Configuring Avaya 96xx SIP Telephones with Disabled 802.1x Supplicant, and an 802.1x Authenticated Attached PC, Connected to a Cisco Catalyst 3750 Multi-domain Authentication (MDA) Switch Port. - Issue 1.0

Abstract

These Application Notes describe the configuration of 802.1x Multi-domain Authentication (MDA) on a Cisco Catalyst 3750 switch port, to support an Avaya 96xx SIP Telephone with an attached PC, where the PC is challenged by the Cisco switch but the Avaya 96xx SIP Telephone is not. 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. The Catalyst 3750 switches are one of the Cisco platforms that support MDA. Typically an MDA port configuration challenges the IP telephone, and a PC attached to the phone, separately. However some network architectures specify that only the attached PC should be challenged.
1. INTRODUCTION................................................................. 4

1.1 Avaya 2.0 96xx SIP Telephone 802.1x Options .............................................................. 4

1.2 Standard 802.1x MDA Authentication – IP Telephone and Attached PC ............................ 5

1.3 802.1x Authentication for an Attached PC Only. ................................................................. 7

1.3.1 MAC Authentication Bypass (MAB) Telephone Authentication ......................................................... 7

1.3.2 PC Authentication .............................................................................................................. 8

2. REFERENCE CONFIGURATION ..................................................... 9

3. EQUIPMENT AND SOFTWARE VALIDATED ........................................ 10

4. CONFIGURE 802.1X MULTI-DOMAIN (MDA) AND MAC AUTHENTICATION BYPASS (MAB) ON THE CISCO CATALYST 3750 ................................................................. 11

4.1 Authentication, Authorization & Accounting (AAA) and DOT1X activation .......................... 11

4.2 Network Interface configuration ............................................................................................... 12

4.3 RADIUS server configuration ............................................................................................... 14

5. AVAYA G450 MEDIA GATEWAY INTERFACE CONFIGURATION .................... 15

6. FREERADIUS CONFIGURATION .................................................................................... 16

6.1 Defining the Cisco Catalyst 3750 as a “client” ...................................................................... 16

6.2 Defining the Avaya 96xx SIP Telephone as a “user” ............................................................... 17

6.3 Defining the PC as a user ....................................................................................................... 18

6.4 Applying Changes to the clients.conf and the users files ..................................................... 18

6.4.1 Starting FreeRADIUS ......................................................................................................... 18

6.4.2 Restarting FreeRADIUS ..................................................................................................... 19

7. CONFIGURE 2.0 AVAYA 9640 SIP TELEPHONES FOR 802.1X MAB .......... 19
7.1 Disabling the 802.1x Supplicant Function on the 2.0 Avaya 9640 SIP Telephone. ......................... 20

7.2 Enabling the 802.1x Proxy Logoff Function on the 2.0 Avaya 9640 SIP Telephone. .................... 23

8. CONFIGURE WINDOWS XP EMBEDDED 802.1X AUTHENTICATION ............. 24

8.1 Enabling 802.1x Authentication on the PC. ............................................................................. 24

8.2 Authenticating the PC. ................................................................................................................. 26

9. VERIFICATION AND TROUBLESHOOTING .......................................................... 27

9.1 Verification. .................................................................................................................................. 27

9.1.1 Avaya 9640 SIP Telephone ....................................................................................................... 27

9.1.2 Attached PC ................................................................................................................................. 27

9.1.3 Cisco Catalyst 3750 Switch ......................................................................................................... 28

9.1.4 Monitoring Phone and PC Authentication on the FreeRADIUS Server ............................. 29

9.2 Troubleshooting ....................................................................................................................... 31

9.2.1 Cisco Catalyst 3750 .................................................................................................................... 31

9.2.2 Restarting the FreeRADIUS Server .......................................................................................... 32

10. CONCLUSIONS ....................................................................................................................... 33

11. REFERENCES ......................................................................................................................... 33

11.1 The following references can be found at www.avaya.com ................................................... 33

11.2 The following references can be found at www.cisco.com ..................................................... 33

11.3 Information regarding the FreeRADIUS server can be found at www.FreeRADIUS.org ............ 33
1. Introduction

These Application Notes describe the configuration of 802.1x Multi-Domain Authentication (MDA) on a Cisco Catalyst 3750 switch port, to support an Avaya 96xx SIP Telephone with an attached PC, where the PC is authenticated via 802.1x by the Cisco switch but the Avaya 96xx SIP Telephone is not. In addition, Cisco MAC Authentication Bypass (MAB) is discussed.

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 two types of port configurations for multiple devices connected to a single switch port: Multi-Host and Multi-Domain. In a Multi-Host configuration, the IP telephone authenticates the port. Any other device connected via the telephone (e.g., a PC) is unchallenged. This configuration presents obvious security issues. In a Multi-Domain configuration, each device connected to a switch port is challenged independently. The Catalyst 3750 switches are one of the Cisco platforms that support MDA.

As described above, an MDA port configuration challenges the IP telephone and an attached PC separately. However some network architectures specify that only the attached PC should be challenged via 802.1x. These Application Notes describe how to configure Avaya 2.0 96xx SIP telephones in such architectures.

Note – These Application Notes describe the provisioning required for MDA and MAB interoperability between a 2.0 Avaya 96xx SIP telephone, an attached PC, a Cisco 3725 Catalyst switch, and a FreeRADIUS authentication server.

Avaya Communication Manager, Avaya SIP Enablement Services (SES), Avaya SIP station provisioning, and DHCP provisioning are not discussed. For additional information on these topics see the references in Section 11.

1.1 Avaya 2.0 96xx SIP Telephone 802.1x Options

The Avaya 96xx SIP telephones support 802.1x authentication. By default these telephones use their MAC addresses as their username. There is no default password so one must be entered when challenged. Avaya 96xx SIP telephones support the receipt of Multicast and/or Unicast EAP frame formats.

