



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the steps for configuring the Extreme Networks Summit X250e-48t and X250e-24t switches to support an Avaya VoIP solution consisting of an Avaya Server, an Avaya Media Gateway and Avaya IP Telephones in network composed of both Extreme Network Summit switches, and Avaya Converged Stackable Switches. Information in these Application Notes has been obtained through *DeveloperConnection* compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring the Extreme Networks Summit X250e-48t and X250e-24t (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-48t and X250e-24t.

The Avaya C363T-PWR, Extreme X250e-48t, and Extreme X250e-24t switches are connected to each other in a full mesh topology. 802.1D Spanning Tree Protocol (STP) is configured in the X250s and Avaya C363T-PWR switches as a layer-2 loop avoidance mechanism. 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 Telephone and the PCs running Odyssey Client are connected to the X250s switches. The Avaya IP Telephone and PCs are individually authenticated through the X250 switch by the IAS via the X250's per port multiple 802.1X supplicant support.

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. The X250e-48t and X250e-24t does not support Power over Ethernet (PoE), therefore the Avaya 9600 IP Telephones are connected into the switch through a power supply not shown.

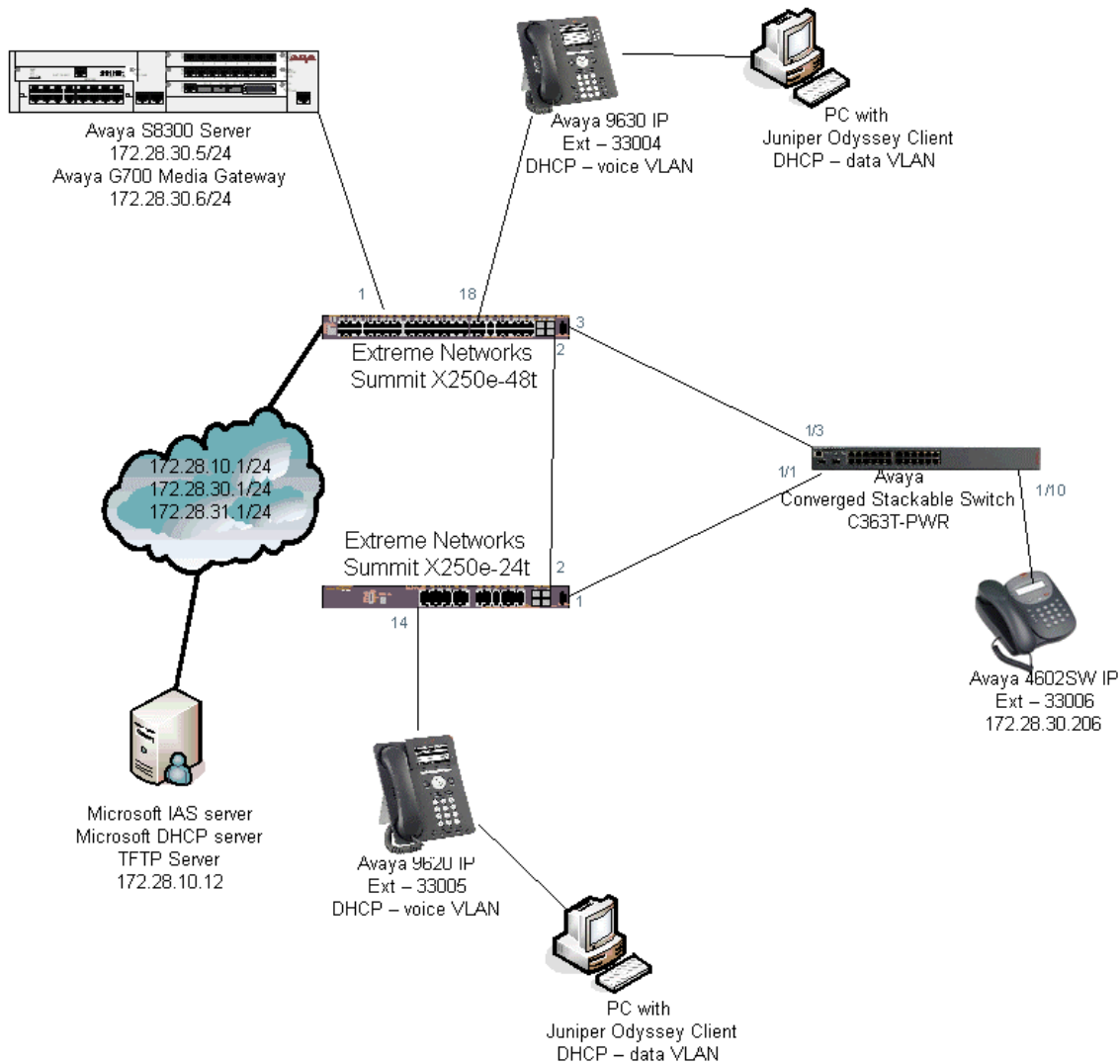


Figure 1: Sample Network Configuration

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 4602SW IP Telephone	R2.3 (H.323)
Avaya C363T-PWR Converged Stackable Switch	SW Version 4.5.14
Extreme Networks X250e-24t	ExtremeXOS 12.0.1.11
Extreme Networks X250e-48t	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-48t and X250e-24t 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-48t

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

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

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>Note: It is important to precede the voice VLAN name with “voice” as it is a required keyword.</p> <pre>X250e-48t # create vlan voice-G700 X250e-48t # config vlan voice-G700 tag 30 X250e-48t # config vlan voice-G700 ipaddress 172.28.30.2/24 (optional) X250e-48t # create vlan data-G700 X250e-48t # config vlan data-G700 tag 31 X250e-48t # config vlan data-G700 ipaddress 172.28.31.2/24 (optional) X250e-48t # create vlan temp</pre>
3.	<p>Configure VLAN assignment for the ports.</p> <p>Note: The VLAN assignment for the user port is dynamically assigned after the Avaya IP Telephone or user has been authenticated.</p> <pre>X250e-48t # config vlan default add port 2,3 untagged X250e-48t # config vlan voice-G700 add port 1,2,3 tagged X250e-48t # config vlan data-G700 add port 1,2,3 tagged</pre>
4.	<p>Configure a default route for the switch.</p> <pre>X250e-48t # configure iproute add default 172.28.31.1 vr vr- default</pre>
5.	<p>Configure spanning tree protocol. The sample network uses the default spanning tree domain s0 (stpd).</p> <pre>X250e-48t # config stpd "s0" add vlan "voice-G700" ports 2,3 dot1d X250e-48t # config stpd "s0" add vlan "data-G700" ports 2,3 dot1d X250e-48t # enable stpd s0</pre>

Step	Description
6.	<p>Configure LLDP for the user ports. The call-server and file-server configuration is used by Avaya IP Telephone to register and obtain setting information.</p> <pre>X250e-48t # configure lldp port 14 advertise vendor-specific dot1p vlan-name X250e-48t # configure lldp port 14 advertise vendor-specific avaya-extreme call-server 172.28.30.5 X250e-48t # configure lldp port 14 advertise vendor-specific avaya-extreme file-server 172.28.10.12 X250e-48t # configure lldp port 14 advertise vendor-specific avaya-extreme dot1p-framing tagged X250e-48t # enable lldp ports 14</pre>
7.	<p>Configure 802.1X authentication for the switch and user ports. The shared-secret must match what is configured in IAS in Section 6.1, Step 3.</p> <pre>X250e-48t # configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.31.2 vr VR-Default X250e-48t # configure radius netlogin primary shared-secret 1234567890 X250e-48t # configure netlogin vlan temp X250e-48t # enable radius netlogin X250e-48t # enable netlogin dot1p X250e-48t # enable netlogin ports 18,20 dot1p</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 settings set in the ip-network-region form in Section 9, Step 2.</p> <pre>X250e-48t # create qosprofile QP7 X250e-48t # configure dot1p type 6 qosprofile QP7</pre>
9.	<p>Save the configuration</p> <pre>X250e-48t # save</pre>

4.2. Configure the X250e-24t

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

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

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>Note: It is important to precede the voice VLAN name with “voice” as it is a required keyword.</p> <pre>X250e-24t # create vlan voice-G700 X250e-24t # config vlan voice-G700 tag 30 X250e-24t # config vlan voice-G700 ipaddress 172.28.30.3/24 (optional) X250e-24t # create vlan data-G700 X250e-24t # config vlan data-G700 tag 31 X250e-24t # config vlan data-G700 ipaddress 172.28.31.3/24 (optional) X250e-24t # create vlan temp</pre>
3.	<p>Configure VLAN assignment for the ports.</p> <p>Note: The VLAN assignment for the user port is dynamically assigned after Avaya IP Telephone or user has been authenticated.</p> <pre>X250e-24t # config vlan default add port 1,2 untagged X250e-24t # config vlan voice-G700 add port 1,2 tagged X250e-24t # config vlan data-G700 add port 1,2 tagged</pre>
4.	<p>Configure a default route for the switch.</p> <pre>X250e-24t # configure iproute add default 172.28.31.1 vr vr- default</pre>
5.	<p>Configure spanning tree protocol. The sample network uses the default spanning tree domain s0 (stpd).</p> <pre>X250e-24t # config stpd "s0" add vlan "voice-G700" ports 1,2 dot1d X250e-24t # config stpd "s0" add vlan "data-G700" ports 1,2 dot1d X250e-24t # enable stpd s0</pre>

Step	Description
6.	<p>Configure LLDP for the user ports.</p> <pre>X250e-24t # <i>configure lldp port 14,16 advertise vendor-specific dot1 vlan-name</i> X250e-24t # <i>configure lldp port 14,16 advertise vendor-specific avaya-extreme call-server 172.28.30.5</i> X250e-24t # <i>configure lldp port 14,16 advertise vendor-specific avaya-extreme file-server 172.28.10.12</i> X250e-24t # <i>configure lldp port 14,16 advertise vendor-specific avaya-extreme dot1q-framing tagged</i> X250e-24t # <i>enable lldp ports 14,16</i></pre>
7.	<p>Configure 802.1X authentication for the switch and user ports. Configure 802.1X authentication for the switch and user ports. The shared-secret must match what is configured in IAS in Section 6.1, Step 3.</p> <pre>X250e-24t # <i>configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.31.3 vr VR-Default</i> X250e-24t # <i>configure radius netlogin primary shared-secret 1234567890</i> X250e-24t # <i>configure netlogin vlan temp</i> X250e-24t # <i>enable radius netlogin</i> X250e-24t # <i>enable netlogin dot1x</i> X250e-24t # <i>enable netlogin ports 14 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 settings set in the ip-network-region form in Section 9, Step 2.</p> <pre>X250e-24t # <i>create qosprofile QP7</i> X250e-24t # <i>configure dot1p type 6 qosprofile QP7</i></pre>
9.	<p>Save the configuration</p> <pre>X250e-24t # <i>save</i></pre>

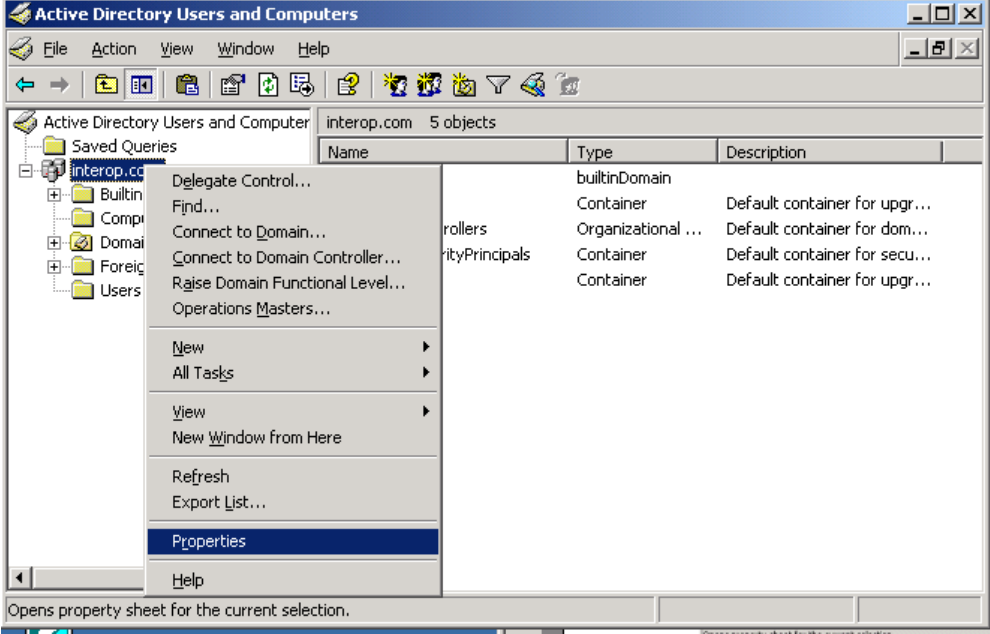
5. Configure the Avaya C363T-PWR Converged Stackable Switch

