AVAYA

Avaya Solution & Interoperability Test Lab

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

Abstract

The IEEE 802.1X standard defines a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. 802.1X provides a means of authenticating and authorizing users attached to a LAN port and of preventing access to that port in cases where the authentication process fails. The Extreme Networks BlackDiamond 8810 supports 802.1X as an authenticator and an Avaya IP Telephone supports 802.1X as a supplicant. Link layer Discovery Protocol (LLDP) is a layer 2 protocol (IEEE standard 802.1AB) that can be used to determine the capabilities of devices. LLDP enables devices to advertise capabilities and media-specific configuration information and to learn information for the connected devices. These Application Notes provide the steps necessary to configure 802.1X and LLDP on the Extreme Networks BlackDiamond 8810 and the Avaya IP telephone with an attached PC. Microsoft Internet Authentication Service is used as the authentication server. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

JZ; Reviewed:
SPOC 12/18/2006
Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.
1 of 39
Extreme-DOT1X.doc

1 Introduction

The 802.1X protocol is an IEEE standard for media-level access control offering the capability to permit or deny network connectivity, control LAN access, and apply traffic policy, based on user or machine identity. The 802.1X protocol consists of three components (or entities):

- Supplicant – a port access entity (PAE) that requests access to the network. For example, an Avaya IP Telephone and the attached PC can be 802.1X supplicants.

- Authenticator – a PAE that facilities the authentication of the supplicant. For example, the Extreme BlackDiamond 8810 functions as an authenticator PAE that controls the physical access to the network based on the authentication status of a supplicant.

- Authentication server – a PAE, typically a Remote Authentication Dial-In User Service (RADIUS) server that actually provides authentication service.

The 802.1X protocol makes use of Extensible Authentication Protocol (EAP) messages. The protocol in 802.1X is called EAP encapsulation over LANs (EAPOL). The Authenticator becomes the middleman for relaying EAP received in 802.1X packets to an authentication server by using the RADIUS format to carry the EAP information.

The IEEE 802.1AB LLDP specification will enable LAN devices to inform each other about their configurations. The 802.1AB standard defines a set of advertisement messages, called type-length-values (TLVs). Avaya IP telephones support TLVs specified in IEEE 802.1AB-2005 and extensions. Through the LLDP protocol, the Avaya IP telephone communicates with the Extreme Networks Switch to learn the voice VLAN ID. There is no longer a need to configure VLAN tagging manually or by DHCP.

LLDP Media Endpoint Discovery (LLDP-MED) protocol is an enhancement to the 802.1AB standard that provides "plug and play" capability for VoIP networks. The Avaya IP telephone's support for LLDP and LLDP-MED extensions provides the ability to use discovered information such as device type, software version and serial number, and other information for inventory management. This same capability also provides a structured workflow for problem diagnosis and root-cause analysis in case of user-reported communication issues.

Figure 1 shows typical 802.1X and LLDP flows for the Avaya IP telephone with an attached PC, the Extreme Networks BlackDiamond 8810 and the Microsoft Internet Authentication Service (IAS). The Avaya IP telephones and the Extreme Networks BlackDiamond 8810 use 802.1-specific information via LLDP to place the Avaya IP telephones in a tagged VLAN.

Avaya IP telephones will be prompted for the 802.1X username and password if the username and password has never been entered (for example, the phone is reset to the manufacturer's default values) or the authentication server rejects the current username and password. The default username is the phone's MAC address. The phone will save the current username and

password entered by a user, which will be used when the phone is restarted (or reset) without resetting its values.
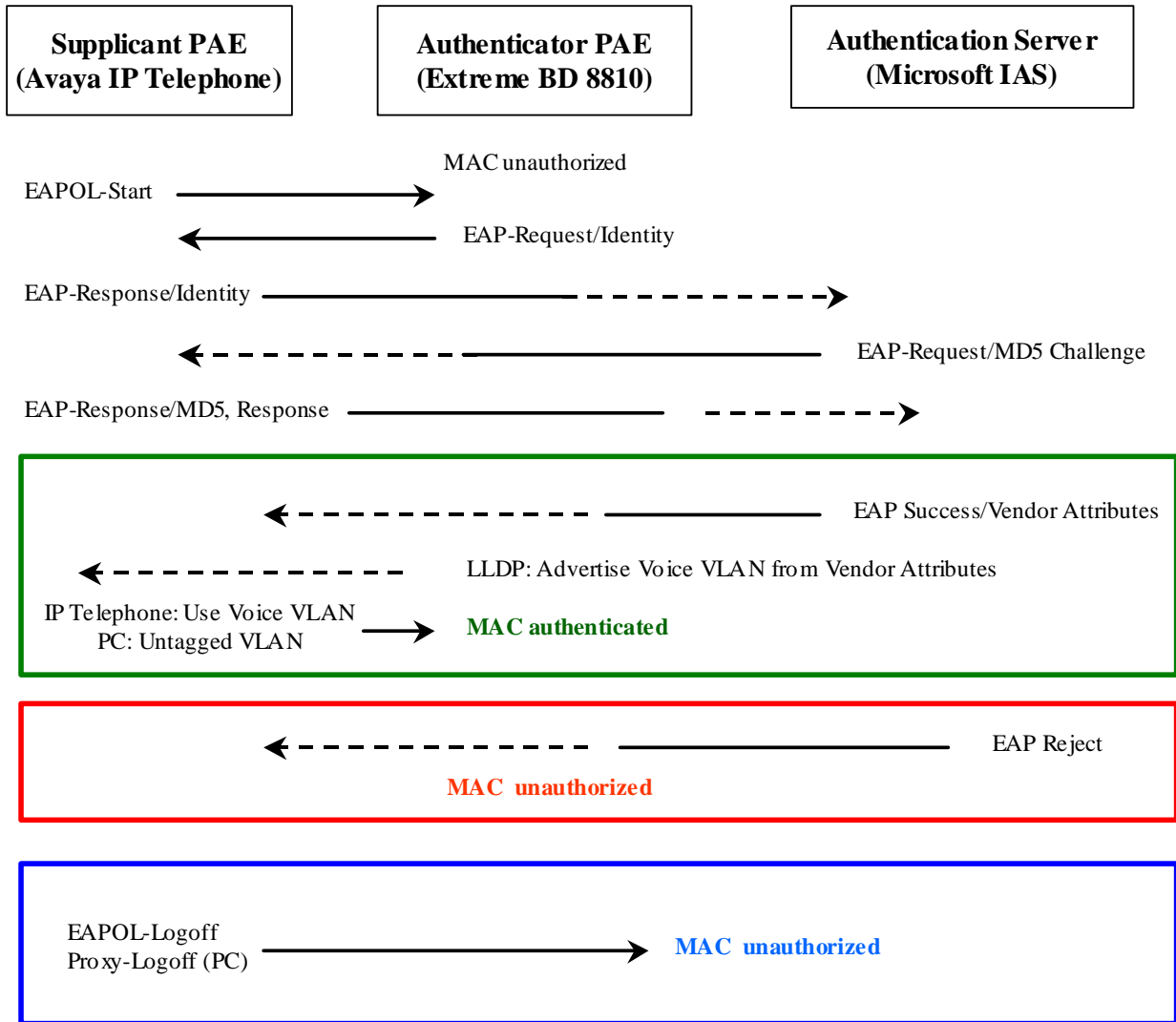
Figure 1: 802.1X Message Exchanges

The following describes the 802.1X flows in **Figure 1**:

1. The supplicant (the Avaya IP Telephone) sends an "EAPOL Start" packet to the authenticator (Extreme Networks BlackDiamond 8810). The IP Telephone will ignore the EAP-request/identity frames from the switch during its booting process.

2. The authenticator responds with an "EAP-Request/Identity" packet to the supplicant.

JZ; Reviewed:
SPOC 12/18/2006

Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.

3 of 39
Extreme-DOT1X.doc

3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator. The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.

4. The authentication server recognizes the packet as an EAP-MD5 type and sends back a challenge message to the authenticator. The authenticator removes the authentication server's frame header and encapsulates the remaining EAP frame into the EAPOL format and then sends it to the supplicant.

5. The supplicant responds to the challenge and the authenticator passes the response onto the authentication server.

6. If the supplicant provides proper identity, the authentication server responds with a success message and associated attributes. The IP telephones logins are configured with the VLAN ID or Name attribute (See **Section 3.2**). No attributes are configured for the PCs. For the IP telephone, the Extreme Networks BlackDiamond 8810 will allow access to the tagged Voice VLAN. For the attached PC, the Extreme Networks BlackDiamond 8810 will allow access to the untagged VLAN.

7. When the VLAN ID or Name attribute is received, the Extreme Networks BlackDiamond 8810 will associate the port connected to the phone to the tagged VLAN, and send the VLAN information to the phone via the LLDP advertisement.

   When the phone recognizes VLAN name "voice" (with any combination of upper/lower case letters) in the LLDP message, the phone will reset and use the VLAN ID. The attached PC is always associated with the untagged VLAN.

8. If the supplicant does not provide proper identity, the authentication server responds with a reject message. The authenticator passes the message onto the supplicant and blocks access to the LAN.

9. When the supplicant logs off, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

10. If the PC attached to the phone is disconnected physically, the phone can be configured to send a proxy logoff message to the authenticator to block the PC access to the LAN (See **Section 3** for details).