The 2.0 Avaya 96xx SIP telephones supported the following 802.1x options. These options may be set via the Avaya 96xx SIP telephone keypad or via the 46xxsettings file (DOT1X and DOT1XSTAT options).

- **Pass-Thru** → The Avaya 96xx SIP telephone passes multicast EAPOL frames between the attached PC and the Authenticator. If the PC is disconnected, no disconnect notification is sent to the Authenticator. (DOT1X)
- **Pass-Thru with Logoff** → This is the same as Pass-Thru but if the PC is disconnected, a proxy EAPOL logoff is sent to the Authenticator. (DOT1X)
- **Pass-Thru - Off** → The phone does not pass any multicast EAPOL authentication
Information to the attached PC. **This mode should not be used in a Cisco MDA configuration.** *(DOT1X)*

- **Supplicant - On** → The telephone responds as a Supplicant to only Unicast challenges. *(DOT1XSTAT)*
- **Supplicant - On – Multicast** → The telephone responds as a Supplicant to either Unicast or Multicast challenges. *(DOT1XSTAT)*
- **Supplicant - Off** → The telephone does **not** respond as a Supplicant to either Unicast or Multicast challenges. *(DOT1XSTAT)*

1.2 Standard 802.1x MDA Authentication – IP Telephone and Attached PC

In a typical MDA configuration, the IP telephone and the attached PC are independently challenged and must request access to the network by specifying a username and password. Commonly the user name is the telephone MAC address. The password can be any string acceptable by the device. Authentication user names and passwords for each Supplicant device must be provisioned in the RADIUS server (see Section 6).

| Note | Some RADIUS servers (e.g., FreeRADIUS) are case sensitive when comparing authentication requests to their user data base entries (MAC addresses). If the Supplicant/Authenticator sends an identity MAC address with upper case letters (or lower case), the same case must be used when defining the user entry in the RADIUS. Otherwise the authentication will fail. |

802.1x authentication 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 shown in **Figure 1**.
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" packet to the authenticator.
4. The Authenticator forwards the "EAP-Response/Identity" information 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 forwards the challenge to the Supplicant.
7. The Supplicant responds to the challenge and the Authenticator passes the response to the Authentication Server.
8. If the Supplicant provides proper identity, the Authentication Server responds with a success message. This success message may contain additional access information (e.g., voice VLAN access) for the Authenticator.
9. The Authenticator passes the success message to the Supplicant and allows access to the LAN.
10. The Supplicant sends an EAPOL logoff to terminate the session.
11. An attached PC follows the same sequence.

The telephone and the attached PC are periodically re-authenticated by the switch. These re-authentications are processed internally by the telephone and PC and require no user intervention. Only after the telephone or PC has issued an EAPOL logoff, will they be re-authenticated.
challenged requiring user input. However if the attached PC is disconnected without issuing the EAPOL logoff, it is possible that a different PC could connect to the telephone and temporarily gain access to the network. Therefore some IP telephones offer an option to issue the EAPOL logoff on behalf of the disconnected PC (proxy logoff) using the PCs’ MAC address.

Switches can issue 802.1x challenges with either Unicast or Multicast based frames. Unicast frames will have the Supplicants’ MAC address as the destination. Multicast frames will typically use the reserved control frame MAC address 0180C2000003 as the destination. How, or if, Supplicants will respond to these formats is based on their supported configurations. The Cisco 3750 Catalyst switch uses Unicast for MDA configured ports.

The Authenticator device may require additional 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).

For additional information on Cisco’s implementation of 802.1x protocol, see [6] and [7]. For additional information on Avaya IP telephone configurations with Cisco MDA, see [5].

1.3 802.1x Authentication for an Attached PC Only

As described above, there may be network architectures where it is desirable for the IP telephones not to use typical 802.1x authentication, however 802.1x authentication is required for any PCs attached to the IP telephones. For these configurations the IP telephones are authenticated via other means and without user intervention. Additionally the IP telephones must be configured to ignore any EAPOL queries from the network (Supplicant function disabled).

These Application Notes describe a method supported by the Cisco 3750 Catalyst switch called MAC Authentication Bypass (MAB). The MAB authentication sequence is as follows.

1.3.1 MAC Authentication Bypass (MAB) Telephone Authentication

In Figure 2 below, an MAB authentication exchange is shown.
1. When MAB is configured on a MDA switch port, and an IP telephone is connected, the switch will attempt to establish an EAP identity from the telephone. Since the telephone is configured not to respond (see Section 7), these EAP Identity requests will time out.
2. When the switch detects any Ethernet packet from the telephone, it notes the telephones’ source MAC address.
3. The switch uses the MAC address of the telephone as its identity (and as its password) and sends this information to the RADIUS server. This differs from the standard Supplicant user name and password as described in Section 1.2.
4. If the RADIUS server has a matching user entry, the RADIUS sends the switch an accept frame containing any additional access information (e.g., voice VLAN access).
5. The switch authorizes the port for the telephone.

Note – As mentioned in Step 3 above, MAB uses the telephone MAC address as the user name and password when authenticating with the RADIUS server. If a telephone is reconfigured to be authenticated as a Supplicant, then the RADIUS server will need a user name/password entry for each authentication mode.

1.3.2 PC Authentication
When a PC is attached to a telephone authenticated with MAB, the PC still uses typical 802.1x authentication between the switch and the PC as described in Section 1.2.
2. Reference Configuration

These application notes used the reference configuration shown in Figure 3.

In the reference configuration, co-resident Avaya Communication Manager and SIP Enablement Services (SES) Edge/Home runs on an Avaya S8300C Server (ICC) installed in an Avaya G450 Media Gateway.

The G450 Media Gateway is provisioned as the network Dynamic Host Configuration Protocol (DHCP) server [4].

The Avaya 9640 SIP telephone and attached PC authenticate via the Cisco 3750 Catalyst switch and the FreeRADIUS server.

