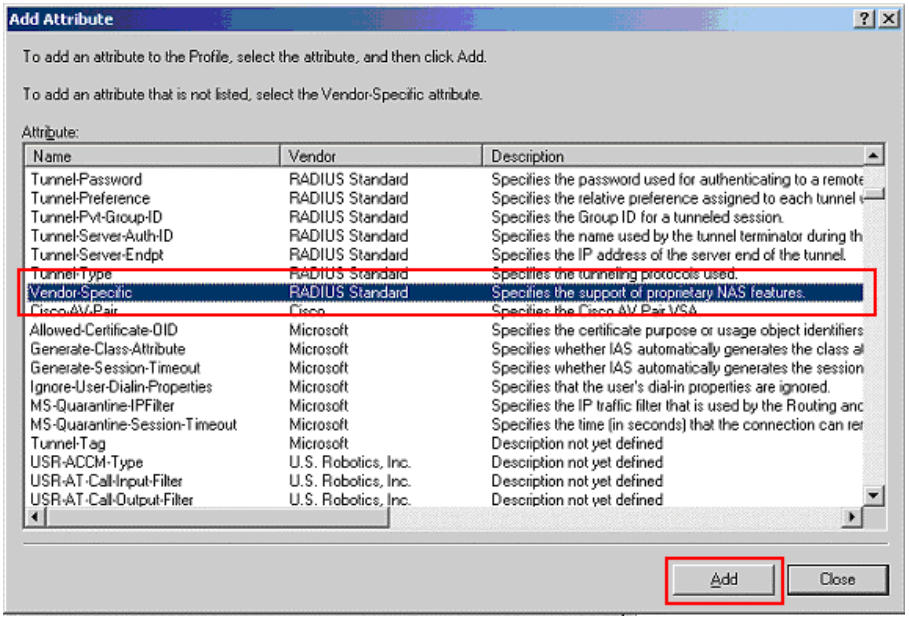
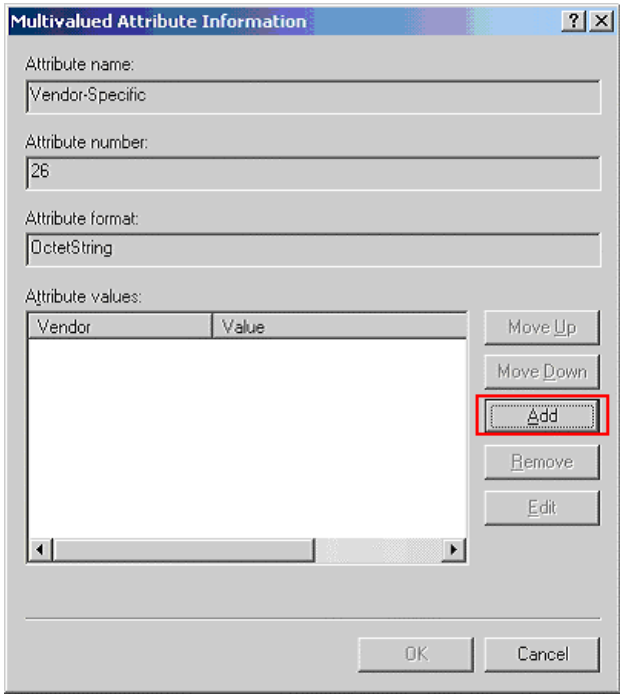
Step	Description
11.	Click **OK** in the Groups pop-up windows to complete. 
12.	Once the windows user group has been added via Steps 8-11, click **Next** to continue. 

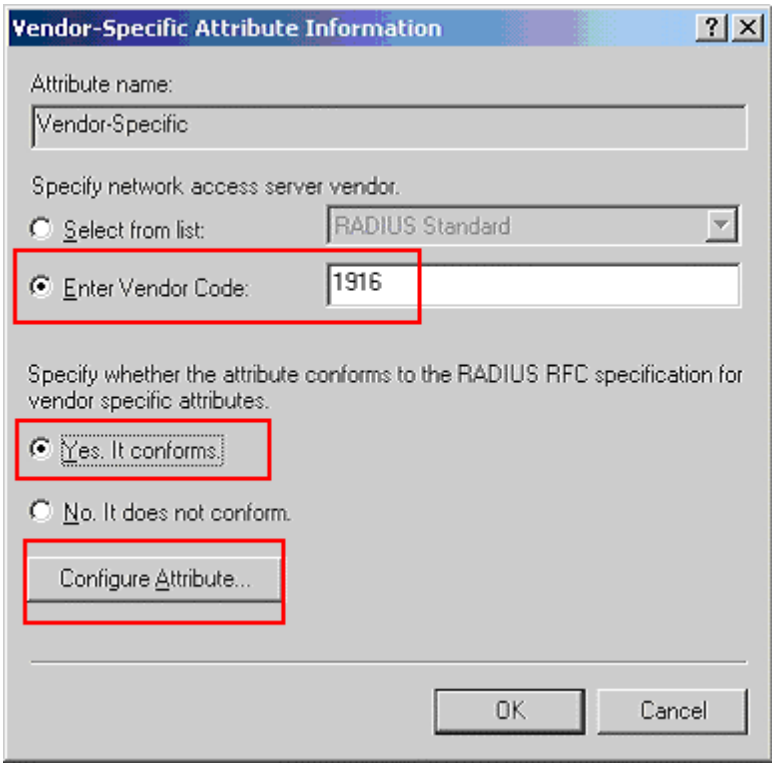
Step	Description
13.	Click the **Grant remote access permission** radio button. Click **Next** to continue. 
14.	Click **Edit Profile** to configure the profile for this access policy. This will display the Edit Dial-in Profile pop-up window. 

