Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Extreme Networks BlackDiamond 12804 to Support Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes present a sample quality of service configuration for the Avaya S8500 Media Server with an Avaya G650 Media Gateway and Avaya IP Telephones using an Extreme Networks BlackDiamond 12804, BlackDiamond 10808 and Avaya C363T-PWR Converged Stackable Switch. The objective of the test was to evaluate interoperability of the products in an Enterprise Local Area Network. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring the Extreme Networks BlackDiamond 12804 to interoperate with Avaya Communication Manager and Avaya G650 Media Gateway in a three-node network consisting of an Avaya C363T-PWR Converged Stackable Switch, an Extreme Networks BlackDiamond 12804 and an Extreme Networks BlackDiamond 10808.

The Extreme Networks BlackDiamond 12804, BlackDiamond 10808, and Avaya C363T-PWR switches are connected to each other in a full mesh topology. Spanning Tree Protocol is configured in all three switches as a layer-2 loop avoidance mechanism. Avaya Communication Manager and Avaya G650 Media Gateway are directly connected into the BlackDiamond 12804 switch.

Infoblox RADIUSone is used to provide 802.1x RADIUS authentication for Avaya IP Telephones and the PC with Funk Odyssey Client that is directly connected into the BlackDiamond 12804. Both MAC and 802.1x Authentications were configured in the BlackDiamond 12804.

Although an Avaya IP Telephone is shown directly attached onto the BlackDiamond 12804, it is actually connected through a passive power supply, since the module used in the sample network does not support Power over Ethernet.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP Telephones are registered with Avaya Communication Manager. Two separate VLANs are configured in the sample network. VLAN v172 is configured to support Avaya Communication Manager, the Avaya G650 Media Gateway and Avaya IP telephones. VLAN v173 is configured to support Data traffic.

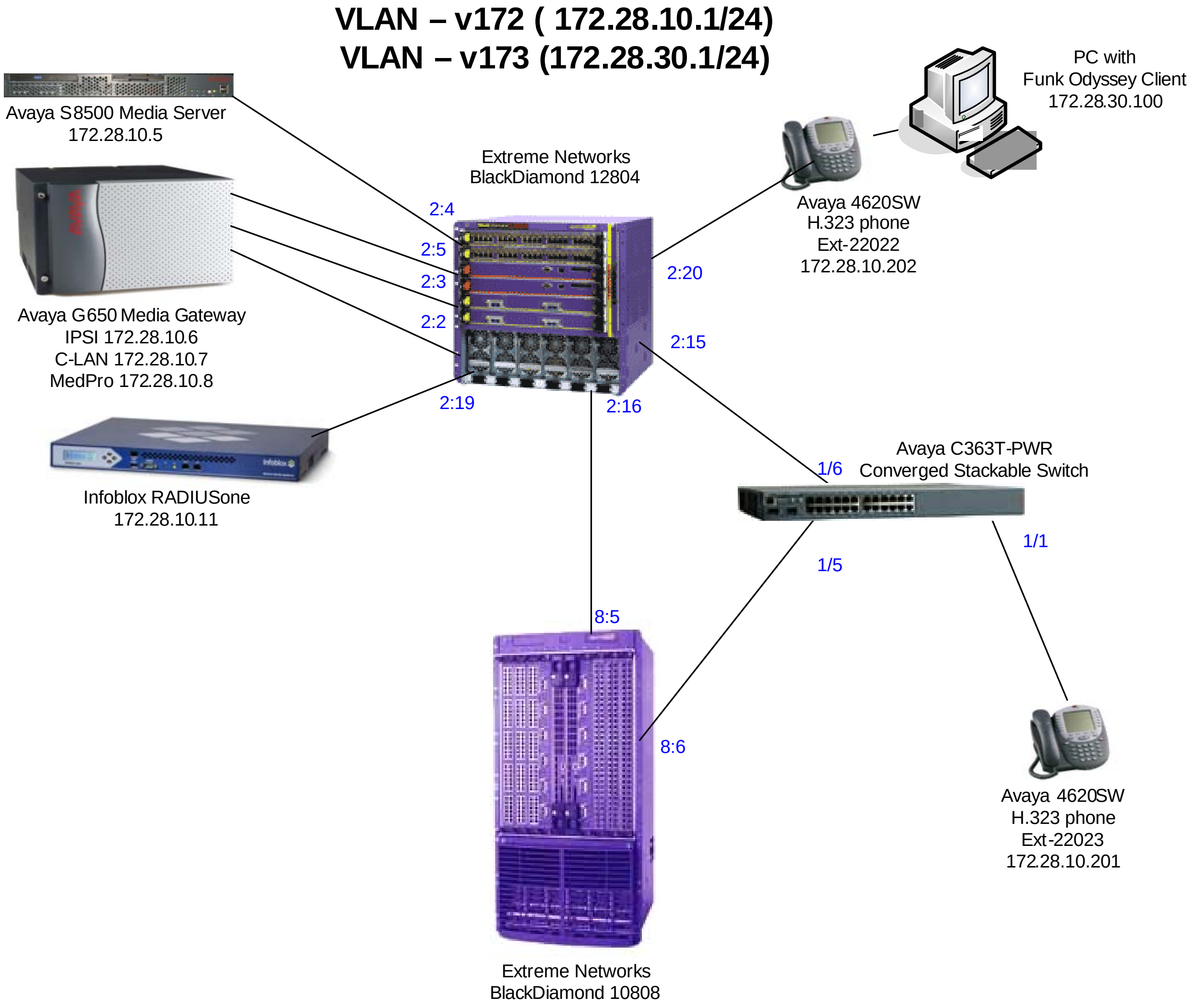


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

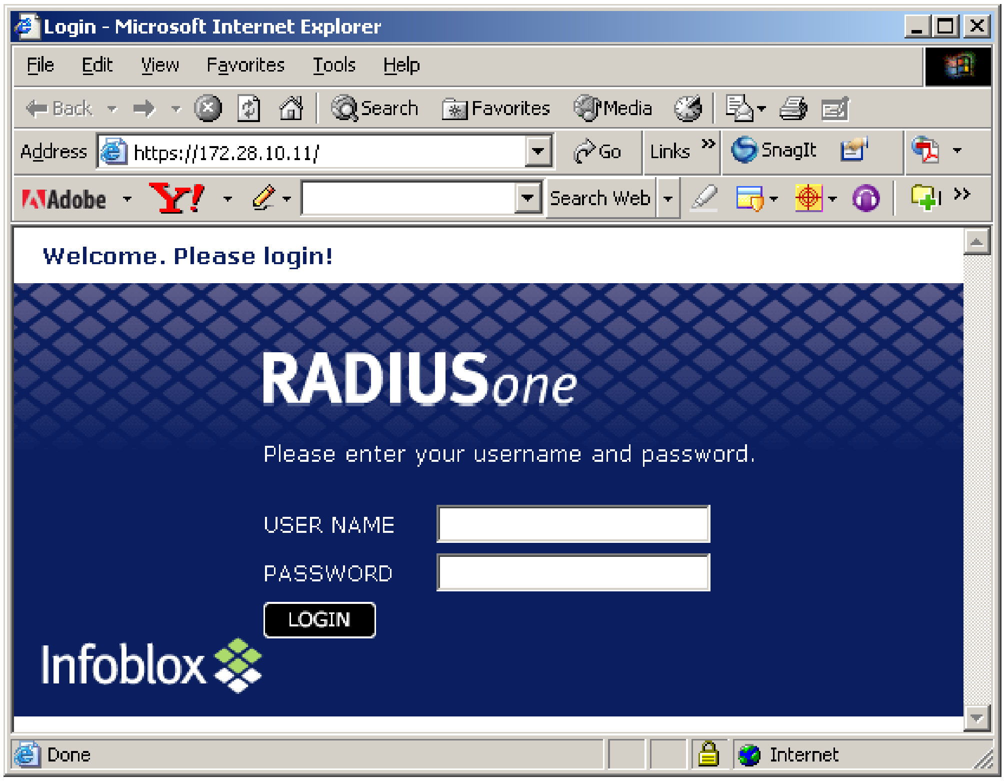
Equipment	Software/Firmware
Avaya S8500 Media Server with Avaya G650 Media Gateway	Avaya Communication Manager 3.1 (R03.1-01.0.628.6) Service Pack 01.0.628-11410
Avaya C363T-PWR Converged Stackable Switch	4.3.10
Avaya 4620SW IP Telephones	2.3
Extreme Networks BlackDiamond 12804	11.4.1.4
Extreme Networks BlackDiamond 10808	11.4.1.4
Infoblox RADIUSone	1.4r1
Funk Odyssey Client for Microsoft Windows	3.03.0.1194

