Avaya Solution & Interoperability Test Lab

Configuring the Extreme Networks Summit X150-48t and X150-24t Switch to support Avaya Communication Manager using RADIUS Authentication – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Extreme Networks Summit X150-24t and X150-48t switches to support an Avaya VoIP solution consisting of an Avaya S8500 Server, an Avaya G650 Media Gateway and Avaya 9600 Series IP Telephones using RADIUS authentication in a network composed of Extreme Networks Summit switches, and an Avaya Converged Stackable Switch. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring the Extreme Networks Summit X150-24t and X150-48t Switches to support an Avaya Voice over IP (VoIP) solution consisting of an Avaya S8500 Server, Avaya G650 Media Gateway, and Avaya 9600 Series IP Telephones in a three-node network composed of an Avaya C363T-PWR Converged Stackable Switch, an Extreme Networks Summit X150-48t Switch (X150-48t) and an Extreme Networks X150-24t Switch (X150-24t). For the remainder of this document, when a comment is referring to both the X150-48t and the X150-24t collectively, they will be referred to simply as the X150s.

The Avaya C363T-PWR, X150-24t, and X150-48t switches are connected to each other in a full mesh topology. 802.1D Spanning Tree Protocol (STP) is configured in the X150s and Avaya C363T-PWR switches as a layer-2 loop avoidance mechanism. Avaya IP Telephones are connected to the different Ethernet switches.

Microsoft Internet Authentication Service (IAS) is used to provide 802.1X RADIUS authentications for Avaya IP Telephones and PCs connected to the X150s. The Avaya IP Telephones and PCs are individually authenticated through the X150s by the IAS via the X150s' per port, multiple 802.1X supplicant support.

Link Layer Discovery Protocol (LLDP) is used to assign Call Server, File Server, and VLAN information to Avaya IP Telephones, and exchange advertisements between the X150s and Avaya IP Telephones.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. 802.1X authentication is enabled on the X150s only. All IP addresses are obtained via Dynamic Host Configuration Protocol (DHCP) unless noted. The "voice" VLAN with IP network 172.28.10.0/24, and the "data" VLAN with IP network 172.28.11.0/24 are used in the sample network. The X150-24t and X150-48t do not support Power over Ethernet (PoE), therefore the Avaya 9600 Series IP Telephones are connected into the switch through an external power supply not shown.

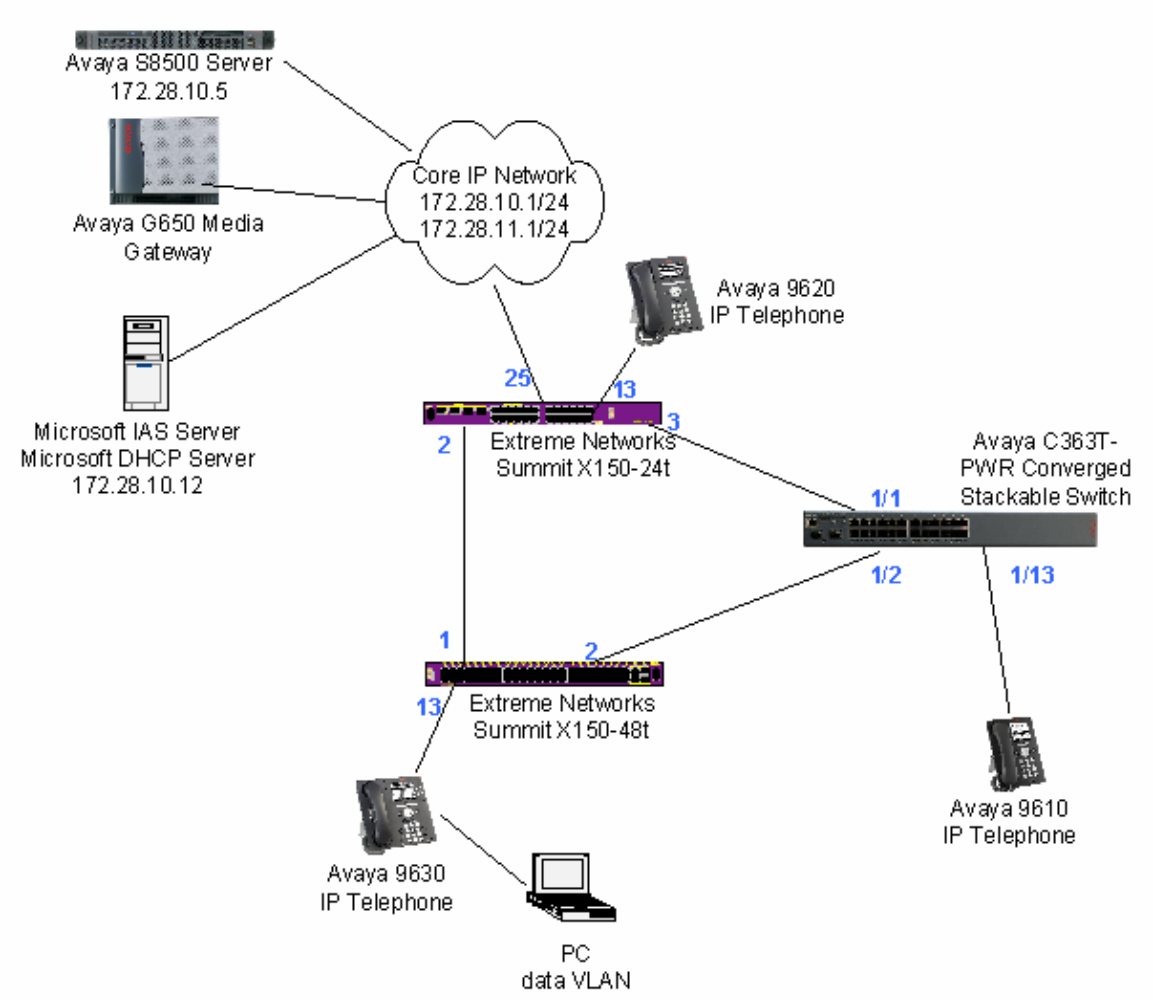


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Server with G650 Media Gateway	Avaya Communication Manager R4.1 (R014x.00.1.731.2)
Avaya 9630 IP Telephone	R 1.5 (H.323)
Avaya 9620 IP Telephone	R 1.5 (H.323)
Avaya 9610 IP Telephone	R 1.5 (H.323)
Avaya C363T-PWR Converged Stackable Switch	SW Version 4.5.18
Extreme Networks X150-24t Switch	ExtremeXOS 12.0.2.18
Extreme Networks X150-48t Switch	ExtremeXOS 12.0.2.18
Microsoft Windows	2003 Server Enterprise Edition
Active Directory Users and Computers	5.2.3790.1830
Internet Authentication Service	5.2.3790.1830
DHCP Server	5.2.3790.1830

4. Configure Extreme Networks Equipment

This section describes the configuration for the Extreme Network X150-24t and X150-48t Switches as shown in **Figure 1**. The configuration shown in this section assumes both X150s are in their factory default configuration.