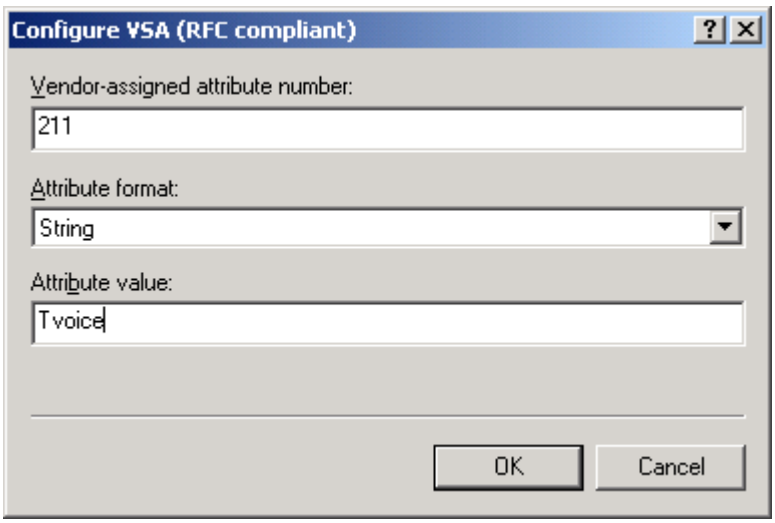
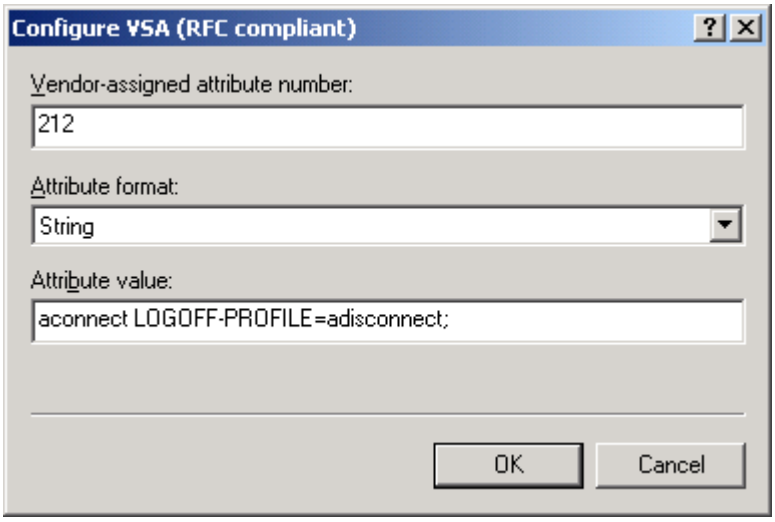
Step	Description
15.	Select the **Authentication** tab in the Edit Dial-in Profile pop-up window. Uncheck all Microsoft authentication protocols as shown in the screen capture below. Click **EAP Methods** to continue. This will display the Select EAP Providers pop-up window. 

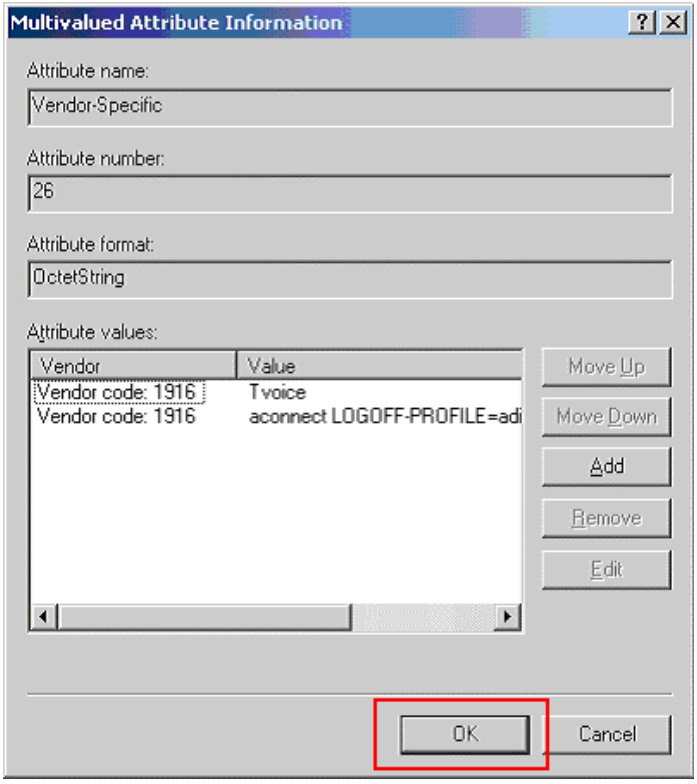
Step	Description
16.	Click **Add** in the Select EAP Providers pop-up window to add a new EAP type. 
17.	Select **MD5-Challenge** in the Add EAP pop-up window. Click **OK** to continue. 

