



**Avaya Solution & Interoperability Test Lab**

---

## **Configuring Extreme Networks BlackDiamond 8800's G48Tc and G58Te2 Modules to Support Avaya IP Telephones with RADIUS Authentication – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring the G48Tc and G48Te2 modules to support an Avaya VoIP solution consisting of Avaya Communication Manager running on Avaya S8500 Server, Avaya G650 Media Gateway and Avaya IP Telephones. The G48Tc and G48Te2, part of Extreme Networks BlackDiamond 8800's C-Series and E-Series modules respectively, are field upgradeable modules with optional Power over Ethernet support providing cost benefit and flexibility. 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

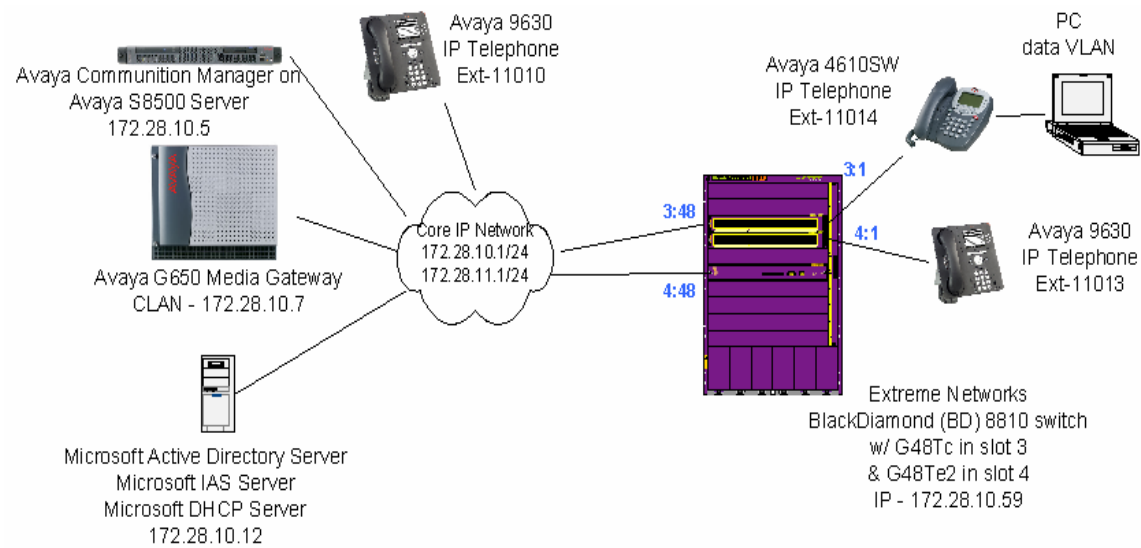
These Application Notes describe a solution for configuring the G48Tc and G48Te2 modules installed in the BlackDiamond (BD) 8810 switch to support an Avaya Voice over IP (VoIP) solution consisting of Avaya Communication Manager running on Avaya S8500 Server, Avaya G650 Media Gateway, and Avaya IP Telephones.

The G48Tc and G48Te2 provide high density 48 ports 10/100/1000 Ethernet connectivity for the BlackDiamond 8800 series switches. They are field upgradeable with an S-POE daughter board to provide for Power over Ethernet (PoE) functionality. Both G48Tc and G48Te2 modules used in these Application Notes have been upgraded with the S-POE daughter board to provide PoE functionality.

Microsoft Internet Authentication Service (IAS) is used to provide 802.1x RADIUS authentications for Avaya IP Telephones and the PCs that are connected to the G48Tc or G48Te2 modules. The Avaya IP Telephones and PCs are individually authenticated through the BD 8810 switch by the IAS.

# 2. Configuration

**Figure 1** illustrates the configuration used in these Application Notes. 802.1x RADIUS authentication is enabled on the BD 8810. All Avaya IP Telephones and the PC obtain their IP address via Dynamic Host Configuration Protocol (DHCP). Avaya Communication Manager and file server information are obtained through Link Layer Discovery Protocol (LLDP). 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.



**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 5.1 (R015x.01.0.414.3)
Avaya 9630 IP Telephone (H.323)	1.5
Avaya 4610SW IP Telephone (H.323)	2.8.3
Extreme Networks BlackDiamond 8810	ExtremeXOS 12.1.1.4
Extreme Networks G48Tc module	12.1.1.4
Extreme Networks G48Te2 module	12.1.1.4
Microsoft Windows running	2003 Server Enterprise Edition
Active Directory Users and Computers	5.2.3790.1830
Internet Authentication Service	5.2.3790.1830
DHCP Server	5.2.3790.1830

### 4. Configure Extreme Networks BlackDiamond 8810

This section describes the configuration for Extreme Networks BD 8810 switch as shown in **Figure 1** using the Command Line Interface (CLI).

1. Log into the BD 8810 switch using the appropriate credentials.

```
Login: username  
Password: *****
```

2. Create and configure the voice and data VLANs. The voice-G650 VLAN is assigned an IP address for the purpose of performing RADIUS authentication. All routing is performed by a router (not shown) inside the Core IP Network. The VLAN name that the Avaya IP Telephones uses must start with the key word “voice”. This key word is used by Avaya IP Telephone to identify which VLAN it should associate with when it receives the VLAN name advertised by LLDP.

```
BD-8810.1 # create vlan voice-G650  
BD-8810.1 # configure vlan voice-G650 tag 10  
BD-8810.1 # configure vlan voice-G650 ipaddress 172.28.10.59/24  
BD-8810.1 # create vlan data-G650  
BD-8810.1 # configure vlan data-G650 tag 11
```

3. Assigned VLANs to the appropriate ports. VLANs are only assigned to the uplink ports 3:48 and 4:48. VLAN for ports connecting to Avaya IP Telephones will be dynamically assigned upon successful authentication by the RADIUS server.

```
BD-8810.1 # configure vlan default add ports 3:48, 4:48
BD-8810.1 # configure vlan voice-G650 add ports 3:48, 4:48 tagged
BD-8810.1 # configure vlan data-G650 add ports 3:48, 4:48 tagged
```

4. Enable and configure LLDP information. LLDP is used to advertise call server and file server IP address information. In the sample configuration, LLDP is configured to send the VLAN name, call server, file server and tagging information to Avaya IP Telephone.

```
BD-8810.1 # enable lldp ports 3:1
BD-8810.1 # configure lldp port 3:1 advertise vendor-specific dot1 vlan-name
BD-8810.1 # configure lldp port 3:1 advertise vendor-specific avaya-extreme call-server 172.28.10.7
BD-8810.1 # configure lldp port 3:1 advertise vendor-specific avaya-extreme file-server 172.28.10.12
BD-8810.1 # configure lldp port 3:1 advertise vendor-specific avaya-extreme dot1q-framing tagged
BD-8810.1 # enable lldp ports 4:1
BD-8810.1 # configure lldp port 4:1 advertise vendor-specific dot1 vlan-name
BD-8810.1 # configure lldp port 4:1 advertise vendor-specific avaya-extreme call-server 172.28.10.7
BD-8810.1 # configure lldp port 4:1 advertise vendor-specific avaya-extreme file-server 172.28.10.12
BD-8810.1 # configure lldp port 4:1 advertise vendor-specific avaya-extreme dot1q-framing tagged
```

5. Enable spanning tree protocol. The spanning tree domain (stpd) s0 is the default stpd that exists on the BD 8810. The following command enables the spanning tree domain s0.

```
BD-8810.1 # enable stpd s0
```

6. Enable and configure RADIUS information. IP address 172.28.10.12 is the IP address of the RADIUS server used. The IP address 172.28.10.59 is the IP address used by the BD 8810 to send an authentication request. This IP address along with the shared secret must match what is configured in the RADIUS server shown in **Section 5.2, Step 2-3**.

```
BD-8810.1 # configure radius netlogin primary server 172.28.10.12 1812
client-ip 172.28.10.59 vr VR-Default
BD-8810.1 # configure radius netlogin primary shared-secret 1234567890
```

7. Enable and configure netlogin. Netlogin needs to be enabled globally as well as on the individual port. The temp VLAN serves as the temporary holding VLAN for any un-authentication port.

```
BD-8810.1 # enable radius netlogin
BD-8810.1 # create vlan temp
BD-8810.1 # configure netlogin vlan temp
```

```
BD-8810.1 # enable netlogin dot1x
BD-8810.1 # enable netlogin ports 3:1, 4:1 dot1x
```

8. Configure the qosprofile for Avaya VoIP traffic. Assign the 802.1p and DiffServ Code Point (DSCP) value configured in Avaya Communication Manager to the appropriate priority queue. **Section 8, Step 1** shows these values configured in Avaya Communication Manager.

```
BD-8810.1 # configure dot1p type 6 qosprofile QP7
BD-8810.1 # configure diffserv examination code-point 46 qosprofile QP7
```