After authentication, the Avaya 9640 SIP telephone is first assigned a data VLAN IP address, instructed to switch to the voice VLAN, and then assigned a voice VLAN IP address by the
DHCP server. The DHCP server also directs the Avaya 9640 SIP telephone to the IP address of Avaya SIP Enablement Services Edge/Home for registration, as well as the address of the HTTP server for file/configuration updates.

When a PC is connected to the back of the Avaya 9640 SIP telephone, it is prompted for an 802.1x username and password by the Cisco Catalyst 3750, which is sent to the FreeRADIUS. If this authentication passes, the Cisco Catalyst 3750 allows the PC to access the data VLAN.

An Avaya 4621 H.323 telephone is also connected to the Cisco Catalyst 3750; however it uses a standard port configuration (no MDA) with no 802.1x authentication. The DHCP server directs the Avaya 4621 H.323 telephone to the IP address of Avaya Communication Manager for registration, as well as the address of the configuration server for file/configuration updates. The 4621 is included in the reference configuration as a call termination point.

3. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Network Component</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-resident Avaya Communication Manager and SIP Enablement Services Edge/Home</td>
<td>R015x.00.0.825.4</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>27.26.0</td>
</tr>
<tr>
<td>Avaya 4621 H.323 Telephone</td>
<td>a20d01b2_8.bin</td>
</tr>
<tr>
<td>Avaya 9640 SIP Telephone</td>
<td>2.0.1.34(5)</td>
</tr>
<tr>
<td>Avaya TFTPServer 2000</td>
<td>3.6.1</td>
</tr>
<tr>
<td>Cisco Catalyst 3750-24PS</td>
<td>c3750-ipservicesk9-mz.122-37.SE.bin</td>
</tr>
<tr>
<td>Microsoft Windows XP with 802.1x Authentication (PC attached to telephone)</td>
<td>Windows XP Professional 2002, SP2</td>
</tr>
<tr>
<td>Microsoft Windows 2000 Server (HTTP Server)</td>
<td>Service Pack 4</td>
</tr>
<tr>
<td>Red Hat Enterprise ES FreeRADIUS Server</td>
<td>R4</td>
</tr>
<tr>
<td>Wireshark Protocol Analyzer</td>
<td>V 0.99.5</td>
</tr>
</tbody>
</table>

Table 1: Reference Configuration Equipment List
4. Configure 802.1x Multi-Domain (MDA) and MAC Authentication Bypass (MAB) on the Cisco Catalyst 3750

The following section describes the configuration on the Cisco Catalyst 3750 to support 802.1x MDA (for the attached PC authentication) as well as MAB (for the Avaya 9640 SIP telephone authentication). Refer to [6] and [7] for more information.

**Note** – All commands are entered via a terminal session using Cisco CLI.

### 4.1 Authentication, Authorization & Accounting (AAA) and DOT1X activation

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>At the Cisco “&gt;” prompt enter <code>enable</code> and the enable password.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter <code>config t</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter <code>aaa new-model</code> – Enables the AAA access control.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter <code>aaa authentication dot1x default group radius</code> – This authentication first tries to contact a RADIUS server.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter <code>aaa authorization network default group radius</code> – Use user-RADIUS authorization for all network-related service requests.</td>
</tr>
<tr>
<td>6.</td>
<td>Enter <code>dot1x system-auth-control</code> – Enable IEEE 802.1x authentication globally on the switch.</td>
</tr>
</tbody>
</table>

Some default values will be added automatically by the switch. The configuration will appear as follows:

```
C3750-PoE#
!
aaa new-model
aaa authentication login default none  (aaa config default value).
aaa authentication dot1x default group radius
aaa authorization network default group radius .
aaa session-id common  (aaa config default value).
dot1x system-auth-control
```

Figure 4 – Cisco Catalyst 3750 AAA and DOT1X Activation
### 4.2 Network Interface configuration