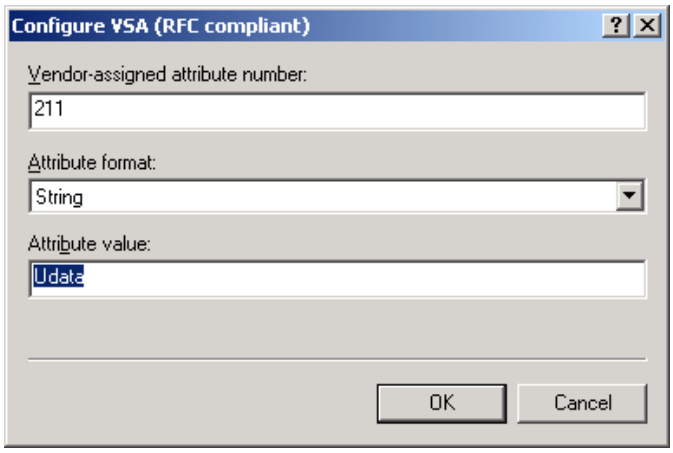
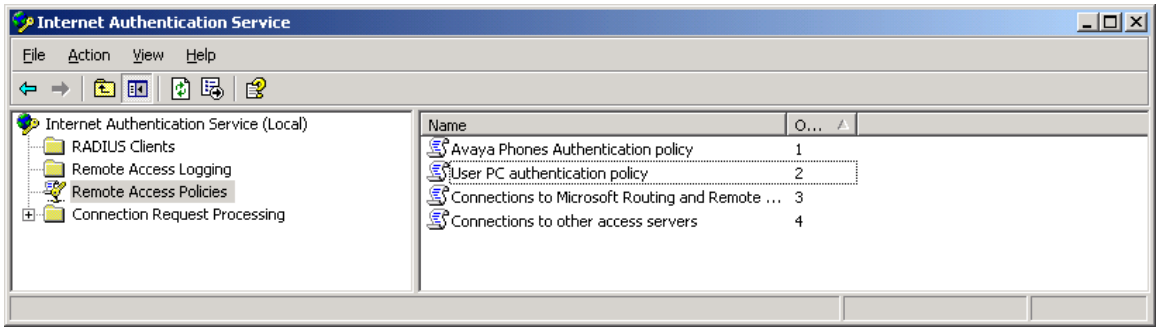
Step	Description
18.	Once the MD5-Challenge EAP type is added, Click **OK** to complete the EAP authentication selection. 
19.	Select the **Advanced** tab in the Edit Dial-in profile pop-up window. Highlight each existing attribute, then click **Remove** to delete it. Click **Add** after all existing attributes have been removed to enter a new attribute. This will display the Add Attribute pop-up window. 

Step	Description
20.	Highlight the **Vendor Specific** attribute name from the list of attributes displayed in the Add Attribute pop-up window. Click **Add** to continue. This will display the Multivalued Attribute Information pop-up window. 
21.	Click **Add** to enter a new Attribute in the Multivalued Attribute Information pop-up window. This will display the Vendor-Specific Attribute Information pop-up window. 

Step	Description
22.	In the Vendor-Specific Attribute Information pop-up window, click on the **Enter Vendor Code** radio button, and enter string **1916** (Extreme Networks Vendor Code). Click on the **Yes, It conforms** radio button. Click **Configure Attribute** to continue. This will display the Configure VSA (RFC compliant) pop-up window. 

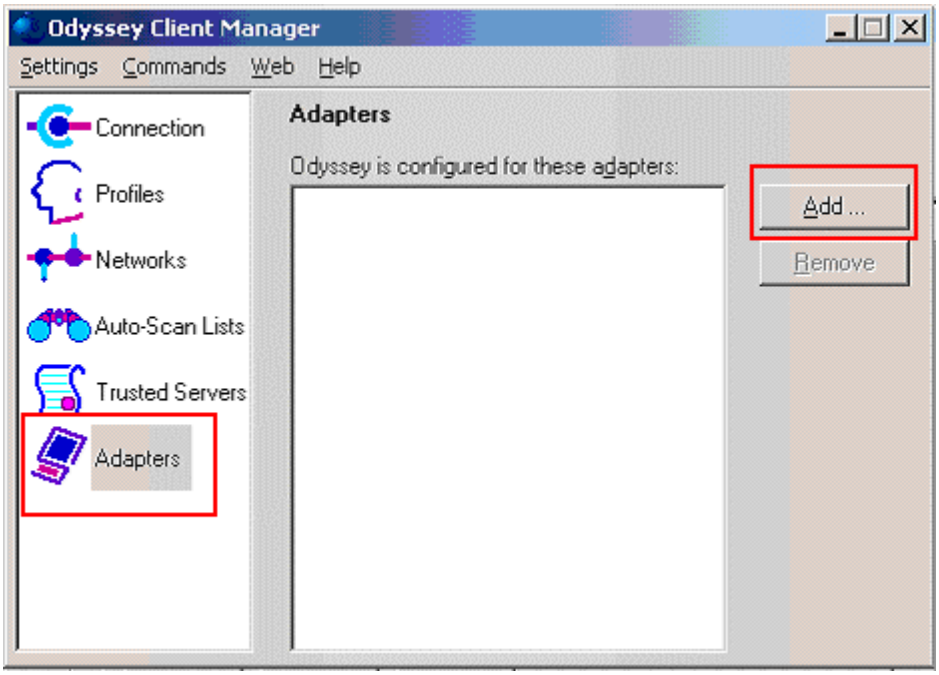
Step	Description
23.	Enter the following field information in the Configure VSA (RFC compliant) pop-up window. The Attribute value "**Tvoice**" signifies that the port should be configured as "Tagged" by the switch and the "voice" VLAN should be assigned. The voice VLAN was created on the switch in **Section 4.1**, **Step 2**. Click **OK** to complete. 
24.	Repeat Step 21 and 22 to configure an additional Attribute. Use the Attribute value "aconnect LOGOFF-PROFILE=adsiconnect" for this attribute. This must match the UP profile name configured in **Section 4.1**, **Steps 7-8**. 

