



Avaya Solution & Interoperability Test Lab

Configuring Extreme Networks Summit X450e-48p to support Avaya Communication Manager and Avaya IP Telephones – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Extreme Networks Summit X450e-48p switch to support an Avaya VoIP solution consisting of Avaya Media Server, Avaya Media Gateway and Avaya IP Telephones. The network is composed of both Extreme Networks and Avaya Converged Stackable Switches. Information in these Application Notes has been obtained through *DeveloperConnection* compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring the Extreme Networks Summit X450e-48p switch to support an Avaya VoIP solution. The sample network consists of an Avaya S8500 Media Server, an Avaya G650 Media Gateway, and Avaya IP Telephones in a three-node network composed of Avaya C363T-PWR Converged Stackable Switch, Extreme Networks Summit X450e-48p and BlackDiamond 12k switch.

The Avaya C363T-PWR Converged Stackable Switch, Extreme Networks Summit X450e-48p and BlackDiamond 12k 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 S8500 Media Server and Avaya G650 Media Gateway are directly connected into the BlackDiamond 12k and Avaya IP Telephones are connected into each of the switches.

The Juniper Steel Belted RADIUS (SBR) is used to provide 802.1X RADIUS authentications for Avaya IP Telephone and the PC running Odyssey Client that are connected into the X450e-48p switch. Both the Avaya IP Telephone and PC are individually authenticated through the X450e-48p by the SBR via the X450e's per port multiple 802.1X supplicant support.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. 802.1X RADIUS authentication is enabled on the X450e-48p switch only. The BlackDiamond 12k does not support Power-over-Ethernet (PoE), therefore a power supply (not shown) was used to power the Avaya IP Telephones connecting into the BlackDiamond 12k during testing. All IP addresses are statically administered. Avaya IP Telephones with extension 22022 and 24000 are end points used for verifying call establishment to and from extension 22023. Juniper Odyssey Client is installed on the PC to perform 802.1X RADIUS authentication.

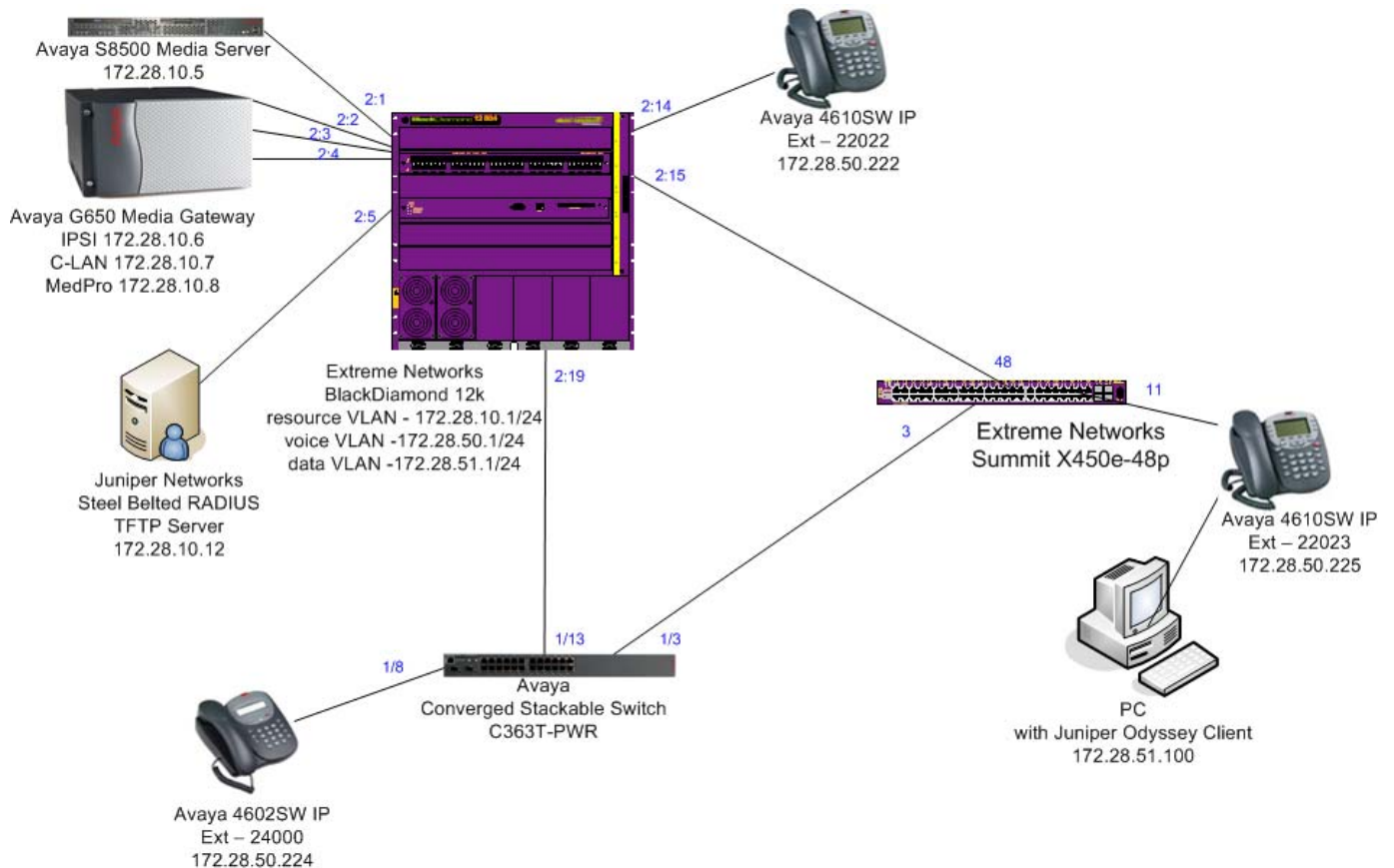


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Media Server	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway	
TN2312BP IPSI	HW03 FW 22
TN799DP C-LAN	HW01 FW 16
TN2302AP IP MedPro	HW18 FW 108
Avaya 4602SW IP Telephone	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone	R2.6 – Application (a10d01b2_6.bin)
Avaya C363T-PWR Converged Stackable Switch	SW Version 4.5.14
Extreme Networks X450e-48P	ExtremeXOS 11.6.1.9
Extreme Networks BlackDiamond 12k	ExtremeXOS 11.4.3.4
Juniper Networks Steel Belted RADIUS	Version 5.4.0 (Build 3149)
Juniper Networks Odyssey Client on PC running Microsoft Windows 2003 Server	4.50.0.2496

4. Configure Extreme Networks equipment

This section describes the configuration for Extreme Network X450e-48p and BlackDiamond 12k as shown in **Figure 1**.

