



Avaya Solution & Interoperability Test Lab

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

Abstract

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. 802.1X provides a means of authenticating and authorizing users attached to a LAN port as well as preventing access to that port in cases where the authentication process fails. The Cisco Catalyst 6509 Switch supports 802.1X as an authenticator and the Avaya 9620 IP Telephone supports 802.1X as a Supplicant, both Pass-thru Mode and Pass-thru Mode with Proxy Logoff. These Application Notes provide the steps necessary to configure 802.1X on the Cisco Catalyst 6509 Switch and the Avaya 9620 IP Telephone with an attached PC using Cisco Secure Access Control Server (ACS). In the sample configuration, the Avaya 9620 IP Telephone functions as the Supplicant and the attached PC is then able to access the enterprise network without the need for individual authentication.

1 Introduction

The 802.1X protocol is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control LAN access, and apply traffic policy, based on user or endpoint identity. 802.1X consists of three components (or entities):

- **Supplicant** – a port access entity (PAE) that requests access to the network. For example, an Avaya IP Telephone and the attached PC can be configured to support 802.1X supplicants.
- **Authenticator** – a PAE that facilitates the authentication of the supplicant. Cisco Catalyst switches function as authenticator PAEs that control the physical access to the network based on the authentication status of a supplicant.
- **Authentication Server** – a PAE, typically a Remote Authentication Dial-In User Service (RADIUS) server, which actually provides authentication service.

802.1X makes use of the Extensible Authentication Protocol (EAP). The EAP implementation in 802.1X is called EAP encapsulation Over LANs (EAPOL). It is currently defined for Ethernet-like LANs including 802.11 Wireless. The authenticator becomes the middleman for relaying EAPOL messages in 802.1X packets to an authentication server by using the RADIUS format to carry the EAP information.

In a typical EAP-MD5 (Extensible Authentication Protocol-Message Digest 5) message exchange for the 802.1X protocol, the authenticator or the supplicant can initiate authentication. When the switch detects a port link state transition from down to up, the switch will send an EAP-request/identity frame to the client to request its identity. When the client receives the frame, it responds with an EAP-response/identity frame. If the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity. **Figure 1** shows typical flow of messages for a supplicant (such as an Avaya IP Telephone or attached PC), an authenticator (such as a Cisco Catalyst 6509 switch) and an authentication server (such as a Cisco Secure ACS) using the EAP-MD5 authentication.

Avaya 9620 IP Telephones can prompt the user for a username and password, which can then be stored in the telephone. For example, the user may be prompted for a username and password if the username and password have never been entered in the phone, if the phone has been reset to the manufacturer's default values, or if the authentication server rejects the current username and password. The default username provided is the phone's MAC address¹. (There is no default password; it must be entered if one has not been stored from a previous authentication request.) Once entered, the phone will save the username and password, and the saved values will be re-used (without prompting the user) when the phone is restarted.

¹ Usernames can be defined in the authentication server as any unique string.

