



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-Unauthenticated. 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

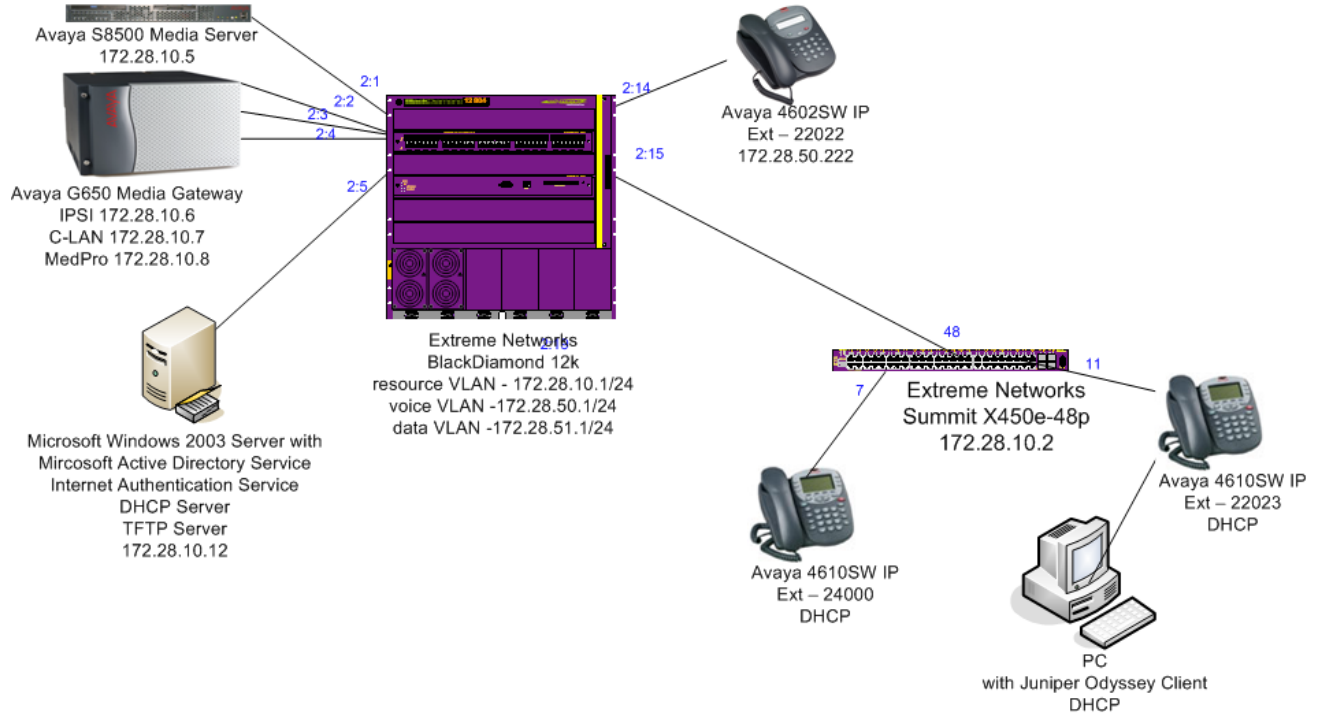


Figure 1: Sample Network Configuration

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: xxxxxxx

Step	Description
2.	<p>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”.</p> <pre>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)</pre>
3.	<p>Configure VLAN assignment for the ports. Port 11 will be dynamically configured via the UP feature as a device is connected to the port.</p> <pre>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</pre>
4.	<p>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.</p> <pre>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</pre>
5.	<p>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.</p> <pre>X450e-48p.1 # create qosprofile QP7 X450e-48p.1 # configure dot1p type 6 qosprofile QP7</pre>

Step	Description
6.	<p>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.</p>
7.	<p>The following illustrates the script for the aconnect profile. This profile will be used by the USER-AUTHENTICATED event.</p> <pre data-bbox="277 527 932 552">X450e-48p.1 # create upm profile aconnect</pre> <pre data-bbox="277 594 1393 1161"> # # 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 # . </pre>
8.	<p>The following illustrates the script for the adisconnect profile. This profile will be used by the USER-UNAUTHENTICATED event.</p> <pre data-bbox="277 1350 980 1375">X450e-48p.1 # create upm profile adisconnect</pre> <pre data-bbox="277 1417 834 1591"> # # adisconnect profile # disable lldp port \$EVENT.USER_PORT # . </pre>

Step	Description
9.	<p>The following illustrates the script for the connect profile. This profile will be used by the DEVICE-DETECT event.</p> <pre>X450e-48p.1 # <i>create upm profile connect</i></pre> <pre># # 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 # .</pre>

Step	Description
10.	<p>The following illustrates the script for the disconnect profile. This profile will be used by the DEVICE-UNDETECT event.</p> <pre>X450e-48p.1 # <i>create upm profile disconnect</i></pre> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre># # 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 # .</pre> </div>
11.	<p>Assign the appropriate profile to each UPM event.</p> <pre>X450e-48p.1 # <i>configure upm event user-authenticated profile aconnect ports 11</i> X450e-48p.1 # <i>configure upm event user-unauthenticated profile adisconnect ports 11</i> X450e-48p.1 # <i>configure upm event device-detect profile connect ports 7</i> X450e-48p.1 # <i>configure upm event device-remove profile disconnect ports 7</i></pre>

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.	<p>Connect to the BD12k switch and log in using appropriate credentials.</p> <pre>login: <i>username</i> password: <i>xxxxxx</i></pre>

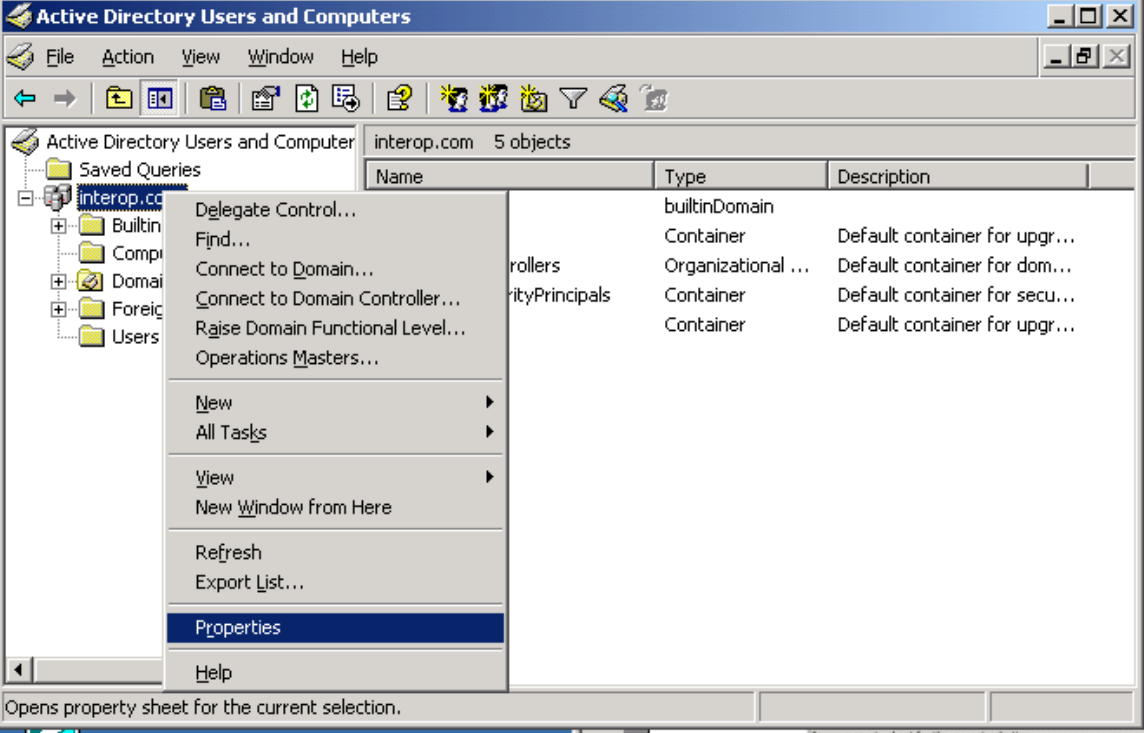
Step	Description
2.	<p>Create the VLANs on the switch.</p> <pre> BD-12804.1 # create vlan resource BD-12804.1 # config vlan resource tag 10 BD-12804.1 # config vlan resource ipaddress 172.28.10.1/24 BD-12804.1 # enable ipforwarding resource BD-12804.1 # create vlan voice BD-12804.1 # config vlan voice 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 </pre>
3.	<p>Configure VLAN assignment for the ports.</p> <pre> 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 </pre>
4.	<p>Enable DiffServ Code-Point examination on the switch for ports connecting to the Avaya S8500 Media Server and G650 Media Gateway.</p> <pre> BD-12804.1 # enable diffserv examination ports 2:1-2:4 </pre>
5.	<p>Configure bootprelay for DHCP request.</p> <pre> BD-12804.1 # configure bootprelay add 172.28.10.12 vr VR-Default </pre>

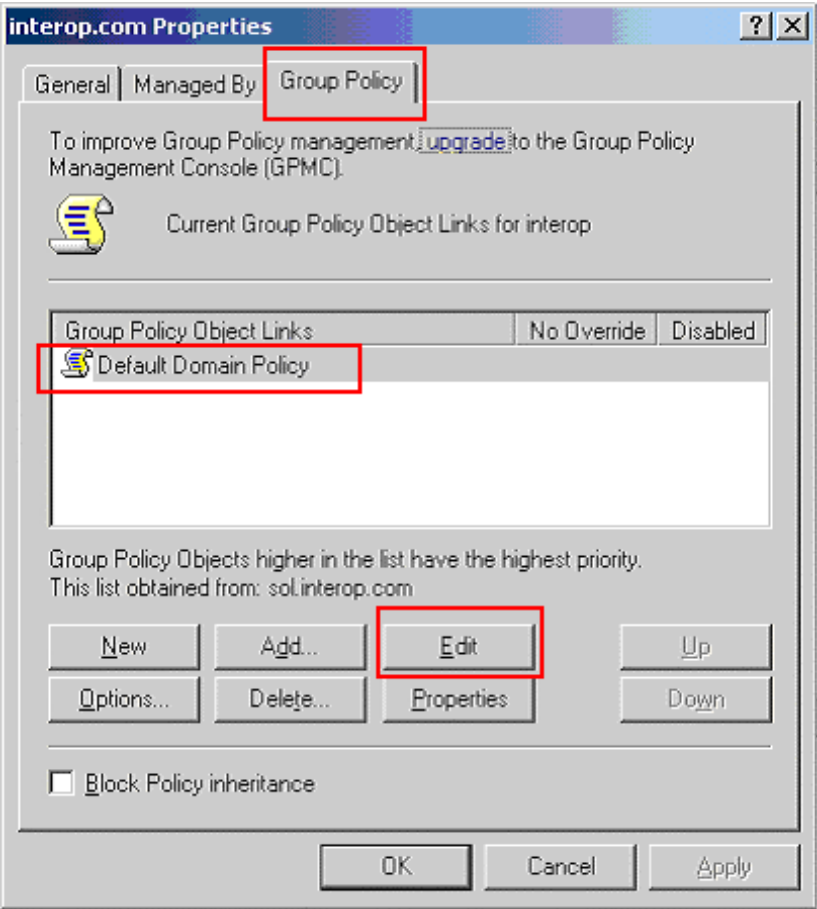
5. Configure Microsoft Services

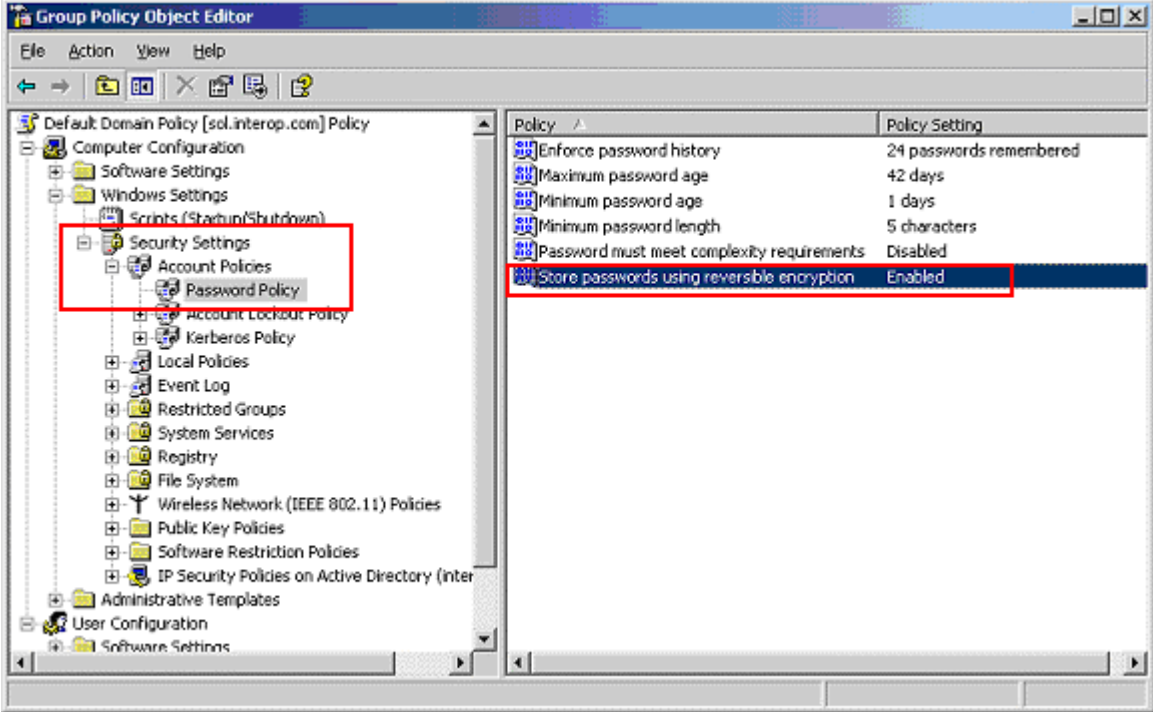
The installation of Microsoft Active Directory and Internet Authentication Services server is beyond the scope of this Application Notes and will not be covered. The configuration of the Microsoft Active Directory Service and Internet Authentication Services needed to support the sample network will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

