Avaya Solution & Interoperability Test Lab

Configuring Extreme Networks Summit X350-24t Switch to support Avaya Server, Avaya Media Gateway and Avaya IP Telephones – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Extreme Networks Summit X350-24t switch to support an Avaya VoIP solution consisting of Avaya Server, Avaya Media Gateway and Avaya IP Telephones in network composed of both Extreme Network switches, and Avaya Converged Stackable Switches. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring the Extreme Networks Summit X350-24t switch to support an Avaya Voice over IP (VoIP) solution consisting of Avaya S8500 Server, Avaya G650 Media Gateway, and Avaya IP Telephones in a three-node network composed of Avaya C363T-PWR Converged Stackable Switch, Summit X350-24t and BlackDiamond 12k.

The 3 switches are connected to each other in a full mesh topology. 802.1D spanning tree protocol is configured in all three switches as a layer-2 loop avoidance mechanism. Avaya S8500 Server and Avaya G650 Media Gateway are directly connected into a switch within the cloud and an Avaya IP Telephones are connected to the X350 switch.

Microsoft Internet Authentication Service (IAS) is used to provide 802.1X RADIUS authentications for Avaya IP Telephone and the PCs that are connected into the X350-24t switch. The Avaya IP Telephone and PCs are individually authenticated through the X350-24t switch by the IAS via the X350-24t'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 X350 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-G650" VLAN with IP network 172.28.10.0/24, and the "data-G650" VLAN with IP network 172.28.11.0/24 are used in the sample network. The X350-24t does not support Power over Ethernet (PoE), therefore the Avaya 4610 IP Telephones are connected into the switch through a power supply not shown.

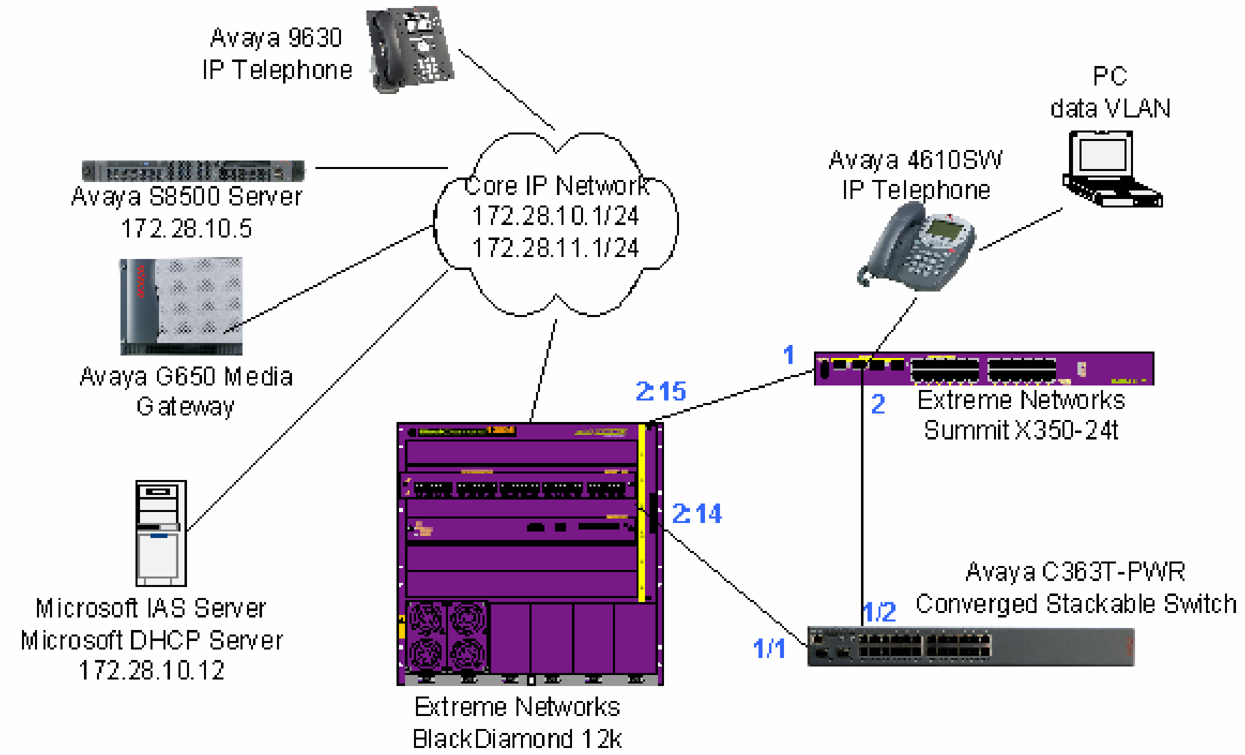


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Server with G650 Media Gateway	Avaya Communication Manager R5.0 (R015x.00.0.825.4)
Avaya 9630 IP Telephone	R 1.5
Avaya 4610SW IP Telephone	R2.8.3
Avaya C363T-PWR Converged Stackable Switch	SW Version 4.5.14
Extreme Networks Summit X350-24t	ExtremeXOS 12.0.3.16
Extreme Networks BlackDiamond 12804	ExtremeXOS 12.0.1.11
Microsoft Windows running	2003 Server Enterprise Edition
Active Directory Users and Computers	5.2.3790.1830
Internet Authentication Service	5.2.3790.1830
DHCP Server	5.2.3790.1830

4. Configure Extreme Networks equipment

This section describes the configuration for Extreme Network as shown in **Figure 1**.

4.1. Configure the X350-24t

This section shows the necessary steps in configuring the X350-24t as shown in **Figure 1**.

Step	Description

1.	Connect to the X350-24t switch and log in using appropriate credential.
	
	`login: username`
	`password: xxxxxx`

Step	Description

2.	Create VLANs on the switch. The IP address assignment is optional. All routing is performed by the BlackDiamond 12k switch which has the IP address 172.28.10.1 and 172.28.11.1 for the voice-G650 and data-G650 VLAN respectively. The “temp” VLAN is used as a temporary VLAN used for 802.1X authentication.
	Note: It is important to precede the voice VLAN name with “voice” as it is a required keyword for Avaya IP Telephone to recognize the appropriate voice VLAN.
	`X350-24t # create vlan voice-G650`
	`X350-24t # config vlan voice-G650 tag 10`
	`X350-24t # config vlan voice-G650 ipaddress 172.28.10.2/24`
	`X350-24t # create vlan data-G650`
	`X350-24t # config vlan data-G650 tag 11`
	`X350-24t # config vlan data-G650 ipaddress 172.28.11.2/24`
	`X350-24t # create vlan temp`

3.	Configure VLAN assignment for the ports.
	Note: The VLAN assignment for the user port is dynamically assigned after Avaya IP Telephone or user has been authenticated, therefore it is not necessary to configure at this time.
	`X350-24t # config vlan default add port 1,2 untagged`
	`X350-24t # config vlan voice-G650 add port 1,2 tagged`
	`X350-24t # config vlan data-G650 add port 1,2 tagged`

4.	Configure a default route for the switch. `X350-24t # configure iproute add default 172.28.11.1 vr vr-default`

5.	Configure spanning tree protocol. The sample network uses the default spanning tree domain s0 (stpd) which by default configured for 802.1d.
	`X350-24t # config stpd "s0" add vlan "voice-G650" ports 1,2 dot1d`
	`X350-24t # config stpd "s0" add vlan "data-G650" ports 1,2 dot1d`
	`X350-24t # enable stpd s0`

Step	Description

6.	Enable and configure LLDP advertisement for the switch port. The call-server and file-server configuration is used by Avaya IP Telephone to register with and obtain setting information from.
	`X350-24t #` ***`configure lldp port 15 advertise vendor-specific dot1 vlan-name`***
	`X350-24t #` ***`configure lldp port 15 advertise vendor-specific avaya-extreme call-server 172.28.10.7`***
	`X350-24t #` ***`configure lldp port 15 advertise vendor-specific avaya-extreme file-server 172.28.10.12`***
	`X350-24t #` ***`configure lldp port 15 advertise vendor-specific avaya-extreme dot1q-framing tagged`***
	`X350-24t #` ***`enable lldp ports 15`***

7.	Configure 802.1X authentication for the switch and user ports. The shared-secret must match what is configured in IAS in **Section 6.2**, **Step 3**.
	`X350-24t #` ***`configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.11.2 vr VR-Default`***
	`X350-24t #` ***`configure radius netlogin primary shared-secret 1234567890`***
	`X350-24t #` ***`configure netlogin vlan temp`***
	`X350-24t #` ***`enable radius netlogin`***
	`X350-24t #` ***`enable netlogin dot1x`***
	`X350-24t #` ***`enable netlogin ports 15 dot1x`***

8.	Configure QoS profile for Avaya VoIP traffic. The X350 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**.
	`X350-24t #` ***`create qosprofile QP6`***
	`X350-24t #` ***`configure dot1p type 6 qosprofile QP6`***

9.	Save the above configuration. `X350-24t #` ***`save`***

4.2. Configure the BlackDiamond 12k

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

Step	Description

1.	Connect to the X350-24t switch and log in using appropriate credential.
	`login:` ***`username`***
	`password:` ***`xxxxxx`***

Step	Description

2.	Create the VLANs on the switch. The IP address assignment is optional. All routing is performed another switch within the cloud which has the IP address 172.28.10.1 and 172.28.11.1 for the voice-G650 and data-G650 VLAN respectively. The “temp” VLAN is used as a temporary VLAN used for 802.1X authentication.
	
	Note: It is important to precede the voice VLAN name with “voice” as it is a required keyword.
	
	`BD12k #` ***`create vlan voice-G650`***
	`BD12k #` ***`config vlan voice-G650 tag 10`***
	`BD12k #` ***`config vlan voice-G650 ipaddress 172.28.10.1/24`***
	`BD12k #` ***`enable ipforwarding voice-G650`***
	`BD12k #` ***`create vlan data-G650`***
	`BD12k #` ***`config vlan data-G650 tag 11`***
	`BD12k #` ***`config vlan data-G650 ipaddress 172.28.11.1/24`***
	`BD12k #` ***`enable ipforwarding data-G650`***
	`BD12k #` ***`create vlan temp`***

3.	Configure VLAN assignment for the ports.
	
	Note: The VLAN assignment for the user port is dynamically assigned after Avaya IP Telephone or user has been authenticated, therefore it is not necessary to configured at this time.
	
	`BD12k #` ***`config vlan default add port 2:14-15 untagged`***
	`BD12k #` ***`config vlan voice-G650 add port 2:14-15 tagged`***
	`BD12k #` ***`config vlan data-G650 add port 2:14-15 tagged`***

4.	Configure spanning tree protocol. The sample network uses the default spanning tree domain s0 (stpd) which by default configured for 802.1d.
	
	`BD12k #` ***`config stpd "s0" add vlan "voice-G650" ports 2:14-15`***
	`dot1d`
	`BD12k #` ***`config stpd "s0" add vlan "data-G650" ports 2:14-15 dot1d`***
	`BD12k #` ***`enable stpd s0`***

10.	Save the above configuration. `BD12k #` ***`save`***

5. Configure the Avaya C363T-PWR Converged Stackable Switch

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

1.	Log in to the Avaya C363T-PWR Converged Stackable Switch using the appropriate credential. Login: ***username*** Password: ***xxxxxx***

2.	Create the VLANs on the switch.
	Note: VLAN c1 must be created in order for the EAPS ring to function successfully.
	`C360-1(super)# set vlan 10 name voice-G650`
	`C360-1(super)# set vlan 11 name data-G650`

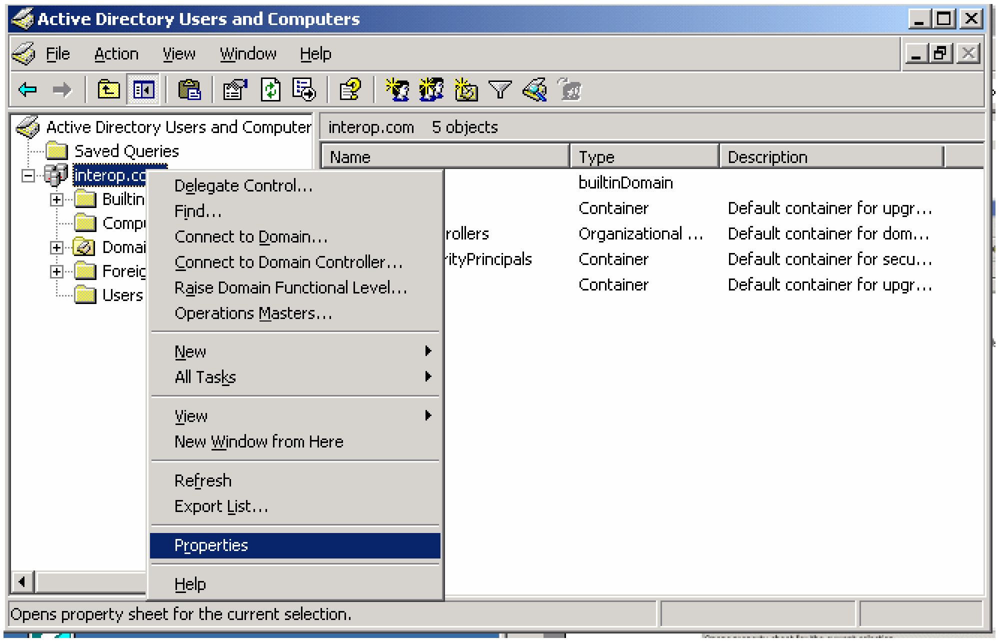
3.	Configure VLAN assignment for the ports.
	`C360-1(super)# set port vlan 10 1/1-1/2`
	`C360-1(super)# set trunk 1/1,1/2 dot1q`
	`C360-1(super)# set port vlan-binding-mode 1/1,1/2 bind-to-configured`