4. Configure Avaya Communication Manager

There is no unique configuration required in Avaya Communication Manager to support the Extreme Networks BlackDiamond 12804 switch or any feature(s) mentioned in this document. For detailed information on the Installation, Maintenance, and Configuration of Avaya Communication Manager, please consult reference [1] and [2].

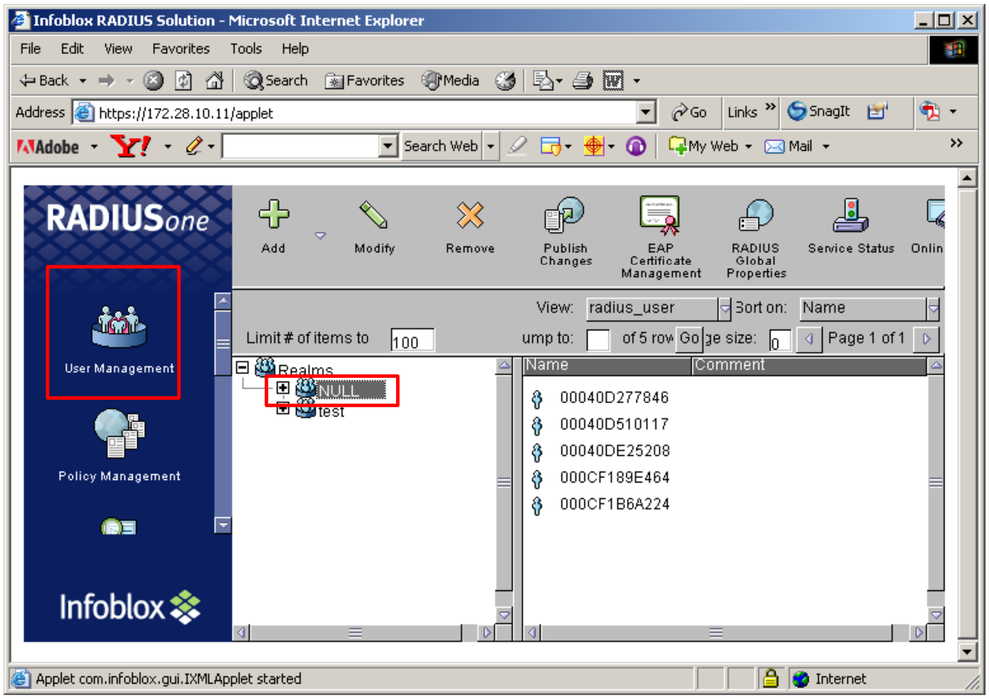
5. Configure Infoblox RADIUSone

The following steps describe how to setup user account on the Infoblox RADIUSone RADIUS server to support 802.1x authentication for Avaya IP Telephones and PC connections from the BlackDiamond 12804 switch.

Step	Description
1.	Connect to the RADIUSone from a Web browser by entering the IP address of RADIUSone as the URL. Log in using the appropriate **USER NAME** and **PASSWORD**.  Login - Microsoft Internet Explorer Address: https://172.28.10.11/ Welcome. Please login! RADIUSone Please enter your username and password. USER NAME PASSWORD

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>2.</b></td><td>

Select **User Management** from the left panel menu. Highlight **NULL** under **Realms**.



Infoblox RADIUS Solution - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.28.10.11/applet
Go Links SnagIt
Adobe Search Web My Web Mail
RADIUSone
Add
Modify
Remove
Publish Changes
EAP Certificate Management
RADIUS Global Properties
Service Status
Onlin
User Management
Policy Management
Infoblox
Realms
NULL
test
Applet com.infoblox.gui.IXMLApplet started
Internet

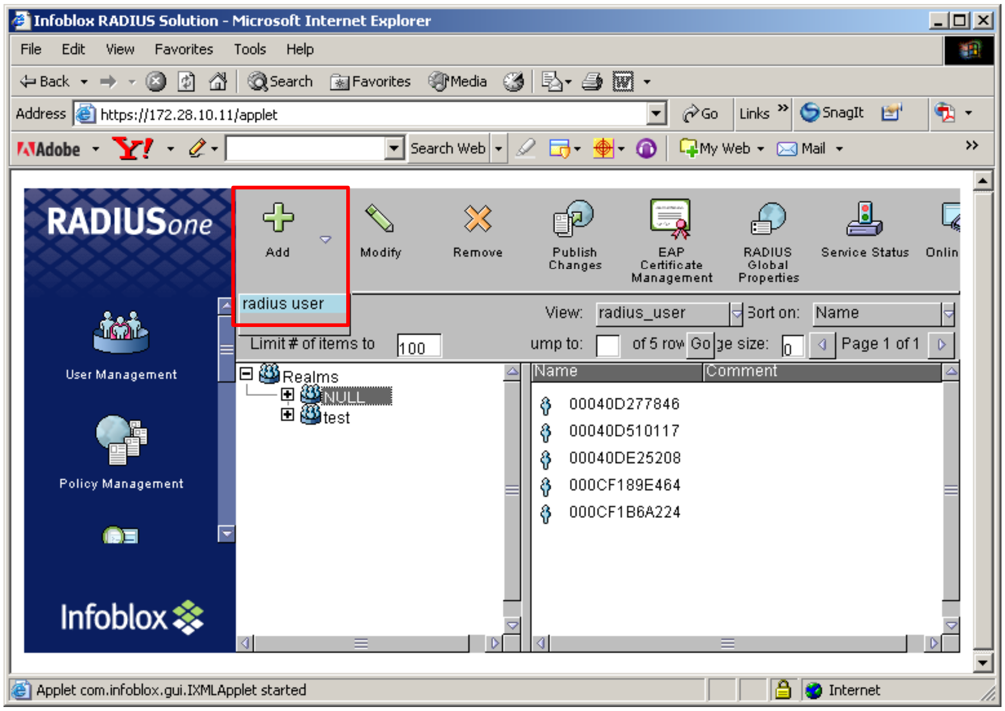
View: radius_user Sort on: Name

Limit # of items to 100 ump to: of 5 row Go ge size: 0 Page 1 of 1

Name	Comment
00040D277846	
00040D510117	
00040DE25208	
000CF189E464	
000CF1B6A224	

</td></tr>
<tr><td><b>3.</b></td><td>

Click on **Add** from the menu bar and select **radius user** from the drop-down menu to add a new RADIUS user.