4.1. Configure the Extreme Networks Summit X150-24t Switch

This section shows the necessary steps in configuring the X150-24t as shown in **Figure 1.**. Connect a PC to the console port of the switch using a null modem serial cable and log in to the switch using the appropriate user ID and password.

```
#
#-------- Remove default VLAN from all ports --------------#
#
configure vlan Default delete ports all
#
#-------- Create VLAN for voice traffic and ---------------#
#-------- assigned IP address and port to VLAN ------------#
#
create vlan "voice"
configure vlan voice tag 10
configure vlan voice ipaddress 172.28.10.21 255.255.255.0
configure vlan voice add ports 2-3,25 tagged
#
#-------- Create VLAN for data traffic and ----------------#
#-------- assigned IP address and port to VLAN ------------#
#
create vlan "data"
```

```
configure vlan data tag 11
configure vlan data ipaddress 172.28.11.21 255.255.255.0
configure vlan data add ports 2-3,25 tagged
#
#-------- Enable and Configure Spanning Tree Protocol -----#
#
configure vlan Default add ports 2-3,25 untagged
enable stpd s0 auto-bind vlan Default
configure stpd s0 add vlan voice port 2-3
configure stpd s0 add vlan data port 2-3
enable stpd s0
#
#-------- Configure RADIUS authentication -----------------#
#
configure radius netlogin primary server 172.28.10.12 1812 client-ip
    172.28.11.21 vr VR-Default
configure radius netlogin primary shared-secret 1234567890
enable radius netlogin
create vlan "temp"
configure netlogin vlan temp
enable netlogin dot1x
enable netlogin ports 13 dot1x
#
#-------- Configure Link Layer Discovery Protocol ---------#
#--- to assign VLAN, Call Server and File Servers' information ---#
#
enable lldp ports 13
configure lldp port 13 advertise vendor-specific dot1 vlan-name
configure lldp port 13 advertise vendor-specific avaya-extreme call-server
    172.28.10.7
configure lldp port 13 advertise vendor-specific avaya-extreme file-server
    172.28.10.12
configure lldp port 13 advertise vendor-specific avaya-extreme dot1q-framing
    tagged
#
#-------- Configure Quality of Service  -------------------#
#-------- dot1p and code-point value must match -----------#
#-------- setting in Avaya Communication Manager ----------#
#
create qosprofile "QP7"
configure dot1p type 6 qosprofile QP7
configure diffserv examination code-point 46 qosprofile QP7
configure qosscheduler strict-priority
#
```

4.2. Configure the Extreme Networks Summit X150-48t Switch

This section shows the necessary steps in configuring the X150-48t as shown in **Figure 1**. Connect a PC to the console port of the switch using a null modem serial cable and log in to the switch using the appropriate user ID and password.

```
#
#-------- Remove default VLAN from all ports -------------#
#
```

```
configure vlan Default delete ports all
#
#-------- Create VLAN for voice traffic and ---------------#
#-------- assigned IP address and port to VLAN ------------#
#
create vlan "voice"
configure vlan voice tag 10
configure vlan voice ipaddress 172.28.10.22 255.255.255.0
configure vlan voice add ports 1-2 tagged
#
#-------- Create VLAN for data traffic and ----------------#
#-------- assigned IP address and port to VLAN ------------#
#
create vlan "data"
configure vlan data tag 11
configure vlan data ipaddress 172.28.11.22 255.255.255.0
configure vlan data add ports 1-2 tagged
#
#-------- Enable and Configure Spanning Tree Protocol -----#
#
configure vlan Default add ports 1-2 untagged
enable stpd s0 auto-bind vlan Default
configure stpd s0 add vlan voice port 1-2
configure stpd s0 add vlan data port 1-2
enable stpd s0
#
#-------- Configure RADIUS authentication -----------------#
#
configure radius netlogin primary server 172.28.10.12 1812 client-ip
    172.28.11.22 vr VR-Default
configure radius netlogin primary shared-secret 1234567890
enable radius netlogin
create vlan "temp"
configure netlogin vlan temp
enable netlogin dot1x
enable netlogin ports 13 dot1x
#
#-------- Configure Link Layer Discovery Protocol ---------#
#------- to assign VLAN, Call Server and File Servers' information ---#
#
enable lldp ports 13
configure lldp port 13 advertise vendor-specific dot1 vlan-name
configure lldp port 13 advertise vendor-specific avaya-extreme call-server
    172.28.10.7
configure lldp port 13 advertise vendor-specific avaya-extreme file-server
    172.28.10.12
configure lldp port 13 advertise vendor-specific avaya-extreme dot1q-framing
    tagged
#
#-------- Configure Quality of Service  -------------------#
#-------- dot1p and code-point value must match -----------#
#-------- setting in Avaya Communication Manager ----------#
#
create qosprofile "QP7"
configure dot1p type 6 qosprofile QP7
configure diffserv examination code-point 46 qosprofile QP7
```

```
configure qosscheduler strict-priority
#
```

5. Configure the Avaya C363T-PWR Converged Stackable Switch

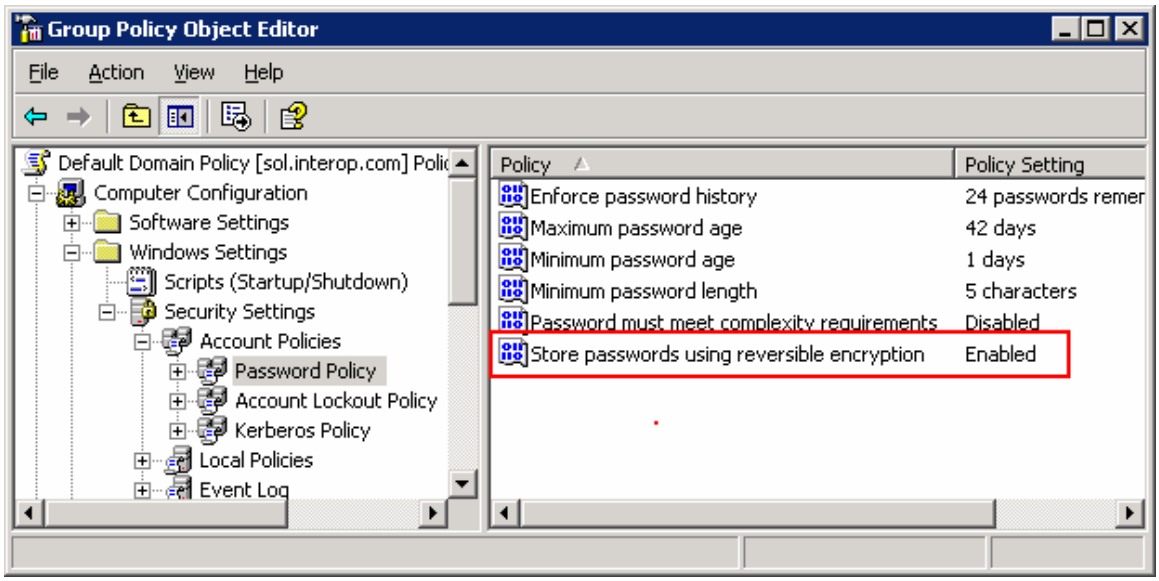
This section shows the steps for configuring the Avaya C363T-PWR Converged Stackable Switch.

```
set vlan 10 name voice
set vlan 11 name data
set trunk 1/1-2,13 dot1q
set port vlan-binding-mode 1/1-2,13 bind-to-configured
set port vlan 11 1/13
```