6. Configure Microsoft services

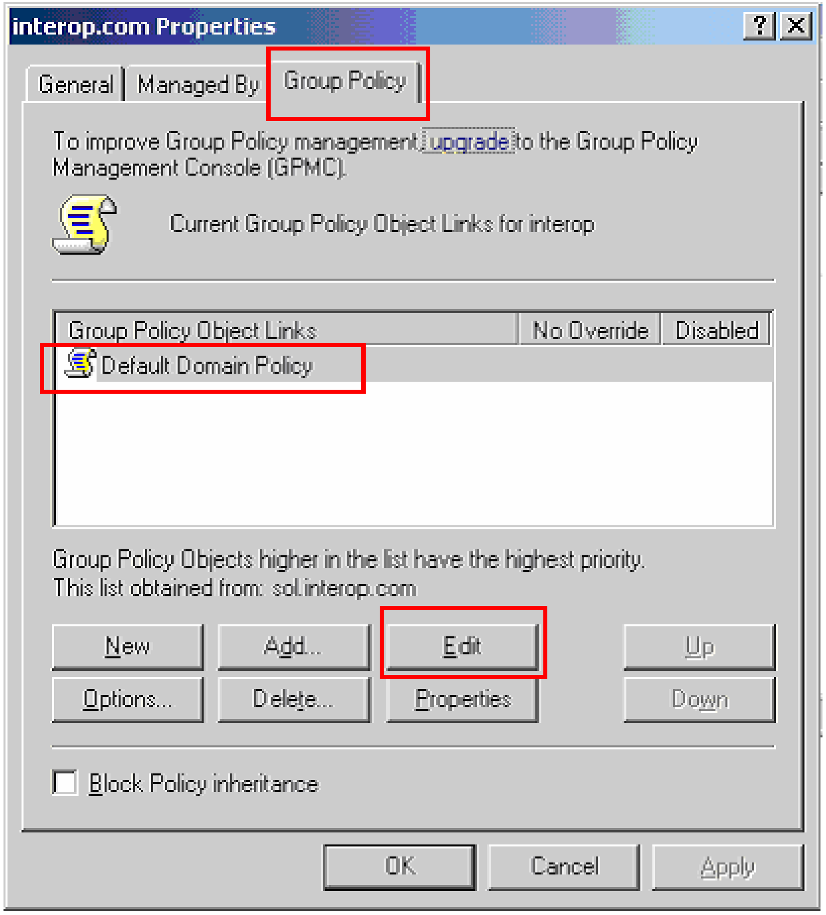
Active Directory Service and Internet Authentication Service are used in the sample network. The following sub-section will shows the steps in configuring these two services

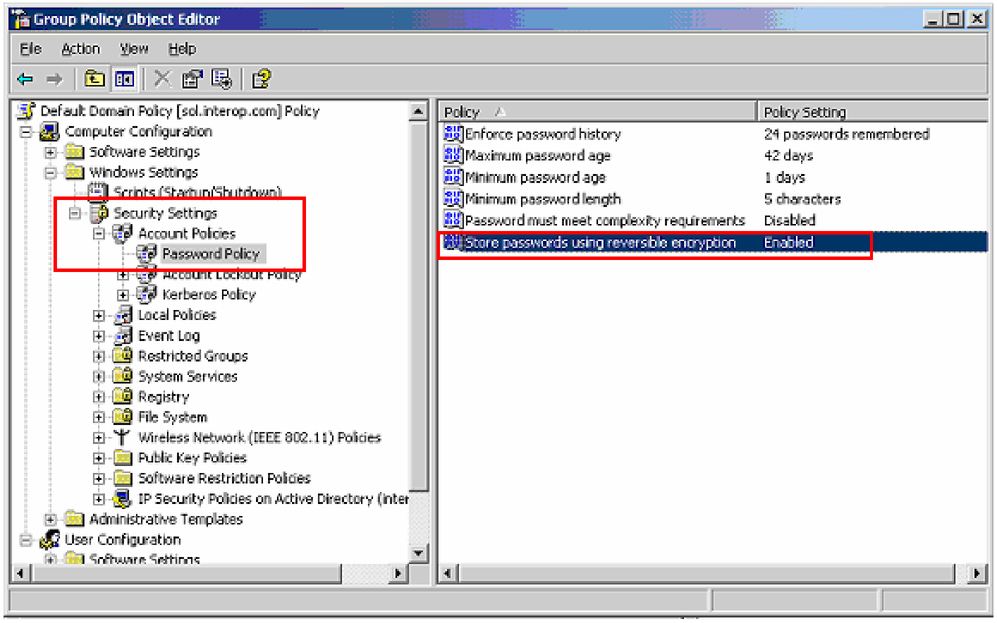
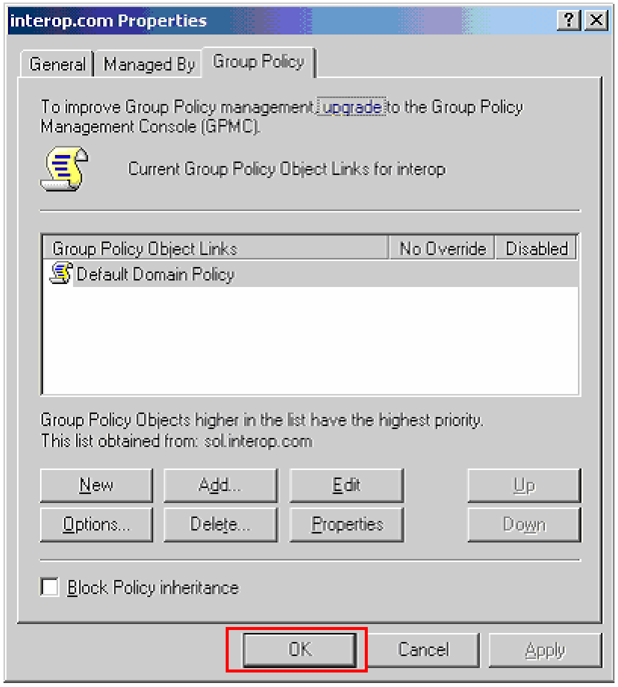
6.1. Configure Microsoft Active Directory Service

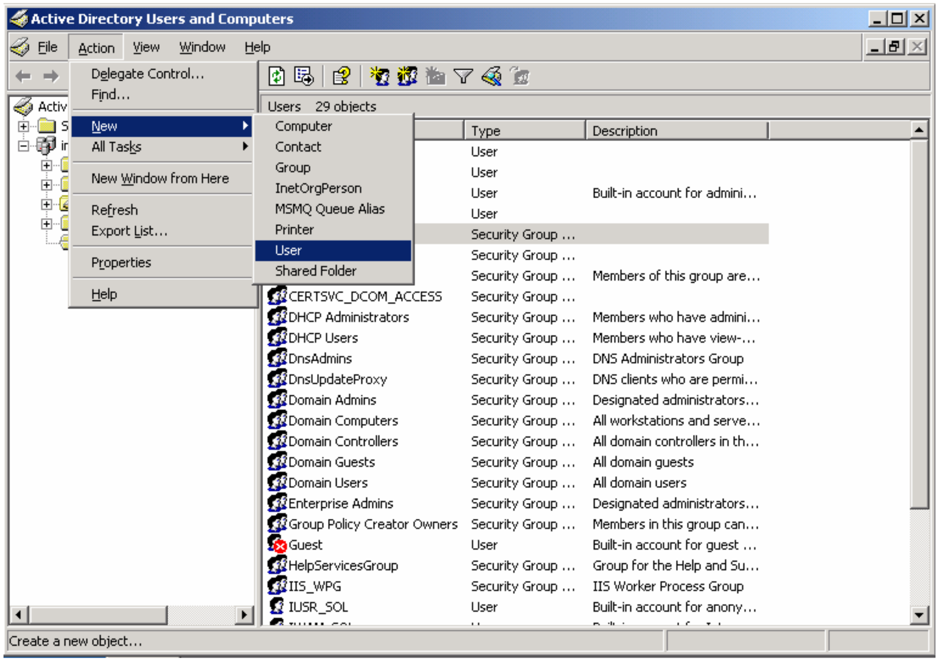
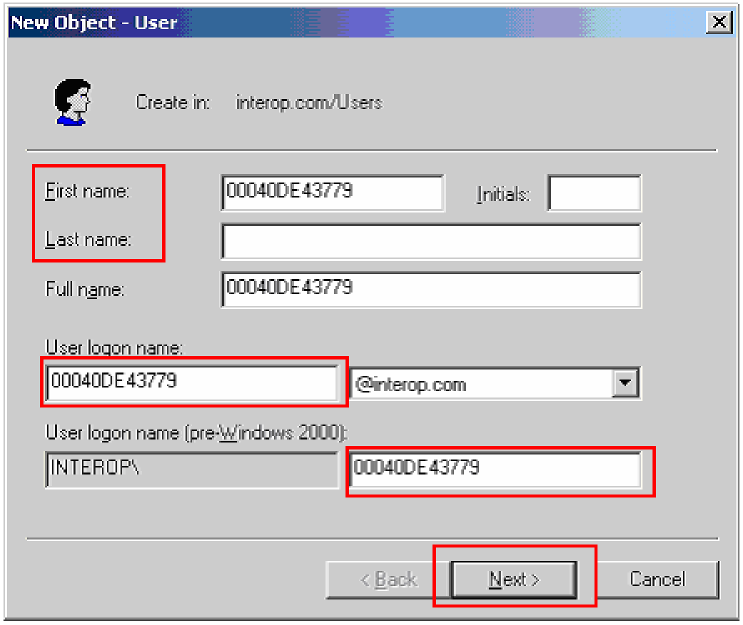
This section shows the necessary steps in configuring the Microsoft Active Directory server as shown in the **Figure 1** to support the Avaya IP Telephones and PC.

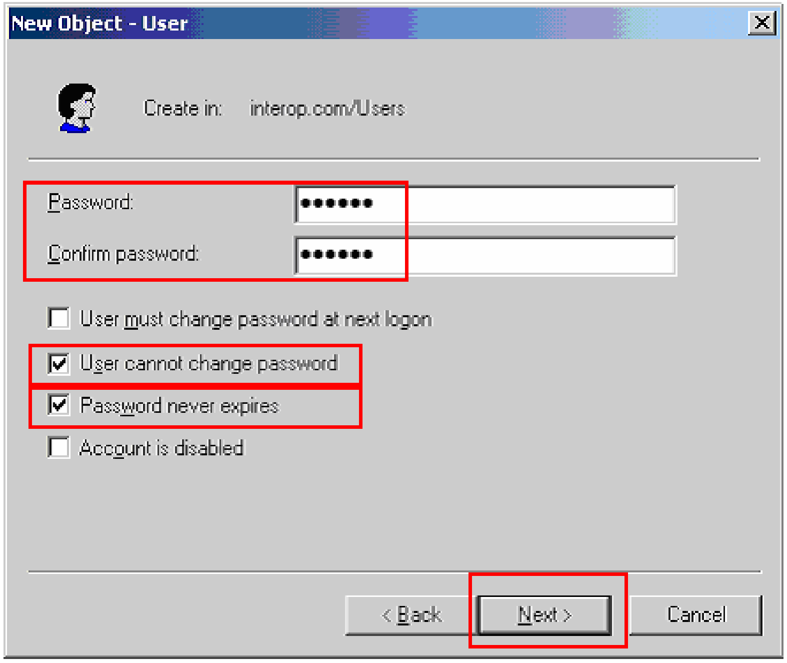
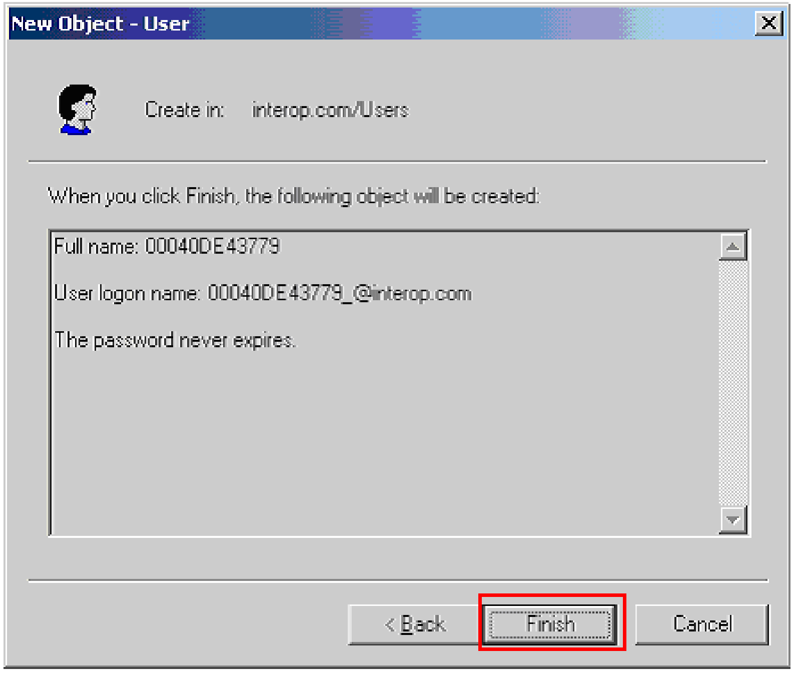
Step	Description
1.	Invoke the Active Directory Users and Computers window under Administrative Tools of a Microsoft Windows system. Configure the active directory domain properties by highlighting the Active Directory domain then right click and select **Properties**. 

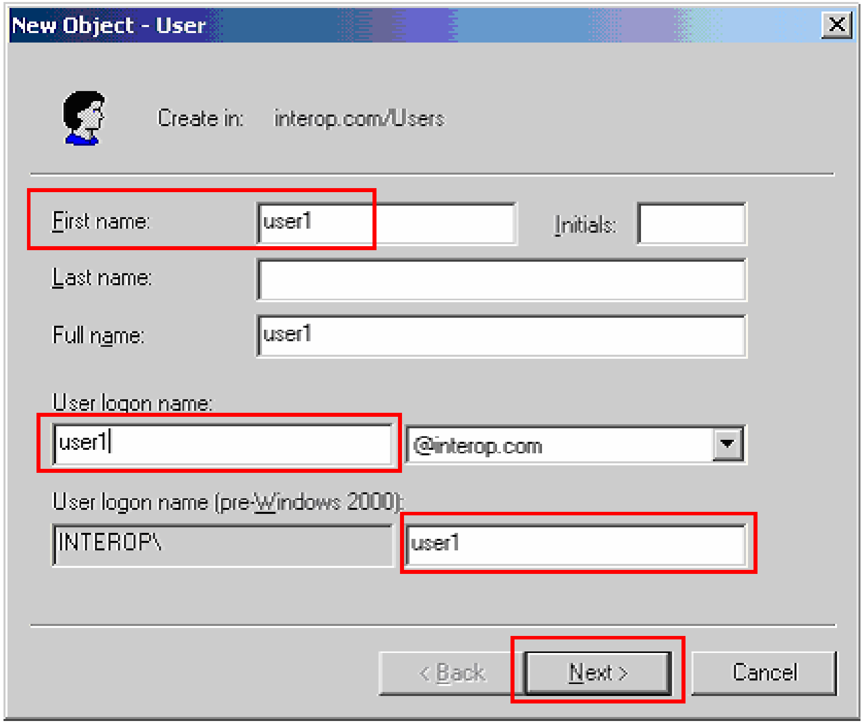
Opens property sheet for the current selection.