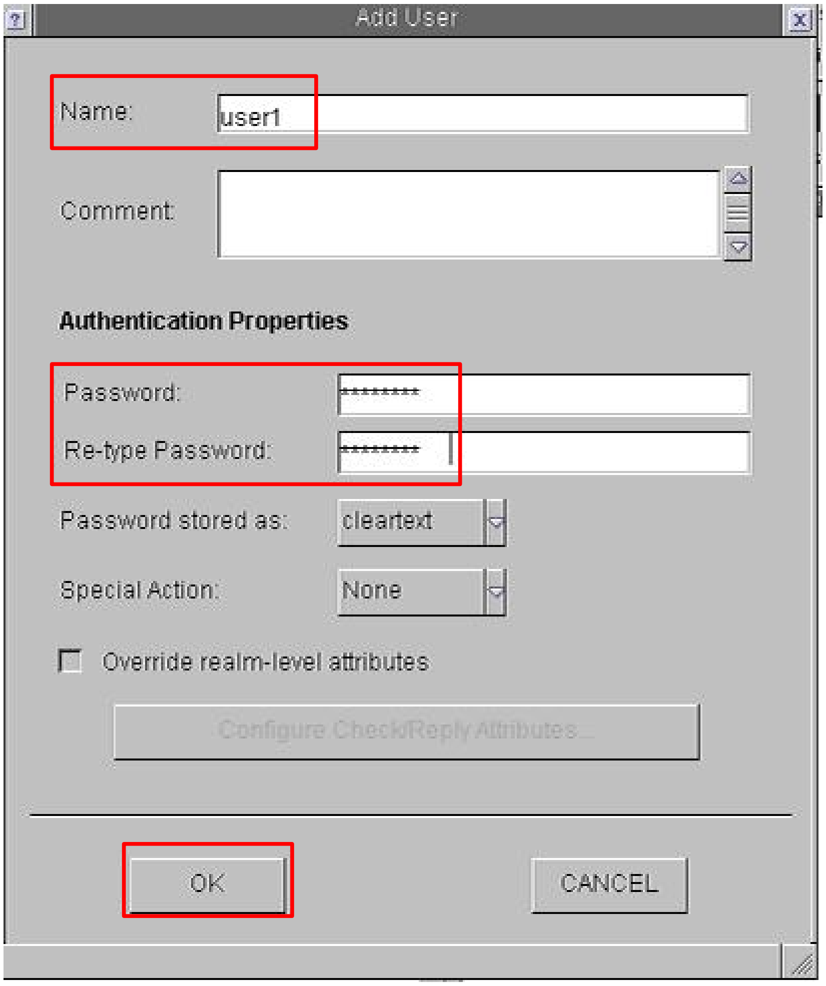
Infoblox RADIUS Solution - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.28.10.11/applet
Go Links SnagIt
Adobe Search Web My Web Mail
RADIUSone
Add
Modify
Remove
Publish Changes
EAP Certificate Management
RADIUS Global Properties
Service Status
Onlin
radius user
User Management
Policy Management
Infoblox
Realms
NULL
test
Applet com.infoblox.gui.IXMLApplet started
Internet