Figure 2 shows the network diagram used in these Application Notes. The PCs attached to the Avaya IP telephones are installed with the Funk Odyssey client software (802.1X client software). The Avaya IP Telephones support EAP-MD5 authentication. EAP-MD5 is also used for the attached PCs in these Application Notes.
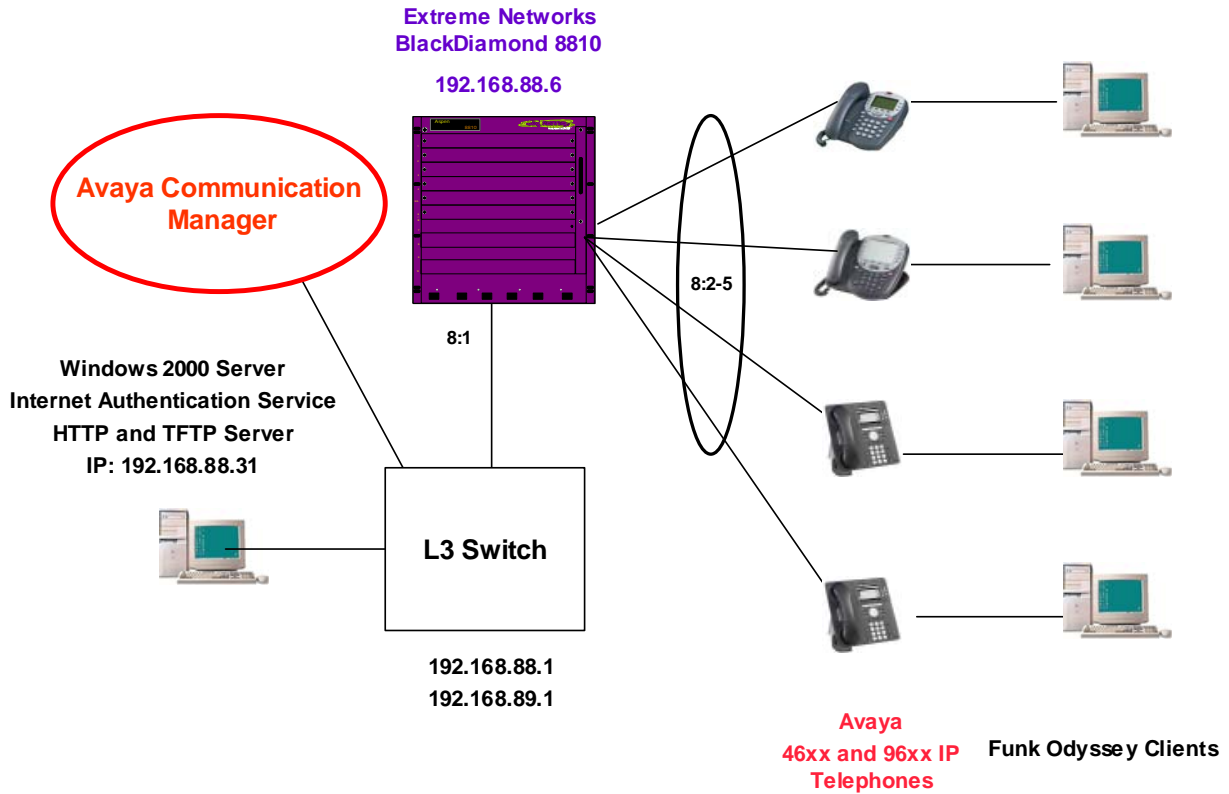
Figure 2 – 802.1X Configuration With Avaya IP Telephones

2 Equipment and Software Validated

Table 1 below shows the versions verified in these Application Notes.

Equipment	Software
Avaya Communication Manager (Avaya S8500 Media Server with Avaya G650 Media Gateway)	3.1.2
Avaya 9610 IP Telephone	1.2 H.323 (1_20r19)
Avaya 9620 IP Telephone	1.2 H.323 (1_20r19)
Avaya 9630 IP Telephone	1.2 H.323 (1_20r19)
Avaya 9640 IP Telephone	1.2 H.323 (1_20r19)
Avaya 9650 IP Telephone	1.2 H.323 (1_20r19)
Avaya 4610SW IP Telephone	2.6
Avaya 4620SW IP Telephone	2.6
Avaya 4621SW IP Telephone	2.6
Avaya 4622SW IP Telephone	2.6
Avaya TFTP Server (for 4600-Series Telephones)	3.6.1
Extreme Networks BlackDiamond 8810 with G48P-41512 Blade	11.5.2.8 XOS
Apache HTTP Server (for 9600-Series Telephones)	2.0.54
Microsoft Internet Authentication Service (IAS)	Microsoft Windows 2000 Advanced Server
Funk Odyssey Client	4.30

Table 1: Equipment and Software Validated

3 Configurations

The Extreme Networks XOS supports an Avaya IP telephone with an attached PC to be individually and independently authenticated. To put the IP telephone in a tagged VLAN, the 802.1-specific information must be configured on the Extreme Networks BlackDiamond 8810 and the Authentication Server.

Avaya IP telephones support three 802.1X operational modes. The operational mode can be changed by pressing "mute80219#" ("mute8021x") on the Avaya 4600-Series IP telephones or by pressing the Craft Access Code (the default is "mutecraft#" or "mute27238#") 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 telephone itself, with PAE multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected from the IP telephone, the phone will send an EAPOL-Logoff for the attached PC.

- **Supplicant Mode** – Unicast or multicast supplicant operation for the IP telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

Since most 802.1X clients use the Multicast MAC address for the EAPOL messages, the IP telephone must be configured to the **pass-thru** or **p-t w/Logoff** mode to pass-through these Multicast 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 Extreme Networks BlackDiamond 8810 receives the logoff message, the PC will be removed from the authorized MAC list.

3.1 Configuring 802.1X and LLDP on the Extreme Networks BlackDiamond 8810

The Extreme Networks XOS supports network login. Network login controls the admission of user packets into a network by allowing MAC addresses from users that are properly authenticated. When network login is enabled on a port, that port does not forward any packets until authentication takes place.

Network login is capable of three types of authentication: web-based, MAC-based and 802.1X. 802.1X will be used in these Application Notes.

The following screen shows the annotated netlogin and dot1x configuration.

```
! --- Configure a "temp" VLAN used by netlogin
create vlan "temp"

! --- Enable network login
enable radius netlogin

! --- Configure network login on a "temp" VLAN
configure netlogin vlan temp

! --- Enable 802.1x globally
enable netlogin dot1x

! --- Enable 802.1x re-authentication for a high security
configure netlogin dot1x timers server-timeout 30 quiet-period 60 reauth-
period 3600 supp-resp-timeout 30
```

The following screen shows the BlackDiamond 8810 Voice VLAN configuration. The Voice VLAN is configured with VLAN ID 88 and IP address 192.168.88.6. Port 8:1 is connected to the L3 switch and is configured with tagged VLAN 88.

```
create vlan "Voice"
configure vlan Voice tag 88
configure vlan Voice ipaddress 192.168.88.6 255.255.255.0
enable ipforwarding vlan Voice
configure vlan Voice add ports 8:1 tagged
```

The BlackDiamond 8810 is configured to use Microsoft IAS as a RADIUS server. The following screen shows the configuration. The Microsoft IAS runs on port 1812 with IP address 192.168.88.31. The shared secret must match the Microsoft IAS configuration.

```
configure radius netlogin primary server 192.168.88.31 1812 client-ip
192.168.88.6 vr VR-Default
configure radius netlogin primary shared-secret 1234567890123
```

The following shows the configuration for VLAN 89. Ports 8:2 through 8:5 are connected to the Avaya IP telephones and are configured with the untagged VLAN 89. The attached PCs will be associated with VLAN 89. Port 8:1 is connected to the L3 switch and is configured with tagged VLAN 89.

```
create vlan "data-vlan"
configure vlan data-vlan tag 89
configure vlan data-vlan add ports 8:1 tagged
configure vlan data-vlan add ports 8:2-5 untagged
```

Enable 802.1X on ports 8:2 through 8:5.

```
enable netlogin ports 8:2-5 dot1x
```

Microsoft IAS will be configured (**Section 3.3**) to send tagged VLAN 88 via Vendor Specific Attribute (VSA) 211 to the BlackDiamond 8810. When the BlackDiamond 8810 receives the VSA, the BlackDiamond 8810 will move the phone's MAC address to the forwarding database in VLAN 88. The ports will be dynamically assigned to tagged VLAN 88.

When LLDP and LLDP-MED are enabled on ports 8:2 through 8:5, the BlackDiamond 8810 will send the VLAN 88 associated with the VLAN named "Voice" to the phones when the ports are configured to **advertise vendor-specific dot1 vlan-name**. An Avaya IP Telephone receiving this information will reset and use VLAN 88.

To limit the delay for the phone to receive the dynamic LLDP advertisement, configure the LLDP transmit interval to be 5 seconds or less.

```
! --- Enable LLDP
enable lldp ports 8:2-5

! --- Enable LLDP Media Capabilities
configure lldp port 8:2-5 advertise vendor-specific med capabilities

! --- Enable ports 8:2-5 to advertise vlan-names.
configure lldp port 8:2-5 advertise vendor-specific dot1 vlan-name


! --- Configure LLDP transmit interval to 5 seconds on ports 8:2-5
configure lldp transmit-interval 5
```
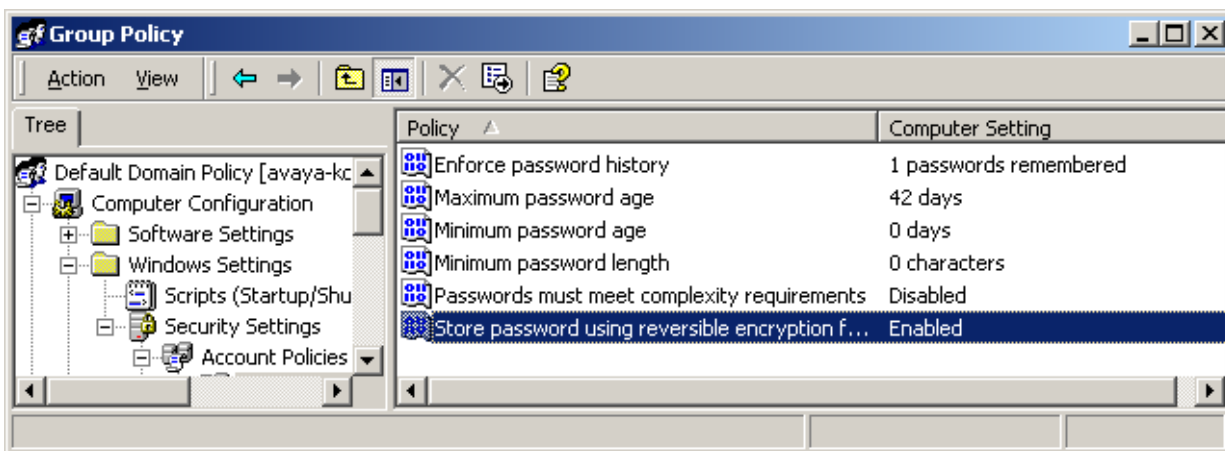
3.2 Configuring the Active Directory Server

In the sample configuration, the Microsoft IAS and the active directory run on the same Microsoft Advanced 2000 Server. The intent of this section is to illustrate relevant aspects of the configuration used for the testing.