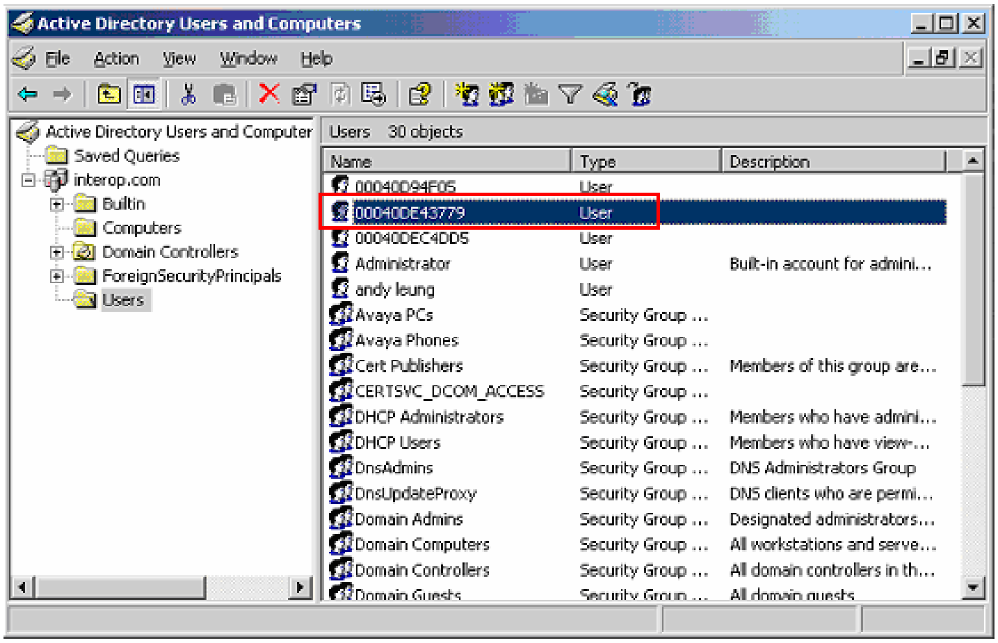
Step	Description
2.	Select the **Group Policy** tab in the properties window. Highlight the **Default Domain Policy** then click **Edit** to display the Group Policy Object Editor.  interop.com Properties General Managed By Group Policy New Add... Edit Up Options... Delete... Properties Down OK Cancel Apply To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC). Current Group Policy Object Links for interop Group Policy Object Links | No Override | Disabled Default Domain Policy Group Policy Objects higher in the list have the highest priority. This list obtained from: sol.interop.com □ Block Policy inheritance

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**.  Group Policy Object Editor File Action View Help Default Domain Policy [sol.interop.com] Policy Computer Configuration Software Settings Windows Settings Scripts (Startup/Shutdown) Security Settings Account Policies Password Policy Account Lockout Policy Kerberos Policy Local Policies Event Log Restricted Groups System Services Registry File System Wireless Network (IEEE 802.11) Policies Public Key Policies Software Restriction Policies IP Security Policies on Active Directory (inter Administrative Templates User Configuration Software Settings 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
4.	Click **OK** on the domain properties pop-up window to complete.  interop.com Properties General Managed By Group Policy To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC). Current Group Policy Object Links for interop Group Policy Object Links — No Override — Disabled Default Domain Policy Group Policy Objects higher in the list have the highest priority. This list obtained from: sol.interop.com New Add... Edit Up Options... Delete... Properties Down ☐ Block Policy inheritance

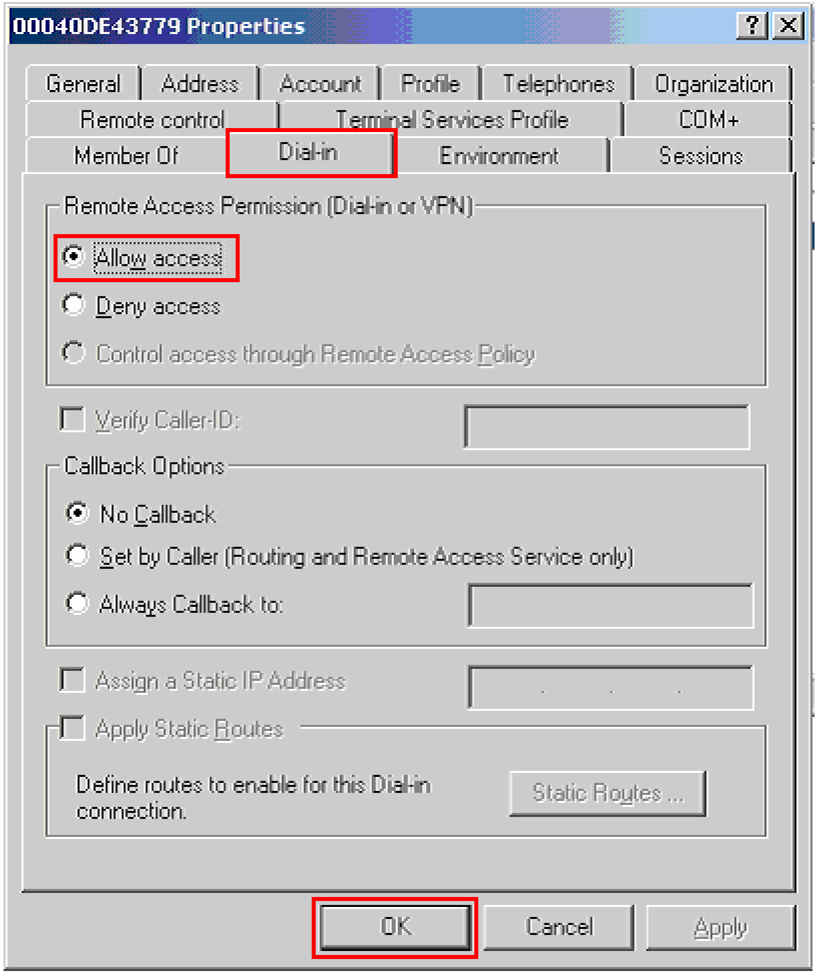
Step	Description
5.	Create a new user ID for an Avaya IP Telephone user and a PC user. From the Active Directory Users and Computers window menu, select **Action** → **New** → **User** to begin creating a new user ID.  Active Directory Users and Computers File Action View Window Help Delegate Control… Find… New All Tasks New Window from Here Refresh Export List… Properties Help Computer Contact Group InetOrgPerson MSMQ Queue Alias Printer User Shared Folder Users 29 objects Type Description User User User Built-in account for admini… User Security Group … Security Group … 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 Domain Users Security Group … All domain users Enterprise Admins Security Group … Designated administrators… Group Policy Creator Owners Security Group … Members in this group can… Guest User Built-in account for guest … HelpServicesGroup Security Group … Group for the Help and Su… IIS_WPG Security Group … IIS Worker Process Group IUSR_SOL User Built-in account for anony… Create a new object…
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.  Create in: interop.com/Users First name: 00040DE43779 Initials: Last name: Full name: 00040DE43779 User logon name: 00040DE43779 @interop.com User logon name (pre-Windows 2000): INTEROP\ 00040DE43779

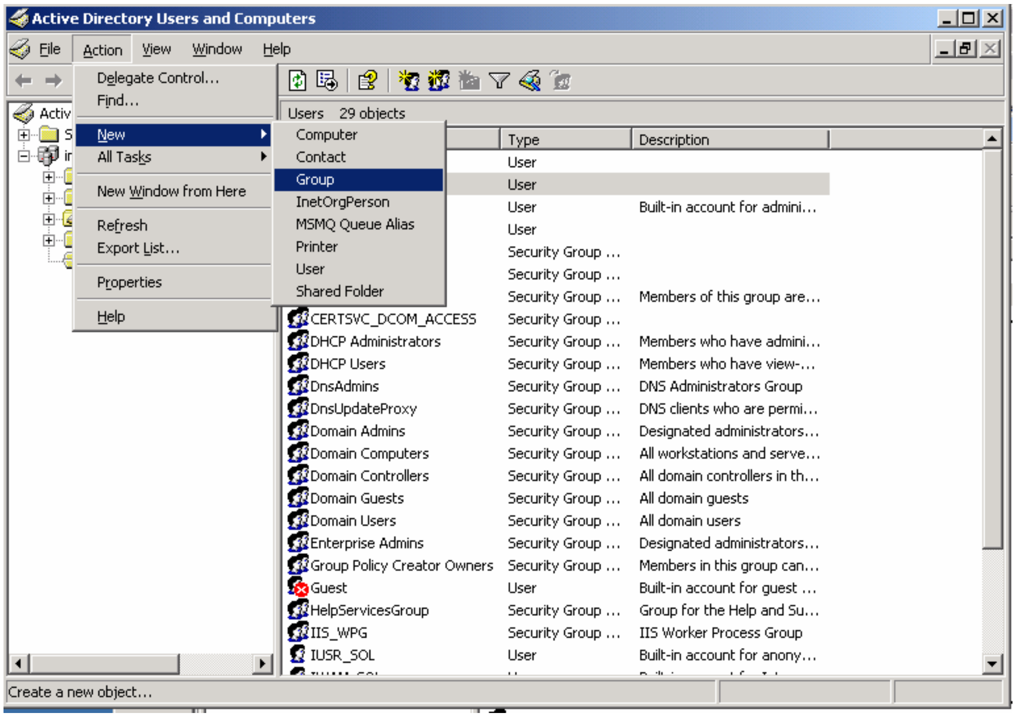
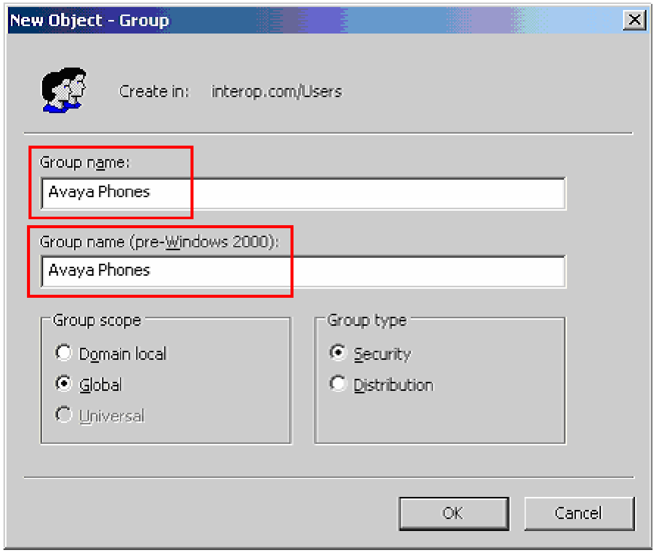
Step	Description
7.	Enter a **Password** for the user ID. For an Avaya IP Telephone, enter a numeric password. Select the **User cannot change password** and **Password never expires** fields. Click **Next** to continue.  New Object - User Create in: interop.com/Users Password: ●●●●●● Confirm password: ●●●●●● ☐ User must change password at next logon ☑ User cannot change password ☑ Password never expires ☐ Account is disabled
8.	Click **Finish** to complete.  New Object - User Create in: interop.com/Users When you click Finish, the following object will be created: Full name: 00040DE43779 User logon name: 00040DE43779_@interop.com The password never expires.

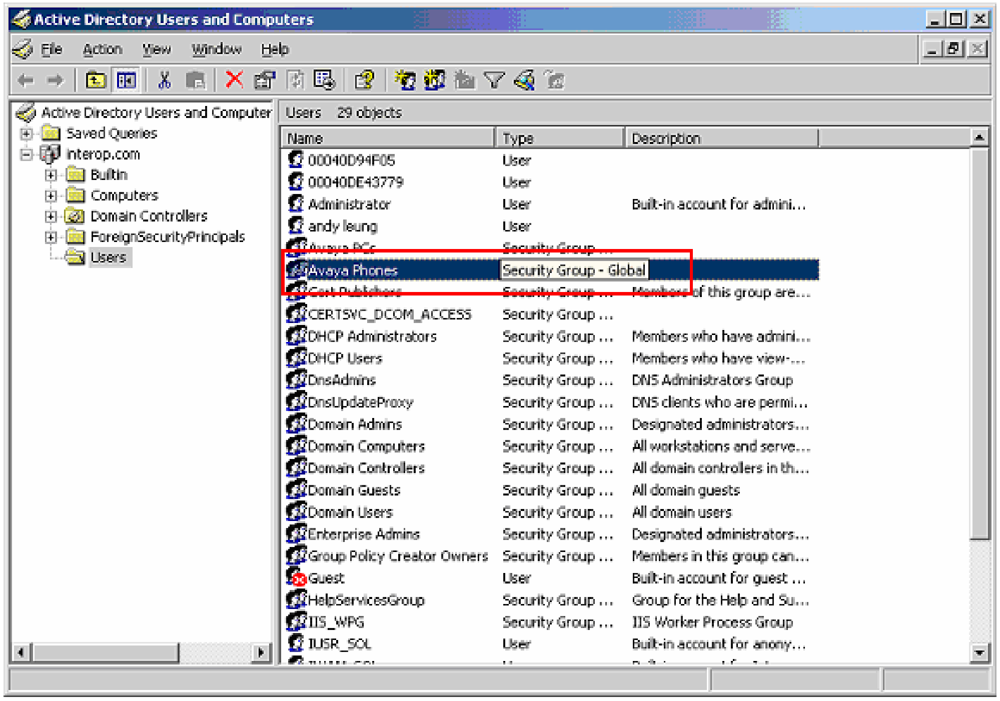
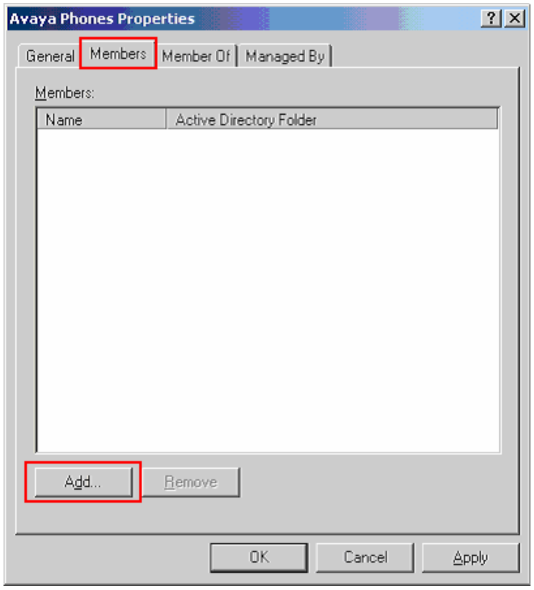
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>Repeat Steps 5-8 to create a user ID for the PC. Below is a screen capture for user ID “user1” used for the PC for log in.