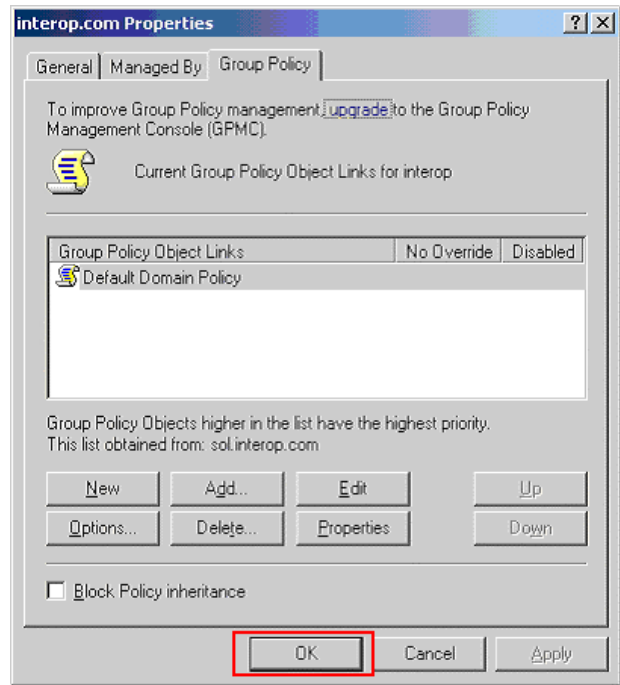
Step	Description																		
1.	<p>Invoke the Active Directory Users and Computers window under Administrative Tools of a Microsoft Windows system. Configure the active directory domain properties by highlighting the Active Directory domain then right click and select Properties.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' console window. The left pane shows a tree view with 'interop.com' selected. The right pane displays a table of objects in the domain:</p> <table border="1" data-bbox="662 730 1442 905"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>builtinDomain</td> <td>builtinDomain</td> <td></td> </tr> <tr> <td>Controllers</td> <td>Container</td> <td>Default container for upgr...</td> </tr> <tr> <td>Domain Controllers</td> <td>Organizational ...</td> <td>Default container for dom...</td> </tr> <tr> <td>SecurityPrincipals</td> <td>Container</td> <td>Default container for secu...</td> </tr> <tr> <td>Users</td> <td>Container</td> <td>Default container for upgr...</td> </tr> </tbody> </table> <p>The context menu is open over the 'interop.com' folder, and the 'Properties' option is highlighted. The status bar at the bottom reads: 'Opens property sheet for the current selection.'</p>	Name	Type	Description	builtinDomain	builtinDomain		Controllers	Container	Default container for upgr...	Domain Controllers	Organizational ...	Default container for dom...	SecurityPrincipals	Container	Default container for secu...	Users	Container	Default container for upgr...
Name	Type	Description																	
builtinDomain	builtinDomain																		
Controllers	Container	Default container for upgr...																	
Domain Controllers	Organizational ...	Default container for dom...																	
SecurityPrincipals	Container	Default container for secu...																	
Users	Container	Default container for upgr...																	

Step	Description
2.	<p>Select the Group Policy tab in the properties window. Highlight the Default Domain Policy then click Edit to display the Group Policy Object Editor.</p>  <p>The screenshot shows the 'interop.com Properties' dialog box with the 'Group Policy' tab selected. The 'Default Domain Policy' is highlighted in the list of Group Policy Object Links. The 'Edit' button is also highlighted.</p>

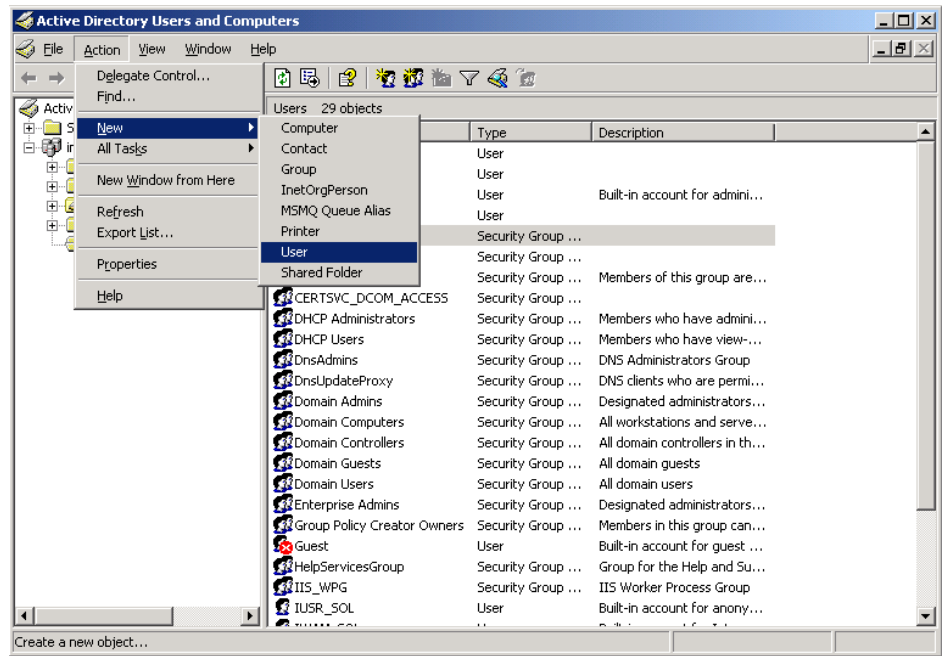
Step	Description														
3.	<p>From the Group Policy Object Editor, Navigate to Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy on the left panel. Double click on Store passwords using reversible encryption policy on the right, and change the setting to Enabled.</p>  <p>The screenshot shows the Group Policy Object Editor window. The left pane displays a tree view of policy categories. The path Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy is highlighted with a red box. The right pane shows a list of password policies. The policy Store passwords using reversible encryption is selected and highlighted with a red box, and its setting is Enabled.</p> <table border="1" data-bbox="803 525 1442 709"> <thead> <tr> <th>Policy</th> <th>Policy Setting</th> </tr> </thead> <tbody> <tr> <td>Enforce password history</td> <td>24 passwords remembered</td> </tr> <tr> <td>Maximum password age</td> <td>42 days</td> </tr> <tr> <td>Minimum password age</td> <td>1 days</td> </tr> <tr> <td>Minimum password length</td> <td>5 characters</td> </tr> <tr> <td>Password must meet complexity requirements</td> <td>Disabled</td> </tr> <tr> <td>Store passwords using reversible encryption</td> <td>Enabled</td> </tr> </tbody> </table>	Policy	Policy Setting	Enforce password history	24 passwords remembered	Maximum password age	42 days	Minimum password age	1 days	Minimum password length	5 characters	Password must meet complexity requirements	Disabled	Store passwords using reversible encryption	Enabled
Policy	Policy Setting														
Enforce password history	24 passwords remembered														
Maximum password age	42 days														
Minimum password age	1 days														
Minimum password length	5 characters														
Password must meet complexity requirements	Disabled														
Store passwords using reversible encryption	Enabled														

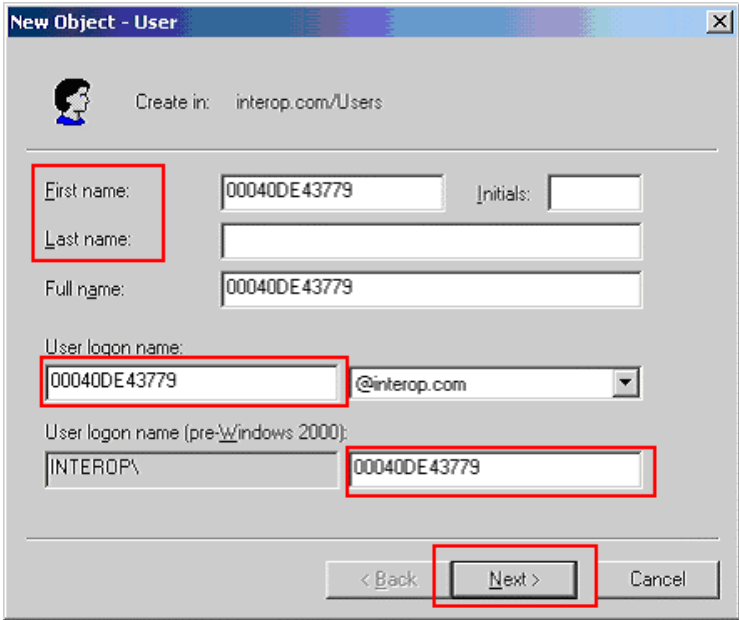
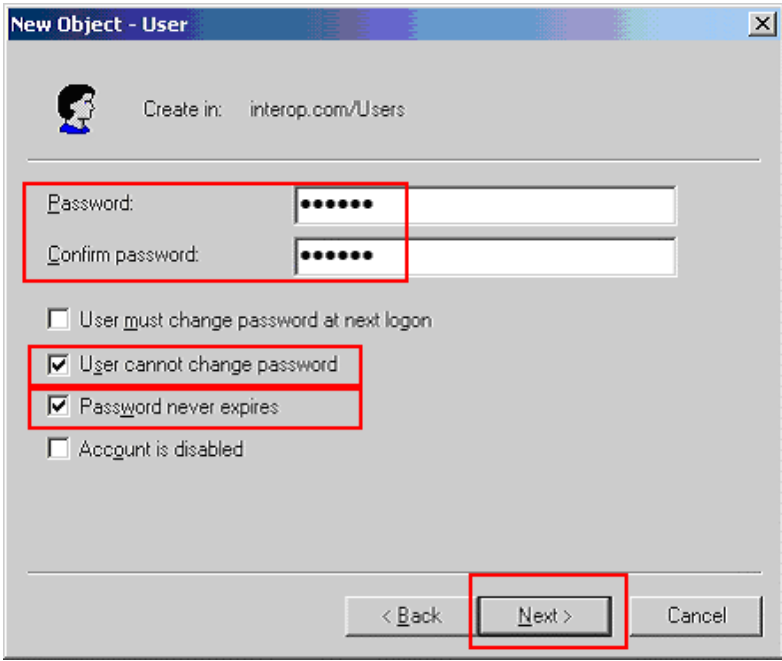
Step	Description
------	-------------

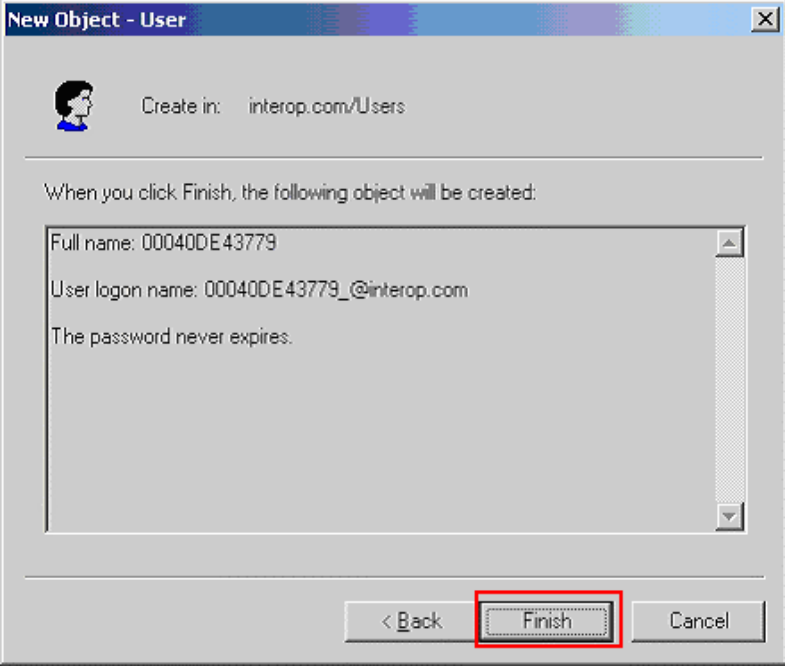
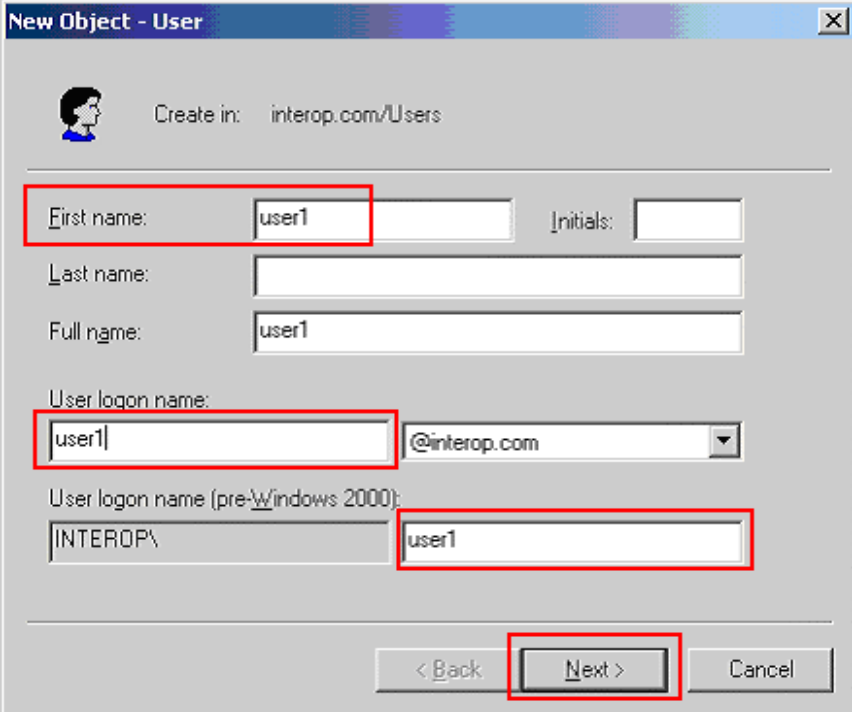
4. Click **OK** on the domain properties pop-up window to complete.