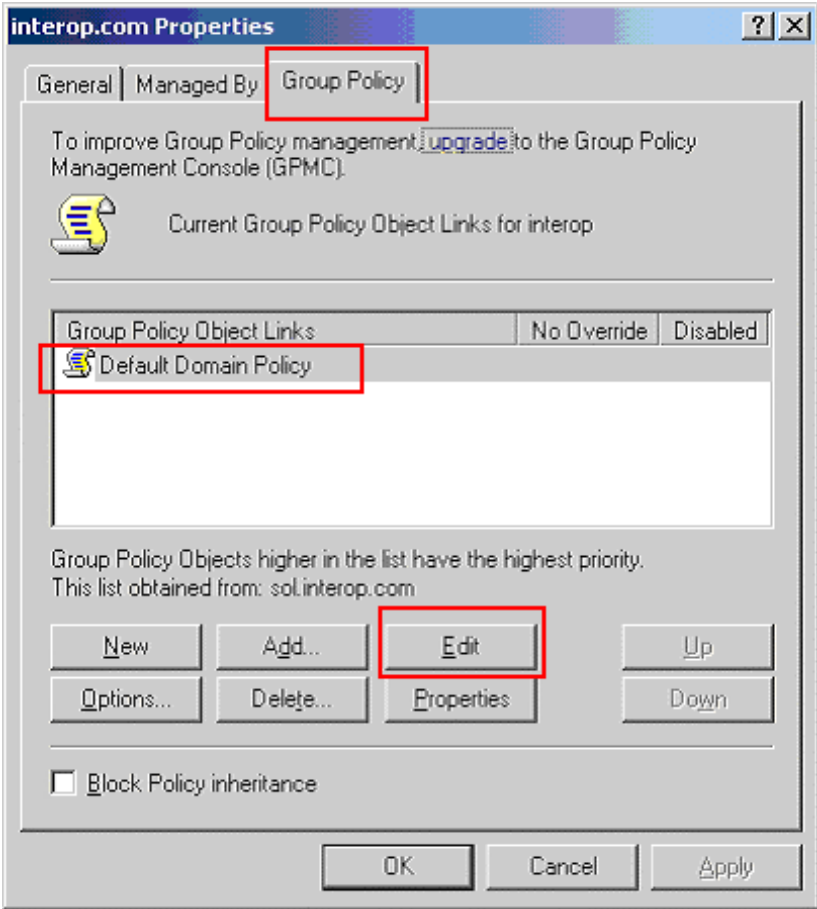
This section shows the steps for configuring the Avaya C363T-PWR Converged Stackable Switch.

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

6. Configure Microsoft Active Directory Service

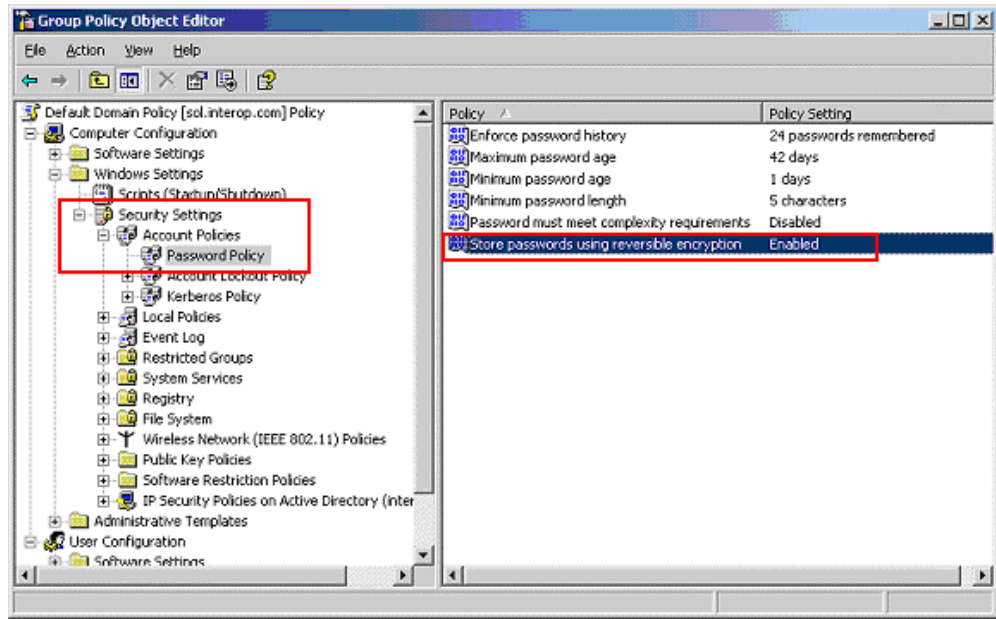
This section shows the necessary steps in configuring the Microsoft Active Directory server as shown in the **Figure 1** to support the Avaya IP Telephones and PC.

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 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 shows a table of objects in the domain:</p> <table border="1" data-bbox="673 735 1339 1197"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>builtinDomain</td> <td>Container</td> <td>Default container for upgr...</td> </tr> <tr> <td>rollers</td> <td>Organizational ...</td> <td>Default container for dom...</td> </tr> <tr> <td>ityPrincipals</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>A context menu is open over the 'interop.com' folder, with 'Properties' highlighted. The status bar at the bottom reads 'Opens property sheet for the current selection.'</p>		Name	Type	Description	builtinDomain	Container	Default container for upgr...	rollers	Organizational ...	Default container for dom...	ityPrincipals	Container	Default container for secu...		Container	Default container for upgr...
Name	Type	Description														
builtinDomain	Container	Default container for upgr...														
rollers	Organizational ...	Default container for dom...														
ityPrincipals	Container	Default container for secu...														
	Container	Default container for upgr...														

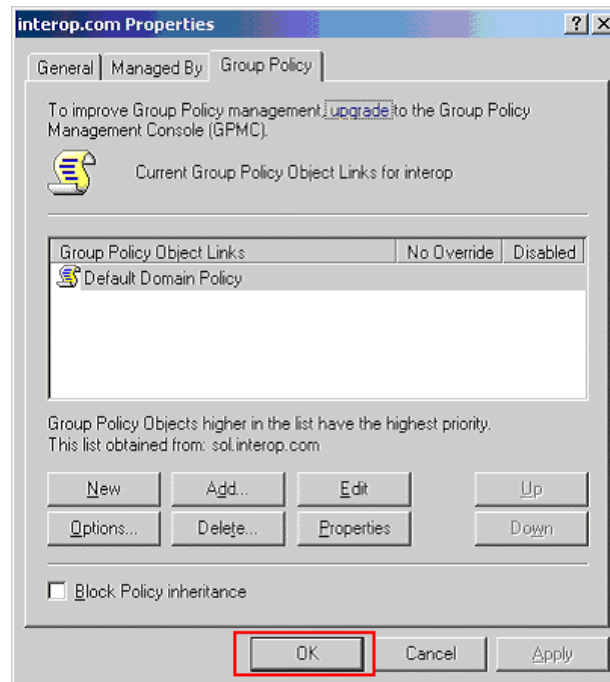
Step	Description
2.	<p>Select the Group Policy tab in the properties window. Highlight the Default Domain Policy then click Edit to display the Group Policy Object Editor.</p>  <p>The screenshot shows the 'interop.com Properties' dialog box. The 'Group Policy' tab is selected and highlighted with a red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

