Avaya Solution & Interoperability Test Lab

Configuring Cisco 802.1x Multi-domain Authentication (MDA) on a Cisco Catalyst 3750, with Avaya 96xx and 46xx Series IP Telephones - Issue 1.0

Abstract

These Application Notes describe the configuration of Cisco 802.1x Multi-domain Authentication (MDA) on a Cisco Catalyst 3750, with Avaya 9620, 9630, 4621SW, and 4610SW IP Telephones. 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. Cisco supports an 802.1x configuration called multi-domain authentication (MDA) on Catalyst 3750 switches. In this type of port configuration, the IP telephone and a PC attached to the phone are authenticated separately.

1. Introduction

These Application Notes describe the configuration of Cisco 802.1x Multi-domain Authentication (MDA) implementation on a Cisco Catalyst 3750, with Avaya 96xx and 46xx series IP Telephones. 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. Cisco supports an 802.1x configuration called multi-domain authentication (MDA) on Catalyst 3750 switches. In this type of port configuration, the IP telephone and a PC attached to the phone are authenticated separately. In the reference configuration, Avaya 46xx and 96xx series IP telephones were tested with the Catalyst 3750 in a multi-domain configuration.

802.1x is comprised of three primary components. Each is referred to as a Port Access Entity (PAE).

- ***Supplicant*** – Client device requesting network access (e.g. IP phones and attached PCs).
- ***Authenticator*** – Network device that facilitates the Supplicant authorization requests (e.g. Cisco Catalyst 3750).
- ***Authentication Server*** – A Remote Authentication Dial-in User Server (RADIUS) which provides the authentication service (e.g. FreeRadius).

The 802.1x protocol utilizes Extensible Authentication Protocol (EAP) messages. This use of EAP by 802.1x is called EAP Over LANs (EAPOL). The typical 802.1x protocol sequence is as follows:

1. The supplicant sends an “EAPOL Start” message to the Authenticator.
2. The Authenticator responds with an “EAP-Request/Identity” message to the Supplicant.
3. The Supplicant responds with an “EAP-Response/Identity” message to the Authenticator.
4. The Authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the Authentication Server.
5. The Authentication Server recognizes the packet as an EAP-MD5 type and sends back a challenge message to the Authenticator.
6. The Authenticator removes the Authentication Server’s frame header, encapsulates the remaining EAP frame into the EAPOL format, and then sends it to the Supplicant.
7. The Supplicant responds to the challenge and the Authenticator passes the response onto the Authentication Server.
8. If the Supplicant provides proper identity, the Authentication Server responds with a success message. The Authenticator passes the message onto the Supplicant and allows access to the LAN.

For additional information on the 802.1x protocol, see [1] and [2].

In a multi-domain configuration the IP telephone and the attached PC must independently request access to the network by specifying a username and password. Therefore these authentication entries for each Supplicant device must be provisioned in the RADIUS server (see **Section 6**).

The Avaya 46xx and 96xx series IP telephones support 802.1x. These phones use their MAC addresses as their username by default. There is no default password.

The Avaya 46xx and 96xx IP telephones support three 802.1x modes for attached PCs.

- ***Pass-Thru*** – The phone passes the PC 802.1x authentication through to the Authenticator. If the PC is disconnected, no disconnect notification is sent to the Authenticator.
- ***Pass-Thru with Logoff*** - The phone passes the PC 802.1x authentication information through to the Authenticator. If the PC is disconnected, an 802.1x logoff message is sent to the Authenticator.
- ***Supplicant*** – The phone does not pass any authentication information from the attached PC. **This mode should not be used in a multi-domain configuration.**

The Authenticator device may require information from the RADIUS called attributes. Attributes specify additional authorization information such as whether access to a particular VLAN is allowed for a Supplicant. These attributes can be vendor specific.

Cisco uses a RADIUS attribute called "***Cisco AVPair***". In this reference configuration, a Cisco AVPair is used by the RADIUS to tell the Cisco Catalyst 3750 that a Supplicant (IP telephone) is allowed on the voice VLAN (see **Section 6**).

2. Reference Configuration

These application notes used the reference configuration shown in **Figure 1**.

