

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.

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.

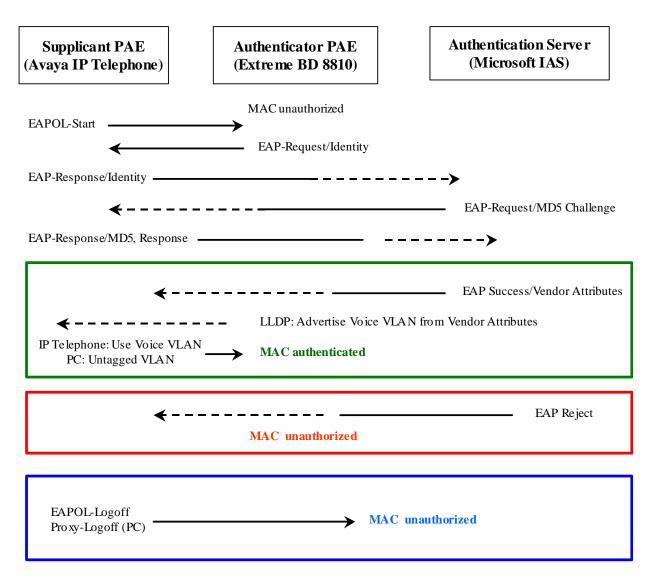
The IEEE 802.1AB LLDP specification will enable LAN devices to inform each other about their configurations. The 802.1AB standard defines a set of advertisement messages, called type-length-values (TLVs). Avaya IP telephones support TLVs specified in IEEE 802.1AB-2005 and extensions. Through the LLDP 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.





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.

- 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.