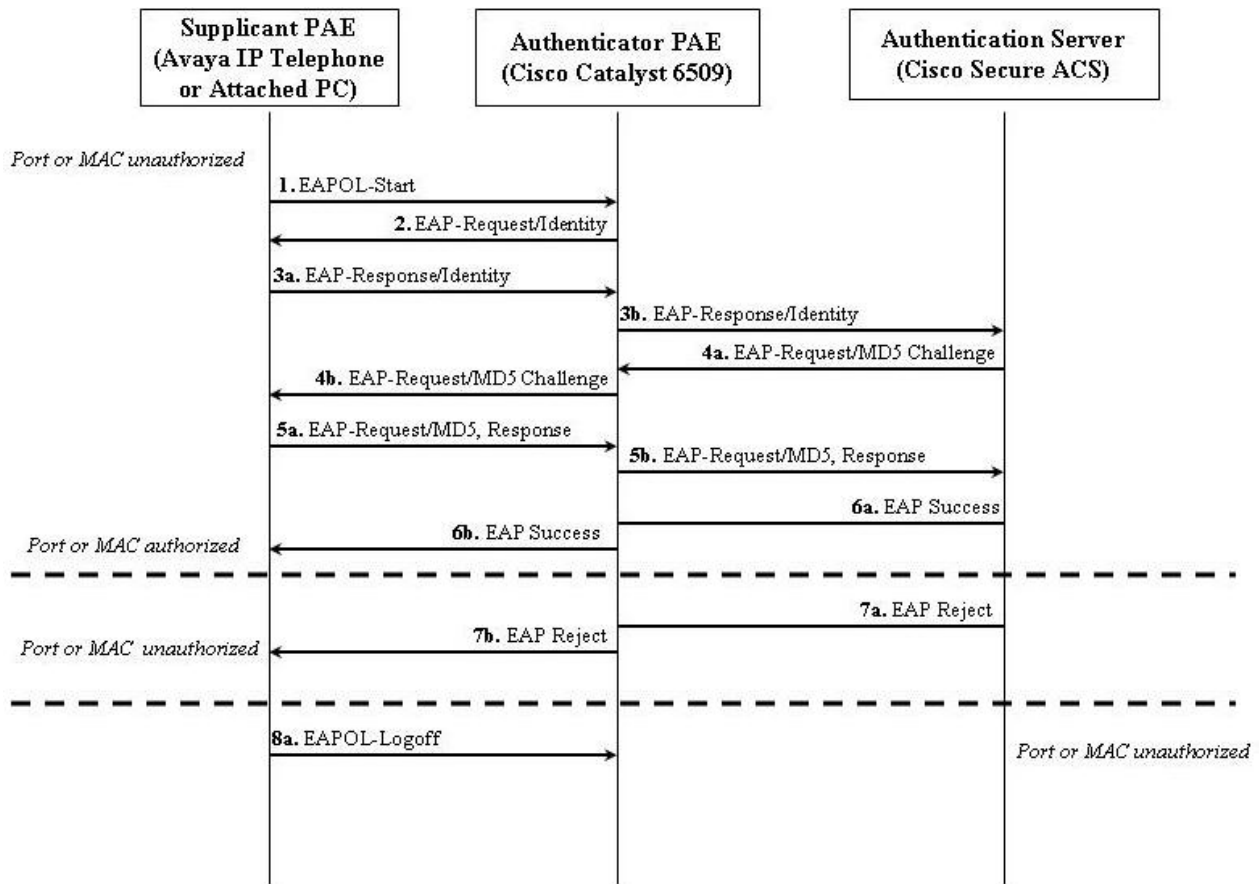


Figure 1: 802.1X Message Exchanges

The following describes the flow of 802.1X messages shown in **Figure 1** and replicated in the verification of these Application Notes:

1. The supplicant sends an “EAPOL Start” packet to the authenticator (a Cisco Catalyst 6509 switch). If the Avaya 9620 IP Telephone is in Supplicant Mode, it will ignore the “EAP-Request/Identity” frames from the Cisco Catalyst 6509 switch during its booting process.
2. The authenticator responds with an “EAP-Request/Identity” packet to the supplicant.
3. The supplicant responds with an "EAP-Response/Identity" packet to the authenticator (3a). The authenticator strips the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server (A Cisco Secure ACS) (3b).
4. The authentication server recognizes the packet as an EAP-MD5 type and sends back a Challenge message to the authenticator (4a). The authenticator removes the

authentication server's frame header, encapsulates the remaining EAP frame into the EAPOL format, and sends it to the supplicant (4b).

5. The supplicant responds to the Challenge message (5a) and the authenticator passes the response onto the authentication server (5b).
6. If the supplicant provides proper identification, the authentication server responds with a Success message (6a). The authenticator passes the message onto the supplicant (6b) and allows access to the LAN.
7. If the supplicant does not provide proper identification, the authentication server responds with a Reject message (7a). The authenticator passes the message onto the supplicant (7b) and blocks access to the LAN.
8. When the supplicant is disabled or reset, the supplicant sends an EAPOL-Logoff message, which prompts the authenticator to block access to the LAN.

For the configuration primarily addressed in this document, EAP-MD5 authentication was used on the Cisco Catalyst 6509 switch, Cisco Secure ACS, and Avaya 9620 IP Telephones. The settings that define this configuration, and the resulting behavior, are summarized as follows:

Avaya 9620 IP Telephone Settings		Cisco Catalyst 6509 Authentication Mode	Behavior
802.1X Mode	PC Port		
Supplicant	Enabled	Multi-Host	Phone authenticates port; attached PC can access network without the need for authentication

Figure 2 shows the network diagram used in these Application Notes.