Create in: interop.com/Users
First name: user1
Initials:
Last name:
Full name: user1
User logon name: user1 @interop.com
User logon name (pre-Windows 2000): INTEROP\ user1
</td></tr>
<tr><td>10.</td><td>After creating the user ID, begin editing its property by double clicking on the user ID in the Active Directory Users and Computers window.


Active Directory Users and Computer
Saved Queries
interop.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 30 objects
<table>
<tr><th>Name</th><th>Type</th><th>Description</th></tr>
<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>
</table></td></tr>
</table>

Step	Description
11.	Select the **Dial-in** tab in the user properties window. Enable remote access by clicking on the **Allow access** radio button. Click **OK** to complete. Repeat this step for all Avaya IP Telephone and PC user IDs.  00040DE43779 Properties General Address Account Profile Telephones Organization Remote control Terminal Services Profile COM+ Member Of Dial-in Environment Sessions Remote Access Permission (Dial-in or VPN) ● Allow access ○ Deny access ○ Control access through Remote Access Policy □ Verify Caller-ID: Callback Options ● No Callback ○ Set by Caller (Routing and Remote Access Service only) ○ Always Callback to: □ Assign a Static IP Address □ Apply Static Routes Define routes to enable for this Dial-in connection. Static Routes ... OK Cancel Apply

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.  Active Directory Users and Computers File Action View Window Help Delegate Control… / Find… / New / All Tasks / New Window from Here / Refresh / Export List… / Properties / Help Computer / Contact / Group / InetOrgPerson / MSMQ Queue Alias / Printer / User / Shared Folder Users 29 objects Type / Description User User User / Built-in account for admini… User Security Group … Security Group … 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 Domain Users / Security Group … / All domain users Enterprise Admins / Security Group … / Designated administrators… Group Policy Creator Owners / Security Group … / Members in this group can… Guest / User / Built-in account for guest … HelpServicesGroup / Security Group … / Group for the Help and Su… IIS_WPG / Security Group … / IIS Worker Process Group IUSR_SOL / User / Built-in account for anony… Create a new object…
13.	Create a group for Avaya IP Telephones. The sample network uses the name Avaya Phones for this group. Click **OK** to complete.  New Object - Group Create in: interop.com/Users Group name: Avaya Phones Group name (pre-Windows 2000): Avaya Phones Group scope: ○ Domain local ● Global ○ Universal Group type: ● Security ○ Distribution OK Cancel

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 property by double clicking on the Group in the Active Directory Users and Computers window. 
16.	Select the **Members** tab in the group Properties window. Click **Add** to continue. 

Active Directory Users and Computers

Active Directory Users and Computer
Saved Queries
interop.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

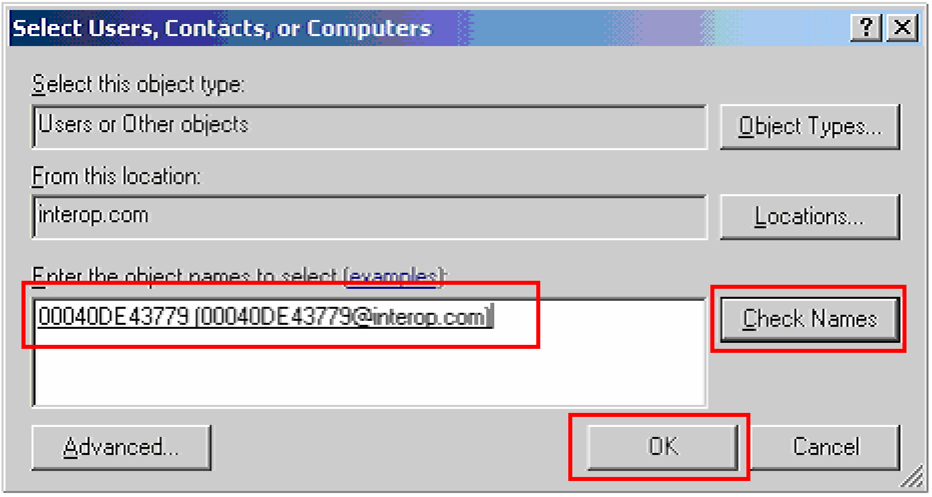
Users 29 objects

Name	Type	Description
00040D94F05	User	
00040DE43779	User	
Administrator	User	Built-in account for admini...
andy leung	User	
Avaya PCs	Security Group ...	
Avaya Phones	Security Group - Global	
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
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_SOL	User	Built-in account for anony...

Avaya Phones Properties

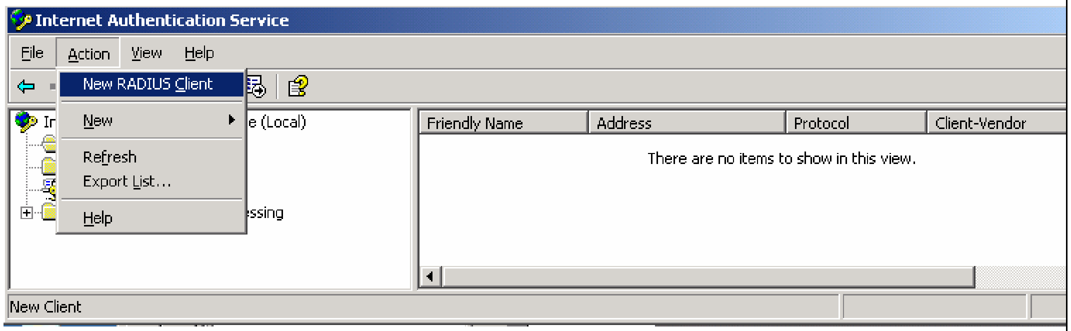
Members:

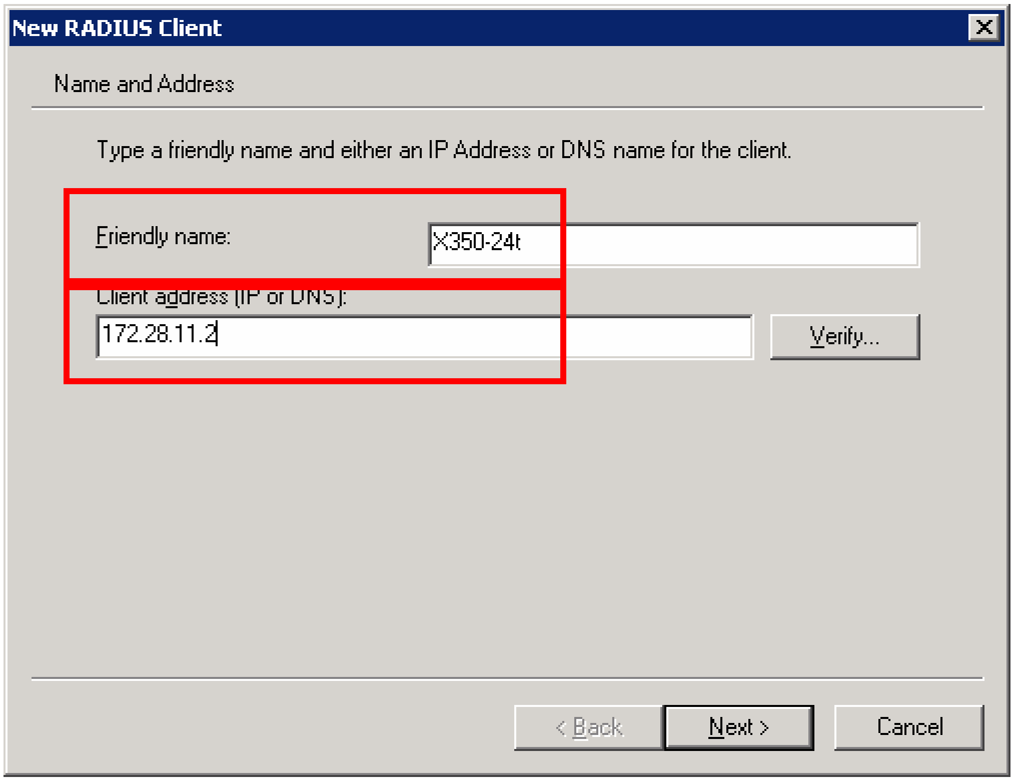
Name	Active Directory Folder

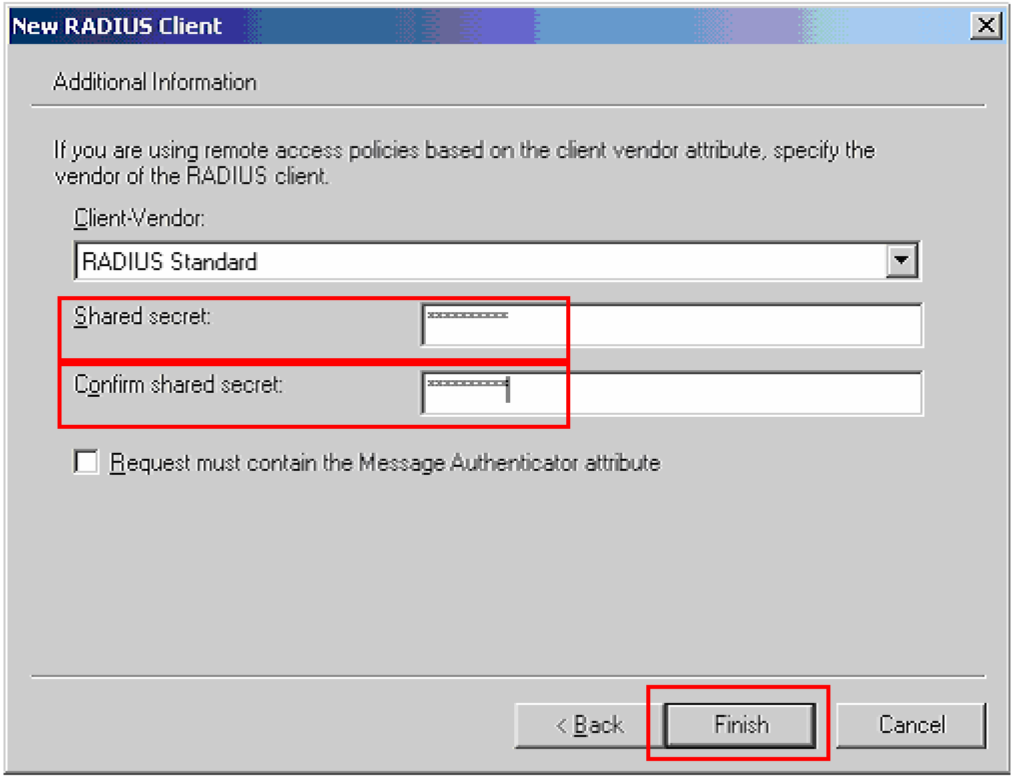
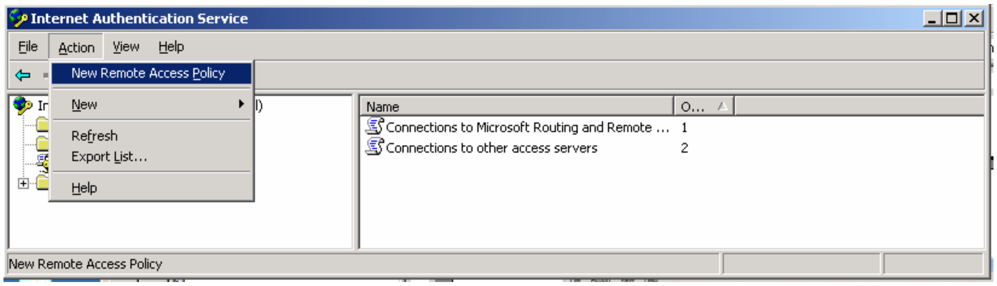
Step	Description
17.	Enter the user ID that should be assigned to the Avaya Phones group. This should be the user ID for the Avaya IP Telephone. Use **Check Names** to assist in searching for the user ID. Click **OK** to complete.  Select this object type: Users or Other objects From this location: interop.com Enter the object names to select (examples): 00040DE43779 (00040DE43779@interop.com) Select Users, Contacts, or Computers Object Types... Locations... Check Names Advanced... OK Cancel
18.	Repeat Steps 15-17 to add members to the PCs user group.

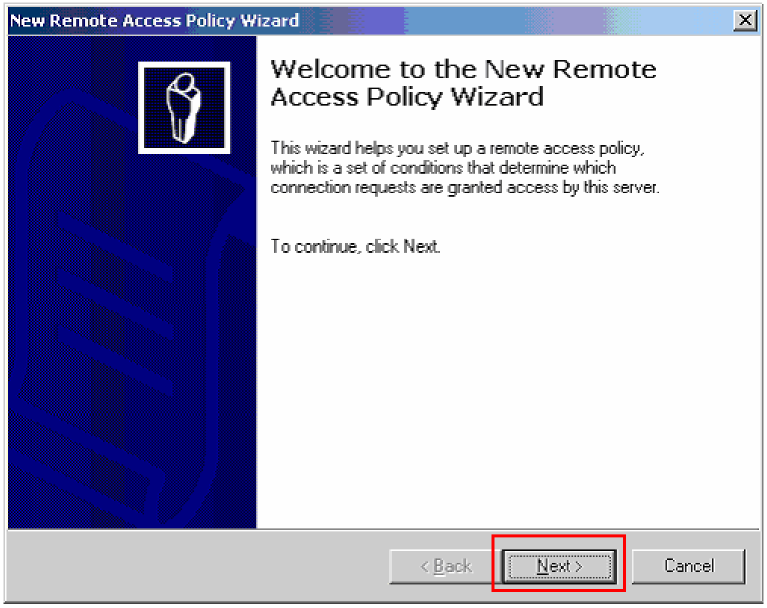
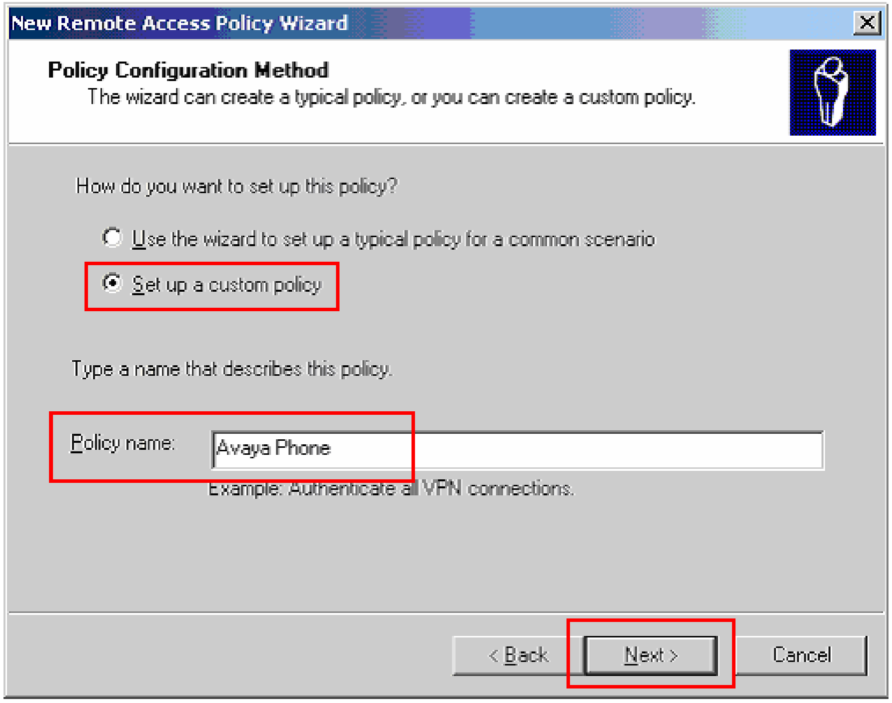
6.2. Configure Microsoft Internet Authentication Services (IAS) Server