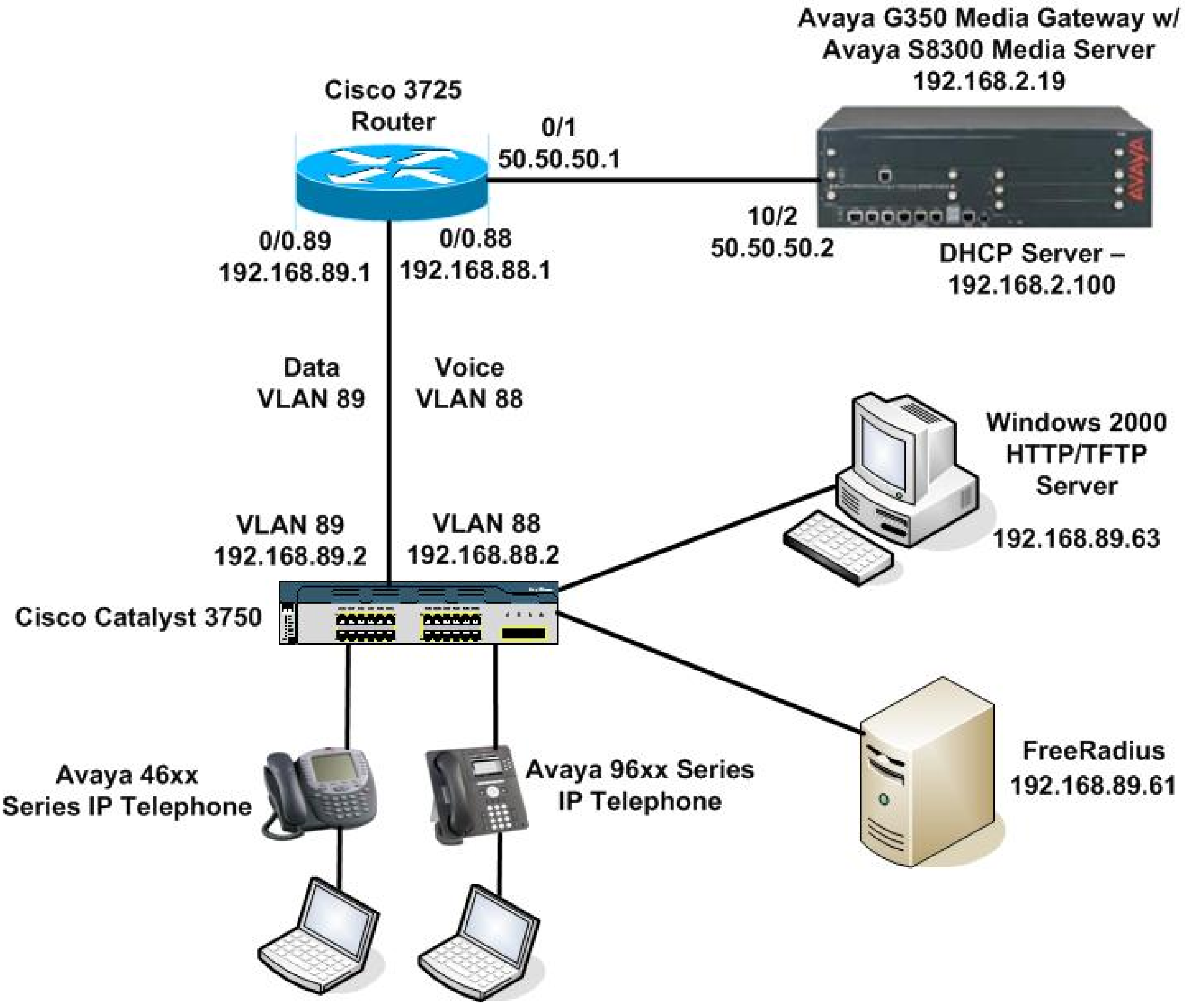


Figure 1 – Reference Configuration

Avaya Communication Manager runs on the S8300 Media Server (ICC) installed in the Avaya G350 Media Gateway.

The G350 Media Gateway is provisioned as the network Dynamic Host Configuration Protocol (DHCP) server (see **Section 4**). The Avaya IP telephones authenticate via the Cisco Catalyst 3750 and the FreeRadius server (see **Sections 5**, **6**, and **7**).

The Avaya IP telephones are first assigned data VLAN IP addresses, instructed to switch to the voice VLAN, and then assigned voice IP addresses by the DHCP server. The DHCP server also directs the Avaya IP telephones to the IP address of Avaya Communication Manager for registration.

When the PCs are connected to the back of the Avaya IP telephones, they prompt for an 802.1x username and password which are sent to the FreeRadius. If this authentication passes, the Cisco Catalyst 3750 allows the PCs to access the data VLAN.

3. Equipment and Software Validated

The following equipment and software were used to test the sample configuration.

Network Component	Software Version
Avaya S8300 Media Server	Avaya Communication Manager 4.0 (Load 727)
Avaya 4610 SW IP Telephone	2.7 H.323 (112706)
Avaya 4621 SW IP Telephone	2.7 H.323 (112706)
Avaya 9620 IP Telephone	1.2 H.323 (010807)
Avaya 9630 IP Telephone	1.2 H.323 (010807)
Avaya G350 Media Gateway (DHCP Server)	26.27.0
Avaya TFTPServer 2000	3.6.1
Cisco Catalyst 3750-24PS	c3750-ipservicesk9-mz.122-35.SE.bin
Cisco 3725 Router	c3725-ipvoicek9-mz.124-12.bin
Microsoft Windows XP with 802.1x Authentication	Windows XP Professional 2002, SP2
Microsoft Windows 2000 Server (HTTP Server)	Service Pack 4
Red Hat Enterprise ES FreeRADIUS Server	R4 1.1.1

Table 1: Test Equipment List

4. Configure DHCP on Avaya G350

In this reference configuration the Avaya G350 was used as the DHCP server. After the Avaya IP telephones are authenticated, they initiate a DCHP discovery/request. The Avaya 46xx IP telephones use DHCP option 176. The Avaya 96xx IP telephones use DHCP option 242. The DHCP sequence proceeds as shown in **Figure 2**. For additional information on Avaya DHCP implementation, see [1] and [2].

	Sends	
Phone	**DHCP Discover** (data) →	
	← **DHCP Offer** (data IP address + data option 176 or 242)	**DHCP Server**
Phone	**DHCP Request** (data IP address from Offer) →	
	← **DHCP Ack** (data IP address + data option 176 or 242)	**DHCP Server**
Phone	**DHCP Release** (the phone will now switch to the voice VLAN) →	
Phone	**DHCP Discover** (voice) →	
	← **DHCP Offer** (voice IP address + voice option 176 or 242)	**DHCP Server**
Phone	**DHCP Request** (voice IP address from Offer) →	
	← **DHCP Ack** (voice IP address + voice option 176 or 242)	**DHCP Server**

Figure 2 – Avaya IP Telephone DHCP Sequence

Table 2 shows the DHCP parameters used in the reference configuration.

DHCP Scope	**Option 3 Router**	**Option 176 46xx Phone**	**Option 242 96xx Phone**
Data Addresses – 192.168.89.100-150	192.168.89.1	L2Q=1,L2QVLAN=88	L2Q=1,L2QVLAN=88
Voice Addresses – 192.168.88.100-150	192.168.88.1	MCIPADD=192.168.2.19, MCPORT=1719,TFTPSRVR= 192.168.89.63	MCIPADD=192.168.2.19,MCPORT= 1719,HTTPSRVR=192.168.89.63

Table 2: DHCP Scope Configuration

Figure 3 shows the CLI output from the Avaya G350 DHCP configuration. For more information on DHCP functionality refer to [2].

```
############# enable the DHCP server ############
ip dhcp-server
ip dhcp ping packets
############# Configure “pool 1” for data ############
ip dhcp pool 1
 name "DHCP for Data"
 start-ip-addr 192.168.89.100 → phones will be assigned IP addresses 100-150 on the data VLAN
 end-ip-addr 192.168.89.150  →
 default-router 192.168.89.1
 option 176 → 46xx phones are directed to switch to the voice VLAN (88)
  value ascii "L2Q=1,L2QVLAN=88"
 exit
 option 242 → 96xx phones are directed to switch to the voice VLAN (88)
  value ascii "L2QVLAN=88"
 exit
ip dhcp activate pool 1 → DHCP pool 1 is activated
############# Configure “pool 2” for voice ############
ip dhcp pool 2
 name "DHCP for Voice"
 start-ip-addr 192.168.88.100  → phones will be assigned IP addresses 100-150 on the voice VLAN
 end-ip-addr 192.168.88.150   →
 default-router 192.168.88.1
 option 176 → 46xx phones are directed to register to 192.168.2.19, and use TFTP server 192.168.89.63
  value ascii "MCIPADD=192.168.2.19,MCPORT=1719,TFTPSRVR=192.168.89.63"
 exit
 option 242→ 96xx phones are directed to register to 192.168.2.19, and use HTTP server 192.168.89.63
  value ascii "MCIPADD=192.168.2.19,MCPORT=1719,HTTPSRVR=192.168.89.63"
 exit
ip dhcp activate pool 2 → DHCP pool 2 is activated
exit
```

Figure 3 – Avaya G350 DHCP Configuration

5. Configure 802.1x Multi-domain on Cisco Catalyst 3750

The following section describes the configuration on the Cisco Catalyst 3750 to support 802.1x multi-domain mode. Refer to [5] for more information.