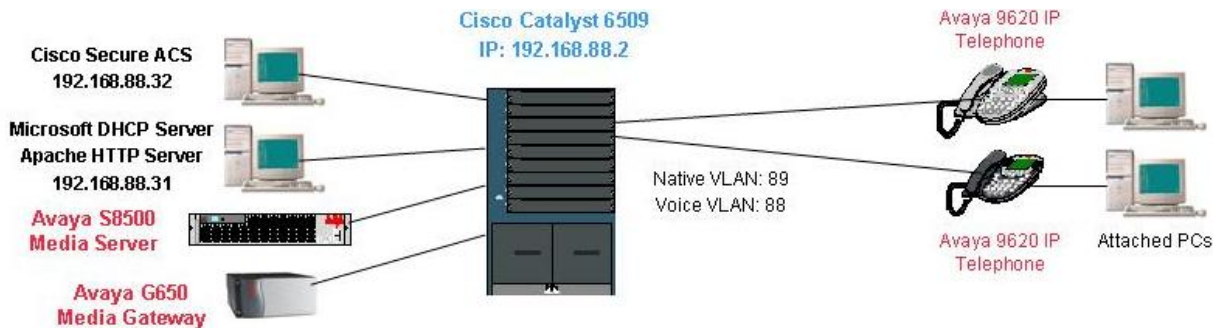


Figure 2 – 802.1X Configuration with Avaya 9620 IP Telephones

2 Equipment and Software Validated

Table 1 shows the versions verified in these Application Notes.

Equipment	Software
Avaya Communication Manager Avaya S8500 Media Server	3.1.1 (load 628.7)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MEDPRO (TN2302AP)	HW12 FW030 HW01 FW017 HW11 FW108
Avaya 9620 IP Telephone	1.00
Cisco Catalyst 6509 WS-F6K-GE48-AF (PoE module)	CatOS 8.5(3)
Microsoft Windows 2000 Server	Service Pack 4
Cisco Secure Access Control Server (ACS)	4.0
Microsoft Windows XP Professional	Version 2, Service Pack 2
Funk Odyssey Client	4.30

Table 1: Equipment and Software Validated

3 Configure DHCP for Avaya IP Telephones

Table 2 summarizes the Dynamic Host Configuration Protocol (DHCP) configuration. The following describes how the Avaya 9620 IP Telephone works with the DHCP server after the 802.1X authentication succeeds.

Consider the example of Avaya 9620 IP Telephones and computers configured for DHCP in **Figure 2**. If the Avaya 9620 IP Telephone is set to the manufacturer’s default configuration, it will send a clear DHCP request initially. The Cisco Catalyst 6509 Switch port connected to the Avaya 9620 IP Telephone is configured with both a native VLAN ID 89 and auxiliary (voice) VLAN ID 88 for the port. The clear DHCP request will be associated with the native VLAN 89 on the port. The Cisco Catalyst 6509 switch is configured with the router interface on that VLAN, which has IP address 192.168.89.1. When the router interface relays the DHCP request to the configured DHCP server 192.168.88.31, the DHCP server associates this request with the 192.168.89.0 scope and returns a reply with an Option 242 string of “L2QVLAN=88,”, instructing the requestor to enable 802.1Q tagging with VLAN ID 88. The Avaya 9620 IP Telephone receiving this reply will release the supplied IP address and issue a new DHCP request with VLAN ID 88. This request will be associated with the voice VLAN on the port. The DHCP server associates this request with scope 192.168.88.0 and replies with an IP address from that scope as well as several parameters in Option 242.

When the attached PC issues a DHCP request, it will send a clear DHCP request. This request will be served in the same way as the initial request from the phone. However, the computer will ignore Option 242 values specifying a new VLAN because this option is Avaya-specific and is assumed not to be used by non-Avaya devices. Therefore, no new DHCP request is issued.

If 802.1X is enabled on the Cisco Catalyst 6509 switch ports with connected Avaya 9620 IP Telephones with an attached PC, the Cisco Catalyst 6509 switch must allow forwarding of traffic from the Avaya 9620 IP Telephones on the native VLAN and voice VLAN. If port security is enabled on these ports, the maximum number of secure MAC addresses must be set to 3 (the PC’s MAC on the native VLAN, the phone’s MAC on the native VLAN and the phone’s MAC on the voice VLAN).

DHCP Scope	Option 3 Router	Option 242 String	Notes
192.168.88.0	192.168.88.1	MCIPADD=192.168.88.22,HTTPSRVR=192.168.88.31	For Voice VLAN
192.168.89.0	192.168.89.1	L2QVLAN=88	For native VLAN

Table 2 – DHCP Configuration Summary

NOTE: When the Avaya 9620 IP Telephone uses one of the two Pass-thru Modes, the DHCP server only needs to be configured with the DHCP option for the voice VLAN. An administrator must configure the Avaya 9620 IP Telephone manually to use the voice VLAN so that it issues a DHCP request only on the voice VLAN.

