



**Avaya Solution & Interoperability Test Lab**

---

## **Configuring Extreme Networks Summit X250e-48p and X250e-24p Switch to support Avaya Communication Manager – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring the Extreme Networks Summit X250e-48p and X250e-24p switches to support an Avaya VoIP solution consisting of an Avaya Server, an Avaya Media Gateway and Avaya IP Telephones in a network composed of both Extreme Networks, and Avaya Ethernet switches. 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

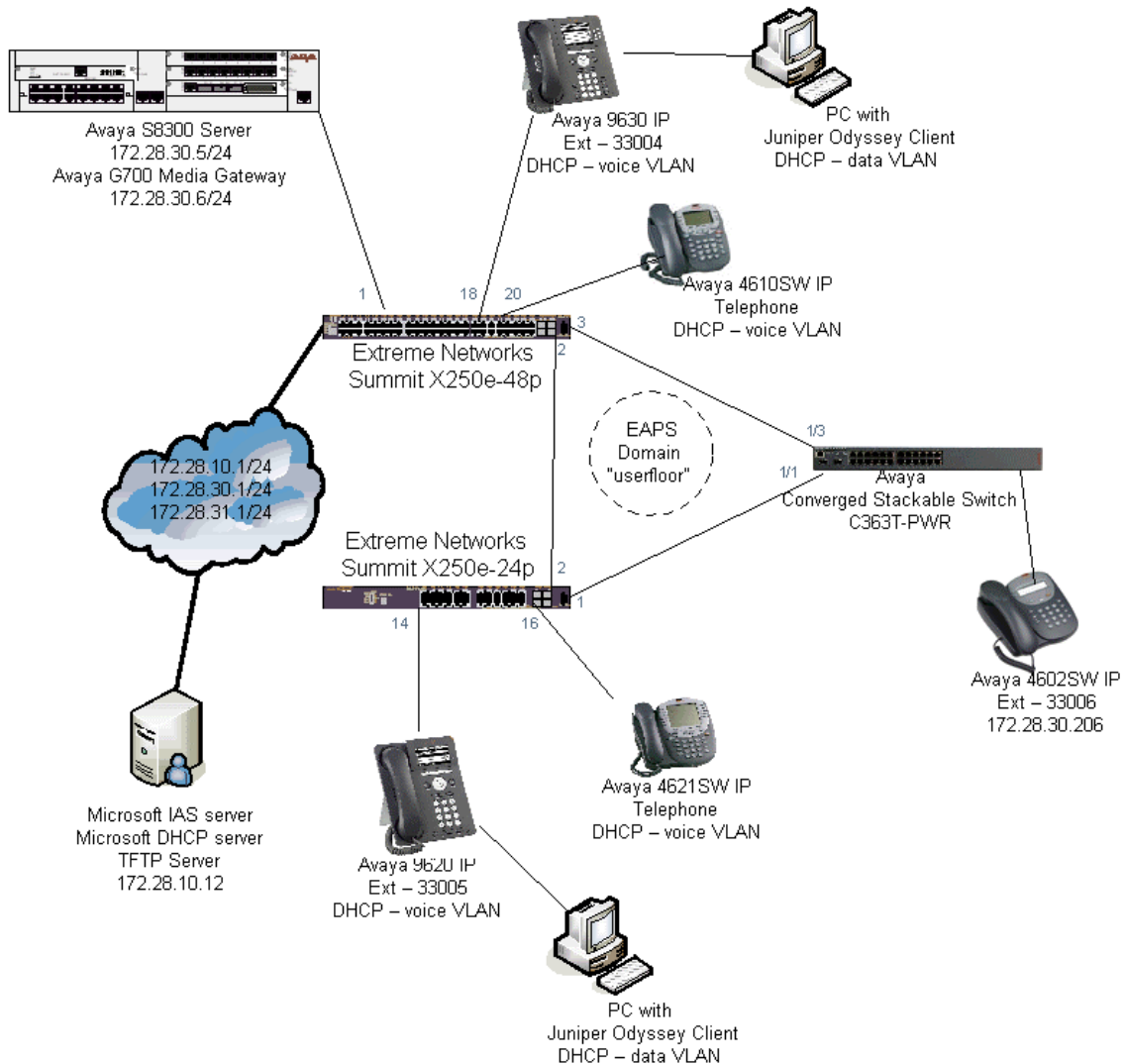
These Application Notes describe a solution for configuring the Extreme Networks Summit X250e-48p and X250e-24p (X250) switches to support an Avaya Voice over IP (VoIP) solution consisting of an Avaya S8300 Server, Avaya G700 Media Gateway, and Avaya IP Telephones in a three-node network composed of Avaya C363T-PWR Converged Stackable Switch, Summit X250e-48p and X250e-24p.

The Avaya C363T-PWR, Extreme X250e-48p, and Extreme X250e-24p switches are connected to each other in a full mesh topology. Ethernet Automatic Protection Switching (EAPS) is configured in the X250e switches as a layer-2 loop avoidance mechanism instead of standard Spanning Tree Protocol (STP). The Avaya C363T-PWR switch will interoperate with EAPS as a Transit node. Avaya S8300 Server and Avaya G700 Media Gateway are directly connected into a switch within the cloud and the Avaya IP Telephones are connected to various switches.

Microsoft Internet Authentication Service (IAS) is used to provide 802.1X RADIUS authentications for Avaya IP Telephones and the PCs running Odyssey Client are connected to the X250s switches. The Avaya IP Telephones and PCs are individually authenticated through the X250 switch by the IAS via the X250's per port multi-suplicant support. LLDP, 802.1x and QoS are configured.

## 2. Configuration

**Figure 1** illustrates the configuration used in these Application Notes. 802.1X authentication is enabled on the X250s only. All IP addresses are obtained via Dynamic Host Configuration Protocol (DHCP) unless noted. The “Resources” VLAN with IP network 172.28.10.0/24, the “voice-G700” VLAN with IP network 172.28.30.0/24, and the “data-G700” VLAN with IP network 172.28.31.0/24 are used in the sample network.



**Figure 1: Sample Network Configuration**

### 3. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8300 Server with G700 Media Gateway	Avaya Communication Manager R4.0 (R014.0.730.5)
Avaya 9630 IP Telephone	R 1.2.1
Avaya 9620 IP Telephone	R 1.2.1
Avaya 4621SW IP Telephone	R 2.8 (H.323)
Avaya 4610SW IP Telephone	R 2.8 (H.323)
Avaya 4602SW IP Telephone	R2.3 (H.323)
Avaya C363T-PWR Converged Stackable Switch	SW Version 4.5.14
Extreme Networks X250e-24p	ExtremeXOS 12.0.1.11
Extreme Networks X250e-48p	ExtremeXOS 12.0.1.11
Microsoft Windows	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
TFTP Server	
Juniper Networks Odyssey Client on PC running Microsoft Windows 2003 Server	4.50.0.2496

### 4. Configure Extreme Networks equipment

This section describes the configuration for Extreme Network X250e-48p and X250e-24p as shown in **Figure 1**. The configuration shows in this section assumes both Extreme Networks switches are in their factory default configuration.

#### 4.1. Configure the X250e-48p

This section shows the necessary steps in configuring the X250e-48p as shown in the **Figure 1**.

Step	Description
1.	Connect to the X250e-48p switch and log in using the appropriate credentials.  login: <b>username</b> password: <b>xxxxxxx</b>

Step	Description
2.	<p>Create VLANs on the switch. The IP address assignment is optional. All routing is performed by another switch within the cloud which serves as the default gateway for the voice-G700 and data-G700 VLAN and has the IP address of 172.28.30.1 and 172.28.31.1 respectively. VLAN “c1” is the control VLAN for EAPS. The “temp” VLAN is used as a temporary VLAN for 802.1X authentication.</p> <p><b>Note:</b> It is important to precede the voice VLAN with the word “voice” as it is a required keyword.</p> <pre>X250e-48p # create vlan voice-G700 X250e-48p # config vlan voice-G700 tag 30 X250e-48p # config vlan voice-G700 ipaddress 172.28.30.2/24 (optional) X250e-48p # create vlan data-G700 X250e-48p # config vlan data-G700 tag 31 X250e-48p # config vlan data-G700 ipaddress 172.28.31.2/24 (optional) X250e-48p # create vlan c1 X250e-48p # config vlan c1 tag 111 X250e-48p # configure vlan c1 qosprofile qp8 X250e-48p # create vlan temp</pre>
3.	<p>Configure VLAN assignment for the ports.</p> <p><b>Note:</b> The VLAN assignment for the user port is dynamically assigned after the Avaya IP Telephone or user has been authenticated.</p> <pre>X250e-48p # config vlan default delete port all X250e-48p # config vlan c1 add port 2,3 tagged X250e-48p # config vlan voice-G700 add port 1,2,3 tagged X250e-48p # config vlan data-G700 add port 1,2,3 tagged</pre>
4.	<p>Configure a default route for the switch.</p> <pre>X250e-48p # configure iproute add default 172.28.31.1 vr vr-default</pre>
5.	<p>Configure EAPS as the layer-2 loop avoidance protocol. The sample network uses “userfloor” as the EAPS domain name.</p> <pre>X250e-48p # create eaps userfloor X250e-48p # configure eaps userfloor mode master X250e-48p # configure eaps userfloor primary port 2 X250e-48p # configure eaps userfloor secondary port 3 X250e-48p # configure eaps userfloor add control vlan c1 X250e-48p # configure eaps userfloor add protected vlan data-G700 X250e-48p # configure eaps userfloor add protected vlan voice-G700 X250e-48p # enable eaps X250e-48p # enable eaps userfloor</pre>

Step	Description
6.	<p>Configure LLDP for the user ports. The call-server and file-server information are used by Avaya IP Telephone for registration and obtaining configuration information.</p> <pre>X250e-48p # <i>configure lldp port 18,20 advertise vendor-specific dot1p vlan-name</i> X250e-48p # <i>configure lldp port 18,20 advertise vendor-specific avaya-extreme call-server 172.28.30.5</i> X250e-48p # <i>configure lldp port 18,20 advertise vendor-specific avaya-extreme file-server 172.28.10.12</i> X250e-48p # <i>configure lldp port 18,20 advertise vendor-specific avaya-extreme dot1q-framing tagged</i> X250e-48p # <i>enable lldp ports 18,20</i></pre>
7.	<p>Configure 802.1X authentication for the switch and user ports. The share-secret must match what is configured in IAS in <b>Section 6.1, Step 3</b>.</p> <pre>X250e-48p # <i>configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.31.2 vr VR-Default</i> X250e-48p # <i>configure radius netlogin primary shared-secret 1234567890</i> X250e-48p # <i>configure netlogin vlan temp</i> X250e-48p # <i>enable radius netlogin</i> X250e-48p # <i>enable netlogin dot1x</i> X250e-48p # <i>enable netlogin ports 18,20 dot1x</i></pre>
8.	<p>Configure QoS profile for Avaya VoIP traffic. The X250 switches only have qp1 and qp8 by default. The dot1p type should match the call control and audio 802.1p priority setting configured in the ip-network-region form in <b>Section 9, Step 2</b>.</p> <pre>X250e-48p # <i>create qosprofile QP7</i> X250e-48p # <i>configure dot1p type 6 qosprofile QP7</i></pre>
9.	<p>Save the configuration</p> <pre>X250e-24p # <i>save</i></pre>

## 4.2. Configure the X250e-24p

This section shows the necessary steps in configuring the X250e-24p as shown in the **Figure 1**.

Step	Description
1.	<p>Connect to the X250e-48p switch and log in using the appropriate credentials.</p> <pre>login: <i>username</i> password: <i>xxxxxxx</i></pre>
2.	<p>Create VLANs on the switch. The IP address assignment is optional. All routing is performed by another switch within the cloud which serves as the default gateway for the voice-G700 and data-G700 VLAN and has the IP address of 172.28.30.1 and 172.28.31.1 respectively. VLAN “c1” is the control VLAN for EAPS. The “temp” VLAN is used as a temporary VLAN for 802.1X authentication.</p> <p><b>Note:</b> It is important to precede the voice VLAN with the word “voice” as it is a required keyword.</p> <pre>X250e-24p # <i>create vlan voice-G700</i> X250e-24p # <i>config vlan voice-G700 tag 30</i> X250e-24p # <i>config vlan voice-G700 ipaddress 172.28.30.3/24 (optional)</i> X250e-24p # <i>create vlan data-G700</i> X250e-24p # <i>config vlan data-G700 tag 31</i> X250e-24p # <i>config vlan data-G700 ipaddress 172.28.31.3/24 (optional)</i> X250e-24p # <i>create vlan c1</i> X250e-24p # <i>config vlan c1 tag 111</i> X250e-24p # <i>configure vlan c1 qosprofile qp8</i> X250e-24p # <i>create vlan temp</i></pre>
3.	<p>Configure VLAN assignment for the ports.</p> <p><b>Note:</b> The VLAN assignment for the user port is dynamically assigned after the Avaya IP Telephone or user has been authenticated.</p> <pre>X250e-24p # <i>config vlan default delete port all</i> X250e-24p # <i>config vlan c1 add port 1,2 tagged</i> X250e-24p # <i>config vlan voice-G700 add port 1,2 tagged</i> X250e-24p # <i>config vlan data-G700 add port 1,2 tagged</i></pre>
4.	<p>Configure a default route for the switch.</p> <pre>X250e-24p # <i>configure iproute add default 172.28.31.1 vr vr-default</i></pre>

Step	Description
5.	<p>Configure EAPS as the layer-2 loop avoidance protocol. The sample network uses “userfloor” as the EAPS domain name.</p> <pre>X250e-24p # create eaps userfloor X250e-24p # configure eaps userfloor mode transit X250e-24p # configure eaps userfloor primary port 2 X250e-24p # configure eaps userfloor secondary port 1 X250e-24p # configure eaps userfloor add control vlan c1 X250e-24p # configure eaps userfloor add protected vlan data-G700 X250e-24p # configure eaps userfloor add protected vlan voice-G700 X250e-24p # enable eaps X250e-24p # enable eaps userfloor</pre>
6.	<p>Configure LLDP for the user ports. The call-server and file-server information are used by Avaya IP Telephone for registration and obtaining configuration information.</p> <pre>X250e-24p # configure lldp port 14,16 advertise vendor-specific dot1p vlan-name X250e-24p # configure lldp port 14,16 advertise vendor-specific avaya-extreme call-server 172.28.30.5 X250e-24p # configure lldp port 14,16 advertise vendor-specific avaya-extreme file-server 172.28.10.12 X250e-24p # configure lldp port 14,16 advertise vendor-specific avaya-extreme dot1q-framing tagged X250e-24p # enable lldp ports 14,16</pre>
7.	<p>Configure 802.1X authentication for the switch and user ports. The share-secret must match what is configured in IAS in <b>Section 6.1, Step 3</b>.</p> <pre>X250e-24p # configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.31.3 vr VR-Default X250e-24p # configure radius netlogin primary shared-secret 1234567890 X250e-24p # configure netlogin vlan temp X250e-24p # enable radius netlogin X250e-24p # enable netlogin dot1x X250e-24p # enable netlogin ports 18,20 dot1x</pre>
8.	<p>Configure QoS profile for Avaya VoIP traffic. The X250 switches only have qp1 and qp8 by default. The dot1p type should match the call control and audio 802.1p priority setting configured in the ip-network-region form in <b>Section 9, Step 2</b>.</p> <pre>X250e-24p # create qosprofile QP7 X250e-24p # configure dot1p type 6 qosprofile QP7</pre>
9.	<p>Save the configuration</p> <pre>X250e-24p # save</pre>