5.1 Authentication, Authorization & Accounting (AAA) and DOT1X activation

The following commands define the AAA and DOT1X attributes on the Cisco switch.

```
C3750-PoE#
!
aaa new-model   → Enables the AAA access control.
!
aaa authentication login default none   → (aaa config default value).
!
aaa authentication dot1x default group radius   → This authentication first tries to contact a
RADIUS server.
!
aaa authorization network default group radius   → Use user-RADIUS authorization for all
network-related service requests.
!
aaa session-id common   → (aaa config default value).
!
dot1x system-auth-control   → Enable IEEE 802.1x authentication globally on the switch.
!
```

Figure 4 – Cisco Catalyst 3750 AAA and DOT1X Activation

5.2 Interface configuration

The following commands define the Cisco switch interfaces to the Avaya 46xxx and 96xx telephones as well as the interfaces to the RADIUS server and the network router.

```
########## Interface for 96xx phones##########
interface FastEthernet1/0/1
description 96xx phone
switchport mode access   → The port is set to access unconditionally and operates as a non-trunking,
single VLAN interface
switchport access vlan 89   → Configure the interface as a static access port with the VLAN ID of the
access mode VLAN (data VLAN)
switchport voice vlan 88   → The VLAN to be used for voice traffic.
dot1x pae authenticator   → (default dot1x value displayed by switch)
dot1x port-control auto   → Enable IEEE 802.1x authentication on the port and cause the port to
change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange.
dot1x host-mode multi-domain   → Enable MDA on a switch port.
dot1x reauthentication   → Enables periodic re-authentication of the client.
dot1x timeout reauth-period 30   → Set the number of seconds between re-authentication attempts.
!
##########The Interface for 46xx phone is configured the same as the 96xx interface##########
interface FastEthernet1/0/2
 description 46xx phone
 switchport access vlan 89
 switchport mode access
 switchport voice vlan 88
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-domain
 dot1x reauthentication
 dot1x timeout reauth-period 30
!
########Interface to the 3725 Router#########
interface FastEthernet1/0/21
description To Router
switchport trunk encapsulation dot1q → Set the encapsulation format on the trunk port to IEEE
802.1Q.
switchport mode trunk   → Set the port to trunk unconditionally. The port is a trunking VLAN Layer
2 interface.
!
########Interface to the FreeRadius#########
interface FastEthernet1/0/22
 description RADIUS
 switchport access vlan 89
!
#########Voice VLAN 88 Interface###########
interface Vlan88
 ip address 192.168.88.2 255.255.255.0
```

```
!
#########Data VLAN 89 Interface############
interface Vlan89
 ip address 192.168.89.2 255.255.255.0
!
#######Routing Information###########
ip default-gateway 192.168.89.1
ip route 192.168.2.0 255.255.255.0 192.168.89.1
```

Figure 5 – Cisco Catalyst 3750 Interface and Routing Configuration

5.3 RADIUS server configuration

The following commands define the RADIUS server to the Cisco Catalyst 3750. Note that the key value specified below must match those defined in the FreeRadius ***clients.conf*** file (see **Section 6**).

```
radius-server host 192.168.89.61 auth-port 1812 acct-port 1813 key 1234567890123  → This specifies the  IP address of the FreeRadius, accounting and authorization UDP ports, and encryption key used between the FreeRadius and the Cisco switch.
!
radius-server source-ports 1645-1646  → This specifies the UDP ports used by the Cisco Catalyst 3750 to communicate with the RADIUS
!
```

Figure 6 – Cisco Catalyst 3750 RADIUS Configuration

6. Configure FreeRadius 802.1x Authentication

Refer to [7] for detailed information on how to install and configure the FreeRadius server on the Red Hat operating system.

6.1 Defining the Cisco Catalyst 3750 as a "client".

The Cisco Catalyst must be defined in the FreeRadius as a client.

Note – The *secret* value below must match the *key* value defined in the Cisco Catalyst 3750 (see **Section 5.3**).

Step	Description
1.	From the FreeRadius console change to the ***raddb*** directory by entering; ***cd /usr/local/etc/raddb***
2.	Open the ***clients.conf*** file.
3.	Go to the bottom of the file and add the following entry; ***Client 192.168.89.2/24 {*** → *IP address of the Cisco Catalyst 3750* ***secret = 1234567890123*** → *Authentication key* ***shortname = C3750*** → *Name of client* ***NAS-IP-Address = 192.168.89.2*** → *IP address of the Cisco Catalyst 3750* ***}*** → *This bracket must be entered*
4.	Save and close the file.

6.2 Defining the Avaya 46xx and 96xx Telephones as “users”.

Each telephone and the PC must be defined as users in the FreeRadius.

Note – All indicated quote characters (“) are required.

Step	Description
1.	From the FreeRadius console change to the ***raddb*** directory by entering; ***cd /usr/local/etc/raddb***
2.	Open the ***users*** file.
3.	Go to the bottom of the file and add the following entry; ***xxxxxxxxxxxx User-Password == "123456"*** ***Cisco-AVPair == "device-traffic-class=voice"*** → *xxxxxxxxxxxx is the MAC address of the phone and “123456” is the 802.1x password that will be entered on the phone.* → *The Cisco-AVPair line tells the Cisco Catalyst 3750 that this user (phone) can access the voice VLAN.*
4.	Repeat **Step 3** for each phone. The following is an example of a completed phone user list. *00040DE97552 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"* *00040DECB9A9 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"* *00096E0E57F5 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"* *00040DED76F9 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"*
5.	Save and close the file.

6.3 Defining the PC as a *user*.

The PC must be defined in the FreeRadius as a user.

Note – All indicated quote characters (“) are required.

Step	Description
1.	From the FreeRadius console change to the ***raddb*** directory by entering; ***cd /usr/local/etc/raddb***
2.	Open the ***users*** file.
3.	Go to the bottom of the file and add the following entry; ***pcuser User-Password == "123456"*** *→ pcuser is the User Name that must be entered on the PC 802.1x login window.* *→ 123456 is the password that must be entered on the PC 802.1x login window.*
4.	Repeat **step 3** for each PC user. The following is an example of a completed user list after the PCs have been entered. **Note –** The phone and PC user entries can be inter-dispersed in the ***users*** file. *00040DE97552 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"* *Tony User-Password == "123456"* *00040DECB9A9 User-Password == "123456"* *Cisco-AVPair == "device-traffic-class=voice"* *John User-Password == "123456"* *Jim User-Password == "123456"*
5.	Save and close the file.