9. Save the new configuration.

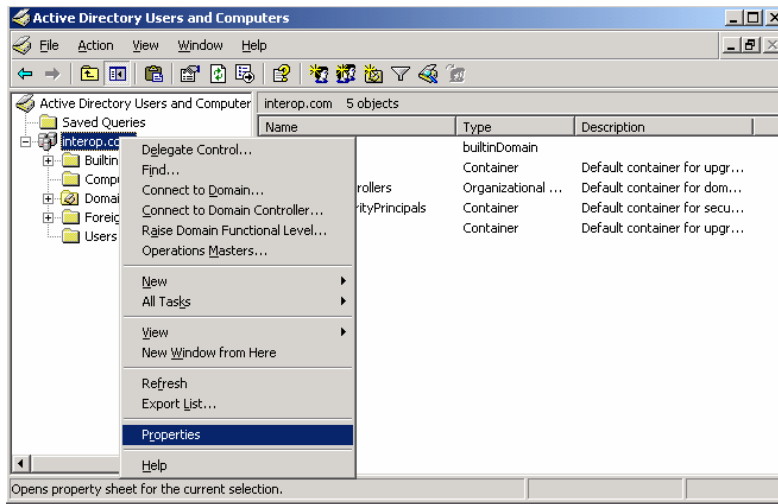
```
BD-8810.1 # save
```

## 5. Configure Microsoft Services

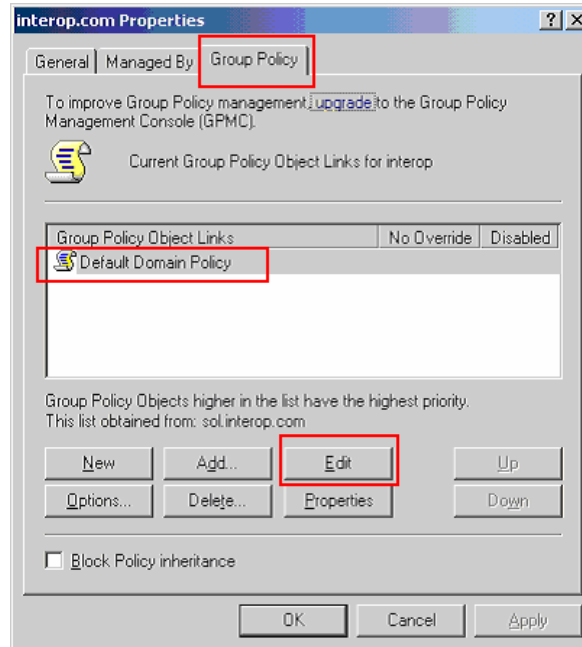
### 5.1. Configure Microsoft Active Directory Service

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

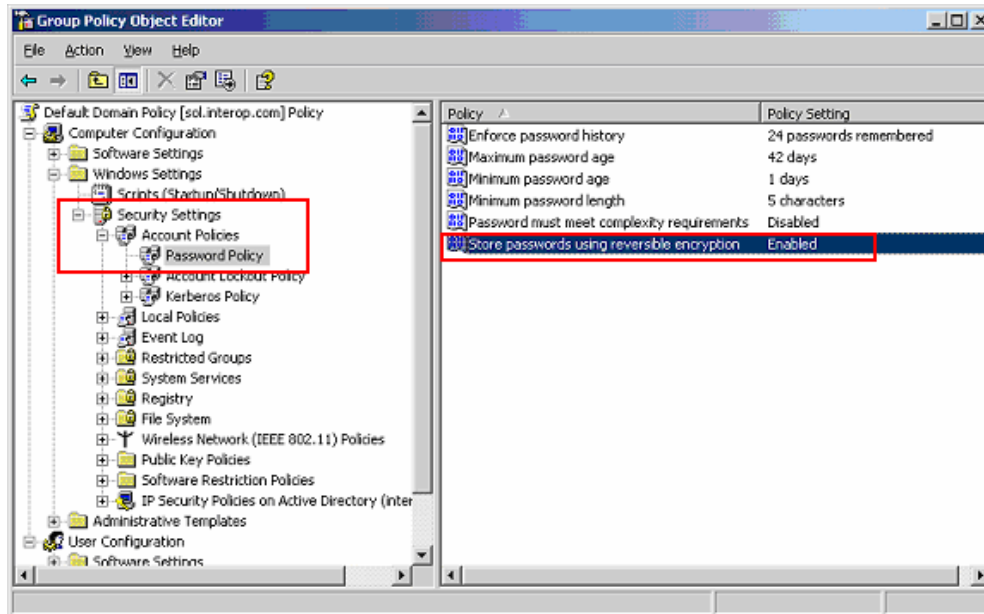
1. Invoke the Active Directory Users and Computers window under Administrative Tools of a Microsoft Windows system. Configure the active directory domain properties by highlighting the Active Directory domain then right click and select **Properties**.



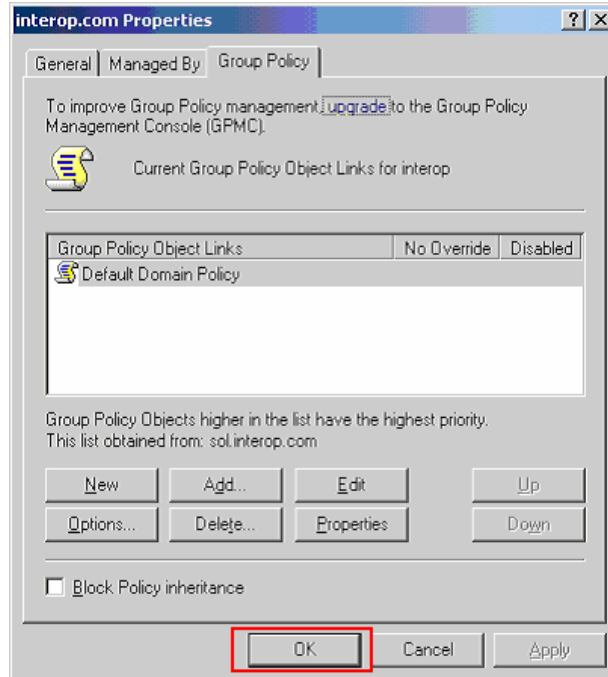
2. Select the **Group Policy** tab in the properties window. Highlight the **Default Domain Policy** then click **Edit** to display the **Group Policy Object Editor**.



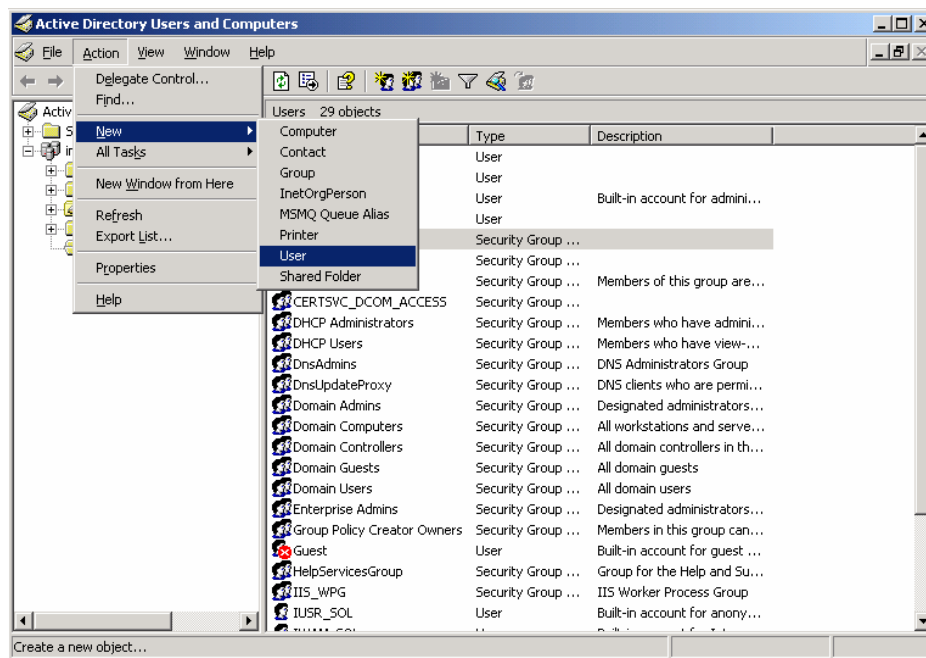
3. From the Group Policy Object Editor, Navigate to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy** on the left panel. Double click on **Store passwords using reversible encryption policy** on the right, and change the setting to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



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



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.



- 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.

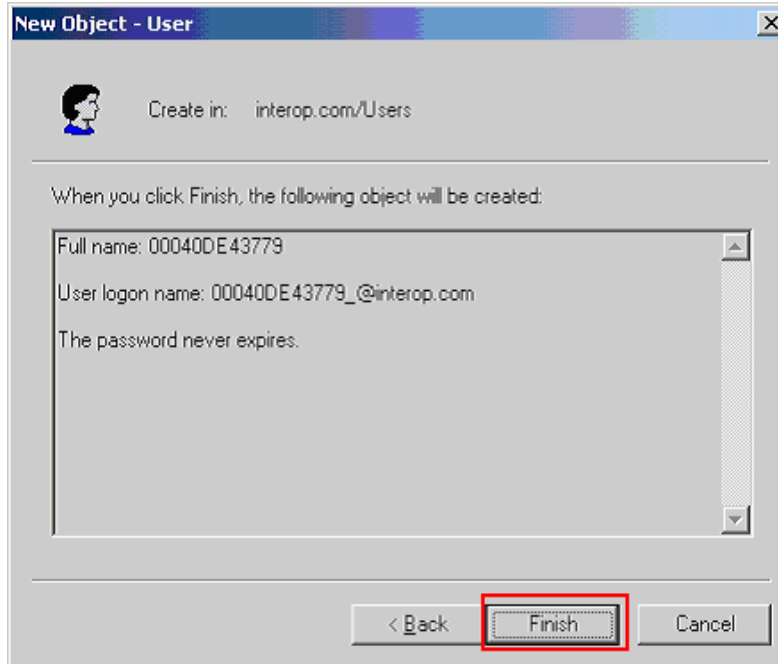
The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'interop.com/Users'. The 'First name' field contains '00040DE43779', and the 'Last name' field is empty. The 'Full name' field contains '00040DE43779'. The 'User logon name' field contains '00040DE43779' and the domain dropdown is set to '@interop.com'. The 'User logon name (pre-Windows 2000)' field contains 'INTEROP\00040DE43779'. The 'Next >' button is highlighted with a red box.