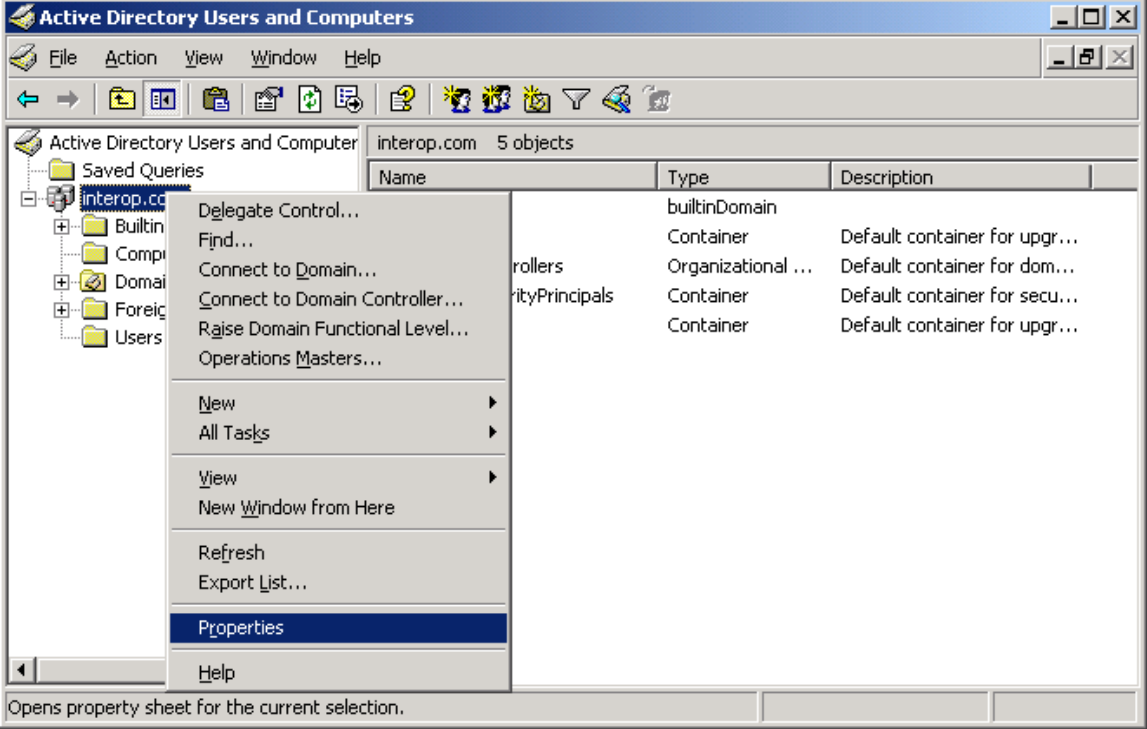
## 5. Configure the Avaya C363T-PWR Converged Stackable Switch

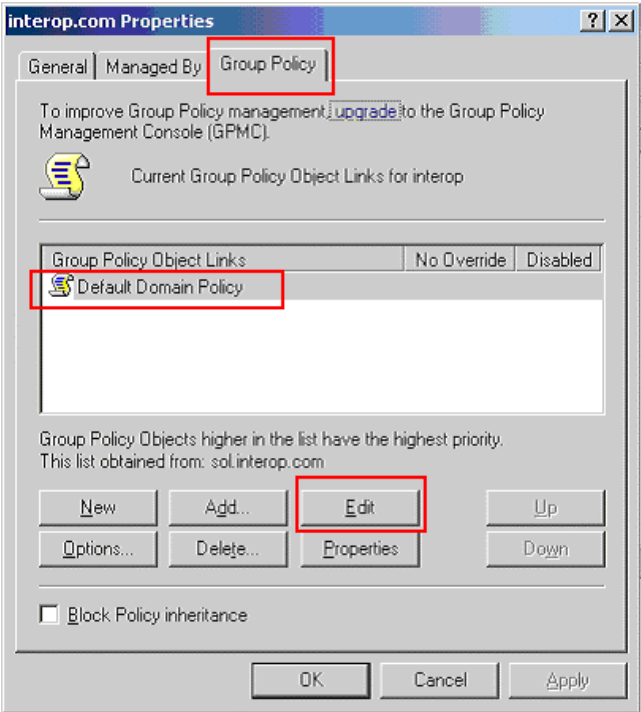
This section shows the steps for configuring the Avaya C363T-PWR Converged Stackable Switch.

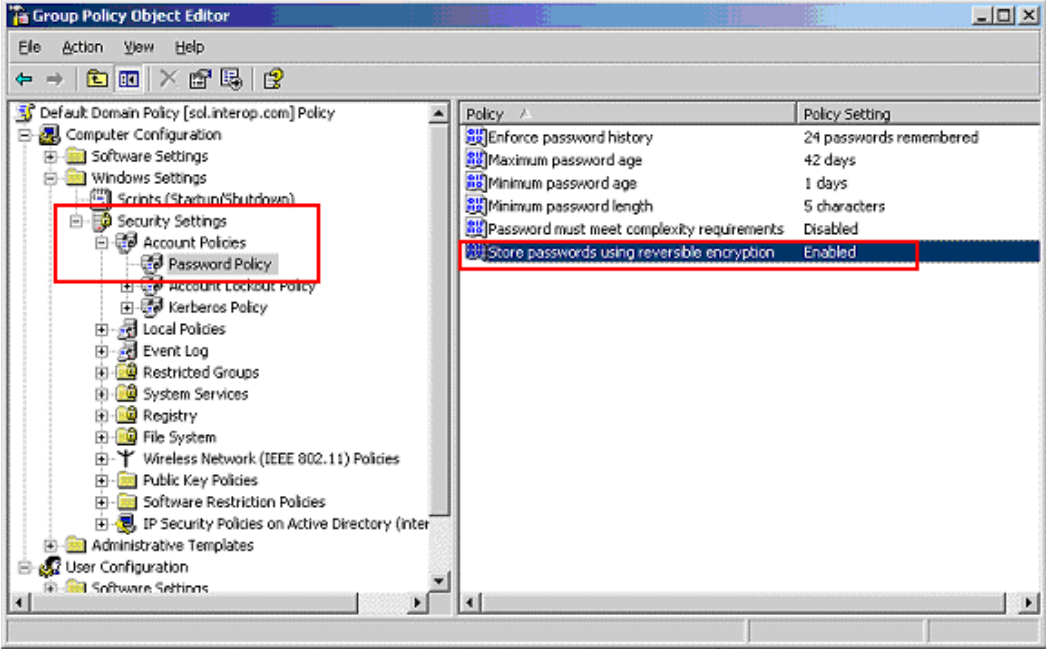
<b>1.</b>	Log in to the Avaya C363T-PWR Converged Stackable Switch using the appropriate credentials.  Login: <i>username</i> Password: <i>xxxxxx</i>
<b>2.</b>	Create the VLANs on the switch.  <b>Note:</b> VLAN c1 must be created in order for the EAPS ring to function successfully.  C360-1(super)# <i>set vlan 30 name voice-G700</i> C360-1(super)# <i>set vlan 31 name data-G700</i> C360-1(super)# <i>set vlan 111 name c1</i>
<b>3.</b>	Configure VLAN assignment for the ports.  C360-1(super)# <i>set port vlan 31 1/10</i> C360-1(super)# <i>set trunk 1/1,1/3,1/10 dot1q</i> C360-1(super)# <i>set port vlan-binding-mode 1/1,1/3,1/10 bind-to-configured</i>

## 6. Configure 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.

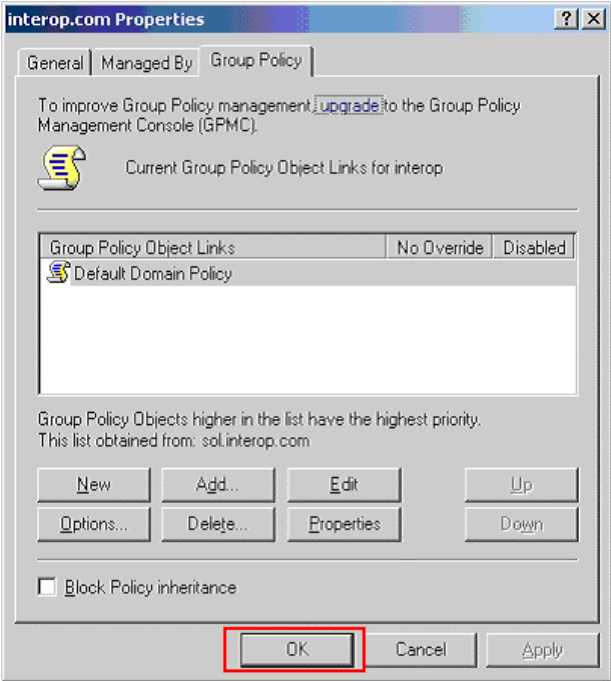
Step	Description																		
1.	<p>Invoke the Active Directory Users and Computers window under Administrative Tools of a Microsoft Windows system. Configure the active directory domain properties by highlighting the Active Directory domain then right click and select <b>Properties</b>.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' console window. The left pane shows a tree view with 'interop.com' selected. The right pane shows a table of objects in the domain:</p> <table border="1" data-bbox="714 724 1477 913"> <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>rollers</td> <td>Container</td> <td>Default container for upgr...</td> </tr> <tr> <td>SecurityPrincipals</td> <td>Organizational ...</td> <td>Default container for dom...</td> </tr> <tr> <td></td> <td>Container</td> <td>Default container for secu...</td> </tr> <tr> <td></td> <td>Container</td> <td>Default container for upgr...</td> </tr> </tbody> </table> <p>The 'Properties' option is highlighted in the context menu. The status bar at the bottom reads: 'Opens property sheet for the current selection.'</p>	Name	Type	Description	builtinDomain	builtinDomain		rollers	Container	Default container for upgr...	SecurityPrincipals	Organizational ...	Default container for dom...		Container	Default container for secu...		Container	Default container for upgr...
Name	Type	Description																	
builtinDomain	builtinDomain																		
rollers	Container	Default container for upgr...																	
SecurityPrincipals	Organizational ...	Default container for dom...																	
	Container	Default container for secu...																	
	Container	Default container for upgr...																	

Step	Description
2.	<p>Select the <b>Group Policy</b> tab in the properties window. Highlight the <b>Default Domain Policy</b> then click <b>Edit</b> 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 'Group Policy Object Links' list contains one entry, 'Default Domain Policy', which is highlighted. The 'Edit' button is also highlighted. The 'Block Policy inheritance' checkbox is unchecked. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.</p>

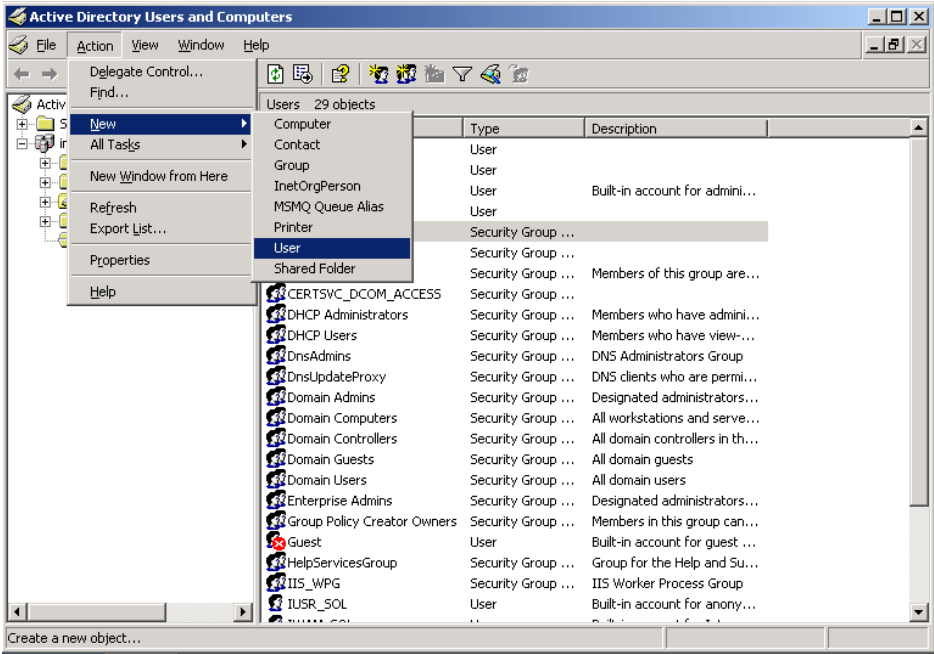
Step	Description														
3.	<p>From the Group Policy Object Editor, navigate to <b>Computer Configuration</b> → <b>Windows Settings</b> → <b>Security Settings</b> → <b>Account Policies</b> → <b>Password Policy</b> on the left panel. Double click on <b>Store passwords using reversible encryption policy</b> on the right, and change the setting to <b>Enabled</b>.</p>  <p>The screenshot shows the Group Policy Object Editor window. The left pane displays a tree view of policy categories. A red box highlights the path: Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Account Policies &gt; Password Policy. The right pane shows a list of password-related policies. A red box highlights the 'Store passwords using reversible encryption' policy, which is currently set to 'Enabled'.</p> <table border="1" data-bbox="857 520 1442 682"> <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														

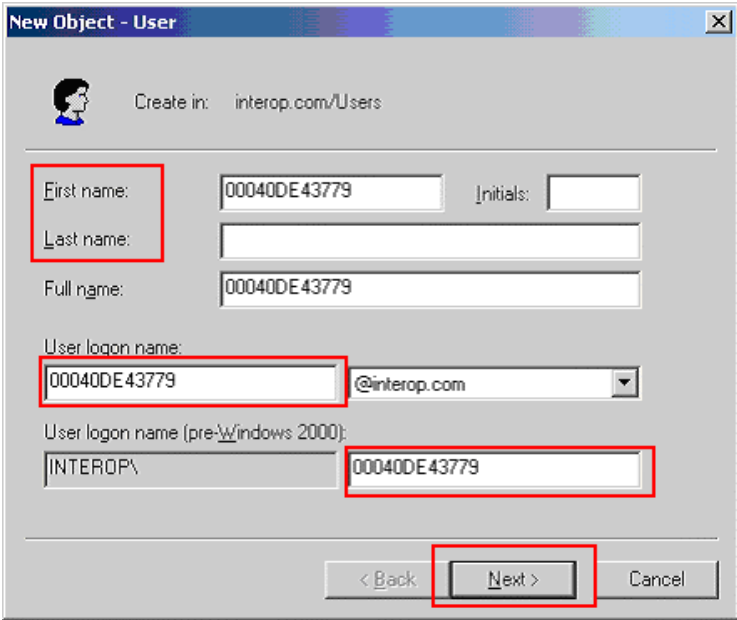
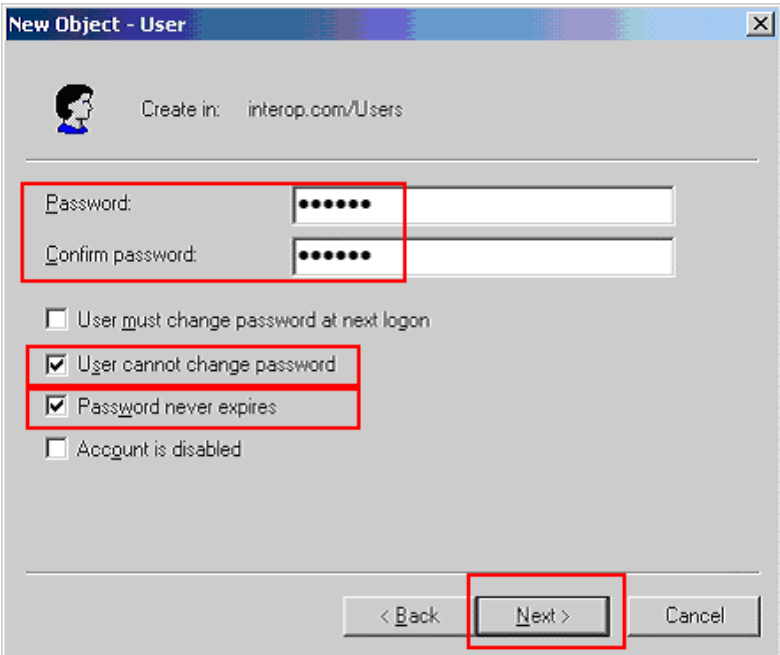
Step	Description
------	-------------