6.4 Applying Changes to the *clients.conf* and the *users* files.

Once the ***clients.conf*** and the ***users*** files have been modified and saved, the FreeRadius can be started. If the FreeRadius is already running, then it must be restarted for the changes to the ***clients.conf*** and the ***users*** files to take effect.

6.4.1 Starting FreeRadius

Step	Description
1.	From the FreeRadius console enter; ***radiusd -X***

Note - The ***radiusd -X*** command not only starts the FreeRadius, it also displays authentication requests and replies on the FreeRadius console (see **Section 10.2.4.1**).

6.4.2 Restarting FreeRadius

Step	Description
1.	The active FreeRadius process must be identified. From the FreeRadius console enter; ***ps –ef | grep radiusd*** The console will show a display similar to the following; ***root 9920 16720 0 Mar02 pts/2 00:01:08 radiusd -X*** Take note of the first numeric value (e.g. 9920). This is the radiusd process number.
2.	Using the process number identified in **Step 1**, stop the FreeRadius process by entering; ***kill -9 9920***
3.	Start FreeRadius again by entering; ***radiusd -X***

7. Configure Avaya 96xx and 46xx Series IP Telephones for 802.1x

After defining the phone's 802.1x ID and password in the RADIUS server, the ID and password must be administered on the phones. The MAC address of the phone can be used as its 802.1x ID. The Avaya 46xx and 96xx IP telephones use their MAC addresses by default. However, an 802.1x password must be provisioned.

Note – The phone 802.1x authentication values must match those specified in the FreeRadius server ***users*** file (see **Section 6.2**).

7.1 Avaya 96xx Series IP Telephone

7.1.1 Setting the 802.1x ID and Password.

Step	Description

1.	When the phone boots for the first time, or after performing Craft level "***CLEAR***" or "***802.1x***" procedures (see [3] for information on executing these procedures), the 96xx phone will display the following by default, where ***XXXXXXXXXXXX*** is the MAC address of the phone.
	`802.1x ID=xxxxxxxxxxxx`
	`#=OK New=`
	Press **#** to accept the MAC address as the phone's 802.1x ID.

2.	The phone will then present the following display.
	`Password=`
	`#=OK`
	Enter the password defined in the RADIUS for this phone and then press **#**. The phone will complete its boot process and authenticate to the RADIUS. The phone will then complete DHCP server processing and register to Avaya Communication Manager.

7.2 Avaya 46xx Series IP Telephone

The 802.1x authentication procedure is the same as for the Avaya 96xx telephone. Refer to [4] for more information.

8. Configure Windows XP Embedded 802.1x Authentication

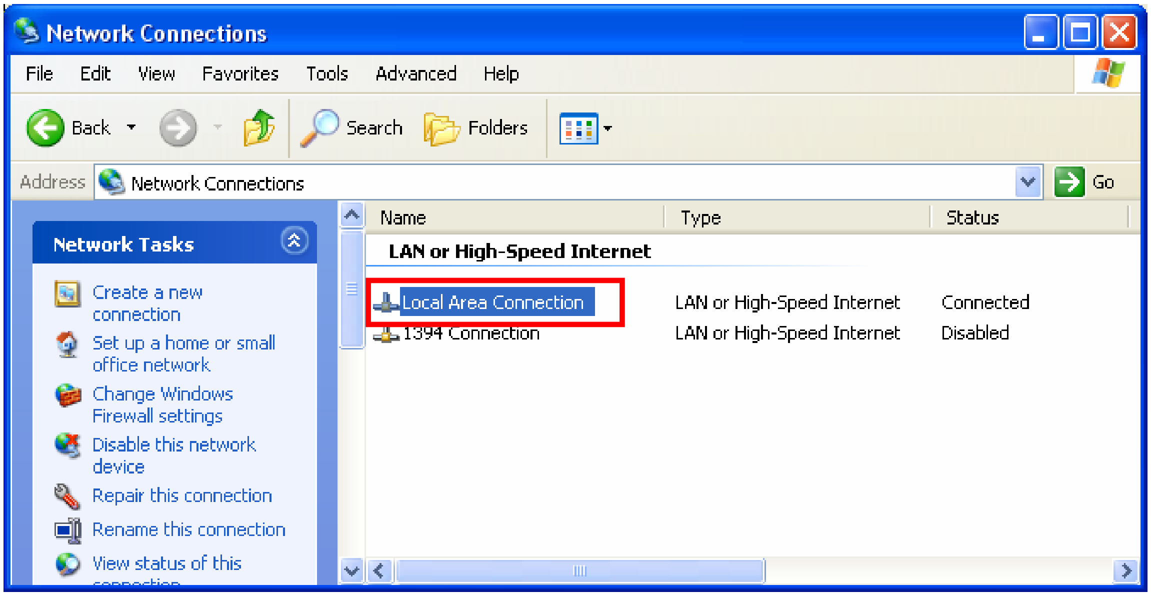
When multi-domain is specified on the Cisco Catalyst 3750, a PC connected to the Avaya 96xx or 46xx series IP telephone will be authenticated separately from the telephone. The PC must be configured to provide 802.1x credentials. Windows XP provides an embedded 802.1x authentication process. Add-on 802.1x client programs are also available. These Application Notes refer to the Windows XP imbedded 802.1x authentication process.

Note – These application notes assume that appropriate IP addressing for the PC, either via DHCP or static, has been provided.