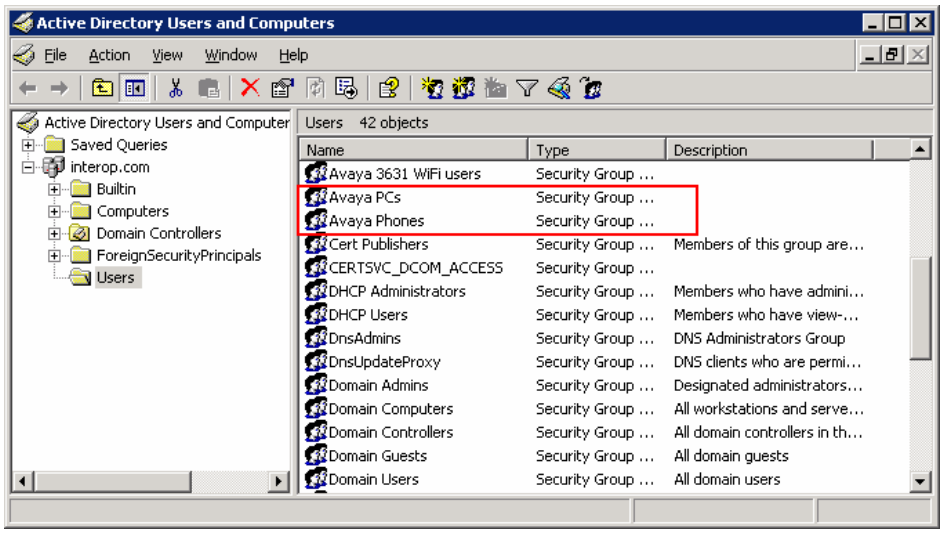
6. Configure Microsoft Active Directory Service

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

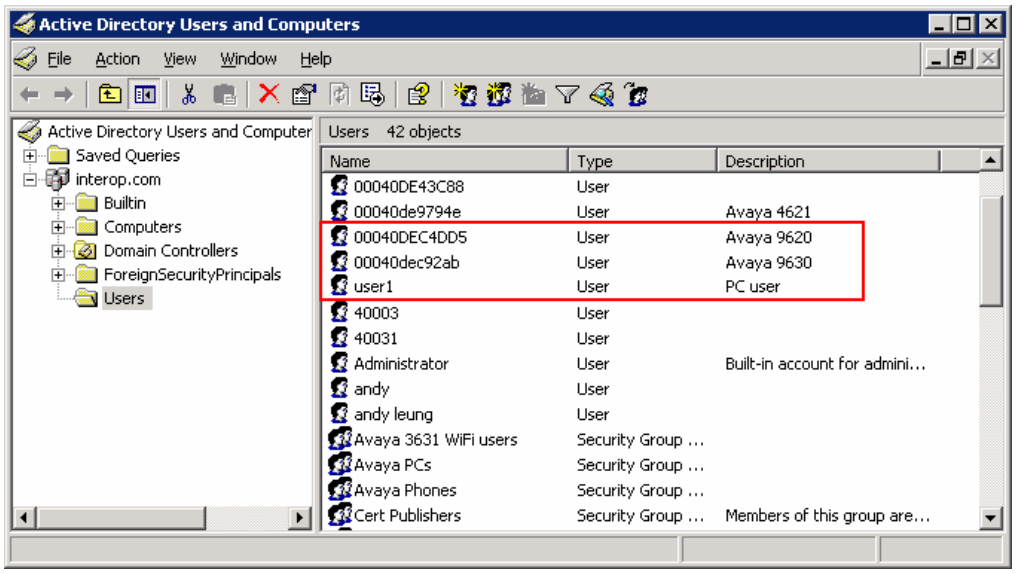
1. Configure the Password Policy for the Active Directory Server so that reversible encryption is enabled as shown the screen capture below. The Group Policy Object Editor can be accessed by right-clicking the Active Directory domain then selecting properties, and then select the Default Domain Policy under the Group Policy tab.



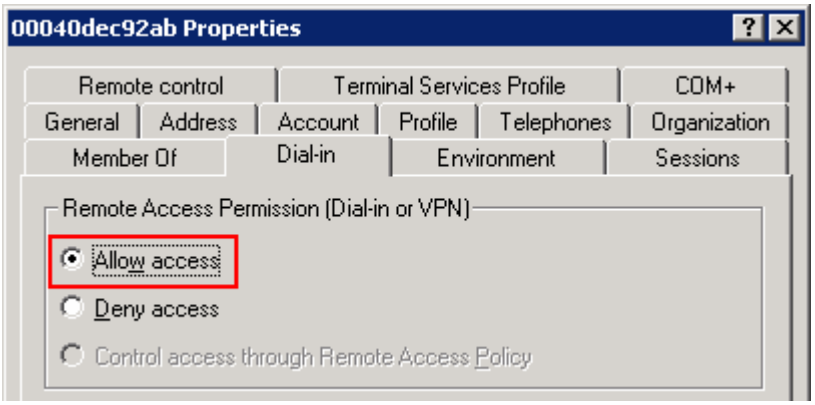
2. Create Windows user groups for the Avaya IP telephones and PC users to facilitate administration by right-clicking on **Users → New → Group**. The sample configuration uses the name **Avaya PCs** for PC users and **Avaya Phones** for Avaya IP telephones. To access the **Active Directory Users and Computers** window select **Start→ Programs → Administrative Tools → Active Directory Users and Computers**.



3. Create a "User logon name" for Avaya IP telephones and the PCs in the Active Directory by right-clicking on **Users → New → User**. By default, Avaya IP telephones use the Media Access Control (MAC) address as the "User logon name". Assign each user as the member of the appropriate Windows user groups created in **Step 2**.