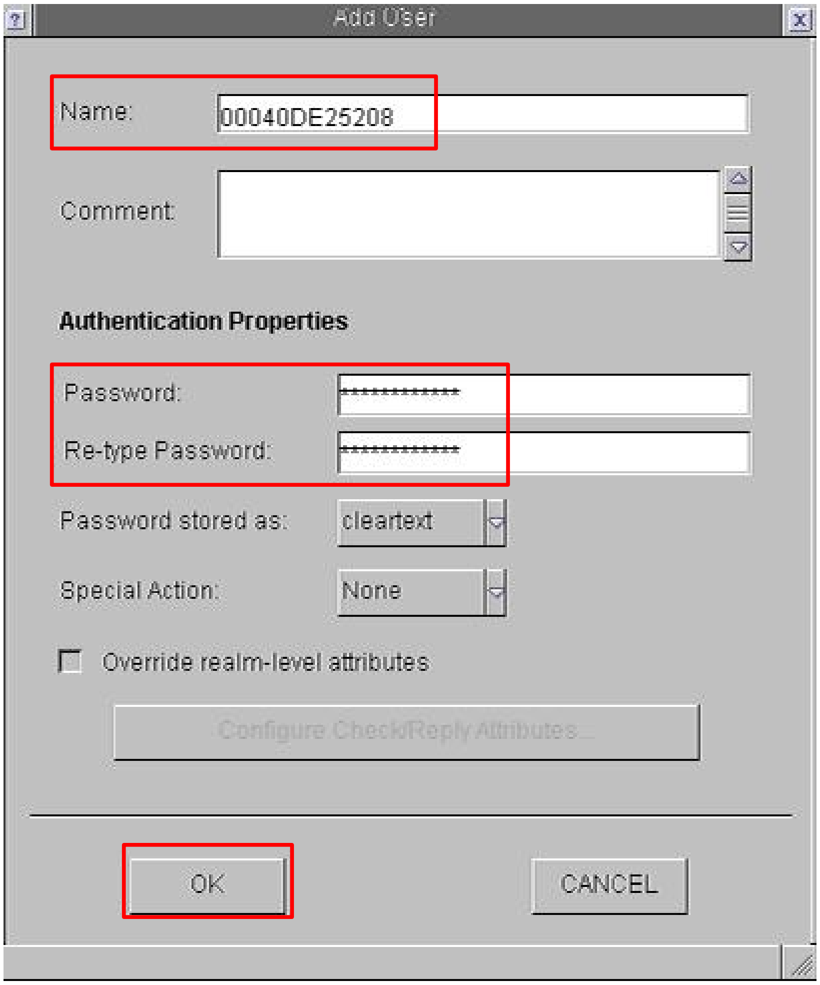
View: radius_user Sort on: Name

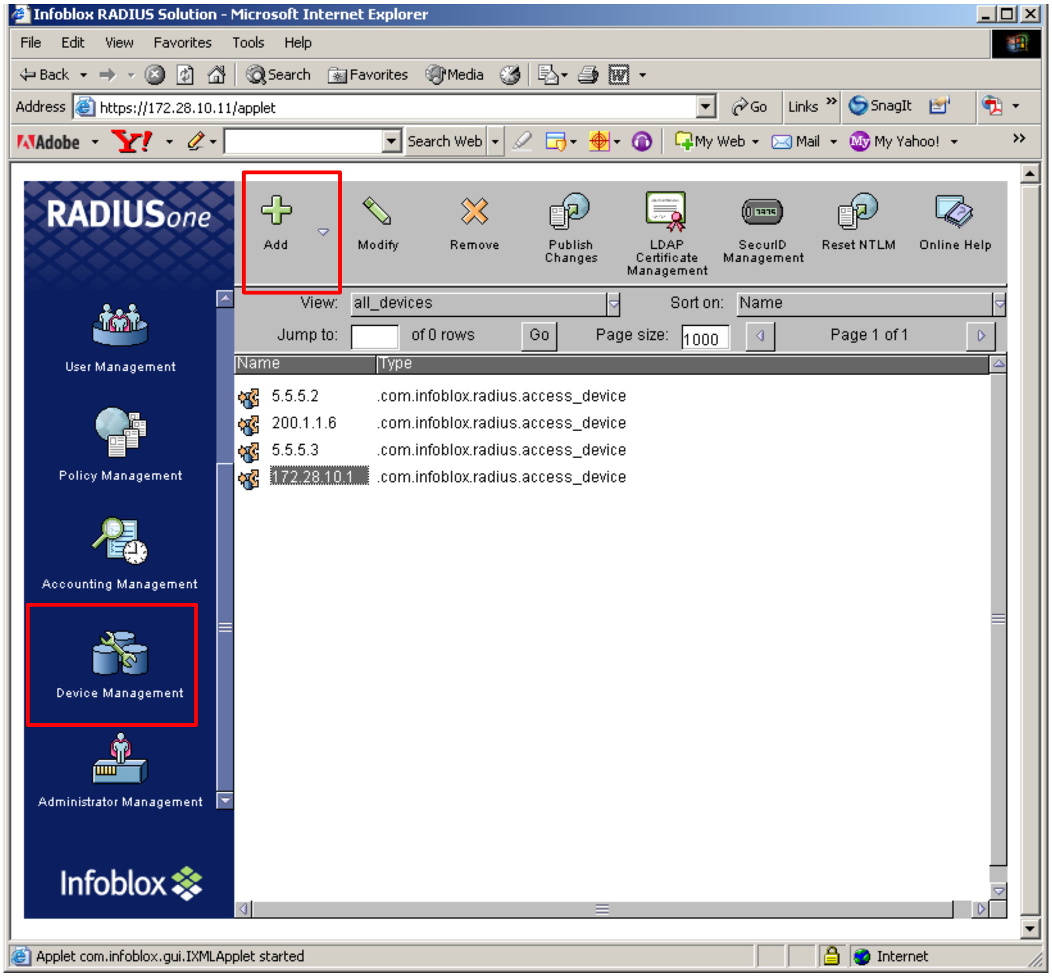
Limit # of items to 100 ump to: of 5 row Go ge size: 0 Page 1 of 1

Name	Comment
00040D277846	
00040D510117	
00040DE25208	
000CF189E464	
000CF1B6A224	

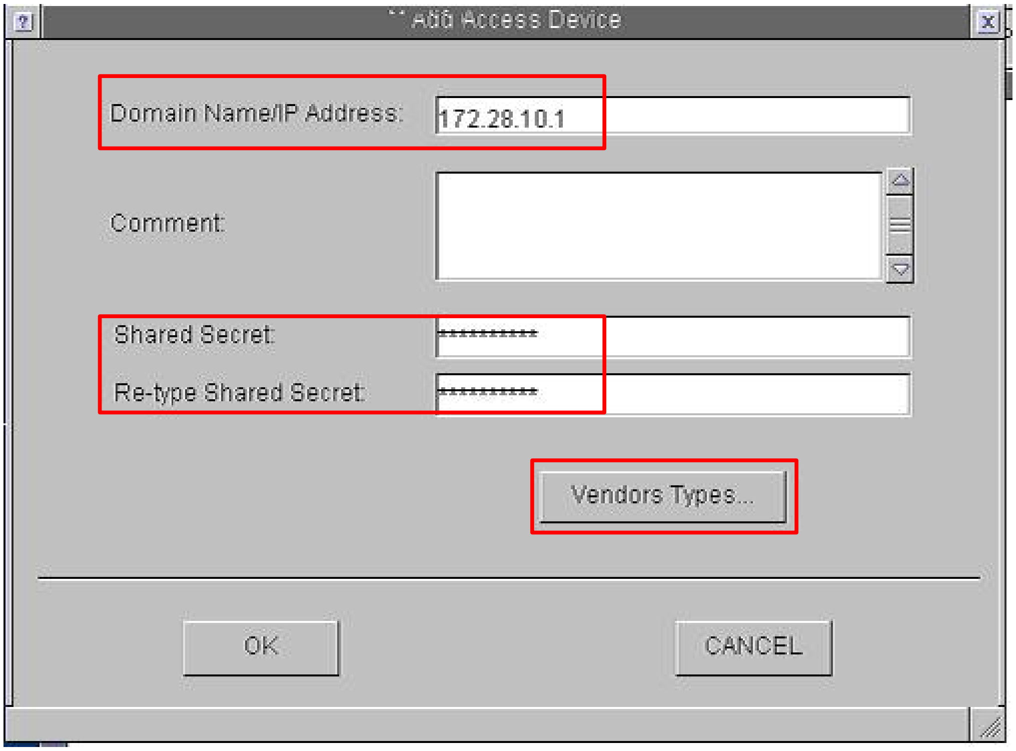
</td></tr>
</table>

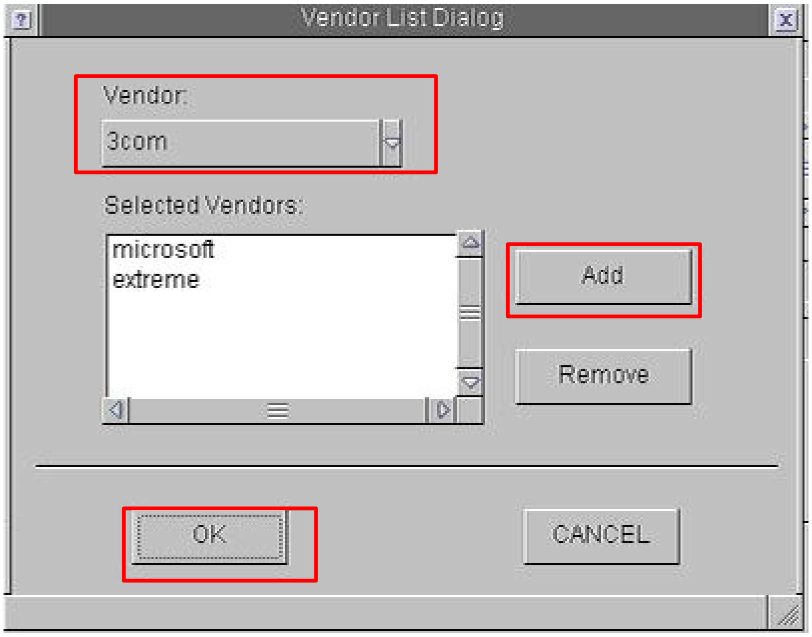
Step	Description
4.	From the **Add User** pop-up window, enter the **Name** and **Password**. The Funk Odyssey client in Section 6, Step 4 will use this information to perform RADIUS authentication. Click **OK** to complete.  Name: user1 Comment: **Authentication Properties** Password: ********* Re-type Password: ********* Password stored as: cleartext Special Action: None ☐ Override realm-level attributes