8.1 Enabling 802.1x Authentication

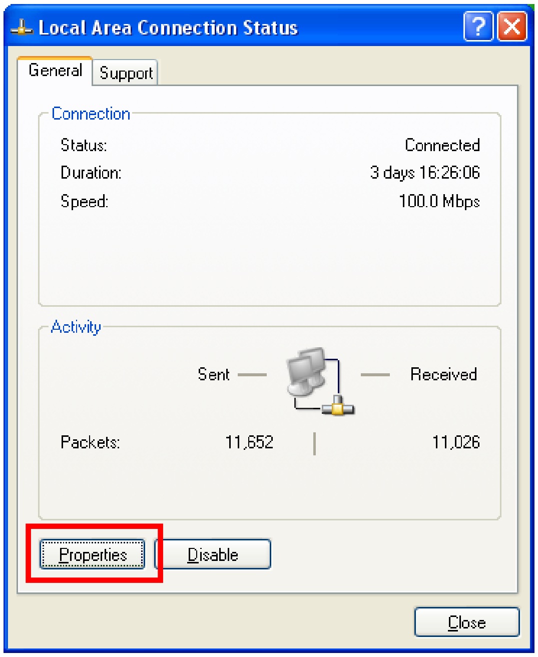
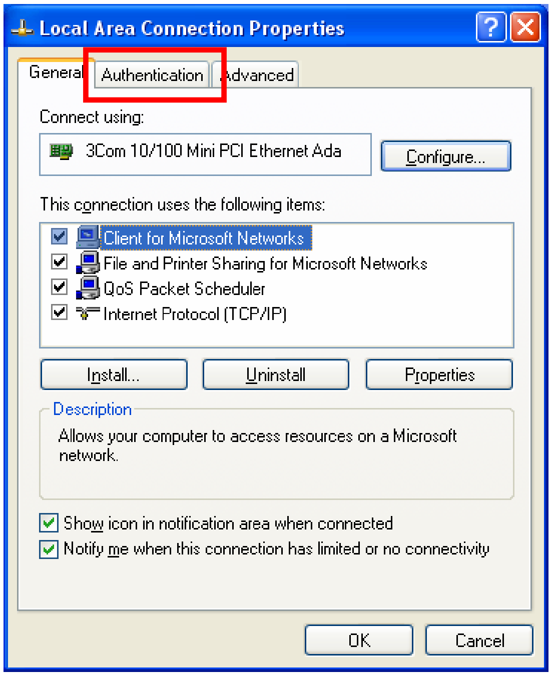
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

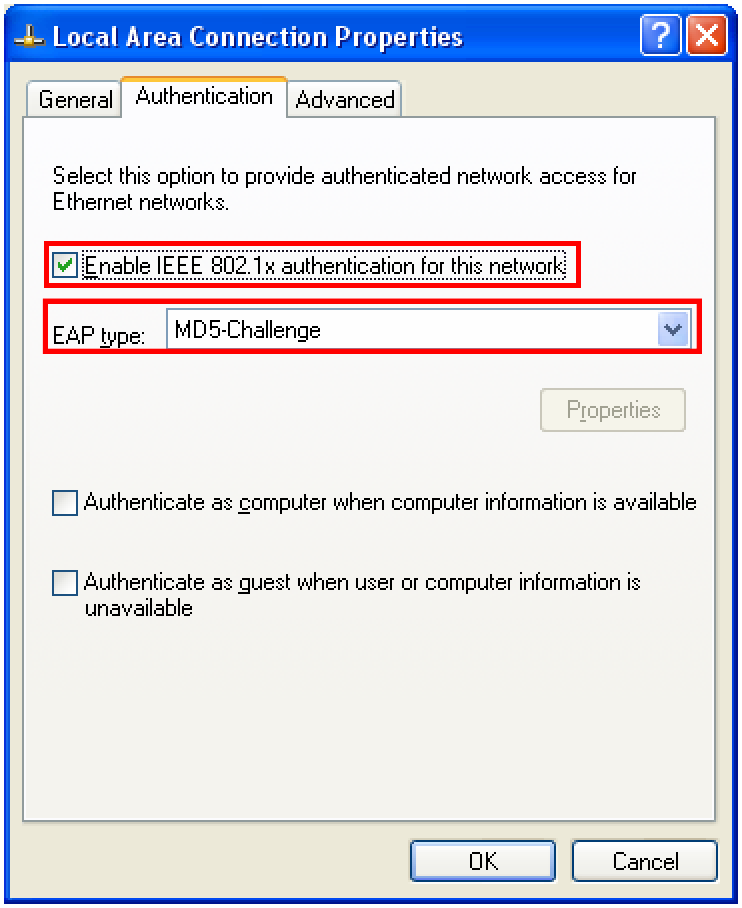
Before connecting the PC to the Avaya IP telephone, go to ***Start* → *Control Panel* → *Network Connections*** and select the appropriate network interface.



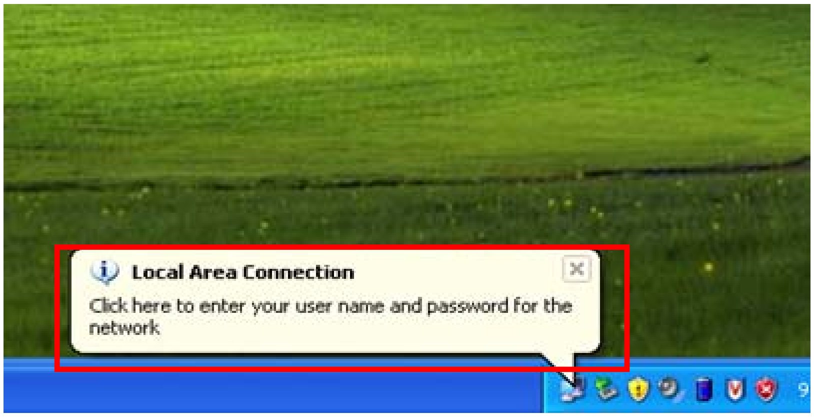
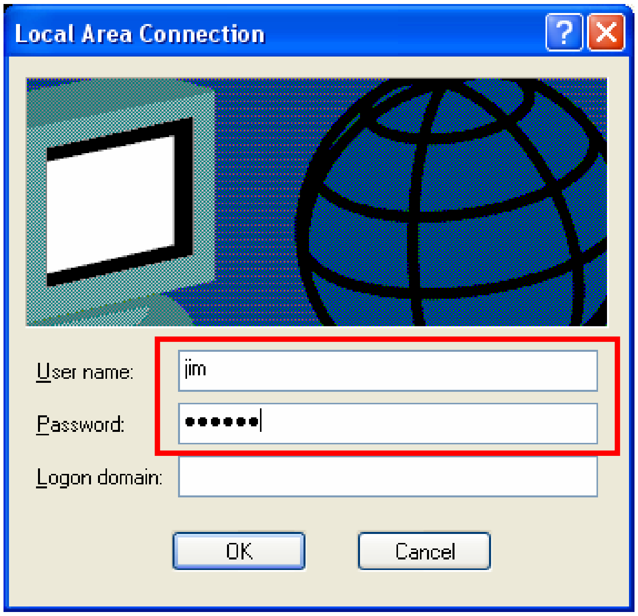
Name	Type	Status
LAN or High-Speed Internet		
Local Area Connection	LAN or High-Speed Internet	Connected
1394 Connection	LAN or High-Speed Internet	Disabled

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

Step	Description
2.	From the Interface window select → ***Properties***.  Local Area Connection Status General Support Connection Status: Connected Duration: 3 days 16:26:06 Speed: 100.0 Mbps Activity Sent — Received Packets: 11,652 11,026 Properties Disable Close
3.	From the Properties window select →***Authentication***.  Local Area Connection Properties General Authentication Advanced Connect using: 3Com 10/100 Mini PCI Ethernet Ada Configure... This connection uses the following items: ☑ Client for Microsoft Networks ☑ File and Printer Sharing for Microsoft Networks ☑ QoS Packet Scheduler ☑ Internet Protocol (TCP/IP) Install... Uninstall Properties Description Allows your computer to access resources on a Microsoft network. ☑ Show icon in notification area when connected ☑ Notify me when this connection has limited or no connectivity OK Cancel

Step	Description
4.	From the Authentication window, check the ***Enable IEEE 802.1x authentication*** box and set the ***EAP type*** to ***MD5-Challenge***.  Local Area Connection Properties General Authentication Advanced Properties OK Cancel Select this option to provide authenticated network access for Ethernet networks. ☑ Enable IEEE 802.1x authentication for this network EAP type: MD5-Challenge □ Authenticate as computer when computer information is available □ Authenticate as guest when user or computer information is unavailable
5.	Exit the interface configuration by clicking ***OK***, ***OK***, and ***Close***. Then close the Network Connections window.