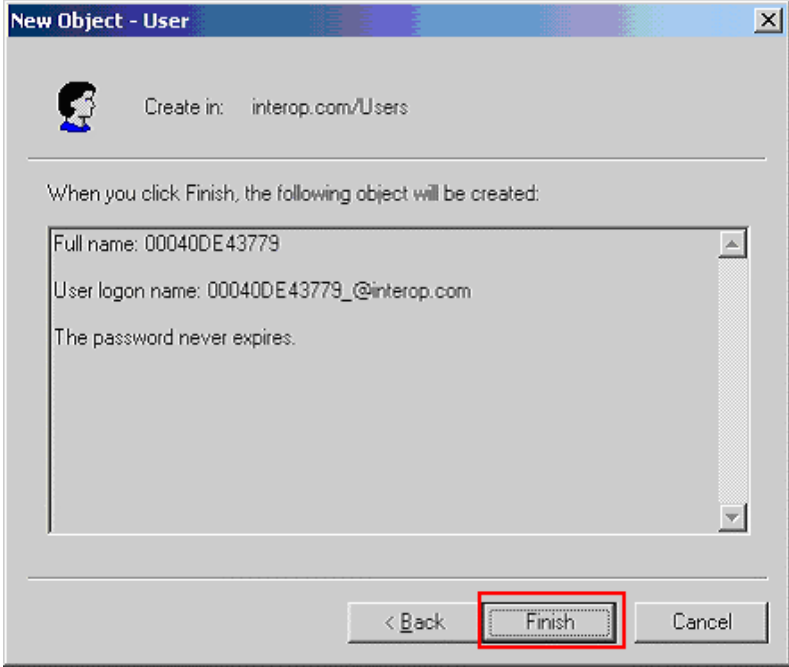
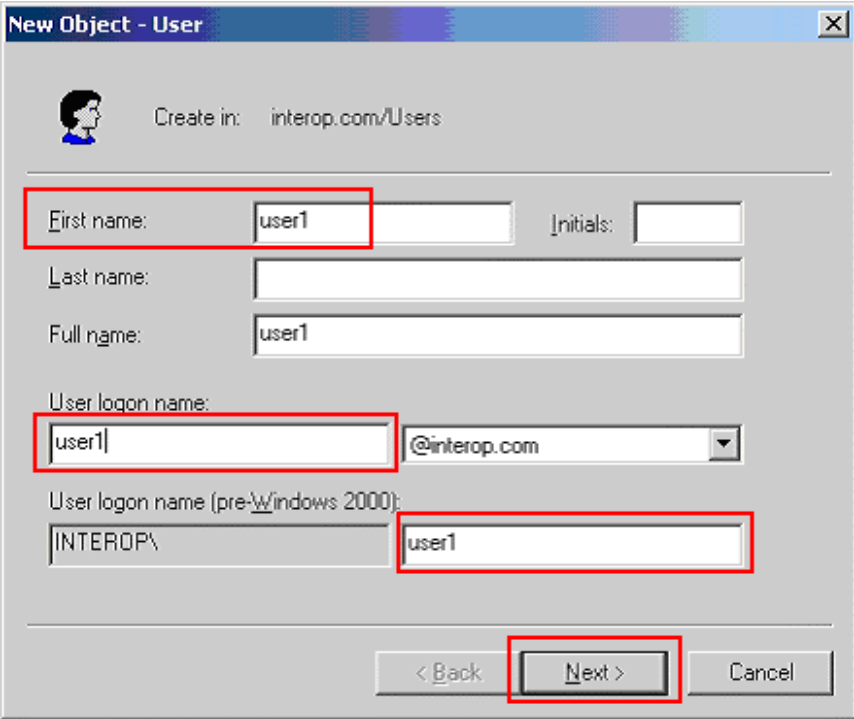
4. Click **OK** on the domain properties pop-up window to complete.

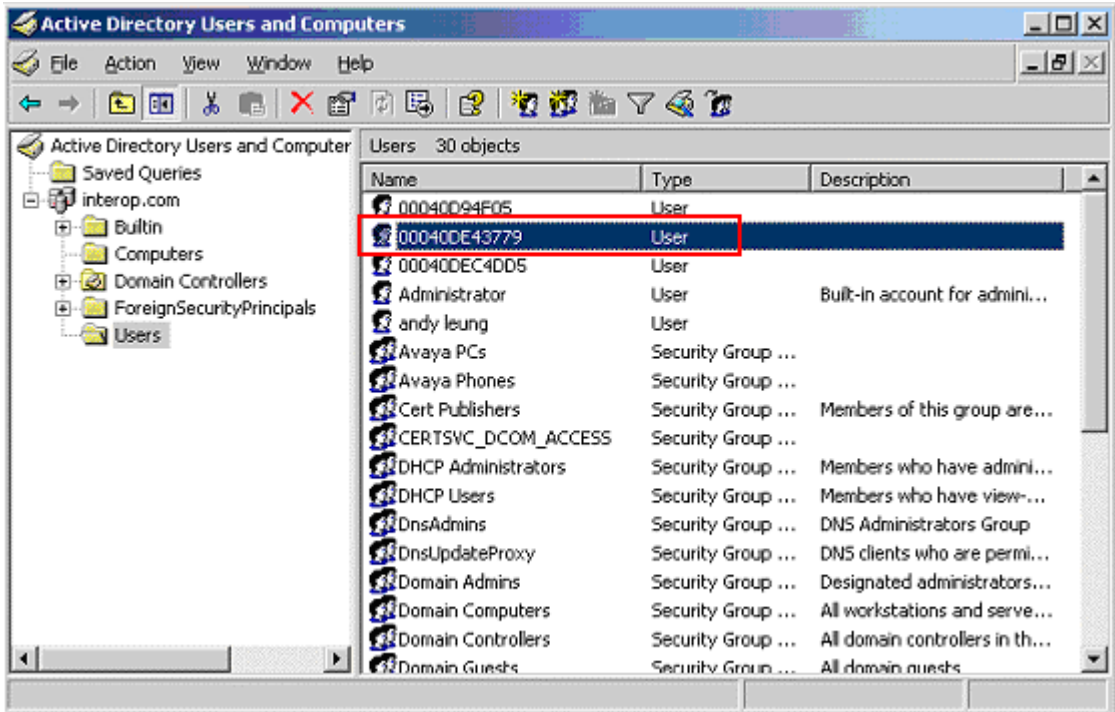


5. Create a new user ID for an Avaya IP Telephone user and a PC user. From the Active Directory Users and Computers window menu, select **Action** → **New** → **User** to begin creating a new user ID.

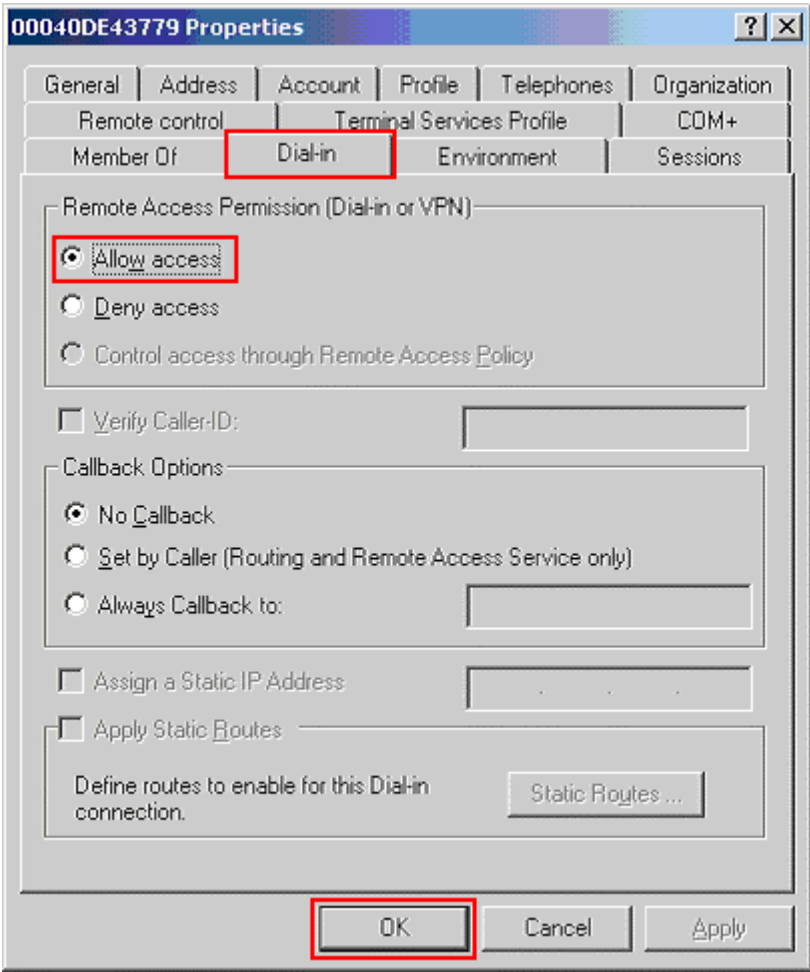


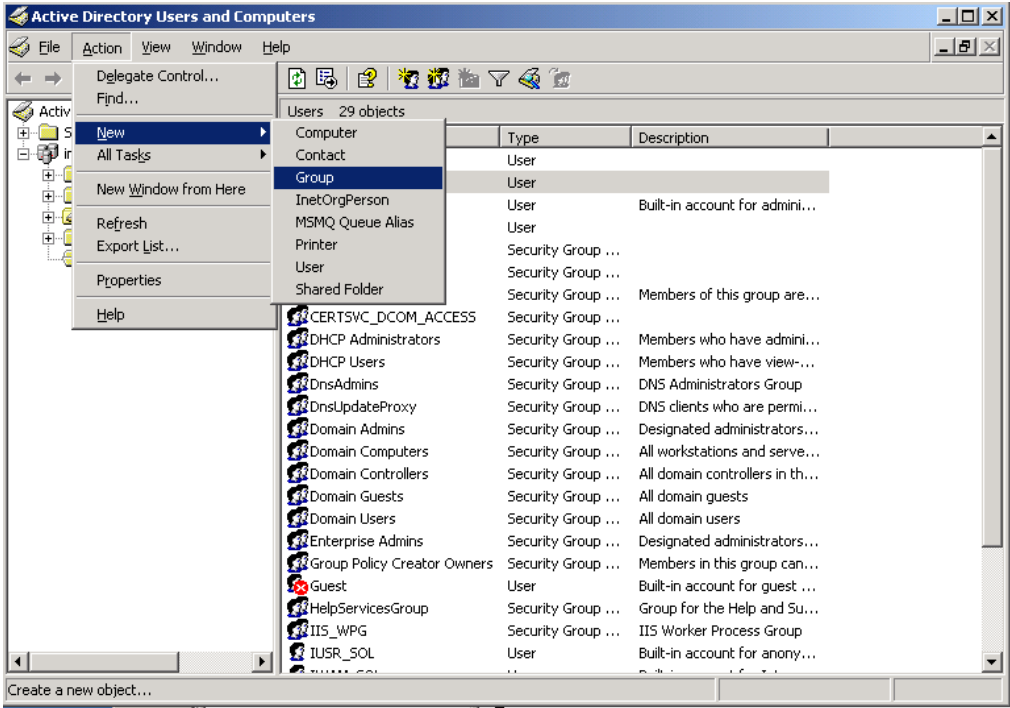
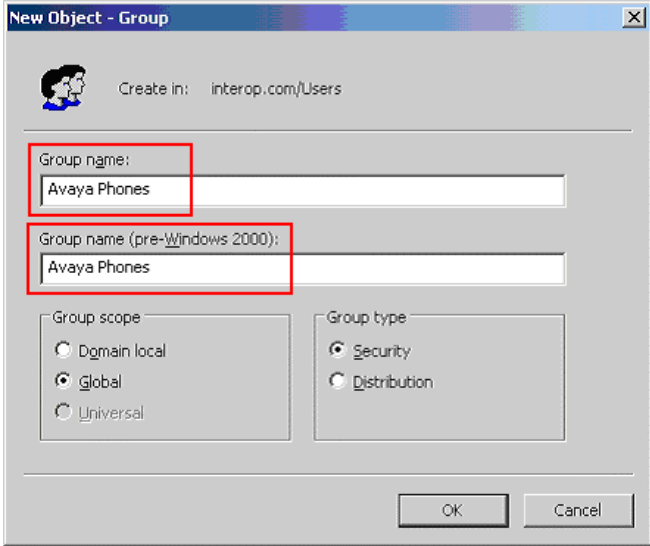
Step	Description
6.	<p>For an Avaya IP Telephone, enter the phone's MAC address as the <b>User logon name</b>. The <b>First name</b> and <b>Last name</b> are for information only. Click <b>Next</b> to continue.</p> 
7.	<p>Enter a <b>Password</b> for the user ID. For an Avaya IP Telephone, enter a numeric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

Step	Description
8.	<p>Click <b>Finish</b> to complete.</p>  <p>The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: interop.com/Users'. Below that, it states 'When you click Finish, the following object will be created:'. A scrollable area contains the following text: 'Full name: 00040DE43779', 'User logon name: 00040DE43779_@interop.com', and 'The password never expires.'. At the bottom, there are three buttons: '&lt; Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red rectangular box.</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 the 'New Object - User' dialog box with input fields. The 'Create in:' field is 'interop.com/Users'. The 'First name:' field contains 'user1' and is highlighted with a red box. The 'Initials:' field is empty. The 'Last name:' field is empty. The 'Full name:' field contains 'user1'. The 'User logon name:' field contains 'user1' and is highlighted with a red box. The domain dropdown menu is set to '@interop.com'. The 'User logon name (pre-Windows 2000):' field contains 'INTEROP\' and the 'user1' field is highlighted with a red box. At the bottom, there are three buttons: '&lt; Back', 'Next &gt;', and 'Cancel'. The 'Next &gt;' button is highlighted with a red rectangular box.</p>