4.1. Configure the Extreme Networks Summit X450e-48p

This section shows the necessary steps in configuring the X450e-48p as shown in **Figure 1**.

Step	Description
1.	Connect to the X450e-48p switch and log in using appropriate credential. login: <i>username</i> password: <i>xxxxxxx</i>
2.	Create the VLANs on the switch. The IP address assignment is optional. All routing is performed by the BlackDiamond 12k. X450e-48p.1 # <i>create vlan temp</i> X450e-48p.1 # <i>create vlan voice</i> X450e-48p.1 # <i>config vlan voice tag 50</i> X450e-48p.1 # <i>config vlan voice ipaddress 172.28.50.2/24 (optional)</i> X450e-48p.1 # <i>create vlan data</i> X450e-48p.1 # <i>config vlan data tag 51</i> X450e-48p.1 # <i>config vlan data ipaddress 172.28.51.2/24 (optional)</i>

Step	Description
3.	<p>Configure spanning tree on the switch. 802.1D spanning tree was used in the sample network.</p> <pre>X450e-48p.1 # configure stpd s0 add vlan voice ports 3,48 dot1d X450e-48p.1 # configure stpd s0 add vlan data ports 3,48 dot1d X450e-48p.1 # enable stpd s0</pre>
4.	<p>Configure VLAN assignment for the ports.</p> <pre>X450e-48p.1 # config vlan default add port 3,48 untagged X450e-48p.1 # config vlan voice add port 3,11,48 tagged X450e-48p.1 # config vlan data add port 11 untagged X450e-48p.1 # config vlan data add port 3,48 tagged</pre>
5.	<p>Configure the switch for RADIUS authentication and enable the switch port for netlogin. The shared-secret must match the one configured in Section 6, Step 2.</p> <pre>X450e-48p.1 # configure radius netlogin primary server 172.28.10.12 1812 client-ip 172.28.10.2 vr VR-Default X450e-48p.1 # configure radius netlogin primary shared-secret 1234567890 X450e-48p.1 # enable radius netlogin X450e-48p.1 # configure netlogin vlan temp X450e-48p.1 # enable netlogin dot1x X450e-48p.1 # enable netlogin ports 11 dot1x</pre>
6.	<p>By default the X450e-48p only has two priority queues, QP1 and QP8. Configure a new QoS profile QP7 on the switch and remap 802.1P priority 6 to this new profile. In the sample configuration the Avaya IP Telephones uses 802.1P tag 6 for media and signaling traffic. Section 9, Step 3 shows where to configure this setting in Avaya Communication Manager. 802.1P examination is enabled by default on the X450e-48p switch; therefore there is no need to enter any additional command to enable this feature on the port.</p> <pre>X450e-48p.1 # create qosprofile "QP7" X450e-48p.1 # configure dot1p type 6 qosprofile QP7</pre>

4.2. Configure the BlackDiamond 12k

This section shows the necessary steps in configuring the BlackDiamond 12k as shown in **Figure 1**.

Step	Description
1.	<p>Connect to the BlackDiamond 12k switch and log in using appropriate credential.</p> <pre>login: username password: xxxxxxx</pre>

Step	Description
2.	<p>Create the VLANs on the switch.</p> <pre> BD-12804.1 # create vlan resource BD-12804.1 # config vlan resource tag 10 BD-12804.1 # config vlan resource ipaddress 172.28.10.1/24 BD-12804.1 # enable ipforwarding resource BD-12804.1 # create vlan voice BD-12804.1 # config vlan voice tag 50 BD-12804.1 # config vlan voice ipaddress 172.28.50.1/24 BD-12804.1 # enable ipforwarding voice BD-12804.1 # create vlan data BD-12804.1 # config vlan data tag 51 BD-12804.1 # config vlan data ipaddress 172.28.51.1/24 BD-12804.1 # enable ipforwarding data </pre>
3.	<p>Configure spanning tree on the switch. 802.1D spanning tree was used in the sample network.</p> <pre> BD-12804.1 # stpd s0 add vlan voice ports 2:15,2:19 dot1d BD-12804.1 # stpd s0 add vlan data ports 2:15,2:19 dot1d BD-12804.1 # enable stpd s0 </pre>
4.	<p>Configure VLAN assignment for the ports.</p> <pre> BD-12804.1 # config vlan default add port 2:15,2:19 untagged BD-12804.1 # config vlan resource add port 2:1-2:5 untagged BD-12804.1 # config vlan voice add port 2:14,2:15,2:19 tagged BD-12804.1 # config vlan data add port 2:15,2:19 tagged </pre>
5.	<p>Enable DiffServ Code-Point examination on the switch for port connecting to the Avaya S8500 Media Server and Avaya G650 Media Gateway.</p> <pre> BD-12804.1 # enable diffserv examination ports 2:1-2:4 </pre>

5. Configure the Avaya C363T-PWR Converged Stackable Switch

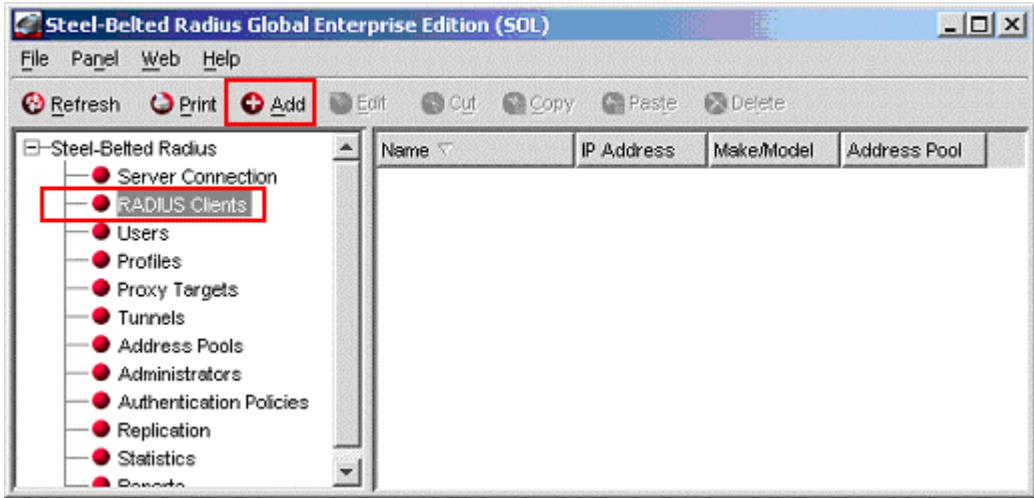
This section shows the steps for configuring the Avaya C363T-PWR Converged Stackable Switch.