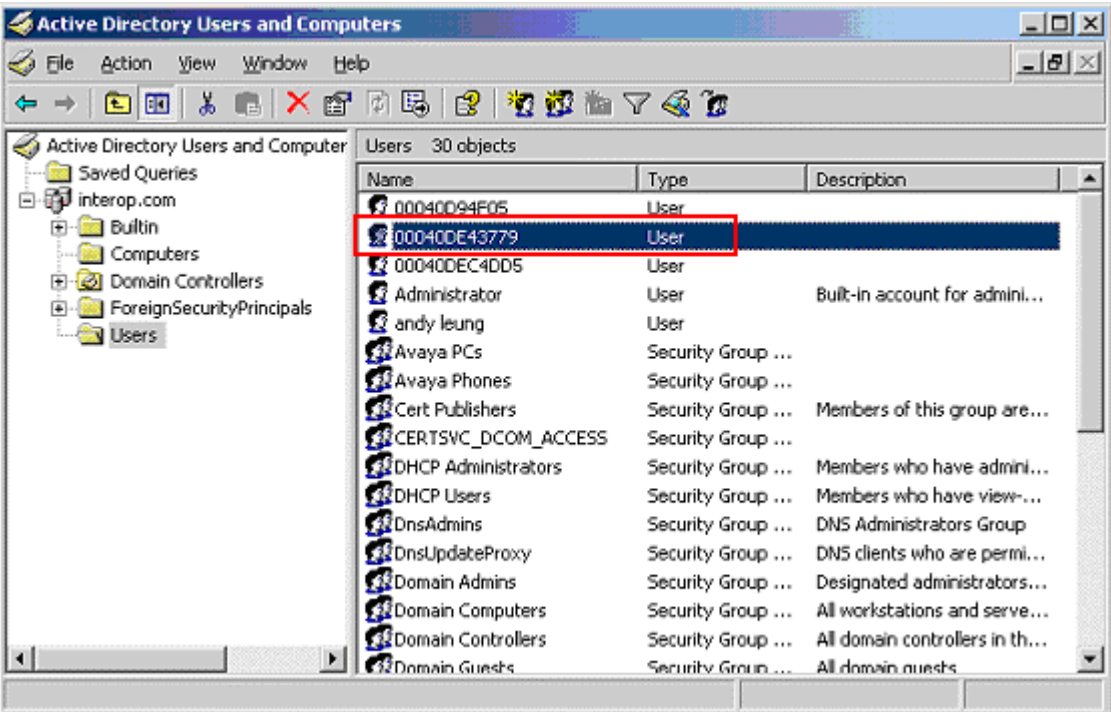


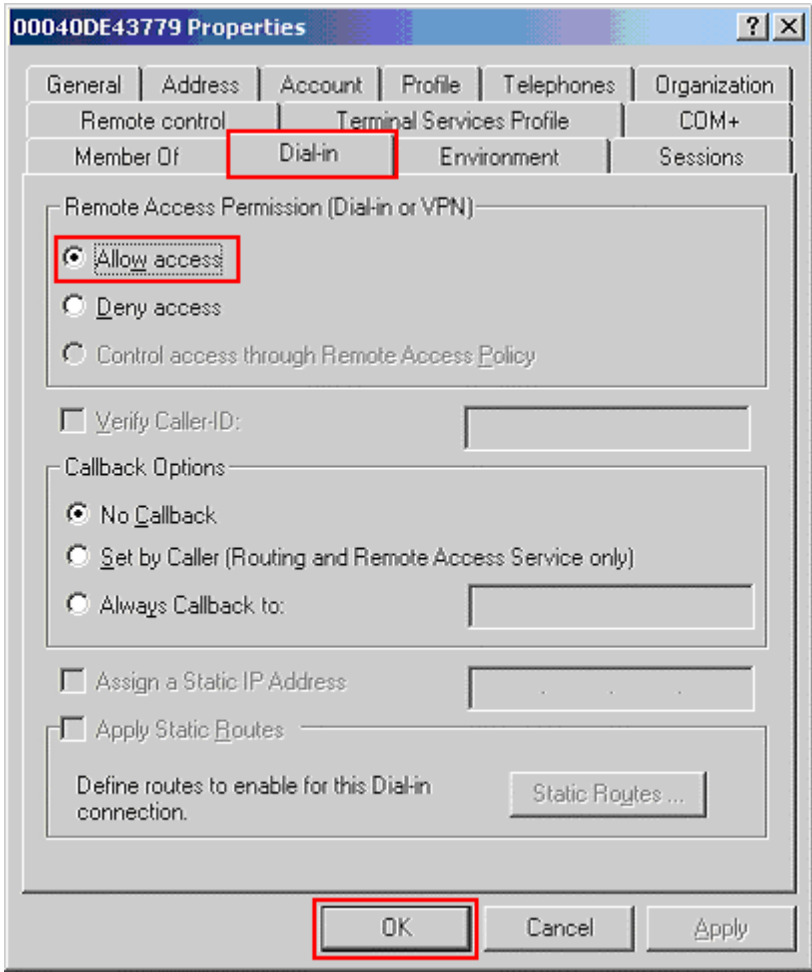
5. Create a new user ID for an Avaya IP Telephone user and a PC user. From the Active Directory Users and Computers window menu, select **Action** → **New** → **User** to begin creating a new user ID.

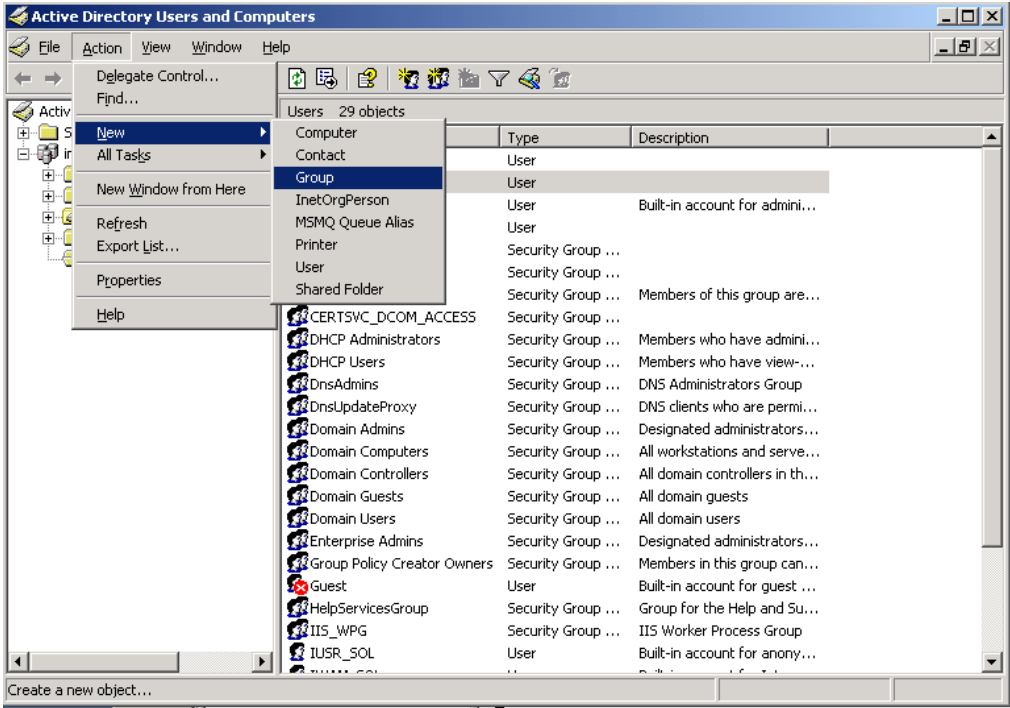
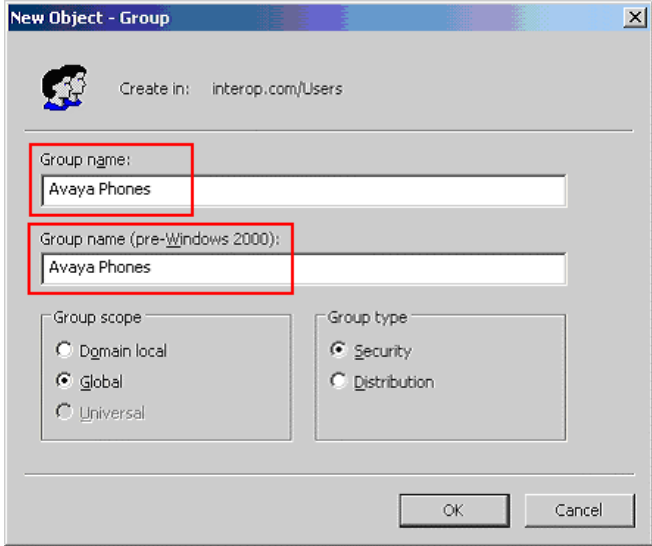


Step	Description
6.	<p>For an Avaya IP Telephone, enter the phone's MAC address as the User logon name. The First name and Last name are for information only. Click Next to continue.</p> 
7.	<p>Enter a Password for the user ID. For an Avaya IP Telephone, enter a numeric password. Select the User cannot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

Step	Description
8.	<p>Click Finish to complete.</p>  <p>The screenshot shows a dialog box titled "New Object - User" with a close button (X) in the top right corner. Below the title bar, there is a small icon of a person and the text "Create in: interop.com/Users". A horizontal line separates this from the main content area. The main content area contains the text "When you click Finish, the following object will be created:" followed by a scrollable text box with the following text: "Full name: 00040DE43779", "User logon name: 00040DE43779_@interop.com", and "The password never expires." At the bottom of the dialog box, there are three buttons: "< Back", "Finish" (highlighted with a red box), and "Cancel".</p>
9.	<p>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.</p>  <p>The screenshot shows a dialog box titled "New Object - User" with a close button (X) in the top right corner. Below the title bar, there is a small icon of a person and the text "Create in: interop.com/Users". A horizontal line separates this from the main content area. The main content area contains several input fields: "First name:" with "user1" entered (highlighted with a red box), "Initials:" (empty), "Last name:" (empty), "Full name:" with "user1" entered, "User logon name:" with "user1" entered in the first part (highlighted with a red box) and "@interop.com" in the dropdown menu, "User logon name (pre-Windows 2000):" with "INTEROP\" in the first part and "user1" in the second part (both highlighted with red boxes). At the bottom of the dialog box, there are three buttons: "< Back", "Next >" (highlighted with a red box), and "Cancel".</p>

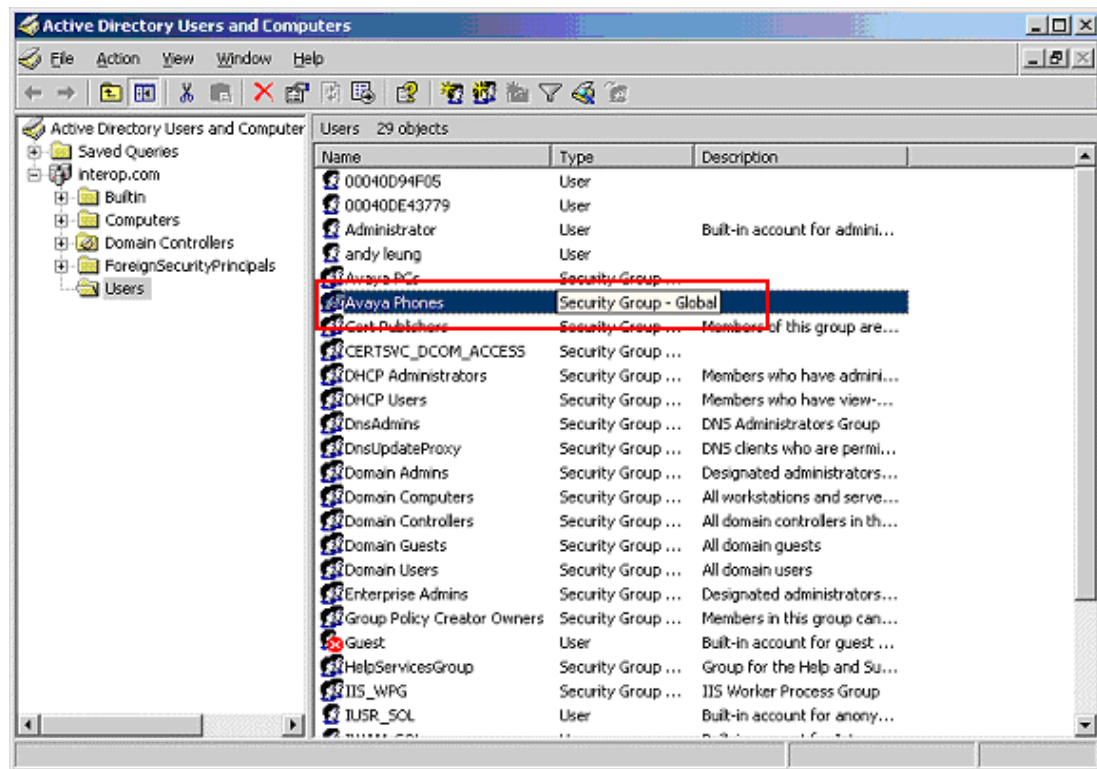
Step	Description																																																						
10.	<p>After creating the user ID, begin editing its property by double clicking on the user ID in the Active Directory Users and Computers window.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' window. The left pane shows the tree structure with 'Users' selected. The right pane displays a list of 30 objects. The user '00040DE43779' is highlighted in blue and has a red rectangular box drawn around it. Other users listed include 'Administrator', 'andy leung', and 'Domain Guests'. Security groups like 'Avaya PCs', 'Avaya Phones', and 'Domain Admins' are also visible.</p> <table border="1" data-bbox="673 499 1414 1010"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>00040D94F05</td> <td>User</td> <td></td> </tr> <tr> <td>00040DE43779</td> <td>User</td> <td></td> </tr> <tr> <td>00040DEC4DD5</td> <td>User</td> <td>Built-in account for admini...</td> </tr> <tr> <td>Administrator</td> <td>User</td> <td></td> </tr> <tr> <td>andy leung</td> <td>User</td> <td></td> </tr> <tr> <td>Avaya PCs</td> <td>Security Group ...</td> <td></td> </tr> <tr> <td>Avaya Phones</td> <td>Security Group ...</td> <td></td> </tr> <tr> <td>Cert Publishers</td> <td>Security Group ...</td> <td>Members of this group are...</td> </tr> <tr> <td>CERTSVC_DCOM_ACCESS</td> <td>Security Group ...</td> <td></td> </tr> <tr> <td>DHCP Administrators</td> <td>Security Group ...</td> <td>Members who have admini...</td> </tr> <tr> <td>DHCP Users</td> <td>Security Group ...</td> <td>Members who have view-...</td> </tr> <tr> <td>DnsAdmins</td> <td>Security Group ...</td> <td>DNS Administrators Group</td> </tr> <tr> <td>DnsUpdateProxy</td> <td>Security Group ...</td> <td>DNS clients who are permi...</td> </tr> <tr> <td>Domain Admins</td> <td>Security Group ...</td> <td>Designated administrators...</td> </tr> <tr> <td>Domain Computers</td> <td>Security Group ...</td> <td>All workstations and serve...</td> </tr> <tr> <td>Domain Controllers</td> <td>Security Group ...</td> <td>All domain controllers in th...</td> </tr> <tr> <td>Domain Guests</td> <td>Security Group ...</td> <td>All domain guests</td> </tr> </tbody> </table>	Name	Type	Description	00040D94F05	User		00040DE43779	User		00040DEC4DD5	User	Built-in account for admini...	Administrator	User		andy leung	User		Avaya PCs	Security Group ...		Avaya Phones	Security Group ...		Cert Publishers	Security Group ...	Members of this group are...	CERTSVC_DCOM_ACCESS	Security Group ...		DHCP Administrators	Security Group ...	Members who have admini...	DHCP Users	Security Group ...	Members who have view-...	DnsAdmins	Security Group ...	DNS Administrators Group	DnsUpdateProxy	Security Group ...	DNS clients who are permi...	Domain Admins	Security Group ...	Designated administrators...	Domain Computers	Security Group ...	All workstations and serve...	Domain Controllers	Security Group ...	All domain controllers in th...	Domain Guests	Security Group ...	All domain guests
Name	Type	Description																																																					
00040D94F05	User																																																						
00040DE43779	User																																																						
00040DEC4DD5	User	Built-in account for admini...																																																					
Administrator	User																																																						
andy leung	User																																																						
Avaya PCs	Security Group ...																																																						
Avaya Phones	Security Group ...																																																						
Cert Publishers	Security Group ...	Members of this group are...																																																					
CERTSVC_DCOM_ACCESS	Security Group ...																																																						
DHCP Administrators	Security Group ...	Members who have admini...																																																					
DHCP Users	Security Group ...	Members who have view-...																																																					
DnsAdmins	Security Group ...	DNS Administrators Group																																																					
DnsUpdateProxy	Security Group ...	DNS clients who are permi...																																																					
Domain Admins	Security Group ...	Designated administrators...																																																					
Domain Computers	Security Group ...	All workstations and serve...																																																					
Domain Controllers	Security Group ...	All domain controllers in th...																																																					
Domain Guests	Security Group ...	All domain guests																																																					