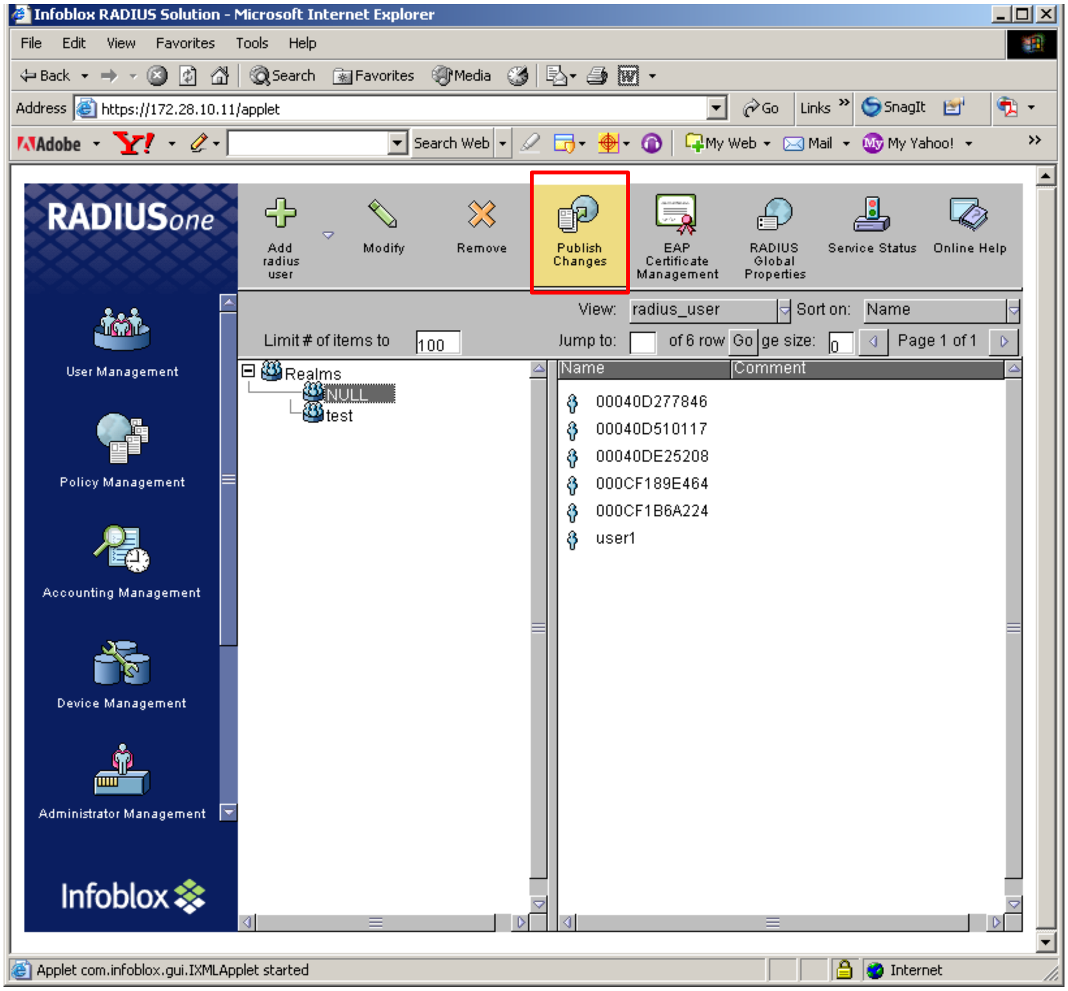
Step	Description
5.	Repeat Step 3 to add an account for the Avaya IP Telephone. Enter the MAC address of the Avaya IP Telephone without any delimiter as the **Name**. Use the same MAC address for **Password**. Click **OK** to complete. **Note:** When the Avaya IP Telephone is connected into the BlackDiamond 12804 switch, the BlackDiamond 12804 will forward the MAC address of the Avaya IP Telephone as both the user name and password to the RADIUS server for authentication.  Add User Name: 00040DE25208 Comment: Authentication Properties Password: ************* Re-type Password: ************* Password stored as: cleartext Special Action: None □ Override realm-level attributes Configure Check/Reply Attributes... OK CANCEL

Step	Description
6.	Select **Device Management** from the left panel menu. Click **Add** from the top menu bar to add a new device. 

Name	Type
5.5.5.2	.com.infoblox.radius.access_device
200.1.1.6	.com.infoblox.radius.access_device
5.5.5.3	.com.infoblox.radius.access_device
172.28.10.1	.com.infoblox.radius.access_device

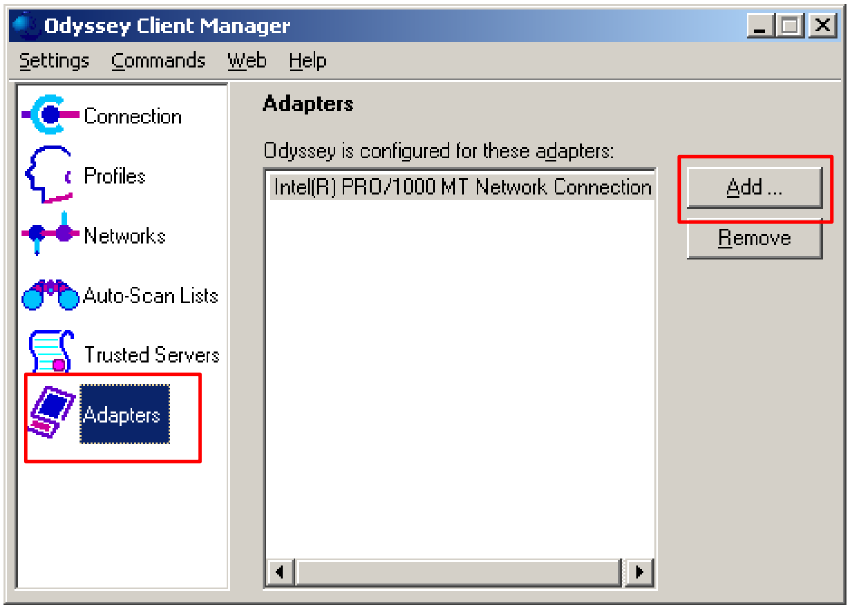
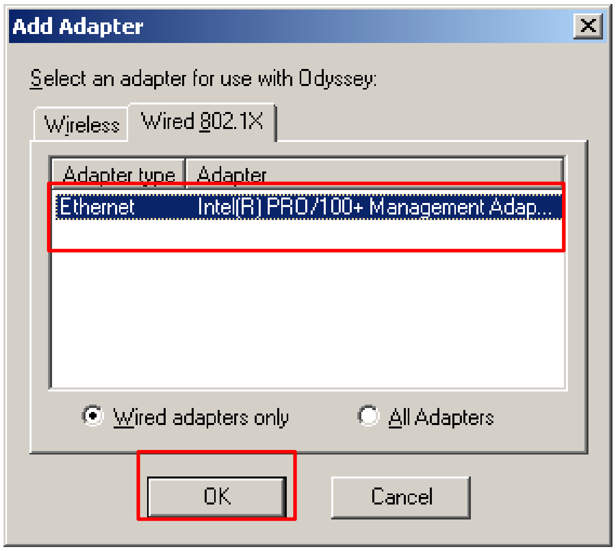
Step	Description
7.	From the **Add Access Device** pop-up window, enter the **Domain Name/IP Address** and **Shared Secret** for the Extreme BlackDiamond 12804. The Shared Secret string will be needed again in Section 7.1 Step 5. Click **Vendors Types** to continue.  Domain Name/IP Address: 172.28.10.1 Comment: Shared Secret: *********** Re-type Shared Secret: ***********