- Enter a **Password** for the user created in **Step 6**. For an Avaya IP Telephone, enter a numeric password. Select the **User cannot change password** and **Password never expires** fields. Click **Next** to continue.

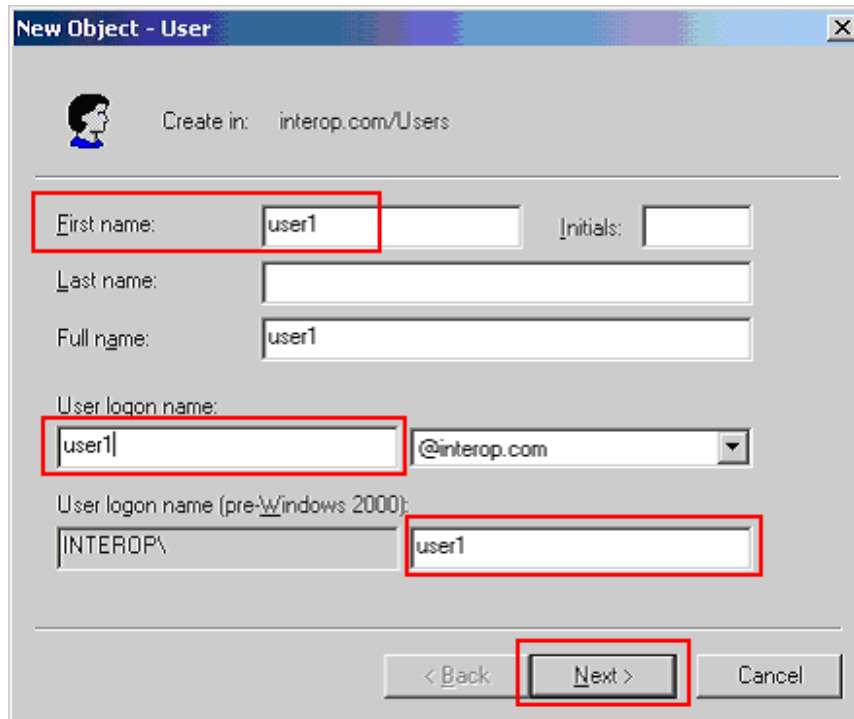
The screenshot shows the 'New Object - User' dialog box. The 'Password' and 'Confirm password' fields are filled with dots and are highlighted with a red box. The 'User cannot change password' and 'Password never expires' checkboxes are checked and highlighted with a red box. The 'Next >' button is highlighted with a red box.



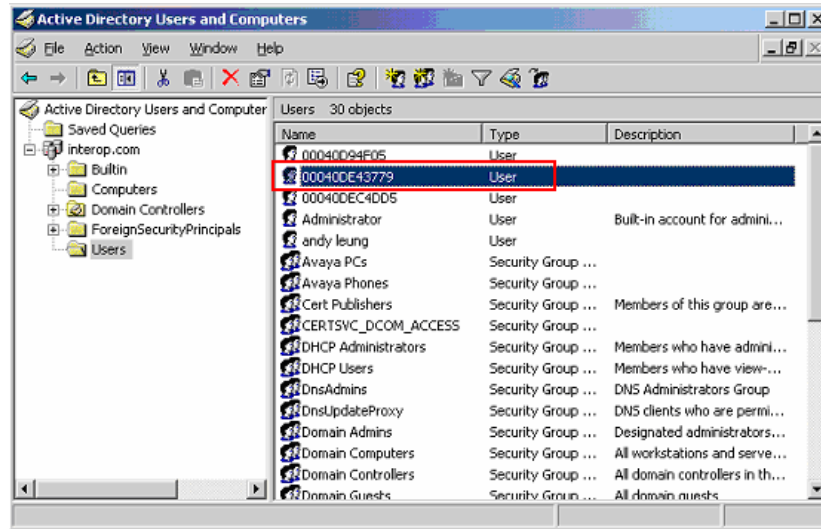
8. Click **Finish** to complete.



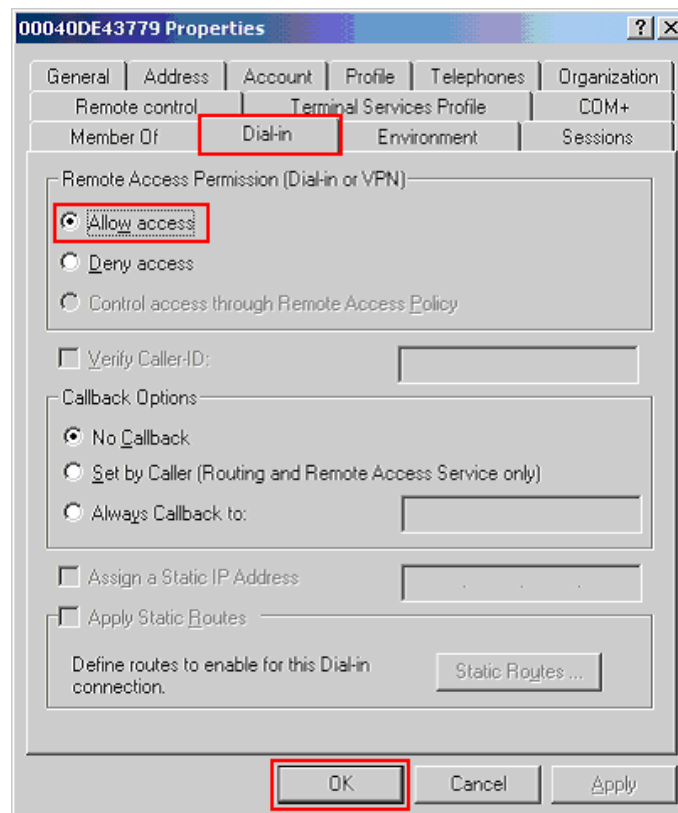
9. Repeat **Steps 5-8** to create a user for the PC. Below is a screen capture for user ID "user1" used by the PC to log in.



10. After creating the user, begin editing its properties by double clicking on the user created in **Step 6-8** in the **Active Directory Users and Computers** window.

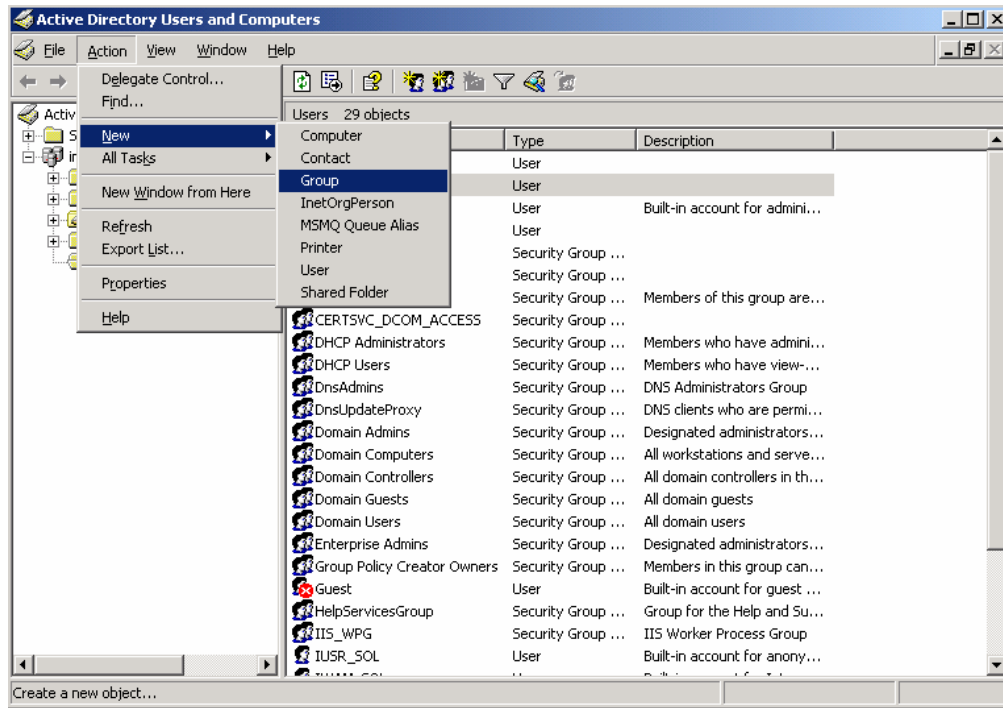


11. Select the **Dial-in** tab in the user **Properties** window. Enable remote access by clicking on the **Allow access** radio button. Click **OK** to complete. Repeat **Steps 10-11** for all Avaya IP Telephone and PC users.