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

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

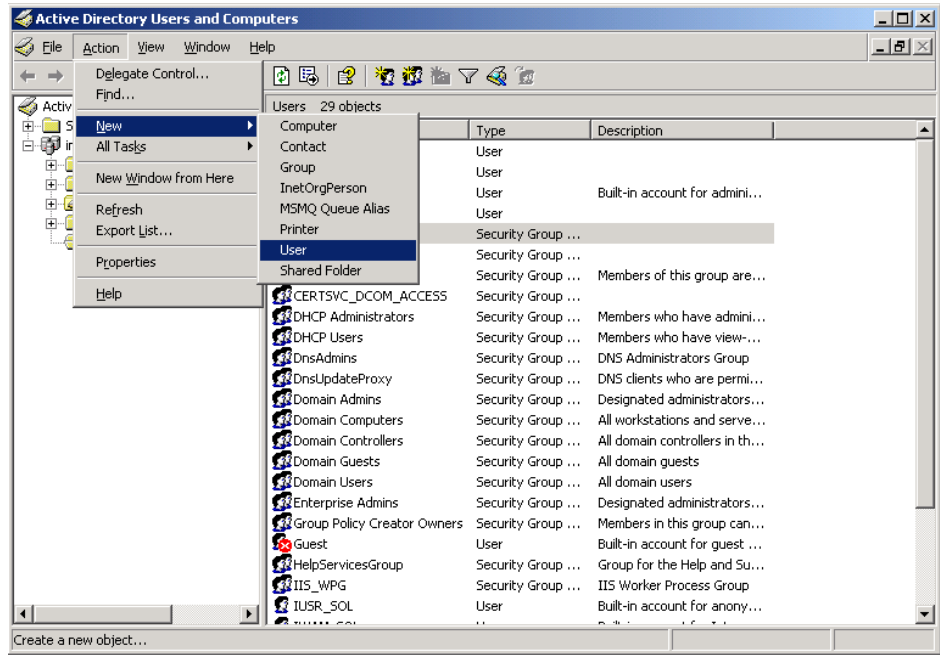


4. Click **OK** on the domain properties pop-up window to complete.

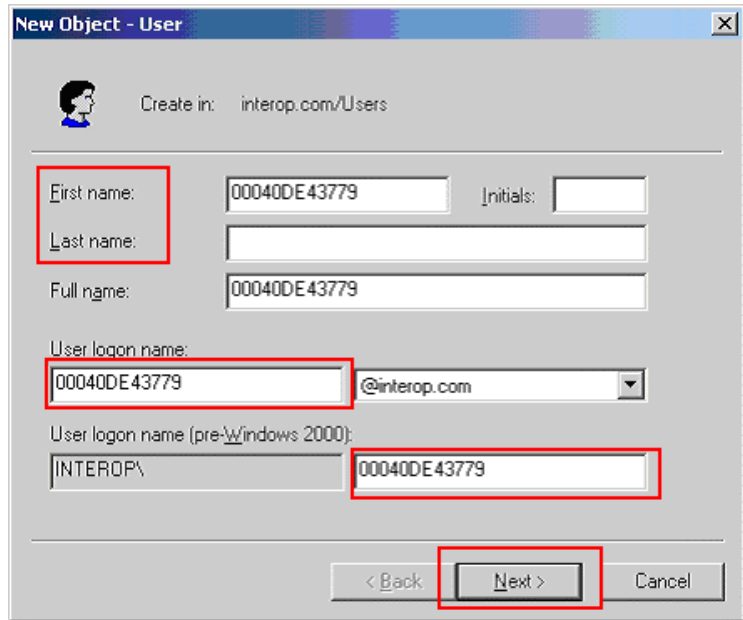


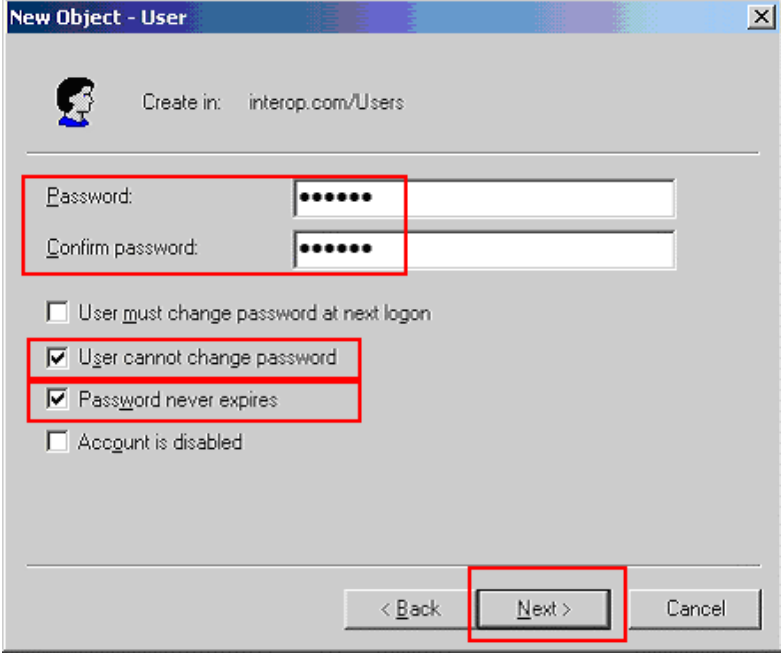
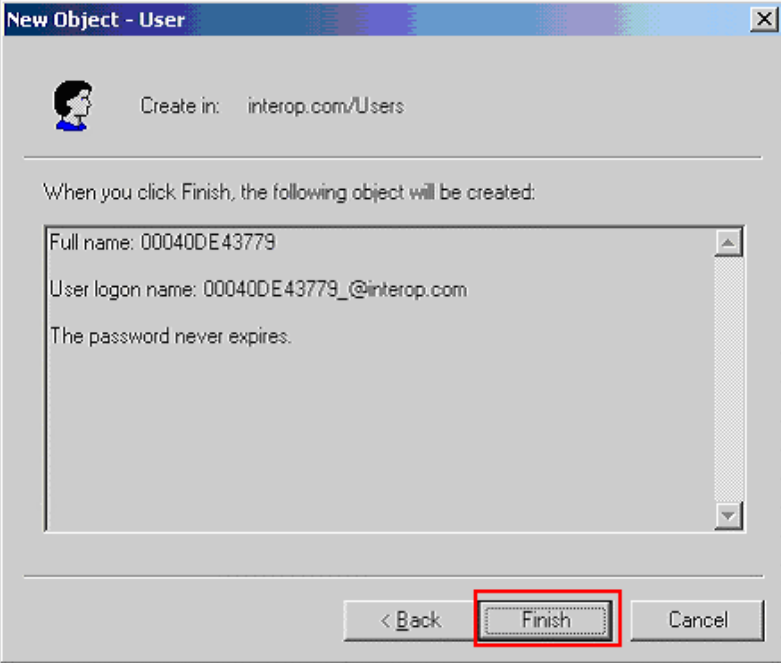
Step	Description
------	-------------

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.



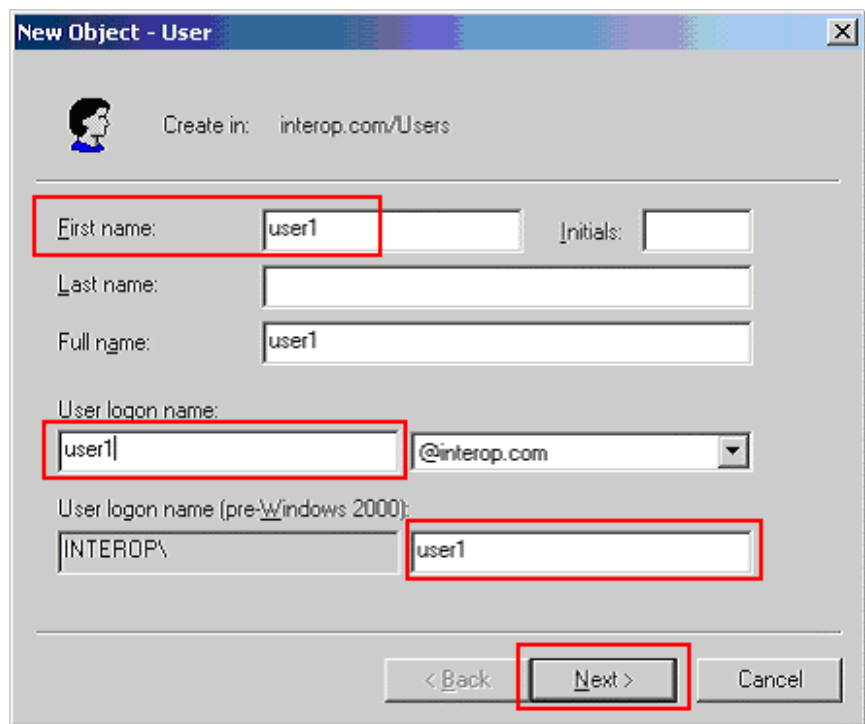
6. For an Avaya IP Telephone, enter the phone's MAC address as the **User logon name**. The **First name** and **Last name** are for information only. Click **Next** to continue.



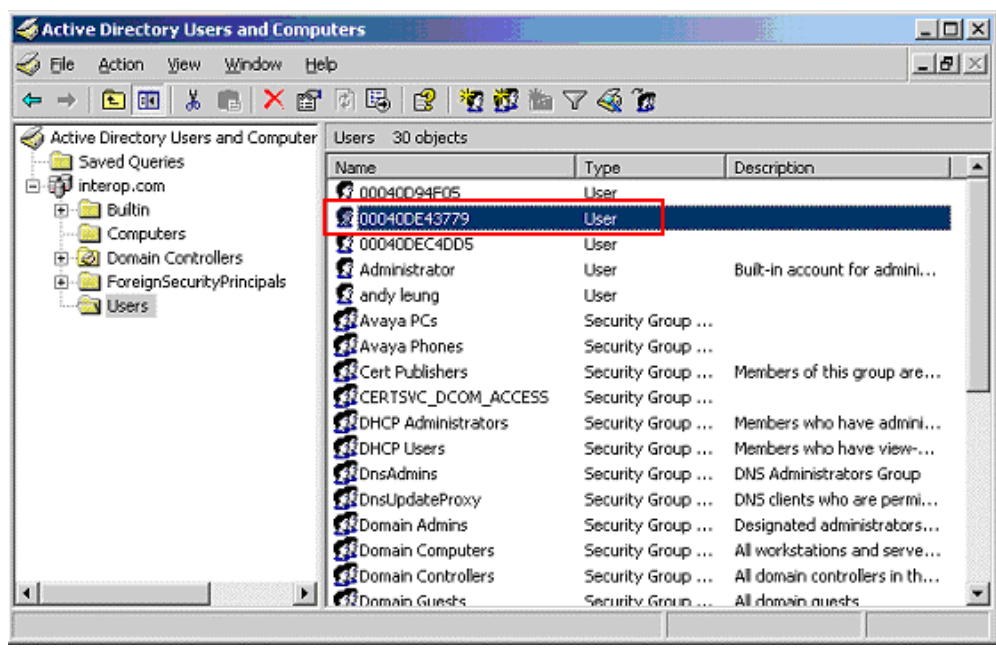
Step	Description
7.	<p>Enter a Password for the user ID. For an Avaya IP Telephone, enter a numeric password. Select the User cannot change password and Password never expires fields. Click Next to continue.</p> 
8.	<p>Click Finish to complete.</p> 

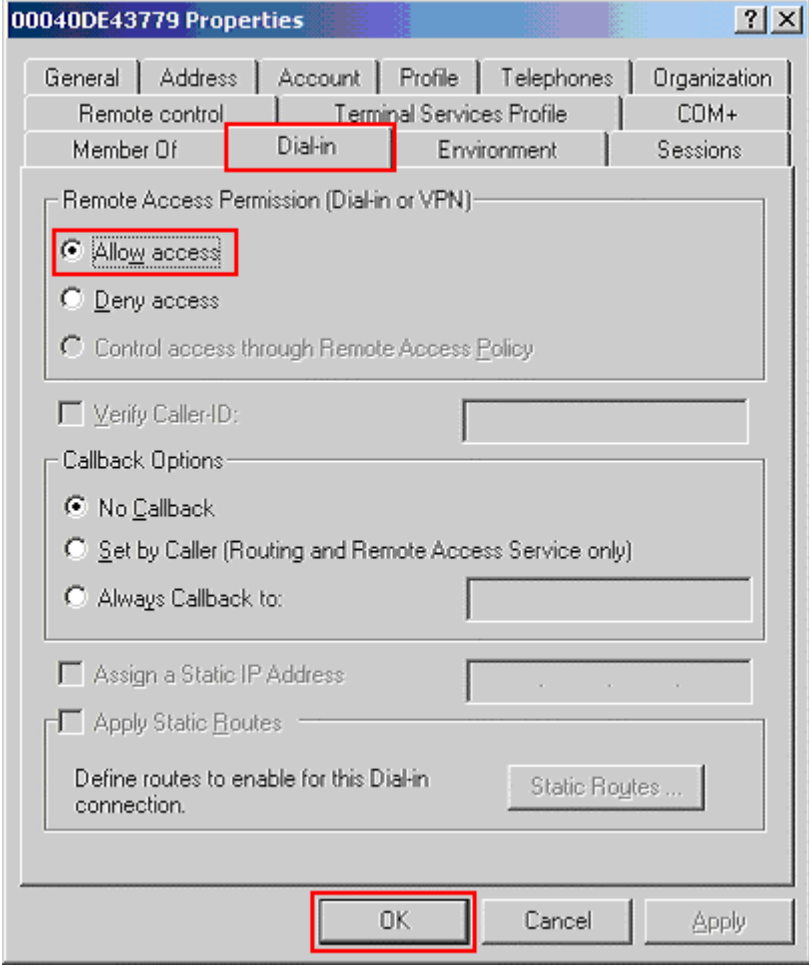
Step	Description
------	-------------

9. Repeat Steps 5-8 to create a user ID for the PC. Below is a screen capture for user ID “user1” used for the PC for log in.



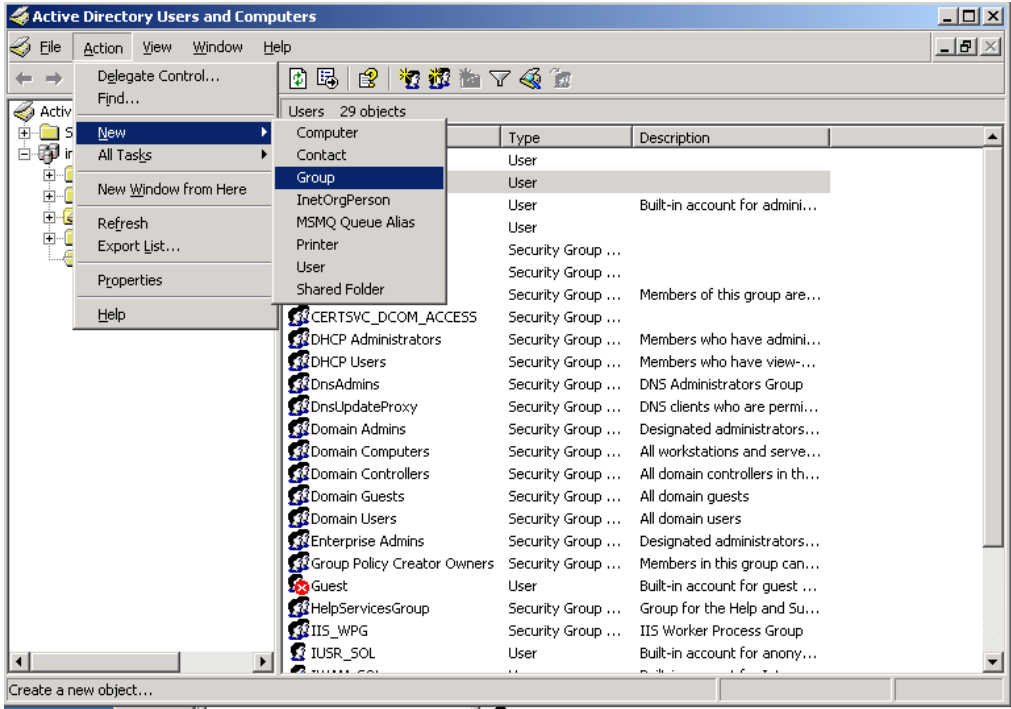
10. After creating the user ID, begin editing its properties by double clicking on the user ID in the Active Directory Users and Computers window.



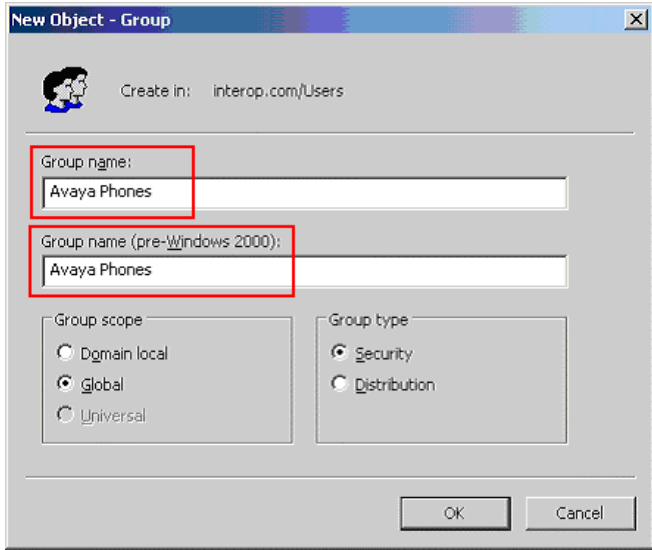
Step	Description
11.	<p>Select the Dial-in tab in the user properties window. Enable remote access by clicking on the Allow access radio button. Click OK to complete. Repeat this step for all Avaya IP Telephone and PC user IDs.</p> 

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

12. Create a new user Group by selecting **Action** → **New** → **Group** from the drop-down menu. The use of a Group facilitates the assignment and management of additional user IDs.