8.2 Authenticating the PC

1.	Connect the PC to the Avaya IP telephone. Once an Ethernet link has been established the PC will display the following message on the desktop;  **Local Area Connection** Click here to enter your user name and password for the network Click on the message box (avoiding the "X" which will cancel the request).
2.	The 802.1x authentication window will open.  Local Area Connection User name: jim Password: •••••• Logon domain: Enter a ***User name*** and ***Password*** that matches user values specified in the RADIUS server (see **Section 6.3**) and click ***OK***. The 802.1x authentication window will close and the PC will authenticate to the RADIUS server.

9. Cisco 3725 Router Configuration

The following section describes the configuration of the Cisco 3725 used in the reference configuration. See [6] for more information.

```
Cisco-3725-main#
########Interface to the Cisco Catalyst 3750 Catalyst#########
interface FastEthernet0/0 → Physical interface.
 description To_3750
 no ip address
 speed 100
 full-duplex
!
interface FastEthernet0/0.88 → Sub-interface for VLAN 88 (voice VLAN).
 encapsulation dot1Q 88 → Enables IEEE 802.1q encapsulation of traffic on a specified VLAN.
 ip address 192.168.88.1 255.255.255.0→ IP address of VLAN 88 sub-interface.
 ip helper-address 192.168.2.100 → IP address of the DHCP server.
!
interface FastEthernet0/0.89  → Sub-interface for VLAN 89 (Data VLAN).
 encapsulation dot1Q 89 → Enables IEEE 802.1q encapsulation of traffic on a specified VLAN.
 ip address 192.168.89.1 255.255.255.0 →  IP address of VLAN 89 sub-interface.
 ip helper-address 192.168.2.100 →  IP address of the DHCP server.
!
interface FastEthernet0/1 → Interface to Avaya G350 Media Gateway.
description To_G350
 ip address 50.50.50.1 255.255.255.0 → IP address of the interface.
 duplex auto
 speed auto
!
ip route 192.168.2.0 255.255.255.0 50.50.50.2 → IP route to the Avaya Communication
Manager and DHCP server IP domain, via the Avaya G350 Media Gateway (50.50.50.2).
!
end
Cisco-3725-main#
```

Figure 7 – Cisco 3725 Router Configuration

10. Verification and Troubleshooting

10.1 Verification

10.1.1 Avaya 46xx and 96xx IP Telephones

Step	Description
1.	After accepting the phones' default MAC address 802.1x ID (select # on the phone keypad) and entering the phones' 802.1x password, verify that the phone completes its DHCP server exchange and registers to Avaya Communication Manager.
2.	Verify dial-tone.
3.	Place a call and verify two-way talk path.

10.1.2 Attached PC

Step	Description
1.	Connect the PC to the back of the Avaya IP telephone. Enter the PCs' 802.1x ***User name*** and ***password*** when prompted. Verify that the PC can ping its default gateway. The default gateway can be found in ***Start → Control Panel → Network Connections → Properties → Internet Protocol (TCP/IP)*** or by entering ***ipconfig*** from a command window.

10.2 Troubleshooting

The following procedures can be used to troubleshoot 802.1x issues. The following examples show successful authentication states.

10.2.1 Cisco Catalyst 3750

10.2.1.1 Debug dot1x all

This command will display all 802.1x transactions on the Cisco Catalyst 3750. The output from this command can be substantial. Therefore for brevity, only lines that verify operation are included. Use the command ***no debug dot1x all*** to disable the debug output.

10.2.1.1.1 Avaya 9630 IP Telephone 802.1x Authentication (MAC address 0040DECB9A9)

```
########The Cisco Catalyst 3750 receives an EAPOL Start from the Avaya 9630#########
1w0d: dot1x-ev:Received pkt saddr =0004.0dec.b9a9 , daddr = 0180.c200.0003, pae-ether-type
= 888e.0100.0011

########Cisco Catalyst 3750 sends EAP- Request/Identity to the 9630 #########
1w0d: dot1x-ev:FastEthernet1/0/3:Sending EAPOL packet to 0004.0dec.b9a9

########The Cisco Catalyst 3750 receives an EAP-Request/Identity from the 9630#########
1w0d: dot1x-packet:Received an EAP packet on the FastEthernet1/0/3 from mac
0004.0dec.b9a9

########The Cisco Catalyst 3750 sends the 9630 EAP-Request/Identity to the FreeRadius#########
1w0d: dot1x-ev:dot1x_sendRespToServer: Response sent to the server from 0004.0dec.b9a9

######The Cisco Catalyst 3750 receives an EAP-Request/MD5 challenge from the FreeRadius######
1w0d: dot1x-packet:Received an EAP request packet from EAP for mac 0004.0dec.b9a9
1w0d: dot1x-sm:Posting EAP_REQ on Client=24E3760

######The Cisco Catalyst 3750 sends the EAP-Request/MD5 challenge to the 9630######
1w0d: dot1x-packet:dot1x_txReq: EAPOL packet sent to client (0004.0dec.b9a9)


######The Cisco Catalyst 3750 receives the EAP-Request/MD5 response from the 9630######
1w0d: dot1x-packet:Received an EAP packet on the FastEthernet1/0/3 from mac
0004.0dec.b9a9

######The Cisco Catalyst 3750 sends the 9630 EAP-Request/MD5 response to the FreeRadius######
1w0d: dot1x-ev:dot1x_sendRespToServer: Response sent to the server from 0004.0dec.b9a9


######The Cisco Catalyst 3750 receives EAP-Success from the FreeRadius######
1w0d: dot1x-sm:Fa1/0/3:0004.0dec.b9a9:auth_bend_response_success_action called


######The Cisco Catalyst 3750 authorizes the 9630 onto the VOICE domain and VLAN 88######
1w0d: dot1x-ev:dot1x_switch_supplicant_add: Adding 0004.0dec.b9a9 on FastEthernet1/0/3
in vlan 88, domain is VOICE
```