Step	Description
11.	<p>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.</p>  <p>The screenshot shows the '00040DE43779 Properties' dialog box with the 'Dial-in' tab selected. The 'Remote Access Permission (Dial-in or VPN)' section has the 'Allow access' radio button selected. The 'OK' button at the bottom is highlighted with a red box.</p>

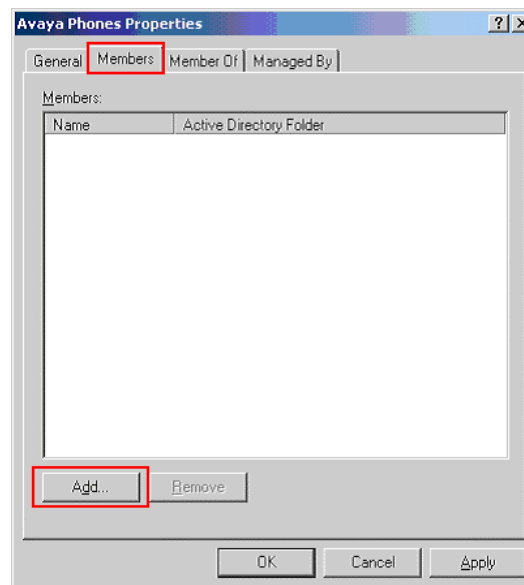
Step	Description
12.	<p>Create a new user Group by selecting Action → New → Group from the drop-down menu. The use of a Group facilitates the assignment and management of additional user IDs.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' console. The 'Action' menu is open, and the 'New' option is selected, which has opened a sub-menu where 'Group' is highlighted. The main window displays a list of 29 objects in the 'Users' container, including various security groups and users.</p>
13.	<p>Create a group for Avaya IP Telephones. The sample network uses the name Avaya Phones for this group. Click OK to complete.</p>  <p>The screenshot shows the 'New Object - Group' dialog box. The 'Create in' field is set to 'interop.com/Users'. Both the 'Group name' and 'Group name (pre-Windows 2000)' fields contain the text 'Avaya Phones'. The 'Group scope' is set to 'Global' and the 'Group type' is set to 'Security'. The 'OK' button is highlighted.</p>
14.	Repeat Steps 12 and 13 to create another user Group for the PC.

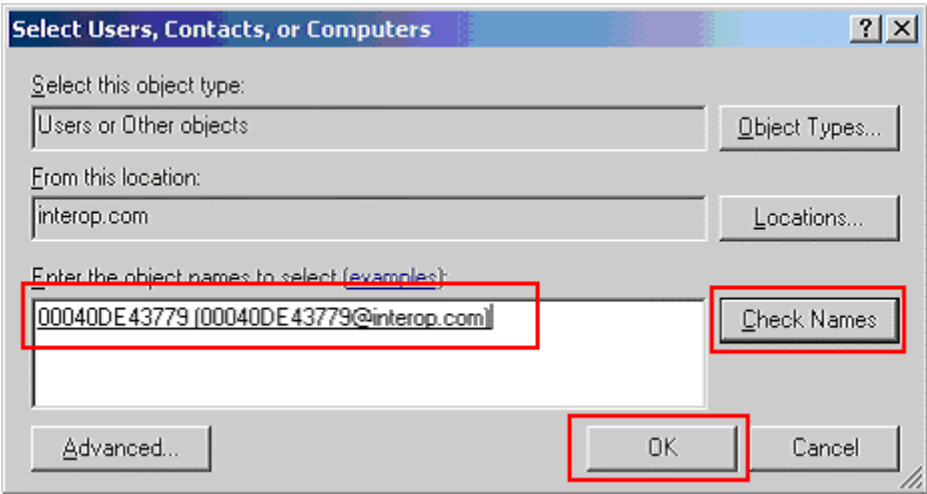
Step	Description
------	-------------

15.	After creating the user Group, begin editing its property by double clicking on the Group in the Active Directory Users and Computers window.
-----	---



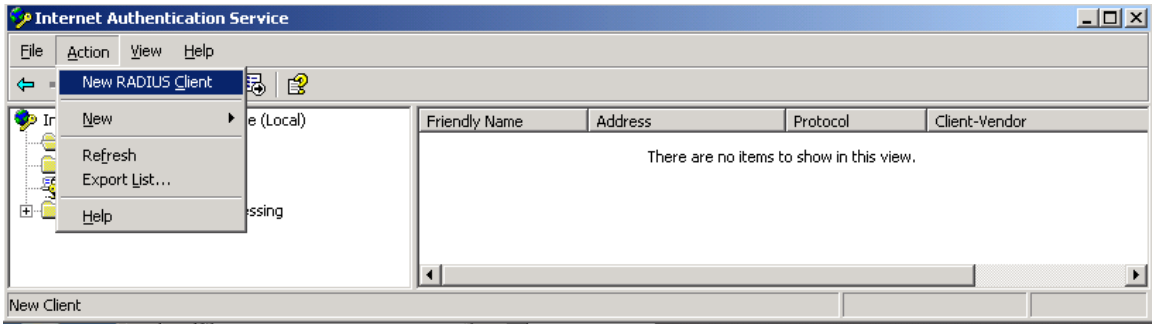
16.	Select the Members tab in the group Properties window. Click Add to continue.
-----	---

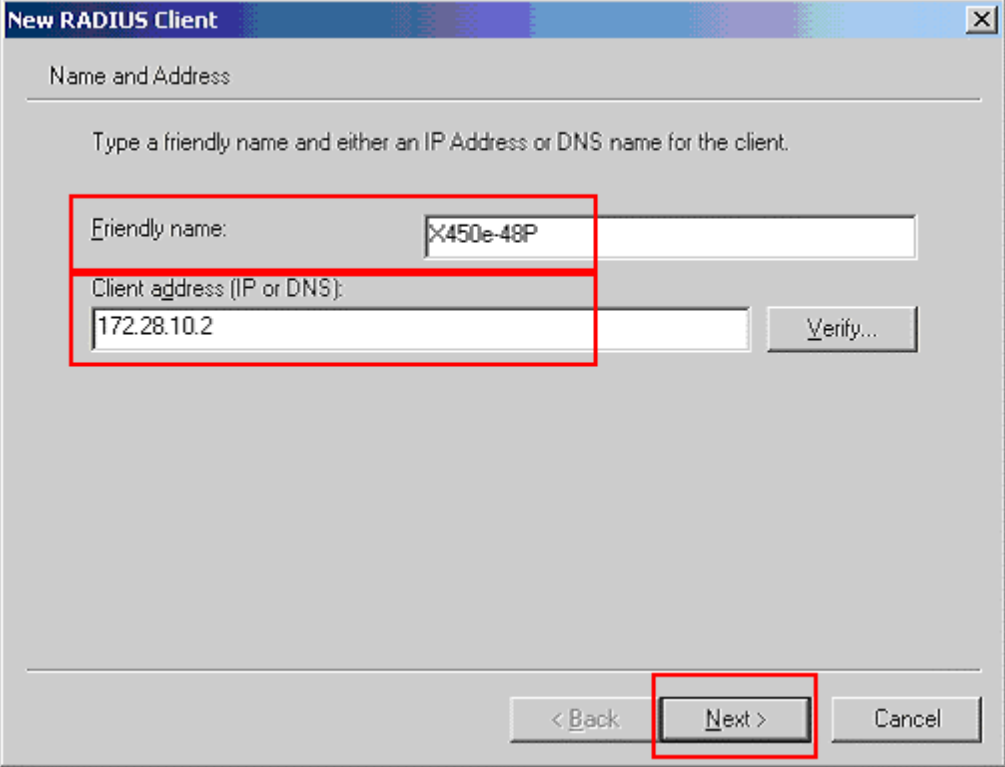


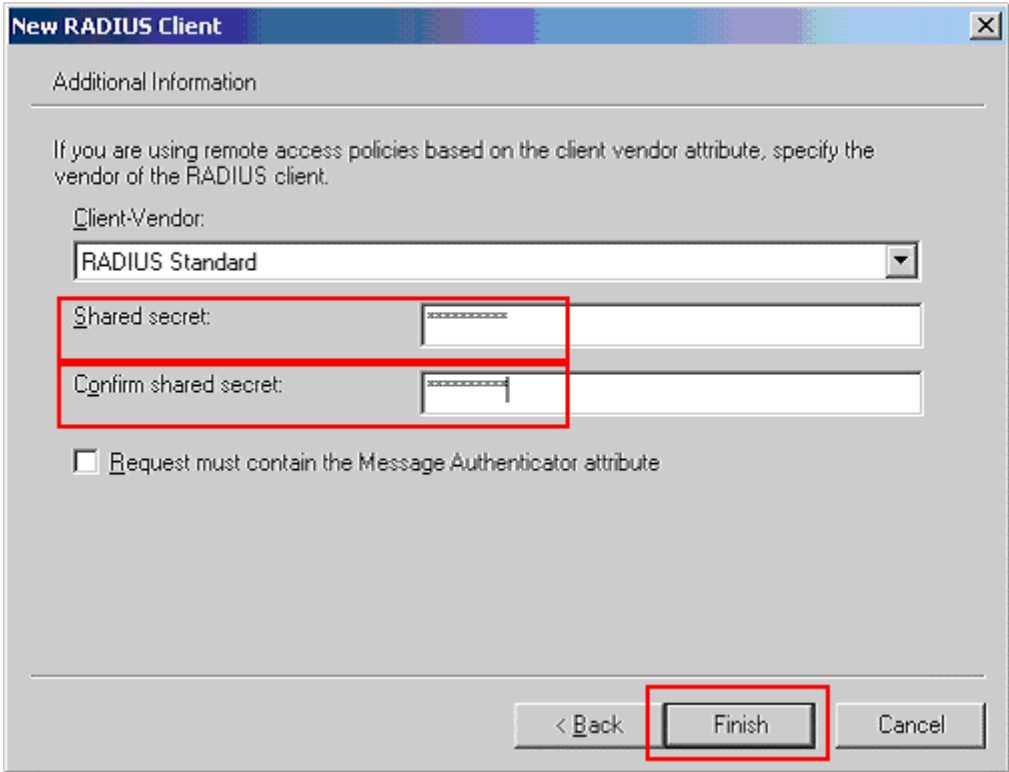
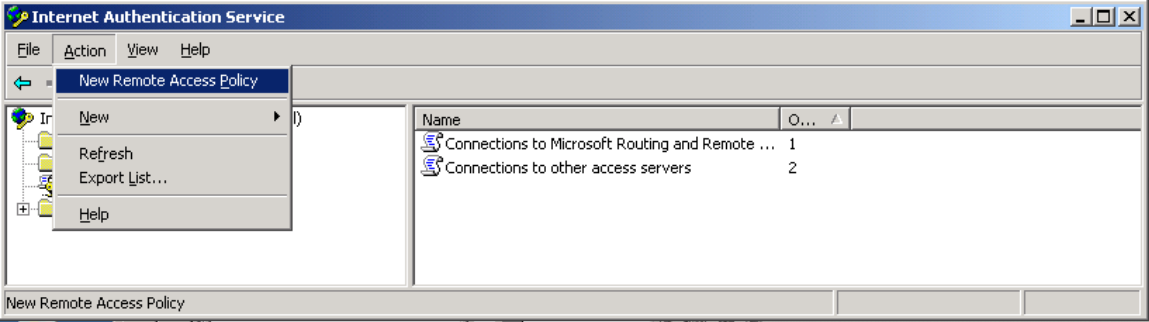
Step	Description
17.	<p>Enter the user ID that should be assigned to the Avaya Phones group. This should be the user ID for the Avaya IP Telephone. Use Check Names to assist in searching for the user ID. Click OK to complete.</p> 
18.	Repeat Steps 15-17 to add members to the PCs user group.