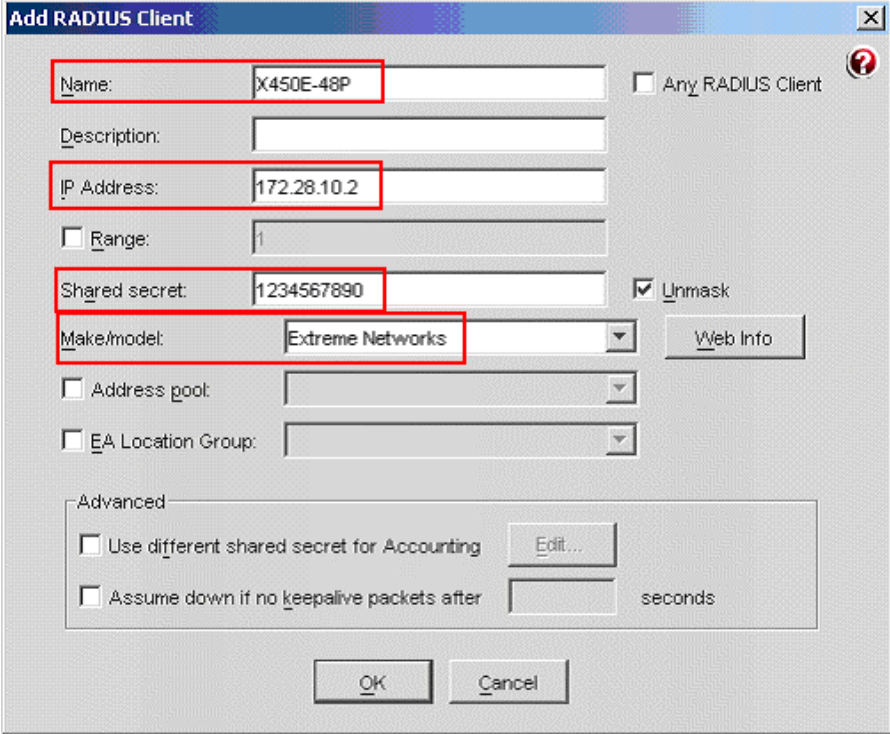
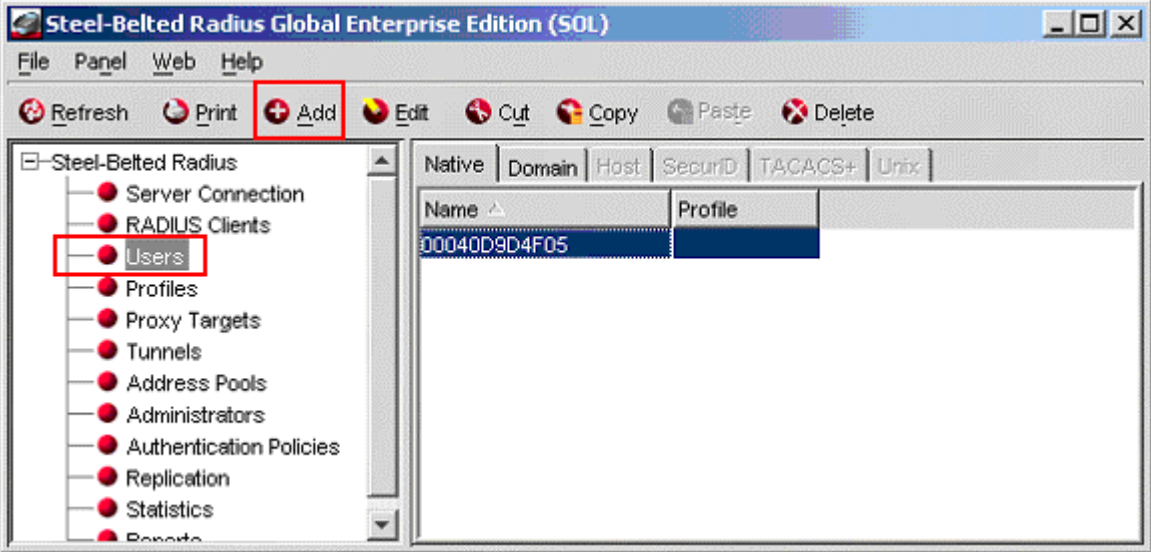
Step	Description
1.	<p>Log in to the Avaya C363T-PWR Converged Stackable Switch using the appropriate credential.</p> <pre> Login: <i>username</i> Password: <i>xxxxxx</i> </pre>