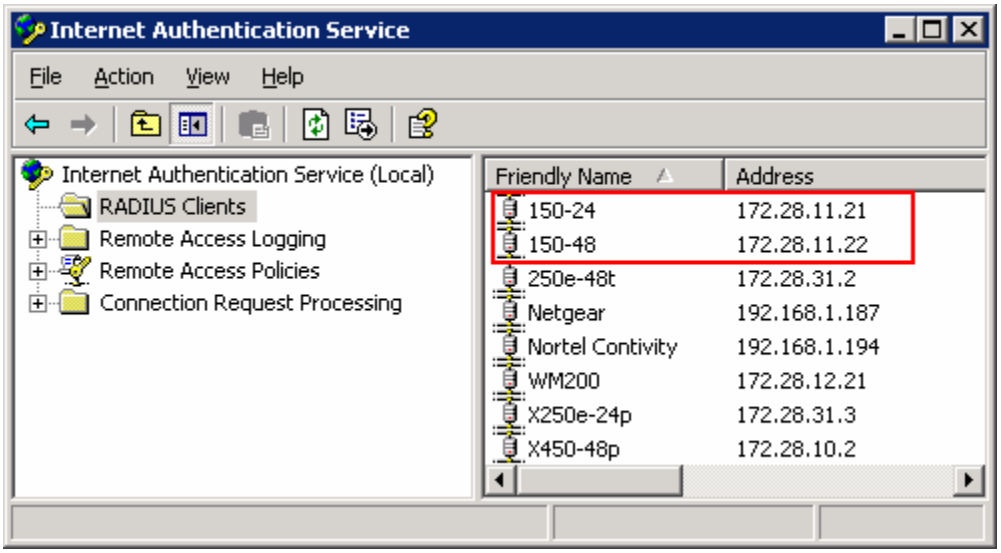
4. For each user ID defined, **Remote Access Permission (Dial-in or VPN)** must be set to **Allow access** on the **Dial-in** tab. Double-click on the desired user name to bring up the user properties windows shown below.



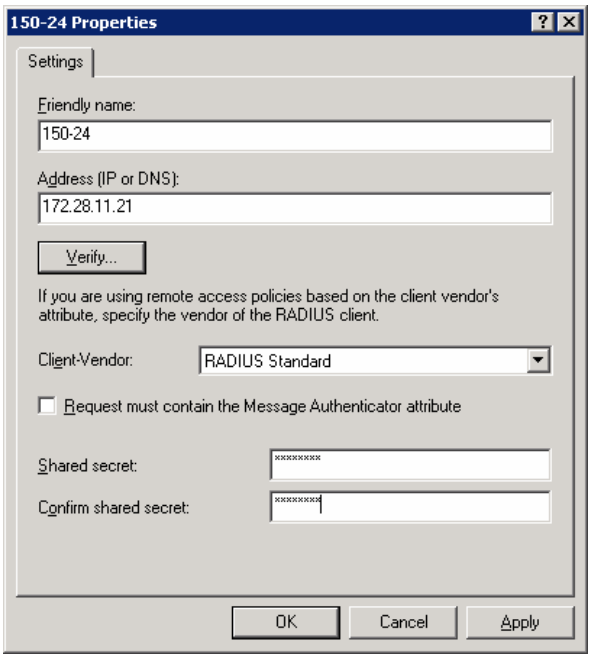
7. Configure Microsoft Internet Authentication Services (IAS) Server

This section shows the steps for configuring the IAS server to support 802.1X authentication for an Avaya IP Telephone and a PC. Open the Internet Authentication Service windows by selecting **Start → Programs → Administrative Tools → Internet Authentication Service**.

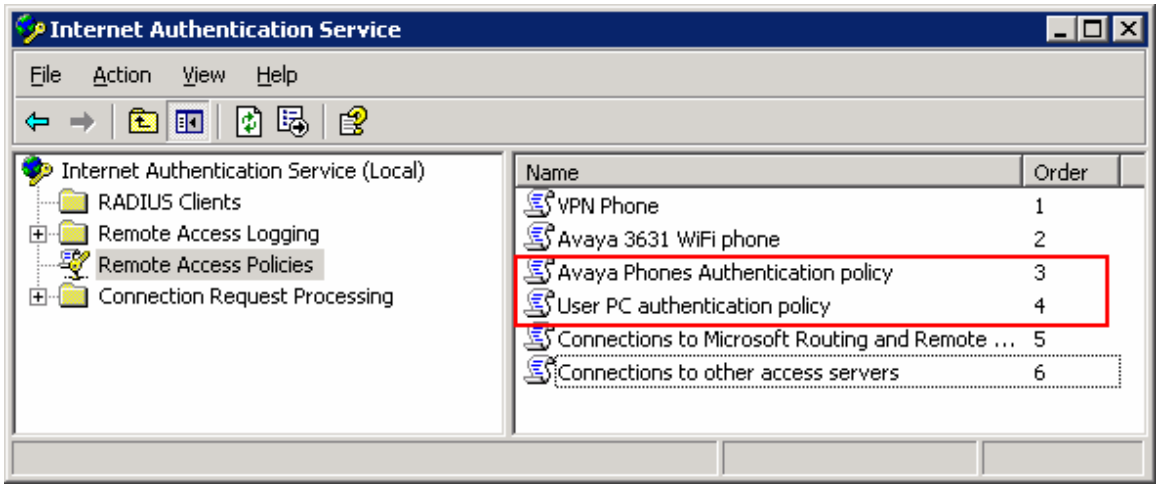
1. Define the Summit X150s switch as a RADIUS client in IAS by right-clicking RADIUS Clients.



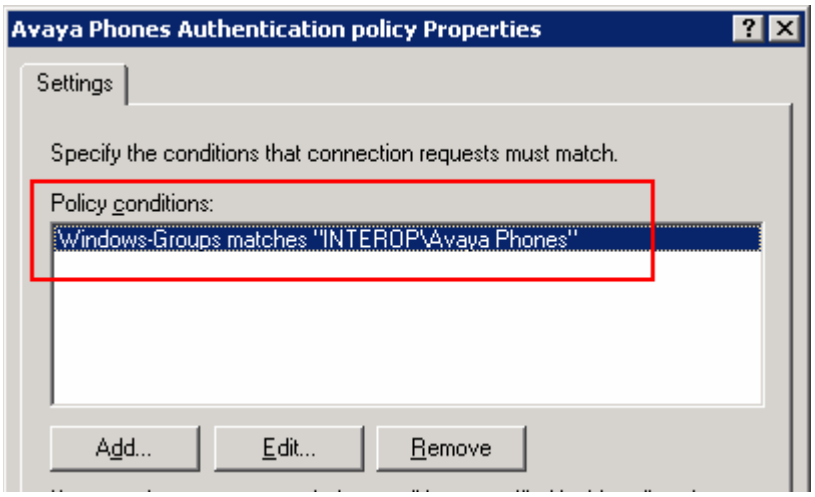
The Shared secret entered when defining the RADIUS client must match the shared-secret configured on the X150s in **Section 4**.