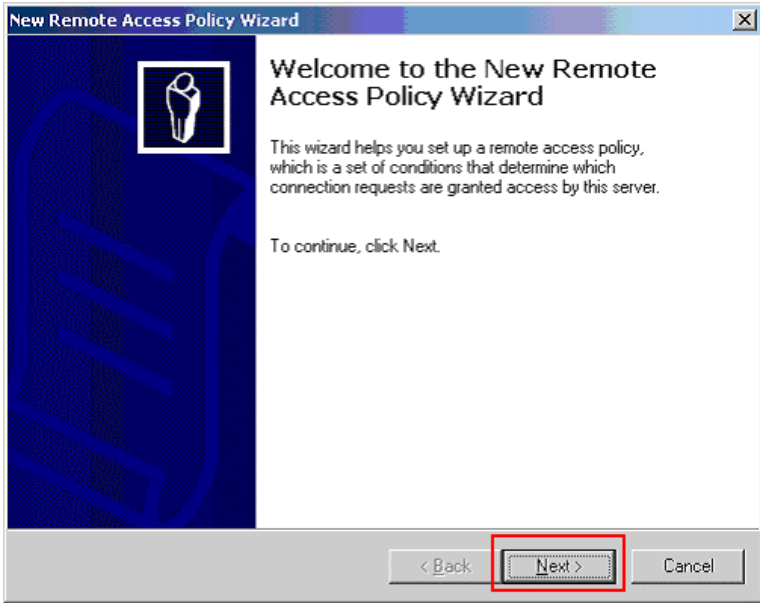
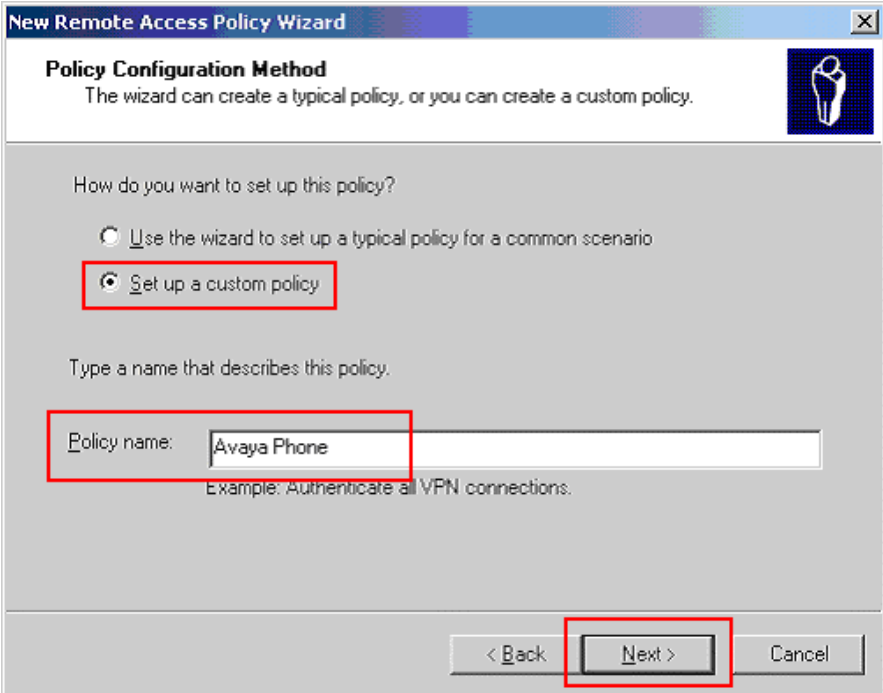
5.2. Configure Microsoft Internet Authentication Services (IAS) Server

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.	<p>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.</p> 

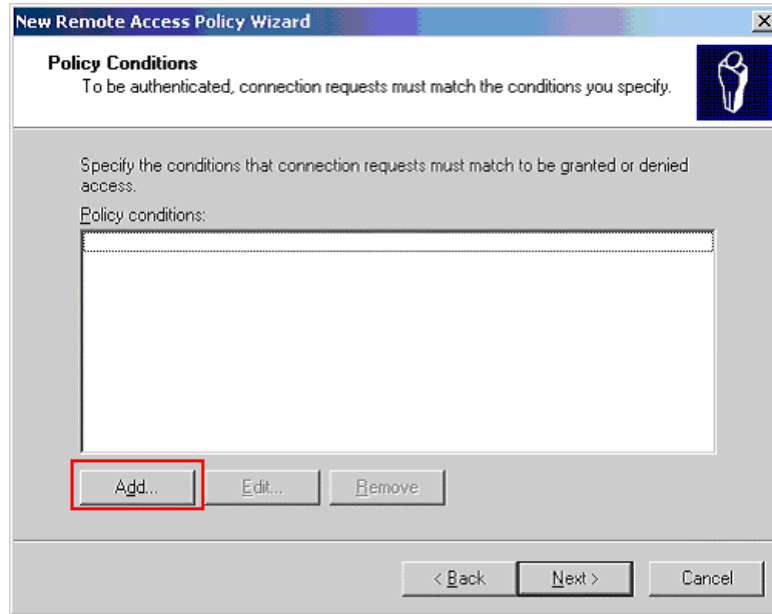
Step	Description
2.	<p>Enter the name and IP address of the X450e-48p switch to create a new RADIUS client. This must match the IP address configured in Section 4.1, Step 4. Click Next to continue.</p> 

Step	Description						
3.	<p>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.</p>  <p>The screenshot shows a dialog box titled "New RADIUS Client". Under "Additional Information", there is a dropdown for "Client-Vendor" set to "RADIUS Standard". Below it are two text input fields: "Shared secret" and "Confirm shared secret", both containing masked characters. A checkbox for "Request must contain the Message Authenticator attribute" is unchecked. At the bottom, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a red box.</p>						
4.	<p>Create a new access policy for the Avaya IP Telephones by clicking on Action → New Remote Access Policy.</p>  <p>The screenshot shows the "Internet Authentication Service" console. The "Action" menu is open, and "New Remote Access Policy" is selected. The main pane shows a list of policies with columns for "Name" and "Connections".</p> <table border="1" data-bbox="690 1360 1414 1535"> <thead> <tr> <th>Name</th> <th>Connections</th> </tr> </thead> <tbody> <tr> <td>Connections to Microsoft Routing and Remote ...</td> <td>1</td> </tr> <tr> <td>Connections to other access servers</td> <td>2</td> </tr> </tbody> </table>	Name	Connections	Connections to Microsoft Routing and Remote ...	1	Connections to other access servers	2
Name	Connections						
Connections to Microsoft Routing and Remote ...	1						
Connections to other access servers	2						

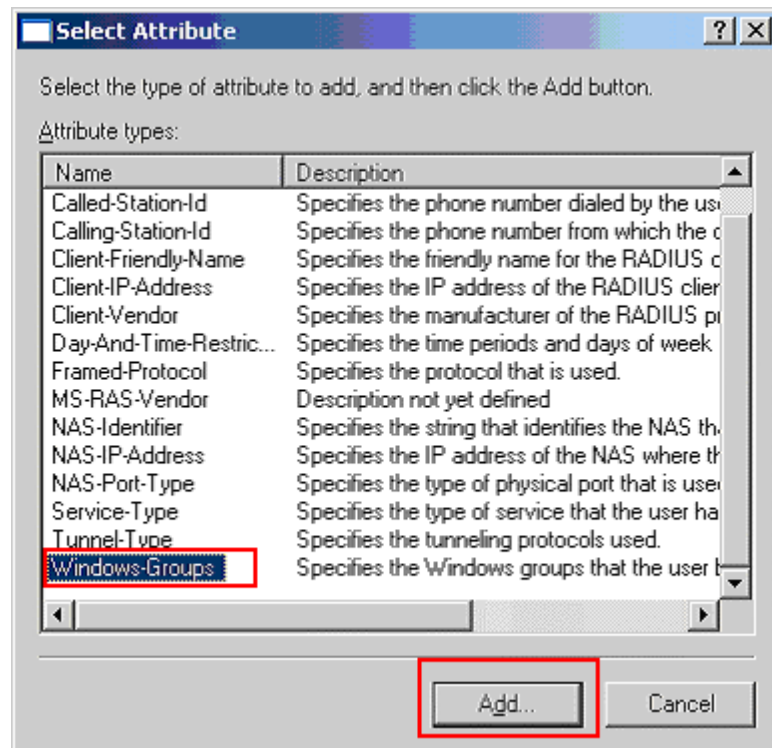
Step	Description
5.	<p>Click Next in the New Remote Access Policy Wizard.</p> 
6.	<p>Select Set up a custom policy radio button and enter a Policy name. The sample network uses the name Avaya Phone. Click Next to continue.</p> 

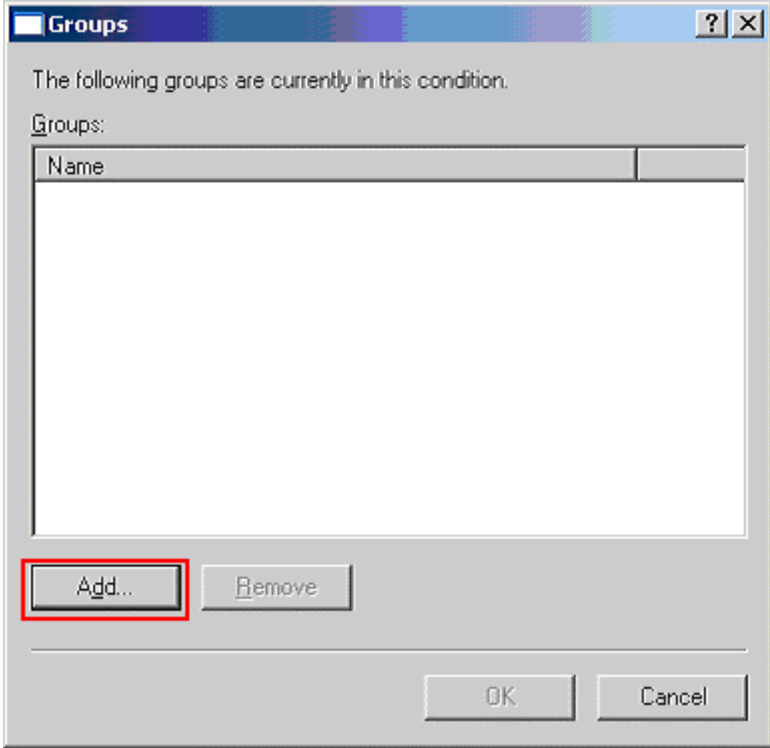
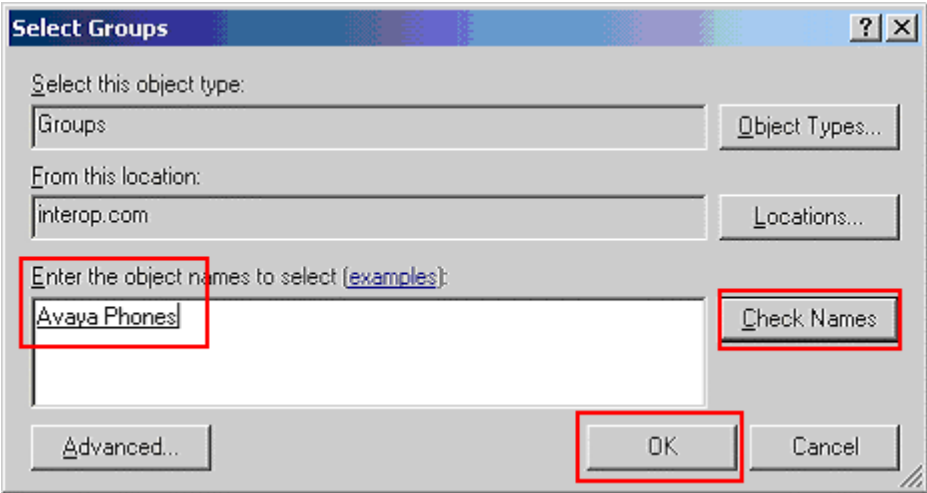
Step	Description
------	-------------

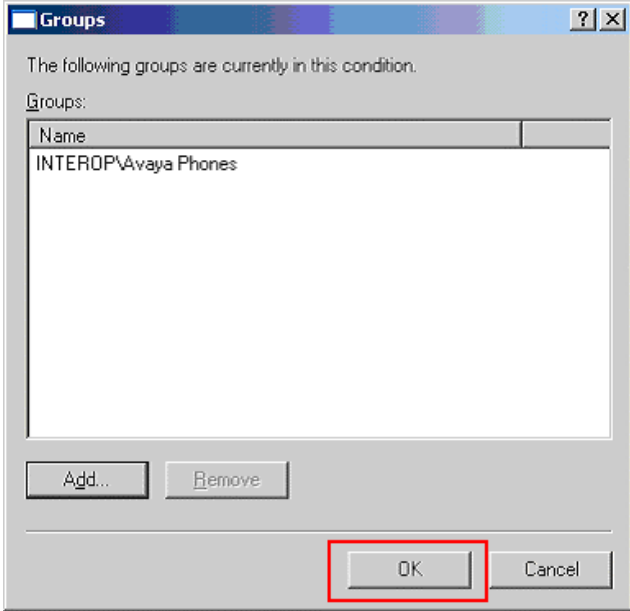
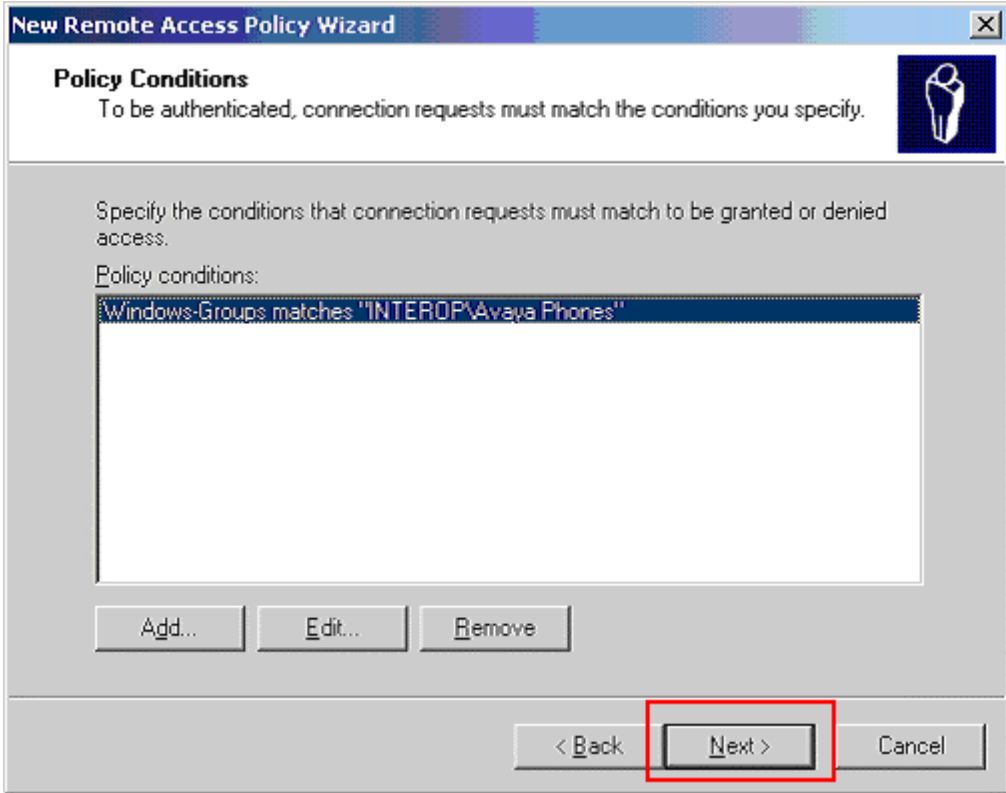
7. Click the Add button to add a new policy condition.