The following commands define the Cisco switch interface to the Avaya 9640 SIP telephone (MDA and MAB authentication), the interface to the Avaya 4621 H.323 telephone (standard port access with no 802.1x authentication), the interface to the Avaya G450 Media Gateway, as well as the interface to the RADIUS server. The interface from the Cisco 3750 to the Avaya G450 Media Gateway is defined as an 802.1q Trunk so that traffic from VLAN 88 (voice) and VLAN 89 (data) can pass between them (see Section 5).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Enter</strong> <code>interface FastEthernet1/0/2</code> <strong>Interface for Avaya 9640 SIP phone</strong></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Enter</strong> <code>switchport mode access</code> → The port is set to access unconditionally and operates as a non-trunking, single VLAN interface.</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Enter</strong> <code>switchport access vlan 89</code> → Configure the interface as a static access port with the VLAN ID of the access mode VLAN (data VLAN).</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Enter</strong> <code>switchport voice vlan 88</code> → The VLAN to be used for voice traffic.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Enter</strong> <code>dot1x port-control auto</code> → 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.</td>
</tr>
<tr>
<td>6.</td>
<td><strong>Enter</strong> <code>dot1x host-mode multi-domain</code> → Enable MDA on a switch port.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Enter</strong> <code>dot1x reauthentication</code> → Enables periodic re-authentication of the client.</td>
</tr>
<tr>
<td>8.</td>
<td><strong>Enter</strong> <code>dot1x timeout reauth-period 60</code> → Set the number of seconds between re-authentication attempts.</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Enter</strong> <code>dot1x mac-auth-bypass</code> → Enables MAB for the Avaya 96xxSIP telephone.</td>
</tr>
<tr>
<td>10.</td>
<td><strong>Enter</strong> <code>exit</code> <strong>Interface to the Avaya 4621 H.323 phone</strong></td>
</tr>
<tr>
<td>11.</td>
<td><strong>Enter</strong> <code>interface FastEthernet1/0/4</code> <strong>Interface to the Avaya 4621 H.323 phone</strong></td>
</tr>
<tr>
<td>12.</td>
<td><strong>Enter</strong> <code>switchport mode access</code> → The port is set to access unconditionally and operates as a non-trunking, single VLAN interface.</td>
</tr>
<tr>
<td>13.</td>
<td><strong>Enter</strong> <code>switchport access vlan 89</code> → Configure the interface as a static access port with the VLAN ID of the access mode VLAN (data VLAN).</td>
</tr>
<tr>
<td>14.</td>
<td><strong>Enter</strong> <code>switchport voice vlan 88</code> → The VLAN to be used for voice traffic.</td>
</tr>
<tr>
<td>15.</td>
<td><strong>Enter</strong> <code>exit</code> <strong>Interface to the Avaya G450 Media Gateway</strong></td>
</tr>
<tr>
<td>16.</td>
<td><strong>Enter</strong> <code>interface FastEthernet1/0/12</code> <strong>Interface to the G450 Media Gateway</strong></td>
</tr>
<tr>
<td>17.</td>
<td><strong>Enter</strong> <code>switchport trunk encapsulation dot1q</code> → Set the encapsulation format on the trunk port to IEEE 802.1Q.</td>
</tr>
<tr>
<td>18.</td>
<td><strong>Enter</strong> <code>switchport trunk allowed vlan 88,89</code> → Set the port to trunk traffic for VLANs 88 (voice) and 89 (data).</td>
</tr>
<tr>
<td>19.</td>
<td><strong>Enter</strong> <code>switchport mode trunk</code> → Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface.</td>
</tr>
<tr>
<td>20.</td>
<td><strong>Enter</strong> <code>exit</code> <strong>Interface to the FreeRADIUS</strong></td>
</tr>
<tr>
<td>21.</td>
<td><strong>Enter</strong> <code>interface FastEthernet1/0/22</code> <strong>Interface to the FreeRADIUS</strong></td>
</tr>
<tr>
<td>22.</td>
<td><strong>Enter</strong> <code>switchport access vlan 89</code> → This configures access to the data VLAN.</td>
</tr>
</tbody>
</table>
23. Enter `exit`  

#######Voice VLAN 88 Interface#######

24. Enter `interface Vlan88`  

This creates the voice VLAN interface.

25. Enter `ip address 192.168.88.2 255.255.255.0`  

This configures the voice VLAN interface IP address.

26. Enter `exit`

#######Data VLAN 89 Interface#######

27. Enter `interface Vlan89`  

This creates the data VLAN interface.

28. Enter `ip address 192.168.89.2 255.255.255.0`  

This configures the data VLAN interface IP address.

29. Enter `exit`

#######Routing Information#######

30. Enter `ip default-gateway 192.168.89.1`  

IP address of the Avaya G450 Media Gateway.

31. Enter `exit`

Some default values will be added automatically by the switch. The configuration will appear as follows:

```bash
interface FastEthernet1/0/2
  description 96xx SIP phone
  switchport mode access
  switchport access vlan 89
  switchport voice vlan 88
  dot1x pae authenticator → (default dot1x value displayed by switch)
  dot1x port-control auto
  dot1x host-mode multi-domain
  dot1x reauthentication
  dot1x timeout reauth-period 60
  dot1x mac-auth-bypass
!
interface FastEthernet1/0/4
  description H.323 phone
  switchport mode access
  switchport access vlan 89
  switchport voice vlan 88
!
interface FastEthernet1/0/12
  description G450
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 88,89
  switchport mode trunk
  speed 100
duplex full
!
interface FastEthernet1/0/22
  description RADIUS
  switchport access vlan 89
```
4.3 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).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter <code>radius-server host 192.168.89.61 auth-port 1812 acct-port 1813 key 1234567890123</code> → This specifies the IP address of the FreeRADIUS, accounting and authorization UDP ports, and encryption key used between the FreeRADIUS and the Cisco switch.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter <code>radius-server source-ports 1645-1646</code> → This specifies the UDP ports used by the Cisco Catalyst 3750 to communicate with the RADIUS.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter <code>exit</code> → This leaves config t mode.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter <code>wr mem</code> → This command saves the configuration.</td>
</tr>
</tbody>
</table>

The configuration will appear as follows:

```
radius-server host 192.168.89.61 auth-port 1812 acct-port 1813 key 1234567890123
radius-server source-ports 1645-1646
```

Figure 6 – Cisco Catalyst 3750 RADIUS Configuration
5. Avaya G450 Media Gateway Interface Configuration

**Note** - Avaya Communication Manager, Avaya SIP Enablement Services (SES), Avaya SIP station provisioning, and DHCP provisioning are not discussed in these Application Notes. For additional information on these subjects refer to [2], [3], and [4].