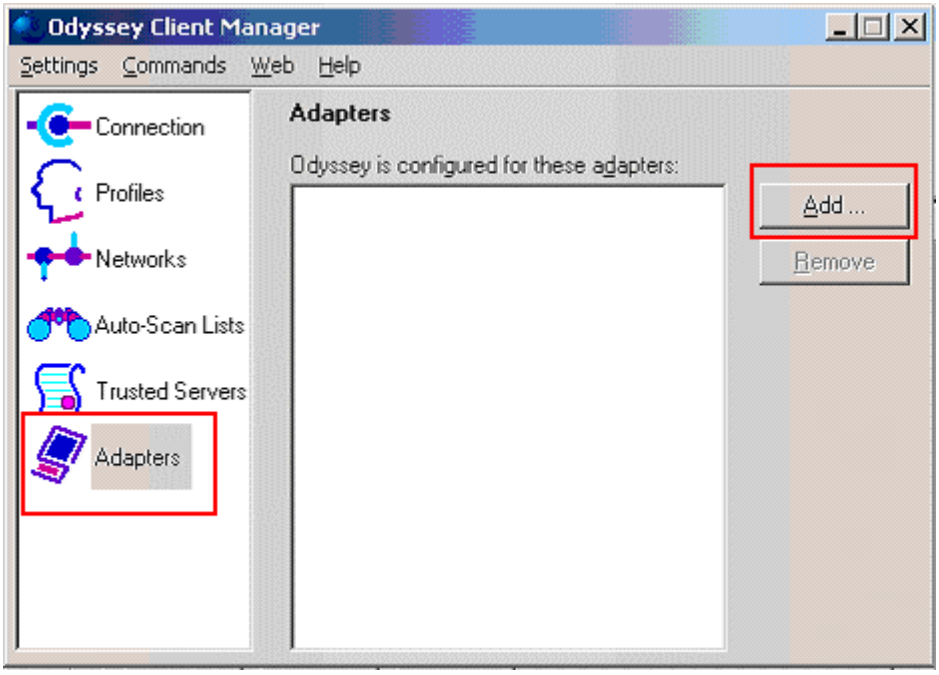
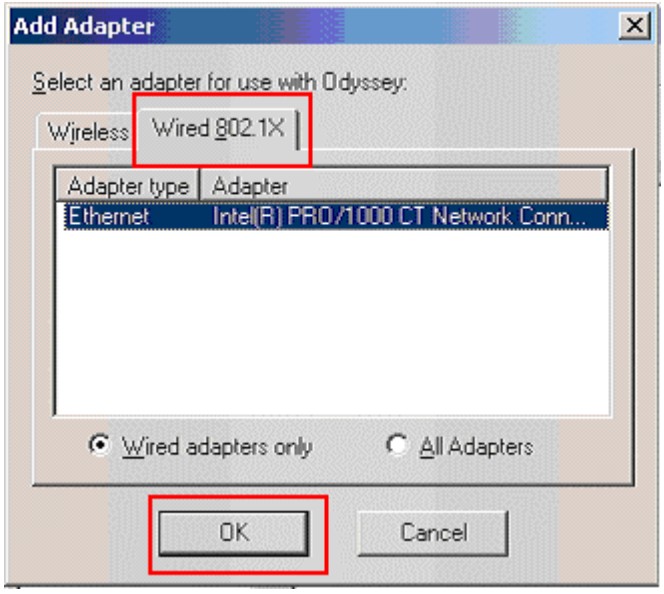
Step	Description
25.	Once all attributes have been entered in Steps 21-24, click **OK** to continue. 
26.	Click **OK** on all preceding pop-up windows to complete the configuration of this access policy.

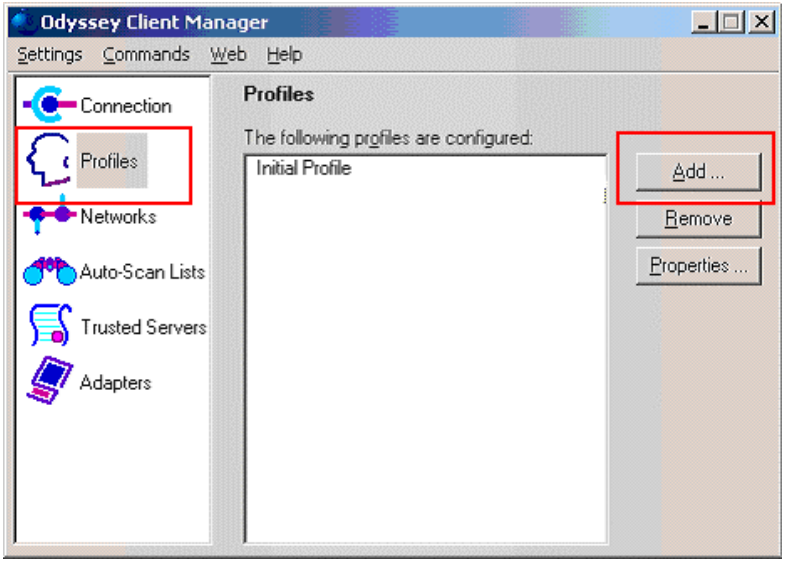
Step	Description
27.	Repeat Steps 4-23 to create a separate policy for a PC. The sample network uses the name **User PC authentication policy** for this new policy. Use the **Udata** value in lieu of what is in Step 24. The **Udata** value indicates to the switch the switch port should be assigned to the data VLAN as Untagged. The data VLAN was created on the switch in Section 4.1, Step 2. 
28.	After completing the above steps, there should be a total of 4 Remote Access Polices. 