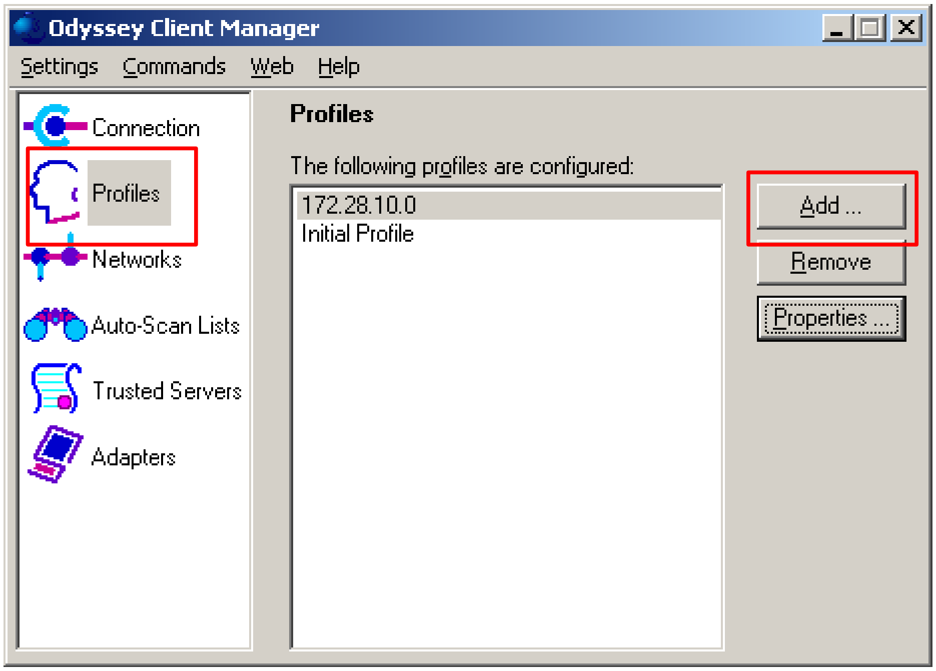
Step	Description
8.	From the **Vendor List Dialog** pop-up window, select **extreme** from the **Vendor** drop-down menu and click **Add**. Select **microsoft** from the **Vendor** drop-down menu and click **Add**. Click **OK** to complete.  Vendor: 3com Selected Vendors: microsoft extreme

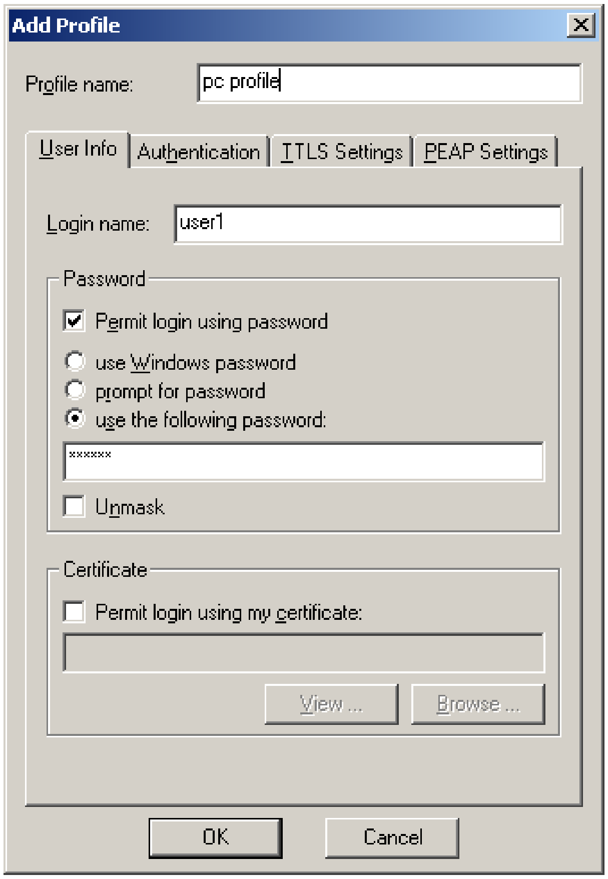
Step	Description
9.	Click **Publish Changes** from the top menu bar to implement the above changes.  Infoblox RADIUS Solution - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Media Address https://172.28.10.11/applet Go Links SnagIt Adobe Search Web My Web Mail My Yahoo! RADIUSone Add radius user Modify Remove Publish Changes EAP Certificate Management RADIUS Global Properties Service Status Online Help User Management Policy Management Accounting Management Device Management Administrator Management Infoblox View: radius_user Sort on: Name Limit # of items to 100 Jump to: of 6 row Go ge size: 0 Page 1 of 1 Realms NULL test Name Comment 00040D277846 00040D510117 00040DE25208 000CF189E464 000CF1B6A224 user1 Applet com.infoblox.gui.IXMLApplet started Internet
10.	Close the Web browser to exit.