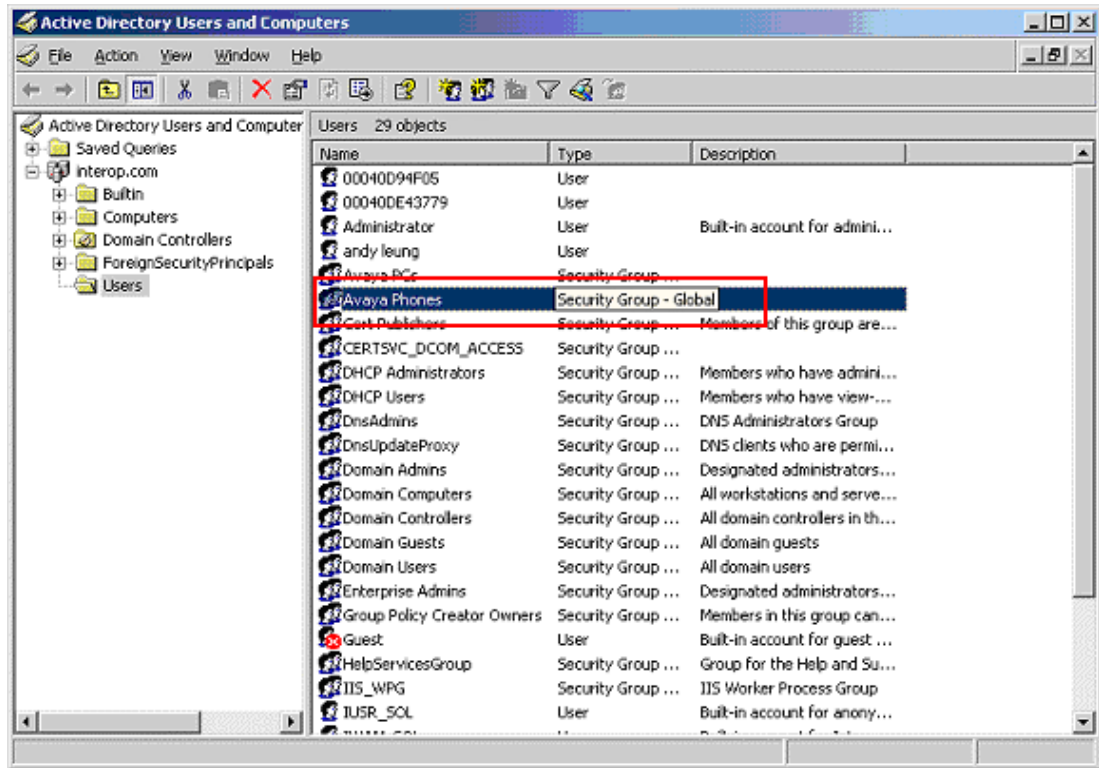
Step	Description																																																						
10.	After creating the user ID, begin editing its properties by double clicking on the user ID in the Active Directory Users and Computers window.																																																						
 <p>The screenshot shows the 'Active Directory Users and Computers' console tree on the left, with the 'Users' folder expanded. The main pane displays a list of 30 objects. The user '00040DE43779' is selected and highlighted with a red rectangular box. The list includes various users and security groups.</p> <table border="1" data-bbox="722 499 1469 1018"> <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></td> </tr> <tr> <td>Administrator</td> <td>User</td> <td>Built-in account for admini...</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		Administrator	User	Built-in account for admini...	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																																																						
Administrator	User	Built-in account for admini...																																																					
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																																																					



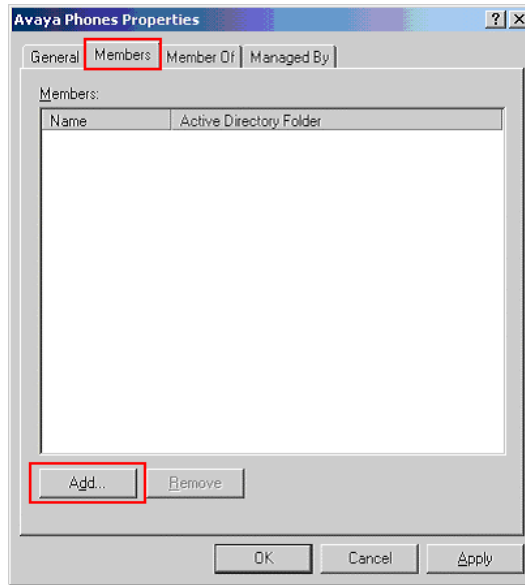
Step	Description
11.	<p>Select the <b>Dial-in</b> tab in the user properties window. Enable remote access by clicking on the <b>Allow access</b> radio button. Click <b>OK</b> to complete. Repeat this step for all Avaya IP Telephone and PC user IDs.</p> 

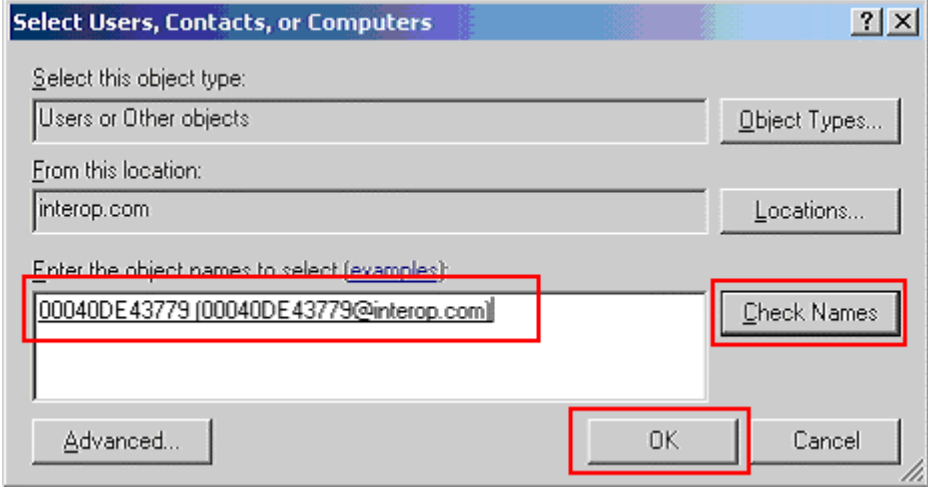
Step	Description
<p><b>12.</b></p>	<p>Create a new user Group by selecting <b>Action</b> → <b>New</b> → <b>Group</b> from the drop-down menu. The use of a Group facilitates the assignment and management of additional user IDs.</p>  <p>The screenshot shows the 'Active Directory Users and Computers' window. 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 existing users and groups, including 'User', 'Security Group ...', and 'Built-in account for admini...'. The 'Group' option in the sub-menu is highlighted in blue.</p>
<p><b>13.</b></p>	<p>Create a group for Avaya IP Telephones. The sample network uses the name Avaya Phones for this group. Click <b>OK</b> to complete.</p>  <p>The screenshot shows the 'New Object - Group' dialog box. The 'Create in:' field is set to 'interop.com/Users'. The 'Group name:' field and the 'Group name (pre-Windows 2000):' field both contain the text 'Avaya Phones'. The 'Group scope' section has 'Global' selected, and the 'Group type' section has 'Security' selected. The 'OK' and 'Cancel' buttons are visible at the bottom.</p>
<p><b>14.</b></p>	<p>Repeat Steps 12 and 13 to create another user Group for the PC.</p>

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



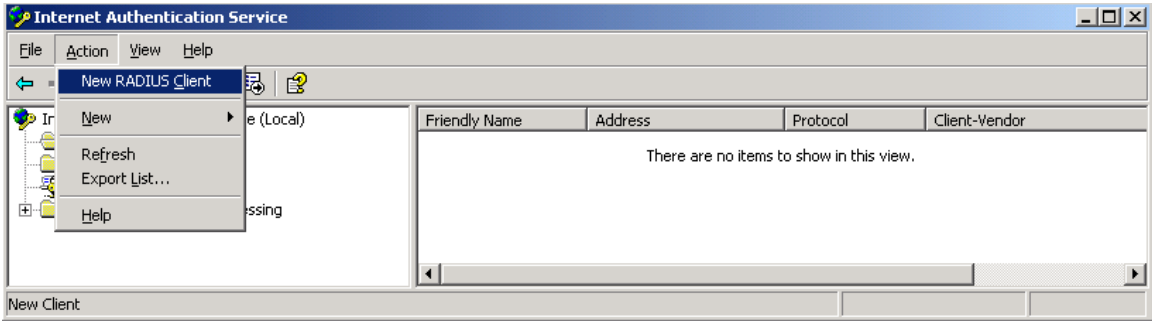
16.	Select the <b>Members</b> tab in the group Properties window. Click <b>Add</b> to continue.
-----	---

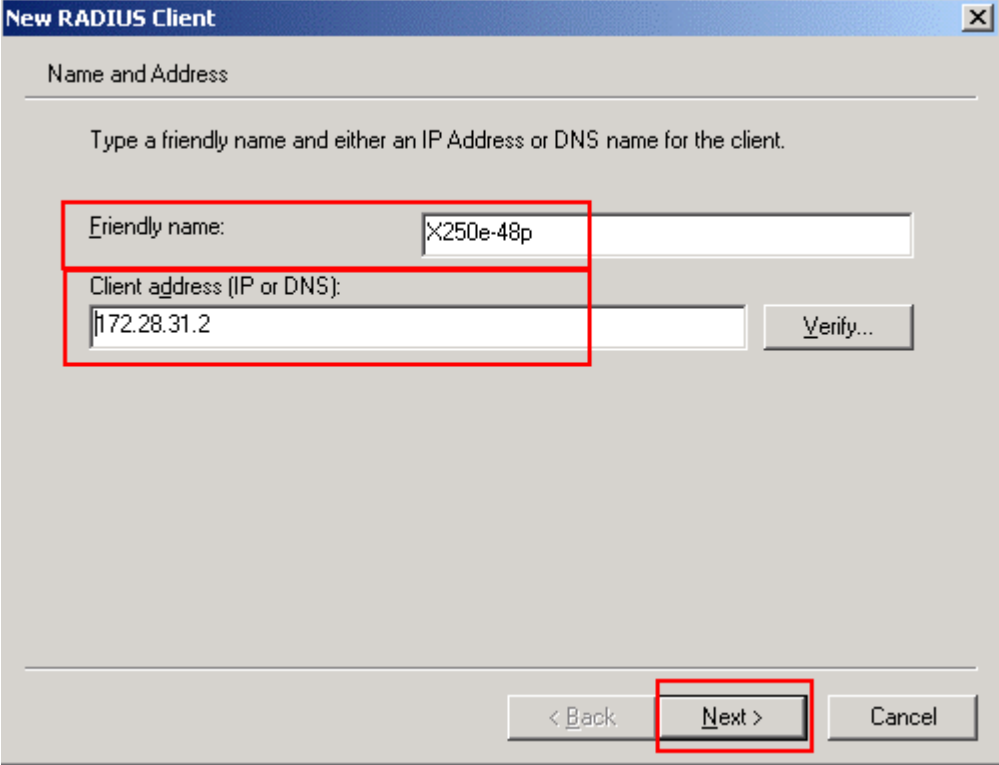


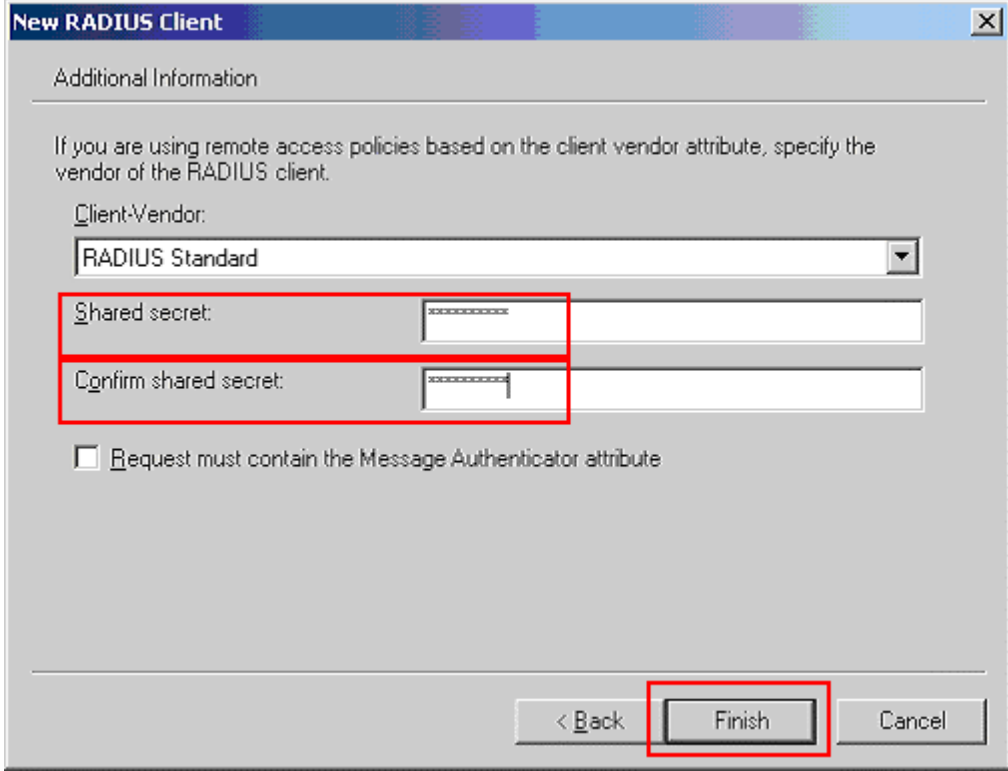
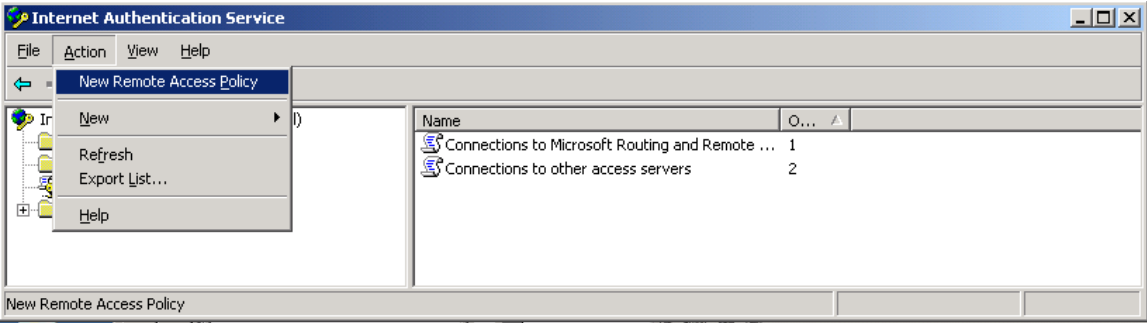
Step	Description
17.	<p>Enter the user ID that should be assigned to the Avaya Phones group. This should be the user ID for the Avaya IP Telephone. Use <b>Check Names</b> to assist in searching for the user ID. Click <b>OK</b> to complete.</p> 
18.	Repeat Steps 15-17 to add members to the PCs user group.