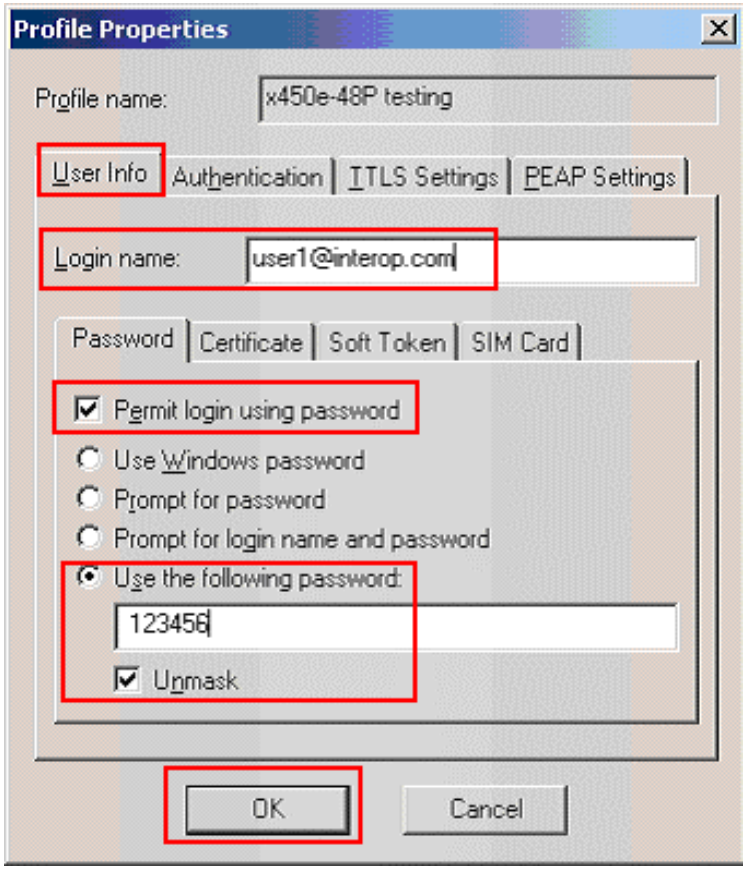
6. Configure the Odyssey client

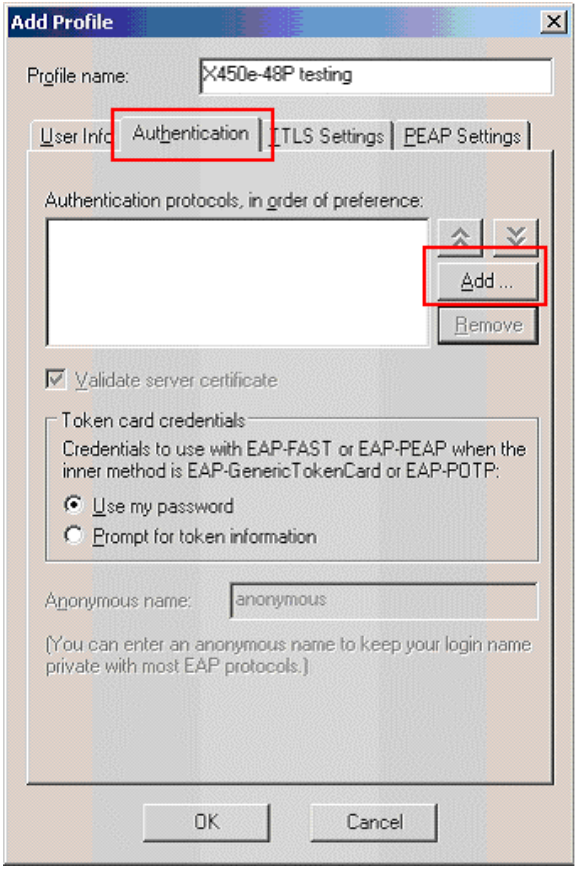
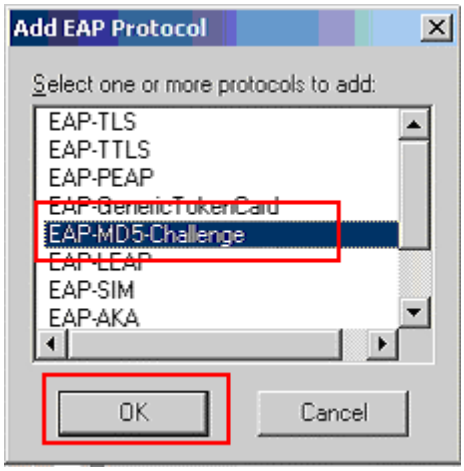
This section shows the steps for configuring the Odyssey Client running on the PC.