Configure passwords to be stored using reversible format to support EAP-MD5. This step is required for MD5.
- From the **Active Directory Users and Computers** screen, right-click the Active Directory domain and select **Properties**.
- Select **Group Policy,** highlight **Default Domain Policy** and click the **Edit** button.
- Set **Store password using reversible encryption to** be **Enabled** for the password policy under Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy tree.

JZ; Reviewed:
SPOC 12/18/2006
Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.
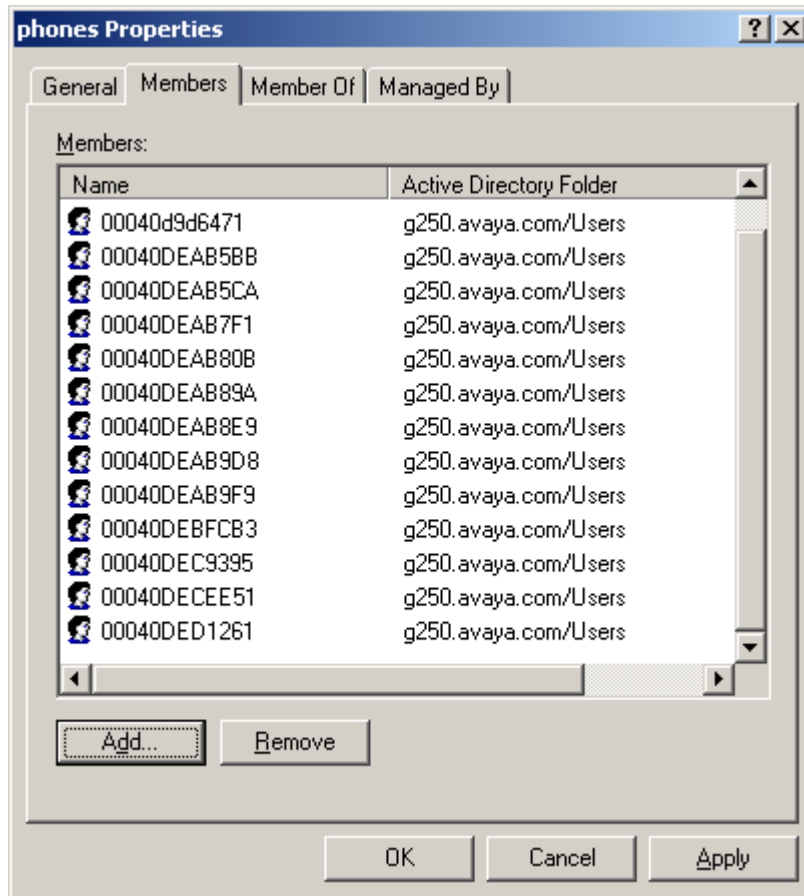9 of 39
Extreme-DOT1X.doc

Create user names and passwords for the phones and PCs. Configure the phone's MAC as its user name. The default user name for the phone is its MAC address (without colons) with upper case letters. To enable Dial-In access and Password Reversible Encryption, check **Store password using reversible encryption** under the **Account** tab. Note that user names are not case sensitive on the Microsoft IAS.
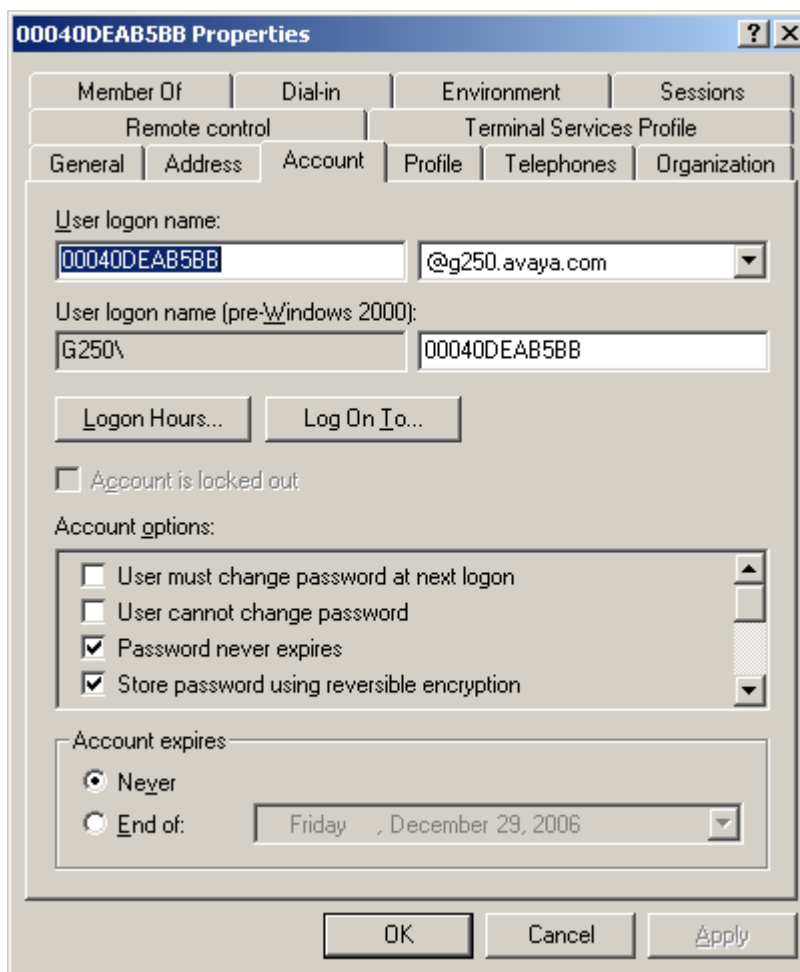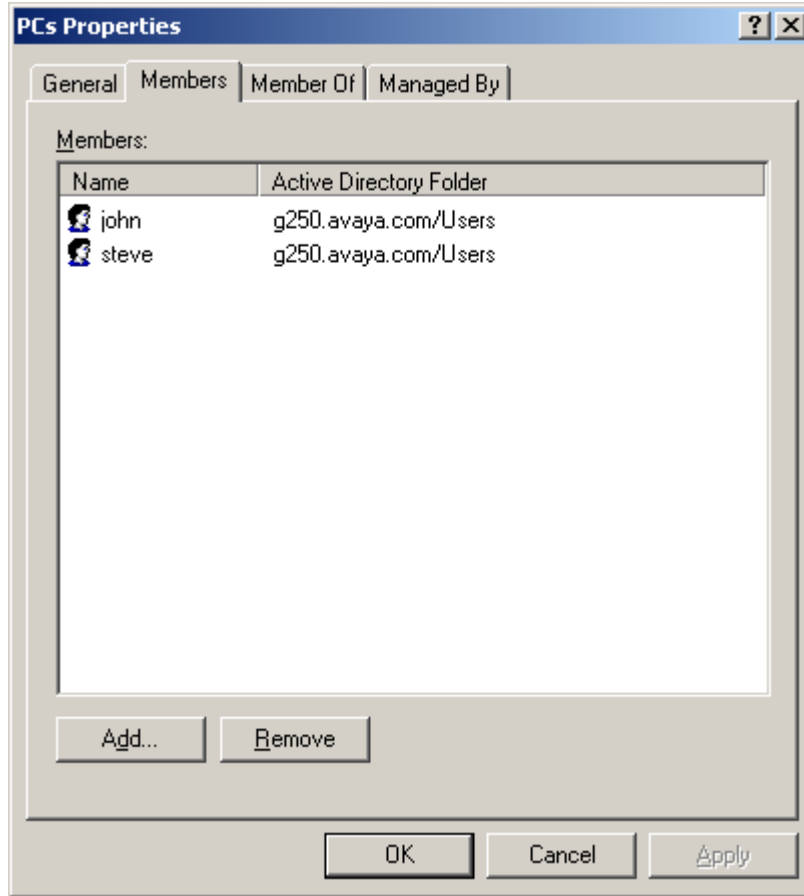
To enable remote access for a user, from a user account **Properties,** select **Allow access** for **Remote Access Permission** under the **Dial-in** tab.
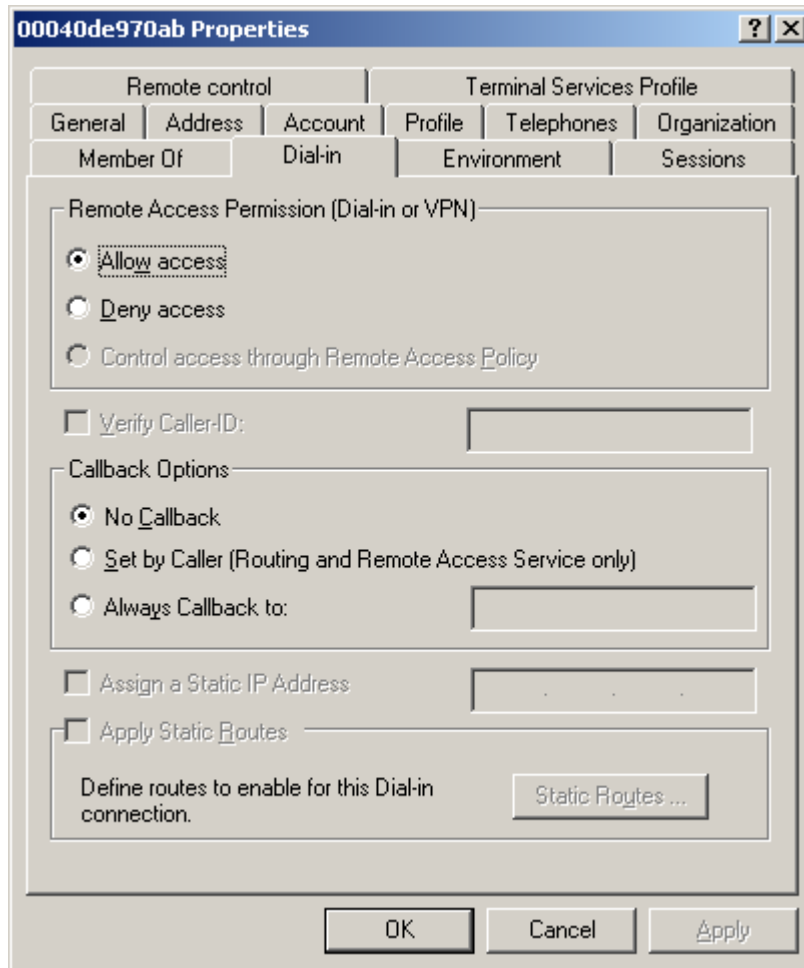
Create a user group named "phones" and add the phones (usernames: MACs of the phones) to the group.
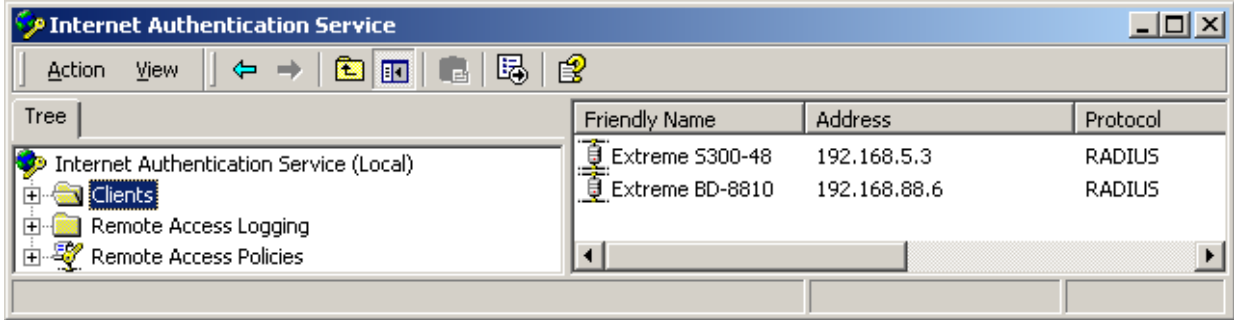
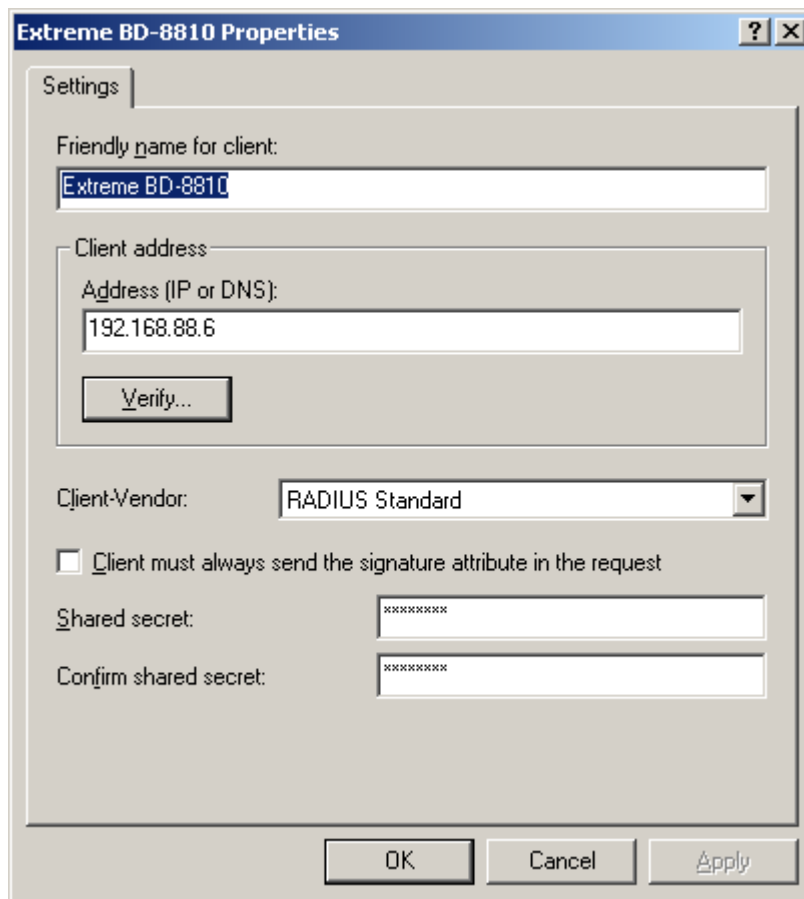Create a user group named "PCs" and add the PCs to the group.

Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.

3.3 Configuring the Microsoft IAS

Open the Microsoft IAS by **Start** → **Programs** → **Administrative Tools** → **Internet Authentication Service**. Right click **Clients** and select **New Client** to add a new client.

The following shows the client configuration for the BlackDiamond 8810. The **Client address** and **Shared secret** must match the configuration on the Extreme Networks BlackDiamond 8810 in **Section 3.1**.

JZ; Reviewed:
SPOC 12/18/2006
Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.
14 of 39
Extreme-DOT1X.doc

The following shows the **Remote Access Policies** for the IP telephones. As configured in **Section 3.2**, the user group "phones" consists of the Avaya IP telephones. Select **Grant remote access permission** under **If a user matches the conditions**.
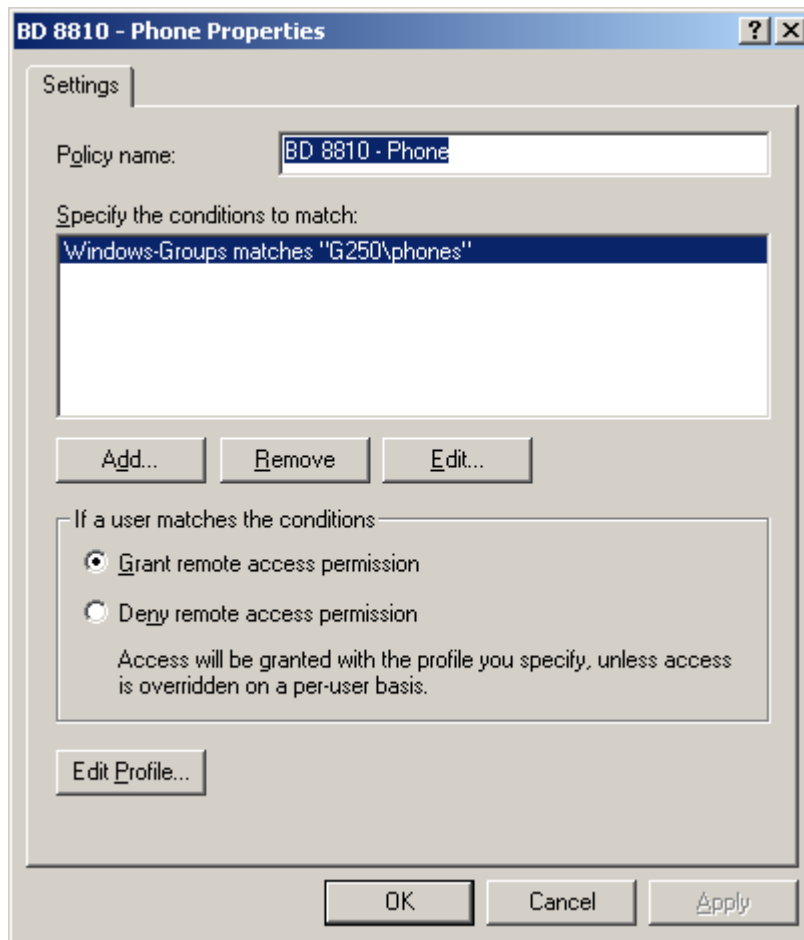
Click **Edit Profile…** button and select the **Authentication** tab. Check the **Extensible-Authentication Protocol** and select **MD5-Challenge** under **Select the EAP type which is acceptable for this policy**.
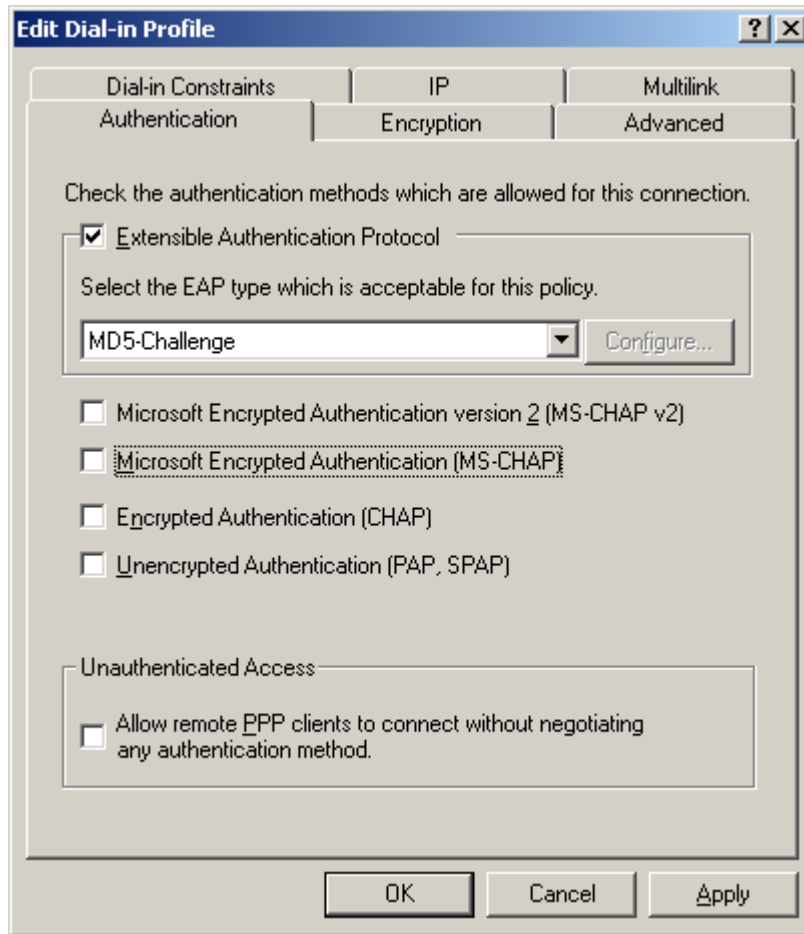
Click the **Advanced tab** and Click **Add….** to display the following screen.
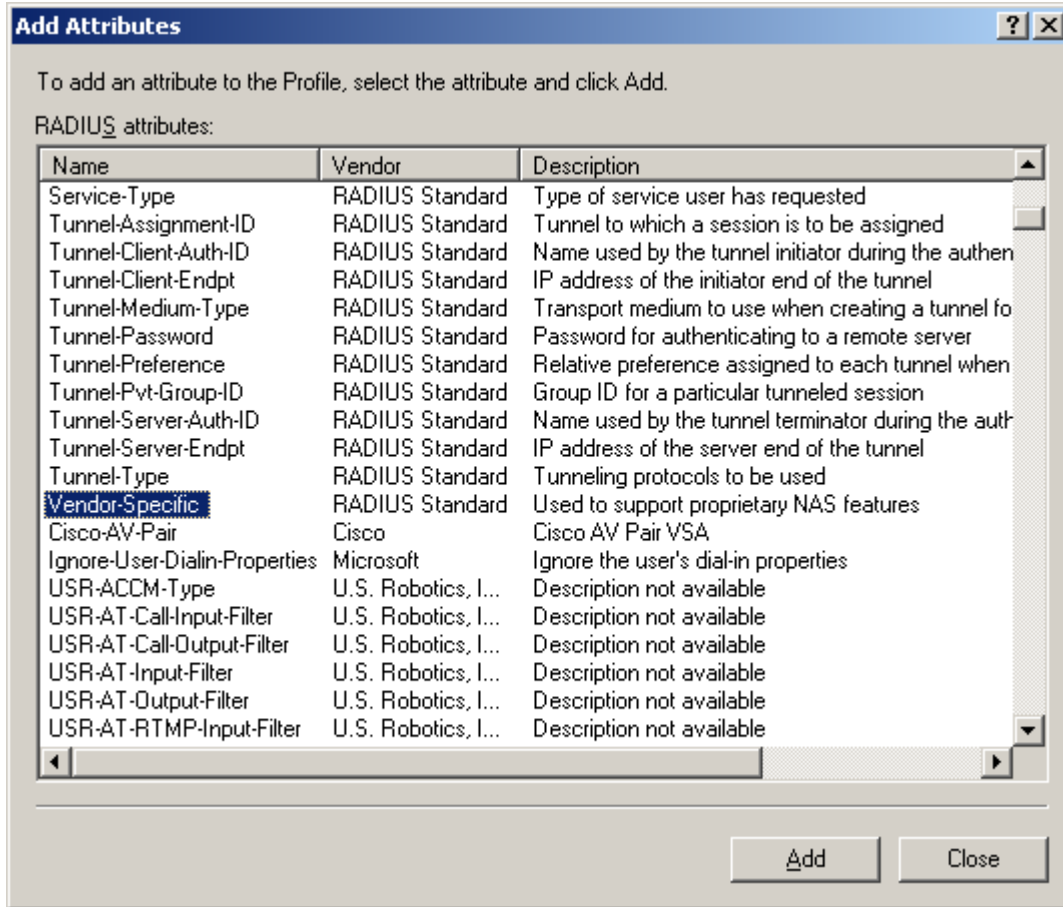
From the prior screen, select **Vendor-Specific** in the **RADIUS attributes** and click the **Add…**
button. The following screen appears.