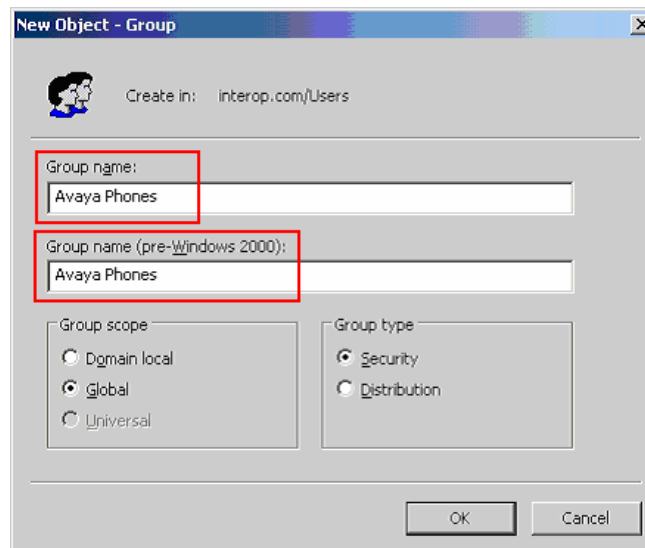


12. Create a new user Group by selecting **Action** → **New** → **Group** from the drop-down menu.

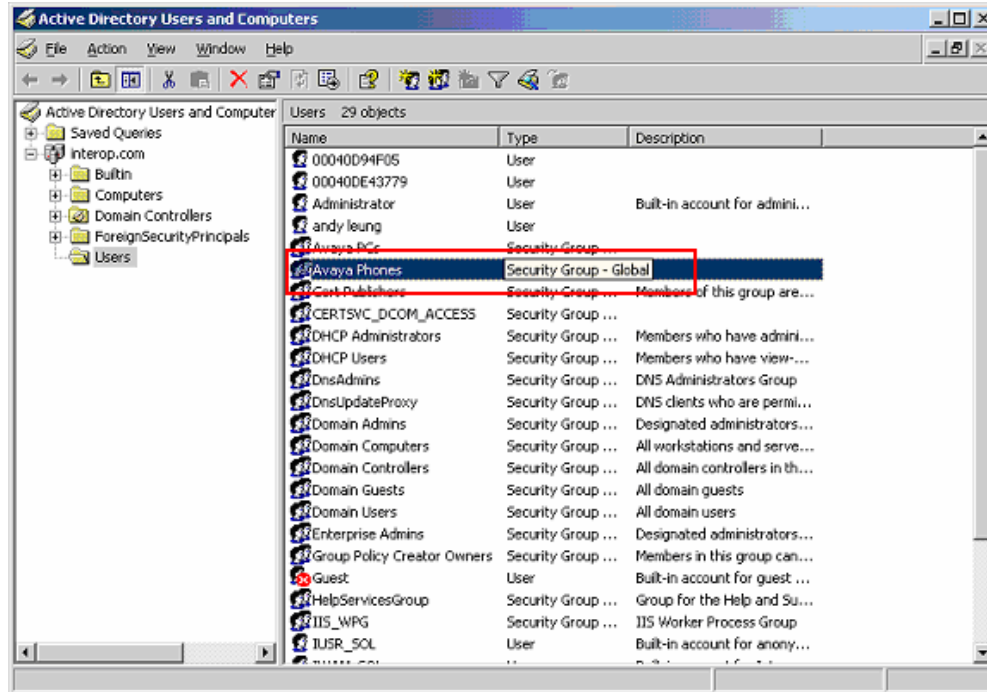
The use of a Group facilitates the assignment and management of additional users.



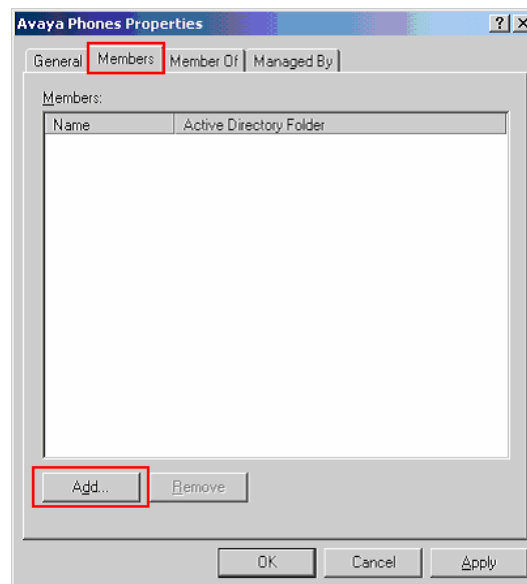
13. Create a group for Avaya IP Telephones. The sample network uses the name **Avaya Phones** for this group. Click **OK** to complete.



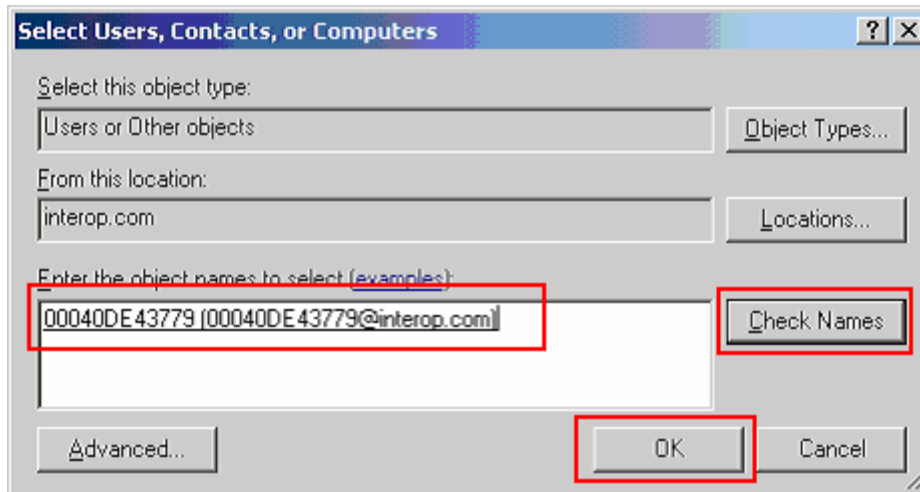
14. Repeat **Steps 12** and **13** to create another user Group for the PC.
15. After creating the user group, begin editing its properties by double clicking on the group in the **Active Directory Users and Computers** window.



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



17. Enter the user that should be assigned to the **Avaya Phones** group. This should be the user for the Avaya IP Telephone. Use **Check Names** to assist in searching for the user. Click **OK** to complete.

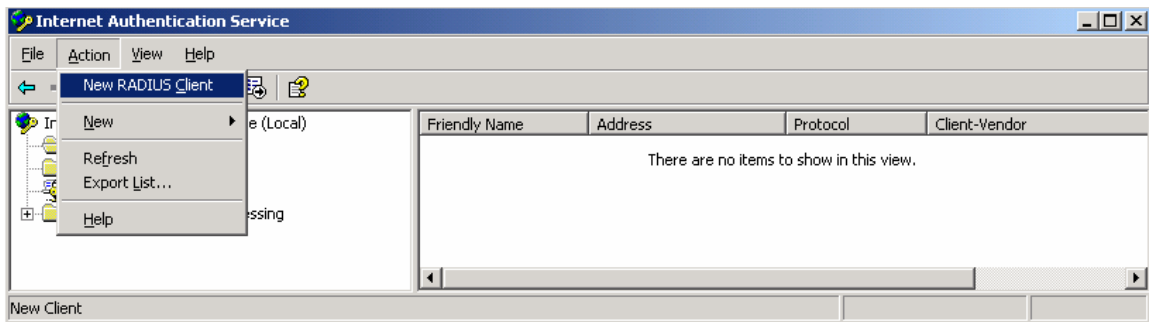


18. Repeat **Steps 15-17** to add members to the PC user group.

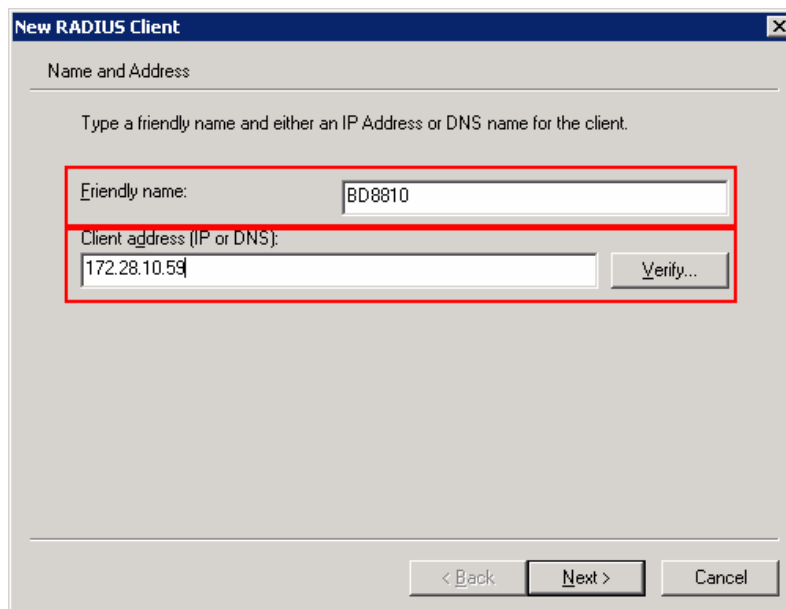
## 5.2. Configure Microsoft Internet Authentication Services (IAS) Server

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

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 the Internet Authentication Service window.



2. Enter the name and IP address of the BD 8810 switch to create a new RADIUS client. This must match the **client-ip** configured in **Section 4, Step 6**. Click **Next** to continue.