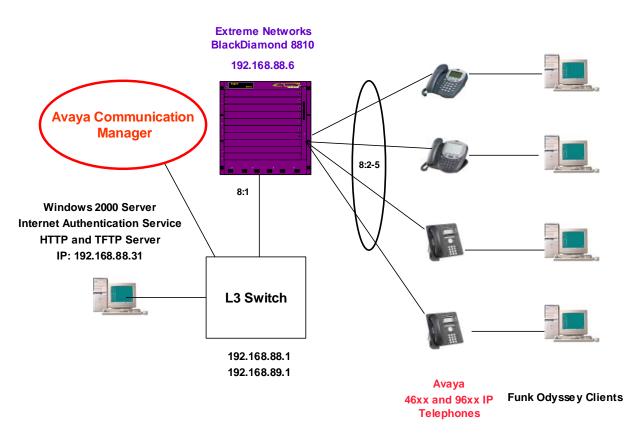


Figure 2 – 802.1X Configuration With Avaya IP Telephones

2 Equipment and Software Validated

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

Equipment	Software	
Avaya Communication Manager (Avaya S8500	3.1.2	
Media Server with Avaya G650 Media Gateway)		
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	11.5.2.8 XOS	
G48P-41512 Blade		
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
```

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. 8 of 39 Extreme-DOT1X.doc 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.

🝠 Group Policy				
$ \Delta ction View $				
Tree	Policy A	Computer Setting		
🛃 Default Domain Policy [avaya-kc 🔺	Enforce password history	1 passwords remembered		
🗐 👧 Computer Configuration	📖 Maximum password age	42 days		
🗄 📄 Software Settings 🛁	🕮 Minimum password age	0 days		
🖃 📄 Windows Settings	🕮 Minimum password length	0 characters		
- 🔄 Scripts (Startup/Shu	Beasswords must meet complexity requirements	Disabled		
🖻 😳 Security Settings	Store password using reversible encryption f	Enabled		
🖻 🛃 Account Policies 🚽				
	•			

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.

00040DEAB5BB Properties
Member Of Dial-in Environment Sessions Remote control Terminal Services Profile General Address Account Profile Telephones Organization
User logon name: 00040DEAB588 User logon name (pre- <u>W</u> indows 2000):
G250\ 000040DEAB5BB
Account is locked out Account options:
□ User must change password at next logon ▲ □ User cannot change password ■ □ Password never expires ■ □ Store password using reversible encryption ▼
Account expires Image: Never Image: December 29, 2006
OK Cancel Apply

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. To enable remote access for a user, from a user account **Properties**, select **Allow access** for **Remote Access Permission** under the **Dial-in** tab.

00040de970ab Properties
Remote control Terminal Services Profile
General Address Account Profile Telephones Organization
Member Of Dial-in Environment Sessions
Remote Access Permission (Dial-in or VPN)
Allow access
© Deny access
C Control access through Remote Access Policy
└── ⊻erify Caller-ID:
Callback Options
• No <u>C</u> allback
Set by Caller (Routing and Remote Access Service only)
O Always Callback to:
Assign a Static IP Address
Apply Static <u>B</u> outes
Define routes to enable for this Dial-in Static Routes
OK Cancel Apply

Create a user group named "phones" and add the phones (usernames: MACs of the phones) to the group.

phones Properties		<u>?</u> ×	
General Members Member Of M	fanaged By		
Members:			
Name	Active Directory Folder		
00040d9d6471	g250.avaya.com/Users		
😨 00040DEAB5BB	g250.avaya.com/Users		
🕵 00040DEAB5CA	g250.avaya.com/Users		
🕵 00040DEAB7F1	g250.avaya.com/Users		
🕵 00040DEAB80B	g250.avaya.com/Users		
🕵 00040DEAB89A	g250.avaya.com/Users		
🖸 00040DEAB8E9	g250.avaya.com/Users		
🖸 🕵 00040DEAB9D8 g250.avaya.com/Users			
2 00040DEAB9F9	g250.avaya.com/Users		
2 00040DEBFCB3	g250.avaya.com/Users		
2 00040DEC9395	g250.avaya.com/Users		
2 00040DECEE51	g250.avaya.com/Users		
1 00040DED1261	g250.avaya.com/Users	-	
•)		
		-	
Add <u>R</u> emove			
	DK Cancel <u>A</u> p	ply	

Create a user group named "PCs" and add the PCs to the group.

PCs Propert	ies	<u>? ×</u>
General N	1embers Member Of Managed By	
Members:		
Name	Active Directory Folder	
🖸 john	g250. avaya.com/Users	
🕵 steve	g250.avaya.com/Users	
A <u>d</u> d	. <u>R</u> emove	
	ОК	Cancel Apply

3.3 Configuring the Microsoft IAS

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

🐓 Internet Authentication Service			
Action View $4 \Leftrightarrow \Rightarrow 1$ 🖪 🖪 🛱 😵			
Tree	Friendly Name	Address	Protocol
Internet Authentication Service (Local)	Extreme S300-48	192.168.5.3	RADIUS
E Clients	Extreme BD-8810	192.168.88.6	RADIUS
E Remote Access Logging			
🗄 💐 Remote Access Policies	•		•

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**.

Extreme BD-8810 Properties	? ×
Settings	
Friendly name for client:	
Extreme BD-8810	
Client address	_
Address (IP or DNS):	_
192.168.88.6	-
<u>⊻</u> erify	
Client-Vendor: RADIUS Standard	-
Client must always send the signature attribute in the request	
Shared secret:	
Confirm shared secret:	
OK Cancel Ap	ply

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

BD 8810 - Phone Properties			
Settings			
Policy name: BD 8810 - Phone			
Specify the conditions to match:			
Windows-Groups matches "G250\phones"			
A <u>d</u> d <u>R</u> emove <u>E</u> dit			
If a user matches the conditions			
<u>G</u> rant remote access permission			