As shown in Section 4.2, an 802.1q Trunk is defined between the Avaya G450 Media Gateway and the Cisco 3750 so that traffic from VLAN 88 (voice) and VLAN 89 (data) can pass between them. Ethernet port 10/3 was used in the reference configuration.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the Avaya G450 Media Gateway console interface using appropriate credentials.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter <strong>interface Vlan 89</strong> → Create interface VLAN 89 (data VLAN).</td>
</tr>
<tr>
<td>3.</td>
<td>Enter <strong>ip address 192.168.89.1 255.255.255.0</strong> → Set the IP address and mask for the interface VLAN 89.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter <strong>icc-vlan</strong> → Set interface VLAN 89 as connection to the Internal Call Controller (S8300c).</td>
</tr>
<tr>
<td>5.</td>
<td>Enter <strong>pmi</strong> → Set interface VLAN 89 as the primary management interface.</td>
</tr>
<tr>
<td>6.</td>
<td>Enter <strong>exit</strong> → leave interface VLAN 89 configuration.</td>
</tr>
<tr>
<td>7.</td>
<td>Enter <strong>interface Vlan 88</strong> → Create interface VLAN 88 (voice VLAN).</td>
</tr>
<tr>
<td>8.</td>
<td>Enter <strong>ip address 192.168.88.1 255.255.255.0</strong> → Set the IP address and mask for the interface VLAN 88.</td>
</tr>
<tr>
<td>9.</td>
<td>Enter <strong>exit</strong> → leave interface VLAN 89 configuration.</td>
</tr>
<tr>
<td>10.</td>
<td>Enter <strong>set port vlan 89 10/3</strong> → Set VLAN 89 as the native VLAN for interface 10/3.</td>
</tr>
<tr>
<td>11.</td>
<td>Enter <strong>set trunk 10/3 dot1q</strong> → Configure interface 10/3 as an 802.1q trunk.</td>
</tr>
<tr>
<td>12.</td>
<td>Enter <strong>set port static-vlan 10/3 89</strong> → Allow VLAN 89 traffic on the trunk.</td>
</tr>
<tr>
<td>13.</td>
<td>Enter <strong>set port static-vlan 10/3 88</strong> → Allow VLAN 88 traffic on the trunk.</td>
</tr>
<tr>
<td>14.</td>
<td>Enter <strong>set mgc list 192.168.88.19</strong> → Enter the IP address of Avaya Communication Manager that the Avaya G450 will register to.</td>
</tr>
<tr>
<td>15.</td>
<td>Enter <strong>copy run start</strong> → This saves the configuration.</td>
</tr>
</tbody>
</table>
The configuration will appear as follows:

```plaintext
interface Vlan 89
  ip address 192.168.89.1 255.255.255.0
  icc-vlan
  pmi
  exit

interface Vlan 88
  ip address 192.168.88.1 255.255.255.0
  exit

set port vlan 89 10/3

set trunk 10/3 dot1q

set port static-vlan 10/3 89

set port static-vlan 10/3 88

set mgc list 192.168.88.19
```

Figure 7 – Avaya G450 Media Gateway Interface Configuration

### 6. FreeRADIUS Configuration

**Note** - Refer to Section 11.3 for information on how to install and configure FreeRADIUS.

#### 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 4.3).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the FreeRADIUS console change to the <code>raddb</code> directory by entering; <code>cd /usr/local/etc/raddb</code></td>
</tr>
<tr>
<td>2.</td>
<td>Open the <code>clients.conf</code> file.</td>
</tr>
<tr>
<td>3.</td>
<td>Go to the bottom of the file and add the following entry; <code>Client 192.168.88.2/24 { secret = 1234567890123 shortname = C3750 NAS-IP-Address = 192.168.88.2 }</code></td>
</tr>
<tr>
<td>4.</td>
<td>Save and close the file.</td>
</tr>
</tbody>
</table>
6.2 Defining the Avaya 96xx SIP Telephone as a user

As described in Section 1.3.1, when MAB is used to authenticate the telephone, the Cisco switch uses the phone’s MAC address as the user ID and the password.

**Note** – All quote characters (") indicated below are required.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the FreeRADIUS console change to the <code>raddb</code> directory by entering; <code>cd /usr/local/etc/raddb</code></td>
</tr>
<tr>
<td>2.</td>
<td>Open the <code>users</code> file.</td>
</tr>
</tbody>
</table>
| 3.   | Go to the bottom of the file and add the following entry;  

```
xxxxxxxxxxxxx    User-Password == "xxxxxxxxxxxxx "  
Cisco-AVPair == "device-traffic-class=voice"
```

→ `xxxxxxxxxxxxx` is the MAC address of the phone. **Note** – The FreeRADIUS database is case sensitive. The upper or lower case letters entered here must match what is sent by the Suppliant/Authenticator.

→ The Cisco-AVPair line tells the Cisco Catalyst 3750 that this user (phone) can access the voice VLAN.

The following is an example of a completed phone user entry for MAB authentication.

```
00040de97552    User-Password == "00040de97552"  
Cisco-AVPair == "device-traffic-class=voice"
```

| 4.   | Save and close the file. |
6.3 Defining the PC as a user
If a PC will be attached to the phone, it must be defined in the FreeRADIUS as a user.

Note – All quote characters (") indicated below are required.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 == "zzzzzz"`  
      | `pcuser` is the User Name that must be entered on the PC 802.1x login window.  
      | `zzzzzz` is the password string that must be entered on the PC 802.1x login window.  
      | The following is an example of a completed MAB authenticated phone and an attached PC user list.  
      | `00040de97552    User-Password == "00040de97552"  
      | `Cisco-AVPair == "device-traffic-class=voice"  
      | `Jim             User-Password == "123456"`  
| 4.   | 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 9).
6.4.2 Restarting FreeRADIUS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | The active FreeRADIUS process must be identified. From the FreeRADIUS console enter; <br>

`ps  –ef  |  grep radiusd`

The console will show a display similar to the following; <br>

`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; <br>

`kill -9  9920`

3.   | Start FreeRADIUS again by entering; <br>

`radiusd  -X`

7. Configure 2.0 Avaya 9640 SIP Telephones for 802.1x MAB

When MAB is provisioned on a port (see Section 1.3.1), the Cisco switch will authenticate the telephone using the telephone MAC address for both the authentication user ID and password. In order for this to occur, the telephone must not respond to the EAP request sent by the switch when it detects that the telephone has been connected. This is accomplished by disabling the Supplicant function on the telephone. The 2.0 version of the Avaya 96xx SIP Telephone supports this option. Although this option can be set via the 46xxsettings file, for a MAB switch configuration, the Supplicant function must be disabled via the telephone keypad. Otherwise the switch will not allow the telephone to access the data VLAN and the HTTP server (where the 46xxsettings file resides).

Note – Options are selected on Avaya 96xx Telephones via the `soft-keys` or `navigation` buttons.
7.1 Disabling the 802.1x Supplicant Function on the 2.0 Avaya 9640 SIP Telephone

Perform the following steps after the Cisco 3750 switch port has been configured for MAB (See Section 4).