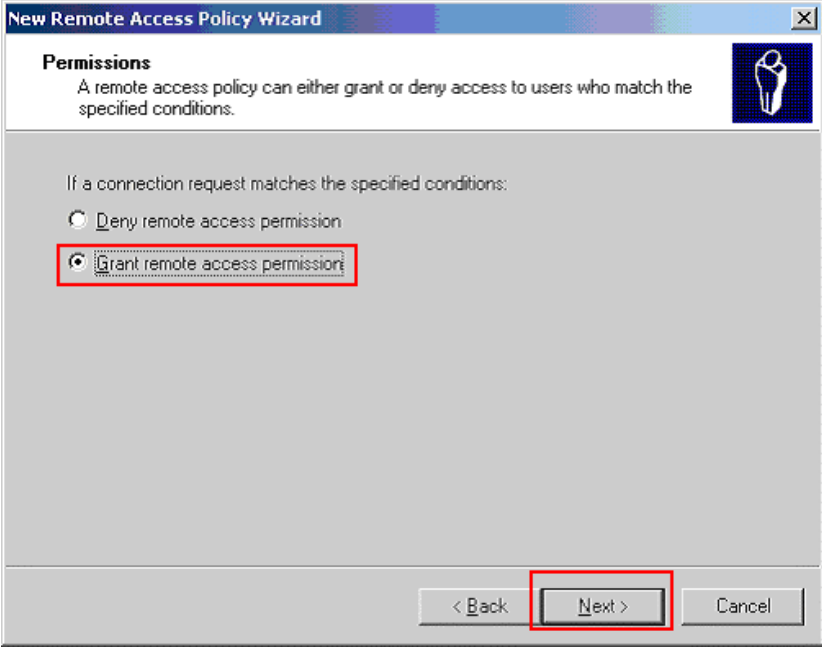
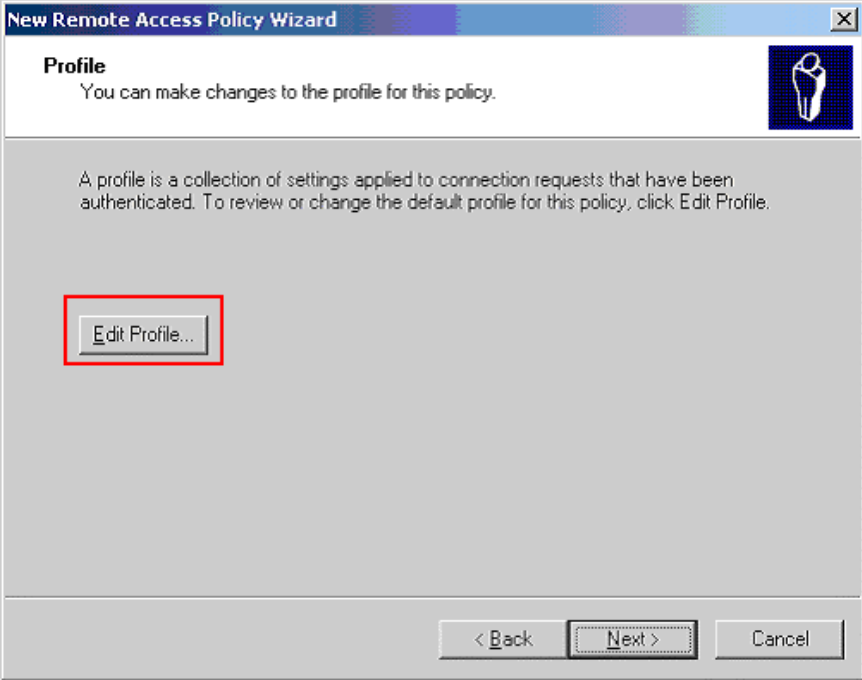


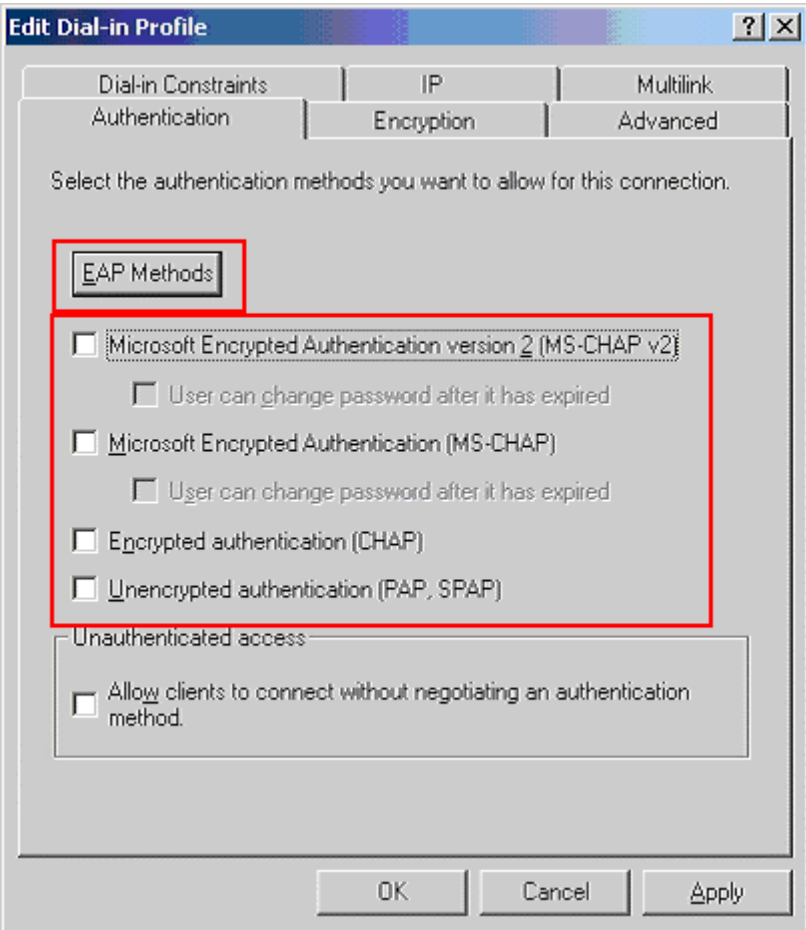
8. Highlight **Windows-Groups** from the Select Attribute pop-up window. Click **Add** to continue.

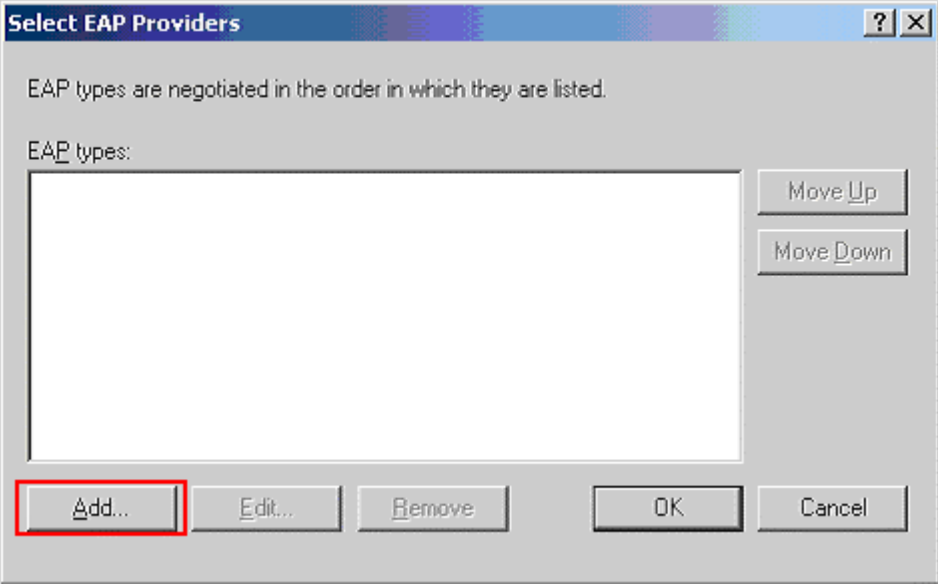
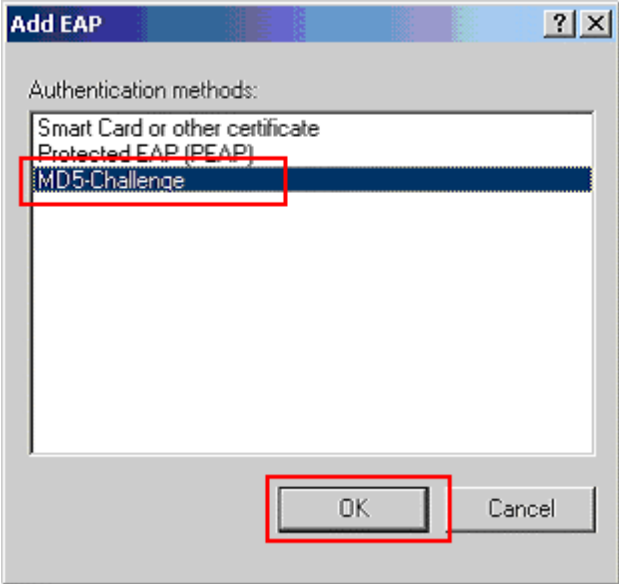


Step	Description
9.	<p>Click Add in the Groups pop-up window to add a windows group.</p> 
10.	<p>Enter the Active Directory user group created in Section 5.1, Steps 12-13. Use Check Names to assist in searching for the user group. Click OK to complete.</p> 

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

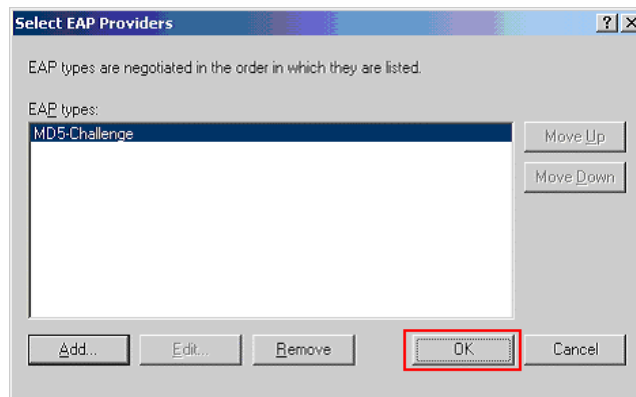
Step	Description
13.	<p>Click the Grant remote access permission radio button. Click Next to continue.</p>  <p>The screenshot shows a window titled "New Remote Access Policy Wizard" with a "Permissions" section. It contains the text: "A remote access policy can either grant or deny access to users who match the specified conditions." Below this, it says "If a connection request matches the specified conditions:" followed by two radio buttons: "Deny remote access permission" (unselected) and "Grant remote access permission" (selected). The "Grant" option is enclosed in a red rectangular box. At the bottom of the window, there are three buttons: "< Back", "Next >" (highlighted with a red box), and "Cancel".</p>
14.	<p>Click Edit Profile to configure the profile for this access policy. This will display the Edit Dial-in Profile pop-up window.</p>  <p>The screenshot shows a window titled "New Remote Access Policy Wizard" with a "Profile" section. It contains the text: "You can make changes to the profile for this policy." Below this, it says: "A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile." A button labeled "Edit Profile..." is highlighted with a red rectangular box. At the bottom of the window, there are three buttons: "< Back", "Next >" (highlighted with a red box), and "Cancel".</p>

Step	Description
15.	<p>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.</p> 

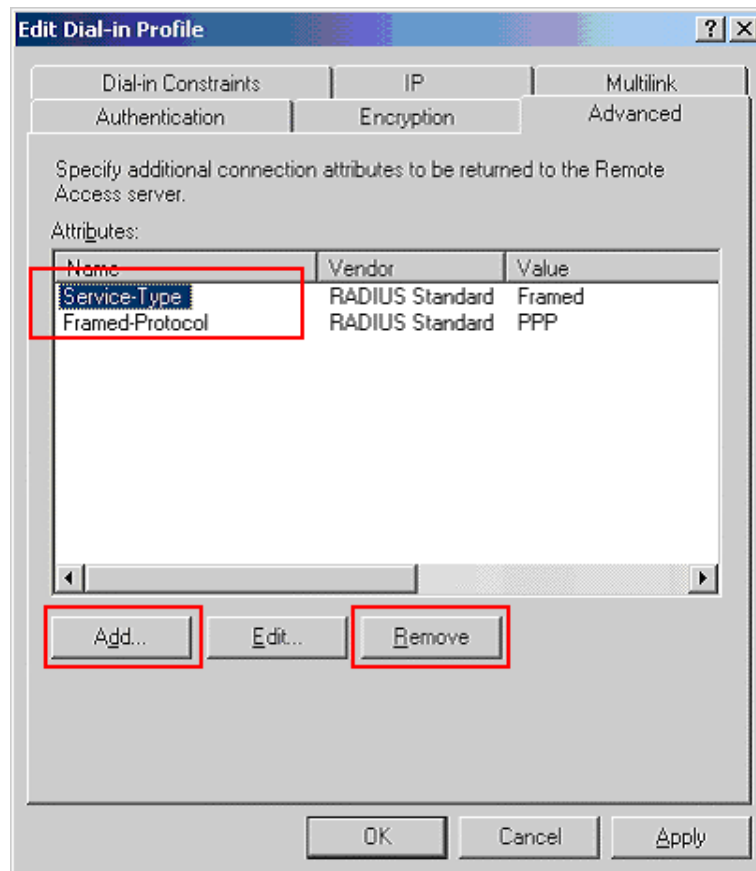
Step	Description
16.	<p>Click Add in the Select EAP Providers pop-up window to add a new EAP type.</p> 
17.	<p>Select MD5-Challenge in the Add EAP pop-up window. Click OK to continue.</p> 

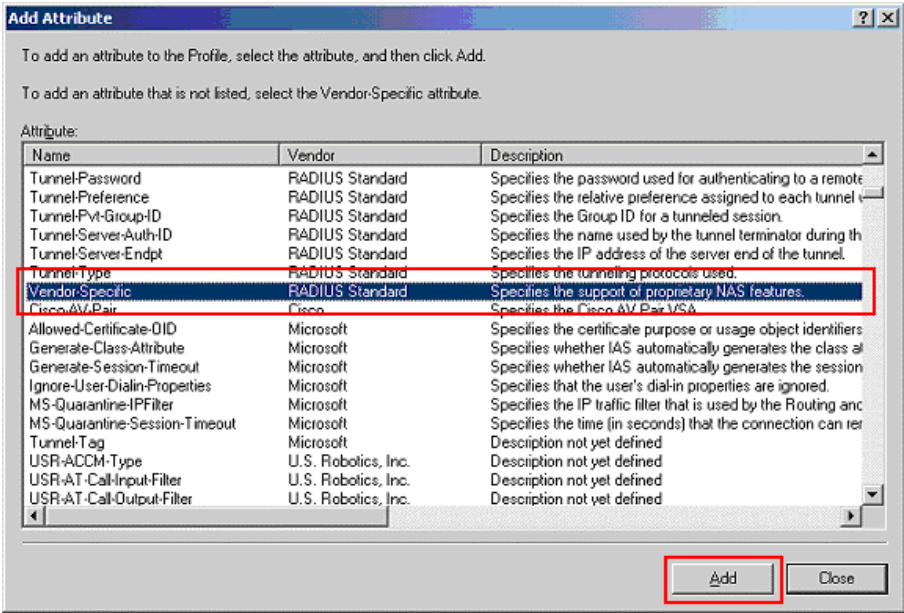
Step	Description
------	-------------

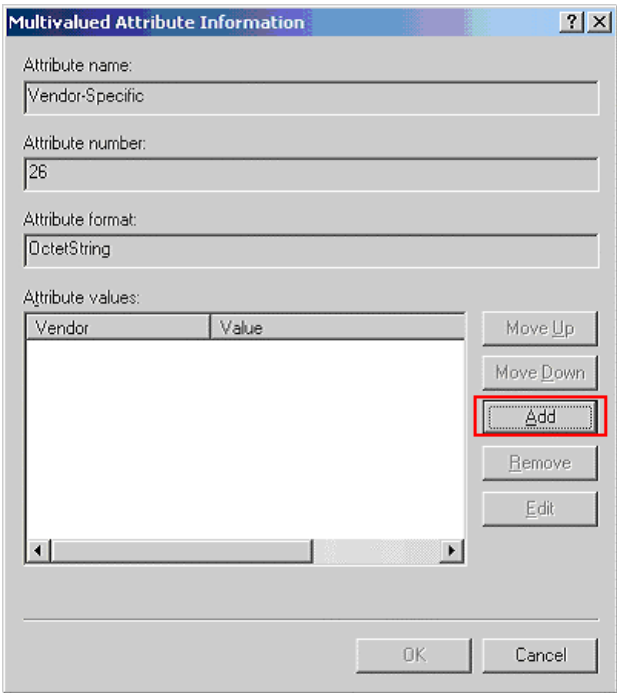
18. Once the MD5-Challenge EAP type is added, Click **OK** to complete the EAP authentication selection.