The screenshot shows the 'New RADIUS Client' dialog box. The title bar reads 'New RADIUS Client'. The main area is titled 'Name and Address' and contains the instruction: 'Type a friendly name and either an IP Address or DNS name for the client.' There are two input fields: 'Friendly name:' with the value 'BD8810' and 'Client address (IP or DNS):' with the value '172.28.10.59'. A 'Verify...' button is located to the right of the second field. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Enter the **Shared secret** that will be used for this client. This **Shared secret** field value must match the information configured in the switch in **Section 4, Step 6**. 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

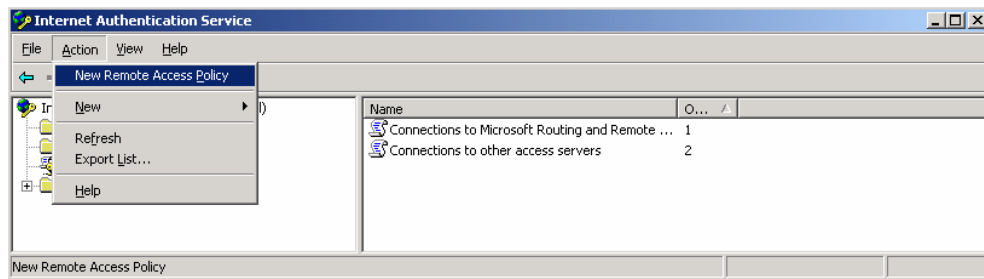
Shared secret: [ ]

Confirm shared secret: [ ]

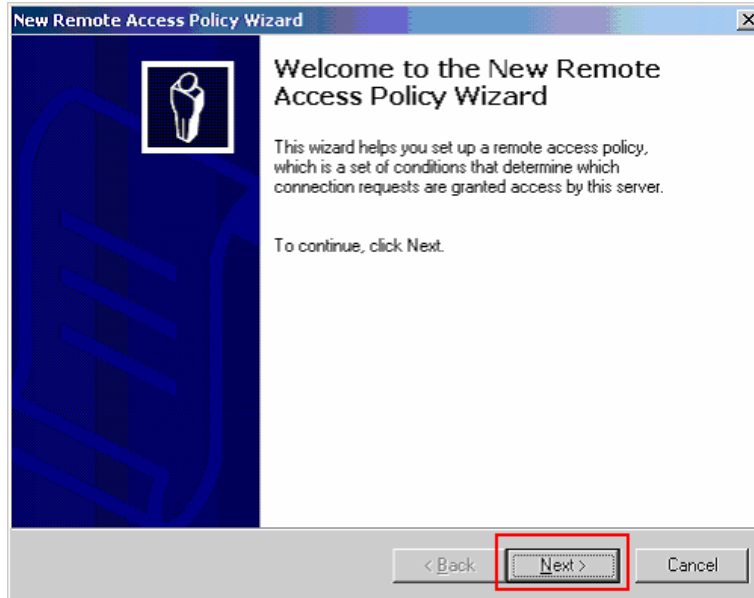
Request must contain the Message Authenticator attribute

< Back Finish Cancel

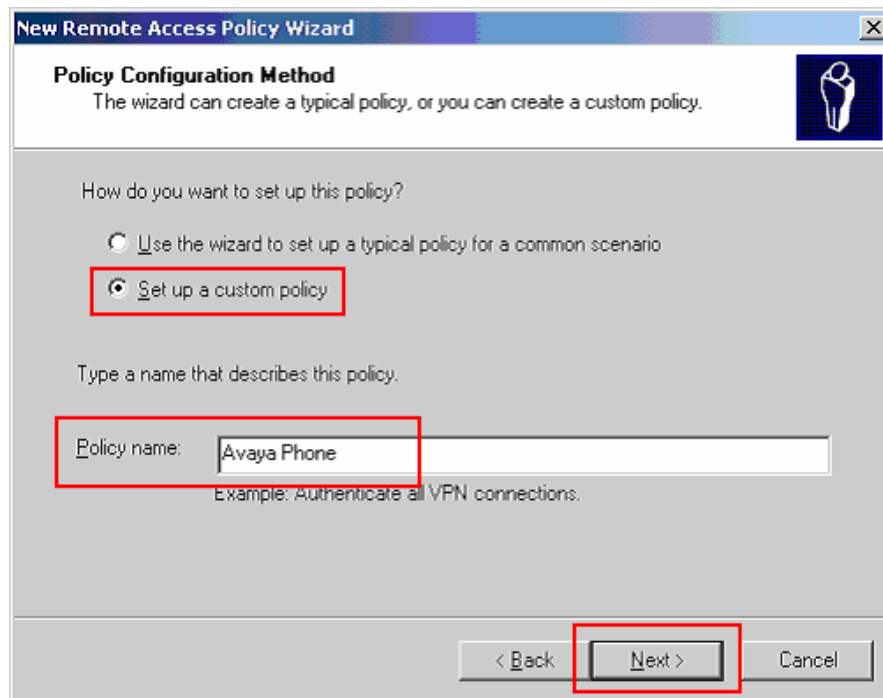
4. Create a new access policy for the Avaya IP Telephones by clicking on **Action** → **New Remote Access Policy**.



5. Click **Next** in the **New Remote Access Policy Wizard**.

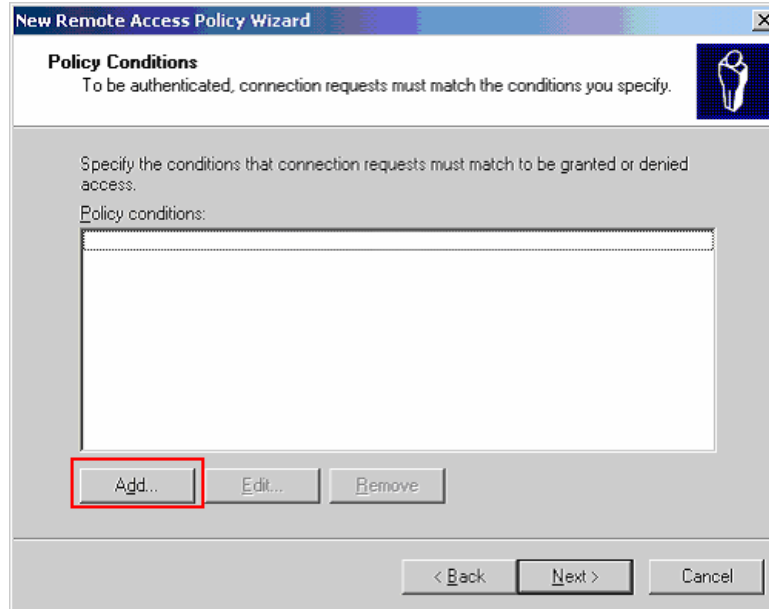


6. Select **Set up a custom policy** radio button and enter a **Policy name**. The sample network uses the name **Avaya Phone**. Click **Next** to continue.

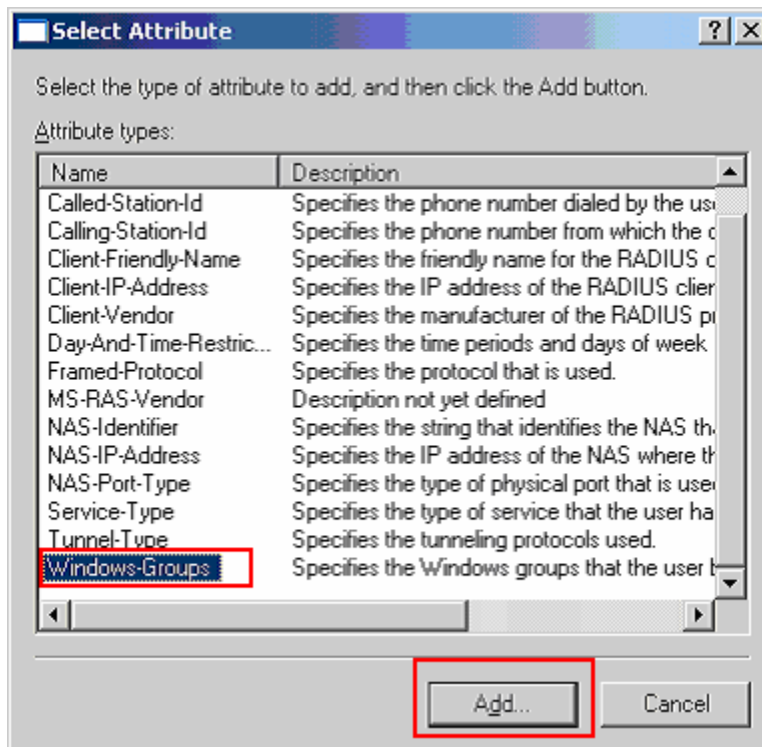




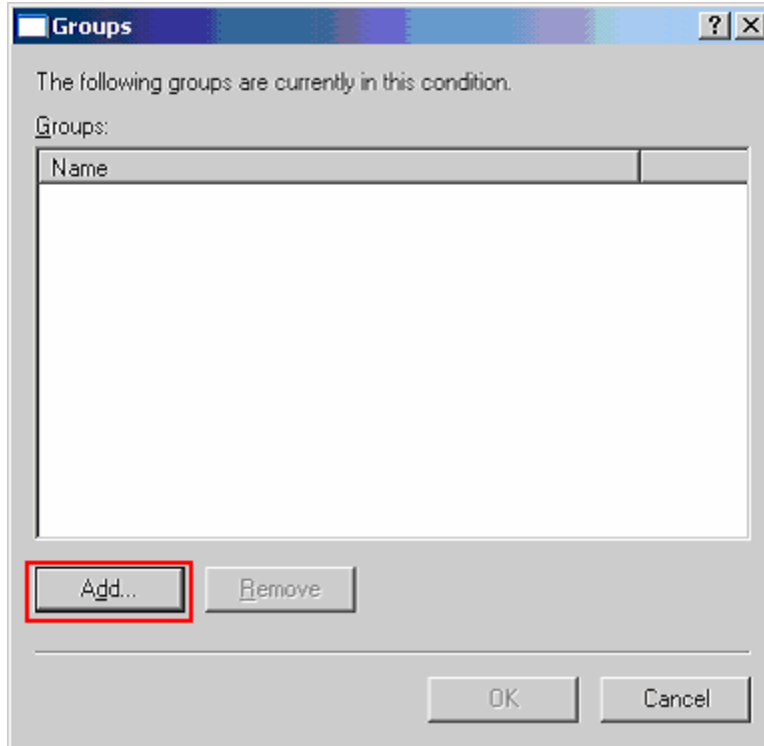
7. Click the **Add** button to add a new policy condition.