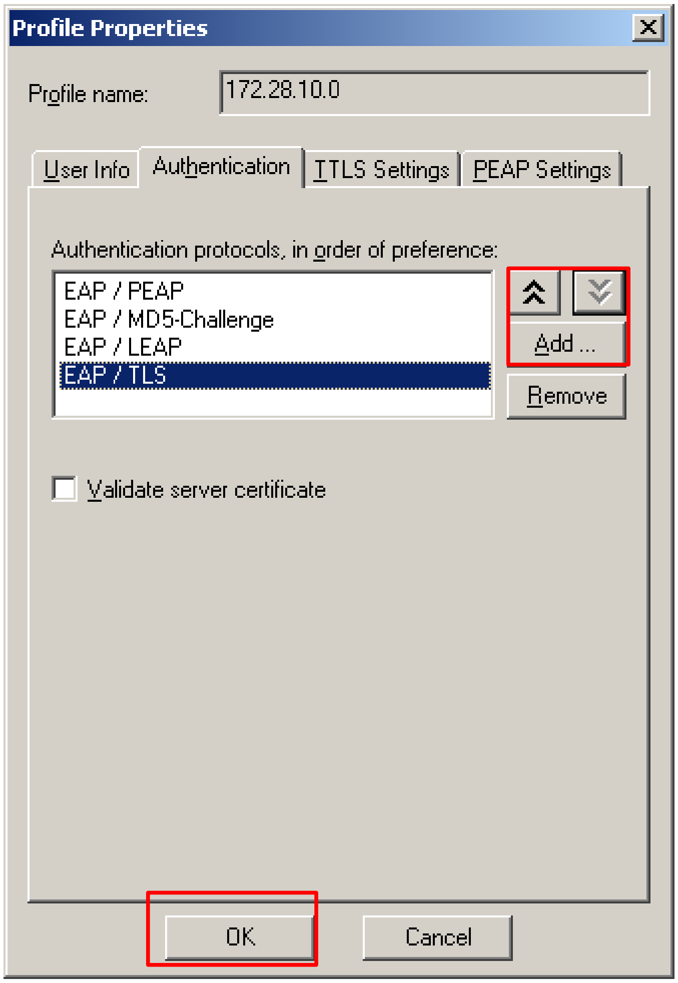
6. Configure the Funk Odyssey Client

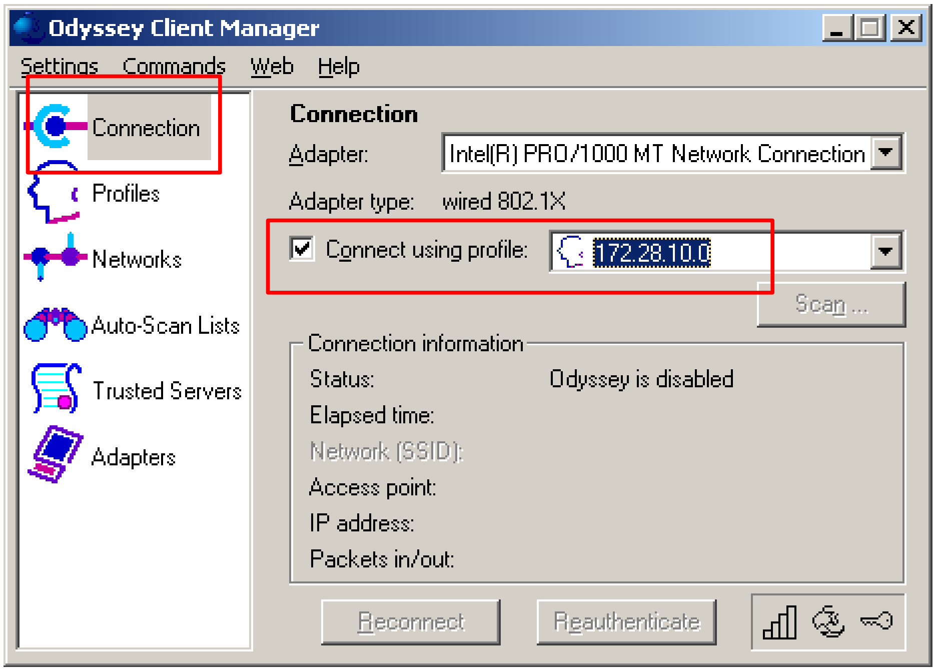
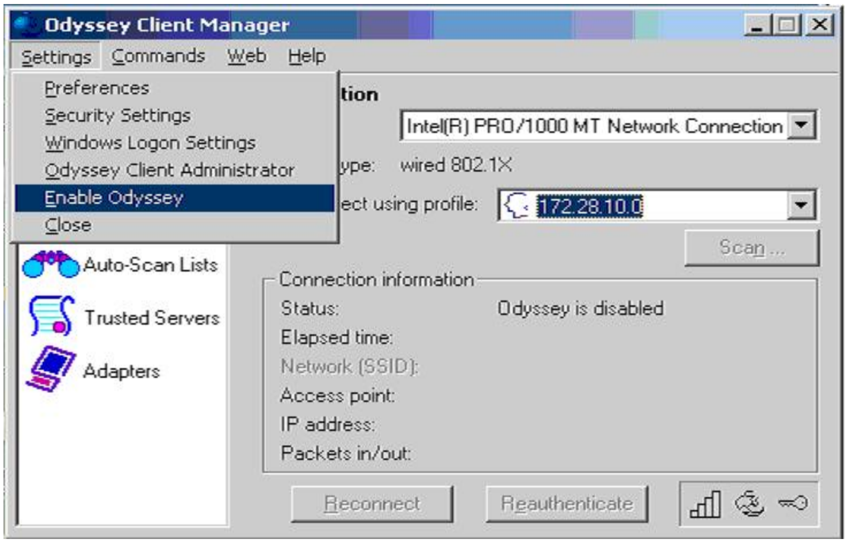
The following steps describe setup for the Funk Odyssey Client running on the PC needed for 802.1x authentication.

Step	Description
1.	Open the Odyssey Client Manager on the PC. Select **Adapters** from the left menu item. Click the **Add** button on the right to display the **Add Adapter** window.  Odyssey Client Manager Settings Commands Web Help Connection Profiles Networks Auto-Scan Lists Trusted Servers Adapters Adapters Add ... Remove Odyssey is configured for these adapters: Intel(R) PRO/1000 MT Network Connection
2.	From the **Add Adapter** pop-up window, select the appropriate Ethernet adapter that will be used to connect onto the network. Click **OK** to complete.  Select an adapter for use with Odyssey: Adapter type: Ethernet Adapter: Intel(R) PRO/100+ Management Adap... ● Wired adapters only ○ All Adapters

Step	Description
3.	Define a profile by highlighting **Profiles** from the left menu item. Click **Add** on the right to display the Add profile window.  Odyssey Client Manager Settings Commands Web Help Connection Profiles Networks Auto-Scan Lists Trusted Servers Adapters Add ... Remove Properties ... **Profiles** The following profiles are configured: 172.28.10.0 Initial Profile

Step	Description
4.	Select the **User Info** tab from the **Add Profile** pop-up window. Enter a **Profile name**, **Login name**, and **password** for this profile. The **Loin name** and **Password** must match what was configured in Section 5, Step 4. Click on the **Authentication** tab to continue.  Add Profile Profile name: pc profile User Info Authentication TTLS Settings PEAP Settings Login name: user1 Password ☑ Permit login using password ○ use Windows password ○ prompt for password ● use the following password: ****** □ Unmask Certificate □ Permit login using my certificate: View ... Browse ... OK Cancel

Step	Description
5.	Under the Authentication tab, select the appropriate type of authentication protocol by clicking on the **Add** button. Highlight any protocol and click on the ︽ button to change the order of preference as to which authentication protocol to use. The sample configuration has EAP/PEAP list first and will use this protocol first for authentication. The rest of the settings are left to their default. Click **OK** to complete.  Profile Properties Profile name: 172.28.10.0 User Info | Authentication | TTLS Settings | PEAP Settings Authentication protocols, in order of preference: EAP / PEAP EAP / MD5-Challenge EAP / LEAP EAP / TLS ︽ ︾ Add ... Remove ☐ Validate server certificate OK Cancel

Step	Description
6.	Click on **Connection** from the left menu and select the appropriate profile from the **Connect using profile** drop-down menu.  Odyssey Client Manager Settings Commands Web Help Connection Profiles Networks Auto-Scan Lists Trusted Servers Adapters Scan ... Reconnect Reauthenticate Connection Adapter: Intel(R) PRO/1000 MT Network Connection Adapter type: wired 802.1X ☑ Connect using profile: 172.28.10.0 Connection information Status: Odyssey is disabled Elapsed time: Network (SSID): Access point: IP address: Packets in/out:
7.	Enable Odyssey by setting the **Settings** from the main menu and select **Enable Odyssey** from the drop-down menu.  Odyssey Client Manager Settings Commands Web Help Preferences Security Settings Windows Logon Settings Odyssey Client Administrator Enable Odyssey Close Auto-Scan Lists Trusted Servers Adapters Scan ... Reconnect Reauthenticate tion Intel(R) PRO/1000 MT Network Connection ype: wired 802.1X ect using profile: 172.28.10.0 Connection information Status: Odyssey is disabled Elapsed time: Network (SSID): Access point: IP address: Packets in/out:

7. Configure Extreme Networks and Avaya Switches

This section describes the configuration for Extreme Networks BlackDiamond 12804, Extreme Networks BlackDiamond 10808, and Avaya C363T-PWR Converged Stackable Switch in the sample configuration.

7.1. Configure Extreme Networks BlackDiamond 12804

The following steps describe the configuration of Extreme Networks BlackDiamond 12804 as shown in the sample network.