Figure 8 – Cisco Catalyst 3750/Avaya 9630 IP Telephone 802.1x Authentication Sequence

10.2.1.1.2 Attached PC Authentication (MAC address 0004764C6843) to Data VLAN 89

```
######The Cisco Catalyst 3750 detects the PC######
a1w0d: dot1x-ev:dot1x_switch_mac_address_notify: MAC 0004.764c.6843 discovered on
FastEthernet1/0/3(89)

########The Cisco Catalyst 3750 receives an EAPOL Start from the PC#########
1w0d: dot1x-ev:Received pkt saddr =0004.764c.6843 , daddr = 0180.c200.0003, pae-ether-
type = 888e.0100.0008

########Cisco Catalyst 3750 sends EAP- Request/Identity to the PC #########
1w0d: dot1x-ev:FastEthernet1/0/3:Sending EAPOL packet to 0004.764c.6843

########The Cisco Catalyst 3750 receives an EAP-Request/Identity from the PC#########
1w0d: dot1x-packet:Received an EAP packet on the FastEthernet1/0/3 from mac
0004.764c.6843

########The Cisco Catalyst 3750 sends the PC EAP-Request/Identity to the FreeRadius#########
1w0d: dot1x-ev:dot1x_sendRespToServer: Response sent to the server from 0004.764c.6843

######The Cisco Catalyst 3750 receives an EAP-Request/MD5 challenge from the FreeRadius######
1w0d: dot1x-packet:Received an EAP packet on the FastEthernet1/0/3 from mac
0004.764c.6843
1w0d: dot1x-sm:Posting EAPOL_EAP on Client=2E359D0

######The Cisco Catalyst 3750 sends the EAP-Request/MD5 challenge to the PC######
1w0d: dot1x-packet:dot1x_txReq: EAPOL packet sent to client (0004.764c.6843)

######The Cisco Catalyst 3750 receives the EAP-Request/MD5 response from the PC######
1w0d: dot1x-packet:Received an EAP packet on the FastEthernet1/0/3 from mac
0004.764c.6843

######The Cisco Catalyst 3750 sends the PC EAP-Request/MD5 response to the FreeRadius######
1w0d: dot1x-ev:dot1x_sendRespToServer: Response sent to the server from 0004.764c.6843

######The Cisco Catalyst 3750 receives EAP-Success from the FreeRadius######
1w0d: dot1x-packet:Received an EAP Success on the FastEthernet1/0/3 for mac
0004.764c.6843

######The Cisco Catalyst 3750 authorizes the PC onto the DATA domain and VLAN 89######
1w0d: Dot1x-ev:dot1x_switch_supplicant_add: Adding 0004.764c.6843 on
FastEthernet1/0/3 in vlan 89, domain is DATA
```

Figure 9 – Cisco Catalyst 3750/Attached PC 802.1x Authentication Sequence

10.2.1.2 Show mac-address-table interface fastethernet 1/0/3

This command displays the MAC addresses and corresponding VLANs, associated with port 1/0/3.

```
C3750-PoE#show dot1x interface fastEthernet 1/0/3 mac-address-table int fastEthernet
1/0/3

        Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  88    0004.0dec.b9a9    STATIC      Fa1/0/3
  89    0004.764c.6843    STATIC      Fa1/0/3
Total Mac Addresses for this criterion: 2
```

Figure 10 – Cisco Catalyst 3750 Dot1x MAC Address/VLAN Port Association

10.2.1.3 Show radius server group all

This command displays the RADIUS servers provisioned on the Cisco Catalyst 3750.

```
C3750-PoE#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
   Server(192.168.88.61:1812,1813) Transactions:
```

Figure 11 – Cisco Catalyst 3750 RADIUS Configuration

10.2.1.4 Show dot1x interface fastethernet 1/0/3 details

The following command shows the Avaya 9630 IP telephone (voice) and attached PC (data) authenticated on port 1/0/3 of the Cisco Catalyst 3750.

```
C3750-PoE#dot1x interface fastEthernet 1/0/3 details
Dot1x Info for FastEthernet1/0/3
-----------------------------------
PAE                    = AUTHENTICATOR
PortControl            = AUTO
ControlDirection       = Both
HostMode               = MULTI_DOMAIN
ReAuthentication       = Enabled
QuietPeriod            = 5
ServerTimeout          = 30
SuppTimeout            = 30
ReAuthPeriod           = 30 (Locally configured)
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
RateLimitPeriod        = 0

Dot1x Authenticator Client List
-------------------------------
Domain                 = VOICE
Supplicant             = 0004.0dec.b9a9
   Auth SM State       = AUTHENTICATED
   Auth BEND SM State  = IDLE
Port Status            = AUTHORIZED
ReAuthPeriod           = 30
ReAuthAction           = Reauthenticate
TimeToNextReauth       = 5
Authentication Method  = Dot1x
Authorized By          = Authentication Server

Domain                 = DATA
Supplicant             = 0004.764c.6843
   Auth SM State       = AUTHENTICATED
   Auth BEND SM State  = IDLE
Port Status            = AUTHORIZED
ReAuthPeriod           = 30
ReAuthAction           = Reauthenticate
TimeToNextReauth       = 15
Authentication Method  = Dot1x
Authorized By          = Authentication Server
```

Figure 12 – Cisco Catalyst 3750 Port 1/0/3 Dot1x Status

10.2.2 FreeRadius Server

10.2.2.1 Starting and Stopping the FreeRadius server

10.2.2.1.1 Starting FreeRadius

Step	Description
1.	From the FreeRadius console enter; ***radiusd -X*** The ***radiusd -X*** command not only starts the FreeRadius, it also displays authentication requests and replies on the FreeRadius console (see **Section 10.2.4.1**).