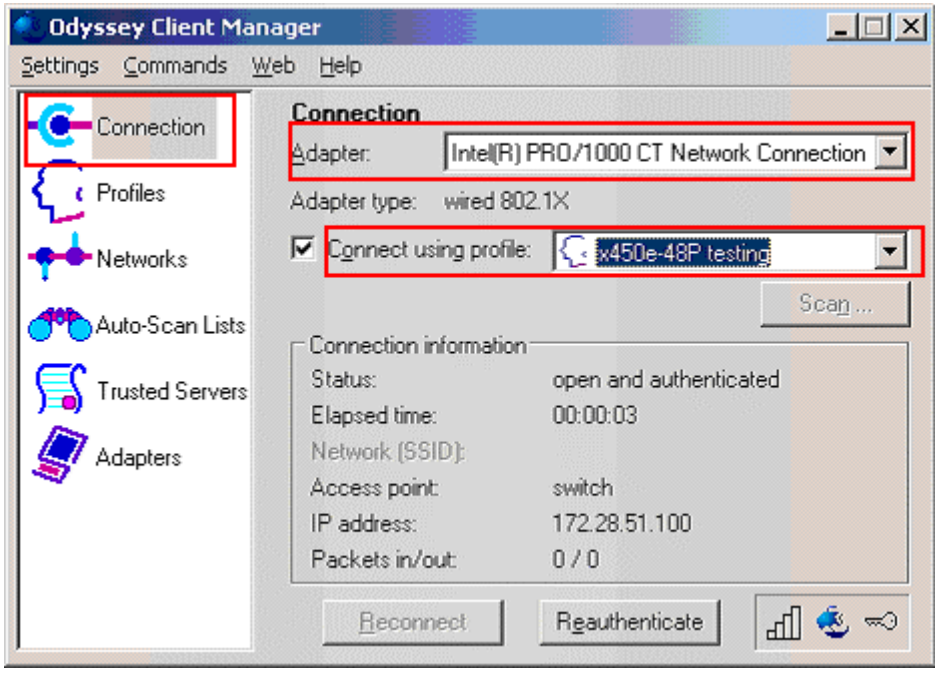
Step	Description
1.	Invoke the Odyssey Client Manager by clicking on **Start → Programs → Funk Software → Odyssey Client → Odyssey Client Manager**. Add a network adapter by selecting **Adapters** on the left panel then click **Add** from the Odyssey Client Manager window. 

2.	Invoke the Odyssey Client Manager by clicking on **Start → Programs → Funk Software → Odyssey Client → Odyssey Client Manager**. Add a network adapter by selecting **Adapters** on the left panel then click **Add** from the Odyssey Client Manager window. 
3.	Click on the **Wired 802.1X** tab in the Add Adapter pop-up window. Select the desired network adapter and click **OK** to complete. 

4.	Add a profile by selecting **Profiles** on the left panel. Click **Add** to continue. 

5.	From the User Info tab in the Add Profile pop-up window, enter the **Login name** and **password**. The Login name and password must match the configuration in Section 5.1 Step 9. Click on the **Authentication** tab to continue. 

6.	Under the **Authentication** tab, click **Add** to add a new authentication protocol. 
7.	In the Add EAP Protocol pop-up window, select **EAP-MD5 Challenge**. Click **OK** to complete. 

8.	To connect the PC to the network, click on Connection in the Odyssey Client Manager left panel. Select the appropriate adapter and connection profile configured in Steps 2 and 3. Once successfully authenticated, the Status should read **open and authenticated**. 

7. Configure the Avaya IP Telephone

This section shows the steps for configuring the Avaya 4610SW IP Phone connected to the X450e-48p switch.

Avaya IP telephones support three 802.1X operational modes. The operational mode can be changed by pressing "mute80219#" ("mute8021x") on the Avaya 4600-Series IP telephones.

- **Pass-thru Mode** – Unicast supplicant operation for the IP telephone itself, with PAE multicast pass-through for the attached PC, but without proxy Logoff (default)

- **Pass-thru with logoff Mode (p-t w/Logoff)** – Unicast supplicant operation for the IP telephone itself, with PAE multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected form the IP telephone, the phone will send an EAPOL-Logoff for the attached PC.

- **Supplicant Mode** – Unicast or multicast supplicant operation for the IP telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

Since most 802.1X clients use the multicast MAC address for the EAPOL messages, the IP telephone must be configured to the **pass-thru** or **p-t w/Logoff** mode to pass-through these multicast

messages. It is recommended to use the **p-t w/Logoff** mode. When the phone is in the **p-t w/Logoff** mode, the phone will do proxy logoff for the attached PC when the PC is physically disconnected. When the X450e-48p receives the logoff message, the PC will be removed from the authorized MAC list.

1.	Press the following key on the Avaya 4610SW IP phone. Mute80219#
2.	Press the "*****" key on the key pad until **p-t w/Logoff** is displayed, then press "**#**" key to complete the configuration.

8. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3] and [4]. The following steps describe the configuration of Avaya Communication Manager.