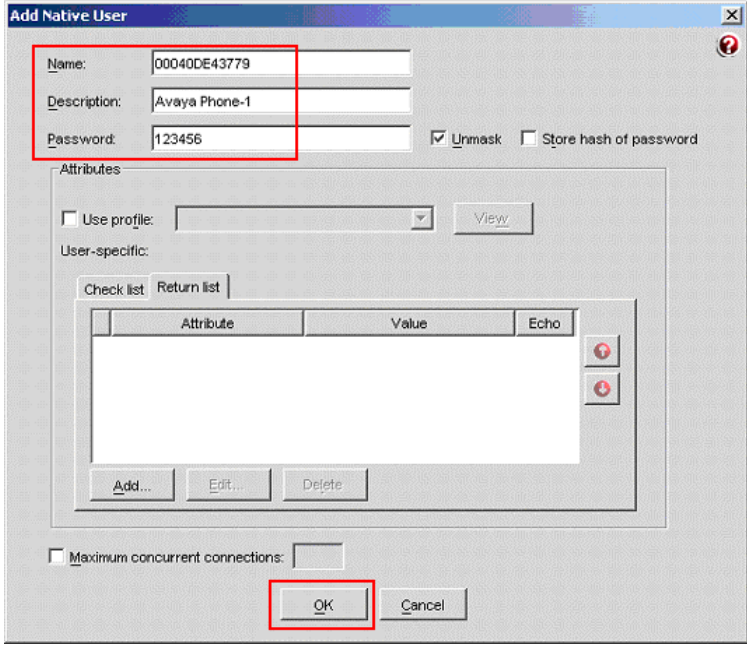
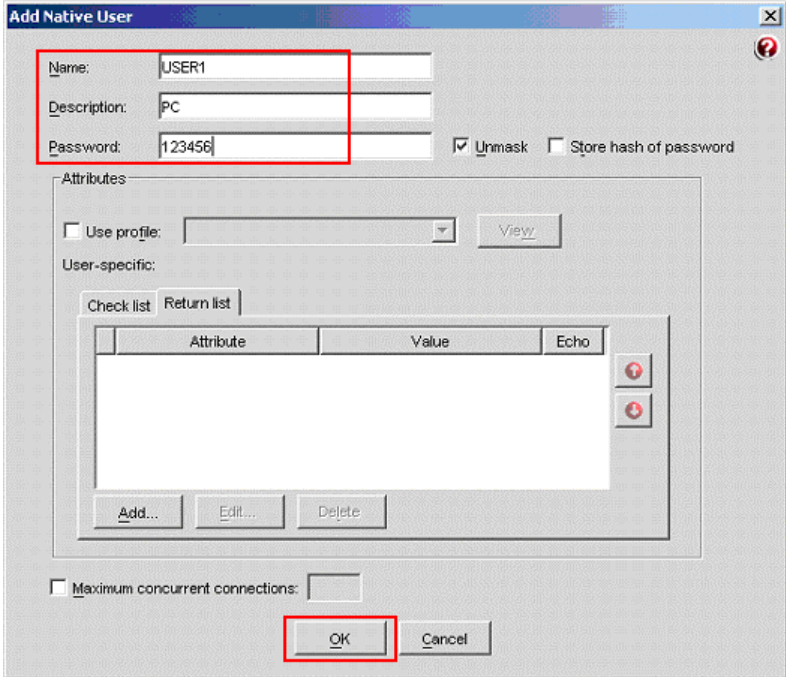
Step	Description
2.	<p>Create the VLANs on the switch.</p> <pre>C360-1(super)# set vlan 10 name resource C360-1(super)# set vlan 50 name voice C360-1(super)# set vlan 51 name data</pre>
3.	<p>Configure VLAN assignment for the ports.</p> <pre>C360-1(super)# set port vlan 50 1/8 C360-1(super)# set port vlan 1 1/3,1/13 C360-1(super)# set trunk 1/3,1/8/1/3 dot1q C360-1(super)# set port vlan-binding-mode 1/3,1/8,1/13 bind-to-configured</pre>

6. Configure Juniper Networks Steel Belted RADIUS

This section shows the steps for configuring the Juniper Networks Steel Belted RADIUS (SBR) server.

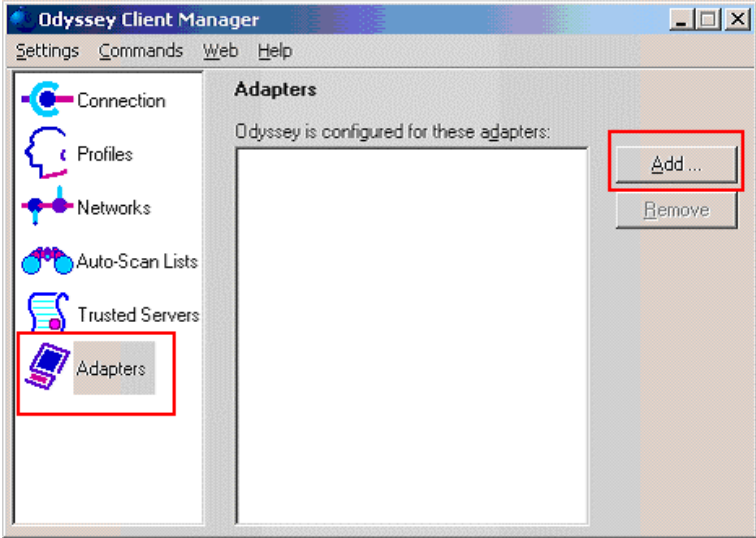
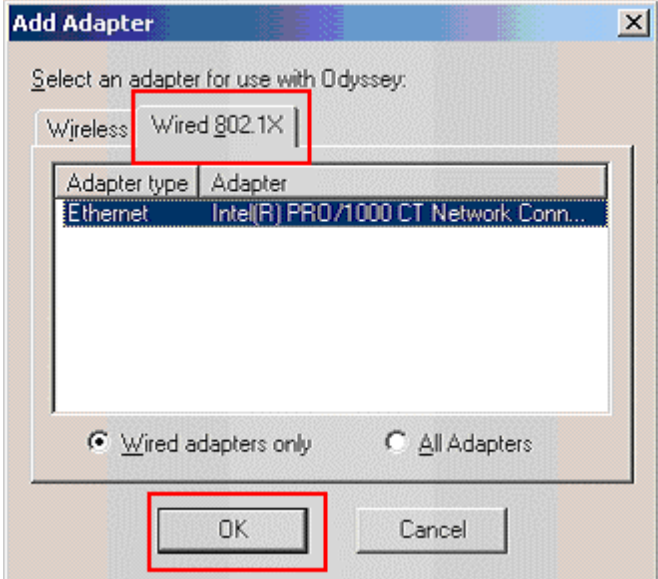
Step	Description
1.	<p>Add a new RADIUS client by highlighting RADIUS Clients on the left panel then click Add after successfully logging into SBR server.</p> 