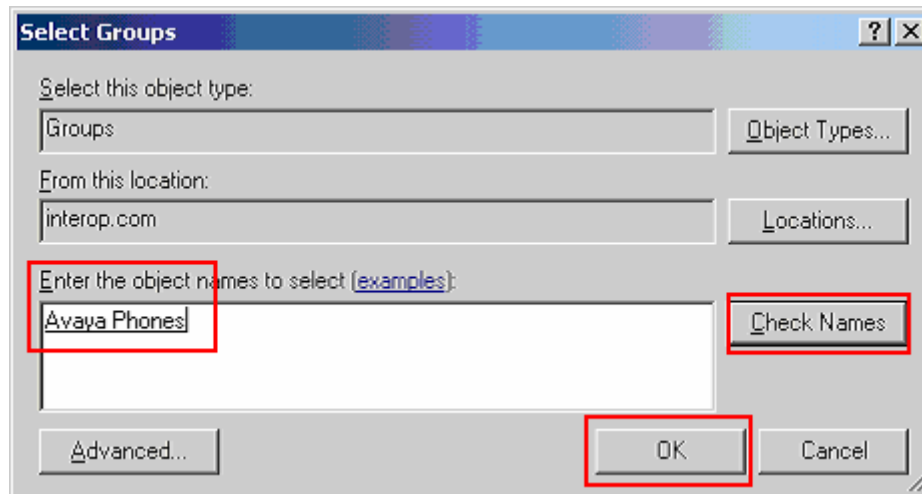
8. Highlight **Windows-Groups** from the **Select Attribute** pop-up window. Click **Add** to continue.



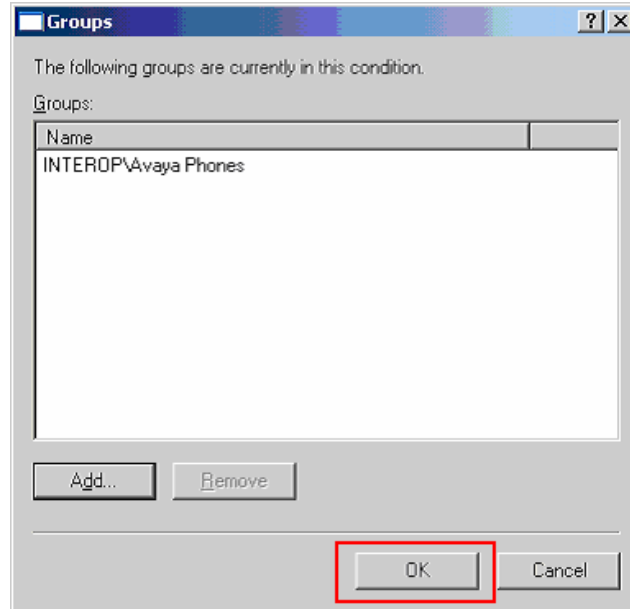
9. Click **Add** in the **Groups** pop-up window to add a windows group.



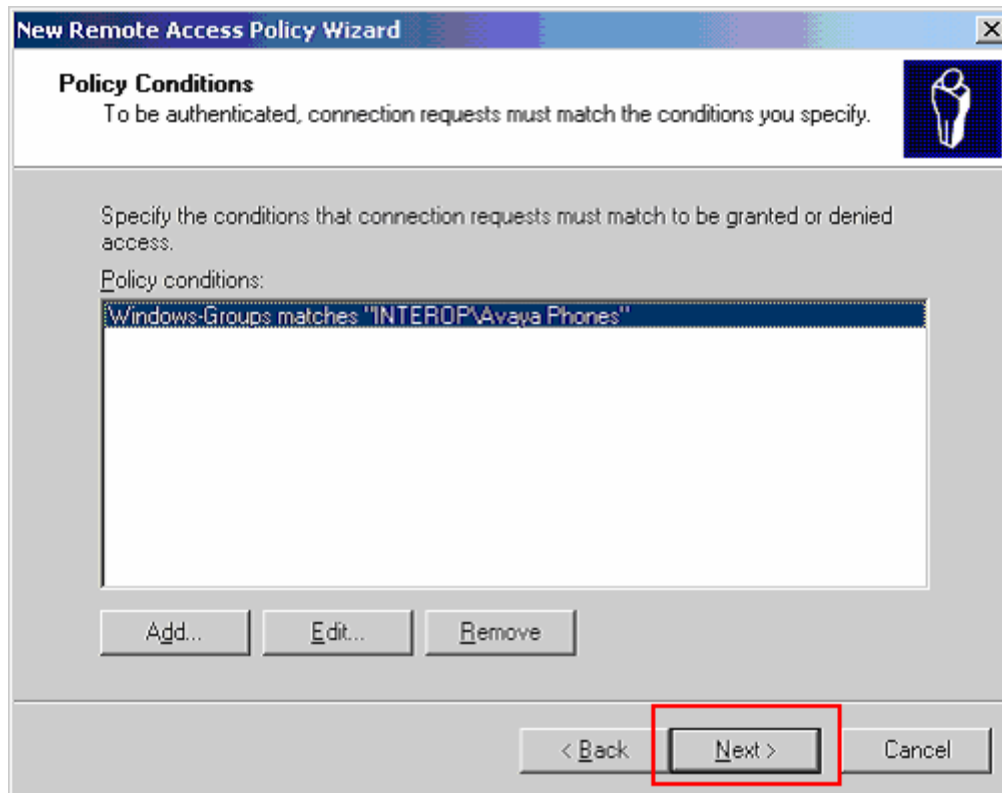
10. Enter the Active Directory user group created in **Section 5.1, Steps 12-13**. Use **Check Names** to assist in searching for the user group. Click **OK** to complete.



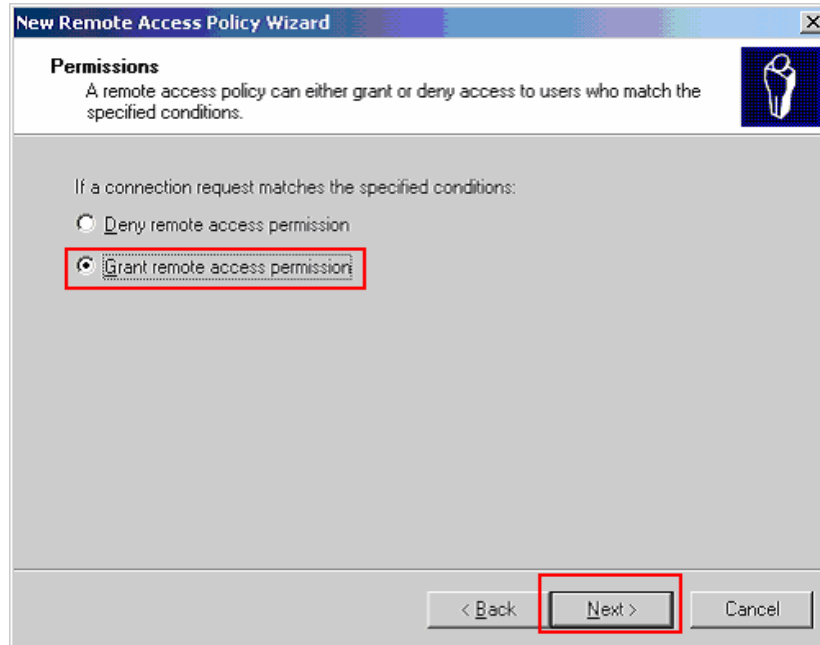
11. Click **OK** in the Groups pop-up windows to complete.