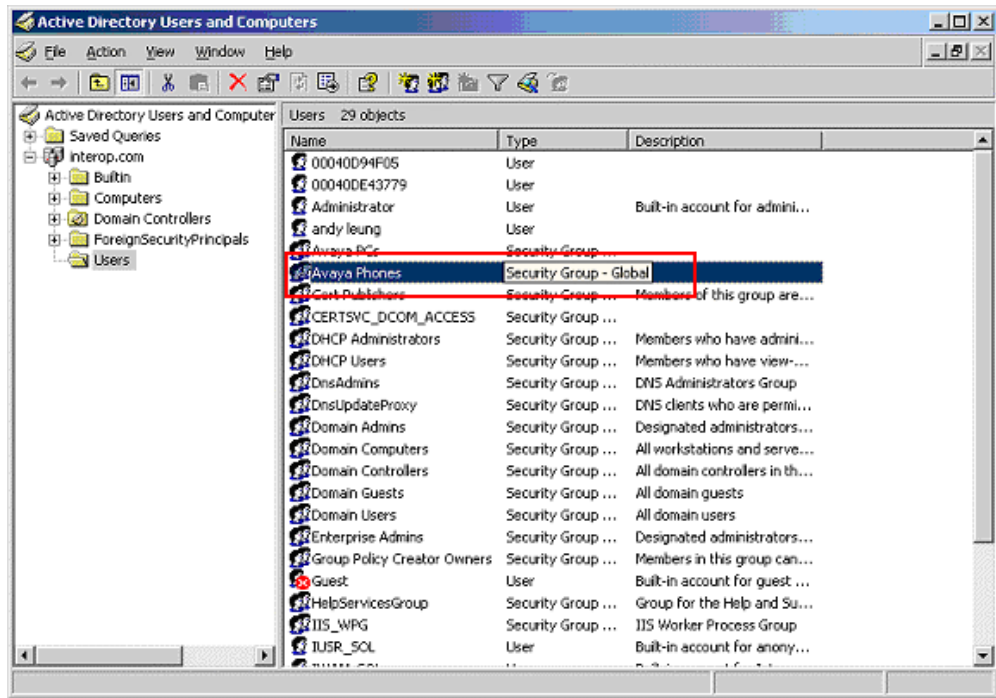


13. Create a group for Avaya IP Telephones. The sample network uses the name Avaya Phones for this group. Click **OK** to complete.

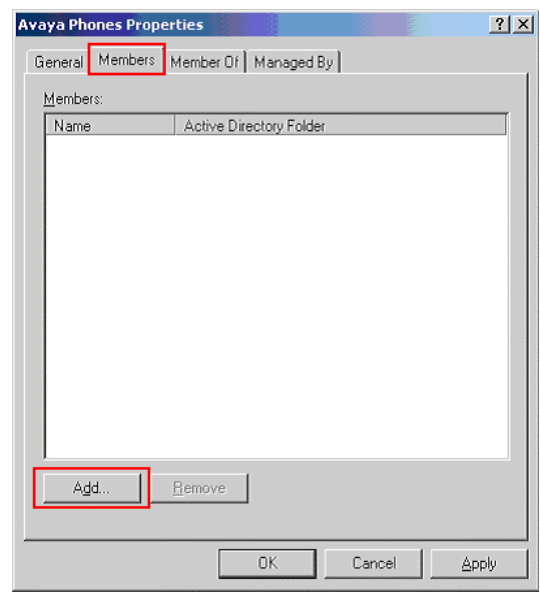


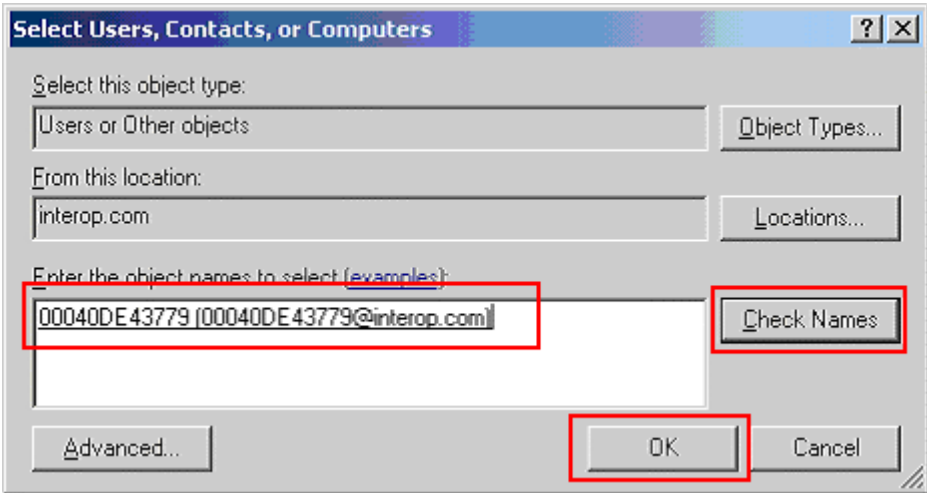
Step	Description
14.	Repeat Steps 12 and 13 to create another user Group for the PC.

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



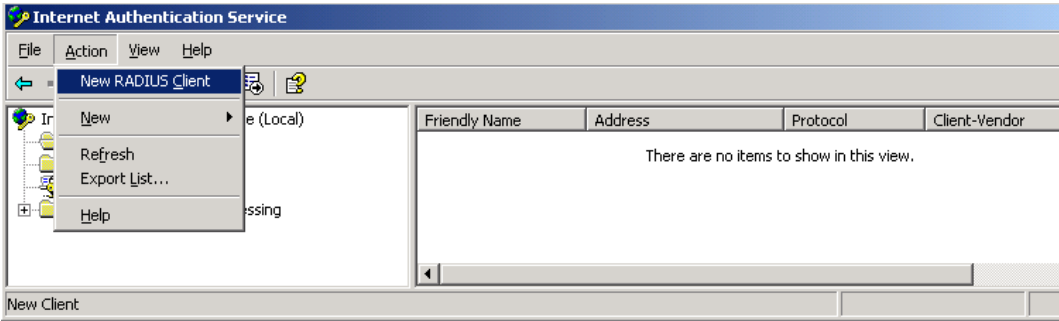
16. Select the **Members** tab in the group Properties window. Click **Add** to continue.

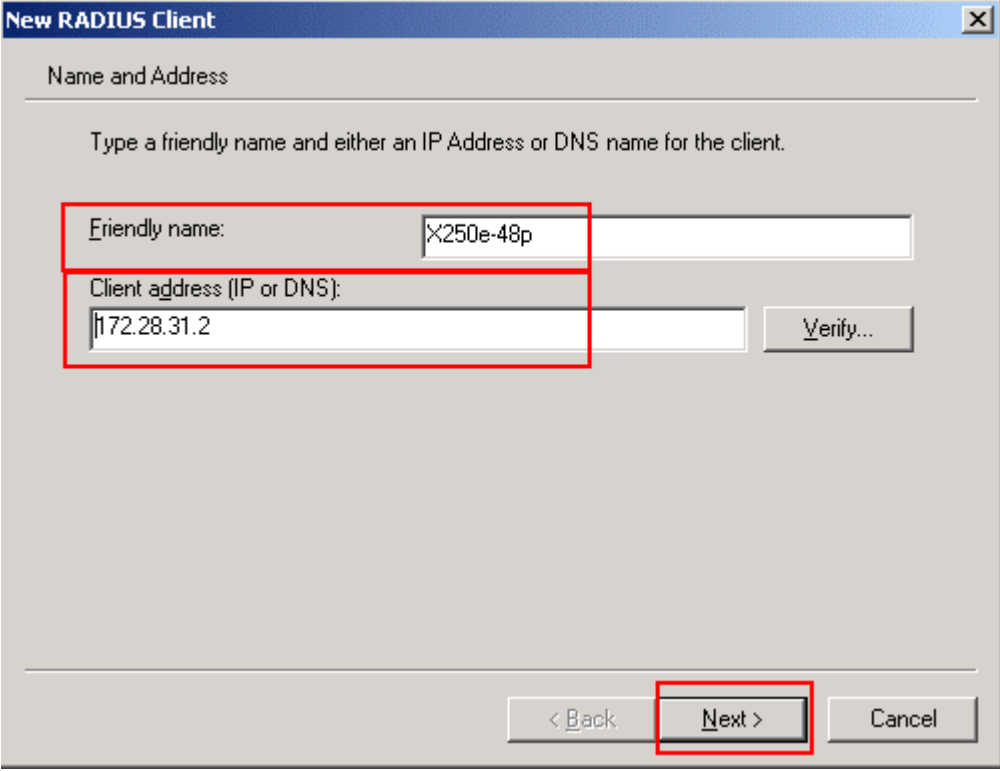


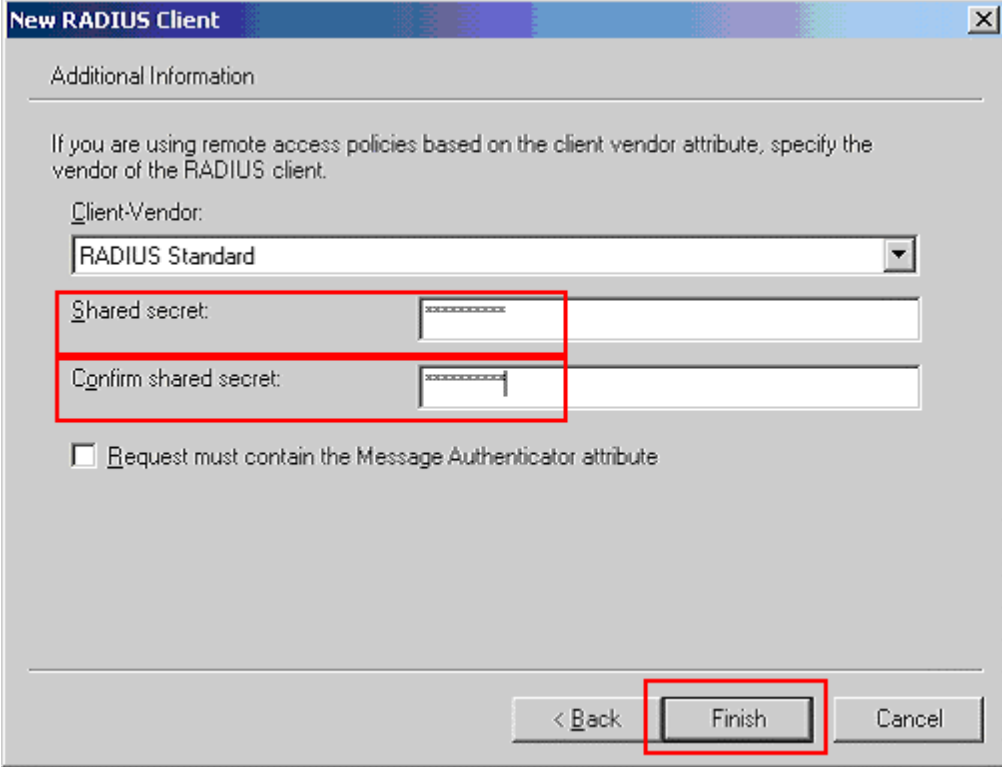
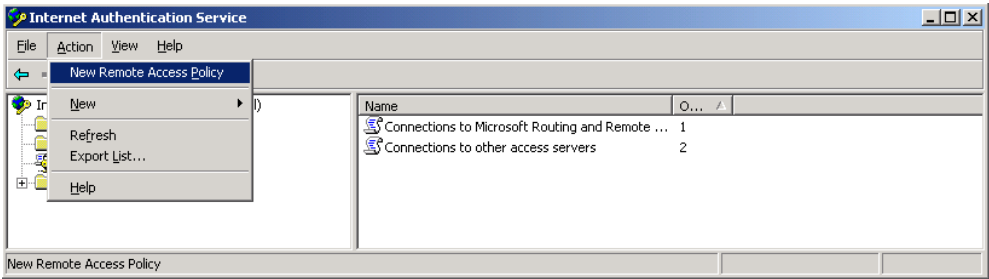
Step	Description
17.	<p>Enter the user ID that should be assigned to the Avaya Phones group. This should be the user ID for the Avaya IP Telephone. Use Check Names to assist in searching for the user ID. Click OK to complete.</p> 
18.	Repeat Steps 15-17 to add members to the PCs user group.