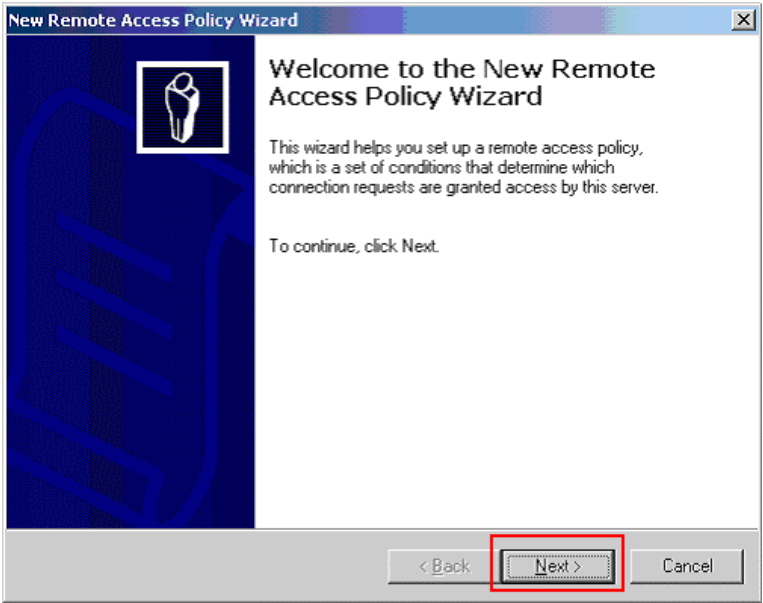
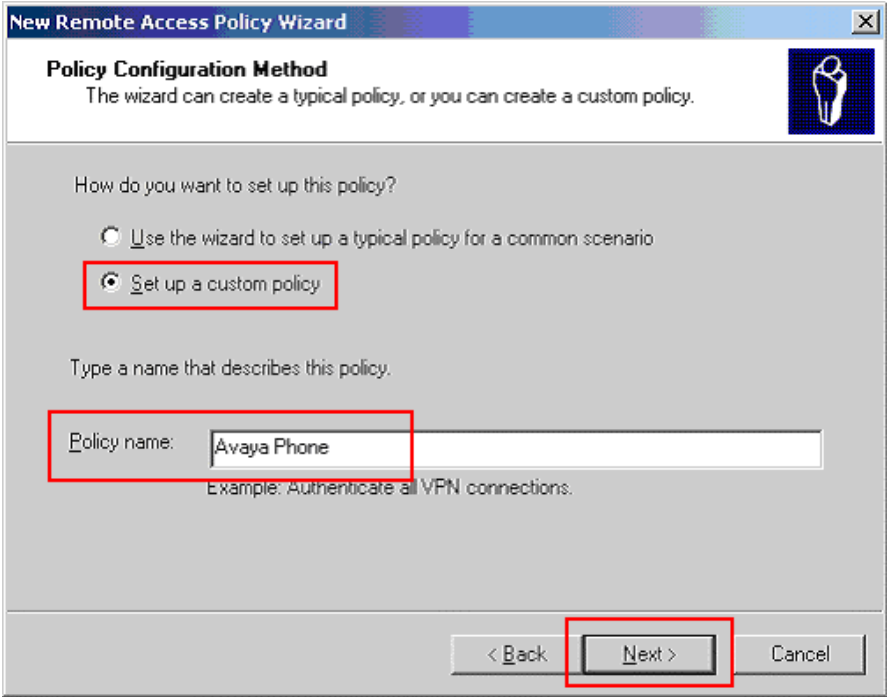
## 6.1. Configure Microsoft Internet Authentication Services (IAS) Server

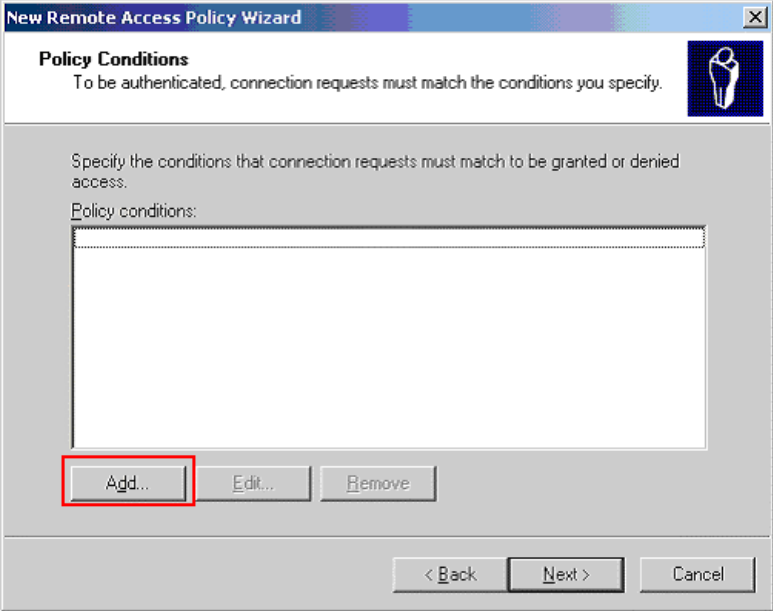
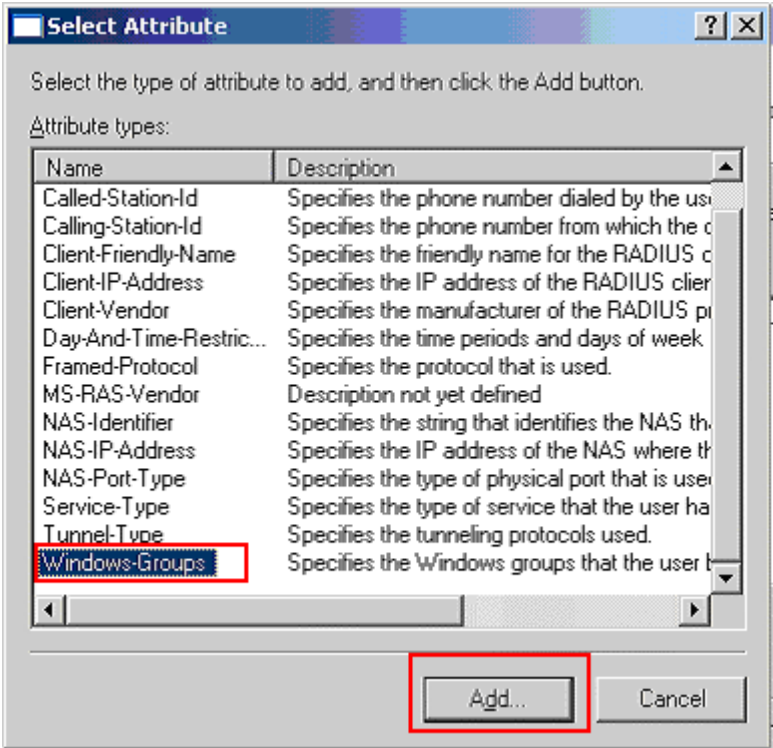
This section shows the steps for configuring the IAS server to support 802.1X authentication for an Avaya IP Telephone and a PC.

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 <b>Action</b> → <b>New RADIUS Client</b> from the drop down menu in Internet Authentication Service window.</p> 


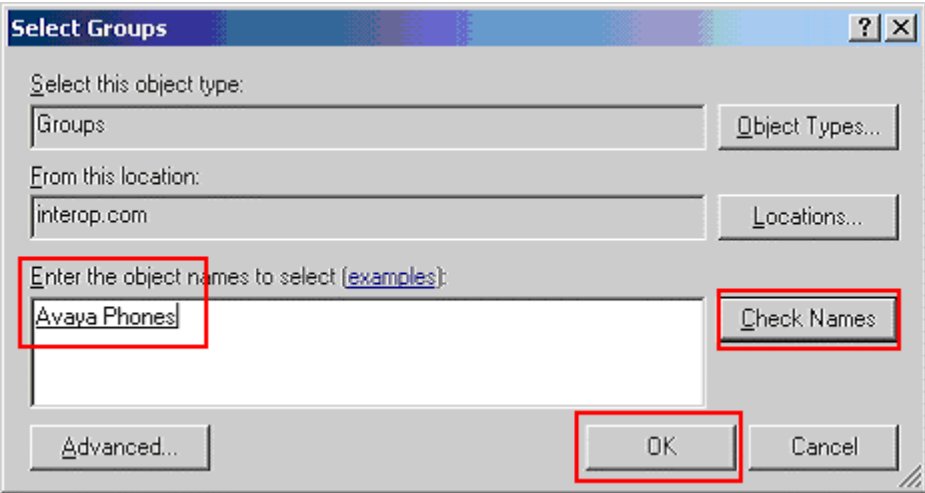
Step	Description
2.	<p>Enter the name and IP address of the X250e-48p switch to create a new RADIUS client. This must match the IP address configured in <b>Section 4.1, Step 4</b>. Click <b>Next</b> to continue.</p> 

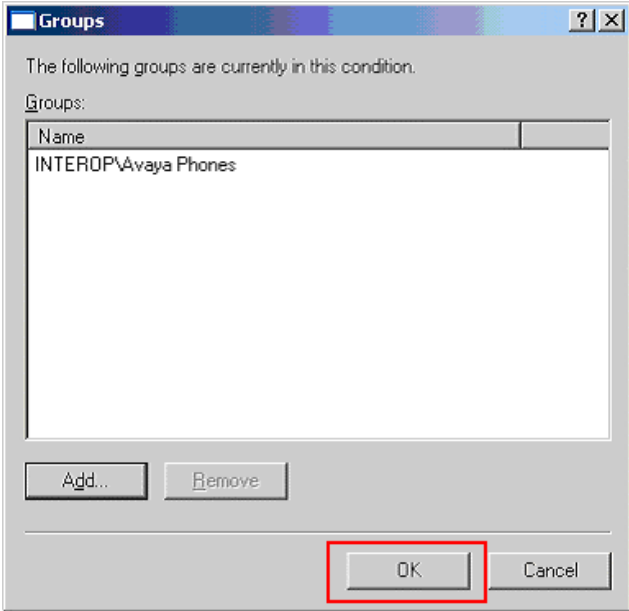
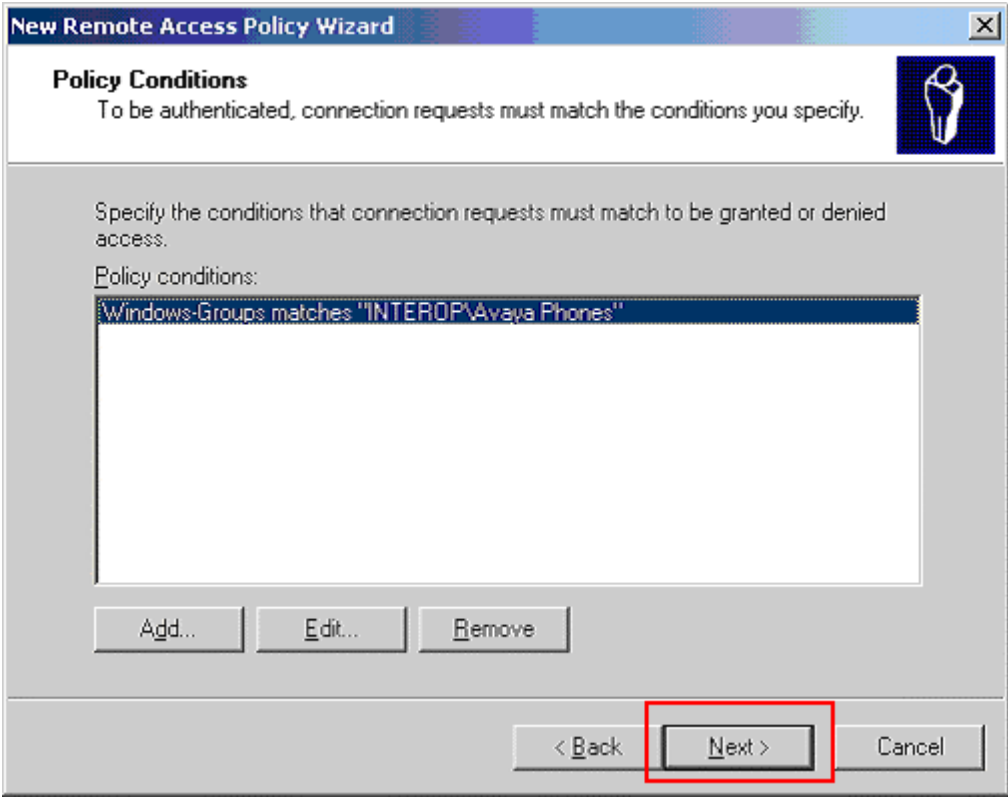
Step	Description
3.	<p>Enter the Shared secret that will be used for this client. This shared secret must match the information configured in the switch in <b>Section 4.1</b> and <b>Section 4.2, Step 7</b>. Click <b>Finish</b> to complete.</p> 
4.	<p>Create a new access policy for the Avaya IP Telephones by clicking on <b>Action → New Remote Access Policy</b>.</p> 

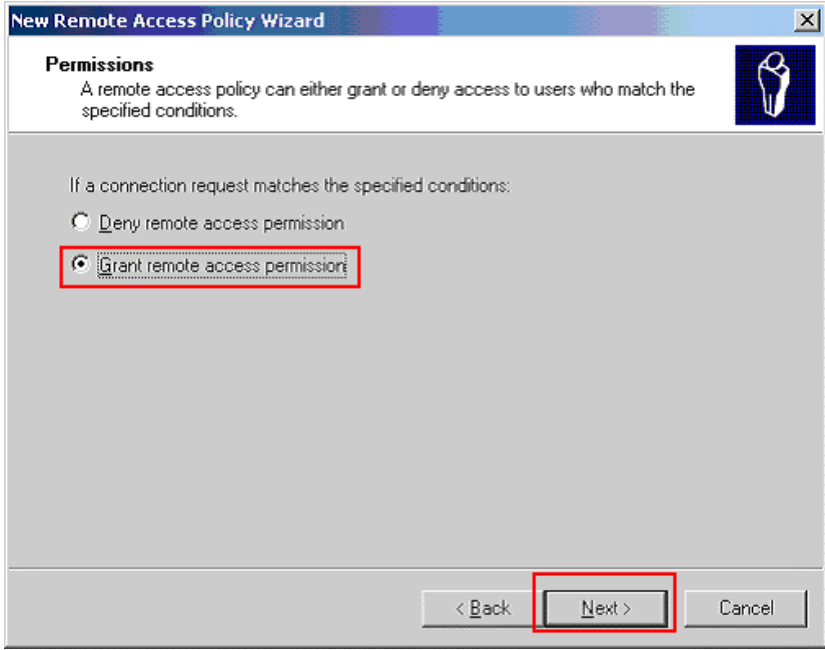
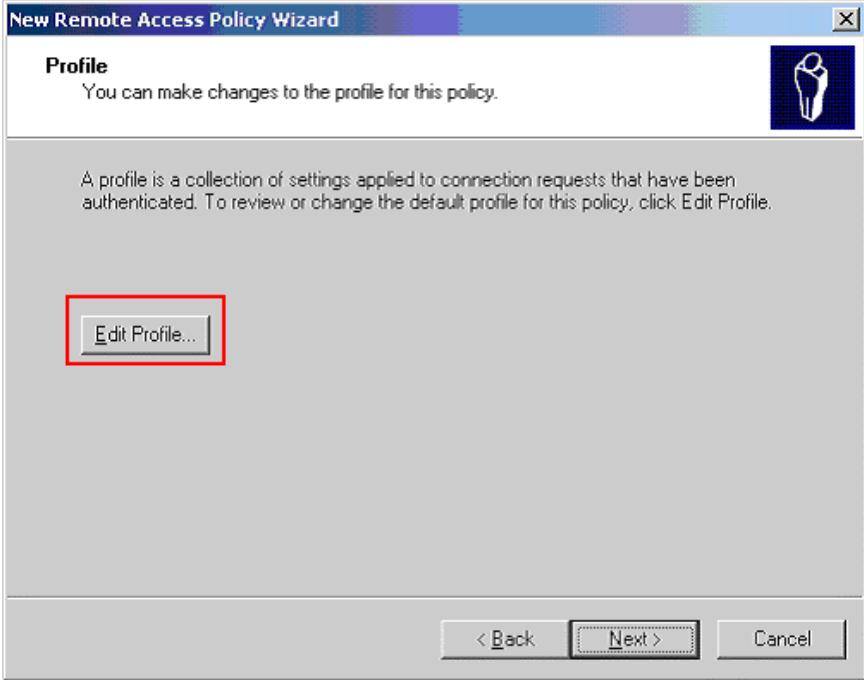
Step	Description
5.	<p>Click <b>Next</b> in the <b>New Remote Access Policy Wizard</b>.</p> 
6.	<p>Select <b>Set up a custom policy</b> radio button and enter a <b>Policy name</b>. The sample network uses the name Avaya Phone. Click <b>Next</b> to continue.</p> 