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect the 2.0 Avaya 9640 SIP Telephone to the Cisco 3750 port configured for MAB.</td>
</tr>
<tr>
<td>2.</td>
<td>Right after the 2.0 Avaya 9640 SIP Telephone boots, press the <em>Program</em> option on the phone.</td>
</tr>
<tr>
<td>3.</td>
<td>The phone will display <em>Enter Command</em>. Enter the <em>Craft</em> level login (see [1] for more information).</td>
</tr>
<tr>
<td>4.</td>
<td>Select the <em>802.1x</em> option.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| 5. | Change the *Supplicant* value to *Off*.
| 6. | If the *pass-thru* value is not set to *pass-thru mode on & proxy logoff*, follow the steps in **Section 7.2**. Otherwise proceed to **Step 7**. |
7. Select the **Save** option.

8. Select the **Exit** option. The phone will reboot.
7.2 Enabling the 802.1x Proxy Logoff Function on the 2.0 Avaya 9640 SIP Telephone

Proxy logoff allows the Avaya 9640 SIP telephone to issue an EAP logoff (using the attached PCs MAC address) should the PC disconnect without issuing a logoff.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Follow Steps 1–4 in Section 7.1.</td>
</tr>
<tr>
<td>2.</td>
<td>Set the <em>pass-thru</em> value to <em>pass-thru mode on &amp; proxy logoff</em>.</td>
</tr>
<tr>
<td>3.</td>
<td>If the <em>Supplicant</em> value is not set to <em>Off</em>, follow the steps in Section 7.1. Otherwise proceed to Step 4.</td>
</tr>
<tr>
<td>4.</td>
<td>Select the <em>Save</em> option.</td>
</tr>
<tr>
<td>5.</td>
<td>Select the <em>Exit</em> option. The phone will reboot.</td>
</tr>
</tbody>
</table>
8. Configure Windows XP Embedded 802.1x Authentication

When MDA is specified on the Cisco Catalyst 3750, a PC connected to the Avaya 9640 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 embedded 802.1x authentication process.

8.1 Enabling 802.1x Authentication on the PC

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Before connecting the PC to the Avaya IP telephone, go to <strong>Start ➔ Control Panel ➔ Network Connections</strong> and double-click the appropriate network interface.</td>
</tr>
</tbody>
</table>

![Network Connections](image)

- **Local Area Connection**: LAN or High-Speed Internet | Connected
- **ISDN Connection**: LAN or High-Speed Internet | Disabled
Step | Description
--- | ---
2. | From the Local Area Connection Status window select *Properties*.

<table>
<thead>
<tr>
<th>Local Area Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td><strong>Connection</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Activity</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

3. | From the Properties window select *Authentication*.

<table>
<thead>
<tr>
<th>Local Area Connection Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Connect using:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>This connection uses the following items:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>Allows your computer to access resources on a Microsoft network.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Show icon in notification area when connected</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Notify me when this connection has limited or no connectivity</strong></td>
</tr>
</tbody>
</table>

<p>| OK | Cancel |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>From the Authentication window, check the <em>Enable IEEE 802.1x authentication</em> box and set the EAP type to <em>MD5-Challenge</em>. &lt;br&gt;<img src="image" alt="Local Area Connection Properties" /></td>
</tr>
<tr>
<td>5.</td>
<td>Exit the interface configuration by clicking <em>OK</em>, <em>OK</em>, and <em>Close</em>. Then close the Network Connections window.</td>
</tr>
</tbody>
</table>

### 8.2 Authenticating the PC

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>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. &lt;br&gt;<img src="image" alt="Local Area Connection" /></td>
</tr>
<tr>
<td></td>
<td>Click on the message box (avoiding the “X” which will cancel the request).</td>
</tr>
</tbody>
</table>
2. The login dialog box will open. Enter the User Name and Password that was defined in the RADIUS (see Section 6) and click on OK (populate the Logon domain field if required).

9. Verification and Troubleshooting

9.1 Verification

The following actions can be taken to verify that MAB and MDA are working correctly.

9.1.1 Avaya 9640 SIP Telephone

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>After connecting to the Cisco 3750 MAB port (1/0/2 in the reference configuration), the Avaya 96x40 SIP telephone will boot, complete its DHCP server exchange, and register to Avaya SIP Enablement Services (SES).</td>
</tr>
<tr>
<td>2.</td>
<td>Verify dial-tone.</td>
</tr>
<tr>
<td>3.</td>
<td>Place a call and verify two-way talk path.</td>
</tr>
</tbody>
</table>

9.1.2 Attached PC

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Connect the PC to the back of the Avaya 9640 SIP telephone. The PC will prompt for a user name and password. Enter the PCs’ 802.1x user name and password that was provisioned in the RADIUS server.</td>
</tr>
<tr>
<td>2.</td>
<td>Verify that the PC can access the network.</td>
</tr>
</tbody>
</table>
9.1.3 Cisco Catalyst 3750 Switch