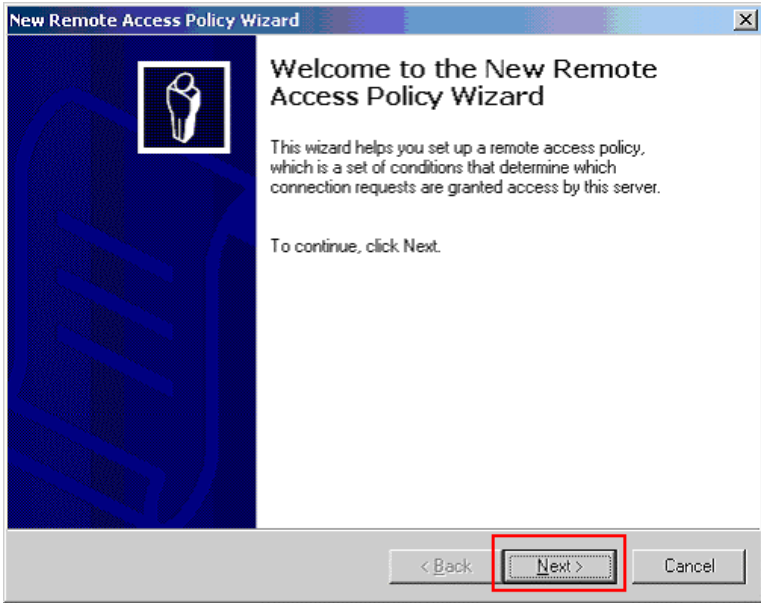
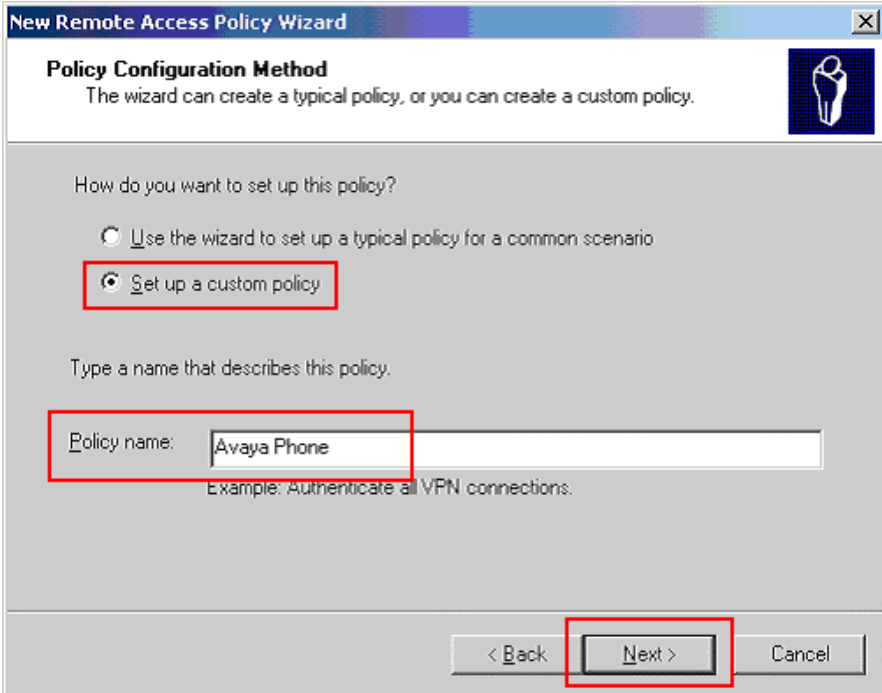
6.1. Configure Microsoft Internet Authentication Services (IAS) Server

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

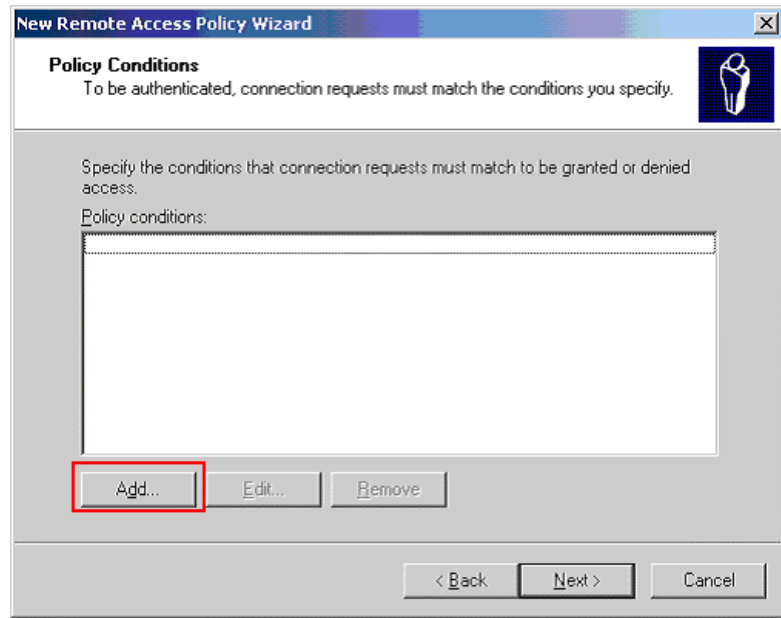
Step	Description
2.	<p>Enter the name and IP address of the X250e-48t switch to create a new RADIUS client. This must match the IP address configured in Section 4.1, Step 4. Click Next to continue.</p> 

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> 
4.	<p>Create a new access policy for the Avaya IP Telephones by clicking on Action → New Remote Access Policy.</p> 

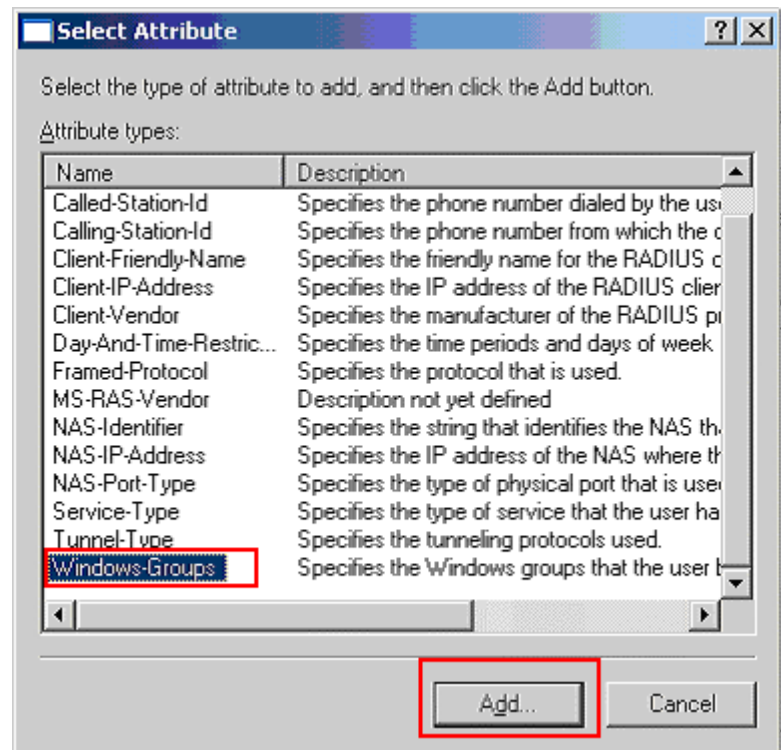
Step	Description
5.	<p>Click Next in the New Remote Access Policy Wizard.</p> 
6.	<p>Select Set up a custom policy radio button and enter a Policy name. The sample network uses the name Avaya Phone. Click Next to continue.</p> 


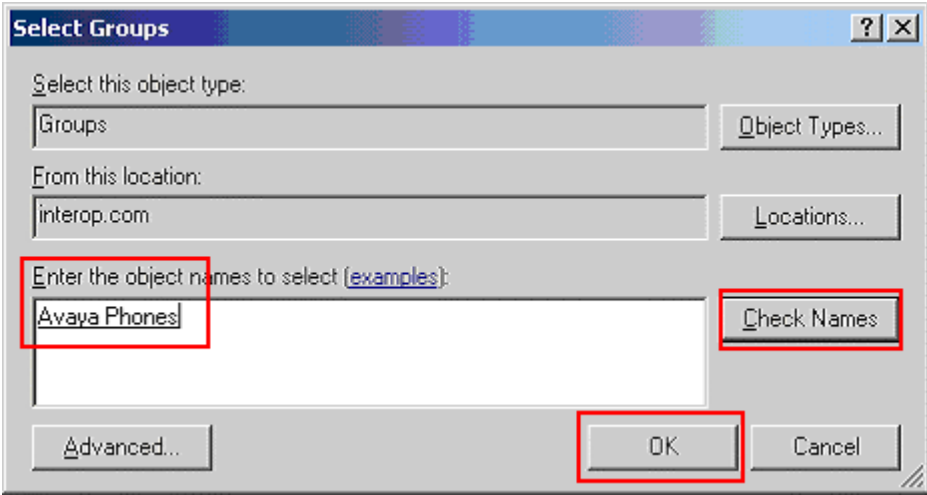
Step	Description
------	-------------

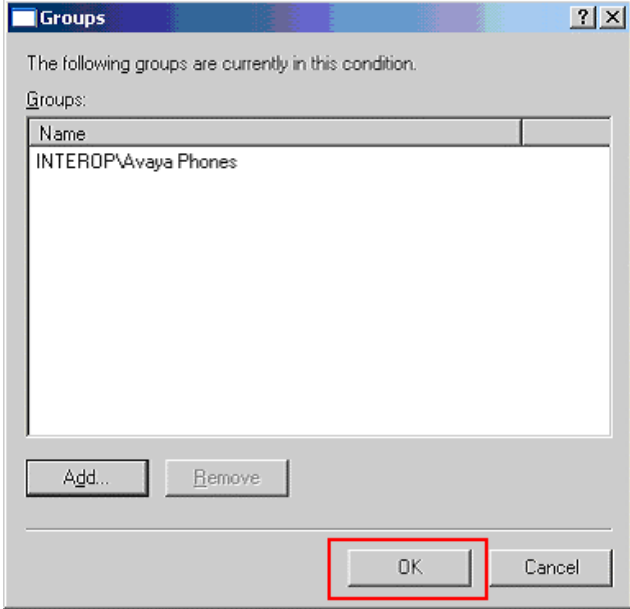
7. Click the Add button to add a new policy condition.