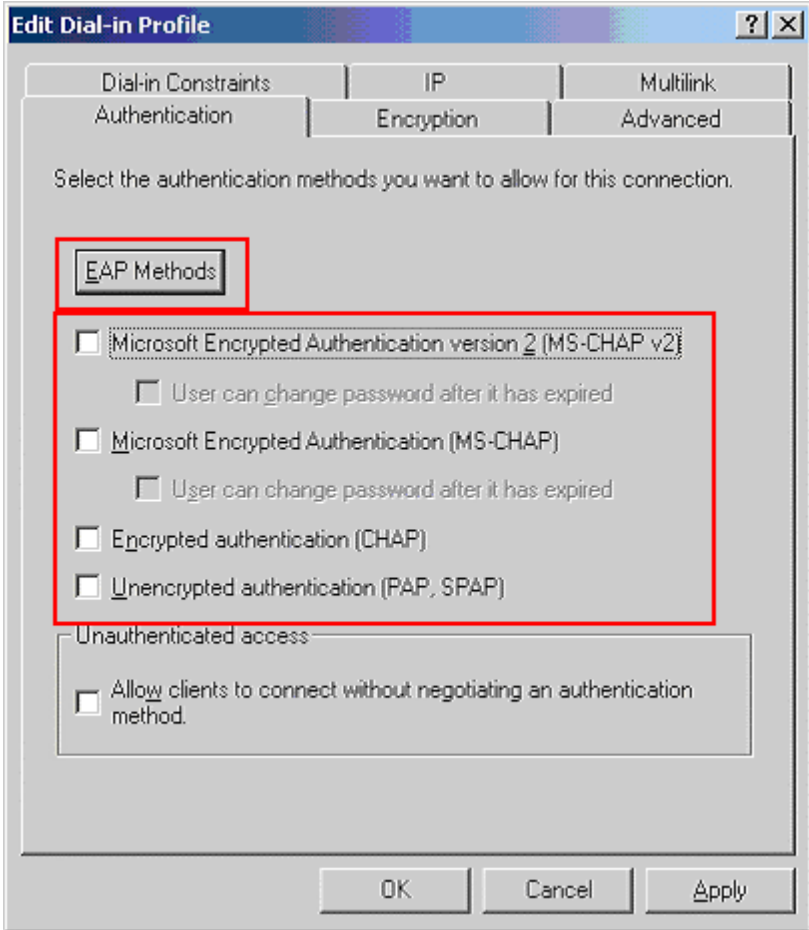
Step	Description																														
7.	<p>Click the <b>Add</b> button to add a new policy condition.</p> 																														
8.	<p>Highlight <b>Windows-Groups</b> from the Select Attribute pop-up window. Click <b>Add</b> to continue.</p>  <table border="1" data-bbox="548 1205 1256 1682"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Called-Station-Id</td> <td>Specifies the phone number dialed by the user.</td> </tr> <tr> <td>Calling-Station-Id</td> <td>Specifies the phone number from which the call originates.</td> </tr> <tr> <td>Client-Friendly-Name</td> <td>Specifies the friendly name for the RADIUS client.</td> </tr> <tr> <td>Client-IP-Address</td> <td>Specifies the IP address of the RADIUS client.</td> </tr> <tr> <td>Client-Vendor</td> <td>Specifies the manufacturer of the RADIUS client.</td> </tr> <tr> <td>Day-And-Time-Restriction</td> <td>Specifies the time periods and days of week when access is allowed.</td> </tr> <tr> <td>Framed-Protocol</td> <td>Specifies the protocol that is used.</td> </tr> <tr> <td>MS-RAS-Vendor</td> <td>Description not yet defined</td> </tr> <tr> <td>NAS-Identifier</td> <td>Specifies the string that identifies the NAS through which the user is connecting.</td> </tr> <tr> <td>NAS-IP-Address</td> <td>Specifies the IP address of the NAS where the user is connecting.</td> </tr> <tr> <td>NAS-Port-Type</td> <td>Specifies the type of physical port that is used.</td> </tr> <tr> <td>Service-Type</td> <td>Specifies the type of service that the user has requested.</td> </tr> <tr> <td>Tunnel-Type</td> <td>Specifies the tunneling protocols used.</td> </tr> <tr> <td>Windows-Groups</td> <td>Specifies the Windows groups that the user belongs to.</td> </tr> </tbody> </table>	Name	Description	Called-Station-Id	Specifies the phone number dialed by the user.	Calling-Station-Id	Specifies the phone number from which the call originates.	Client-Friendly-Name	Specifies the friendly name for the RADIUS client.	Client-IP-Address	Specifies the IP address of the RADIUS client.	Client-Vendor	Specifies the manufacturer of the RADIUS client.	Day-And-Time-Restriction	Specifies the time periods and days of week when access is allowed.	Framed-Protocol	Specifies the protocol that is used.	MS-RAS-Vendor	Description not yet defined	NAS-Identifier	Specifies the string that identifies the NAS through which the user is connecting.	NAS-IP-Address	Specifies the IP address of the NAS where the user is connecting.	NAS-Port-Type	Specifies the type of physical port that is used.	Service-Type	Specifies the type of service that the user has requested.	Tunnel-Type	Specifies the tunneling protocols used.	Windows-Groups	Specifies the Windows groups that the user belongs to.
Name	Description																														
Called-Station-Id	Specifies the phone number dialed by the user.																														
Calling-Station-Id	Specifies the phone number from which the call originates.																														
Client-Friendly-Name	Specifies the friendly name for the RADIUS client.																														
Client-IP-Address	Specifies the IP address of the RADIUS client.																														
Client-Vendor	Specifies the manufacturer of the RADIUS client.																														
Day-And-Time-Restriction	Specifies the time periods and days of week when access is allowed.																														
Framed-Protocol	Specifies the protocol that is used.																														
MS-RAS-Vendor	Description not yet defined																														
NAS-Identifier	Specifies the string that identifies the NAS through which the user is connecting.																														
NAS-IP-Address	Specifies the IP address of the NAS where the user is connecting.																														
NAS-Port-Type	Specifies the type of physical port that is used.																														
Service-Type	Specifies the type of service that the user has requested.																														
Tunnel-Type	Specifies the tunneling protocols used.																														
Windows-Groups	Specifies the Windows groups that the user belongs to.																														

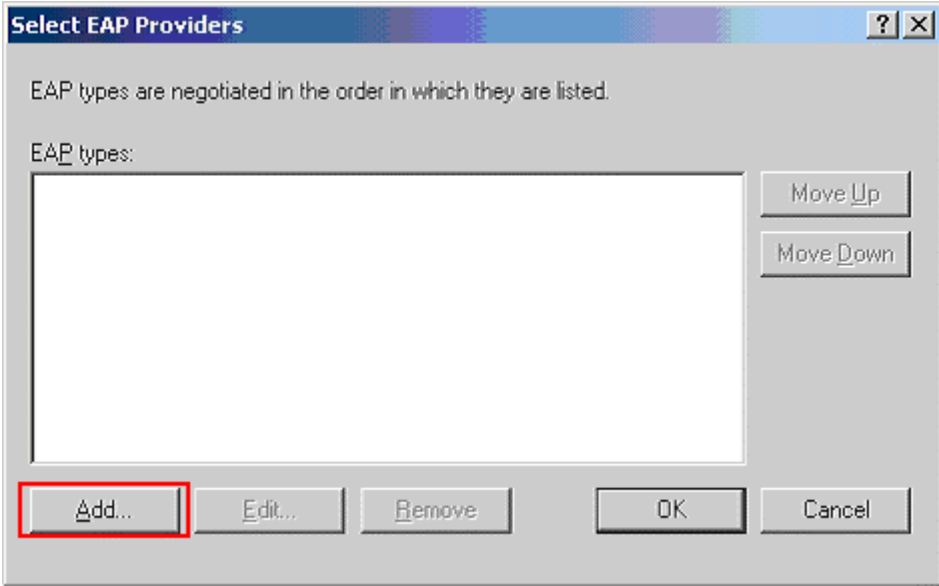
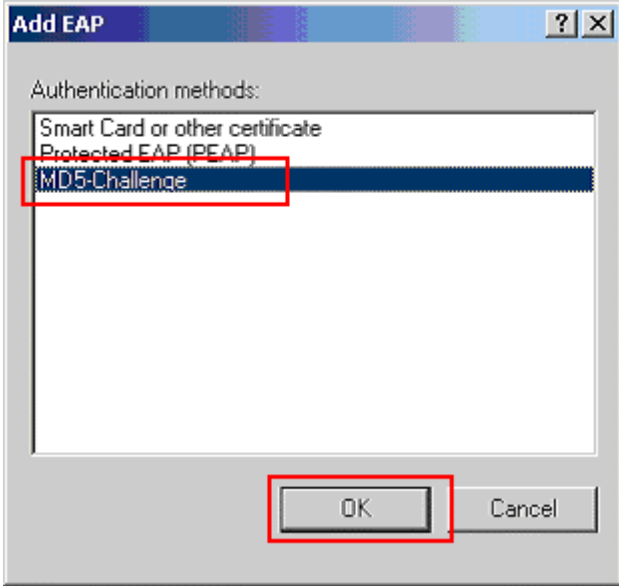


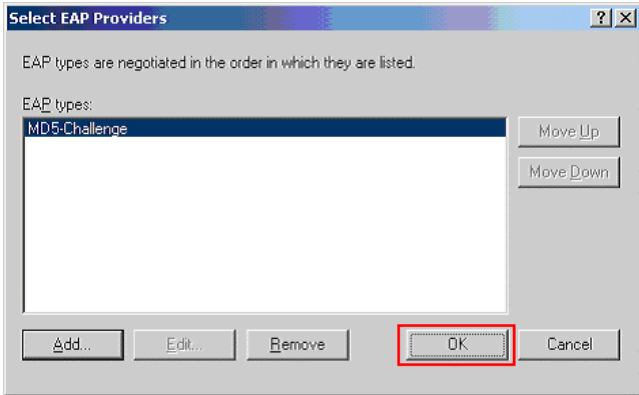
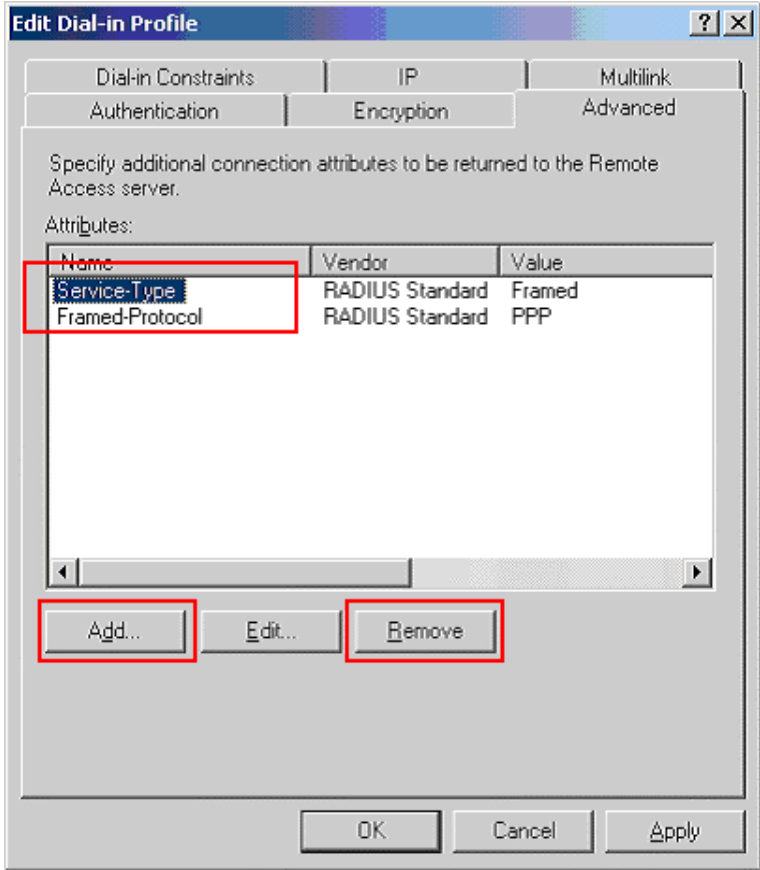
Step	Description
9.	<p>Click <b>Add</b> in the Groups pop-up window to add a Windows group.</p> 
10.	<p>Enter the Active Directory user group created in <b>Section 5.1, Steps 12-13</b>. Use <b>Check Names</b> to assist in searching for the user group. Click <b>OK</b> to complete.</p> 

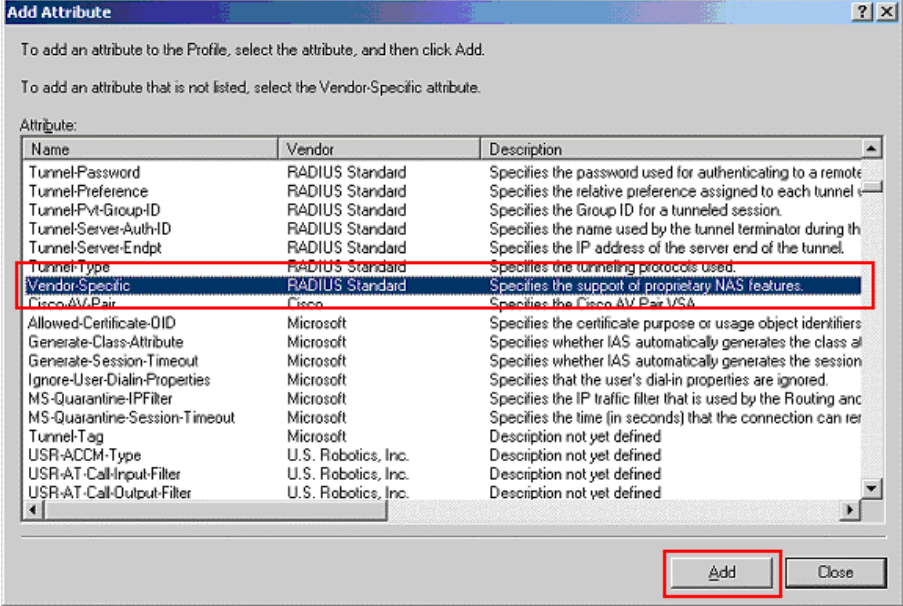
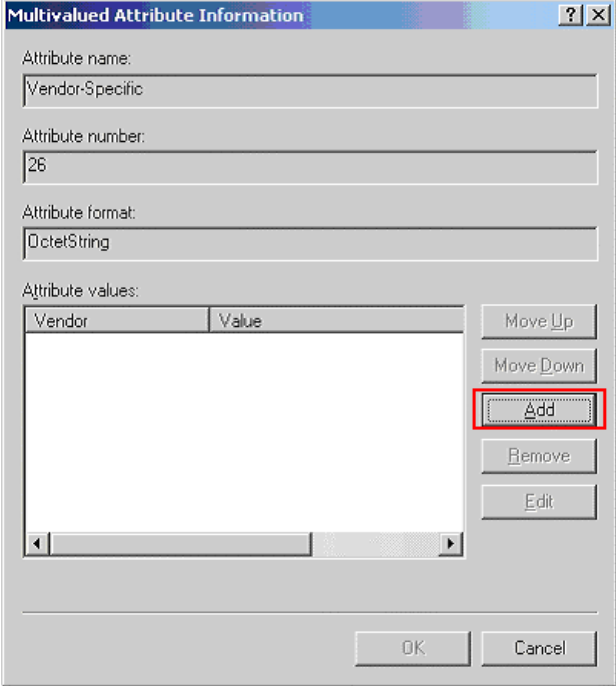
Step	Description
11.	<p>Click <b>OK</b> in the Groups pop-up window to complete.</p> 
12.	<p>Once the Windows user group has been added via <b>Steps 8-11</b>, click <b>Next</b> to continue.</p> 