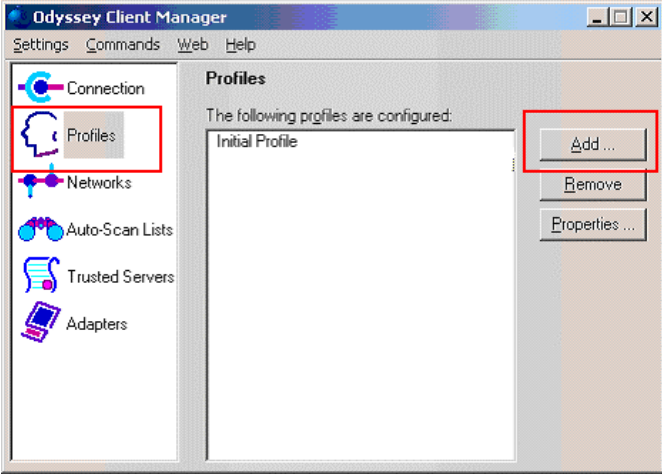
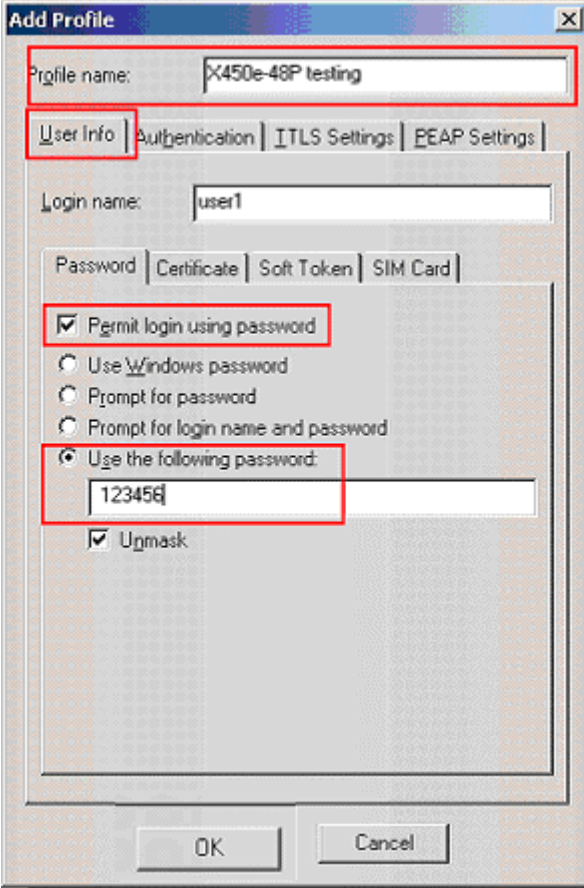
Step	Description
2.	<p>Enter the Name, IP Address, Shared Secret, and the Make/model of the RADIUS client. In this case the RADIUS client is the X450e-48p switch. The shared secret must match what is used by the X450e-48p switch in Section 4.1, Step 5. All other settings are default, and the Unmask check box was selected to facilitate illustration only. Click Ok to complete.</p> 
3.	<p>Highlight Users on the left panel and click Add to create a new user ID for the Avaya IP Telephones and PC.</p> 

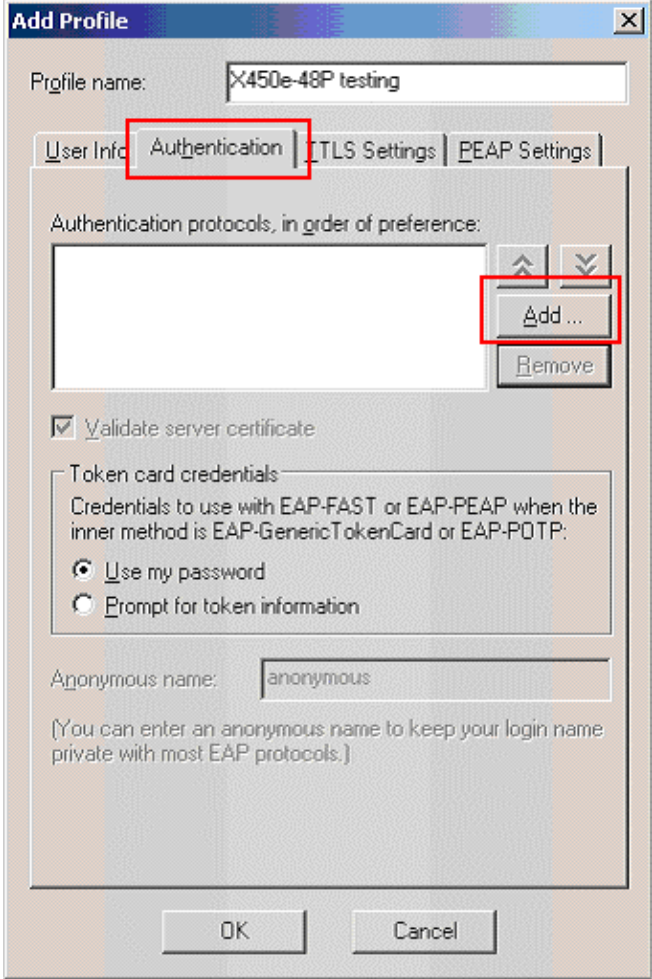
Step	Description
4.	<p>To create a user ID for the Avaya IP Telephones, enter the Avaya Phone's MAC address as the Name, a password for the Avaya IP Telephones to login, and a Description for the user ID. This password will need to be entered on the Avaya IP Telephones in order for the phone to login successfully. Click Ok to complete.</p> 
5.	<p>Repeat Step 3 to create a user ID for the PC. Enter the Name, Description and Password the PC will use to log in. Click Ok to complete.</p> 