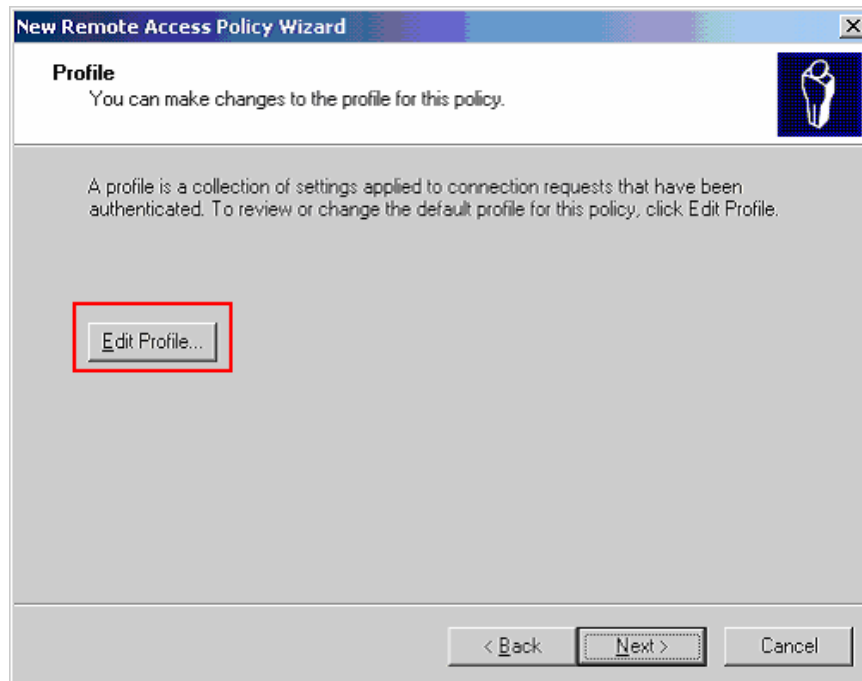
12. Once the windows user group has been added via **Steps 8-11**, click **Next** to continue.



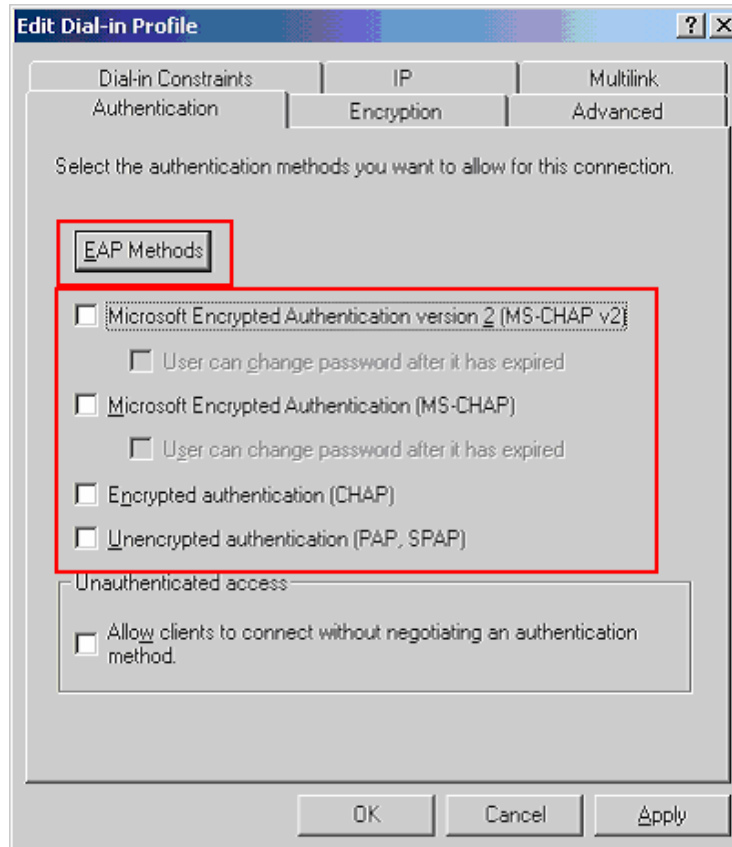
13. Enable the **Grant remote access permission** radio button. Click **Next** to continue.



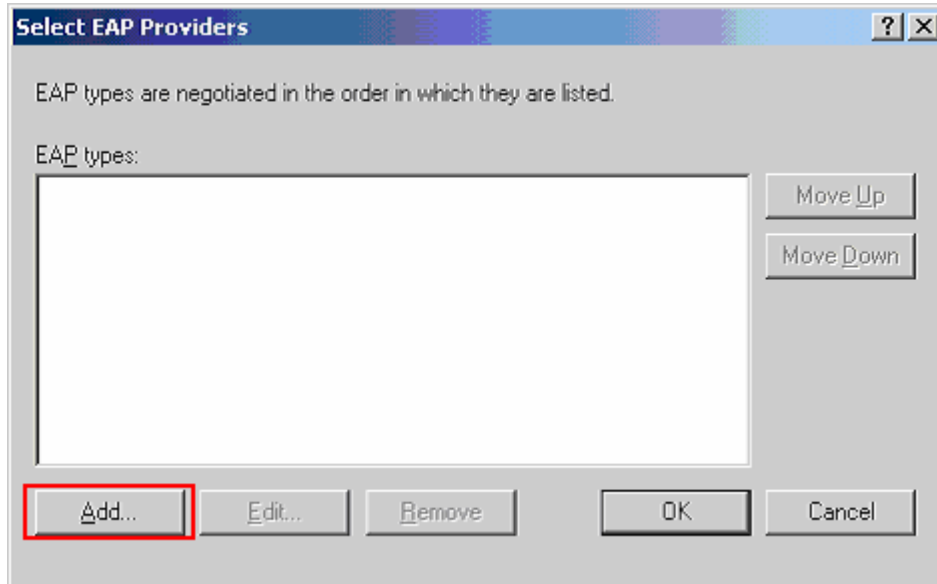
14. Click **Edit Profile** to configure the profile for this access policy. This will display the **Edit Dial-in Profile** pop-up window.



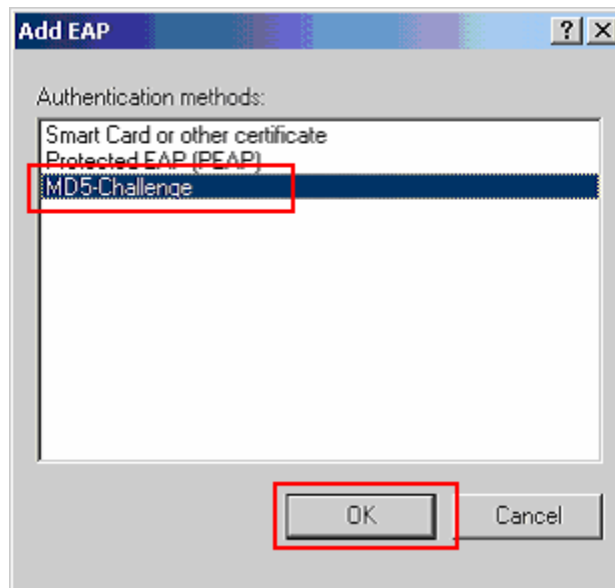
15. Select the **Authentication** tab in the **Edit Dial-in Profile** pop-up window. Uncheck all Microsoft authentication protocols as shown in the screen capture below. Click **EAP Methods** to continue. This will display the **Select EAP Providers** pop-up window.



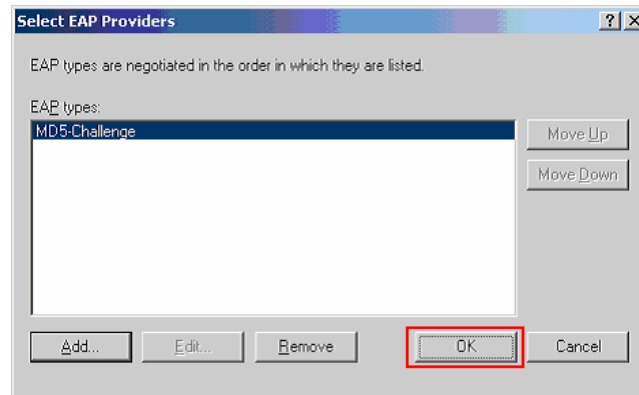
16. Click **Add** in the **Select EAP Providers** pop-up window to add a new EAP type.



17. Select **MD5-Challenge** in the **Add EAP** pop-up window. Click **OK** to continue.



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

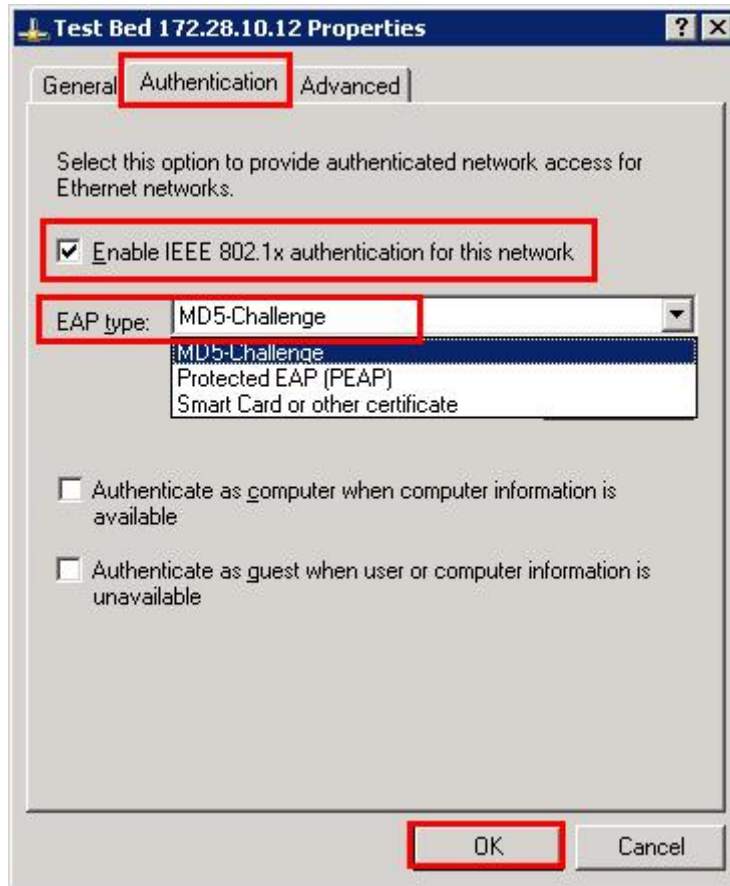


19. Repeat **Steps 4-18** to create an access policy for the PC user.

## 6. Configure the PC

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

1. Open the property 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.





## 7. Configure the Avaya IP Phone

This section shows the steps for configuring the Avaya 4610 SW IP Telephone connected into the BlackDiamond 8810 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 from the IP telephone, the phone will send an EAPOL-Logoff for the attached PC.
- **Supplicant Mode** – Unicast or multicast supplicant operation for the IP telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

Since most 802.1x clients use the multicast MAC address for the 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 BlackDiamond 8810 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 the “#” key to complete the configuration.