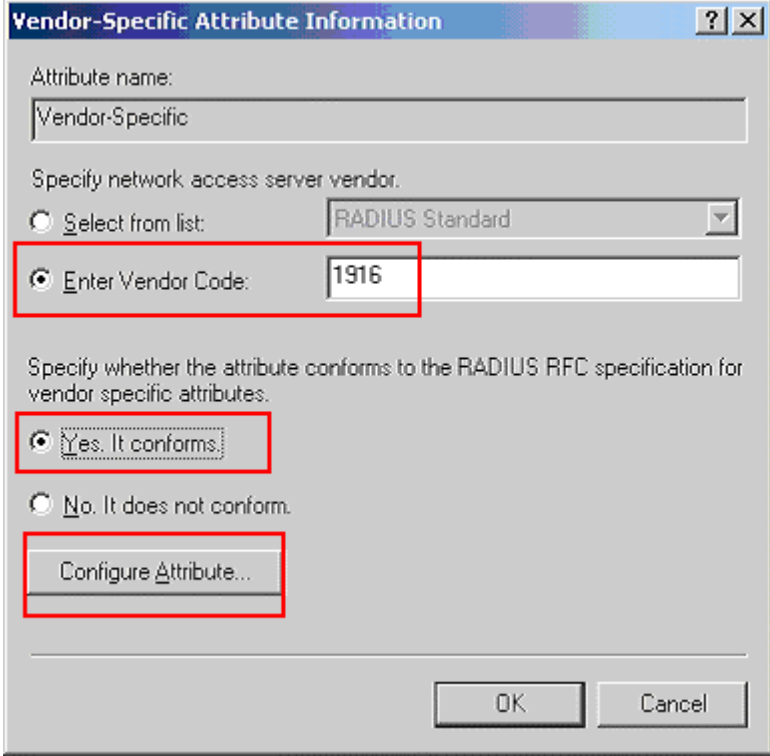
Step	Description
13.	<p>Click the <b>Grant remote access permission</b> radio button. Click <b>Next</b> to continue.</p>  <p>The screenshot shows a window titled "New Remote Access Policy Wizard" with a close button (X) in the top right corner. The main heading is "Permissions" with a sub-heading "A 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 remote access permission" radio button is enclosed in a red rectangular box. At the bottom of the window, there are three buttons: "&lt; Back", "Next &gt;", and "Cancel". The "Next &gt;" button is also enclosed in a red rectangular box.</p>
14.	<p>Click <b>Edit Profile</b> 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 close button (X) in the top right corner. The main heading is "Profile" with a sub-heading "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." In the center of the window, there is a button labeled "Edit Profile...". This button is enclosed in a red rectangular box. At the bottom of the window, there are three buttons: "&lt; Back", "Next &gt;", and "Cancel".</p>

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

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

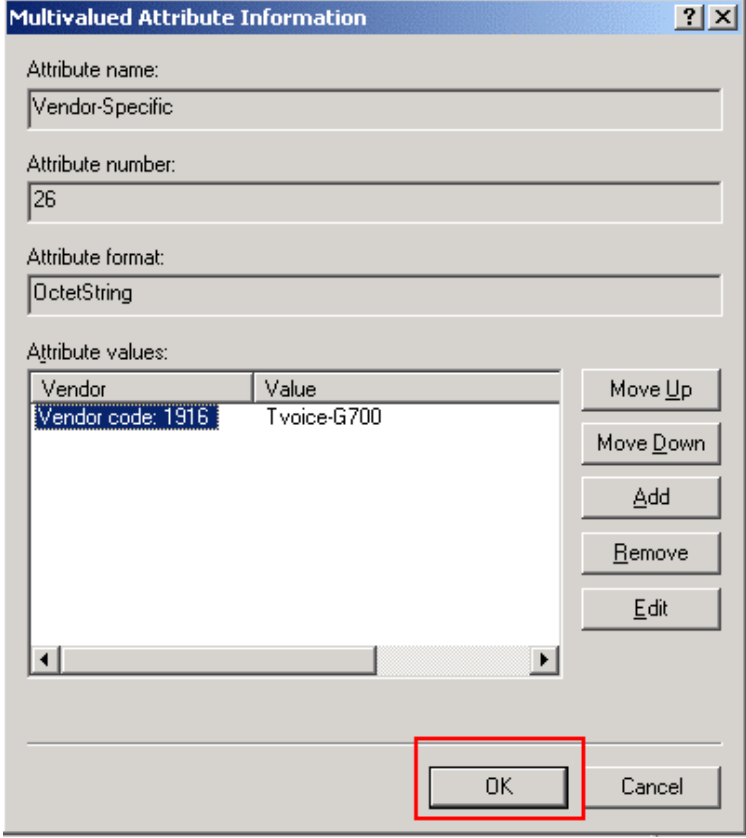
Step	Description									
18.	<p>Once the MD5-Challenge EAP type is added, Click <b>OK</b> to complete the EAP authentication selection.</p>  <p>The screenshot shows a dialog box titled "Select EAP Providers". It contains a list of EAP types with "MD5-Challenge" selected. There are "Move Up" and "Move Down" buttons to the right of the list. At the bottom, there are "Add...", "Edit...", "Remove", "OK", and "Cancel" buttons. The "OK" button is highlighted with a red box.</p>									
19.	<p>Select the <b>Advanced</b> tab in the Edit Dial-in Profile pop-up window. Highlight each existing attribute, then click <b>Remove</b> to delete it. Click <b>Add</b> after all existing attributes have been removed to enter a new attribute. This will display the Add Attribute pop-up window.</p>  <p>The screenshot shows the "Edit Dial-in Profile" dialog box with the "Advanced" tab selected. It contains a table of attributes. The "Service-Type" and "Framed-Protocol" rows are highlighted with red boxes. Below the table, the "Add...", "Edit...", and "Remove" buttons are also highlighted with red boxes.</p> <table border="1" data-bbox="542 1192 1230 1535"> <thead> <tr> <th>Name</th> <th>Vendor</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Service-Type</td> <td>RADIUS Standard</td> <td>Framed</td> </tr> <tr> <td>Framed-Protocol</td> <td>RADIUS Standard</td> <td>PPP</td> </tr> </tbody> </table>	Name	Vendor	Value	Service-Type	RADIUS Standard	Framed	Framed-Protocol	RADIUS Standard	PPP
Name	Vendor	Value								
Service-Type	RADIUS Standard	Framed								
Framed-Protocol	RADIUS Standard	PPP								

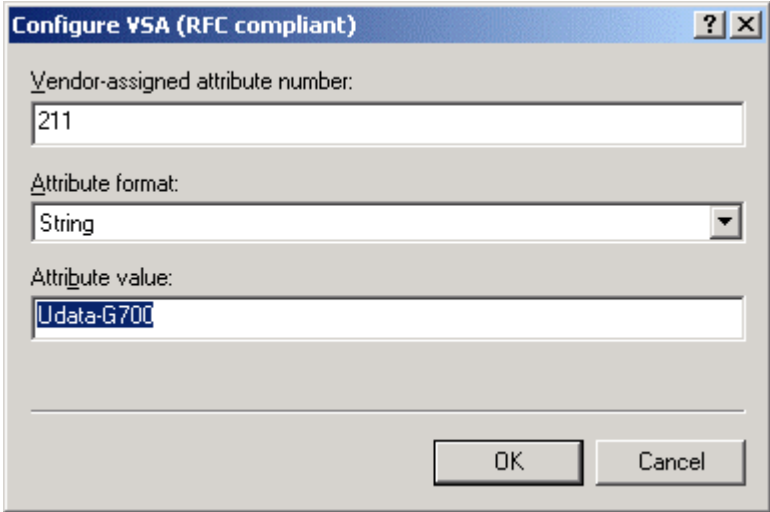
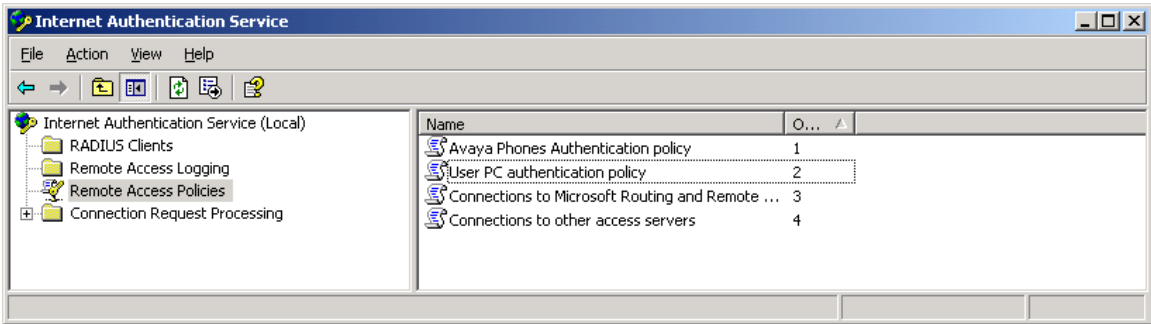
Step	Description																																																									
20.	<p>Highlight the <b>Vendor Specific</b> attribute name from the list of attributes displayed in the Add Attribute pop-up window. Click <b>Add</b> to continue. This will display the Multi-valued Attribute Information pop-up window.</p>  <p>The screenshot shows the 'Add Attribute' dialog box with a table of attributes. The 'Vendor-Specific' attribute is highlighted in blue. The 'Add' button at the bottom right is also highlighted with a red box.</p> <table border="1" data-bbox="467 512 1328 898"> <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><b>Vendor-Specific</b></td> <td><b>RADIUS Standard</b></td> <td><b>Specifies the support of proprietary NAS features.</b></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 dialin 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.	<b>Vendor-Specific</b>	<b>RADIUS Standard</b>	<b>Specifies the support of proprietary NAS features.</b>	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 dialin 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.																																																								
<b>Vendor-Specific</b>	<b>RADIUS Standard</b>	<b>Specifies the support of proprietary NAS features.</b>																																																								
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 dialin 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 <b>Add</b> to enter a new Attribute in the Multi-valued 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. The 'Add' button is highlighted with a red box.</p> <table border="1" data-bbox="613 1440 1052 1692"> <thead> <tr> <th>Vendor</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Vendor	Value																																																							
Vendor	Value																																																									

Step	Description
22.	<p>In the Vendor-Specific Attribute Information pop-up window, click on the <b>Enter Vendor Code</b> radio button, and enter string <b>1916</b> (Extreme Networks Vendor Code). Click on the <b>Yes, It conforms</b> radio button. Click <b>Configure Attribute</b> 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 “<b>Tvoice-G700</b>” signifies that the port should be configured as “Tagged” with “voice-G700” VLAN assigned. The voice VLAN was created on the switch in <b>Section 4.1, Step 2</b>. Click <b>OK</b> to complete.</p> <div data-bbox="516 415 1279 919" style="border: 1px solid gray; padding: 10px; margin: 10px auto; width: fit-content;"> <p>The screenshot shows a dialog box titled "Configure VSA (RFC compliant)". It has a standard Windows-style title bar with a question mark icon and a close button (X). The dialog contains three input fields:         <ul style="list-style-type: none"> <li><b>Vendor-assigned attribute number:</b> A text box containing the value "211".</li> <li><b>Attribute format:</b> A dropdown menu currently showing "String".</li> <li><b>Attribute value:</b> A text box containing the value "Tvoice-G700".</li> </ul>         At the bottom right of the dialog are two buttons: "OK" and "Cancel".       </p> </div>

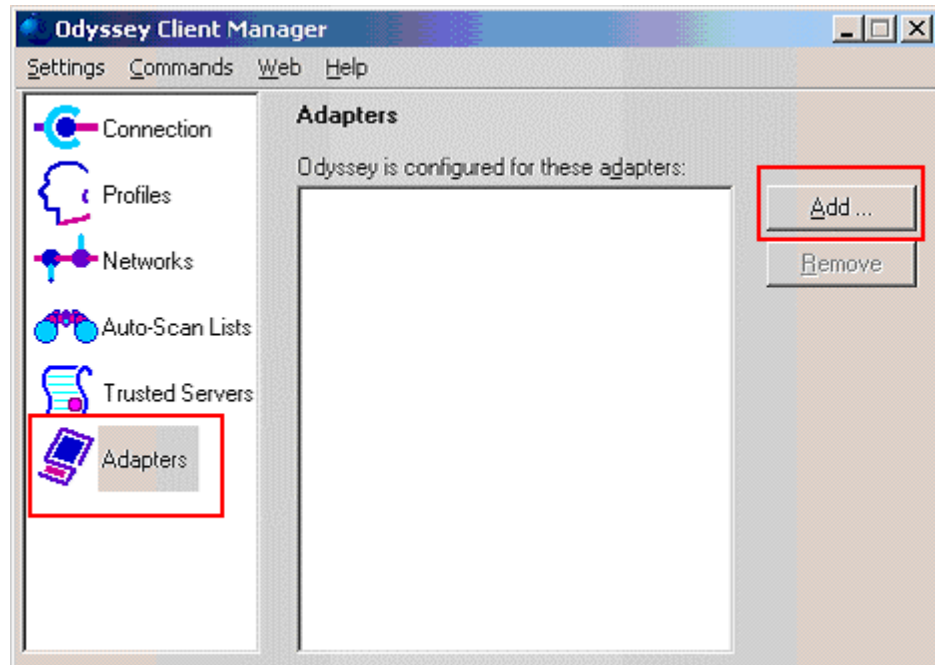
Step	Description
24.	<p data-bbox="326 233 1284 268">Once all attributes have been entered in Steps 21-24, click <b>OK</b> to continue.</p> 
25.	<p data-bbox="326 1178 1451 1247">Click <b>OK</b> on all preceding pop-up windows to complete the configuration of this access policy.</p>

Step	Description
26.	<p>Repeat Steps 4-23 to create a separate policy for a PC. The sample network uses the name <b>User PC authentication policy</b> for this new policy. Use the <b>Udata-G700</b> value in lieu of what is in <b>Step 23</b>. The <b>Udata-G700</b> value indicates to the switch the switch port should be assigned to the “data-G700” VLAN as Untagged. The data VLAN was created on the switch in <b>Section 4.1, Step 2</b>.</p> 
27.	<p>After completing the above steps, there should be a total of 4 Remote Access Policies.</p> 

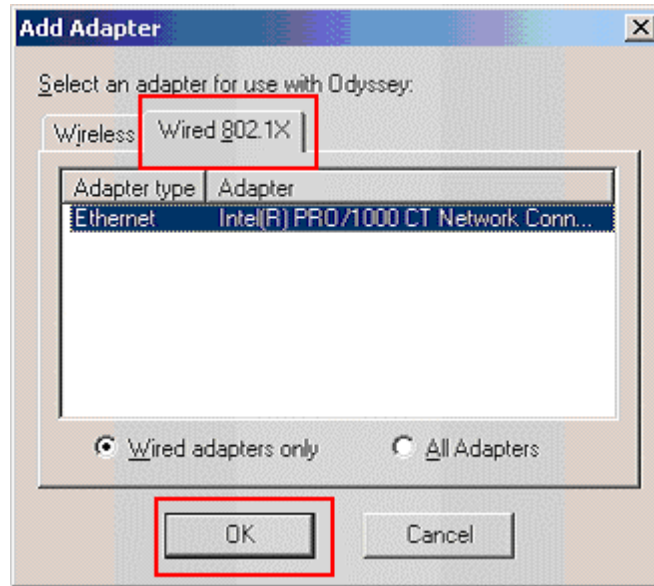
## 7. Configure the Odyssey client

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

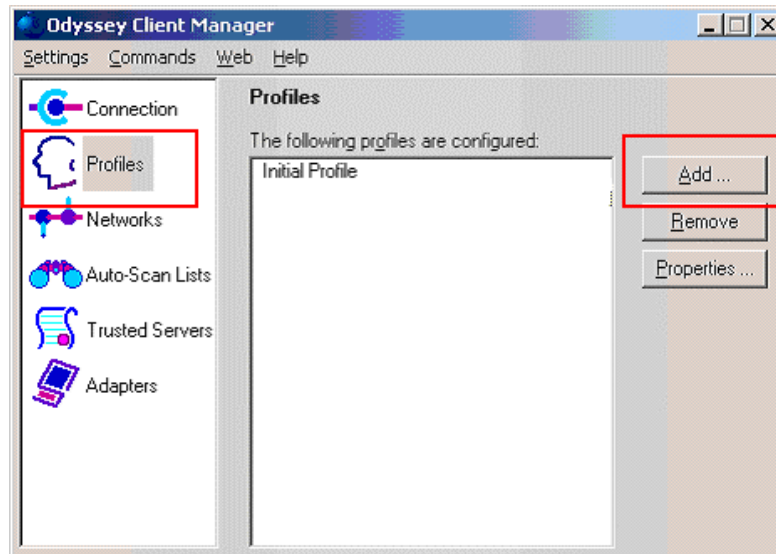
1. Start the Odyssey Client by clicking **Start > Programs > Juniper Networks > Odyssey Access Client > Odyssey Access Client Manager**. Add a network adapter by selecting **Adapters** on the left panel then click **Add** from the Odyssey Client Manager window.