Click the **Add** button, and the following screen appears. Select **Enter Vendor Code** under **Specific network access server vendor** and enter the value 1916, which is the Extreme Networks Vendor ID.
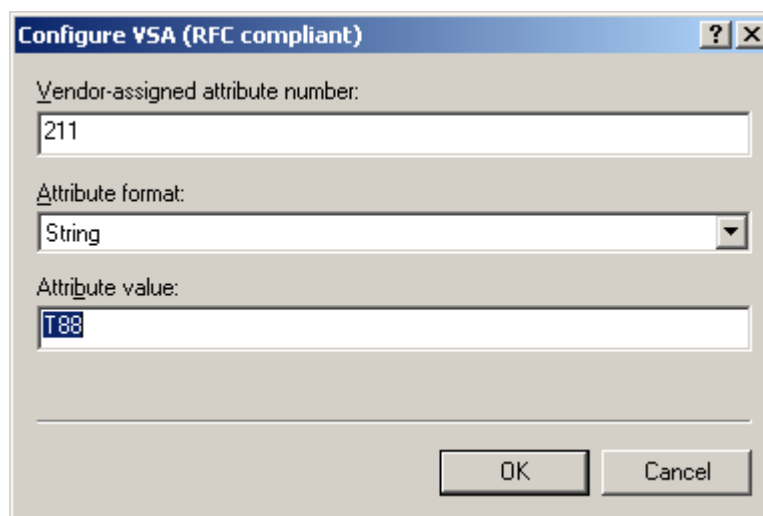
Click the **Configure Attribute…** button and configure the Vendor Specific Attribute (VSA). Enter 211 for the **Vendor-assigned attribute number**. Select String for the **Attribute format**, and T88 or Tvoice for the **Attribute value**. VSA 211 is used to support a tagged VLAN. T88 means tagged VLAN ID 88 and Tvoice means tagged VLAN name voice. Once the Microsoft IAS authenticates the phone, the Microsoft IAS will send VSA 211 to the BlackDiamond 8810. The BlackDiamond 8810 will move the phone's MAC address dynamically into the tagged VLAN (note that VLAN 88 or VLAN voice is not statically configured on ports connected to the phones). The BlackDiamond 8810 will also send this VLAN ID associated with its name "Voice" (configured on the BlackDiamond 8810) to the phone via LLDP Media advertisement. When the phone identifies the VLAN name as "Voice" ("Voice" is a key word), the phone will reset and use this tagged VLAN. The BlackDiamond 8810 will forward tagged "Voice" VLAN packets after the phone is authenticated again. The phone should be able to reach the DHCP and TFTP server and register to Avaya Communication Manager if configured properly.

The following shows the Remote Access Policies for the PCs. As configured in **Section 3.2**, The user group "PCs" consists of the PCs. Select **Grant remote access permission** under **If a user matches the conditions**.
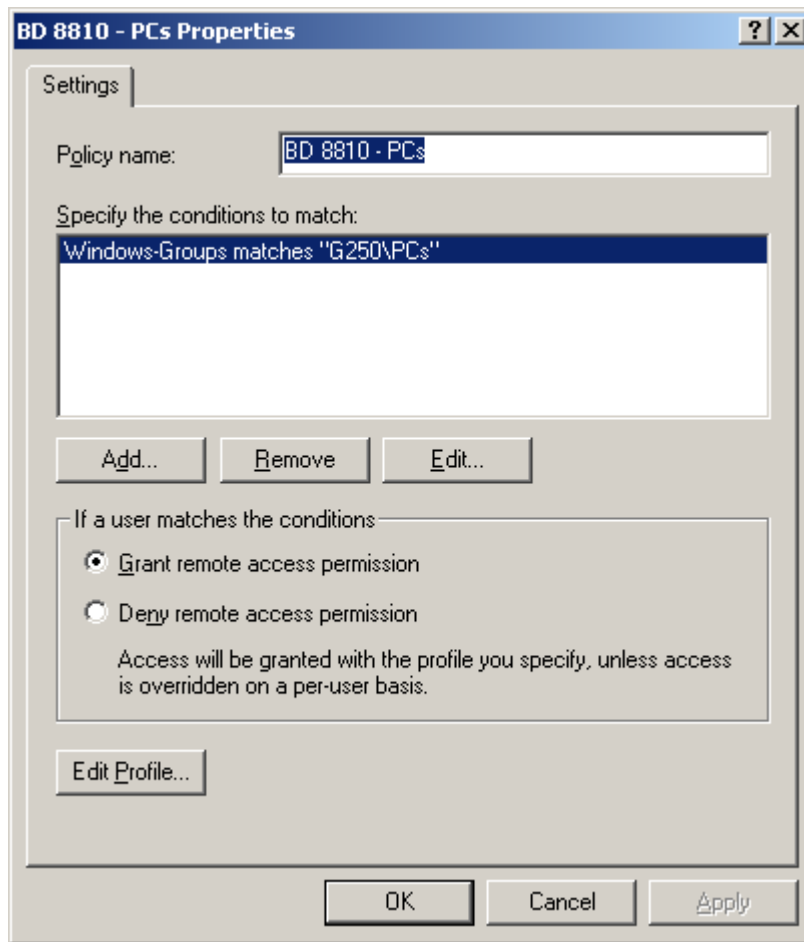
Click the **Edit Profile…** button and select the **Authentication** tab. Check the **Extensible-Authentication Protocol** and select **MD5-Challenge** under **Select the EAP type which is acceptable for this policy**.
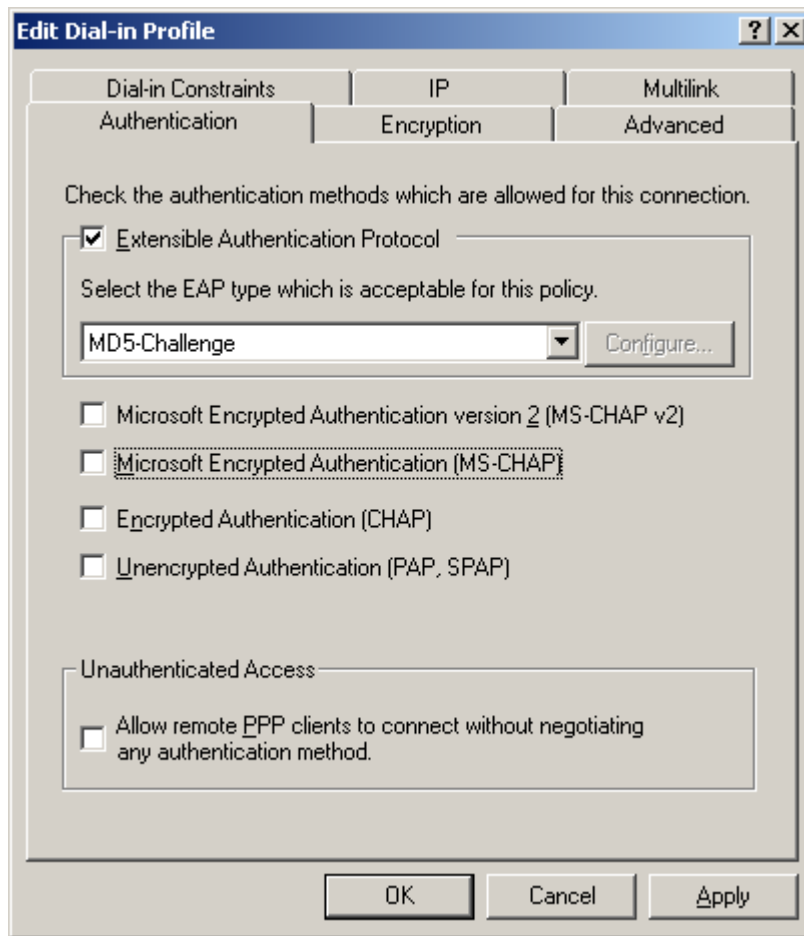
3.4 Configuring the Odyssey Client