Step	Description

1.	Connect to the BlackDiamond 12804. Log in using the appropriate login ID and password.
	`login:`
	`password:`
	`BD-12804 #`

2.	By default all ports belong to VLAN default. Remove the default VLAN from all the ports that will be used in the sample configuration. Disable port 2:15, and 2:16 to prevent spanning tree loop from occurring.
	`BD-12804 # configure vlan default delete ports 2:2-2:5,2:15-16,2:19-20`
	`BD-12804 # disable port 2:15,2:26`

3.	Create VLAN v172 for Avaya IP Telephones, and VLAN v173 for data traffic.
	`BD-12804 # create vlan v172`
	`BD-12804 # config vlan v172 tag 172`
	`BD-12804 # config vlan v172 ipaddress 172.28.10.1/24`
	`BD-12804 # create vlan v173`
	`BD-12804 # config vlan v173 tag 173`
	`BD-12804 # config vlan v173 ipaddress 172.28.30.1/24`
	`BD-12804 # enable ipforwarding`

4.	Assign the appropriate VLAN(s) to each port. Configure port 2:20 with two VLAN.
	`BD-12804 # config vlan v172 add port 2:2-5,2:19 untag`
	`BD-12804 # config vlan v172 add port 2:15-16,2:20 tag`
	`BD-12804 # config vlan v173 add port 2:20 untag`

Step	Description

5.	Configure and enable RADIUS authentication. For Avaya IP Telephone, the MAC address is used for authentication. The PC will use user name and password for authentication.
	Note: The **client-ip address** and the **shared-secret string** used below must match what was configured in Section 5, Step 7.
	`BD-12804 # configure radius primary server 172.28.10.11 client-ip 172.28.10.1`
	`BD-12804 # config radius netlogin primary shared-secret <shared-secret string>`
	`BD-12804 # config netlogin add mac-list`
	`--- Use colon delimited format to enter the phone MAC address ---`
	`BD-12804 # enable netlogin dot1x mac <phone MAC address>`
	`BD-12804 # enable netlogin ports 2:20 dot1x mac`

6.	Enable DiffServ examination. `BD-12804 # enable diffserv examination ports 2:2-2:5,2:20`

7.	Configure Spanning Tree Protocol.
	`BD-12804 # config vlan default add ports 2:15-16`
	`--- vlan v172 was added to port 2:15 & 2:16 in step 3 ---`
	`BD-12804 # config stpd s0 mode dot1d`
	`BD-12804 # config stpd s0 add default ports 2:15,2:16`
	`BD-12804 # config stpd s0 add v172 ports 2:15,2:16`
	`BD-12804 # enable stpd s0`

8.	Enable all ports that has previously disabled. `BD-12804 # enable ports 2:15,2:16`

7.2. Configure Extreme Networks BlackDiamond 10808

The following steps describe the configuration of Extreme Networks BlackDiamond 10808 as shown in the sample network.

Step	Description

1.	Connect to the BlackDiamond 10808. Log in using the appropriate login ID and password.
	`login:`
	`password:`
	`BD-10808 #`

2.	Disable port 8:5, and 8:6 to prevent spanning tree loop from occurring. `BD-10808 # disable port 8:5,8:6`

Step	Description

3.	Create VLAN v172 for Avaya IP Telephones, and VLAN v173 for data traffic.
	`BD-10808 # create vlan v172`
	`BD-10808 # config vlan v172 tag 172`

4.	Assign the appropriate VLAN(s) to each port. Configure port 2:20 with two VLAN. `BD-10808 # config vlan v172 add port 8:5,8:6 tag`

5.	Configure Spanning Tree Protocol.
	`--- vlan v172 was added to port 2:15 & 2:16 in step 4 ---`
	`BD-10808 # config stpd s0 mode dot1d`
	`BD-10808 # config stpd s0 add default ports 8:5,8:6`
	`BD-10808 # config stpd s0 add v172 ports 8:5,8:6`
	`BD-10808 # enable stpd s0`

6.	Enable all ports that have been previously disabled. `BD-10808 # enable ports 8:5,8:6`

7.3. Configure Avaya C363T-PWR Converged Stackable Switch

The following steps describe the configuration of Avaya C363T-PWR Converged Stackable Switch as shown in the sample network.

Step	Description
1.	From a terminal emulation program, connect to the Avaya C363T-PWR Converged Stackable Switch via the console port with the following terminal setting. **Bits per second:** *9600* **Data bits:** *8* **Parity:** *None* **Stop bits:** *1*

2.	Create a VLAN ***v172*** for the Avaya IP Telephone, and assigned this VLAN to the appropriate ports.
	`C360-1(super)# set vlan 172 name v172`
	`C360-1(super)# set trunk 1/1 dot1q`
	`C360-1(super)# set trunk 1/11 dot1q`
	`C360-1(super)# set port vlan-binding-mode 1/1 bind-to-configured`
	`C360-1(super)# set port vlan-binding-mode 1/11 bind-to-configured`

3.	Configure Spanning Tree Protocol.
	`C360-1(super)# set spantree version common-spanning-tree`
	`C360-1(super)# set spantree enable`

8. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Extreme Networks BlackDiamond 12804 to support Avaya Communication Manager, Avaya G650 Media Gateway and Avaya IP Telephones.

8.1. General Test Approach

The general test approach was to configure the BlackDiamond 12804 in a basic sample network similar to how the switch may be implemented in an enterprise environment. A C363T-PWR was used in the sample network to verify basic layer-2 and layer-3 interoperability. QoS was verified by injecting simulated data traffic into the network while calls were being established and maintained with Avaya IP Telephones.

The main objectives were to verify the BlackDiamond 12804 supports the following:

- QoS for VoIP traffic.
- Port based Link Aggregation.
- 802.1D Spanning Tree Protocol.
- 802.1W Rapid Spanning Tree Protocol.
- 802.1x Authentication.
- RIP interoperability.
- OSPF interoperability with.

8.2. Test Results

The Extreme Networks BlackDiamond 12804 successfully achieved all main objectives. The 802.1D Spanning Tree Protocol and 802.1W Rapid Spanning Tree Protocol were verified by disconnecting the inter-switch link, changing the bridge priority and observing converged result. Basic RIP and OSPF interoperability was tested through the use of route propagation between static route configured on the Avaya C363T-PWR and BlackDiamond 12804 switch.

9. Verification Steps

The following steps may be used to verify the configuration:

- Place call between the Avaya IP Telephones.
- Use the “show port <port #> info detail” command on the BlackDiamond 12804 to display port configuration detail.
- Use the “show netlogin” command on the BlackDiamond 12804 to verify authentication information.

10. Support

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

11. Conclusion

These Application Notes have described the administration steps required to configure a basic three nodes network consist of Avaya C363T-PWR Converged Stackable Switch and Extreme Networks BlackDiamond 12804 switch to support Avaya Communication Manager, Avaya G650 Media Gateway, and Avaya IP Telephones.

12. Additional References

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 1, June 2005

[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0

[3] *Administration for Network Connectivity for Avaya Communication Manager,* Doc # 555-233-504, Issue 6, May 2003

[4] *Avaya Application Solutions: IP Telephony Deployment Guide,* Doc# 555-245-600, Issue 4.3, February 2006

[5] *ExtremeWare XOS Concepts Guide, Software Version 11.4,* Part Number: 100218-00 Rev 01, March 2006

[6] *ExtremeWare XOS Command Reference Guide, Software Version 11.4,* Part Number: 100219-00 Rev 01, March 2006

[7] *ExtremeWare CommandReference Guide, Software Version 7.5,* Part Number: 10021 Rev. 01, October 2005

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

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

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