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the Cisco CLI enter the command <code>show dot1x interface fastethernet 1/0/2 detail</code>. The following information will be displayed.</td>
</tr>
</tbody>
</table>

```
C3750-PoE# show dot1x interface fastEthernet 1/0/2 detail

Dot1x Info for FastEthernet1/0/2
-----------------------------------
PAE                        = AUTHENTICATOR
PortControl                = AUTO
ControlDirection            = Both
HostMode              = MULTI_DOMAIN (port is set as MDA)
ReAuthentication            = Enabled
QuietPeriod                 = 60
ServerTimeout               = 30
SuppTimeout                 = 30
ReAuthPeriod                = 60 (Locally configured)
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30
RateLimitPeriod             = 0
Mac-Auth-Bypass             = Enabled (MAB is enabled on the port)
Inactivity Timeout          = None

Dot1x Authenticator Client List
-------------------------------
Domain                    = DATA (access to data VLAN)
Supplicant                = 0011.433d.9aa6 (PC MAC address)
  Auth SM State            = AUTHENTICATED (PC is authenticated)
  Auth BEND SM State       = IDLE
Port Status                = AUTHORIZED (PC is authorized on the port)
ReAuthPeriod               = 60
ReAuthAction               = Reauthenticate
TimeToNextReauth           = 9
Authentication Method      = Dot1x (PC was authenticated via 802.1x)
Authorized By              = Authentication Server (FreeRADIUS)
Vlan Policy                = N/A

Domain                    = VOICE (access to voice VLAN)
Supplicant                = 0004.0dee.7664 (9640 MAC address)
  Auth SM State            = AUTHENTICATED (9640 is authenticated)
  Auth BEND SM State       = REQUEST
Port Status                = AUTHORIZED (9640 is authorized on the port)
ReAuthPeriod               = 60
ReAuthAction               = Reauthenticate
TimeToNextReauth           = 0
Authentication Method      = MAB (9640 was authenticated via MAB)
Authorized By              = Authentication Server (FreeRADIUS)
```

Figure 8 – Cisco 3750 Port Monitor
9.1.4 Monitoring Phone and PC Authentication on the FreeRADIUS Server

The following messages display on the FreeRADIUS console for every 802.1x or MAB authentication request.

9.1.4.1 MAB - Avaya 96xx SIP Telephone

In the example shown in Figure 9, the Cisco 3750 (192.168.88.2) does a MAB authorization request for the Avaya 9640 SIP telephone (MAC address 00040dEE7674) to the FreeRADIUS server.

```bash
###rad_recv: Access-Request packet from host 192.168.88.2:1645, id=235, length=138
   User-Name = "00040dee7664"
   User-Password = "00040dee7664"
   Service-Type = Call-Check
   Framed-MTU = 1500
   Called-Station-Id = "00-0F-8F-CE-4B-84"
   Calling-Station-Id = "00-04-0D-EE-76-64"
   Message-Authenticator = 0xf978e939025f980ce0dc4304f46551f3
   NAS-Port-Type = Ethernet
   NAS-Port = 50102
   NAS-IP-Address = 192.168.88.2

Processing the authorize section of radiusd.conf

modcall: entering group authorize for request 25579
   modcall[authorize]: module "preprocess" returns ok for request 25579
   modcall[authorize]: module "chap" returns noop for request 25579
   modcall[authorize]: module "mschap" returns noop for request 25579
   rlm_realm: No '@' in User-Name = "00040dee7664", looking up realm NULL
   rlm_realm: No such realm "NULL"
   ## modcall[authorize]: module "suffix" returns noop for request 25579
   rlm_eap: No EAP-Message, not doing EAP
   modcall[authorize]: module "eap" returns noop for request 25579
   # users: Matched entry 00040dee7664 at line 138
   modcall[authorize]: module "files" returns ok for request 25579
   modcall: leaving group authorize (returns ok) for request 25579

#auth: type Local
auth: user supplied User-Password matches local User-Password
Sending Access-Accept of id 235 to 192.168.88.2 port 1645
   #Cisco-AVPair == "device-traffic-class=voice"
Finished request 25579
```

**Figure 9 – FreeRADIUS/Cisco 3750 MAB Authentication for Avaya 9640 SIP Telephone**
9.1.4.2 PC Attached to the Avaya 9640 SIP Telephone – 802.1x Authentication

In the example shown in Figure 10, the Cisco 3750 (192.168.88.2) does an 802.1x authorization request to the FreeRADIUS server for the PC (MAC address 0011433d9aa6) attached to the Avaya 9640 SIP telephone.

```
rad_recv: Access-Request packet from host 192.168.88.2:1645, id=238, length=156
   User-Name = "jim"
   Service-Type = Framed-User
   Framed-MTU = 1500
   Called-Station-Id = "00-0F-8F-CE-4B-84"
   Calling-Station-Id = "00-11-43-3D-9A-A6"
   EAP-Message = 0x020400190410637ab1cf4b99bf1365532e89b7a9e11f6a696d
   Message-Authenticator = 0x5db1378b8696aec0924a3852533021d7
   NAS-Port-Type = Ethernet
   NAS-Port = 50102
   State = 0x420e237b9314f6686df60af4a379fe6
   NAS-IP-Address = 192.168.88.2
Processing the authorize section of radiusd.conf
modcall: entering group authorize for request 25584
modcall[authorize]: module "preprocess" returns ok for request 25584
modcall[authorize]: module "chap" returns noop for request 25584
modcall[authorize]: module "mschap" returns noop for request 25584
   rlm_realm: No '@' in User-Name = "jim", looking up realm NULL
   rlm_realm: No such realm "NULL"
modcall[authorize]: module "suffix" returns noop for request 25584
rlm_eap: EAP packet type response id 4 length 25
   rlm_eap: No EAP Start, assuming it's an on-going EAP conversation
modcall[authorize]: module "eap" returns updated for request 25584
   users: Matched entry jim at line 144
modcall[authorize]: module "files" returns ok for request 25584
modcall: leaving group authorize (returns updated) for request 25584
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 25584
rlm_eap: Request found, released from the list
rlm_eap: EAP/md5
   rlm_eap: processing type md5
   rlm_eap: Freeing handler
modcall[authenticate]: module "eap" returns ok for request 25584
modcall: leaving group authenticate (returns ok) for request 25584
Sending Access-Accept of id 238 to 192.168.88.2 port 1645
   EAP-Message = 0x03040004
   Message-Authenticator = 0x00000000000000000000000000000000
   User-Name = "jim"
Finished request 25584
```

Figure 10 – FreeRADIUS/Cisco 3750 802.1x Authentication for PC Attached to the Avaya 9640 SIP Telephone
### 9.2 Troubleshooting

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

#### 9.2.1 Cisco Catalyst 3750

The Cisco 3750 Catalyst switch can be used to examine the traffic between itself, the Avaya 9640 SIP telephone, the attached PC, and the RADIUS server.