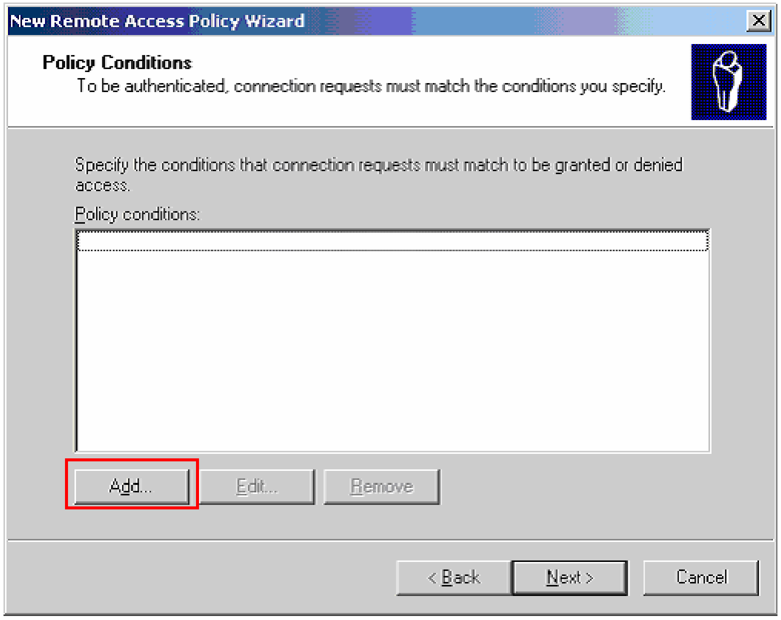
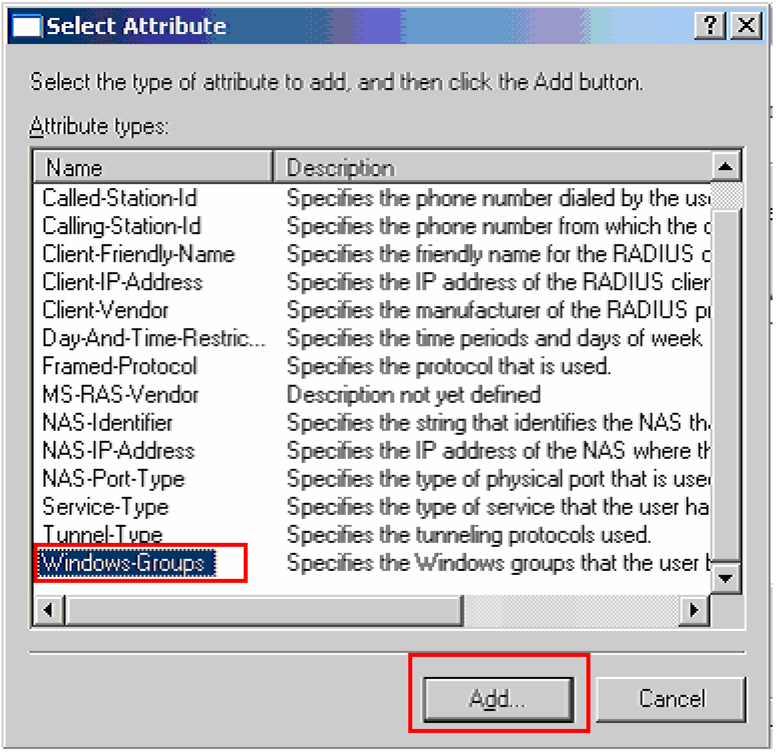
This section shows the steps for configuring the IAS server to support 802.1X authentication for an Avaya IP Telephone and a PC.

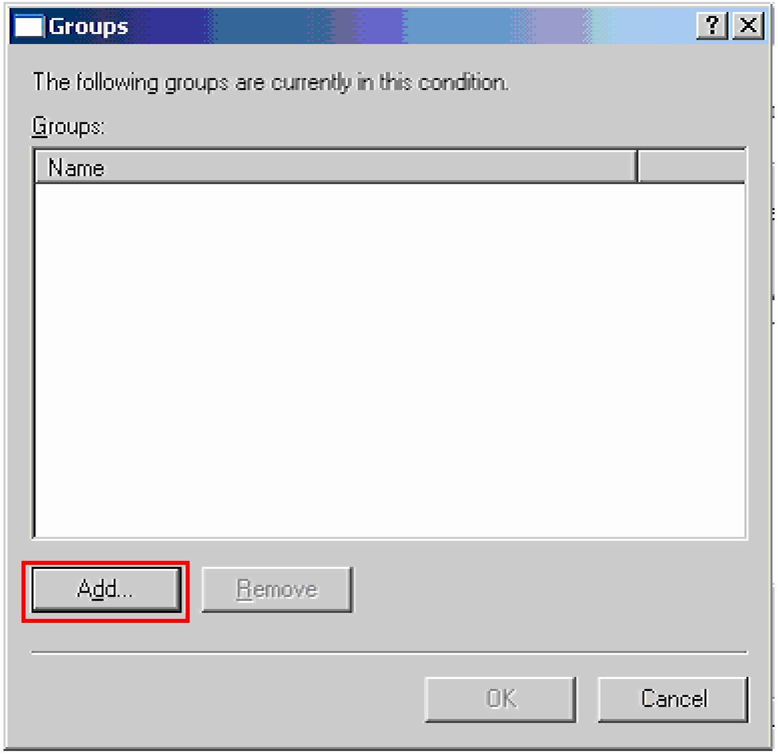
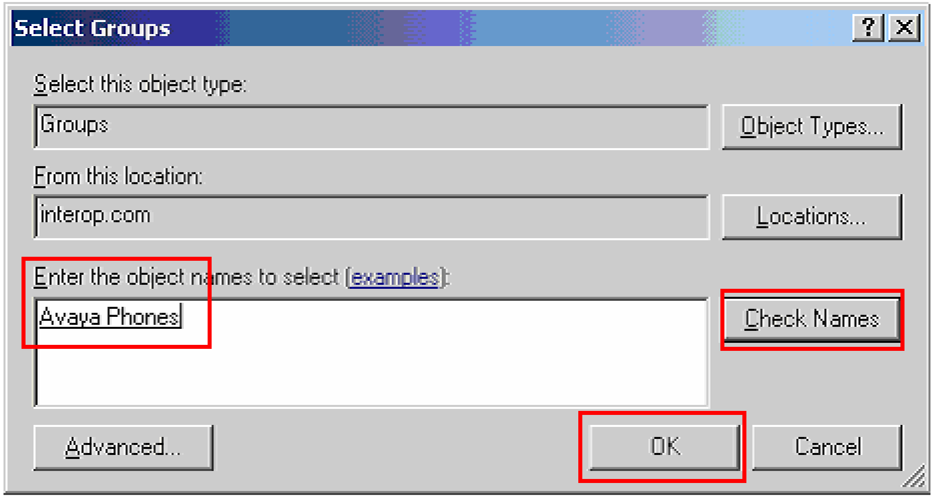
Step	Description
1.	Invoke the Internet Authentication Service window under Administrative Tools of the Microsoft Windows system. Create a new RADIUS client by selecting **Action → New RADIUS Client** from the drop down menu in Internet Authentication Service window.  There are no items to show in this view. Internet Authentication Service File Action View Help New RADIUS Client New Refresh Export List... Help Ir e (Local) ssing Friendly Name Address Protocol Client-Vendor New Client

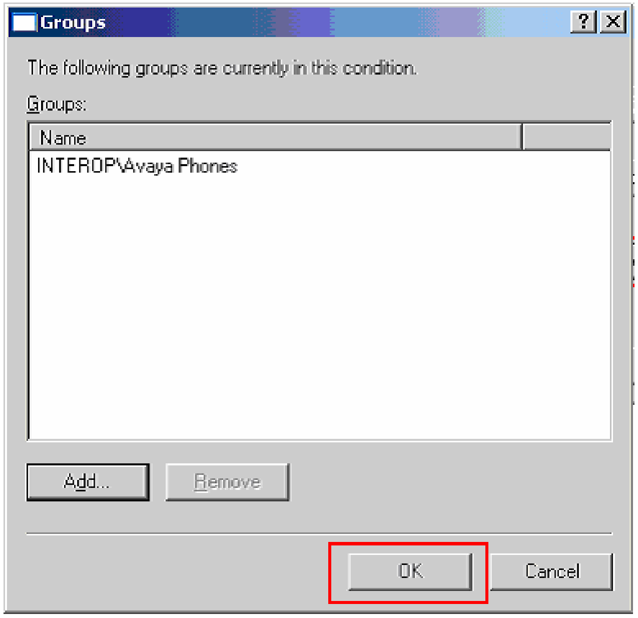
Step	Description
2.	Enter the name and IP address of the X350-24t switch to create a new RADIUS client. This must match the IP address configured in **Section 4.1**, **Step 7.** Click **Next** to continue.  New RADIUS Client Name and Address Type a friendly name and either an IP Address or DNS name for the client. Friendly name: X350-24t Client address (IP or DNS): 172.28.11.2

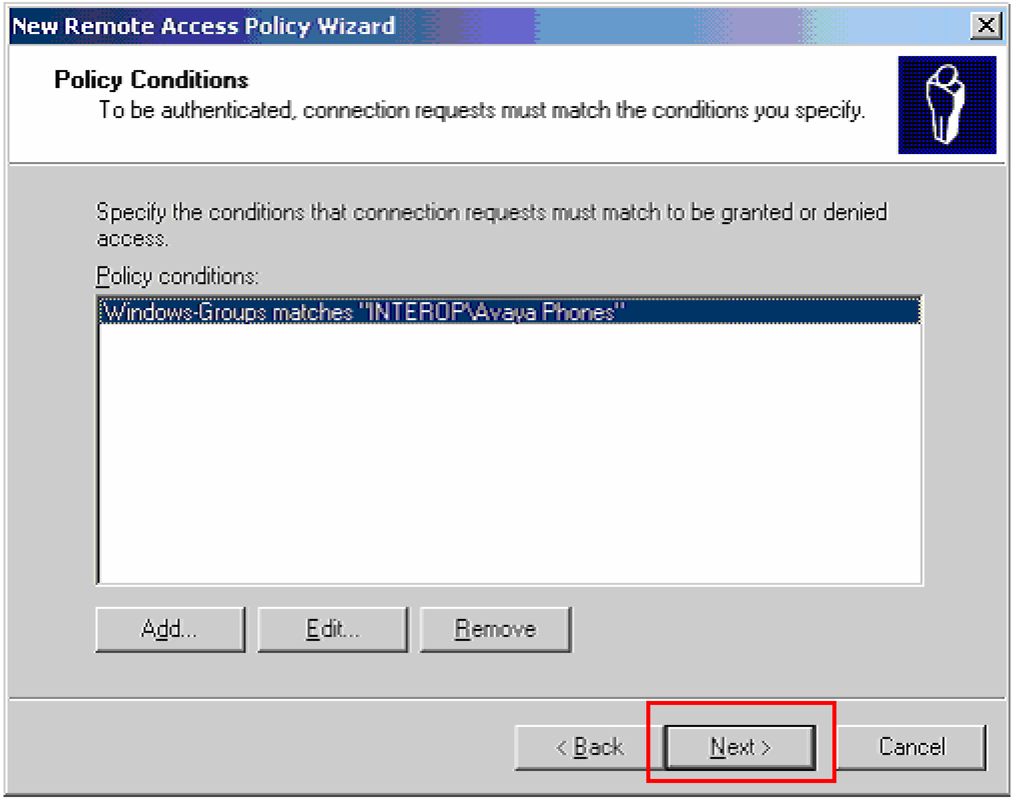
Step	Description
3.	Enter the Shared secret that will be used for this client. This shared secret must match the information configured in the switch in **Section 4.1**, **Step 7**. Click **Finish** to complete.  New RADIUS Client Additional Information If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client. Client-Vendor: RADIUS Standard Shared secret: *********** Confirm shared secret: *********** □ Request must contain the Message Authenticator attribute
4.	Create a new access policy for the Avaya IP Telephones by clicking on **Action → New Remote Access Policy**.  Internet Authentication Service File Action View Help New Remote Access Policy New Refresh Export List... Help Name | O... Connections to Microsoft Routing and Remote ... | 1 Connections to other access servers | 2 New Remote Access Policy

Step	Description
5.	Click **Next** in the **New Remote Access Policy Wizard**.  New Remote Access Policy Wizard Welcome to the New Remote Access Policy Wizard This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server. To continue, click Next.
6.	Select **Set up a custom policy** radio button and enter a **Policy name**. The sample network uses the name Avaya Phone. Click Next to continue.  New Remote Access Policy Wizard **Policy Configuration Method** The wizard can create a typical policy, or you can create a custom policy. How do you want to set up this policy? ○ Use the wizard to set up a typical policy for a common scenario ● Set up a custom policy Type a name that describes this policy. Policy name: Avaya Phone Example: Authenticate all VPN connections.