Step	Description
1.	Add a new station for an Avaya IP Telephone using the **add station** command. Configure the following fields. • **Extension:** ***22023*** (Extension number for the Avaya Telephone) • **Type:** ***4610*** (Avaya Telephone type used for this extension) • **Port:** ***IP*** (Type of connection for the Avaya Telephone) • **Security Code:** ***1234*** (Security code used by the Avaya Telephone to register with Avaya Communication Manager) • **Direct IP-IP Audio Connections:** ***y*** (Enable Shuffling)

Step	Description
	The first two pages of the **add station 22023** configuration are shown below. Repeat this step for each station.

```
add station 22023                                              Page   1 of   4
                                      STATION

Extension: 22023                            Lock Messages? n          BCC: 0
     Type: 4610                             Security Code: 1234        TN: 1
     Port: IP                             Coverage Path 1:            COR: 1
     Name: Room 18                        Coverage Path 2:            COS: 1
                                          Hunt-to Station:

STATION OPTIONS
              Loss Group: 19              Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 22023
            Speakerphone: 2-way                   Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal                  Media Complex Ext:
   Survivable Trunk Dest? y                              IP SoftPhone? n



                                                      Customizable Labels? y
```

```
add station 22023                                              Page   2 of   4
                                      STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                                Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? y                       Restrict Last Appearance? y
  Active Station Ringing: single          Conf/Trans on Primary Appearance? n
                                                       EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed
        Multimedia Mode: enhanced
    MWI Served User Type:                        Display Client Redirection? n
              AUDIX Name:                       Select Last Used Appearance? n
                                                  Coverage After Forwarding? s

                                               Direct IP-IP Audio Connections? y
 Emergency Location Ext: 22023     Always Use? n      IP Audio Hairpinning? y
```

2.	Use the "display ip-network-region" command to display the 802.1P setting configured in Avaya Communication Manager. Both Call Control and Audio 802.1P priority are set to 6. In the sample configuration, all IP Telephones are in network region 1.

```
display ip-network-region 1                                     Page   1 of
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
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: 3029
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
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

9. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Extreme Networks Universal Port (UP) feature to program Avaya IP Telephones.

9.1. General Test Approach

Instead of using DHCP option 176 to program the Avaya Media Server, TFTP server and VLAN tagging information, a Universal Port profile was used to program the Avaya IP Telephones. The following four trigger events were compliance-tested.

- Device-Detect
- Device-Undetect
- User-Authenticated
- User-Unauthenticated

9.2. Test Results

The Extreme Networks Universal Port feature successfully achieved all objectives. The Avaya IP Telephones successfully received appropriate IP addresses via LLDP advertisement within the UP profile and registered with the correct server. VLANs were correctly assigned to the switch port based on 802.1x authentication.

10. Verification Steps

The following steps may be used to verify the configuration. All screens in this section are from the X450e-48p.

Step	Description
1.	Place calls using the Avaya IP Telephones.
2.	Verify the PCs have network connectivity.

3.	Use the "show upm profiles" command to verify that the upm profiles have been assigned to the correct port.
	
	`X450e-48p.8 # show upm profiles`
	`==========`
	`UPM Profile  Events  Flags Ports`
	`==========`
	`aconnect  User-Authenticated  e  11`
	`adisconnect  User-Unauthenticated  e  11`
	`connect  Device-Detect  e  7`
	`disconnect  Device-Undetect  e  7`
	`==========`
	`Number of UPM Profiles: 4`
	`Flags: d - disabled, e - enabled`

Step	Description
4.	Use the "show netlogin" command to verify that authentication has been enabled and the authentication status of the Avaya IP Telephone and PC.

```
X450e-48p.15 # show netlogin

NetLogin Authentication Mode : web-based DISABLED;  802.1x ENABLED;  mac-based D
ISABLED
NetLogin VLAN                : "temp"
NetLogin move-fail-action    : Deny
NetLogin Client Aging Time   : 5 minutes
Dynamic VLAN Creation        : Disabled
Dynamic VLAN Uplink Ports    : None

-----------------------------------------------
        Web-based Mode Global Configuration
-----------------------------------------------
Base-URL                 : network-access.com
Default-Redirect-Page    : http://www.extremenetworks.com
Logout-privilege         : YES
Netlogin Session-Refresh : ENABLED; 3 minutes
-----------------------------------------------

-----------------------------------------------
        802.1x Mode Global Configuration
-----------------------------------------------
Quiet Period                     : 60
Supplicant Response Timeout      : 30
Re-authentication period         : 3600
RADIUS server timeout            : 30
EAPOL MPDU version to transmit   : v1
-----------------------------------------------

Port: 11,  Vlan: data,  State: Enabled,  Authentication: 802.1x,  Guest Vlan <No
t Configured>: Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:e4:37:79  0.0.0.0          No            0              00040DE43779
00:12:3f:25:26:60  0.0.0.0          Yes   802.1x  3593           user1@interop.com
-----------------------------------------------

Port: 11,  Vlan: voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan <N
ot Configured>: Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:e4:37:79  172.28.50.225    Yes   802.1x  3463           00040DE43779
```

Step	Description
5.	Use the "show lldp neighbors detail" command to verify the LLDP information for the Avaya IP Telephones.