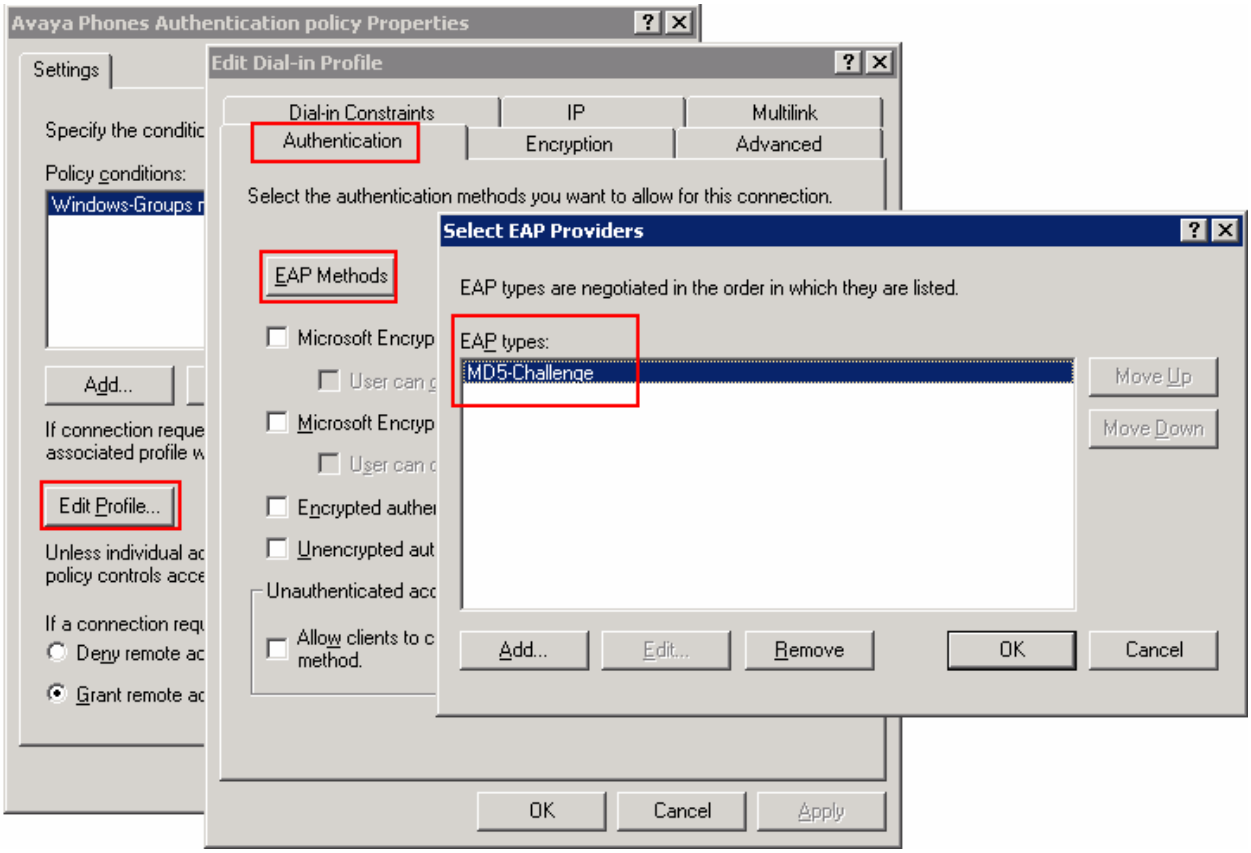
2. Create Remote Access Policies for the Avaya IP telephones and for the PC users by right-clicking on **Remote Access Policies → New Remote Access Policy.** The sample network defined the policy **Avaya Phones Authentication policy** for Avaya IP telephones, and the policy **User PC authentication policy** for PC users.



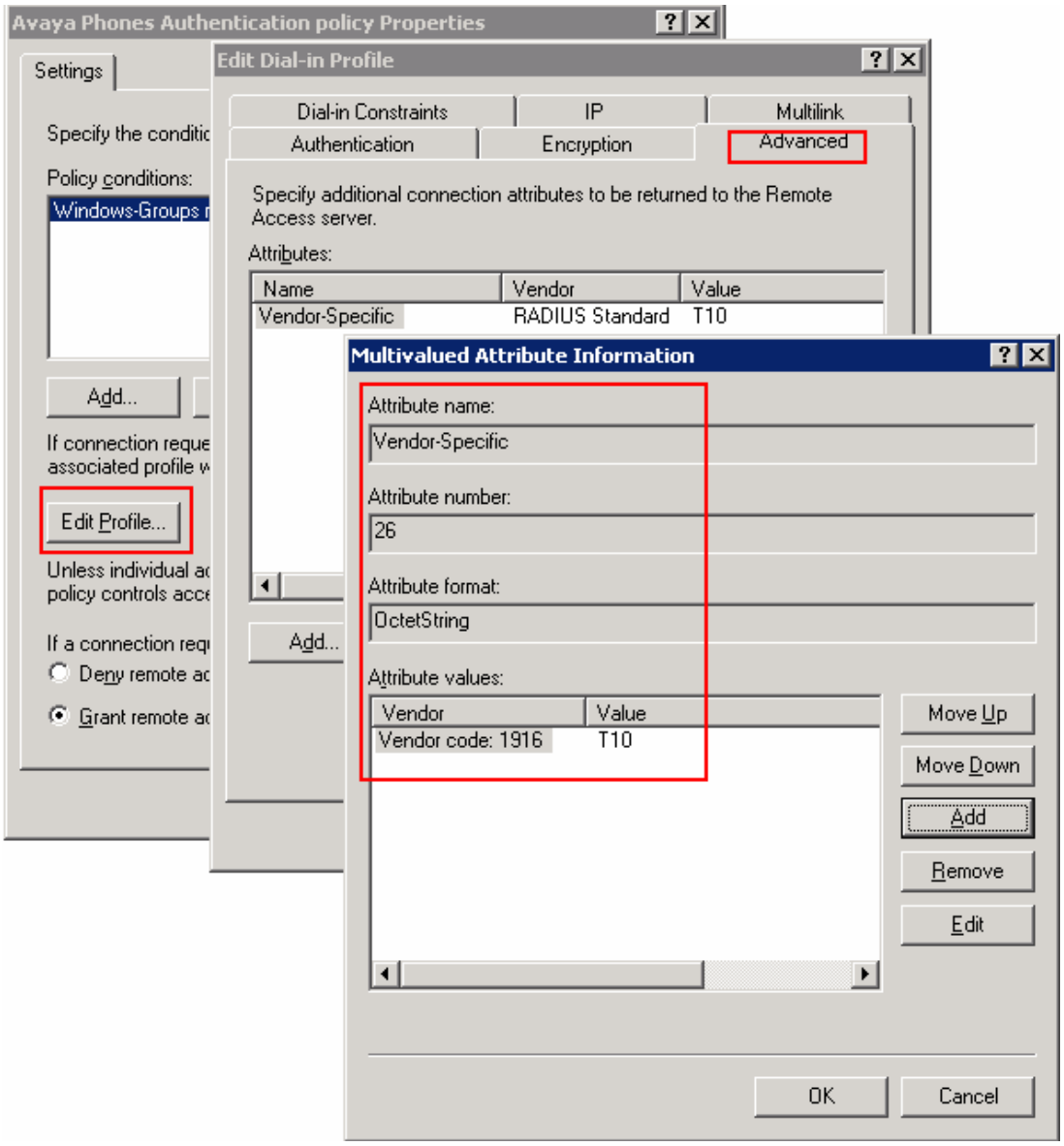
3. The **Avaya Phones Authentication policy** is defined for Windows user group **Avaya Phones** of the INTEROP domain defined in **Section 6**, **Step 2**.