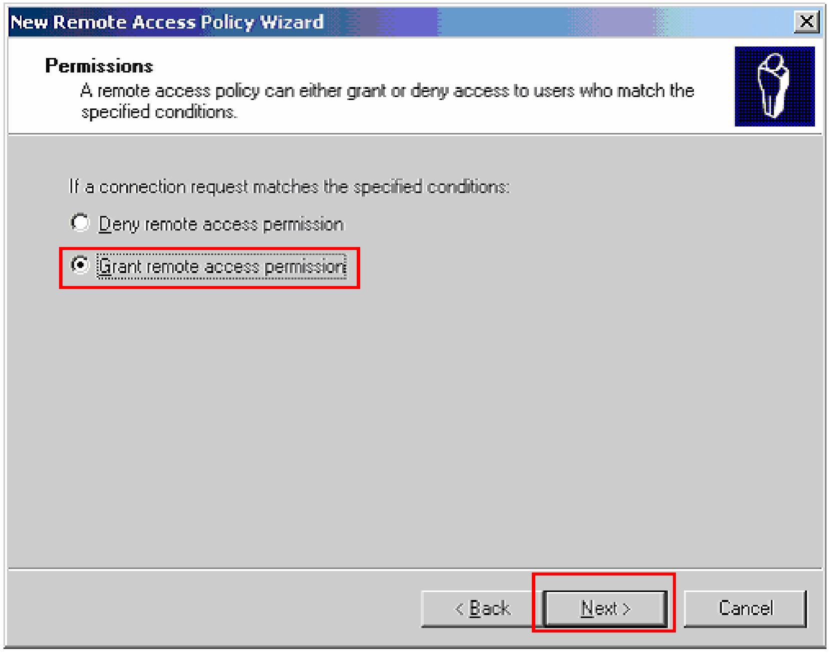
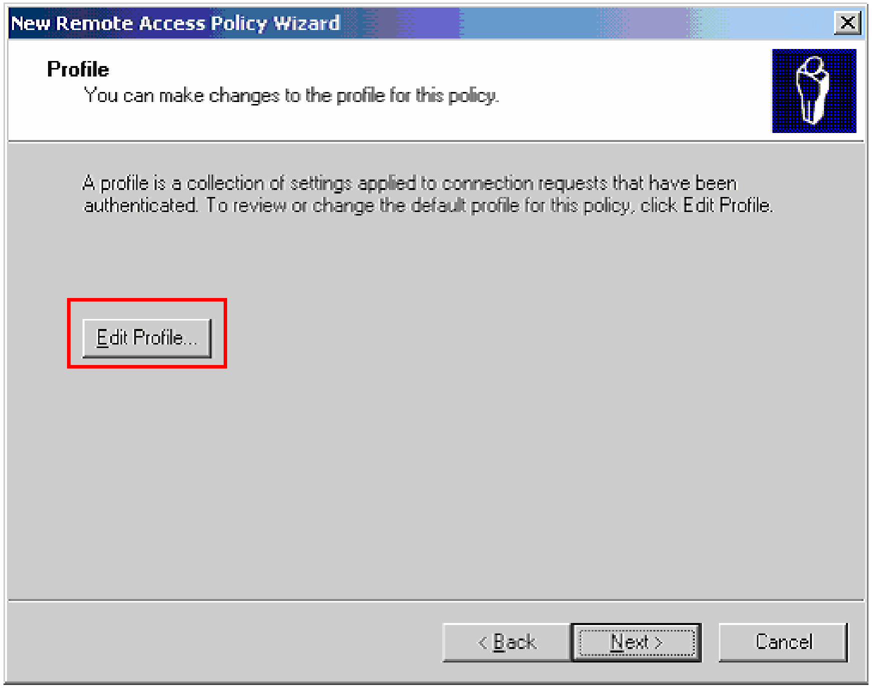
Step	Description
7.	Click the Add button to add a new policy condition.  New Remote Access Policy Wizard **Policy Conditions** To be authenticated, connection requests must match the conditions you specify. Specify the conditions that connection requests must match to be granted or denied access. Policy conditions:
8.	Highlight **Windows-Groups** from the Select Attribute pop-up window. Click **Add** to continue.  Select Attribute Select the type of attribute to add, and then click the Add button. Attribute types: Name — Description Called-Station-Id — Specifies the phone number dialed by the us Calling-Station-Id — Specifies the phone number from which the c Client-Friendly-Name — Specifies the friendly name for the RADIUS c Client-IP-Address — Specifies the IP address of the RADIUS clier Client-Vendor — Specifies the manufacturer of the RADIUS pi Day-And-Time-Restric... — Specifies the time periods and days of week Framed-Protocol — Specifies the protocol that is used. MS-RAS-Vendor — Description not yet defined NAS-Identifier — Specifies the string that identifies the NAS th NAS-IP-Address — Specifies the IP address of the NAS where th NAS-Port-Type — Specifies the type of physical port that is use Service-Type — Specifies the type of service that the user ha Tunnel-Type — Specifies the tunneling protocols used. Windows-Groups — Specifies the Windows groups that the user b

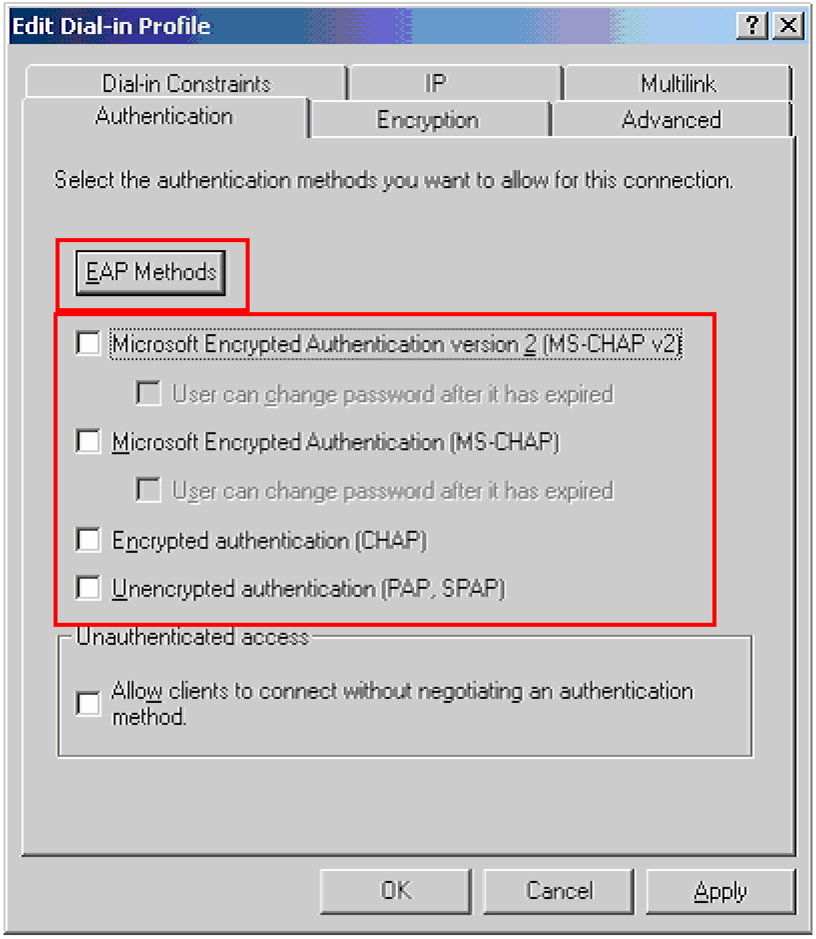
Step	Description
9.	Click **Add** in the Groups pop-up window to add a windows group.  Groups The following groups are currently in this condition. Groups: Name Add... Remove OK Cancel
10.	Enter the Active Directory user group created in **Section 6.1**, **Steps 12-13**. Use **Check Names** to assist in searching for the user group. Click **OK** to complete.  Select Groups Object Types... Locations... Check Names Advanced... OK Cancel Select this object type: Groups From this location: interop.com Enter the object names to select (examples): Avaya Phones

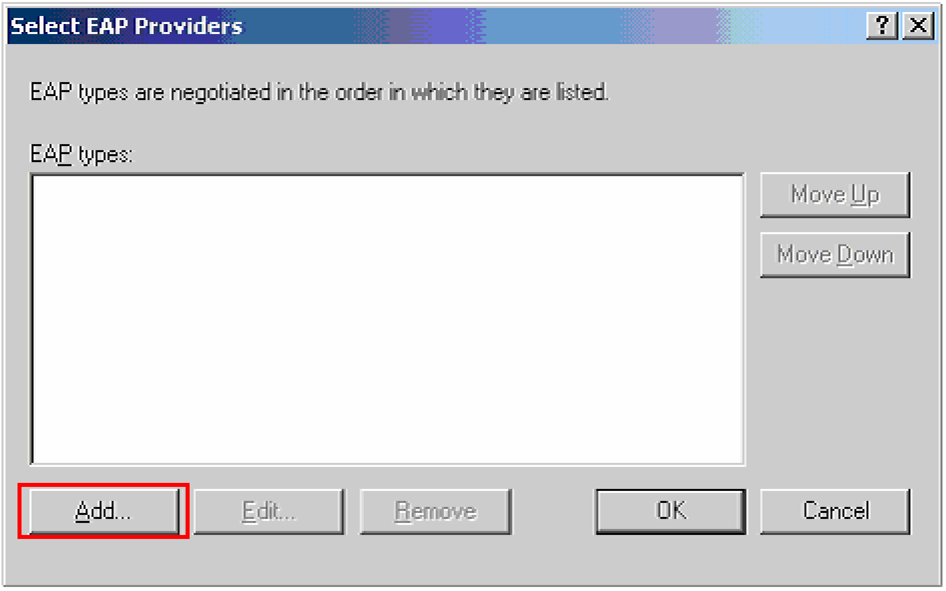
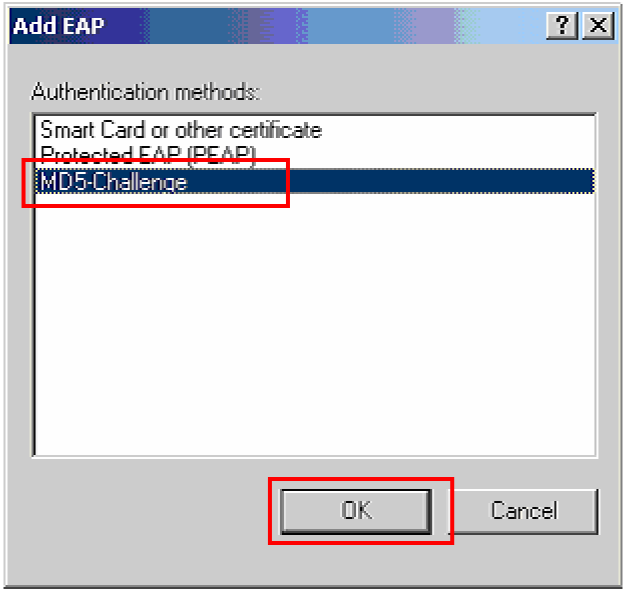
Step	Description
11.	Click **OK** in the Groups pop-up windows to complete.  The following groups are currently in this condition. Groups: Name INTEROP\Avaya Phones

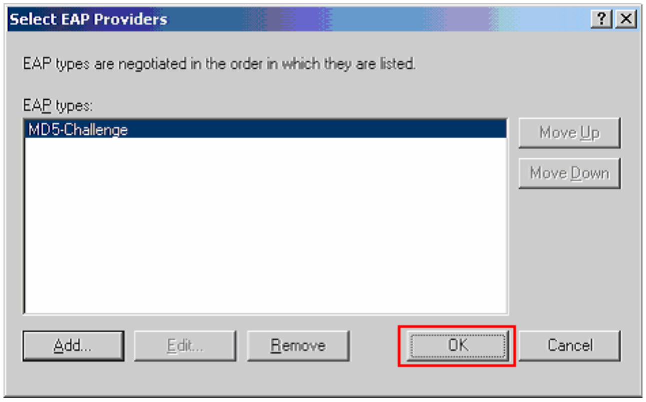
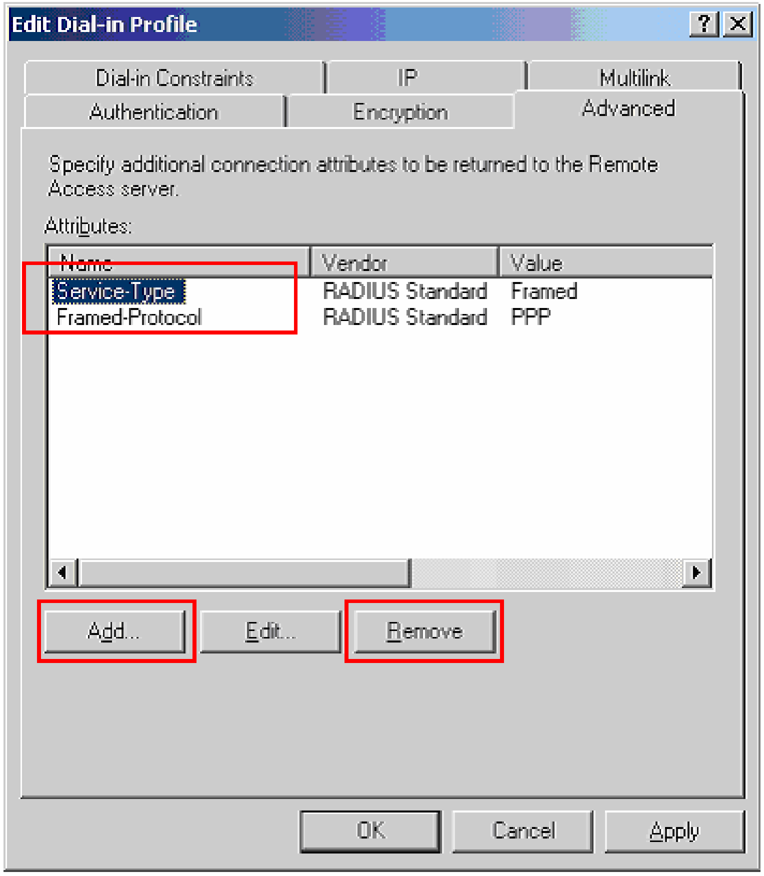
Step	Description
12.	Once the windows user group has been added via **Steps 8-11**, click **Next** to continue.  Specify the conditions that connection requests must match to be granted or denied access. Policy conditions: Windows-Groups matches "INTEROP\Avaya Phones"

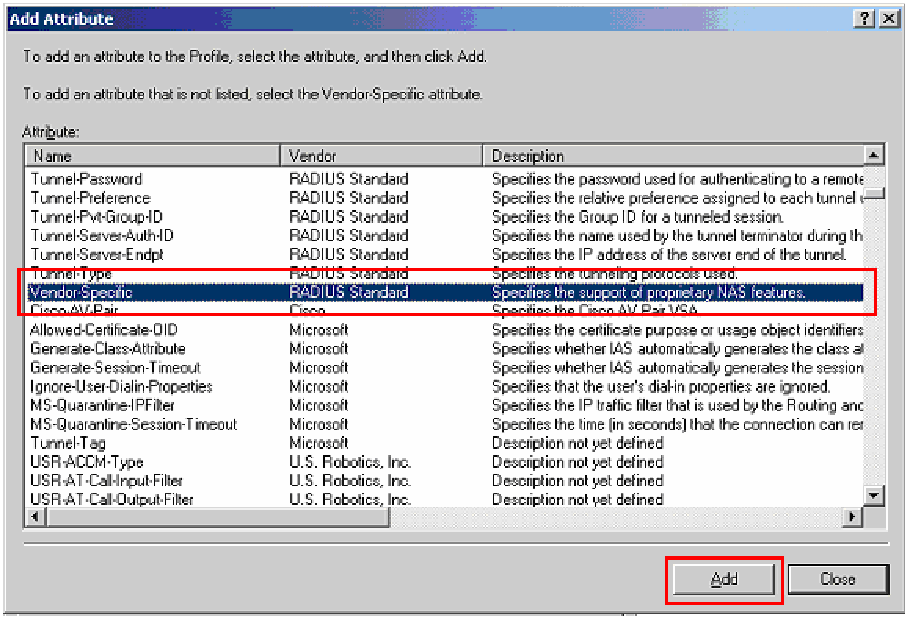
New Remote Access Policy Wizard
Policy Conditions
To be authenticated, connection requests must match the conditions you specify.
Add...
Edit...
Remove
< Back
Next >
Cancel

Step	Description
13.	Click the **Grant remote access permission** radio button. Click **Next** to continue.  New Remote Access Policy Wizard **Permissions** A remote access policy can either grant or deny access to users who match the specified conditions. If a connection request matches the specified conditions: ○ Deny remote access permission ● Grant remote access permission
14.	Click **Edit Profile** to configure the profile for this access policy. This will display the Edit Dial-in Profile pop-up window.  New Remote Access Policy Wizard **Profile** You can make changes to the profile for this policy. 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.