```
e-48p.15 # show lldp neighbors detailed

------------------------------------------------------------------------------
LLDP Port 11 detected 1 neighbor
  Neighbor: (5.1)172.28.50.225/00:04:0D:E4:37:79, age 7 seconds
    - Chassis ID type: Network address (5); Address type: IPv4 (1)
      Chassis ID     : 172.28.50.225
    - Port ID type: MAC address (3)
      Port ID     : 00:04:0D:E4:37:79
    - Time To Live: 120 seconds
    - System Name: "AVAE43779"
    - System Capabilities : "Bridge, Telephone"
      Enabled Capabilities: "Bridge, Telephone"
    - Management Address Subtype: IPv4 (1)
      Management Address        : 172.28.50.225
      Interface Number Subtype  : System Port Number (3)
      Interface Number          : 1
      Object ID String          : "1.3.6.1.4.1.6889.1.69.1.7"
    - IEEE802.3 MAC/PHY Configuration/Status
      Auto-negotiation       : Supported, Enabled (0x03)
      Operational MAU Type   : 100BaseTXFD (16)
    - MED Capabilities: "MED Capabilities, Network Policy, Inventory"
      MED Device Type : Endpoint Class III (3)
    - MED Network Policy
      Application Type  : Voice (1)
      Policy Flags      : Known Policy, Tagged (0x1)
      VLAN ID           : 50
      L2 Priority       : 6
      DSCP Value        : 46
    - MED Hardware Revision: "4610D01A"
    - MED Firmware Revision: "b10d01b2_6.bin"
    - MED Software Revision: "a10d01b2_6.bin"
    - MED Serial Number: "06N521004978"
    - MED Manufacturer Name: "Avaya"
    - MED Model Name: "4610"
    - Avaya/Extreme Conservation Level Support
      Current Conservation Level: 0
      Typical Power Value       : 4.0 Watts
      Maximum Power Value       : 6.0 Watts
    - Avaya/Extreme Call Server(s): 172.28.10.7
    - Avaya/Extreme IP Phone Address: 172.28.50.225 255.255.255.0
      Default Gateway Address       : 172.28.50.1
    - Avaya/Extreme CNA Server: 0.0.0.0
    - Avaya/Extreme File Server(s): 0.0.0.0
    - Avaya/Extreme IEEE 802.1q Framing: Tagged
```

6.	Use the "show upm history" command to display the status of upm script execution. The Exec-Id can be used to obtain additional information for the event.

```
X450e-48p.1 # show upm history
--------------------------------------------------------------------------------
Exec-Id   Event/Timer          Profile          Port Status Time run
--------------------------------------------------------------------------------
3        User-Authenticated   aconnect         11   Pass   2007-01-03 06:41:39

2        User-Unauthenticated adisconnect      11   Pass   2007-01-03 06:41:10

1        User-Authenticated   aconnect         11   Pass   2007-01-03 06:41:03
```

Step	Description
7.	Use the "show upm history exec-id <exec-id>" obtained from the previous step to display detailed information regarding the upm script executed. The example below shows that the **aconnect** profile was invoked by the **User-Authenticated** Event and successfully executed (**Pass**). Should the Execution Status indicate Fail, the output would indicate which command caused the profile to fail execution.

```
X450e-48p.2 # show upm history exec-id 3

UPM Profile: aconnect
Event:  User-Authenticated      , Time run: 2007-01-03 06:41:39
Execution Identifier: 3         Execution Status: Pass
Execution Information:
1 # enable cli scripting
2 # configure cli mode non-persistent
3 # set var EVENT.USERNAME 00040DE43779
4 # set var EVENT.NUMUSERS 1
5 # set var EVENT.USER_VLAN voice
6 # set var EVENT.USER_IP 0.0.0.0
7 # set var EVENT.NAME USER-AUTHENTICATED
8 # set var EVENT.TIME 1167835299
9 # set var EVENT.USER_MAC 00:04:0d:e4:37:79
10 # set var EVENT.USER_PORT 11
11 # set var EVENT.PROFILE aconnect
12 # set var acm 172.28.10.7
13 # set var fileserver 0.0.0.0
14 # enable lldp port $EVENT.USER_PORT
15 # configure lldp port $EVENT.USER_PORT advertise vendor-specific dot1 vlan-na
me
16 # configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extrem
e call-server $acm
17 # configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extrem
e file-server $fileserver
18 # configure lldp port $EVENT.USER_PORT advertise vendor-specific avaya-extrem
e dot1q-framing tag
```

11. Conclusion

These Application Notes have described the steps required to configure the Universal Port (UP) feature with the Extreme Network X450e-48p switch. Avaya IP Telephones using DHCP and 802.1X authentication were verified to interoperate successfully with UP framework.

12. Support

For technical support on the Extreme Networks product, contact Extreme Networks at (800) 998-2408, or refer to http://www.extremenetworks.com

13. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006

[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005

[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 11, February 2006

[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006

[5] *Configuring Link Layer Discovery Protocol (LLDP) and 802.1X Protocol on Extreme Networks BlackDiamond 8810 for an Avaya IP Telephone with an Attached PC*, Issue 1.1, Dec 18, 2006

Product documentation for Extreme Networks products may be found at http://www.extremenetworks.com

[6] *ExtremeWare XOS Concepts Guide, Software Version 11.6*, Part number 100247-00 Rev. 01, 2006

[7] *ExtremeWare XOS Command Reference Guide, Software Version 11.6*, Part number 100246-00 Rev. 01, 2006

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 Developer*Connection* Program at devconnect@avaya.com.