##### 9.2.1.1 Port Monitor to Protocol Analyzer

Traffic on the Cisco 3750 port connected to the telephone and attached PC can be monitored by a protocol analyzer connected to a different port. In the reference configuration Wireshark protocol analyzer software was used. The Avaya 9640 SIP telephone and the attached PC were connected to switch port 1/0/2. A PC running Wireshark was connected to switch port 1/0/24. Traffic between the Cisco switch and the RADIUS server can be monitored in a similar fashion.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the Cisco CLI enter the command <code>config t</code>.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter <code>monitor session 1 source interface Fa1/0/2</code> This sets the source traffic to be monitored.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter <code>monitor session 1 destination interface Fa1/0/24 encapsulation replicate</code> This sets the destination of the monitored traffic.</td>
</tr>
<tr>
<td>4.</td>
<td>The “no” form of these commands is used to disable monitoring.</td>
</tr>
</tbody>
</table>

##### 9.2.1.2 Debug dot1x all

The `debug dot1x all` Cisco CLI command will display all MDA and MAB transactions on the Cisco Catalyst 3750. Use the command `no debug dot1x all` to disable the debug output.

**Note** - The output from this command can be substantial. Therefore for brevity, only lines that verify operation are included.

##### 9.2.1.2.1 Avaya 9640 SIP Telephone (MAC address 00040dee7664) MAB Authentication

```
2d19h: dotlx-ev:FastEthernet1/0/2:Sending EAPOL packet to 0004.0dee.7664
2d19h: dotlx-ev:dotlx_mgr_send_eapol: Sending out EAPOL packet on FastEthernet1/0/2
2d19h: dotlx-ev:Received an EAP Timeout on FastEthernet1/0/2 for mac 0004.0dee.7664
2d19h: dotlx-sm:Posting AUTH_TIMEOUT on Client=3C4778C
2d19h: dotlx_auth Fal/0/2: auth_authenticating -> auth_fallback
2d19h: dotlx_auth_mab : initial state mab_initialize has enter
2d19h: dotlx_auth_mab : during state mab_initialize, got event 1(mabContinue)
2d19h: dotlx_auth_mab : mab_initialize -> mab_authorizing
2d19h: dotlx_auth_mab : during state mab_authorizing, got event 3(mabResult)
2d19h: dotlx_auth_mab : mab_authorizing -> mab_terminate
2d19h: dotlx-sm:Posting AUTH_SUCCESS on Client=3C4778C
2d19h: dotlx-ev:dotlx_switch_supplicant_add:Adding 0004.0dee.7664 on FastEthernet1/0/2 in vlan 88, domain is VOICE
```

**Figure 11 – Cisco Catalyst 3750/Avaya 9640 SIP Telephone MAB Authentication**
### 9.2.1.2.2 Attached PC (MAC address 0011433d9aa6) MDA Authentication

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2d19h</td>
<td>dot1x-ev:dot1x_mgr_send_eapol: Sending out EAPOL packet on FastEthernet1/0/2</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-ev:Received an EAPOL frame on interface FastEthernet1/0/2</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-ev:Received pkt saddr =0011.433d.9aa6 , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0019</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-packet:Received an EAP packet on the FastEthernet1/0/2 from mac 0011.433d.9aa6</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-packet:Received an EAP Success on the FastEthernet1/0/2 for mac 0011.433d.9aa6</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-sm:Posting EAP_SUCCESS on Client=3B968E4</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-switch_authc_success called on interface FastEthernet1/0/2</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-sm:Posting AUTHC_SUCCESS on Client=3B968E4</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-ev:dot1x_vlan_assign_authc_success called on interface FastEthernet1/0/2</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-ev:dot1x_switch_supplicant_add: Adding 0011.433d.9aa6 on FastEthernet1/0/2 in vlan 89, domain is DATA</td>
</tr>
<tr>
<td>2d19h</td>
<td>dot1x-ev:dot1x_switch_port_vp_authorized: Setting FastEthernet1/0/2 to AUTHORIZED</td>
</tr>
</tbody>
</table>

*Figure 12 – Cisco Catalyst 3750/Attached PC MDA Authentication Sequence*

### 9.2.2 Restarting the FreeRADIUS Server

Whenever configuration changes are made to the FreeRADIUS databases (adding, modifying or removing a client or user), the FreeRADIUS must be restarted.

#### 9.2.2.1 Stopping and Restarting FreeRADIUS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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` |

The `radiusd -X` command not only starts the FreeRADIUS, it also displays all authentication requests and replies on the FreeRADIUS console.
10. Conclusions

As illustrated in these Application Notes, 2.0 Avaya 96xx SIP Telephones with attached PCs can support separate authentication states via the Cisco Catalyst 3750 ports configured for Multi-Domain Authentication (MDA). The Cisco Catalyst 3750 uses MAC Authentication Bypass (MAB) to authenticate the 2.0 Avaya 96xx SIP Telephones instead of the standard 802.1x Supplicant processing. However a PC attached to the 2.0 Avaya 96xx SIP Telephones, is authenticated via 802.1x processes. A FreeRADIUS server is used to process both types of authentication requests. The FreeRADIUS authentication can also authorize the 2.0 Avaya SIP Telephone to access the voice VLAN, while the attached PC is only authorized to access the data VLAN.

11. References

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


[5] Configuring Cisco 802.1x Multi-domain Authentication (MDA) on a Cisco Catalyst 3750, with Avaya 96xx and 46xx IP Telephones - Issue 1

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

[6] Catalyst 3750 Switch Software Configuration Guide, 12.2(37)SE, OL-8550-03, Chapter 10, Configuring IEEE 802.1x Port-Based Authentication


11.3 Information regarding the FreeRADIUS server can be found at www.FreeRADIUS.org
©2008 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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com