After the Funk Odyssey Client Software is installed on a client PC, start the Funk Odyssey Client Manager through **Start → Programs → Funk Software → Odyssey Client → Odyssey Client Manager**. The following shows the Funk Odyssey Client Manager. Click **Profiles** and then click **Add** or highlight the existing profile and press **Properties**.

Double-click **MD5** profile. Click the **User Info** tab in the following screen and enter a **Login name** as configured on the Microsoft IAS. Check **Permit login using password**. Select **prompt for password** or **use the following password**. When **prompt for password** is selected, a window will pop up on the client to request a password when a new connection is made, or the current password fails the authentication.

Click the **Authentication** tab from the profile screen and add **EAP-MD5-Challenge** as an authentication protocol. Ignore the **TTLS Settings** and **PEAP Settings** tabs, which are not related to EAP-MD5.

Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.
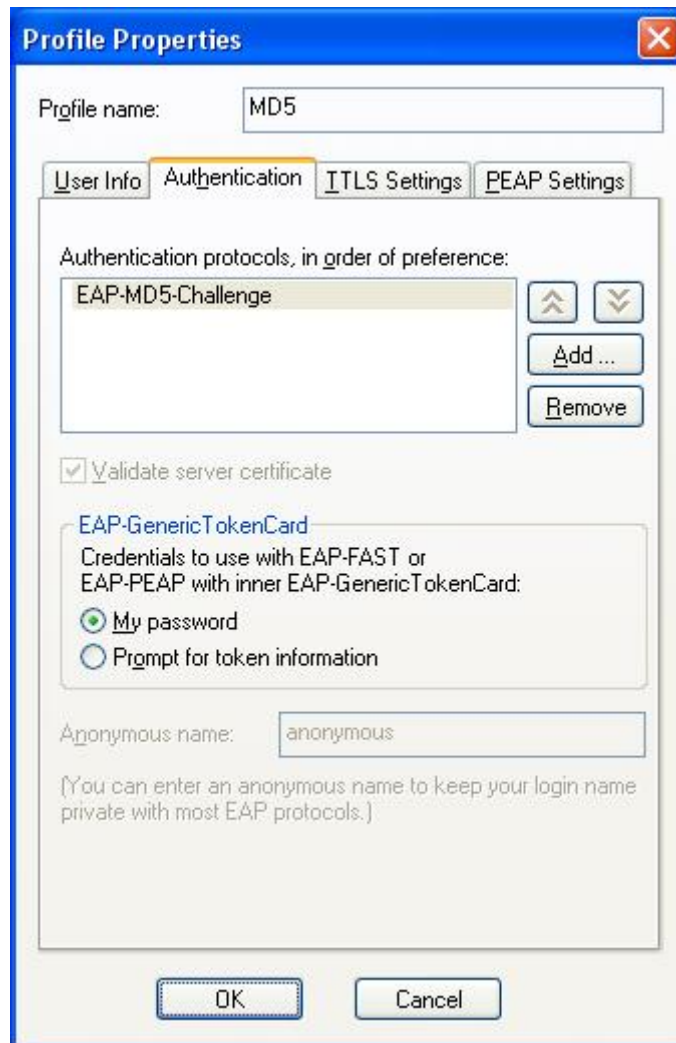
Click the **Adapters** icon from **Odyssey Client Manager,** and add the wired Ethernet adapter.
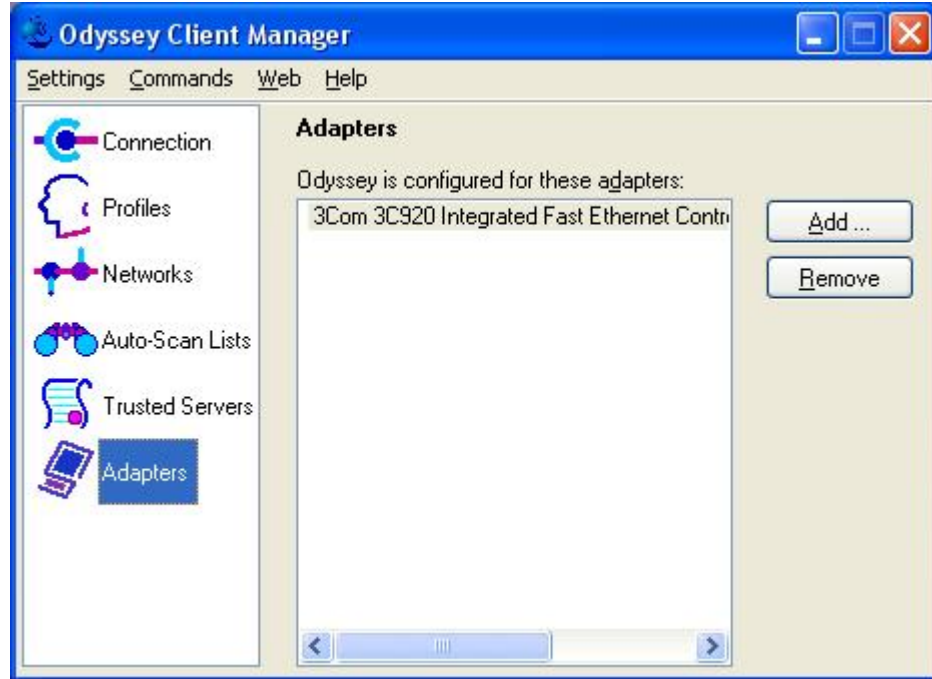
Click the **Connection** icon from the **Odyssey Client Manager**. Select the Ethernet adapter in the **Adapter** field, check the **Connect using profile** box and select the profile for the MD5. If the client is authenticated, the **Status** for the **Connection information** should be **open and authenticated**.
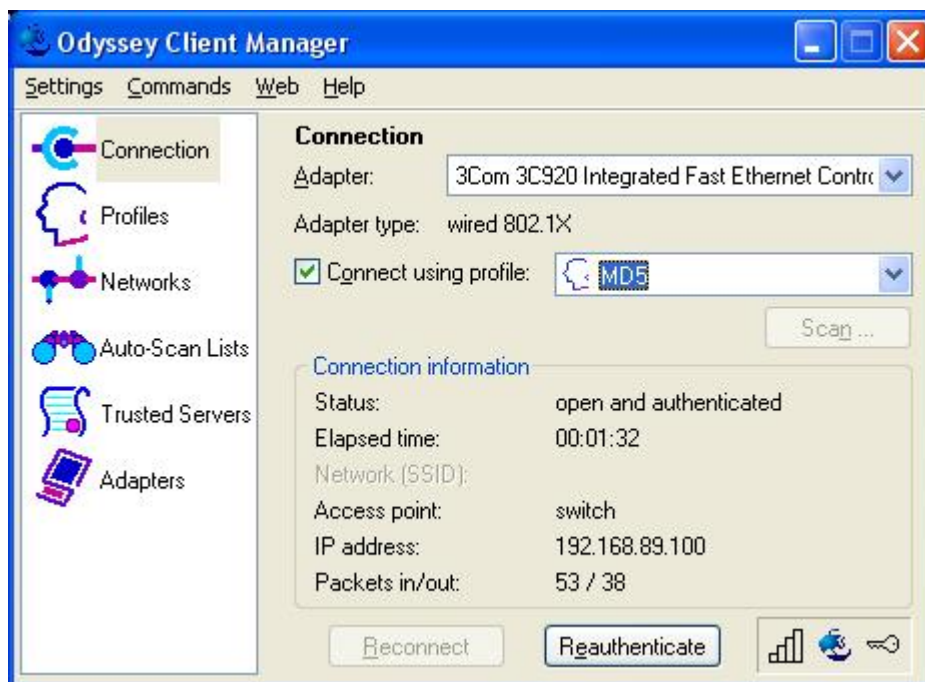
4 Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Extreme Networks BlackDiamond 8810 to interoperate with Avaya IP Telephones with LLDP and 802.1X.