Please refer to reference [4] for information regarding how to configure the different 802.1x modes of operation on the 9600 Series telephone.

## 8. Configure Avaya Communication Manager

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

1. Use the “display ip-network-region” command to display the DSCP and 802.1P settings configured in the Avaya Communication Manager. Both DIFFSERV/TOS PARAMETERS for Call Control PHB and Audio PHB priority are set to 46 with 802.1P/Q PARAMETERS for Call Control and Audio set to 6.

```
display ip-network-region 1                               Page 1
of 19                                                    of 19
                                                    IP NETWORK REGION
Region: 1
Location:          Authoritative Domain: interop.com
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? n
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
```

## 9. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the G48Tc and G48Te2 modules in supporting and interoperating with Avaya IP Telephones.

### 9.1. 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 G48Tc and G48Te2 supports the following:

- 802.1D
- 802.1w
- LLDP advertisement & programming of Avaya IP Telephones
- Dynamic native VLAN assignment using RADIUS attributes.
- 802.1x authentication with multiple supplicant per port
- Quality of Server (QoS) support based on 802.1p, DiffServ Code Point (DSCP), or VLAN priority

### 9.2. Test Results

The Extreme Networks G48Tc and G48Te2 modules successfully achieved the above objectives. Quality of Service for VoIP traffic was maintained throughout testing in the presence of simulated competing traffic. 802.1D and 802.1w spanning tree correctly converged when the active link was disconnected or when the bridging priority was changed. LLDP correctly reported the attribute of both Avaya 4600 and 9600 series IP Telephones and was successful in sending call server, file server and tagging information to Avaya IP Telephones. Multiple supplicants support was verified by connecting and successfully gaining access to the network from a PC onto the authentication required Ethernet switch port through an Avaya IP Telephone.

## 10. Verification Steps

The following steps may be used to verify the configuration:

1. Use the **show stpd s0 port** command to verify spanning tree port status

```
* BD-8810.89 # show s0 port
Port   Mode   State      Cost  Flags      Priority Port ID Designated
Bridge
3:1    802.1D FORWARDING 200000 eRppad--- 128     8101
80:00:00:04:0d:3b:4e:ff
4:1    802.1D BLOCKING  200000 eAppad--- 128     8181
80:00:00:04:0d:3b:4e:ff
```

2. Use the **show radius** command to verify whether authentication request was received from the supplicant.

```
BD-8810.7 # show radius
Switch Management Radius: disabled
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   : 172.28.10.59 (VR-Default)
  Shared secret    : 3>:>?75<;5

Access Requests  : 125           Access Accepts    : 62
Access Rejects   : 1             Access Challenges : 62
Access Retransmits: 0           Client timeouts   : 0
Bad authenticators: 0           Unknown types     : 0
Round Trip Time  : 0
```

3. Use the **show dot1p** command to verify dot1p priority assignment.

```
BD-8810.89 # 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 diffserv examination** command to verify DSCP priority assignment.

```
BD-8810.9 # show diffserv examination
CodePoint->QOSProfile mapping:
 00->QP1 01->QP1 02->QP1 03->QP1 04->QP1 05->QP1 06->QP1 07->QP1
 08->QP1 09->QP1 10->QP1 11->QP1 12->QP1 13->QP1 14->QP1 15->QP1
 16->QP1 17->QP1 18->QP1 19->QP1 20->QP1 21->QP1 22->QP1 23->QP1
 24->QP1 25->QP1 26->QP1 27->QP1 28->QP1 29->QP1 30->QP1 31->QP1
 32->QP1 33->QP1 34*>QP7 35->QP1 36->QP1 37->QP1 38->QP1 39->QP1
 40->QP1 41->QP1 42->QP1 43->QP1 44->QP1 45->QP1 46*>QP7 47->QP1
 48*>QP7 49->QP1 50->QP1 51->QP1 52->QP1 53->QP1 54->QP1 55->QP1
 56->QP8 57->QP8 58->QP8 59->QP8 60->QP8 61->QP8 62->QP8 63->QP8
```

- Use the **show port <port#> qosmonitor** command to verify traffic is being sent to the appropriate priority queue.

```
BD-8810.94 # show port 4:48 qosmonitor
Qos Monitor Req Summary                               Mon Aug  4 08:03:40 2008
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
=====
4:48   739387  0      0      0      0      74848  0      1
=====
> indicates Port Display Name truncated past 8 characters
0->Clear counters  U->Page up  D->Page down  ESC->exit
```

- Use the **show lldp detail** command to verify LLDP advertisement is being configured with the appropriate information.

```
BD-8810.55 # show lldp detail
LLDP transmit interval           : 5 seconds
LLDP transmit hold multiplier    : 4 (used TTL = 20 seconds)
LLDP transmit delay              : 2 seconds
LLDP SNMP notification interval  : 5 seconds
LLDP reinitialize delay          : 2 seconds
LLDP-MED fast start repeat count : 3
LLDP Port Configuration:
Port   Rx      Tx      SNMP      Optional enabled transmit TLVs
      Mode   Mode   Notification  LLDP  802.1  802.3  MED  AvEx
=====
3:1    Enabled Enabled  --          --D--  --N    ----  ----  -CFQ
  AvEx Call-Server: IP Address(es)=172.28.10.7
  AvEx File-Server: IP Address(es)=172.28.10.12
  AvEx 802.1Q Framing: Mode=tagged
4:1    Enabled Enabled  --          --D--  --N    ----  ----  -CFQ
  VLAN: voice-G650-andy          ----  --N    ----  ----  ----
  AvEx Call-Server: IP Address(es)=172.28.10.7
  AvEx File-Server: IP Address(es)=172.28.10.12
  AvEx 802.1Q Framing: Mode=tagged
```

```

=====
===
Notification: (L) lldpRemTablesChange, (M) lldpXMedTopologyChangeDetected
LLDP Flags : (P) Port Description, (N) System Name, (D) System
Description
                (C) System Capabilities, (M) Mgmt Address
802.1 Flags : (P) Port VLAN ID, (p) Port & Protocol VLAN ID, (N) VLAN
Name
802.3 Flags : (M) MAC/PHY Configuration/Status, (P) Power via MDI
                (L) Link Aggregation, (F) Frame Size
MED Flags : (C) MED Capabilities, (P) Network Policy,
                (L) Location Identification, (p) Extended Power-via-MDI
AvEx Flags : (P) PoE Conservation Request, (C) Call Server, (F) File
Server
                (Q) 802.1Q Framing

```

7. Use the **show netlogin** command to verify netlogin status and configuration. The abbreviated output below shows both the PC and Avaya IP Telephone have both been authenticated at port 3:1 and port 3:1 been assigned to the corresponding VLANs.

```

BD-8810.82 # show netlogin

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

-----

Port: 3:1, Vlan: data-G650, State: Enabled, Authentication: 802.1x
Guest Vlan <Not Configured>: Disabled
Authentication Failure Vlan <Not Configured>: Disabled
Authentication Service-Unavailable Vlan <Not Configured>: Disabled

MAC                IP address      Authenticated  Type      ReAuth-Timer
User
00:0c:f1:89:e4:64  0.0.0.0         Yes, Radius    802.1x    3477
user1

-----

Port: 3:1, Vlan: voice-G650, State: Enabled, Authentication: 802.1x
Guest Vlan <Not Configured>: Disabled
Authentication Failure Vlan <Not Configured>: Disabled
Authentication Service-Unavailable Vlan <Not Configured>: Disabled

MAC                IP address      Authenticated  Type      ReAuth-Timer
User
00:04:0d:e4:3c:05  172.28.10.53   Yes, Radius    802.1x    3494
00040DE43C05

```

## 11. Support

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

## 12. Conclusion

These Application Notes have described the administration steps required to configure the Extreme Networks G48Tc and G48Te2 modules within the BlackDiamond 8810 switch to support an Avaya VoIP solution using 802.1x authentications depicted in **Figure 1**. The Avaya VoIP solution depicted consists of Avaya Communication Manager running on Avaya S8500 Server with Avaya G650 Media Gateway, and Avaya IP Telephones.

## 13. Additional References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 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 One-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 2.0, Doc# 16-300698, Issue 5, May 2008
- [5] *Avaya IP Telephony Implementation Guide*, May 1, 2006

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

- [6] *ExtremeXOS Concepts Guide*, Software Version 12.1, May, 2008, Part number: 100272-00 Rev. 02
- [7] *ExtremeXOS Command Reference Guide*, Software Version 12.1, May, 2008, Part number: 100273-00 Rev. 02

---

**©2008 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).