2. Click on the **Wired 802.1X** tab in the Add Adapter pop-up window. Select the desired network adapter and click **Ok** to complete.



3. Add a profile by selecting **Profiles** on the left panel then click **Add** to continue.



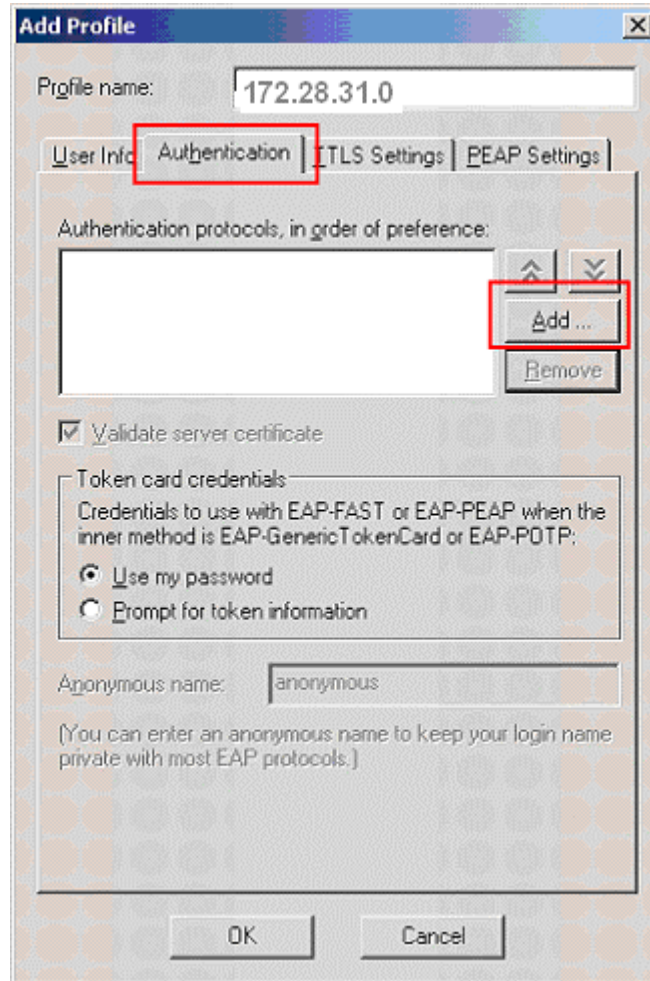
4. From the User Info tab in the Add Profile pop-up window. Enter the **Login name** and **password**. The Login name and password must match what was setup in Section 6 Step 5. Click on the **Authentication** tab to continue.

The screenshot shows the 'Add Profile' dialog box with the following details:

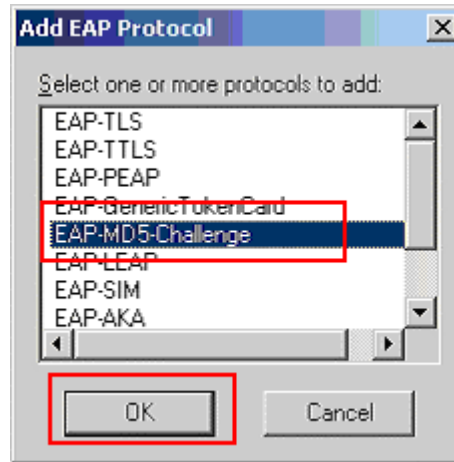
- Profile name:** 172.28.31.0
- Tab:** User Info
- Login name:** user1
- Password:**
  - Permit login using password
  - use Windows password
  - prompt for password
  - use the following password: 123456
  - Upmask
- Certificate:**
  - Permit login using my certificate:

Buttons at the bottom: OK, Cancel

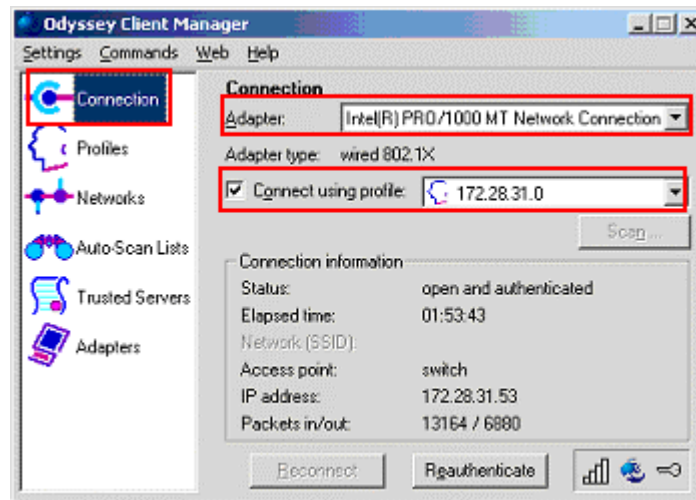
5. Under the **Authentication** tab, click **Add** to Add to add a new authentication protocol.



6. In the Add EAP Protocol pop-up window, select **EAP-MD5 Challenge**. Click **Ok** to complete.



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



## 8. Configure the Avaya IP Phone

This section shows the steps for configuring the Avaya 4610 SW IP Phone connected into the X250e-48p switch.

Avaya IP telephones support three 802.1X operational modes. The operational mode can be changed by pressing "mute80219#" ("mute 8021x") on the Avaya 4600-Series IP telephones or "mute27237#" (mute craft) on the Avaya 9600-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 telephones 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 Extensible Authentication Protocol over LAN (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 X250e-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.  Mute82019#
2.	Press the “*” key on the key pad until <b>p-t w/Logoff</b> is displayed, then press “#” key to complete the configuration.

## 9. 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. The following screens are from the System Access Terminal (SAT). Log in with the appropriate credentials.

Step	Description
1.	<p>Add a new station for the Avaya IP Telephones to the Avaya Communication Manager using the <b>add station</b> command. Configure the following fields.</p> <ul style="list-style-type: none"> <li>• <b>Extension:</b> <i>33004</i> (Extension number for the Avaya Telephone)</li> <li>• <b>Type:</b> <i>9630</i> (Avaya Telephone type used for this extension)</li> <li>• <b>Port:</b> <i>IP</i> (Type of connection for the Avaya Telephone)</li> <li>• <b>Security Code:</b> <i>1234</i> (Security code used by the Avaya Telephone to register with Avaya Communication Manager)</li> <li>• <b>Direct IP-IP Audio Connections:</b> <i>y</i> (Enable Shuffling)</li> </ul> <p>The first two pages of the <b>add station 33004</b> configuration are shown below. Repeat this step for each station.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> add station 33004                                     Page 1 of 4                                      STATION Extension: 33004                                     Lock Messages? n          BCC: 0   Type: 9630   Security Code: 123456     TN: 1   Port: S00003                                       Coverage Path 1: 99      COR: 1   Name: Ext-33004                                       Coverage Path 2:         COS: 1                                      Hunt-to Station: STATION OPTIONS           Loss Group: 19           Speakerphone: 2-way           Display Language: english Survivable GK Node Name:           Survivable COR: internal           Survivable Trunk Dest? y           Time of Day Lock Table:           Personalized Ringing Pattern: 1           Message Lamp Ext: 33004           Mute Button Enabled? y           Button Modules: 0           Media Complex Ext:           IP SoftPhone? n           Customizable Labels? y </pre> </div>

Step	Description
2.	<p>Use the “display ip-network-region” command to display the 802.1P setting configured in the Avaya Communication Manager. Verify that both <b>Call Control 802.1p Priority</b> and <b>Audio 802.1P Priority</b> are set to 6.</p> <pre data-bbox="350 375 1440 905"> display ip-network-region 1                                     Page 1 of   IP NETWORK REGION Region: 10 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: 3329 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 </pre>

## 10. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the X250s in supporting Avaya Communication Manager, Avaya Media Gateway and Avaya IP Phones in a network composed of both Extreme Networks and Avaya switches.

### 10.1. General Test Approach

Quality of Service was verified by injecting simulated traffic into the network using a traffic generator while calls were being established and maintained using Avaya IP Telephones. The objectives were to verify the X250e-48p and X250e-24p supports the following:

- 802.1X multiple supplicant support
- interoperability of basic 802.1D and 802.1w spanning tree
- Layer-2, and Layer-3 based Quality of Service
- Basic calling performed by Avaya IP Phones (e.g., place/receive call, transfer, DTMF pass-through)
- EAPS
- Link Layer Discovery Protocol (LLDP) for configuring the Avaya 4600 and 9600 series IP Telephones
- Ethernet Automatic Protection Switching (EAPS)

## 10.2. Test Results

The Extreme Networks X250e-48p and X250e-24p switches successfully achieved the above objectives. Quality of Service for VoIP traffic was maintained throughout testing in the presence of competing simulated traffic. 802.1D and 802.1w spanning tree as well as EAPS correctly converged when active link was disconnected or when bridging priority was changed. LLDP also correctly reported the attributes of both Avaya 4600 and 9600 series IP Telephones.

## 11. Verification Steps

The following steps may be used to verify the configuration:

- Use the “show eaps <eaps domain>” command on the Extreme switches to verify the operation of EAPS.

```
X250e-48p # show eaps userfloor
Name: userfloor
State: Complete                               Running: Yes
Enabled: Yes      Mode: Master
Primary port:    2          Port status: Up Tag status: Tagged
Secondary port: 3          Port status: Blocked Tag status: Tagged
Hello timer interval: 1 sec 0 millise
Fail timer interval: 3 sec
Fail Timer expiry action: Send alert
Last update: From Master Id 00:04:96:27:7f:e3, at Fri Apr 13 21:17:55 2007
EAPS Domain has following Controller Vlan:
  Vlan Name      VID
  c1             111
EAPS Domain has following Protected Vlan(s):
  Vlan Name      VID
  data-G700      31
  voice-G700     30
Number of Protected Vlans: 2
```

- Use the “show radius” command on the X250e-48p and X250e-24p to verify whether RADIUS setting such as **IP address** and **Client address** are correct. A successful log in by an 802.1X client shows 2 Access Requests, 1 Access Accepts, and 1 Access Challenges in the counter.

```
X250e-48p # show radius
Switch Management Radius: enabled
Switch Management Radius server connect time out: 3 seconds
Switch Management Radius Accounting: disabled
Switch Management Radius Accounting server connect time out: 3 seconds
Netlogin Radius: enabled
Netlogin Radius server connect time out: 3 seconds
Netlogin Radius Accounting: disabled
Netlogin Radius Accounting server connect time out: 3 seconds

Primary Netlogin Radius server:
  Server name      :
  IP address       : 172.28.10.12
  Server IP Port   : 1812
  Client address   : 172.28.31.2 (VR-Default)
  Shared secret    : 3>:>?75<;5
```

<b>Access Requests</b> : 2	<b>Access Accepts</b> : 1
Access Rejects : 0	<b>Access Challenges</b> : 1
Access Retransmits: 0	Client timeouts : 0
Bad authenticators: 0	Unknown types : 0
Round Trip Time : 0	

- Use the “show netlogin” command on the X250e-48p and X250e-24p to verify if 802.1X is enabled or if the PC or Avaya IP Phone has successfully been authenticated. The output also shows which VLAN the client is authenticated onto. Note that the Avaya IP Phones (MAC address 00:04:0d:e4:37:79) is only authenticated in the voice VLAN even though its MAC address is displayed in the data VLAN.

```
X250e-48p # 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: 18, Vlan: data, State: Enabled, Authentication: 802.1x, Guest Vlan <Not
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
-----

Port: 18, 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
-----
```

- Use the “show lldp neighbors detail” command on the X250 switch to LLDP information.

```
X250e-48p # show lldp neighbors detail

-----
LLDP Port 18 detected 1 neighbor
Neighbor: (5.1)172.28.30.51/00:04:0D:EC:92:AB, age 13 seconds
- Chassis ID type: Network address (5); Address type: IPv4 (1)
  Chassis ID       : 172.28.30.51
- Port ID type: MAC address (3)
  Port ID        : 00:04:0D:EC:92:AB
- Time To Live: 120 seconds
- System Name: "AVAEC92AB"
- System Capabilities : "Bridge, Telephone"
  Enabled Capabilities: "Bridge"
- Management Address Subtype: IPv4 (1)
  Management Address       : 172.28.30.51
  Interface Number Subtype : System Port Number (3)
  Interface Number        : 1
  Object ID String        : "1.3.6.1.4.1.6889.1.69.2.2"
- 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                   : 30
  L2 Priority                : 6
  DSCP Value                 : 46
- MED Hardware Revision: "9630D01A"
- MED Firmware Revision: "hb96xxual_21.bin"
- MED Software Revision: "ha96xxual_21.bin"
- MED Serial Number: "06N534779862"
- MED Manufacturer Name: "Avaya"
- MED Model Name: "9630"
- Avaya/Extreme Conservation Level Support
  Current Conservation Level: 0
  Typical Power Value       : 0.0 Watts
  Maximum Power Value      : 0.0 Watts
  Conservation Power Level : 1=0.0W
- Avaya/Extreme Call Server(s): 172.28.30.5
- Avaya/Extreme IP Phone Address: 172.28.30.51 255.255.255.0
  Default Gateway Address      : 172.28.30.1
- Avaya/Extreme CNA Server: 0.0.0.0
- Avaya/Extreme File Server(s): 172.28.10.12
- Avaya/Extreme IEEE 802.1q Framing: Tagged
```

- Use the “show dot1p” command on the X250e-48p and X250e-24p switch has the correct 802.1P to QoS Profile assignment.

```
X250e-48p # show dot1p
802.1p Priority Value      QoS Profile
        0                QP1
        1                QP1
        2                QP1
        3                QP1
        4                QP1
        5                QP1
        6                QP7
        7                QP8
```

- Use the “show trunk” command on the Avaya C363T-PWR Converged Stackable Switch to verify trunk settings.

```
C360-1(super)# set trunk

Port    Mode  Binding mode                Native vlan
-----
1/1     dot1q bound to configured vlans   1
1/2     off   statically bound           1
1/3     dot1q bound to configured vlans 1
1/4     off   statically bound           1
1/5     off   statically bound           1
1/6     off   statically bound           1
1/7     off   statically bound           1
1/8     off   statically bound           1
1/9     off   statically bound           1
1/10    dot1q bound to configured vlans 31
1/11    off   statically bound           1
1/12    off   statically bound           1
```

## 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. Conclusion

These Application Notes have described the administration steps required to configure the Extreme Networks X250e-48p and X250e-24p switch to support an Avaya VoIP solution depicted in **Figure 1** which is composed of an Avaya Server, Avaya Media Gateway, and Avaya IP Phones.

## 14. 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 3.1, February 2007
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 3, February 2007
- [3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 12, February 2007
- [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>

- [1] *ExtremeXOS Concepts Guide, Software Version 12.0*, Part number 100262-00 Rev. 01, 2007
- [2] *ExtremeXOS Command Reference Guide, Software Version 12.0*, Part number 100261-00 Rev. 01, 2007



---

**©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](mailto:devconnect@avaya.com).