C Deny remote access permission			
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.			
Edit <u>P</u> rofile			
OK Cancel Apply			

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.

Edit Dial-in Profile		<u>? ×</u>		
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced		
Check the authentication methods which are allowed for this connection. Image: Extensible Authentication Protocol Select the EAP type which is acceptable for this policy.				
MD5-Challenge		Configure		
 Microsoft Encrypted Authentication version <u>2</u> (MS-CHAP v2) Microsoft Encrypted Authentication (MS-CHAP) Encrypted Authentication (CHAP) Unencrypted Authentication (PAP, SPAP) 				
Unauthenticated Access Allow remote <u>P</u> PP clients to connect without negotiating any authentication method.				
	ОК Са	ancel Apply		

Click the Advanced tab and Click Add.... to display the following screen.

Funnel-Assignment-ID F Funnel-Client-Auth-ID F	RADIUS Standard RADIUS Standard RADIUS Standard	Description Type of service user has requested Tunnel to which a session is to be assigned
Funnel-Client-Auth-ID		Tunnel to which a session is to be assigned
		-
Funnel-Client-Endot F		Name used by the tunnel initiator during the authen
•	RADIUS Standard	IP address of the initiator end of the tunnel
	RADIUS Standard	Transport medium to use when creating a tunnel fo
	RADIUS Standard	Password for authenticating to a remote server
	RADIUS Standard	Relative preference assigned to each tunnel when
	RADIUS Standard	Group ID for a particular tunneled session
	RADIUS Standard	Name used by the tunnel terminator during the auth
· · · · · · · · · · · · · · · · · · ·	RADIUS Standard	IP address of the server end of the tunnel
	RADIUS Standard	Tunneling protocols to be used
	RADIUS Standard	Used to support proprietary NAS features
	Cisco	Cisco AV Pair VSA
2	Microsoft	Ignore the user's dial-in properties
	U.S. Robotics, I	Description not available
	U.S. Robotics, I	Description not available
	U.S. Robotics, I	Description not available
	U.S. Robotics, I	Description not available
JSR-AT-Output-Filter l	U.S. Robotics, I	Description not available
JSR-AT-RTMP-Input-Filter l	U.S. Robotics, I	Description not available

From the prior screen, select **Vendor-Specific** in the **RADIUS attributes** and click the **Add...** button. The following screen appears.

Multivalued Attribute I	nformation		? ×
Attribute name:			
Vendor-Specific			
Attribute number:			
26			
Attribute format:			
OctetString			
Attribute values:			
Vendor	Value		Move <u>U</u> p
			Move <u>D</u> own
			Add
			<u>R</u> emove
			<u>E</u> dit
•		Þ	
		OK.	Cancel

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.

Vendor-Specific Attribute Information	? ×
Attribute name:	
Vendor-Specific	
Specify network access server vendor.	
C Select from list:	7
Enter Vendor Code: 1916	
Specify whether the attribute conforms to the RADIUS RFC specifical vendor specific attributes.	ition for
Yes. It conforms.	
\bigcirc No. It does not conform.	
Configure <u>A</u> ttribute	
OK Car	ncel

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.

Configure VSA (RFC compliant)	? >	١
Vendor-assigned attribute number:		
211		
<u>Attribute format:</u>		
String	•	
Attri <u>b</u> ute value:		
T88		
	OK Cancel	

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.

BD 8810 - PCs Properties
Settings
Policy name: BD 8810 - PCs
Specify the conditions to match:
Windows-Groups matches "G250\PCs"
A <u>d</u> d <u>R</u> emove <u>E</u> dit
☐ If a user matches the conditions
<u>G</u> rant remote access permission
Deny remote access permission
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.
E dit <u>P</u> rofile
OK Cancel Apply

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.

Edit Dial-in Profile		<u>? ×</u>
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Check the authentication Extensible Authentication Select the EAP type white		
MD5-Challenge		Configure
Unauthenticated Access Allow remote <u>P</u> PP cli any authentication m	ents to connect without n	egotiating
	ОК Са	ancel Apply

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 \rightarrow Programs \rightarrow Funk Software \rightarrow Odyssey Client \rightarrow 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.

💩 Odyssey Client Ma	inager	
<u>Settings</u> <u>Commands</u> <u>W</u>	eb <u>H</u> elp	
Connection Profiles Networks Auto-Scan Lists STrusted Servers Adapters	Profiles The following profiles are configured: Initial Profile MD5	<u>A</u> dd <u>R</u> emove 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.