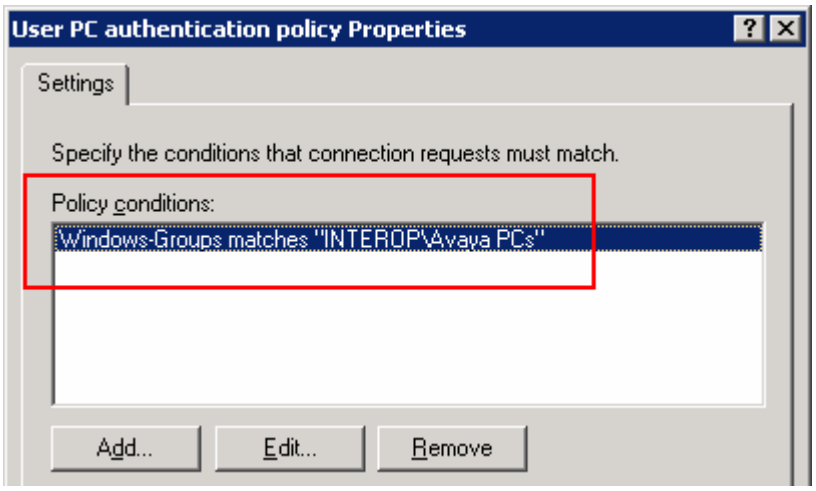
4. The **Avaya Phones Authentication policy** is configured so that an **EAP type** of **MD5-Challenge** is used for authentication.



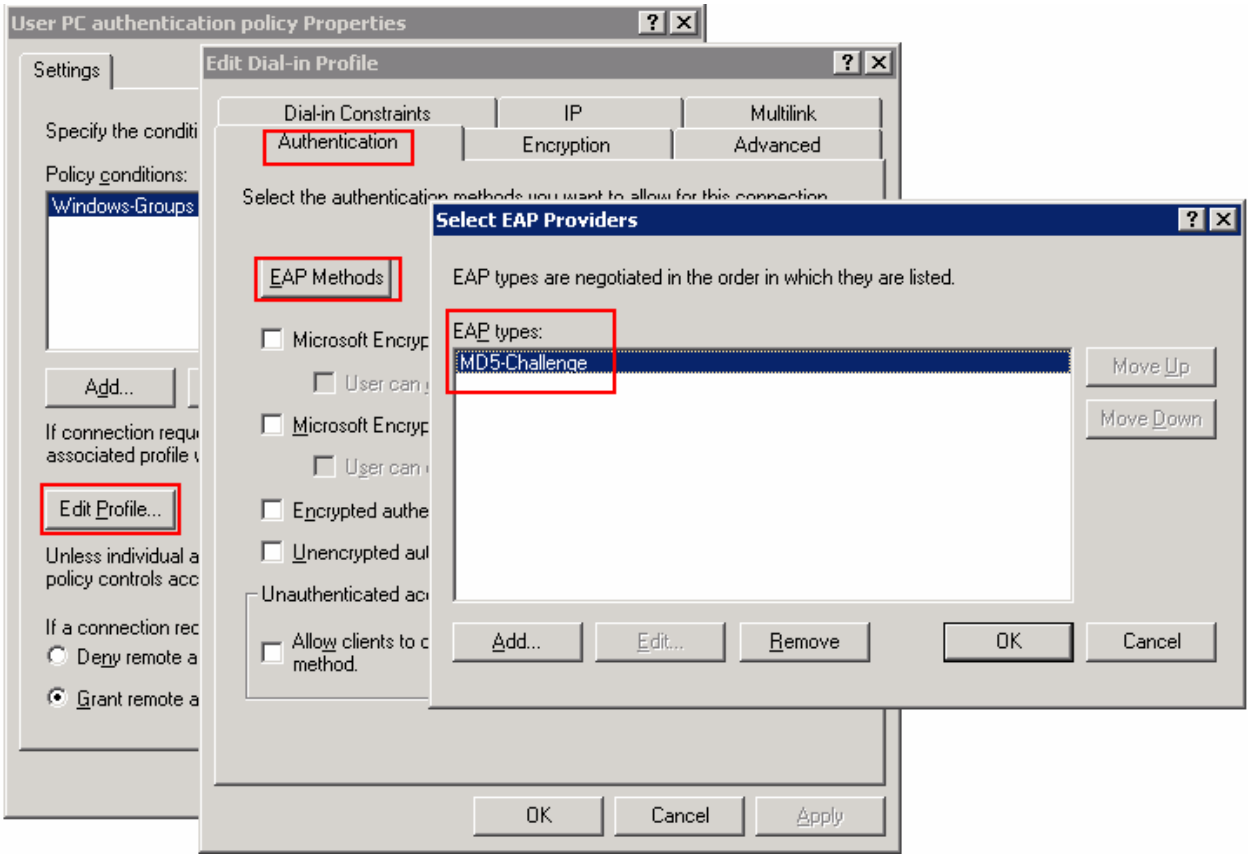
5. The **Avaya Phones Authentication Policy** is set with an attribute of **T10** for **Vendor code 1916**. The value **T10** correspond with the voice VLAN defined in the X150s. The **T** signifies that the switch port should be set as **Tagged**, and the number **10** is the VLAN tag used for the voice VLAN. Alternatively, the value **Tvoice** can also be used in place of **T10**.