Step	Description
15.	Select the **Authentication** tab in the Edit Dial-in Profile pop-up window. Uncheck all Microsoft authentication protocols as shown in the screen capture below. Click **EAP Methods** to continue. This will display the Select EAP Providers pop-up window.  Edit Dial-in Profile Dial-in Constraints | IP | Multilink | Authentication | Encryption | Advanced Select the authentication methods you want to allow for this connection. EAP Methods □ Microsoft Encrypted Authentication version 2 (MS-CHAP v2) □ User can change password after it has expired □ Microsoft Encrypted Authentication (MS-CHAP) □ User can change password after it has expired □ Encrypted authentication (CHAP) □ Unencrypted authentication (PAP, SPAP) Unauthenticated access □ Allow clients to connect without negotiating an authentication method. OK | Cancel | Apply

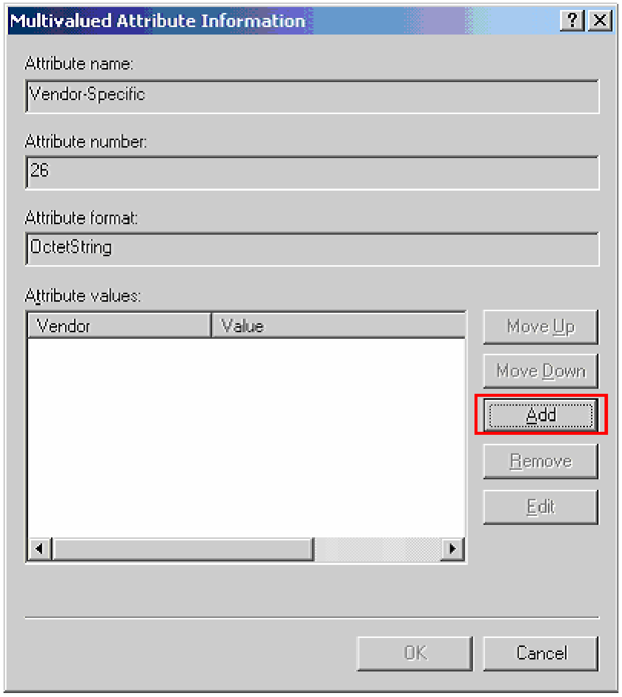
Step	Description
16.	Click **Add** in the Select EAP Providers pop-up window to add a new EAP type.  Select EAP Providers EAP types are negotiated in the order in which they are listed. EAP types: Move Up Move Down Add... Edit... Remove OK Cancel
17.	Select **MD5-Challenge** in the Add EAP pop-up window. Click **OK** to continue.  Add EAP Authentication methods: Smart Card or other certificate Protected EAP (PEAP) MD5-Challenge OK Cancel

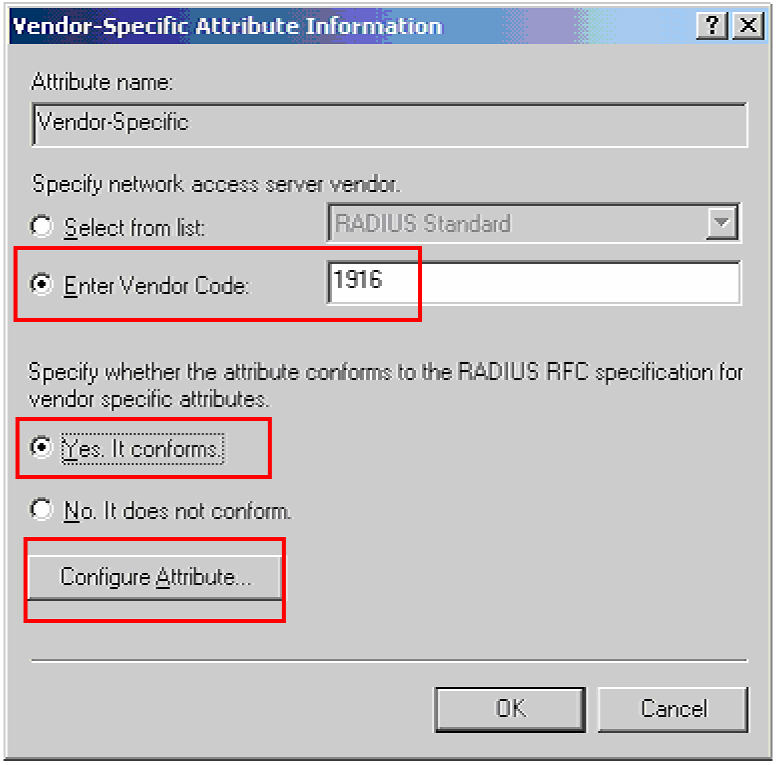
Step	Description
18.	Once the MD5-Challenge EAP type is added, Click **OK** to complete the EAP authentication selection.  Select EAP Providers EAP types are negotiated in the order in which they are listed. EAP types: MD5-Challenge Move Up Move Down Add... Edit... Remove OK Cancel
19.	Select the **Advanced** tab in the Edit Dial-in profile pop-up window. Highlight each existing attribute, and 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.  Edit Dial-in Profile Dial-in Constraints IP Multilink Authentication Encryption Advanced Specify additional connection attributes to be returned to the Remote Access server. Attributes: Name — Vendor — Value Service-Type — RADIUS Standard — Framed Framed-Protocol — RADIUS Standard — PPP Add... Edit... Remove OK Cancel Apply

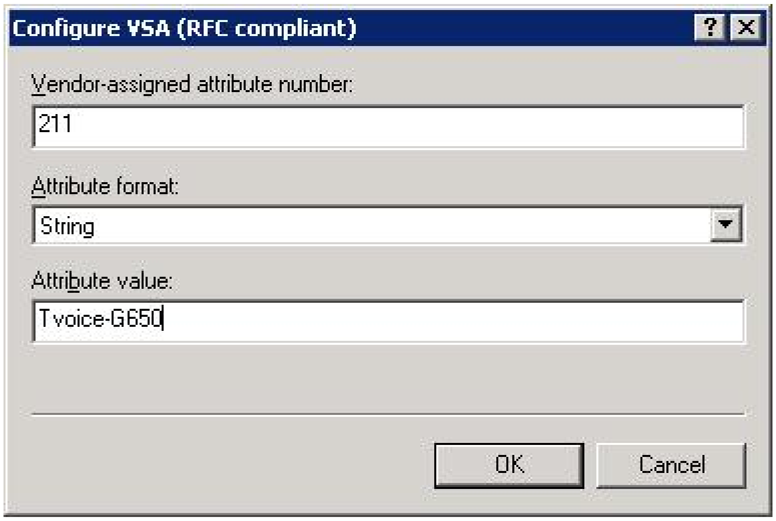
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>20.</b></td><td>Highlight the <b>Vendor Specific</b> attribute name from the list of attributes displayed in the Add Attribute pop-up window. Click <b>Add</b> to continue. This will display the Multivalued Attribute Information pop-up window.


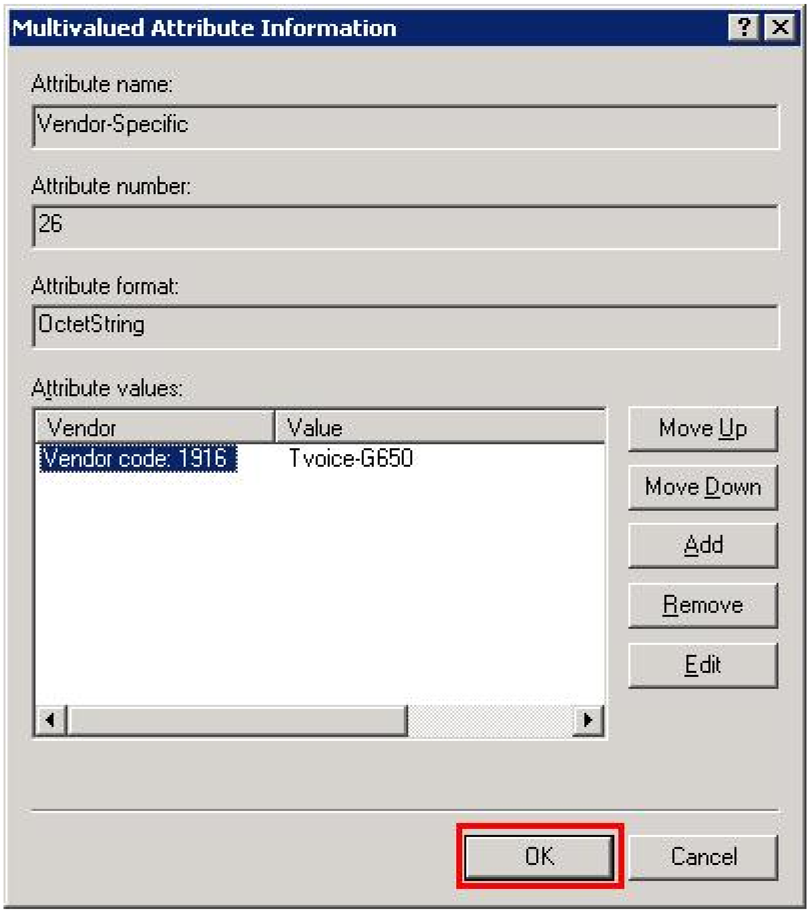
To add an attribute to the Profile, select the attribute, and then click Add.
To add an attribute that is not listed, select the Vendor-Specific attribute.
Attribute:
<table>
<tr><th>Name</th><th>Vendor</th><th>Description</th></tr>
<tr><td>Tunnel-Password</td><td>RADIUS Standard</td><td>Specifies the password used for authenticating to a remote</td></tr>
<tr><td>Tunnel-Preference</td><td>RADIUS Standard</td><td>Specifies the relative preference assigned to each tunnel</td></tr>
<tr><td>Tunnel-Pvt-Group-ID</td><td>RADIUS Standard</td><td>Specifies the Group ID for a tunneled session.</td></tr>
<tr><td>Tunnel-Server-Auth-ID</td><td>RADIUS Standard</td><td>Specifies the name used by the tunnel terminator during th</td></tr>
<tr><td>Tunnel-Server-Endpt</td><td>RADIUS Standard</td><td>Specifies the IP address of the server end of the tunnel.</td></tr>
<tr><td>Tunnel-Type</td><td>RADIUS Standard</td><td>Specifies the tunneling protocols used.</td></tr>
<tr><td>Vendor-Specific</td><td>RADIUS Standard</td><td>Specifies the support of proprietary NAS features.</td></tr>
<tr><td>Cisco-AV-Pair</td><td>Cisco</td><td>Specifies the Cisco AV Pair VSA</td></tr>
<tr><td>Allowed-Certificate-OID</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 al</td></tr>
<tr><td>Generate-Session-Timeout</td><td>Microsoft</td><td>Specifies whether IAS automatically generates the session</td></tr>
<tr><td>Ignore-User-Dialin-Properties</td><td>Microsoft</td><td>Specifies that the user's dial-in properties are ignored.</td></tr>
<tr><td>MS-Quarantine-IPFilter</td><td>Microsoft</td><td>Specifies the IP traffic filter that is used by the Routing anc</td></tr>
<tr><td>MS-Quarantine-Session-Timeout</td><td>Microsoft</td><td>Specifies the time (in seconds) that the connection can rei</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>
</table>

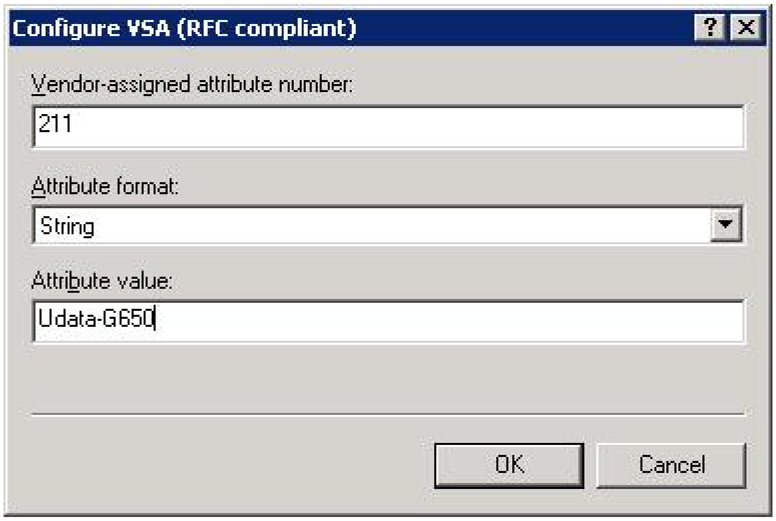
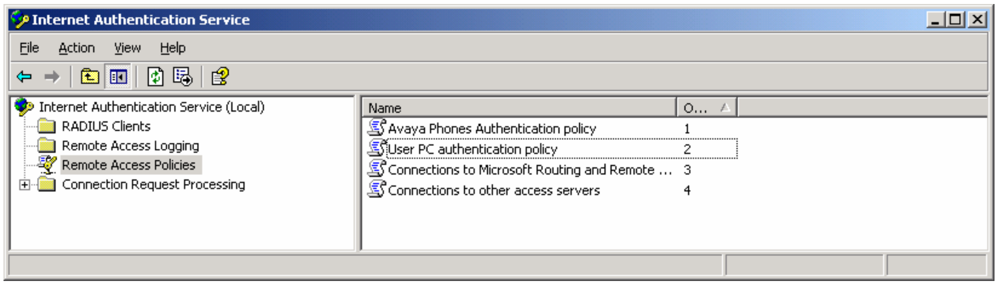
</td></tr>
</table>

Step	Description
21.	Click **Add** to enter a new Attribute in the Multivalued Attribute Information pop-up window. This will display the Vendor-Specific Attribute Information pop-up window.  Multivalued Attribute Information Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor Value Move Up Move Down Add Remove Edit OK Cancel

Step	Description
22.	In the Vendor-Specific Attribute Information pop-up window, click on the **Enter Vendor Code** radio button, and enter string **1916** (Extreme Networks Vendor Code). Click on the **Yes, It conforms** radio button. Click **Configure Attribute** to continue. This will display the Configure VSA (RFC compliant) pop-up window.  Vendor-Specific Attribute Information Attribute name: Vendor-Specific Specify network access server vendor. ○ Select from list: RADIUS Standard ● Enter Vendor Code: 1916 Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes. ● Yes. It conforms. ○ No. It does not conform.