ofile Prope	erties
Pr <u>o</u> file name:	MD5
<u>U</u> ser Info A	ut <u>h</u> entication ITLS Settings PEAP Settings
Login name:	steve
Password	Certificate Soft Token SIM Card
P <u>e</u> rmit le	ogin using password
	ndows password for password
	following password:
	nask
C	OK Cancel

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.

Profile Properties	
Pr <u>o</u> file name:	MD5
User Info Authentic	ation ITLS Settings PEAP Settings
Authentication proto	cols, in order of preference:
EAP-MD5-Challeng	
	nCard with EAP-FAST or ner EAP-GenericTokenCard:
Anonymous name:	anonymous
(You can enter an a private with most EA	nonymous name to keep your login name P protocols.)
ОК	Cancel

Click the Adapters icon from Odyssey Client Manager, and add the wired Ethernet adapter.

💩 Odyssey Client M	anager	
<u>S</u> ettings <u>C</u> ommands ⊻	⊻eb <u>H</u> elp	
Connection Profiles Networks Auto-Scan Lists Trusted Servers Adapters	Adapters Odyssey is configured for these adapters: 3Com 3C920 Integrated Fast Ethernet Contri	Add Remove
	× • • • •	

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**.

💩 Odyssey Client Ma	anager			
<u>S</u> ettings <u>C</u> ommands <u>W</u>	<u>/</u> eb <u>H</u> elp			
	Connection Adapter:	3Com 3C	920 Integrated Fast Eth	nernet Contra 💌
	Adapter type:	wired 802	.1X	
	Connect usi	ng profile:		~
Auto-Scan Lists	Connection in Status: Elapsed time: Network (SSI Access point: IP address:	D):	open and authenticat 00:01:32 switch 192.168.89.100	Sca <u>n</u>
	Packets in/o	ut	53 / 38	
	Beconn	ect	Reauthenticate	Щ 🍕 🗠

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 secondsLLDP 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 Optional enabled transmit TLVs Rx Tx SNMP Mode Mode Notification LLDP 802.1 802.3 MED AVEX 8:2 Enabled Enabled ------N ____ C----8:3 Enabled Enabled --____ --N ----C---____ Enabled Enabled ----N C---8:4 ____ ____ ____ Enabled Enabled --8:5 ----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 : (C) MED Capabilities, (P) Network Policy, MED Flags (L) Location Identification, (p) Extended Power-via-MDI AVEx Flags : (P) PoE Conservation Request, (C) Call Server, (F) File Server (Q) 802.1Q Framing

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.

00:03:47:42:38:b3 Voice(0088) 0000 0000 0000 00:04:0d:4a:d1:99 Voice(0088) 0000 0000 0000 0000 00:04:0d:4a:d1:99 Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:4a:f5:42 Voice(0088) 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 <	d mi d mi d mi npm d mi npm npm	8:1 8:1 8:1 8:1 8:2 8:1 8:3 8:4 8:5 8:1
00:04:0d:4a:d1:99 Voice(0088) 0000 0000 0000 00:04:0d:4a:f5:42 Voice(0088) 0000 0000 0000 0000 00:04:0d:4b:d8:6f Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:6d:3d:79 Voice(0088) 0000 0000 0000 0000 0000 0000 00:04:0d:ea:b9:d8 Voice(0088) 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 <td< td=""><td>d mi d mi npm d mi npm npm</td><td>8:1 8:1 8:2 8:1 8:3 8:4 8:5</td></td<>	d mi d mi npm d mi npm npm	8:1 8:1 8:2 8:1 8:3 8:4 8:5
00:04:0d:4a:f5:42 Voice(0088) 0000 0000 0000 00:04:0d:4b:d8:6f Voice(0088) 0000 0000 0000 0000 00:04:0d:6d:3d:79 Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:6d:3d:79 Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:ea:b9:d8 Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:ea:b9:d8 Voice(0088) 0000 0000 0000 0000 0000 00:08:83:74:62:00 Voice(0088) 0000 0000 0000 0000 0000 0000 00:12:3f:79:10:c2 Voice(0088) 0000 0000 0000 0000 0000 00:a0:c9:21:e8:cd Voice(0088) 0000 0000 0000 0000 0000	d mi npm d mi npm npm npm	8:1 8:2 8:1 8:3 8:4 8:5
O0:04:0d:4b:d8:6f Voice(0088) 0000 0000 r 00:04:0d:6d:3d:79 Voice(0088) 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 r 00:04:0d:ea:b5:bb Voice(0088) 0000 0000 r 00:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r 00:00:00:00:00:00:00:00:00:00:00:00:00:	npm 1 mi npm npm npm	8:2 8:1 8:3 8:4 8:5
00:04:0d:6d:3d:79 Voice(0088) 0000 0000 0000 00:04:0d:9d:64:71 Voice(0088) 0000 0000 0000 0000 00:04:0d:ea:b5:bb Voice(0088) 0000 0000 0000 0000 0000 00:04:0d:ea:b9:d8 Voice(0088) 0000 0000 0000 0000 0000 0000 00:08:83:74:62:00 Voice(0088) 0000 0000 0000 0000 0000 00:12:3f:79:10:c2 Voice(0088) 0000 0000 0000 0000 0000 00:a0:c9:21:e8:cd Voice(0088) 0000 0000 0000 0000 0000 00:d0:02:bd:ff:ff Voice(0088) 0000 0000 0000 0000 0000	l mi npm npm npm	8:1 8:3 8:4 8:5
O0:04:0d:9d:64:71 Voice(0088) 0000 0000 r O0:04:0d:ea:b5:bb Voice(0088) 0000 0000 r O0:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r O0:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r O0:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r O0:08:83:74:62:00 Voice(0088) 0000 0000 c O0:12:3f:79:10:c2 Voice(0088) 0000 0000 c O0:a0:c9:21:e8:cd Voice(0088) 0000 0000 c O0:d0:02:bd:ff:ff Voice(0088) 0000 0000 c	npm npm npm	8:3 8:4 8:5