4.1 General Test Approach

The general test approach was to configure the BlackDiamond 8810 in a basic sample network with Avaya Communication Manager and Avaya IP Telephones, as shown in **Figure 1**.

The main objectives were to verify the BlackDiamond 8810 supports the following:
- Link Layer Discovery Protocol (LLDP)
- 802.1X

4.2 Test Results

The Extreme Networks BlackDiamond 8810 successfully achieved all objectives.

5 Verification Steps

5.1 Verify LLDP on the Extreme Networks BlackDiamond 8810

Use the command **show lldp** to display LLDP configuration. The following screen shows that ports 8:2-5 are enabled with LLDP for Tx and Rx modes. Note that VLAN Name flag is enabled for 802.1-specific information.

```
* BD-8810.16 # show lldp

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
================================================================================
8:2     Enabled   Enabled   --           ----- --N    ----   C---  ----
8:3     Enabled   Enabled   --           ----- --N    ----   C---  ----
8:4     Enabled   Enabled   --           ----- --N    ----   C---  ----
8:5     Enabled   Enabled   --           ----- --N    ----   C---  ----
================================================================================
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
```

JZ; Reviewed:
SPOC 12/18/2006
Solution & Interoperability Test Lab Application Notes
©2006 Avaya Inc. All Rights Reserved.
28 of 39
Extreme-DOT1X.doc

When the phones are authenticated successfully, use the command **show voice** to verify that the ports connected to the phones are moved to Voice VLAN. The following screen shows that ports 8:2-5 are authenticated with tagged Voice VLAN.

```
* BD-8810.18 # show "Voice"
VLAN Interface with name Voice created by user
        Admin State:    Enabled        Tagging:        802.1Q Tag 88
        Virtual router: VR-Default
        Primary IP    : 192.168.88.6/24
        IPv6:           None
        STPD:           None
        Protocol:       Match all unfiltered protocols
        Loopback:       Disabled
        NetLogin:       Disabled
        QosProfile:     None configured
        Ports:  7.       (Number of active ports=5)
           Untag:      8:9
           Tag:        *8:1,  *8:2a,  *8:3a,  *8:4a,  *8:5a
        Flags:     (*) Active, (!) Disabled, (g) Load Sharing port
                   (b) Port blocked on the vlan, (a) Authenticated NetLogin port
                   (u) Unauthenticated NetLogin port, (m) Mac-Based port
```

Use the command **show fdb voice** to verify that the MACs of the phones are associated with Voice VLAN. The following screen shows that the phone's MAC addresses are associated with Voice VLAN on ports 8:2-5.

```
* BD-8810.19 # show fdb  voice
Mac                     Vlan        Age     Use      Flags    Port List
----------------------------------------------------------------------
00:03:32:bd:56:5d       Voice(0088) 0053    0000  d m        8:1
00:03:47:42:38:b3       Voice(0088) 0000    0000  d mi       8:1
00:04:0d:4a:d1:99       Voice(0088) 0000    0000  d mi       8:1
00:04:0d:4a:f5:42       Voice(0088) 0000    0000  d mi       8:1
00:04:0d:4b:d8:6f       Voice(0088) 0000    0000  npm        8:2
00:04:0d:6d:3d:79       Voice(0088) 0000    0000  d mi       8:1
00:04:0d:9d:64:71       Voice(0088) 0000    0000  npm        8:3
00:04:0d:ea:b5:bb       Voice(0088) 0000    0000  npm        8:4
00:04:0d:ea:b9:d8       Voice(0088) 0000    0000  npm        8:5
00:08:83:74:62:00       Voice(0088) 0000    0000  d mi       8:1
00:12:3f:79:10:c2       Voice(0088) 0000    0000  d mi       8:1
00:a0:c9:21:e8:cd       Voice(0088) 0000    0000  d mi       8:1
00:d0:02:bd:ff:ff       Voice(0088) 0000    0000  d mi       8:1
00:d0:c0:ce:d9:54       Voice(0088) 0000    0000  d mi       8:1

Flags : d - Dynamic, s - Static, p - Permanent, n - NetLogin, m - MAC, i -
IP,
        x - IPX, l - lockdown MAC, M - Mirror, B - Egress Blackhole,
        b - Ingress Blackhole, v - MAC-Based VLAN.

Total: 17 Static: 4 Perm: 4 Dyn: 13 Dropped: 0
FDB Aging time: 300
```

Use the command **show lldp detailed** to display LLDP configuration and status. When the IP telephones connected to port 8:2-5 are authenticated and are assigned to Voice VLAN based on the VSA 211 from the Microsoft IAS, the Extreme Networks BlackDiamond 8810 will advertise Voice VLAN to the phone as highlighted in the following screen. If a port connected to an IP telephone is not authenticated on Voice VLAN, that port would not be associated with Voice VLAN.

```
* BD-8810.24 # show lldp detailed

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
=============================================================================
8:2     Enabled    Enabled    --            -----  --N    ----   C---  ----
  VLAN: Voice                                -----  --N    ----   ----  ----
  VLAN: data-vlan                            -----  --N    ----   ----  ----
8:3     Enabled    Enabled    --            -----  --N    ----   C---  ----
  VLAN: Voice                                -----  --N    ----   ----  ----
  VLAN: data-vlan                            -----  --N    ----   ----  ----
8:4     Enabled    Enabled    --            -----  --N    ----   C---  ----
  VLAN: Voice                                -----  --N    ----   ----  ----
  VLAN: data-vlan                            -----  --N    ----   ----  ----
8:5     Enabled    Enabled    --            -----  --N    ----   C---  ----
  VLAN: Voice                                -----  --N    ----   ----  ----
  VLAN: data-vlan                            -----  --N    ----   ----  ----
=============================================================================
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
```

Use the command **show lldp neighbors** to display the summary information for LLDP neighbors. The following screen shows the IP telephones connected to ports 8:2-5.

```
* BD-8810.25 # show lldp neighbors

Port     Neighbor Chassis ID        Neighbor Port ID           TTL     Age
==============================================================================
8:2      (5.1)192.168.88.107        00:04:0D:4B:D8:6F          120     8
8:3      (5.1)192.168.88.106        00:04:0D:9D:64:71          120     11
8:4      (5.1)192.168.88.104        00:04:0D:EA:B5:BB          120     13
8:5      (5.1)192.168.88.102        00:04:0D:EA:B9:D8          120     19
==============================================================================
NOTE: The Chassis ID and/or Port ID might be truncated to fit the screen.
```