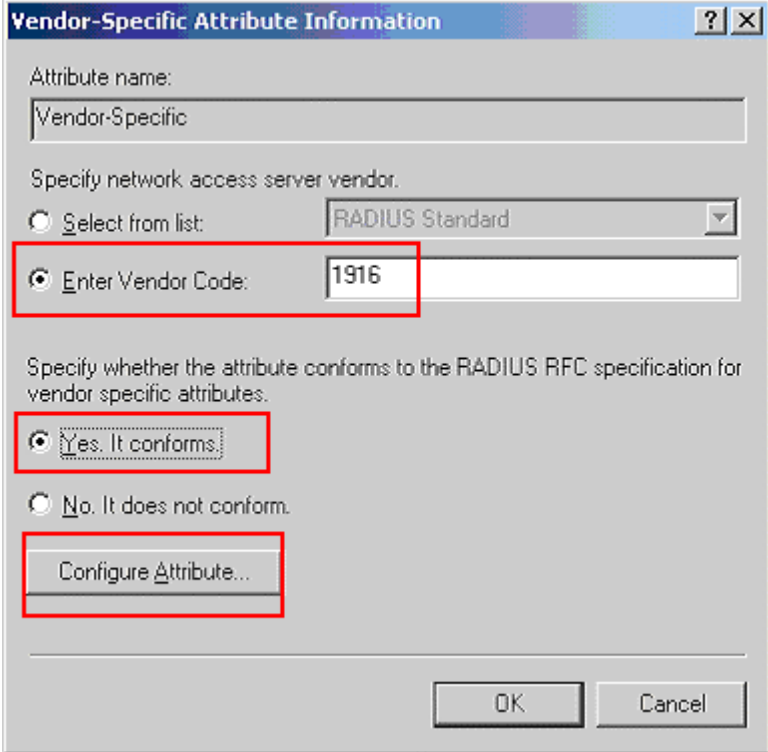


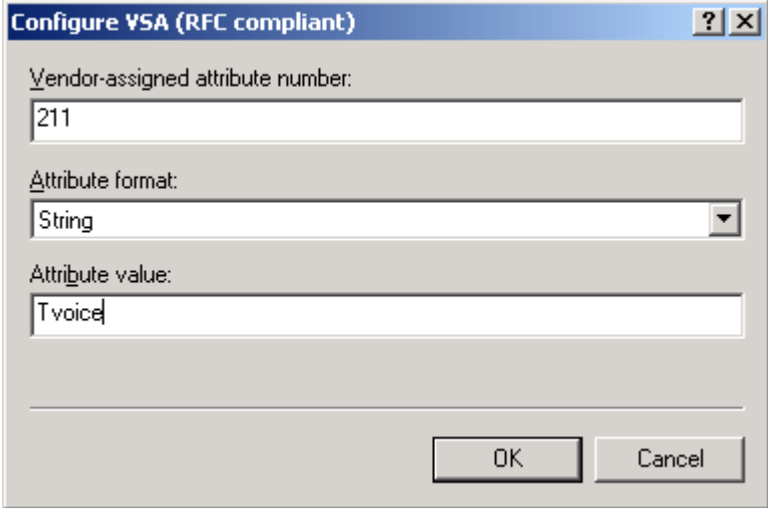
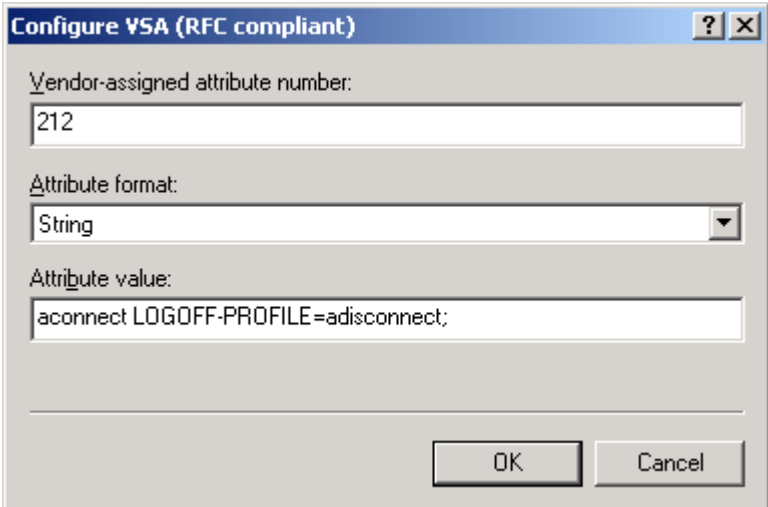
19. Select the **Advanced** tab in the Edit Dial-in profile pop-up window. Highlight each existing attribute, then click **Remove** to delete it. Click **Add** after all existing attributes have been removed to enter a new attribute. This will display the Add Attribute pop-up window.

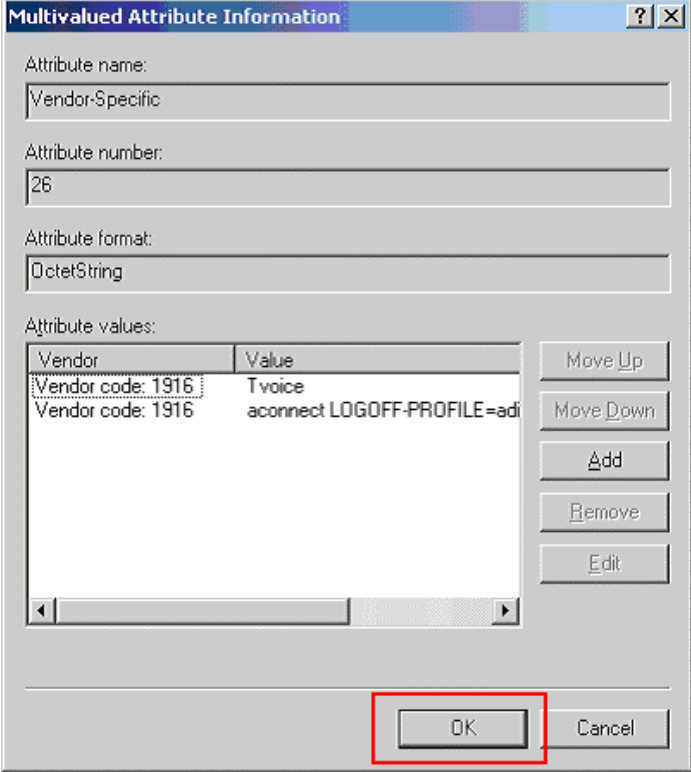


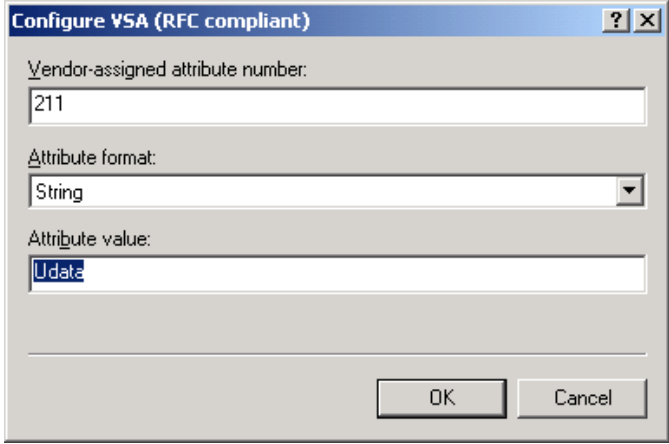
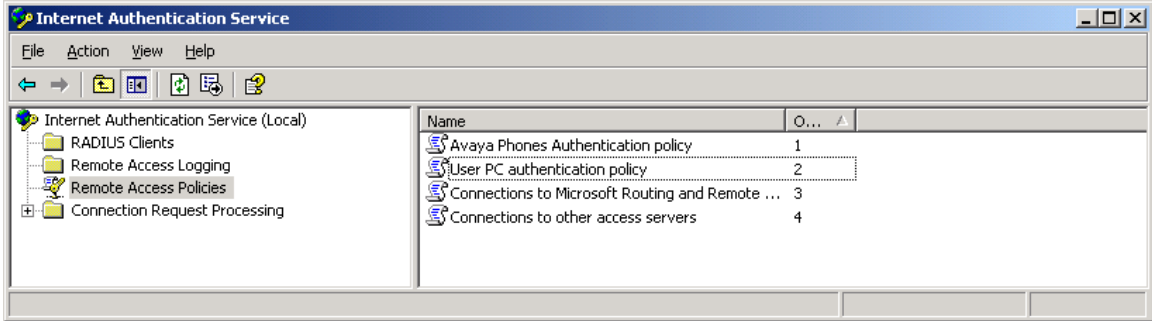
Step	Description																																																									
20.	<p>Highlight the Vendor Specific attribute name from the list of attributes displayed in the Add Attribute pop-up window. Click Add to continue. This will display the Multivalued Attribute Information pop-up window.</p>  <p>The screenshot shows the 'Add Attribute' dialog box with the following table of attributes:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Vendor</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>Tunnel-Password</td><td>RADIUS Standard</td><td>Specifies the password used for authenticating to a remote</td></tr> <tr><td>Tunnel-Preference</td><td>RADIUS Standard</td><td>Specifies the relative preference assigned to each tunnel</td></tr> <tr><td>Tunnel-Pvt-Group-ID</td><td>RADIUS Standard</td><td>Specifies the Group ID for a tunneled session.</td></tr> <tr><td>Tunnel-Server-Auth-ID</td><td>RADIUS Standard</td><td>Specifies the name used by the tunnel terminator during th</td></tr> <tr><td>Tunnel-Server-Endpt</td><td>RADIUS Standard</td><td>Specifies the IP address of the server end of the tunnel.</td></tr> <tr><td>Tunnel-Type</td><td>RADIUS Standard</td><td>Specifies the tunneling protocols used.</td></tr> <tr><td>Vendor-Specific</td><td>RADIUS Standard</td><td>Specifies the support of proprietary NAS features.</td></tr> <tr><td>Cisco-AV-Pair</td><td>Cisco</td><td>Specifies the Cisco AV Pair VSA.</td></tr> <tr><td>Allowed-Certificate-DID</td><td>Microsoft</td><td>Specifies the certificate purpose or usage object identifiers</td></tr> <tr><td>Generate-Class-Attribute</td><td>Microsoft</td><td>Specifies whether IAS automatically generates the class at</td></tr> <tr><td>Generate-Session-Timeout</td><td>Microsoft</td><td>Specifies whether IAS automatically generates the session</td></tr> <tr><td>Ignore-User-Dialin-Properties</td><td>Microsoft</td><td>Specifies that the user's dial-in properties are ignored.</td></tr> <tr><td>MS-Quarantine-IPFilter</td><td>Microsoft</td><td>Specifies the IP traffic filter that is used by the Routing anc</td></tr> <tr><td>MS-Quarantine-Session-Timeout</td><td>Microsoft</td><td>Specifies the time (in seconds) that the connection can ter</td></tr> <tr><td>Tunnel-Tag</td><td>Microsoft</td><td>Description not yet defined</td></tr> <tr><td>USR-ACCM-Type</td><td>U.S. Robotics, Inc.</td><td>Description not yet defined</td></tr> <tr><td>USR-AT-Call-Input-Filter</td><td>U.S. Robotics, Inc.</td><td>Description not yet defined</td></tr> <tr><td>USR-AT-Call-Output-Filter</td><td>U.S. Robotics, Inc.</td><td>Description not yet defined</td></tr> </tbody> </table>	Name	Vendor	Description	Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote	Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel	Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.	Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th	Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.	Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.	Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.	Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.	Allowed-Certificate-DID	Microsoft	Specifies the certificate purpose or usage object identifiers	Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at	Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session	Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.	MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing anc	MS-Quarantine-Session-Timeout	Microsoft	Specifies the time (in seconds) that the connection can ter	Tunnel-Tag	Microsoft	Description not yet defined	USR-ACCM-Type	U.S. Robotics, Inc.	Description not yet defined	USR-AT-Call-Input-Filter	U.S. Robotics, Inc.	Description not yet defined	USR-AT-Call-Output-Filter	U.S. Robotics, Inc.	Description not yet defined
Name	Vendor	Description																																																								
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote																																																								
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel																																																								
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.																																																								
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th																																																								
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.																																																								
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.																																																								
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.																																																								
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.																																																								
Allowed-Certificate-DID	Microsoft	Specifies the certificate purpose or usage object identifiers																																																								
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at																																																								
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session																																																								
Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.																																																								
MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing anc																																																								
MS-Quarantine-Session-Timeout	Microsoft	Specifies the time (in seconds) that the connection can ter																																																								
Tunnel-Tag	Microsoft	Description not yet defined																																																								
USR-ACCM-Type	U.S. Robotics, Inc.	Description not yet defined																																																								
USR-AT-Call-Input-Filter	U.S. Robotics, Inc.	Description not yet defined																																																								
USR-AT-Call-Output-Filter	U.S. Robotics, Inc.	Description not yet defined																																																								

21.	<p>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.</p>  <p>The screenshot shows the 'Multivalued Attribute Information' dialog box with the following fields and buttons:</p> <ul style="list-style-type: none"> Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: (Empty table with columns Vendor and Value) Buttons: Move Up, Move Down, Add (highlighted), Remove, Edit Bottom buttons: OK, Cancel
-----	---