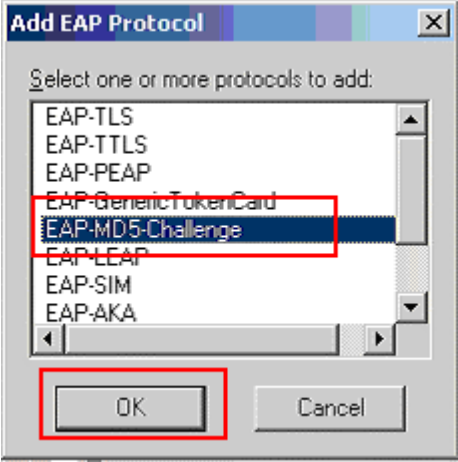
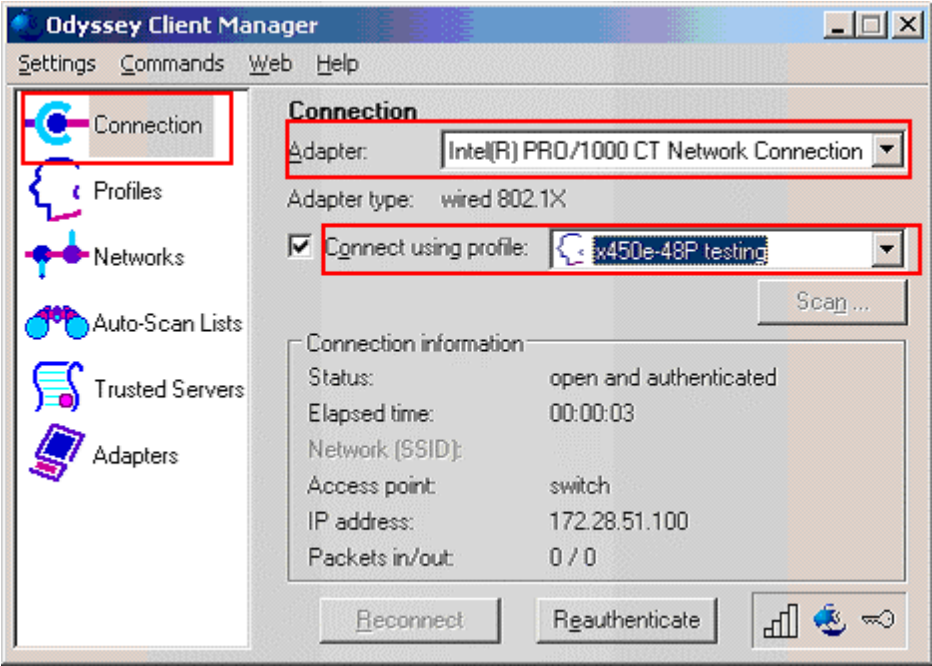
7. Configure the Odyssey client

This section shows the steps for configuring the Odyssey client running on the PC.

Step	Description
1.	Open the Odyssey Client Manager on the PC.
2.	<p>Add a network adapter by selecting Adapters on the left panel then click Add from the Odyssey Client Manager window.</p> 
3.	<p>Click on the Wired 802.1X tab in the Add Adapter pop-up window. Select the desired network adapter and click Ok to complete.</p> 

Step	Description
4.	<p>Add a profile by selecting Profiles on the left panel then click Add to continue.</p>  <p>The screenshot shows the Odyssey Client Manager application window. On the left-hand side, there is a vertical navigation pane with several icons and labels: Connection, Profiles, Networks, Auto-Scan Lists, Trusted Servers, and Adapters. The 'Profiles' icon is highlighted with a red box. In the main area of the window, the 'Profiles' section is active, displaying a list of configured profiles. The list contains one entry, 'Initial Profile'. To the right of this list, there are three buttons: 'Add ...', 'Remove', and 'Properties ...'. The 'Add ...' button is highlighted with a red box.</p>
5.	<p>From the User Info tab in the Add Profile pop-up window. Enter the Login name and password. The Login name and password must match the setup in Section 6, Step 5. Click on the Authentication tab to continue.</p>  <p>The screenshot shows the 'Add Profile' dialog box. At the top, there are four tabs: 'User Info', 'Authentication', 'ITLS Settings', and 'EEAP Settings'. The 'User Info' tab is selected and highlighted with a red box. Below the tabs, there are several input fields and options: <ul style="list-style-type: none"> 'Profile name:' field containing 'X450e-48P testing', highlighted with a red box. 'Login name:' field containing 'user1'. A group of radio buttons for authentication methods: <ul style="list-style-type: none"> 'Permit login using password' is selected and highlighted with a red box. 'Use Windows password' 'Prompt for password' 'Prompt for login name and password' 'Use the following password:' radio button is selected, and the text 'Use the following password:' is highlighted with a red box. A password input field containing '123456', highlighted with a red box. 'Ugmask' checkbox is checked. At the bottom of the dialog box, there are 'OK' and 'Cancel' buttons.</p>

Step	Description
6.	<p>Under the Authentication tab, click Add to Add to add a new authentication protocol.</p>  <p>The screenshot shows the 'Add Profile' dialog box with the 'Authentication' tab selected. The 'Profile name' field contains 'X450e-48P testing'. The 'Authentication protocols, in order of preference:' list is empty. The 'Add ...' button is highlighted with a red box. The 'Validate server certificate' checkbox is checked. The 'Token card credentials' section has 'Use my password' selected. The 'Anonymous name' field contains 'anonymous'. The 'OK' and 'Cancel' buttons are at the bottom.</p>

Step	Description
7.	<p>In the Add EAP Protocol pop-up window, select EAP-MD5 Challenge. Click Ok the Add EAP Protocol pop-up window to complete. Confirm all changes by clicking Ok in previous pop-up window.</p> 
8.	<p>To connect the PC onto the network, click Connection in the left panel of the Odyssey Client Manager. Select the appropriate adapter and connection profile that was configured in Step 3 and 4. Once successfully authenticated, the Status should read open and authenticated.</p> 

8. Configure the Avaya IP Telephones

This section shows the steps for configuring the Avaya 4610 SW IP Phone connected to the X450e-48p switch.

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.

- **Pass-thru Mode** – Unicast supplicant operation for the IP telephone itself, with PAE multicast pass-through for the attached PC, but without proxy Logoff (default).
- **Pass-thru with logoff Mode (p-t w/Logoff)** – Unicast supplicant operation for the IP telephones itself, with PAE multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected from the IP telephone, the phone will send an EAPOL-Logoff for the attached PC.
- **Supplicant Mode** – Unicast or multicast supplicant operation for the IP telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

Since most 802.1X clients use the multicast MAC address for the Extensible Authentication Protocol over LAN (EAPOL) messages, the IP telephone must be configured to the **pass-thru** or **p-t w/Logoff** mode to pass-through these multicast messages. It is recommended to use the **p-t w/Logoff** mode. When the phone is in the **p-t w/Logoff** mode, the phone will do proxy logoff for the attached PC when the PC is physically disconnected. When the X450e-48p receives the logoff message, the PC will be removed from the authorized MAC list.

Step	Description
1.	Press the following keys on the Avaya 4610SW IP phone. Mute82019#
2.	Press the “*” key on the key pad until p-t w/Logoff is displayed, then press “#” key to complete the configuration.

9. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3] and [4]. The following steps describe the configuration of Avaya Communication Manager for configuring a station.

Step	Description
1.	Connect and log into Avaya Communication Manager SAT terminal.

Step	Description
2.	<p>Add a new station to Avaya Communication Manager using the add station command. Configure the following fields.</p> <ul style="list-style-type: none"> • Extension: 22023 (Extension number for the Avaya IP Telephone) • Type: 4610 (Avaya IP Telephone type used for this extension) • Port: IP (Type of connection for the Avaya IP Telephone) • Security Code: 1234 (Security code used by the Avaya IP Telephone to register with Avaya Communication Manager) • Direct IP-IP Audio Connections: y (Enable Shuffling) <p>The first two pages of the add station 22023 configuration are shown below. Repeat step 1 for each additional station.</p> <div style="border: 1px solid black; padding: 10px; background-color: #f0f0f0;"> <pre> add station 22023 Page 1 of 4 STATION Extension: 22023 Lock Messages? n BCC: 0 Type: 4610 Security Code: 1234 TN: 1 Port: IP Coverage Path 1: COR: 1 Name: Room 18 Coverage Path 2: COS: 1 Hunt-to Station: STATION OPTIONS Loss Group: 19 Personalized Ringing Pattern: 1 Message Lamp Ext: 22023 Speakerphone: 2-way Mute Button Enabled? y Display Language: english Survivable GK Node Name: Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? n Customizable Labels? y </pre> </div>

Step	Description
	<pre> add station 22023 Page 2 of 4 STATION FEATURE OPTIONS LWC Reception: spe Auto Select Any Idle Appearance? n LWC Activation? y Coverage Msg Retrieval? y LWC Log External Calls? n Auto Answer: none CDR Privacy? n Data Restriction? n Redirect Notification? y Idle Appearance Preference? n Per Button Ring Control? n Bridged Idle Line Preference? n Bridged Call Alerting? y Restrict Last Appearance? y Active Station Ringing: single Conf/Trans on Primary Appearance? n EMU Login Allowed? n Per Station CPN - Send Calling Number? H.320 Conversion? n Service Link Mode: as-needed Multimedia Mode: enhanced MWI Served User Type: Display Client Redirection? n AUDIX Name: Select Last Used Appearance? n Coverage After Forwarding? s Direct IP-IP Audio Connections? y Emergency Location Ext: 22023 Always Use? n IP Audio Hairpinning? y </pre>
3.	<p>Use the “display ip-network-region” command to display the 802.1P setting configured in the Avaya Communication Manager. Both Call Control and Audio 802.1P priority are set to the value of 6.</p> <pre> display ip-network-region 1 Page 1 of 1 IP NETWORK REGION Region: 10 Location: Authoritative Domain: Name: MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Inter-region IP-IP Direct Audio: yes UDP Port Min: 2048 IP Audio Hairpinning? y UDP Port Max: 3029 DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46 Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 </pre>

10. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the X450e-48p in supporting Avaya Communication Manager, Avaya Media Gateway and Avaya IP Telephones in a network composed of both Extreme Networks and Avaya switches.

10.1. General Test Approach

Quality of Service was verified by injecting simulated traffic into the network using a traffic generator while calls were being established and maintained using Avaya IP Telephones. The objectives were to verify the X450e-48p supports the following:

- 802.1X authentication
- Interoperability of basic 802.1D spanning tree
- Layer-2, Layer-3, port based and VLAN based Quality of Service
- Basic calling performed by Avaya IP Telephones (e.g. place/receive call, transfer, DTMF pass-through)

10.2. Test Results

The Extreme Networks X450e-48p switch successfully achieved the above objectives. Quality of Service for VoIP traffic was maintained throughout testing in the presence of competing simulated traffic. The 802.1D spanning tree correctly converged when the active link was disconnected or when bridging priority was changed.

11. Verification Steps

The following steps may be used to verify the configuration:

- Use the “show stpd <stpd domain>” command on the Extreme Networks switches to verify spanning tree operation. Below is a sample output from the X450e-48p switch. Verify whether the **operational mode** and the **designated root** are set to 802.1D.

```
* X450e-48p.1 # show stpd s0
Stpd: s0                               Stp: ENABLED                               Number of Ports: 2
Rapid Root Failover: Disabled
Operational Mode: 802.1D                Default Binding Mode: 802.1D
802.1Q Tag: (none)
Ports: 3,48
Participating Vlans: Default
Auto-bind Vlans: Default
Bridge Priority: 32768
BridgeID:                               80:00:00:04:96:26:6d:6a
Designated root: 80:00:00:04:0d:7d:d3:ff
RootPathCost: 19                        Root Port: 3
MaxAge: 20s                             HelloTime: 2s                               ForwardDelay: 15s
CfgBrMaxAge: 20s                        CfgBrHelloTime: 2s                         CfgBrForwardDelay: 15s
Topology Change Time: 35s               Hold time: 1s
Topology Change Detected: FALSE         Topology Change: FALSE
Number of Topology Changes: 3
Time Since Last Topology Change: 82886s
```

- Use the “show stpd <stpd domain> ports” command to verify whether the uplink ports are in **forwarding** or **blocking** state.

```
* X450e-48p.2 # show stpd s0 ports
Port  Mode  State  Cost  Flags  Priority  Port ID  Designated Bridge
3    802.1D FORWARDING 19    eRbb-d--- 16      8003    80:00:00:04:0d:7d:d3:ff
48   802.1D FORWARDING 19    eDbb-d--- 16      8030    80:00:00:04:96:26:6d:6a

Total Ports: 2

----- Flags: -----
1:          e=Enable, d=Disable
2: (Port role) R=Root, D=Designated, A=Alternate, B=Backup, M=Master
3: (Config type) b=broadcast, p=point-to-point, e=edge, a=auto
4: (Oper. type) b=broadcast, p=point-to-point, e=edge
5:          p=proposing, a=agree
6: (partner mode) d = 802.1d, w = 802.1w, m = mstp
7:          i = edgeport inconsistency
8:          S = edgeport safe guard active
           s = edgeport safe guard configured but inactive
9:          B = Boundary, I = Internal
```