10.2.2.1.2 Stopping and Restarting FreeRadius

Step	Description
1.	The active FreeRadius process must be identified. From the FreeRadius console enter; ***ps –ef | grep radiusd*** The console will show a display similar to the following; ***root 9920 16720 0 Mar02 pts/2 00:01:08 radiusd -X*** Take note of the first numeric value (e.g. 9920). This is the radiusd process number.
2.	Using the process number identified in **step 1**, stop the FreeRadius process by entering; ***kill -9 9920***
3.	Start FreeRadius again by entering; ***radiusd -X***

10.2.2.2 Monitoring Phone and PC Authentication on the FreeRadius Server

10.2.2.2.1 Avaya 9630 IP Telephone

In the example shown in **Figure 13**, the Avaya 9630 IP telephone (MAC address **00F8FCE4B85**) requests 802.1x authorization from the FreeRadius.

```
###### FreeRadius receives an access request from the Cisco Catalyst 3750 for the Avaya 9630 ######
rad_recv: Access-Request packet from host 192.168.88.2:1645, id=46, length=139
        User-Name = "00040DECB9A9"
        Service-Type = Framed-User
        Framed-MTU = 1500
        Called-Station-Id = "00-0F-8F-CE-4B-85"
        Calling-Station-Id = "00-04-0D-EC-B9-A9"
        EAP-Message = 0x0203001101303030343044454342394139
        Message-Authenticator = 0xa859ffa3238b5bf93d640e32096e9156
        NAS-Port = 50103
        NAS-Port-Type = Ethernet
        NAS-IP-Address = 192.168.88.2
## FreeRadius sends an MD5 challenge and the Cisco AVPair attribute for the Cisco Catalyst 3750
######
rlm_eap_md5: Issuing Challenge
Sending Access-Challenge of id 46 to 192.168.88.2 port 1645
        Cisco-AVPair == "device-traffic-class=voice"
        EAP-Message= 0x010400160410313a9616848cfdb2968938a2f5248dff
        Message-Authenticator= 0x00000000000000000000000000000000
        State = 0xd29df802d08e03e82b72d0d5dd6075b6
###### The Avaya 9630 responds ######
rad_recv: Access-Request packet from host 192.168.88.2:1645, id=47, length=162
        User-Name = "00040DECB9A9"
        Service-Type = Framed-User
        Framed-MTU = 1500
        Called-Station-Id = "00-0F-8F-CE-4B-85"
        Calling-Station-Id = "00-04-0D-EC-B9-A9"
        EAP-Message= 0x020400160410027b1860d61f90a2ae3d9d41987d7bcc
        Message-Authenticator= 0x52c7e66c6b1aaa08c34a1dd7773a5e68
        NAS-Port = 50103
        NAS-Port-Type = Ethernet
        State = 0xd29df802d08e03e82b72d0d5dd6075b6
        NAS-IP-Address = 192.168.88.2
###### The FreeRadius accepts the Avaya 9630 telephone. ######
Sending Access-Accept of id 47 to 192.168.88.2 port 1645
        Cisco-AVPair == "device-traffic-class=voice"
        EAP-Message = 0x03040004
        Message-Authenticator= 0x00000000000000000000000000000000
        User-Name = "00040DECB9A9"
```

Figure 13 – FreeRadius Avaya 9630 802.1x Authentication

10.2.2.2.2 PC Attached to the Avaya 9630 IP Telephone

In the example shown in **Figure 14**, a PC (MAC address ***0004764C6843***, ***User-Name = jim***) is attached to the Avaya 9630 IP telephone and requests 802.1x authorization. The Cisco Catalyst 3750 (***192.168.88.2***) forwards this request to the FreeRadius server.

```
### FreeRadius receives access request from the Cisco Catalyst 3750 for the PC User-Name
“jim” ####
rad_recv: Access-Request packet from host 192.168.88.2:1645, id=52, length=121
        User-Name = "jim"
        Service-Type = Framed-User
        Framed-MTU = 1500
        Called-Station-Id = "00-0F-8F-CE-4B-85"
        Calling-Station-Id = "00-04-76-4C-68-43"
        EAP-Message = 0x02020008016a696d
        Message-Authenticator= 0x42567926799a9339e65ac1fed02de359
        NAS-Port = 50103
        NAS-Port-Type = Ethernet
        NAS-IP-Address = 192.168.88.2
###### FreeRadius sends an MD5 challenge. #####
rlm_eap_md5: Issuing Challenge
Sending Access-Challenge of id 52 to 192.168.88.2 port 1645
        EAP-Message= 0x0103001604109ca78b134f5bedf68dd8ec7a6a14e48b
        Message-Authenticator= 0x00000000000000000000000000000000
        State = 0x137b342d2432d0473285d4dc0c5dd21b
###### The PC responds #####
rad_recv: Access-Request packet from host 192.168.88.2:1645, id=53, length=156
        User-Name = "jim"
        Service-Type = Framed-User
        Framed-MTU = 1500
        Called-Station-Id = "00-0F-8F-CE-4B-85"
        Calling-Station-Id = "00-04-76-4C-68-43"
        EAP-Message  0x0203001904105b6b9fd31e1a0e7f7fdb5f72d1bab1bc6a696d
        Message-Authenticator= 0x3eb8a34a7836ee18f4bf13a3c3380862
        NAS-Port = 50103
        NAS-Port-Type = Ethernet
        State = 0x137b342d2432d0473285d4dc0c5dd21b
        NAS-IP-Address = 192.168.88.2
###### The FreeRadius accepts the PC User-Name ‘jim”. ######
Sending Access-Accept of id 53 to 192.168.88.2 port 1645
        EAP-Message = 0x03030004
        Message-Authenticator= 0x00000000000000000000000000000000
        User-Name = "jim"
```

Figure 14 – FreeRadius Attached PC 802.1x Authentication

11. Conclusions

As illustrated in these Application Notes, Avaya IP Telephones with attached PCs can support separate 802.1x authentication states via Cisco Catalyst 3750 ports configured for 802.1x Multi-Domain Authentication (MDA). The Cisco Catalyst 3750 can use the FreeRADIUS server to authenticate the Avaya IP Telephone and the attached PC. The FreeRadius authentication can authorize the Avaya IP Telephone to access the voice VLAN while the attached PC is only authorized to access the data VLAN.

12. References

12.1 The following references can be found at www.avaya.com.

[1] *Configuring the 802.1x Protocol on a Cisco Catalyst 6509 Switch in Multi-Host Mode with a Cisco Secure Access Control Server to Support Avaya 9620 IP Telephones with an Attached PC - Issue 1.0*

[2] *Configuring 802.1x Protocol on Cisco Catalyst 6509, 4503 and 3750 Switches for Multi-host Mode Supporting an Avaya IP Telephone With an Attached PC - Issue 1.1*

[3] *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide Release 1.2, 16-300694, Issue 3, January 2007*

[4] *Avaya 4600 Series IP Telephone Installation Guide, 555-233-128, Issue 5, November 2006*

12.2 The following references can be found at www.cisco.com.

[5] *Catalyst 3750 Switch Software Configuration Guide, 12.2(35)SE, Chapter 10, Configuring IEEE 802.1x Port-Based Authentication*

[6] *Cisco IOS Interface and Hardware Component Command Reference, Release 12.4*

12.3 FreeRadius server references

[7] *http://www.tldp.org/HOWTO/8021X-HOWTO/*

Additional information regarding the FreeRadius server can be found at **www.freeradius.org.**

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com