O0:04:0d:ea:b5:bb Voice(0088) 0000 0000 r O0:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r O0:08:83:74:62:00 Voice(0088) 0000 0000 r O0:12:3f:79:10:c2 Voice(0088) 0000 0000 r O0:a0:c9:21:e8:cd Voice(0088) 0000 0000 r O0:d0:02:bd:ff:ff Voice(0088) 0000 0000 r	npm npm	8:4 8:5
O0:04:0d:ea:b9:d8 Voice(0088) 0000 0000 r 00:08:83:74:62:00 Voice(0088) 0000 0000 c 00:12:3f:79:10:c2 Voice(0088) 0000 0000 c 00:a0:c9:21:e8:cd Voice(0088) 0000 0000 c 00:d0:02:bd:ff:ff Voice(0088) 0000 0000 c	npm	8:5
D0:08:83:74:62:00Voice(0088)000000000000D0:12:3f:79:10:c2Voice(0088)000000000000D0:a0:c9:21:e8:cdVoice(0088)000000000000D0:d0:02:bd:ff:ffVoice(0088)000000000000	-	
D0:12:3f:79:10:c2Voice(0088)000000000000D0:a0:c9:21:e8:cdVoice(0088)000000000000D0:d0:02:bd:ff:ffVoice(0088)000000000000	1 mi	8:1
D0:a0:c9:21:e8:cdVoice(0088)000000000000D0:d0:02:bd:ff:ffVoice(0088)000000000000		
00:d0:02:bd:ff:ff Voice(0088) 0000 0000 c	d mi	8:1
	d mi	8:1
00:d0:c0:ce:d9:54 Voice(0088) 0000 0000 c	d mi	8:1
	d mi	8:1
<pre>Flags : d - Dynamic, s - Static, p - Permanent, n IP, x - IPX, l - lockdown MAC, M - Mirror, B - H b - Ingress Blackhole, v - MAC-Based VLAN. Fotal: 17 Static: 4 Perm: 4 Dyn: 13 Dropped: 0</pre>	_	

JZ; Reviewed: SPOC 12/18/2006 Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved.

29 of 39 Extreme-DOT1X.doc 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)
                 : 2 seconds
LLDP transmit delay
LLDP SNMP notification interval : 5 seconds
LLDP reinitialize delay : 2 seconds
LLDP-MED fast start repeat count : 3
LLDP Port Configuration:
                                   Optional enabled transmit TLVs
Port
      Rx
               Τx
                        SNMP
                      Notification LLDP 802.1 802.3 MED AVEX
               Mode
      Mode
_____
     Enabled Enabled --
8:2
                                    ----N
                                               ____
                                                      C---
                                               ----
 VLAN: Voice
                                    ____
                                         --N
                                                      ____
                                                           ____
                                    ----N
 VLAN: data-vlan
                                               ____
                                                      ____
                                                           _ _ _ _
      Enabled Enabled --
                                   ----- C---- C----
8:3
 VLAN: Voice
                                    ----N
                                               ____
                                                      ____
                                    ----- --N -----
                                                      _ _ _ _
 VLAN: data-vlan
                                    ----N
                                               ____
8:4
      Enabled Enabled
                                                      C---
 VLAN: Voice
                                          --N
                                    ____
                                               ____
                                                      ____
 VLAN: data-vlan
                                    ____
                                         --N
                                               ____
                                                      ____
                                                      C---
8:5 Enabled Enabled
                        _ _
                                    ----N
                                               _ _ _ _
                                                           _ _ _ _
 VLAN: Voice
                                    ----N
                                                ----
                                                      ____
                                                           ----
                                    ----N
 VLAN: data-vlan
                                                ____
_____
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) 802.10 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)
                       : 88
      VLAN ID
                   : 6
     L2 Priority
      DSCP Value
                       : 46
     MED Hardware Revision: "4620D01B"
```