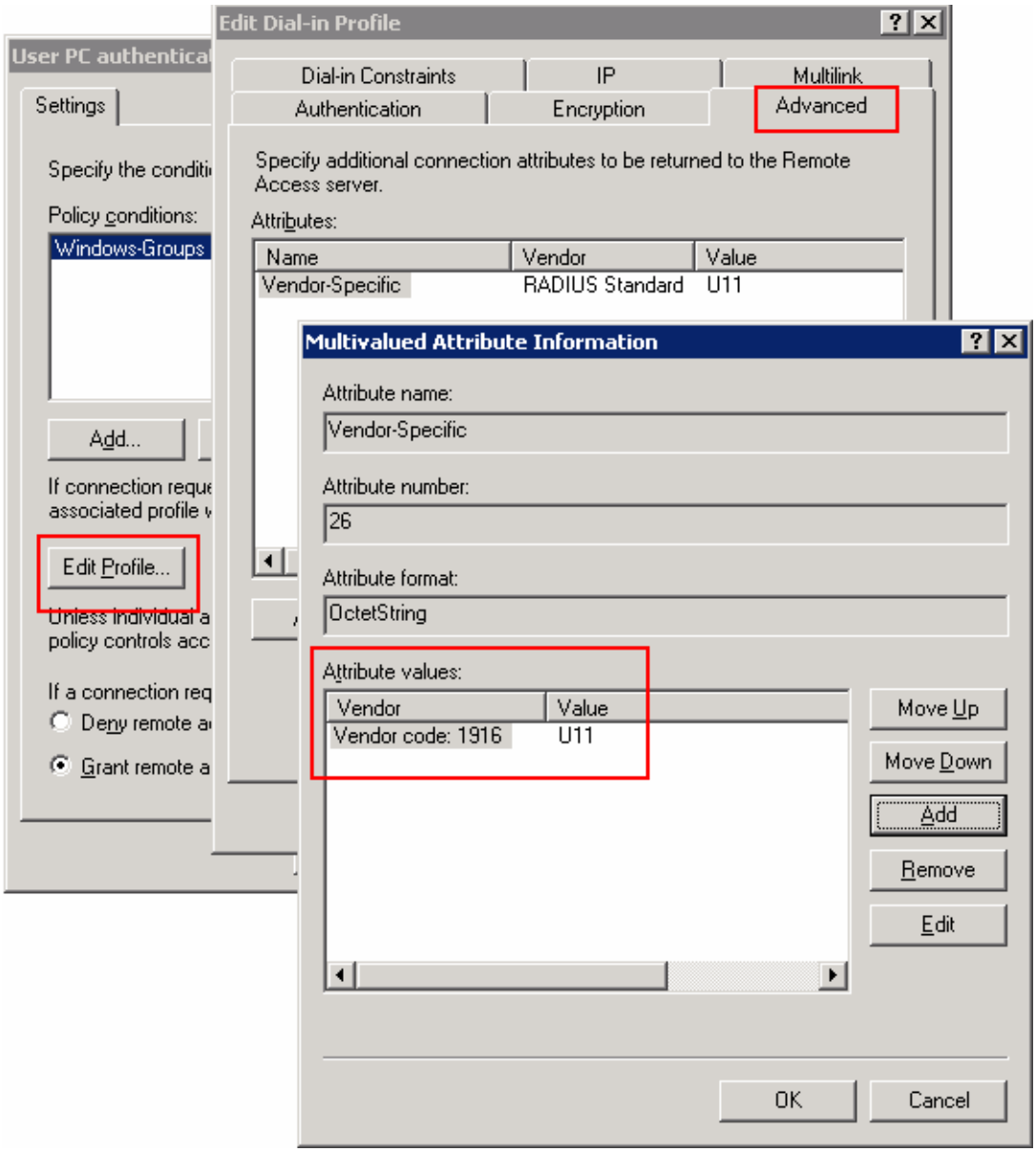
6. The **User PC authentication policy** is defined for Windows user group **Avaya PCs** defined in **Section 6**, **Step 2** for the INTEROP domain.



7. The **User PC authentication policy** is configured so that an **EAP type** of **MD5-Challenge** is used for authentication.



8. The **User PC authentication Policy** is set with an attribute of **U11** for **Vendor code 1916**. The value **U11** corresponds with the data VLAN defined in the X150s. The **U** signifies that the switch port should be set as **Untagged**, and the number **11** is the VLAN tag used for the **data** VLAN. Alternatively, the value **Udata** can also be used in place of **U11**.



8. Configure the Avaya 9600 Series IP Telephones

This section shows the steps for configuring the Avaya 9600 Series IP Telephones connected into the X150s.

Avaya 9600 Series IP Telephones support three 802.1X operational modes. The operational mode can be changed by pressing“mute27237#” (mute craft) on the Avaya 9600Series 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 form the IP telephone, the phone will send an Extensible Authentication Protocol over LAN (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 X150s receive the logoff message, the PC will be removed from the authorized MAC list.

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. The following screens are from the System Access Terminal (SAT). Log in with the appropriate credentials.

1. Add a new station for the Avaya IP Telephones to Avaya Communication Manager using the **add station** command. Configure the following bolded fields.

```
add station 11010                                          Page   1 of   4
                                    STATION

Extension: 11010                        Lock Messages? n
     Type: 9610                         Security Code: 123456          TN: 1
     Port: ip                         Coverage Path 1:                 COR: 1
     Name: Ext-11010                  Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 11010
          Speakerphone: none
       Display Language: english
 Survivable GK Node Name:
         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? n
```

2. Use the "display ip-network-region" command to display the 802.1P setting configured in the Avaya Communication Manager. Verify that both **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**. and that **Call Control PHB Value** and **Audio PHB Value** are set to **46**. The **DIFFSERV/TOS PARAMETERS** and **802.1P/Q PARAMETERS** must match the dot1p and diffserv values entered in **Section 4**.

```
display ip-network-region 1                                  Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location: 1       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? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

10. Interoperability Compliance Testing

The Interoperability compliance testing focused on assessing the ability of the X150s in supporting Avaya Communication Manager, the Avaya G650 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 of the testing were to verify that the X150-24t and X150-48t support the following:

- 802.1X multiple supplicant support
- Interoperability of basic 802.1D spanning tree
- Layer-2, and Layer-3 based Quality of Service prioritization
- Basic calling performed by Avaya IP Telephones (e.g., place/receive call, transfer, DTMF pass-through)
- Link Layer Discovery Protocol (LLDP) for receiving Avaya 9600 Series IP Telephones advertised information
- Link Layer Discovery Protocol (LLDP) for provisioning of Avaya 9600 Series IP Telephones

10.2. Test Results

The Extreme Networks Summit X150-48t and X150-24t Switches achieved the above objectives. Quality of Service for VoIP traffic was maintained throughout testing in the presence of competing simulated traffic. 802.1D spanning tree correctly converged when the active link was disconnected or when bridging priority was changed. LLDP also correctly reported the attributes of Avaya 9600 Series IP Telephones and advertised Call Server, File Server, and VLAN information.

11. Verification Steps

The following steps may be used to verify the configuration:

- Use the "show port <port #> qosmonitor" command on the Summit X150 switches to verify VoIP traffic is being transmitted by the correct priority queue. For the sample configuration, VoIP traffic should be in QP7 and all other traffic should be in QP1.

```
X150-48t.1 # show port 1 qosmonitor
Qos Monitor Req Summary                                  Wed Oct 17 01:59:20 2007
Port      QP1       QP2       QP3       QP4       QP5       QP6       QP7       QP8
          Pkt       Pkt       Pkt       Pkt       Pkt       Pkt       Pkt       Pkt
          Xmts      Xmts      Xmts      Xmts      Xmts      Xmts      Xmts      Xmts
================================================================================
1         1022650   0         0         0         0         0         669694    57
```

- Use the “show stpd <stpd domain>” command on the Summit X150 switches to verify the operation of the Spanning Tree Protocol (STP). Verify that STP is enabled and that Operational Mode is 802.1D. Verify that the voice and data VLANs are listed as Participating Vlans.

```
* X150-24t.17 # show stpd s0
Stpd: s0                Stp: ENABLED            Number of Ports: 4
Rapid Root Failover: Disabled
Operational Mode: 802.1D                        Default Binding Mode: 802.1D
802.1Q Tag: (none)
Ports: 1,2,3,25
Participating Vlans: data,Default,voice
Auto-bind Vlans: Default
Bridge Priority: 32768
BridgeID:               80:00:00:04:96:27:a7:5b
Designated root:        80:00:00:04:0d:3c:32: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: TRUE
Number of Topology Changes: 26
Time Since Last Topology Change: 12s
```

- Use the “show radius” command on the X150-48t and X150-24t to verify that **IP address** and **Client address** are correct. A successful log in by an 802.1X client shows 2 **Access Requests**, 1 **Access Accepts**, and 1 **Access Challenges** in the counter.