Use the command **shows LLDP neighbors detailed** to display detailed LLDP information. The LLDP and LLDP-MED advertised from the Avaya IP telephone can be displayed on the Extreme Networks BlackDiamond 8810. Avaya IP telephones support type, length, and value referred to as TLVs based on IEEE 802.1AB and extensions. The following screen highlights some of the information that Avaya IP telephones can advertise via LLDP.

```
* BD-8810.27 # show lldp neighbors detailed

------------------------------------------------------------------------------
LLDP Port 8:2 detected 1 neighbor
  Neighbor: (5.1)192.168.88.107/00:04:0D:4B:D8:6F, age 29 seconds
    - Chassis ID type: Network address (5); Address type: IPv4 (1)
      Chassis ID      : 192.168.88.107
    - Port ID type: MAC address (3)
      Port ID         : 00:04:0D:4B:D8:6F
    - Time To Live: 120 seconds
    - System Name: "AVA4BD86F"
    - System Capabilities : "Bridge, Telephone"
      Enabled Capabilities: "Bridge, Telephone"
    - Management Address Subtype: IPv4 (1)
      Management Address          : 192.168.88.107
      Interface Number Subtype  : System Port Number (3)
      Interface Number          : 1
      Object ID String          : "1.3.6.1.4.1.6889.1.69.1.5"
    - 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           : 88
      L2 Priority       : 6
      DSCP Value        : 46
    - MED Hardware Revision: "4620D01B"
```

```
         - MED Firmware Revision: "b20d01b2_6.bin"
         - MED Software Revision: "a20d01b2_6.bin"
         - MED Serial Number: "031653041528"
         - MED Manufacturer Name: "Avaya"
         - MED Model Name: "4620"
       - Avaya/Extreme Conservation Level Support
         Current Conservation Level: 0
         Typical Power Value        : 5.9 Watts
         Maximum Power Value        : 8.0 Watts
       - Avaya/Extreme Call Server(s): 192.168.88.22
       - Avaya/Extreme IP Phone Address: 192.168.88.107 255.255.255.0
         Default Gateway Address     : 192.168.88.1
       - Avaya/Extreme CNA Server: 0.0.0.0
       - Avaya/Extreme File Server(s): 192.168.88.31
       - Avaya/Extreme IEEE 802.1q Framing: Tagged


-------------------------------------------------------------------------------
LLDP Port 8:3 detected 1 neighbor
  Neighbor: (5.1)192.168.88.106/00:04:0D:9D:64:71, age 2 seconds
       - Chassis ID type: Network address (5); Address type: IPv4 (1)
         Chassis ID      : 192.168.88.106
       - Port ID type: MAC address (3)
         Port ID       : 00:04:0D:9D:64:71
       - Time To Live: 120 seconds
       - System Name: "AVA9D6471"
       - System Capabilities : "Bridge, Telephone"
         Enabled Capabilities: "Bridge, Telephone"
       - Management Address Subtype: IPv4 (1)
         Management Address       : 192.168.88.106
         Interface Number Subtype  : System Port Number (3)
         Interface Number        : 1
         Object ID String        : "1.3.6.1.4.1.6889.1.69.1.12"
       - 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           : 88
         L2 Priority       : 6
         DSCP Value        : 46
         - MED Hardware Revision: "4622D01A"
         - MED Firmware Revision: "b20d01b2_6.bin"
         - MED Software Revision: "a20d01b2_6.bin"
         - MED Serial Number: "051649006119"
         - MED Manufacturer Name: "Avaya"
         - MED Model Name: "4622"
       - Avaya/Extreme Conservation Level Support
         Current Conservation Level: 0
         Typical Power Value        : 4.9 Watts
         Maximum Power Value        : 6.4 Watts
         Conservation Power Level  : 1=4.4W
       - Avaya/Extreme Call Server(s): 192.168.88.22
       - Avaya/Extreme IP Phone Address: 192.168.88.106 255.255.255.0
```

```
          Default Gateway Address       : 192.168.88.1
       - Avaya/Extreme CNA Server: 0.0.0.0
       - Avaya/Extreme File Server(s): 192.168.88.31
       - Avaya/Extreme IEEE 802.1q Framing: Tagged


       -------------------------------------------------------------------------
LLDP Port 8:4 detected 1 neighbor
   Neighbor: (5.1)192.168.88.104/00:04:0D:EA:B5:BB, age 4 seconds
       - Chassis ID type: Network address (5); Address type: IPv4 (1)
         Chassis ID     : 192.168.88.104
       - Port ID type: MAC address (3)
         Port ID        : 00:04:0D:EA:B5:BB
       - Time To Live: 120 seconds
       - System Name: "AVAEAB5BB"
       - System Capabilities : "Bridge, Telephone"
         Enabled Capabilities: "Bridge, Telephone"
       - Management Address Subtype: IPv4 (1)
         Management Address         : 192.168.88.104
         Interface Number Subtype  : System Port Number (3)
         Interface Number          : 1
         Object ID String          : "1.3.6.1.4.1.6889.1.69.2.4"
       - 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           : 88
         L2 Priority       : 5
         DSCP Value        : 56
       - MED Hardware Revision: "9640D01A"
       - MED Firmware Revision: "hb96xxua1_20r19st.bin"
       - MED Software Revision: "ha96xxua1_20r19st.bin"
       - MED Serial Number: "06N507002939"
       - MED Manufacturer Name: "Avaya"
       - MED Model Name: "9640"
       - Avaya/Extreme Conservation Level Support
         Current Conservation Level: 0
         Typical Power Value       : 4.5 Watts
         Maximum Power Value       : 5.5 Watts
         Conservation Power Level  : 1=4.1W
       - Avaya/Extreme Call Server(s): 192.168.88.22
       - Avaya/Extreme IP Phone Address: 192.168.88.104 255.255.255.0
         Default Gateway Address       : 192.168.88.1
       - Avaya/Extreme CNA Server: 0.0.0.0
       - Avaya/Extreme File Server(s): 0.0.0.0
       - Avaya/Extreme IEEE 802.1q Framing: Tagged


       -------------------------------------------------------------------------
LLDP Port 8:5 detected 1 neighbor
   Neighbor: (5.1)192.168.88.102/00:04:0D:EA:B9:D8, age 9 seconds
       - Chassis ID type: Network address (5); Address type: IPv4 (1)
         Chassis ID     : 192.168.88.102
       - Port ID type: MAC address (3)
```

```
    Port ID     : 00:04:0D:EA:B9:D8
  - Time To Live: 120 seconds
  - System Name: "AVAEAB9D8"
  - System Capabilities : "Bridge, Telephone"
    Enabled Capabilities: "Bridge, Telephone"
  - Management Address Subtype: IPv4 (1)
    Management Address        : 192.168.88.102
    Interface Number Subtype  : System Port Number (3)
    Interface Number          : 1
    Object ID String          : "1.3.6.1.4.1.6889.1.69.2.3"
  - 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           : 88
    L2 Priority       : 5
    DSCP Value        : 56
  - MED Hardware Revision: "9650D01A"
  - MED Firmware Revision: "hb96xxua1_20r19st.bin"
  - MED Software Revision: "ha96xxua1_20r19st.bin"
  - MED Serial Number: "06N507003992"
  - MED Manufacturer Name: "Avaya"
  - MED Model Name: "9650"
  - Avaya/Extreme Conservation Level Support
    Current Conservation Level: 0
    Typical Power Value        : 4.8 Watts
    Maximum Power Value        : 5.9 Watts
    Conservation Power Level   : 1=4.7W
  - Avaya/Extreme Call Server(s): 192.168.88.22
  - Avaya/Extreme IP Phone Address: 192.168.88.102 255.255.255.0
    Default Gateway Address      : 192.168.88.1
  - Avaya/Extreme CNA Server: 0.0.0.0
  - Avaya/Extreme File Server(s): 0.0.0.0
        -   Avaya/Extreme IEEE 802.1q Framing: Tagged
```

5.2 Verify 802.1X on the Extreme Networks BlackDiamond 8810

Use the command **show netlogin dot1x** to display dot1x configuration and summary dot1x information. The following screen shows that the IP telephones connected to port 8:2-5 are authenticated successfully on the voice VLAN. The attached PC on port 8:4 is also authenticated on the untagged VLAN 89.

```
* BD-8810.1 # show netlogin dot1x

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

--------------------------------------------------
       802.1x Mode Global Configuration
--------------------------------------------------
Quiet Period                    : 60
Supplicant Response Timeout     : 30
Re-authentication period        : 60
RADIUS server timeout           : 30
EAPOL MPDU version to transmit  : v1
Guest VLAN                      : <Not Configured>
--------------------------------------------------
Port: 8:2,  Vlan: data-vlan,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:
Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:4b:d8:6f  0.0.0.0          No             0             00040D4BD86F
--------------------------------------------------

Port: 8:2,  Vlan: Voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:
Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:4b:d8:6f  0.0.0.0          Yes   802.1x  38            00040D4BD86F
--------------------------------------------------

Port: 8:3,  Vlan: data-vlan,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:
Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:9d:64:71  0.0.0.0          No             0             00040D9D6471
--------------------------------------------------

Port: 8:3,  Vlan: Voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:9d:64:71  0.0.0.0          Yes   802.1x  46            00040D9D6471
--------------------------------------------------

Port: 8:4,  Vlan: data-vlan,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:
Disabled

MAC                IP address       Auth  Type    ReAuth-Timer   User
00:04:0d:ea:b5:bb  0.0.0.0          No             0             00040DEAB5BB
```

```
00:11:11:28:d0:3b  0.0.0.0          Yes  802.1x  34           STEVE
-----------------------------------------------

Port: 8:4,  Vlan: Voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:Disabled

MAC              IP address      Auth Type    ReAuth-Timer   User
00:04:0d:ea:b5:bb  0.0.0.0          Yes  802.1x  59           00040DEAB5BB
-----------------------------------------------

Port: 8:5,  Vlan: data-vlan,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:
Disabled

MAC              IP address      Auth Type    ReAuth-Timer   User
00:04:0d:ea:b9:d8  0.0.0.0          No           0            00040DEAB9D8
-----------------------------------------------

Port: 8:5,  Vlan: Voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan:Disabled

MAC              IP address      Auth Type    ReAuth-Timer   User
00:04:0d:ea:b9:d8  0.0.0.0          Yes  802.1x  0            00040DEAB9D8
```

Use the command **show netlogin port <port #> dot1x detailed** to display detailed information on a port. The following screen shows the detailed dot1x information on port 8:4. The phone with MAC address **00:04:0d:ea:b5:bb** is authenticated on VLAN 88 (Voice VLAN). The attached PC with MAC address **00:11:11:28:d0:3b** is authenticated on the untagged VLAN. The default user name for the phone is its MAC address **00040DEAB5BB** (upper case letters).

```
* BD-8810.2 # show netlogin port 8:4 dot1x detail
Port          : 8:4
Vlan          : data-vlan
Authentication: 802.1x
Port State    : Enabled


     MAC
00:04:0d:ea:b5:bb   : IP=0.0.0.0         Auth=No   User=<unknown>
                    : AuthPAE state=INITIALIZE BackAuth state=IDLE
                    : ReAuth time left=0       ReAuth count=0
                    : Quiet time left=0
00:11:11:28:d0:3b   : IP=0.0.0.0         Auth=Yes  User=STEVE
                    : AuthPAE state=AUTHENTICATED BackAuth state=IDLE
                    : ReAuth time left=43      ReAuth count=0
                    : Quiet time left=0
-------------------------------------------------

Port          : 8:4
Vlan          : Voice
Authentication: 802.1x
Port State    : Enabled


     MAC
00:04:0d:ea:b5:bb   : IP=0.0.0.0          Auth=Yes  User=00040DEAB5BB
                    : AuthPAE state=AUTHENTICATED BackAuth state=IDLE
                    : ReAuth time left=8       ReAuth count=0
                    : Quiet time left=0
```

5.3 Verify the Avaya IP Telephone Operation

Reset the IP telephones to manufacturer's default. Enter the correct password using the default user name (the phone's MAC address) when the phone is prompted for user name and password. Verify that the phone resets and uses Voice VLAN 88 after successful authentication. Verify that the phone can register to Avaya Communication Manager with its extension and password. Verify that calls can be made.

Reset the phone with the current configuration. Verify that the phone can register to Avaya Communication Manager with its extension and password. Verify that calls can be made.

6 Support

For technical support on Extreme Networks products, consult the support pages at http://www.extremenetworks.com/services or contact the Extreme Networks Worldwide TAC at:
• Toll free: 800-998-2408
• Phone: 408-579-2826
  • E-mail: support@extremenetworks.com

7 Conclusion

As illustrated in these Application Notes, Avaya IP telephones can be configured as 802.1X supplicants and the Extreme Networks BlackDiamond 8810 can be configured as an 802.1X authenticator. The Avaya IP telephone and the attached PC can be authenticated individually. When the LLDP 802.1-specific information is used, the Avaya IP telephone and the attached PC can be placed into different VLANs. The Avaya IP telephones can learn the voice VLAN from the Extreme Networks BlackDiamond 8810 via LLDP.

8 Additional References

The following Application Notes can be found at http://www.avaya.com.

[1]   *Configuring 802.1X Protocol On Avaya G250 and G350 Media Gateways For an Avaya IP Telephone With an Attached PC*

[2]   ExtremeWare XOS Concepts Guide for Software version 11.5 can be found at http://www.extremenetworks.com