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

```
- 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)
                        : 1
     Interface Number
     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
```

```
JZ; Reviewed:
SPOC 12/18/2006
```

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. 32 of 39 Extreme-DOT1X.doc

```
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)
```

```
JZ; Reviewed:
SPOC 12/18/2006
```

Solution & Interoperability Test Lab Application Notes33 of 39©2006 Avaya Inc. All Rights Reserved.Extreme-DOT1X.doc

```
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
TSABLED
NetLogin VLAN
                           : "temp"
NetLogin move-fail-action : Deny
NetLogin Client Aging Time : 5 minutes
802.1x Mode Global Configuration
_____
Quiet Period: 60Supplicant Response Timeout: 30Re-authentication period: 60RADIUS 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
MACIP addressAuth TypeReAuth-TimerUser00:04:0d:4b:d8:6f0.0.0.0No000040
                                               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
        00040

                                                              00040D9D6471
_____
Port: 8:3, Vlan: Voice, State: Enabled, Authentication: 802.1x, Guest Vlan: Disabled
۲۲ address
00:04:0d:9d:64:71 0.0.0.0
                                  Auth Type ReAuth-Timer User
                                Yes 802.1x 46
                                                               00040D9D6471
_____
Port: 8:4, Vlan: data-vlan, State: Enabled, Authentication: 802.1x, Guest Vlan:
Disabled
                  IP address Auth Type ReAuth-Timer User
MAC
00:04:0d:ea:b5:bb 0.0.0.0
                                                 0
                                                              00040DEAB5BB
                                  No
```

Solution & Interoperability Test Lab Application Notes35 of 39©2006 Avaya Inc. All Rights Reserved.Extreme-DOT1X.doc

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 MACIP addressAuthTypeReAuth-TimerUser00:04:0d:ea:b5:bb0.0.0.0Yes802.1x5900040DEAB5BB _____ Port: 8:5, Vlan: data-vlan, State: Enabled, Authentication: 802.1x, Guest Vlan: Disabled MACIP addressAuth TypeReAuth-TimerUser00:04:0d:ea:b9:d80.0.0.0No000040 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
 00046
 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
      : data-vlan
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 <u>http://www.extremenetworks.com/services</u> 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 <u>http://www.avaya.com</u>.

- [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 <u>http://www.extremenetworks.com</u>

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at <u>devconnect@avaya.com</u>.