Step	Description
23.	Enter the following field information in the Configure VSA (RFC compliant) pop-up window. The Attribute value "**Tvoice-G650**" 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.  Configure VSA (RFC compliant) Vendor-assigned attribute number: 211 Attribute format: String Attribute value: Tvoice-G650

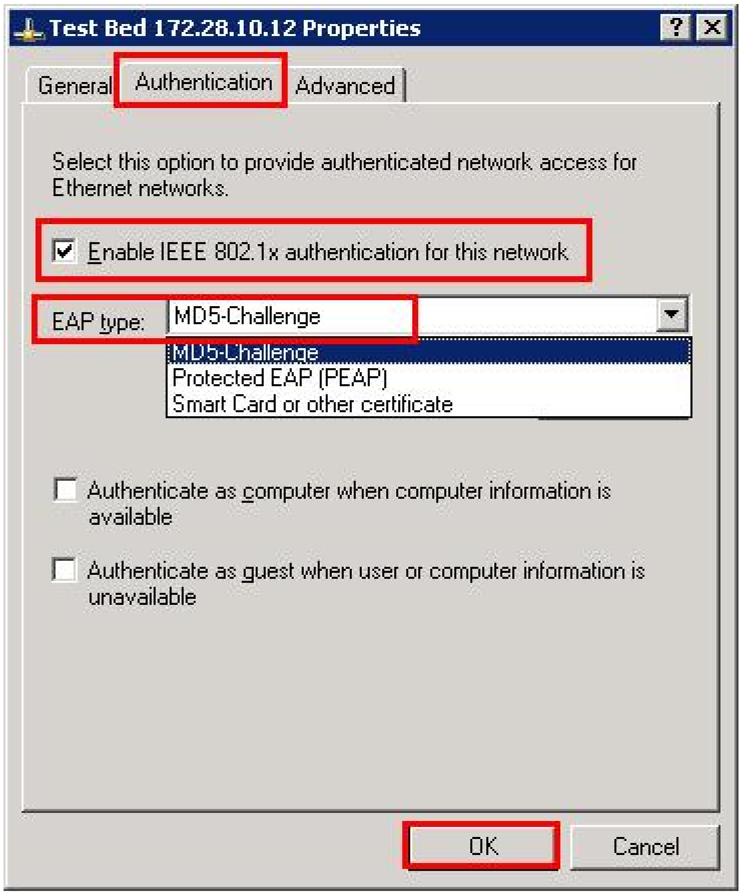
Step	Description
24.	Once all attributes have been entered in **Steps 21-23**, click **OK** to continue.  Multivalued Attribute Information Attribute name: Vendor-Specific Attribute number: 26 Attribute format: OctetString Attribute values: Vendor: Vendor code: 1916 — Value: Tvoice-G650 Move Up Move Down Add Remove Edit OK Cancel
25.	Click **OK** on all preceding pop-up windows to complete the configuration of this access policy.

Step	Description
26.	Repeat **Steps 4-25** 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-G650** value in lieu of what is in **Step 23**. The **Udata-G650** 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**.  Configure VSA (RFC compliant) Vendor-assigned attribute number: 211 Attribute format: String Attribute value: Udata-G650
27.	After completing the above steps, there should be a total of 4 Remote Access Polices.  Internet Authentication Service Internet Authentication Service (Local) RADIUS Clients Remote Access Logging Remote Access Policies Connection Request Processing Name / O... Avaya Phones Authentication policy 1 User PC authentication policy 2 Connections to Microsoft Routing and Remote ... 3 Connections to other access servers 4

7. Configure the PC

This section shows the steps for configuring authentication on the PC.

1. Open the properties window for the network adapter card in Windows. Under the **Authentication** tab, check the **Enable IEEE 802.1x authentication for this network** check box and select MD5-Challenge from the **EAP type** drop down menu. Click **Ok** to complete.



Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: MD5-Challenge

- MD5-Challenge
- Protected EAP (PEAP)
- Smart Card or other certificate

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

8. Configure the Avaya IP Phone

This section shows the steps for configuring the Avaya 4610 SW IP Phone connected into the X350-24t switch.

Avaya IP telephones support three 802.1X operational modes:

- **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 attaced 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.

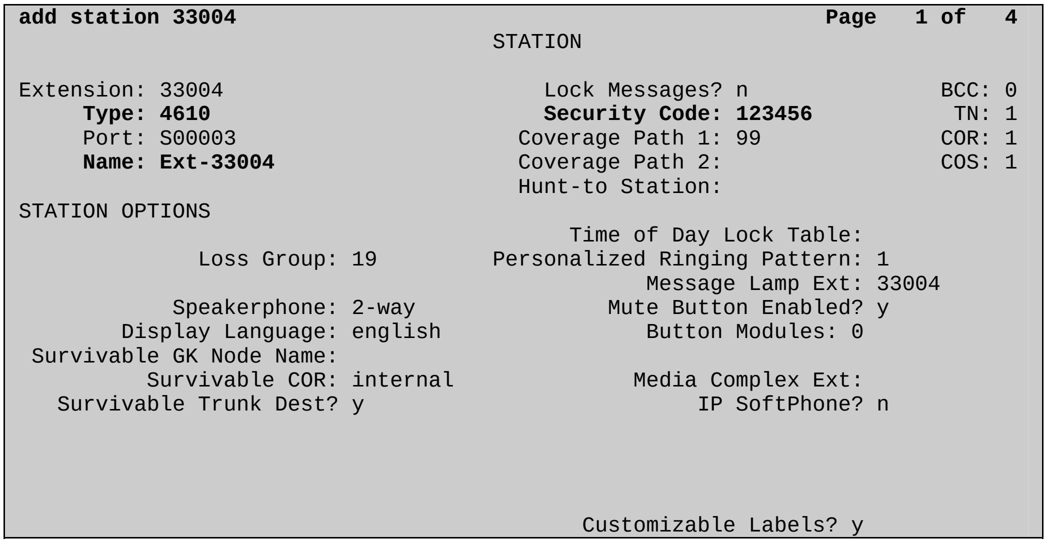
The operational mode can be changed by pressing "mute80219#" ("mute 8021x") on the Avaya 4600-Series IP telephones or "mute27237#" (mute craft) on the Avaya 9600-Series IP telephones.

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 X350-24t 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.

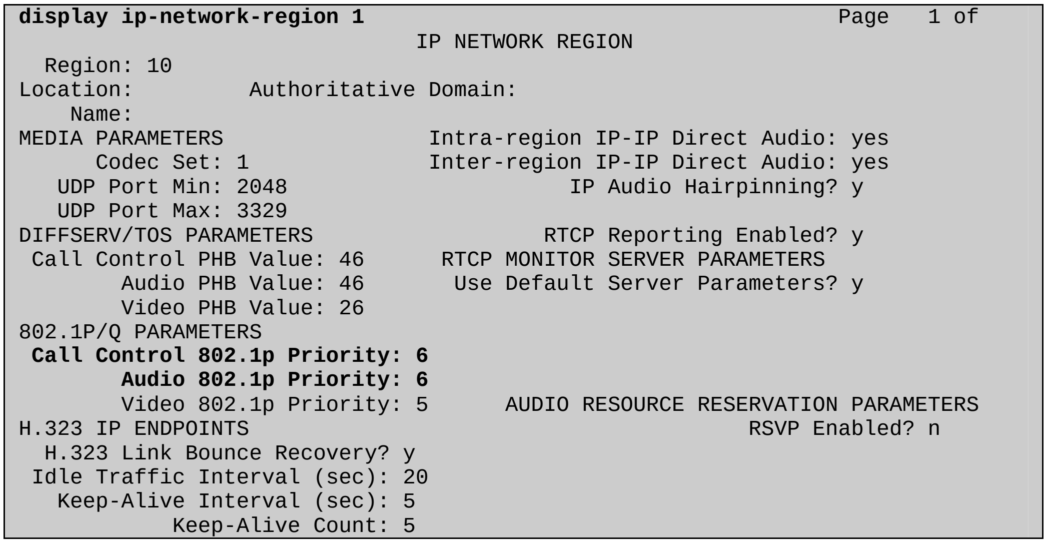
Step	Description
1.	Add a new station for the Avaya IP Telephones to the Avaya Communication Manager using the **add station** command. Configure the following fields. • **Extension:** *33004* (Extension number for the Avaya Telephone) • **Type:** *4610* (Avaya Telephone type used for this extension) • **Port:** *IP* (Type of connection for the Avaya Telephone) • **Security Code:** *123456* (Security code used by the Avaya Telephone to register with Avaya Communication Manager) • **Direct IP-IP Audio Connections:** *y* (Enable Shuffling) The first two pages of the **add station 33004** configuration are shown below. Repeat this step for each station. 

```
add station 33004                                              Page   1 of   4
                                     STATION

Extension: 33004                         Lock Messages? n               BCC: 0
     Type: 4610                          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
                                            Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 33004
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n




                                             Customizable Labels? y
```

Step	Description
2.	Use the “display ip-network-region” command to display the 802.1P setting configured in the Avaya Communication Manager. Both Call Control and Audio 802.1P priority are set to 6. 

```
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
```

10. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the X350s 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 X350-24t supports the following:

- 802.1D
- 802.1W
- LLDP advertisement & interoperability
- Dynamic VLAN assignment using Extreme RADIUS attributes.
- 802.1x authentication with multiple supplicant per port
- Quality of Server (QoS) according to 802.1p or DiffServ

10.2. Test Results

The Extreme Networks X350-24t 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 attribute 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 15 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
==============================================================
15     308      0      0      0      0    5392     0     13
```

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

```
X350-24t # 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: 1,2
Participating Vlans: data-G650,Default,voice-G650
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 X350-24t to verify whether RADIUS setting such as **IP address** and **Client address** are correct. A successful log in by an 802.1X client should show 2 Access Requests, 1 Access Accepts, and 1 Access Challenges in the counter.

```
X350-24t # 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:  172.28.11.2 (VR-Default)
    Shared secret :  3>:>?75<;5
Access Requests   :  2              Access Accepts    :  1
Access Rejects    :  0              Access Challenges :  1
Access Retransmits:  0              Client timeouts   :  0
Bad authenticators:  0              Unknown types     :  0
Round Trip Time   :  0
```

- Use the “show netlogin” command on the X350-24t 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.

```
X350-24t # 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: 15,  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            0              00040DE43779
00:12:3f:25:26:60  0.0.0.0          Yes   802.1x  3593           user1
-----------------------------------------------

Port: 15,  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 port <port#> neighbors detail” command on the X350 switch to LLDP information.

```
X350-24t.110 # show lldp port 15 neighbors detailed

-----------------------------------------------------------------------------
LLDP Port 15 detected 1 neighbor
  Neighbor: (5.1)172.28.10.54/00:04:0D:E4:3C:05, age 3 seconds
    - Chassis ID type: Network address (5); Address type: IPv4 (1)
      Chassis ID     : 172.28.10.54
    - Port ID type: MAC address (3)
      Port ID     : 00:04:0D:E4:3C:05
    - Time To Live: 120 seconds
    - System Name: "AVAE43C05"
    - System Capabilities : "Bridge, Telephone"
      Enabled Capabilities: "Bridge, Telephone"
    - Management Address Subtype: IPv4 (1)
      Management Address        : 172.28.10.54
      Interface Number Subtype  : System Port Number (3)
      Interface Number          : 1
      Object ID String          : "1.3.6.1.4.1.6889.1.69.1.7"
    - IEEE802.3 MAC/PHY Configuration/Status
      Auto-negotiation       : Supported, Enabled (0x03)
      Operational MAU Type   : 100BaseTXFD (16)
    - MED Capabilities: "MED Capabilities, Network Policy, Inventory"
      MED Device Type : Endpoint Class III (3)
    - MED Network Policy
      Application Type  : Voice (1)
      Policy Flags      : Known Policy, Tagged (0x1)
      VLAN ID           : 10
      L2 Priority       : 6
      DSCP Value        : 46
    - MED Hardware Revision: "4610D01A"
    - MED Firmware Revision: "b10d01b2_8_3.bin"
    - MED Software Revision: "a10d01b2_8_3.bin"
    - MED Serial Number: "06N521006142"
    - MED Manufacturer Name: "Avaya"
    - MED Model Name: "4610"
    - Avaya/Extreme Conservation Level Support
      Current Conservation Level: 0
      Typical Power Value       : 4.0 Watts
      Maximum Power Value       : 6.0 Watts
    - Avaya/Extreme Call Server(s): 172.28.10.7
    - Avaya/Extreme IP Phone Address: 172.28.10.54 255.255.255.0
      Default Gateway Address       : 172.28.10.1
    - 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 X350-24t switch has the correct 802.1P to QoS Profile assignment.

```
X350-24t # show dot1p
   802.1p Priority Value     QOS Profile
           0                QP1
           1                QP1
           2                QP1
           3                QP1
           4                QP1
           5                QP1
           6                QP6
           7                QP8
```

- Use the "show trunk" command on the Avaya C363T-PWR Converged Stackable Switch to verify trunk setting.

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

Port   Mode  Binding mode             Native vlan
------ ----- ------------------------ -----------
 1/1   dot1q bound to configured vlans     1
 1/2   dot1q bound to configured vlans     1
 1/3   off   statically bound              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 Summit X350-24t switch to support an Avaya VoIP solution depicted in Figure 1 which 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 4.0, Release 5.0, January 2008

[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 4, Release 5.0, January 2008

[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 13, January 2008

[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

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 DevConnect Program at devconnect@avaya.com.