- Use the “show radius” command on the X450e-48p to verify whether RADIUS setting such as **IP address** and **Client address** are correct. A successful log in by a 802.1X client should show 2 Access Requests, 1 Access Accepts, and 1 Access Challenges in the counter.

```
* X450e-48p.6 # show radius
Switch Management Radius: enabled
Switch Management Radius server connect time out: 3 seconds
Switch Management Radius Accounting: disabled
Switch Management Radius Accounting server connect time out: 3 seconds
Netlogin Radius: enabled
Netlogin Radius server connect time out: 3 seconds
Netlogin Radius Accounting: disabled
Netlogin Radius Accounting server connect time out: 3 seconds

Primary Netlogin Radius server:
  Server name      :
  IP address       : 172.28.10.12
  Server IP Port   : 1812
  Client address   : 172.28.10.2 (VR-Default)
  Shared secret    : 3>:>?75<;5
Access Requests  : 2
Access Rejects    : 0
Access Retransmits: 0
Bad authenticators: 0
Round Trip Time   : 0
Access Accepts   : 1
Access Challenges: 1
Client timeouts   : 0
Unknown types     : 0
```

- Use the “show netlogin” command on the X450e-48p to verify if 802.1X is enabled or if the PC or Avaya IP Telephones has successfully been authenticated. The output also shows which VLAN the client is authenticated onto. Note that the Avaya IP Telephones (MAC address 00:04:0d:e4:37:79) is only authenticated in the voice VLAN even though its MAC address is displayed in the data VLAN.

```
* X450e-48p.15 # show netlogin

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

-----
Web-based Mode Global Configuration
-----
Base-URL                      : network-access.com
Default-Redirect-Page        : http://www.extremenetworks.com
Logout-privilege             : YES
Netlogin Session-Refresh     : ENABLED; 3 minutes

-----

802.1x Mode Global Configuration
-----
Quiet Period                  : 60
Supplicant Response Timeout   : 30
```

```

Re-authentication period      : 3600
RADIUS server timeout        : 30
EAPOL MPDU version to transmit : v1
-----

Port: 11, Vlan: data, State: Enabled, Authentication: 802.1x, Guest Vlan <Not Configured>: Disabled

MAC                IP address      Auth  Type      ReAuth-Timer  User
00:04:0d:e4:37:79  0.0.0.0         No   Type      0              00040DE43779
00:12:3f:25:26:60  0.0.0.0         Yes  802.1x    3593           user1
-----

Port: 11, Vlan: voice, State: Enabled, Authentication: 802.1x, Guest Vlan <Not Configured>: Disabled

MAC                IP address      Auth  Type      ReAuth-Timer  User
00:04:0d:e4:37:79  172.28.50.225  Yes  802.1x    3463           00040DE43779
-----

```

- Use the “show dot1p” command on the X450e-48p switch has the correct 802.1P to QoS Profile assignment.

```

X450e-48p.3 # show dot1p
  802.1p Priority Value      QOS Profile
          0                  QP1
          1                  QP1
          2                  QP1
          3                  QP1
          4                  QP1
          5                  QP1
          6                  QP7
          7                  QP8

```

- Use the “show trunk” command on the Avaya C363T-PWR Converged Stackable Switch to verify port 1/3, 1/8 and 1/13 are set as trunk and are bound to configured vlans.

```

C360-1(super)# show trunk

Port    Mode  Binding mode                Native vlan
-----
 1/1    off  statically bound            1
 1/2    off  statically bound            1
 1/3    dot1q bound to configured vlans  1
 1/4    off  statically bound            1
 1/5    off  statically bound            1
 1/6    off  statically bound            1
 1/7    off  statically bound            1
 1/8    dot1q bound to configured vlans  51
 1/9    off  statically bound            1
 1/10   off  statically bound            1
 1/11   off  statically bound            1
 1/12   off  statically bound            1
 1/13   dot1q bound to configured vlans  1

```

- Use the “show spantree” command on the Avaya C363T-PWR Converged Stackable Switch to verify the Designated Root is correct. All switches should point to the same Designated Root.

```
C360-1(super)# show spantree

Spanning tree state is enabled

Designated Root: 00-04-0d-7d-d3-ff
Designated Root Priority: 32768
Designated Root Cost: 0
Designated Root Port: No root port, Bridge is
Designated root
Root Max Age: 20 Hello Time: 2
Root Forward Delay: 15

Bridge ID MAC ADDR: 00-04-0d-7d-d3-ff
Bridge ID priority: 32768
Bridge Max Age: 20 Bridge Hello Time: 2
Bridge Forward Delay: 15 Tx Hold Count 3
Spanning Tree Version is common spanning tree
Spanning Tree Default Path Costs is according to
common spanning tree
```

Port	State	Cost	Priority
1 /1	not-connected	19	128
1 /2	not-connected	19	128
1 /3	Forwarding	19	128
1 /4	not-connected	19	128
1 /7	not-connected	19	128
1 /8	Forwarding	19	128
1 /9	not-connected	19	128
1 /10	not-connected	19	128
1 /11	not-connected	19	128
1 /12	not-connected	19	128
1 /13	not-connected	19	128
1 /14	not-connected	19	128
1 /15	not-connected	19	128
1 /16	Forwarding	19	128
1 /17	not-connected	19	128
1 /18	not-connected	19	128

12. Support

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

13. Conclusion

These Application Notes have described the administration steps required to configure the Extreme Networks X450e-48p switch to support an Avaya VoIP solution depicted in **Figure 1** which composed of an Avaya S8500 Media Server, an Avaya G650 Media Gateway, and Avaya IP Telephones.

14. Additional References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2.1, May 2006
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005
- [3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 11, February 2006
- [4] *Avaya IP Telephony Implementation Guide*, May 1, 2006
- [5] *Configuring Link Layer Discovery Protocol (LLDP) and 802.1X Protocol on Extreme Networks BlackDiamond 8810 for an Avaya IP Telephone with an Attached PC*, Issue 1.1, Dec 18, 2006

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

- [6] *ExtremeWare XOS Concepts Guide, Software Version 11.6*, Part number 100247-00 Rev. 01, 2006
- [7] *ExtremeWare XOS Command Reference Guide, Software Version 11.6*, Part number 100246-00 Rev. 01, 2006

©2007 Avaya Inc. All Rights Reserved.

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

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