Step	Description
22.	<p>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.</p> 

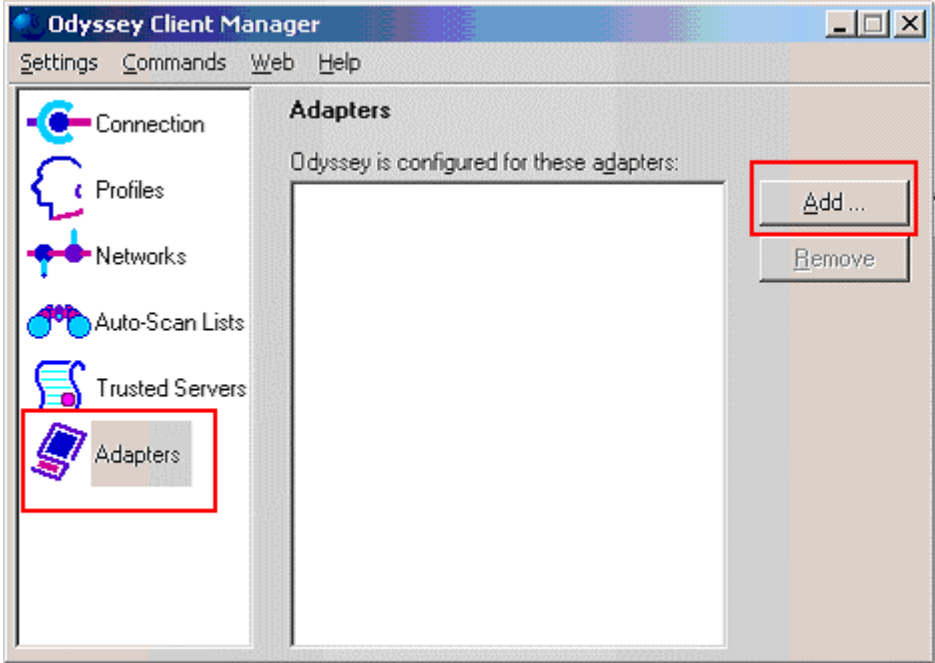
Step	Description
23.	<p>Enter the following field information in the Configure VSA (RFC compliant) pop-up window. The Attribute value “Tvoice” signifies that the port should be configured as “Tagged” by the switch and the “voice” VLAN should be assigned. The voice VLAN was created on the switch in Section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

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

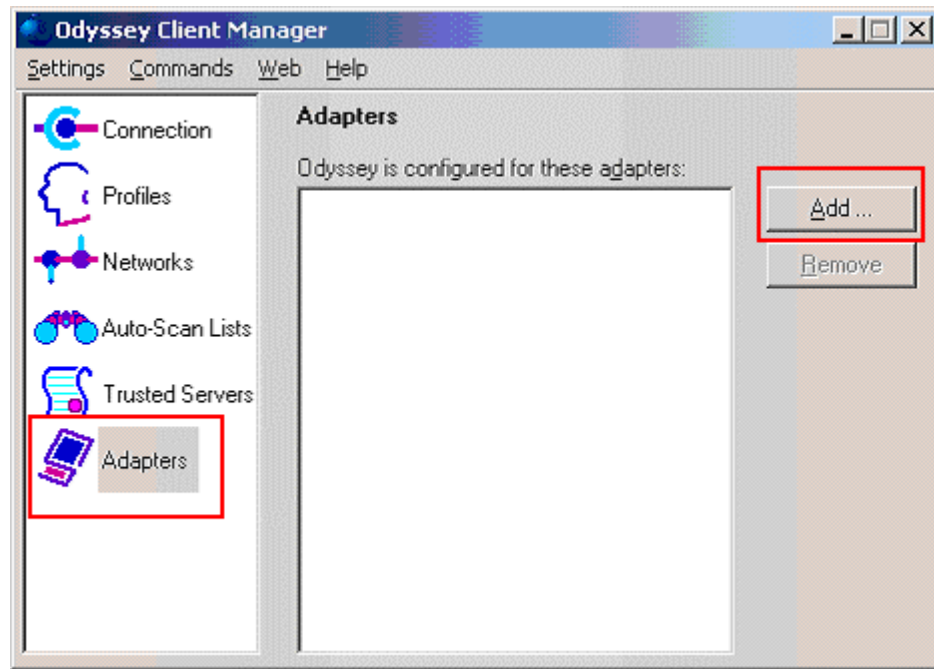
Step	Description
27.	<p>Repeat Steps 4-23 to create a separate policy for a PC. The sample network uses the name User PC authentication policy for this new policy. Use the Udata value in lieu of what is in Step 24. The Udata value indicates to the switch the switch port should be assigned to the data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

6. Configure the Odyssey client

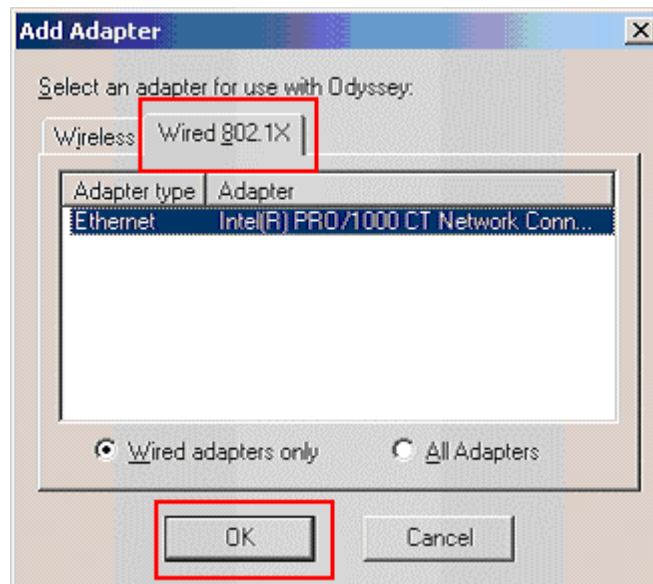
This section shows the steps for configuring the Odyssey Client running on the PC.

Step	Description
1.	<p>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.</p>  <p>The screenshot shows the Odyssey Client Manager application window. The title bar reads "Odyssey Client Manager" and includes standard window controls. Below the title bar is a menu bar with "Settings", "Commands", "Web", and "Help". The main interface is divided into two panes. The left pane contains a vertical list of icons and labels: "Connection", "Profiles", "Networks", "Auto-Scan Lists", "Trusted Servers", and "Adapters". The "Adapters" icon, which depicts a network card, is highlighted with a red rectangular box. The right pane is titled "Adapters" and contains the text "Odyssey is configured for these adapters:" above a large empty white rectangular area. To the right of this area are two buttons: "Add ..." and "Remove". The "Add ..." button is highlighted with a red rectangular box.</p>

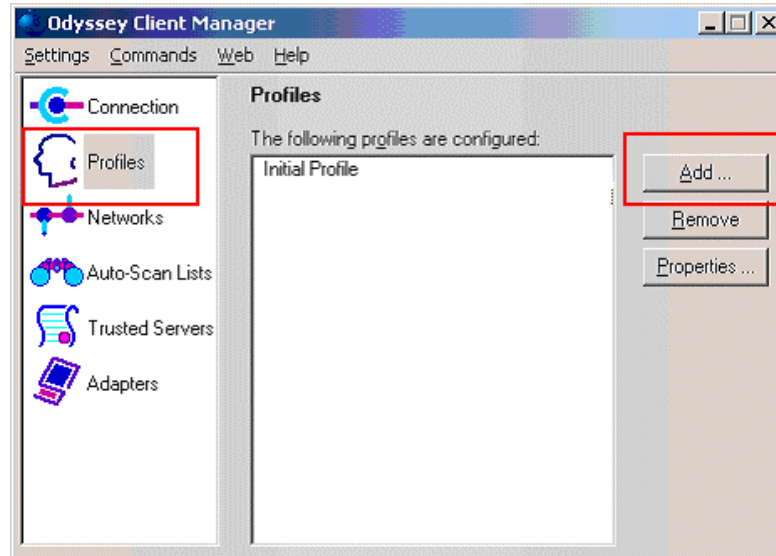
2. Invoke the Odyssey Client Manager by clicking on **Start → Programs → Funk Software → Odyssey Client → Odyssey Client Manager**. Add a network adapter by selecting **Adapters** on the left panel then click **Add** from the Odyssey Client Manager window.



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.

The screenshot shows the 'Profile Properties' dialog box with the 'User Info' tab selected. The 'Profile name' field contains 'x450e-48P testing'. The 'Login name' field contains 'user1@interop.com'. The 'Password' section has four radio button options: 'Permit login using password' (checked), 'Use Windows password', 'Prompt for password', and 'Prompt for login name and password'. Below these is a text field containing '123456' and a checked 'Unmask' checkbox. The 'OK' button is highlighted with a red box.

Profile Properties

Profile name: x450e-48P testing

User Info Authentication ITLS Settings PEAP Settings

Login name: user1@interop.com

Password Certificate Soft Token SIM Card

Permit login using password

Use Windows password

Prompt for password

Prompt for login name and password

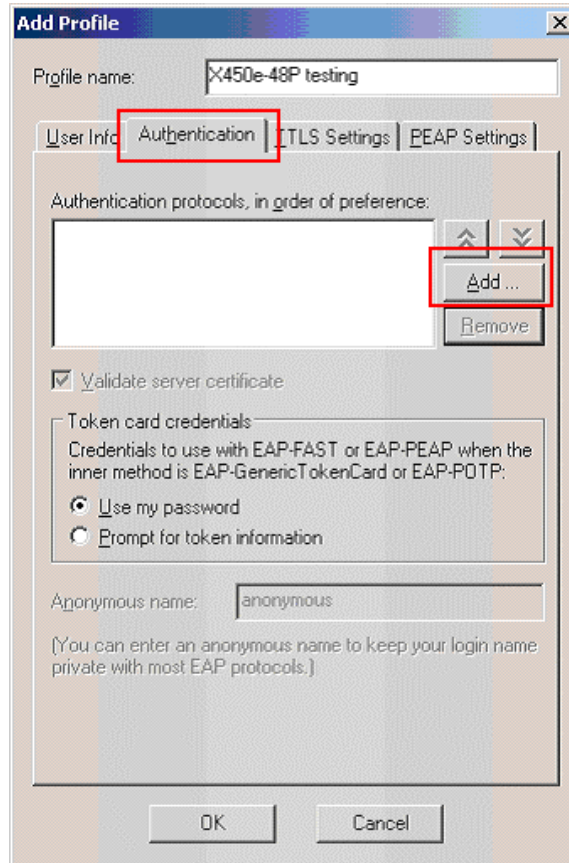
Use the following password:

123456

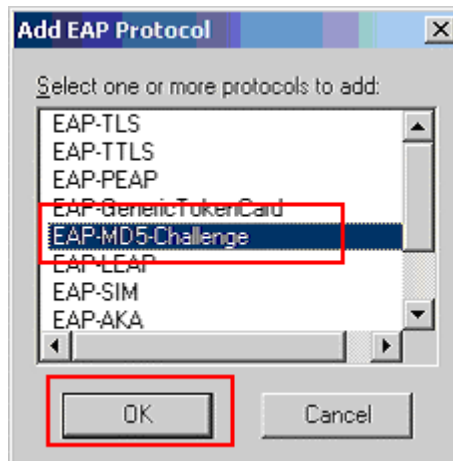
Unmask

OK Cancel

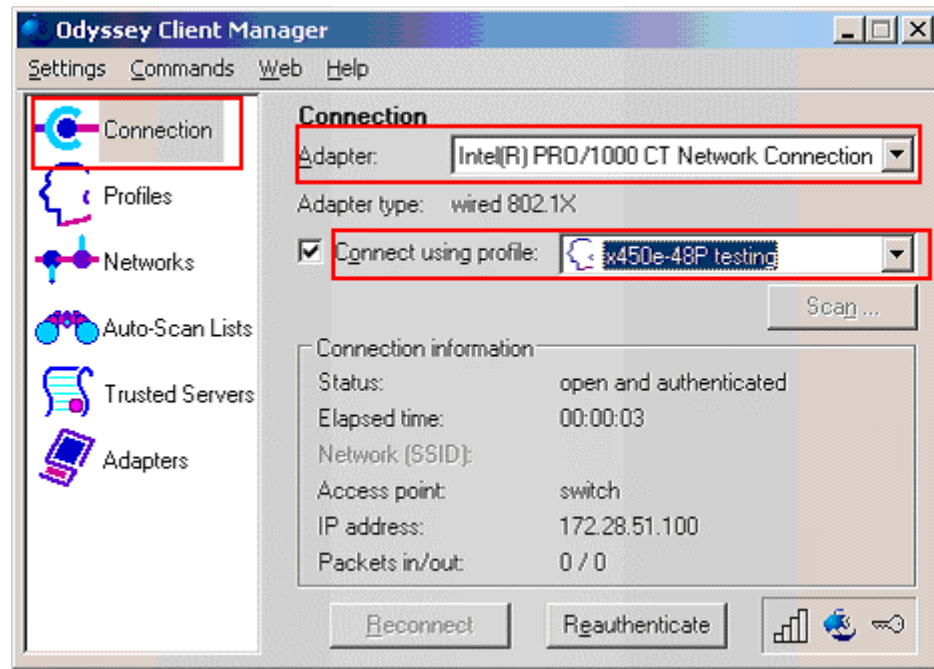
6. Under the **Authentication** tab, click **Add** to add a new authentication protocol.



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 from 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

Step	Description
	<p>The first two pages of the add station 22023 configuration are shown below. Repeat this step for each station.</p> <div data-bbox="302 411 1393 940" style="border: 1px solid black; padding: 5px;"> <pre> 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 </pre> </div> <div data-bbox="302 978 1393 1486" style="border: 1px solid black; padding: 5px;"> <pre> 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 </pre> </div>

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 1
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.	<p>Use the “show upm profiles” command to verify that the upm profiles have been assigned to the correct port.</p> <pre data-bbox="280 688 1409 976">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</pre>

Step	Description
4.	<p>Use the “show netlogin” command to verify that authentication has been enabled and the authentication status of the Avaya IP Telephone and PC.</p> <pre> 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 802.1x 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 </pre>

Step	Description
5.	<p>Use the “show lldp neighbors detail” command to verify the LLDP information for the Avaya IP Telephones.</p> <pre data-bbox="310 338 1382 1423"> 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 </pre>
6.	<p>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.</p> <pre data-bbox="310 1535 1382 1755"> 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 </pre>

Step	Description
7.	<p>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.</p> <pre data-bbox="310 449 1382 1121"> 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 </pre>

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

©2007 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 Developer*Connection* Program at devconnect@avaya.com.