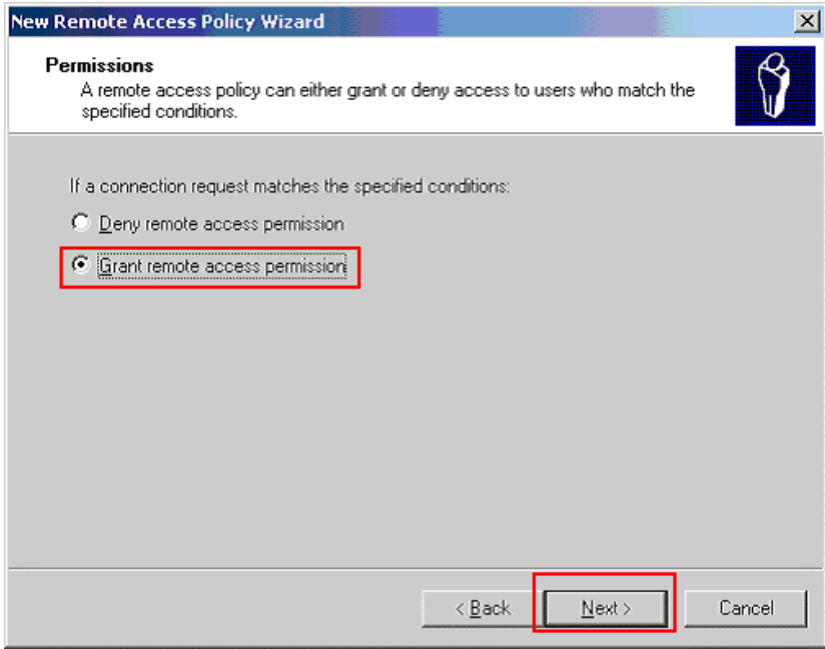
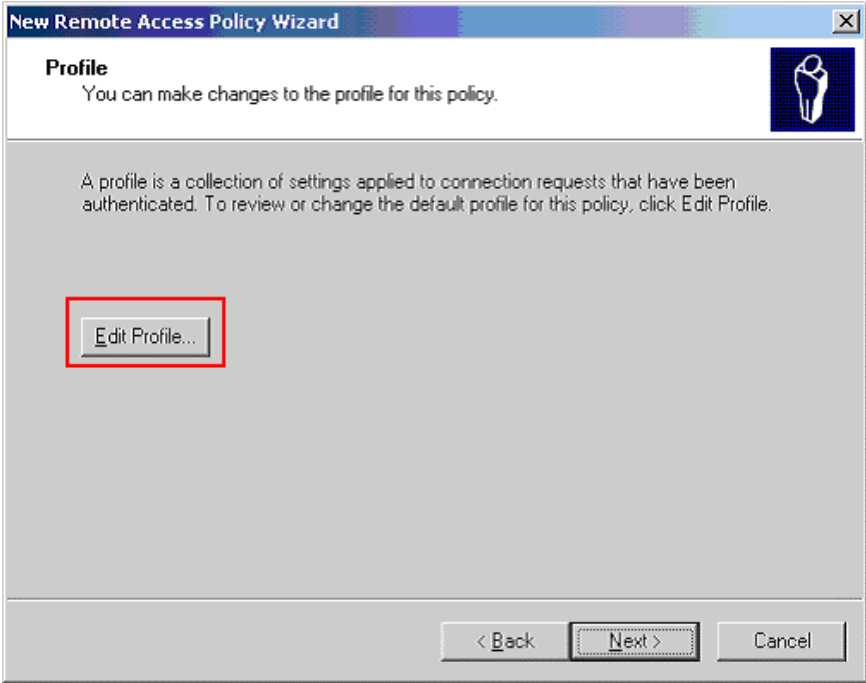
8. Highlight **Windows-Groups** from the Select Attribute pop-up window. Click **Add** to continue.

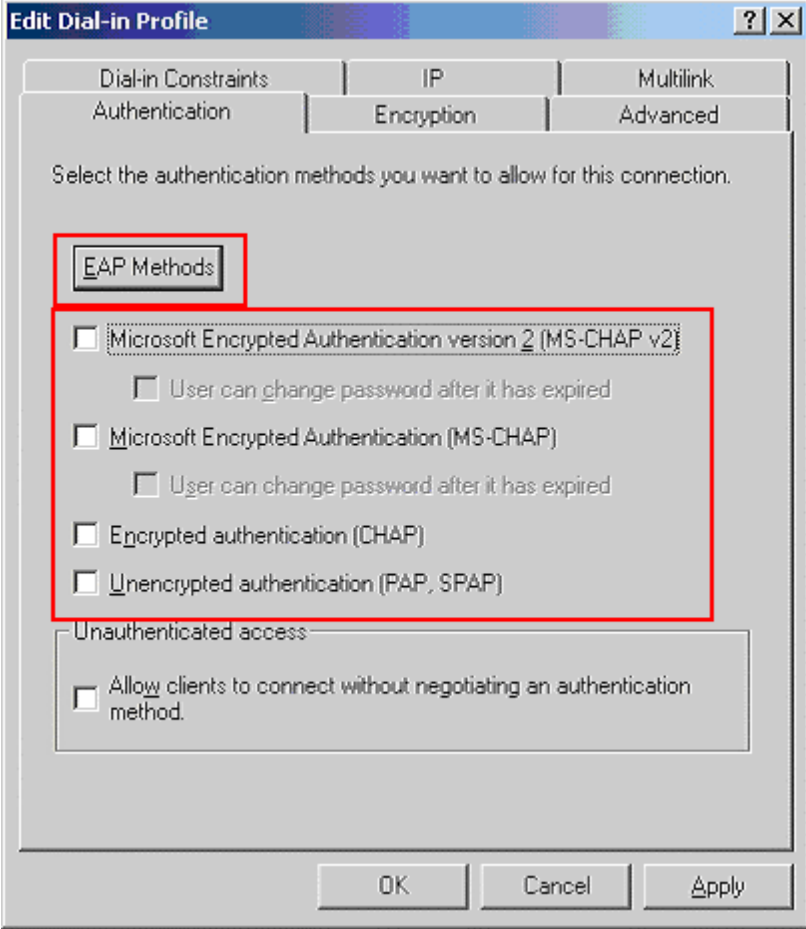


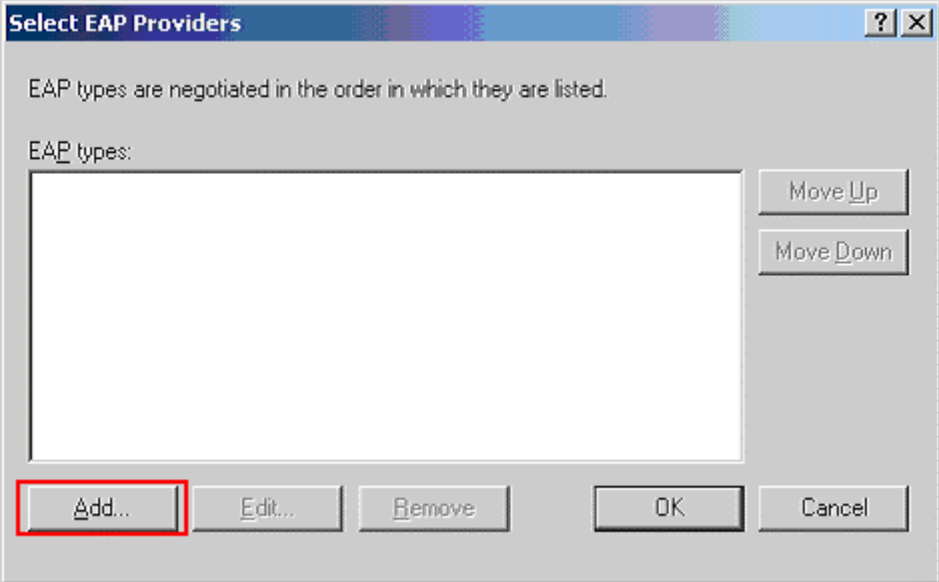
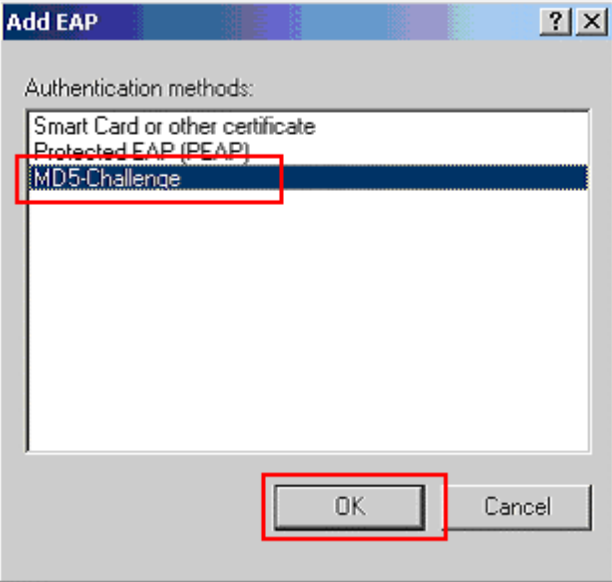
Step	Description
9.	<p>Click Add in the Groups pop-up window to add a Windows group.</p> 
10.	<p>Enter the Active Directory user group created in Section 5.1, Steps 12-13. Use Check Names to assist in searching for the user group. Click OK to complete.</p> 

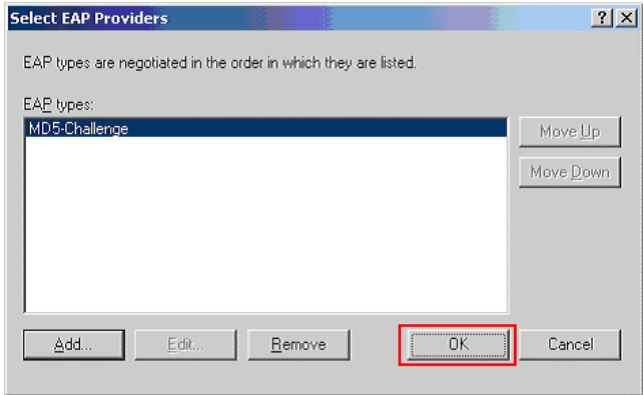
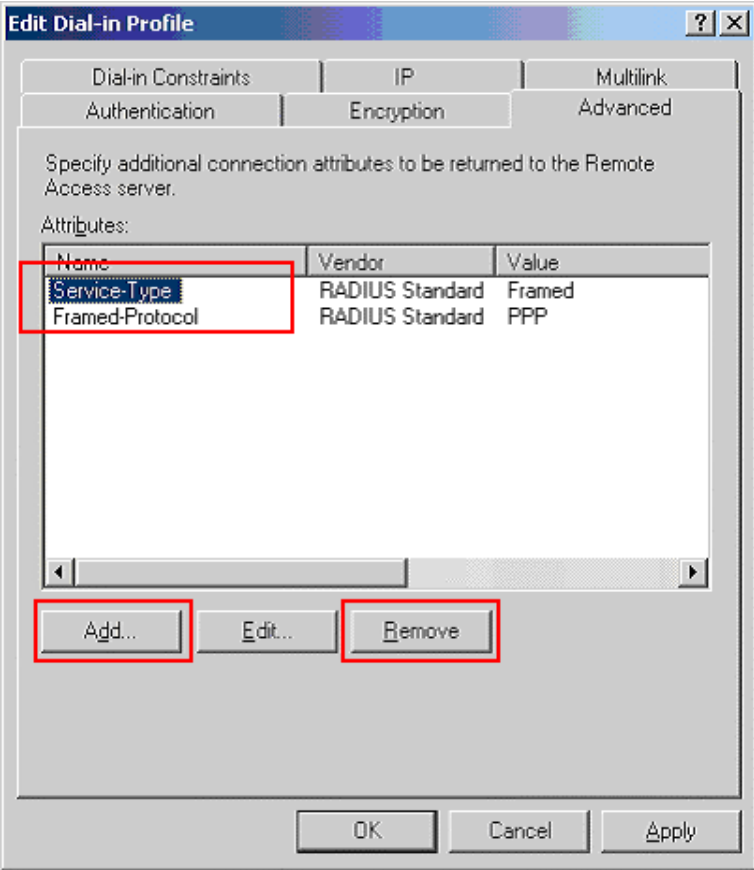
Step	Description
11.	<p data-bbox="326 233 1019 268">Click OK in the Groups pop-up windows to complete.</p> 

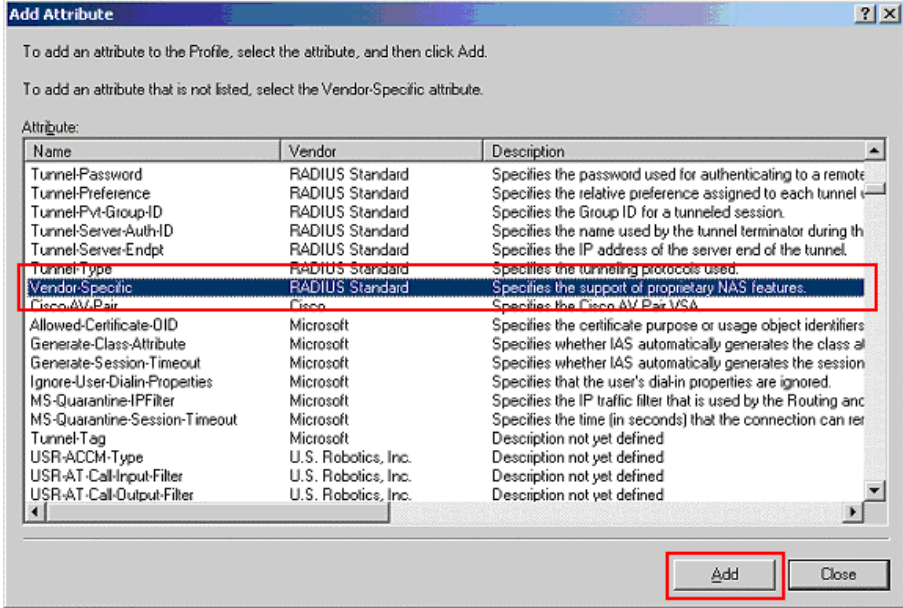
Step	Description
12.	<p>Once the Windows user group has been added via Steps 8-11, click Next to continue.</p>