```
X150-24t.12 # show radius
Switch Management Radius: disabled
Switch Management Radius server connect time out: 3 seconds
Switch Management Radius Accounting: disabled
Switch Management Radius Accounting server connect time out: 3 seconds
Netlogin Radius: enabled
Netlogin Radius server connect time out: 3 seconds
Netlogin Radius Accounting: disabled
Netlogin Radius Accounting server connect time out: 3 seconds

Primary Netlogin Radius server:
    Server name   :
    IP address    :  172.28.10.12
    Server IP Port:  1812
    Client address:  172.28.11.21 (VR-Default)
    Shared secret :  3>:>?75<;5
Access Requests   :  2              Access Accepts    :  1
Access Rejects    :  0              Access Challenges :  1
Access Retransmits:  0              Client timeouts   :  0
Bad authenticators:  0              Unknown types     :  0
Round Trip Time   :  0
```

- Use the “show netlogin” command on the X150-48t and X150-24t to verify if 802.1X is enabled and if a PC or Avaya IP Telephone has successfully been authenticated. The output also shows which VLAN the client is authenticated onto. Note that an Avaya IP Telephone (MAC address 00:04:0d:ec:92:ab) is only authenticated in the voice VLAN even though its MAC address is displayed in the data VLAN. The MAC address of

00:a0:c9:cf:ba:4c belongs to the PC that is connected onto the network through the Avaya IP Telephone, and is only authenticated for the data VLAN.

```
Port: 13,  Vlan: data,  State: Enabled,  Authentication: 802.1x,  Guest Vlan <Not
Configured>: Disabled

MAC               IP address   Authenticated  Type    ReAuth-Timer   User
00:04:0d:ec:92:ab  0.0.0.0      No                     0        00040DEC92AB
00:a0:c9:cf:6a:4c  0.0.0.0      Yes, Radius    802.1x  3596           user1
-----------------------------------------------

Port: 13,  Vlan: voice,  State: Enabled,  Authentication: 802.1x,  Guest Vlan <Not
Configured>: Disabled

MAC               IP address   Authenticated  Type    ReAuth-Timer   User
00:04:0d:ec:92:ab  172.28.10.51 Yes, Radius    802.1x  3441     00040DEC92AB
```

- Use the "show lldp neighbors detail" command on the X150s to show LLDP information.

```
* X150-24t.18 # show lldp neighbors detail

--------------------------------------------------------------------------------
LLDP Port 13 detected 1 neighbor
  Neighbor: (5.1)172.28.10.51/00:04:0D:EC:92:AB, age 21 seconds
    - Chassis ID type: Network address (5); Address type: IPv4 (1)
      Chassis ID     : 172.28.10.51
    - Port ID type: MAC address (3)
      Port ID     : 00:04:0D:EC:92:AB
    - Time To Live: 120 seconds
    - System Name: "AVAEC92AB"
    - System Capabilities : "Bridge, Telephone"
      Enabled Capabilities: "Bridge"
    - Management Address Subtype: IPv4 (1)
      Management Address        : 172.28.10.51
      Interface Number Subtype  : System Port Number (3)
      Interface Number          : 1
      Object ID String          : "1.3.6.1.4.1.6889.1.69.2.2"
    - 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           : 10
      L2 Priority       : 6
      DSCP Value        : 46
    - MED Hardware Revision: "9630D01A"
    - MED Firmware Revision: "hb96xxua1_50.bin"
    - MED Software Revision: "ha96xxua1_50.bin"
    - MED Serial Number: "06N534779862"
    - MED Manufacturer Name: "Avaya"
    - MED Model Name: "9630"
    - Avaya/Extreme Conservation Level Support
      Current Conservation Level: 0
      Typical Power Value       : 0.0 Watts
      Maximum Power Value       : 0.0 Watts
      Conservation Power Level  : 1=0.0W
```

```
    - Avaya/Extreme Call Server(s): 172.28.10.7
    - Avaya/Extreme IP Phone Address: 172.28.10.51 255.255.255.0
      Default Gateway Address       : 172.28.10.1
    - Avaya/Extreme CNA Server: 0.0.0.0
    - Avaya/Extreme File Server(s): 172.28.10.12
    - Avaya/Extreme IEEE 802.1q Framing: Tagged
```

- Use the "show dot1p" command on the X150-48t and X150-24t switches to verify the 802.1P to QoS Profile is assigned correctly.

```
* X150-24t.19 # 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 differv examination" command on the X150-24t and X150-48t switches to verify the diffserv to QoS Profile is assigned correctly.

```
* X150-24t.120 # show diffserv examination
CodePoint->QOSProfile mapping:
        00->QP1 01->QP1 02->QP1 03->QP1 04->QP1 05->QP1 06->QP1 07->QP1
        08->QP1 09->QP1 10->QP1 11->QP1 12->QP1 13->QP1 14->QP1 15->QP1
        16->QP1 17->QP1 18->QP1 19->QP1 20->QP1 21->QP1 22->QP1 23->QP1
        24->QP1 25->QP1 26->QP1 27->QP1 28->QP1 29->QP1 30->QP1 31->QP1
        32->QP1 33->QP1 34->QP1 35->QP1 36->QP1 37->QP1 38->QP1 39->QP1
        40->QP1 41->QP1 42->QP1 43->QP1 44->QP1 45->QP1 46*>QP7 47->QP1
        48->QP1 49->QP1 50->QP1 51->QP1 52->QP1 53->QP1 54->QP1 55->QP1
        56->QP8 57->QP8 58->QP8 59->QP8 60->QP8 61->QP8 62->QP8 63->QP8
```

- Use the "show trunk" command on the Avaya C363T-PWR Converged Stackable Switch to verify trunk settings.

```
C360-1(super)# set trunk

Port   Mode  Binding mode              Native vlan
------ ----- ------------------------ -----------
 1/1   dot1q bound to configured vlans     1
 1/2   dot1q bound to configured vlans     1
 1/3   off   statically bound              1
 1/4   off   statically bound              1
 1/5   off   statically bound              1
 1/6   off   statically bound              1
```

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 X150-48t and X150-24t Switches to support the Avaya VoIP solution depicted in **Figure 1** which is composed of an Avaya S8500 Server, Avaya G650 Media Gateway, and Avaya 9600 Series 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 3.1, February 2007
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 3, February 2007
[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 12, February 2007
[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

[1] *ExtremeXOS Concepts Guide, Software Version 12.0*, Part number 100262-00 Rev. 02, July 2007
[2] *ExtremeXOS Command Reference Guide, Software Version 12.0*, Part number 100261-00 Rev. 02, 2007, July 2007

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