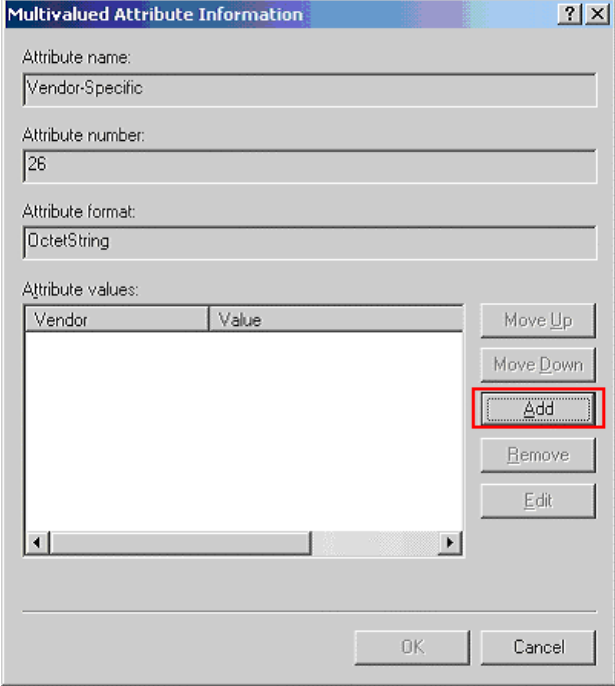
Step	Description
13.	<p>Click the Grant remote access permission radio button. Click Next to continue.</p> 
14.	<p>Click Edit Profile to configure the profile for this access policy. This will display the Edit Dial-in Profile pop-up window.</p> 

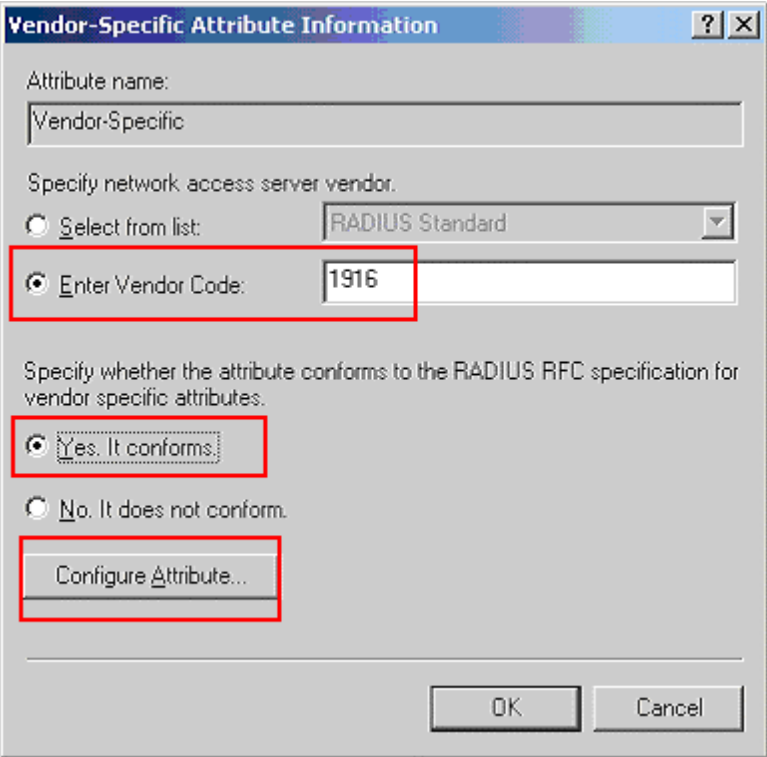
Step	Description
15.	<p>Select the Authentication tab in the Edit Dial-in Profile pop-up window. Uncheck all Microsoft authentication protocols as shown in the screen capture below. Click EAP Methods to continue. This will display the Select EAP Providers pop-up window.</p> 

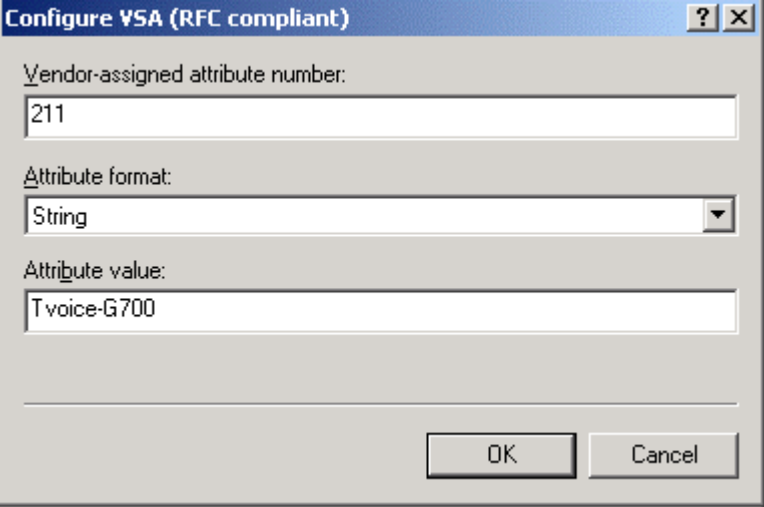
Step	Description
16.	<p>Click Add in the Select EAP Providers pop-up window to add a new EAP type.</p> 
17.	<p>Select MD5-Challenge in the Add EAP pop-up window. Click OK to continue.</p> 

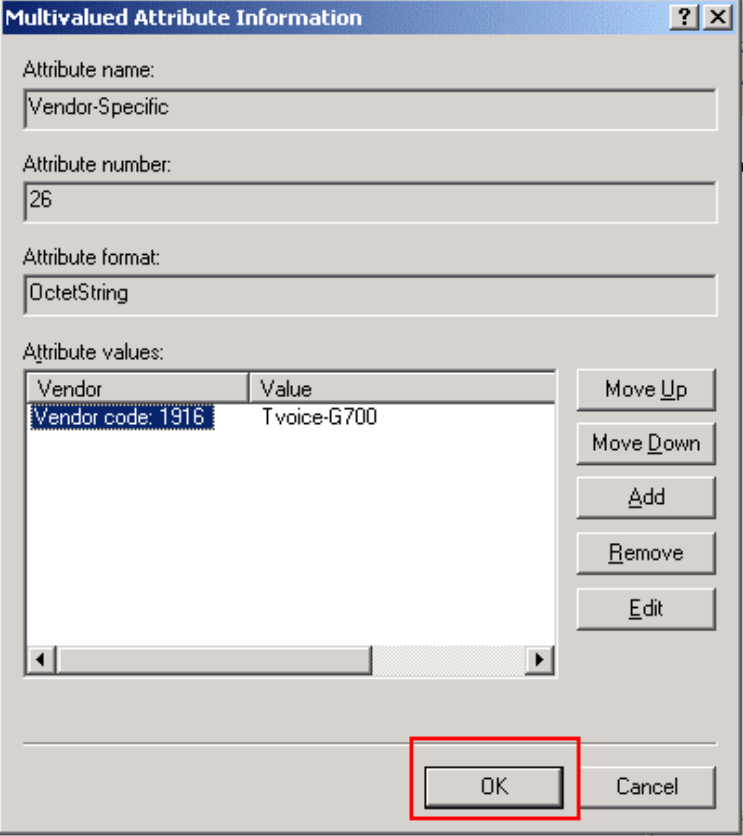
Step	Description
18.	<p>Once the MD5-Challenge EAP type is added, Click OK to complete the EAP authentication selection.</p> 
19.	<p>Select the Advanced tab in the Edit Dial-in Profile pop-up window. Highlight each existing attribute, then click Remove to delete it. Click Add after all existing attributes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

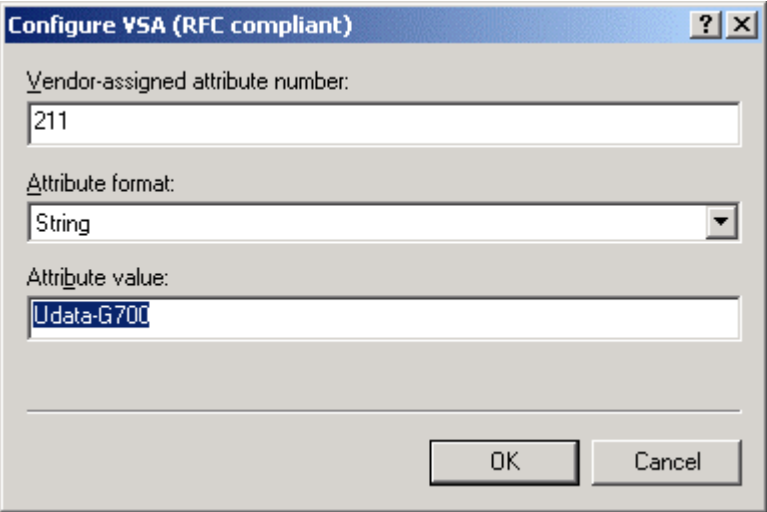
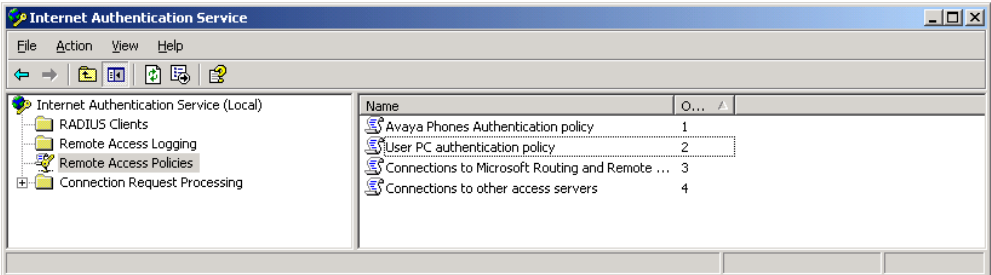
Step	Description																																																									
20.	<p>Highlight the Vendor Specific attribute name from the list of attributes displayed in the Add Attribute pop-up window. Click Add to continue. This will display the Multivalued Attribute Information pop-up window.</p>  <p>The screenshot shows a dialog box titled "Add Attribute" with a list of attributes. The "Vendor-Specific" attribute is selected. The "Add" button is highlighted with a red box.</p> <table border="1" data-bbox="418 514 1279 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-Priv-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-AVPair</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 and</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-Priv-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-AVPair	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 and	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-Priv-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-AVPair	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 and																																																								
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																																																								

Step	Description
21.	<p>Click Add 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 a dialog box titled "Multivalued Attribute Information". It contains several input fields: "Attribute name" with the text "Vendor-Specific", "Attribute number" with "26", and "Attribute format" with "OctetString". Below these is a table for "Attribute values" with columns "Vendor" and "Value". To the right of the table are buttons for "Move Up", "Move Down", "Add", "Remove", and "Edit". The "Add" button is highlighted with a red rectangular box. At the bottom of the dialog are "OK" and "Cancel" buttons.</p>

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-G700” 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> 

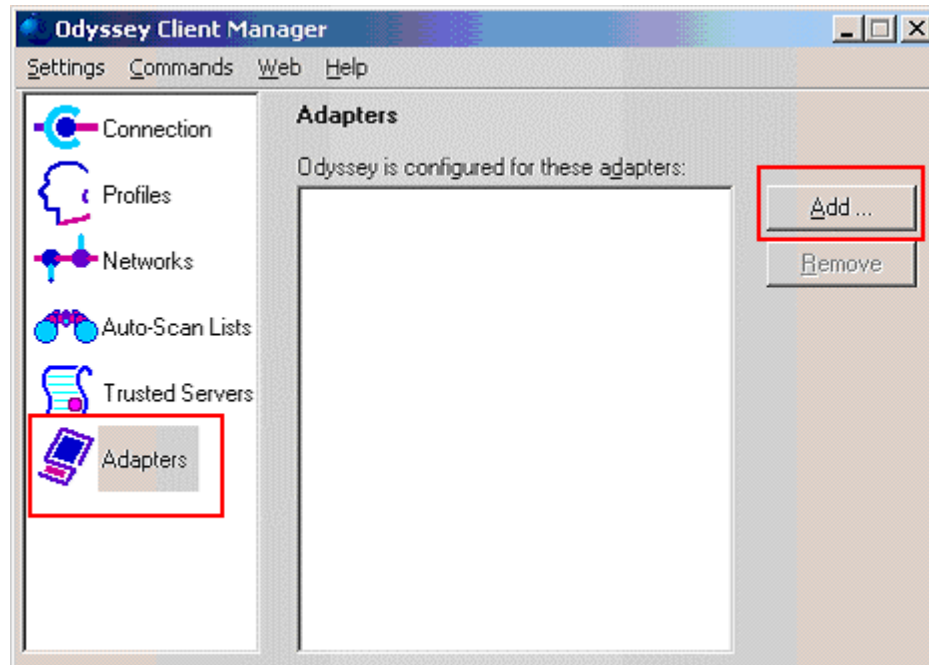
Step	Description
24.	<p>Once all attributes have been entered in Steps 21-24, click OK to continue.</p> 
25.	<p>Click OK on all preceding pop-up windows to complete the configuration of this access policy.</p>

Step	Description
26.	<p>Repeat Steps 4-23 to create a separate policy for a PC. The sample network uses the name User PC authentication policy for this new policy. Use the Udata-G700 value in lieu of what is in Step 24. The Udata-G700 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> 
27.	<p>After completing the above steps, there should be a total of 4 Remote Access Policies.</p> 

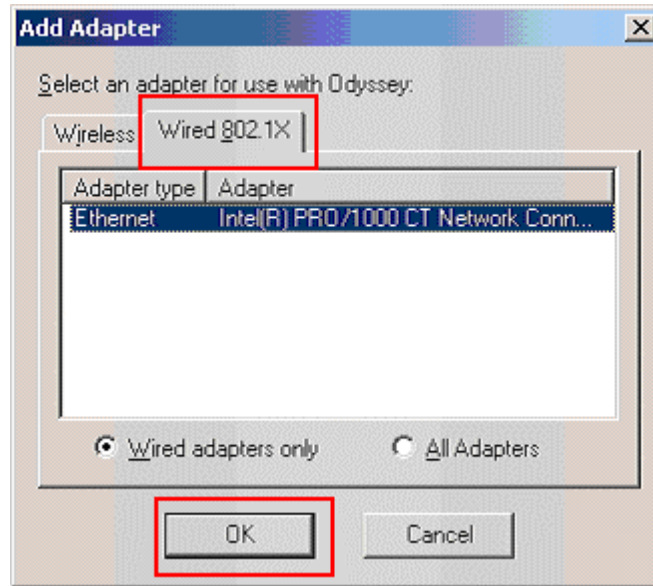
7. Configure the Odyssey client

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

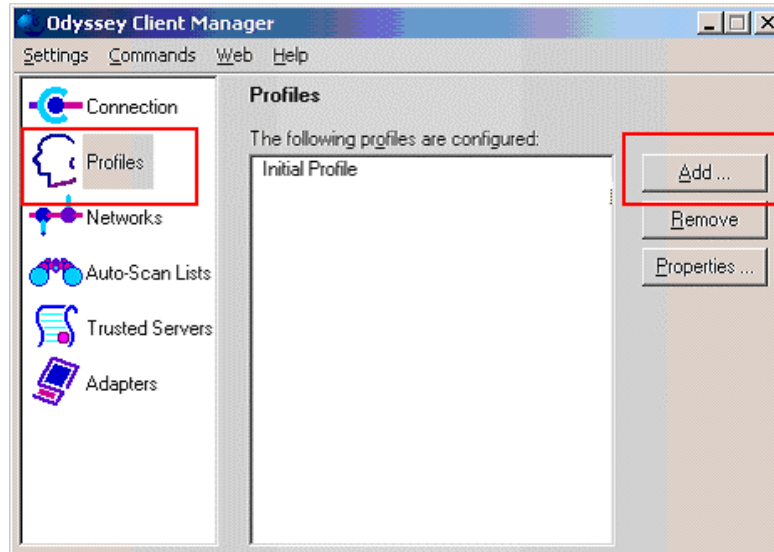
1. Start the Odyssey Client by clicking **Start > Programs > Juniper Networks > Odyssey Access Client > Odyssey Access Client Manager**. Add a network adapter by selecting **Adapters** on the left panel then click **Add** from the Odyssey Client Manager window.



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



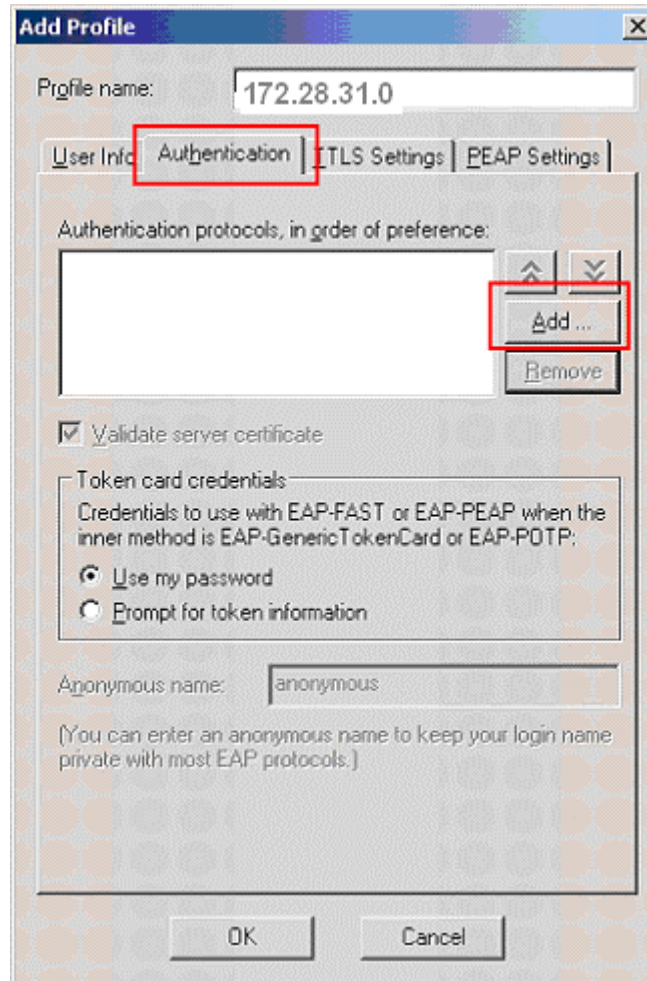
3. Add a profile by selecting **Profiles** on the left panel then click **Add** to continue.



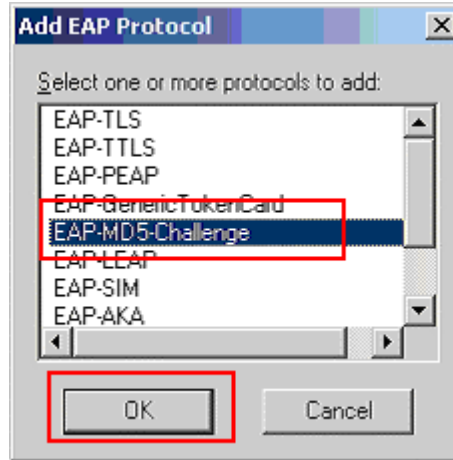
4. From the User Info tab in the Add Profile pop-up window. Enter the **Login name** and **password**. The Login name and password must match what was setup in Section 6 Step 5. Click on the **Authentication** tab to continue.

The screenshot shows the 'Add Profile' dialog box with the 'User Info' tab selected. The 'Profile name' field contains '172.28.31.0'. The 'Login name' field contains 'user1'. Under the 'Password' section, the 'Permit login using password' checkbox is checked. Below it, the 'use the following password' radio button is selected, and the password field contains '123456'. The 'Umask' checkbox is also checked. The 'Certificate' section has the 'Permit login using my certificate' checkbox unchecked. At the bottom, there are 'View ...' and 'Browse ...' buttons, and 'OK' and 'Cancel' buttons at the very bottom.

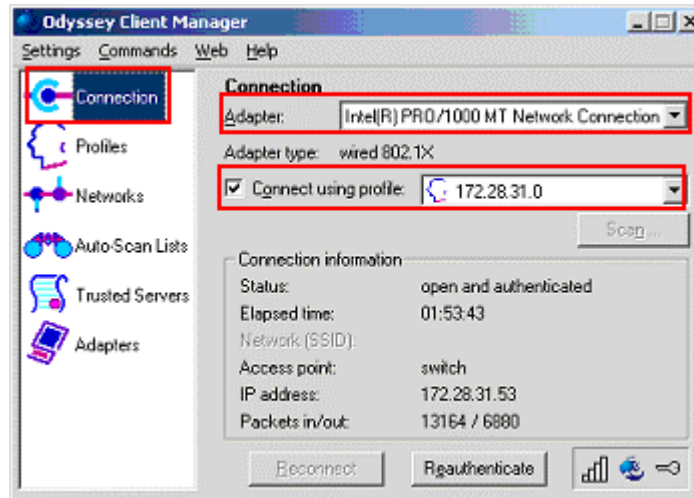
5. Under the **Authentication** tab, click **Add** to Add to add a new authentication protocol.



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-48t 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-48t 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 p-t w/Logoff 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
<p>1.</p>	<p>Add a new station for the Avaya IP Telephones to the Avaya Communication Manager using the add station command. Configure the following fields.</p> <ul style="list-style-type: none"> • Extension: <i>33004</i> (Extension number for the Avaya Telephone) • Type: <i>9630</i> (Avaya Telephone type used for this extension) • Port: <i>IP</i> (Type of connection for the Avaya Telephone) • Security Code: <i>1234</i> (Security code used by the Avaya Telephone to register with Avaya Communication Manager) • Direct IP-IP Audio Connections: <i>y</i> (Enable Shuffling) <p>The first two pages of the add station 33004 configuration are shown below. Repeat this step for each station.</p> <pre style="border: 1px solid black; padding: 10px;"> 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 Time of Day Lock Table: Speakerphone: 2-way Personalized Ringing Pattern: 1 Display Language: english Message Lamp Ext: 33004 Survivable GK Node Name: Mute Button Enabled? y Survivable COR: internal Button Modules: 0 Survivable Trunk Dest? y Media Complex Ext: IP SoftPhone? n Customizable Labels? y </pre>

Step	Description
2.	<p data-bbox="326 233 1360 338">Use the “display ip-network-region” command to display the 802.1P setting configured in the Avaya Communication Manager. Verify that both Call Control 802.1p Priority and Audio 802.1p priority are set to 6.</p> <pre data-bbox="326 373 1360 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-48t and X250e-24t 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 provisioning of Avaya 4600 and 9600 series IP Telephones
- Ethernet Automatic Protection Switching (EAPS)

10.2. Test Results

The Extreme Networks X250e-48t and X250e-24t 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 port <port #> qosmonitor” command on the Extreme switch to verify VoIP traffic is being transmitted by the correct priority queue.

```
X250e-48t.37 # show port 18 qosmonitor
Qos Monitor Req Summary                               Fri Apr 13 20:59:15 2007
Port  QP1    QP2    QP3    QP4    QP5    QP6    QP7    QP8
      Pkt    Pkt    Pkt    Pkt    Pkt    Pkt    Pkt    Pkt
      Xmts  Xmts  Xmts  Xmts  Xmts  Xmts  Xmts  Xmts
=====
18    308    0      0      0      0      0      5392   13
```

- Use the “show stpd <stpd domain>” command on the Extreme switches to verify the operation of the spanning tree protocol.

```
X250e-48t # show stpd s0
Stpd: s0                               Stp: ENABLED           Number of Ports: 2
Rapid Root Failover: Disabled
Operational Mode: 802.1D                Default Binding Mode: 802.1D
802.1Q Tag: (none)
Ports: 2,3
Participating Vlans: data-G700,Default,voice-G700
Auto-bind Vlans: Default
Bridge Priority: 32768
BridgeID:                               80:00:00:04:96:26:68:6b
Designated root:                        80:00:00:04:0d:7d:d3:ff
RootPathCost: 19                        Root Port: 3
MaxAge: 20s                             HelloTime: 2s          ForwardDelay: 15s
CfgBrMaxAge: 20s                         CfgBrHelloTime: 2s    CfgBrForwardDelay: 15s
Topology Change Time: 35s                Hold time: 1s
Topology Change Detected: FALSE           Topology Change: FALSE
Number of Topology Changes: 6
Time Since Last Topology Change: 1854s
```

- Use the “show radius” command on the X250e-48t and X250e-24t 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-48t # 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
  Access Requests  : 2
  Access Rejects   : 0
  Access Retransmits: 0
  Bad authenticators: 0
  Round Trip Time  : 0
  Access Accepts   : 1
  Access Challenges : 1
  Client timeouts  : 0
  Unknown types    : 0

```

- Use the “show netlogin” command on the X250e-48t and X250e-24t 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-48t # 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
<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
-----

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-48t # 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-48t and X250e-24t switch has the correct 802.1P to QoS Profile assignment.

```
X250e-48t # 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-48t and X250e-24t 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.