4 Configure 802.1X on the Cisco Catalyst 6509

The following shows the annotated global RADIUS and 802.1X configuration. The RADIUS authentication secret **must** match the shared key on the Cisco Secure ACS in **Section 5**. When 802.1X is globally enabled, the Cisco Secure ACS will be used for the 802.1X authentication. For more information on configuring the Cisco Catalyst 6509 switch, see [4].

```
! --- Configure radius server
Console> (enable) set radius server 192.168.88.32 primary
192.168.88.32 with auth-port 1812 acct-port 1813 added to radius server
table as primary server

! --- Configure radius authentication secret
Console> (enable) set radius key cisco
Radius key set to cisco

! --- Globally enable the radius authentication
Console> (enable) set dot1x system-auth-control enable
dot1x system-auth-control enabled.
Configured RADIUS servers will be used for dot1x authentication
```

Use the command **show radius** to verify the RADIUS configuration.

```
console> (enable) show radius
Active RADIUS Server           : 192.168.88.32
RADIUS Deadtime                 : 0 minutes
RADIUS Key                     : cisco
RADIUS Retransmit               : 2
RADIUS Timeout                  : 5 seconds
Framed-IP Address Transmit      : Disabled
RADIUS Framed MTU               : 1000 bytes

RADIUS-Server                   Status  Auth-port  Acct-port  Resolved IP
Address
-----
192.168.88.32                 primary 1812     1813
```

Use the command **show dot1x** to verify the 802.1X configuration.

```
Console> (enable) show dot1x
PAE Capability           Authenticator Only
Protocol Version        1
system-auth-control     enabled
max-req                 2
max-reauth-req          2
quiet-period            60 seconds
radius-accounting       disabled
radius-vlan-assignment  enabled

radius-keepalive state  enabled
re-authperiod           3600 seconds
server-timeout          30 seconds
shutdown-timeout        300 seconds
supp-timeout            30 seconds
tx-period               30 seconds
```

The Cisco Catalyst 6509 switch can control the port authorization state. Three control modes can be configured on a port:

- **Force-authorized** – Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. This is the default setting.
- **Force-unauthorized** – Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.
- **Auto** – Enables 802.1X port-based authentication. Whether the port is in the authorized state or the unauthorized state depends on the authentication result. This is the control mode used in the configuration described in these Application Notes.

By default, all ports are configured in the force-authorized mode. The command **set port dot1x port-control** can be used to configure a port in the **force-unauthorized**, **auto** or **force-authorized** mode. It is highly recommended to configure all ports connected to the Avaya 9620 IP Telephones or the PCs in auto mode in order to ensure that only authorized users can access switch ports. The ports connected to the servers, including the Microsoft DHCP server and the Avaya S8500 Media Server in **Figure 1**, are left in force-authorized mode. The following screen shows that ports 7/1 and 7/2 connected to phones are configured in auto mode.

```
Console> (enable) set port dot1x 7/1-2 port-control auto
Ports 7/1-2 dot1x port-control is set to auto.
Trunking disabled for ports 7/1-2 due to Dot1x feature.
Spantree port fast start option enabled for ports 7/1-2.
```


The Cisco Catalyst 6509 switch running Cisco CatOS software supports three modes of authentication: Single-host, Multi-host and Multiple Authentication. The Cisco Catalyst 6509 switch uses a well-known Multicast MAC address 01:80:C2:00:00:03 for all EAPOL messages for the Single-host and Multi-host modes. Note that 802.1X is not supported on a trunk port.

- **Single-host** – In this mode, a port is only allowed to support one 802.1X client on its primary VLAN. Other workstations on that port will be blocked. Single-host mode cannot support an IP Telephone with an attached PC.

Multi-host - For the Cisco Catalyst 6509 switch running Cisco CatOS software, when a port is configured with an auxiliary VLAN and a native VLAN, the 802.1X authentication only applies to the native VLAN, and the auxiliary VLAN will bypass the 802.1X. This is the mode of authentication used in the configuration described in these Application Notes.

- **Multiple Authentication** – Multiple Authentication mode is only supported on the Cisco CatOS software and is a Cisco proprietary protocol. This mode allows multiple dot1x-hosts on a port and every host is authenticated separately. Since Multiple Authentication mode does not support an auxiliary VLAN, the Avaya 9620 IP Telephone and an attached PC could not be put in different VLANs in this case, although they may be authenticated individually. This mode is not covered in these Application Notes.

By default, 802.1X Multi-host mode is disabled. Use the command **set port dot1x <port#> multiple-host enable** to enable 802.1X Multi host mode on the specified ports.

```
Console> (enable) set port dot1x 7/1-2 multiple-host enable
Ports 7/1-2 Multiple-host option enabled.
```

The following screen shows that a native VLAN 89 and an auxiliary VLAN 88 are configured on ports 7/1 and 7/2. The native VLAN will be used for the attached PCs and the auxiliary VLAN 88 used for the Avaya 9620 IP Telephones.


```
Console> (enable) set vlan 89 7/1-2
console> (enable) set port auxiliaryvlan 7/1-2 88
```

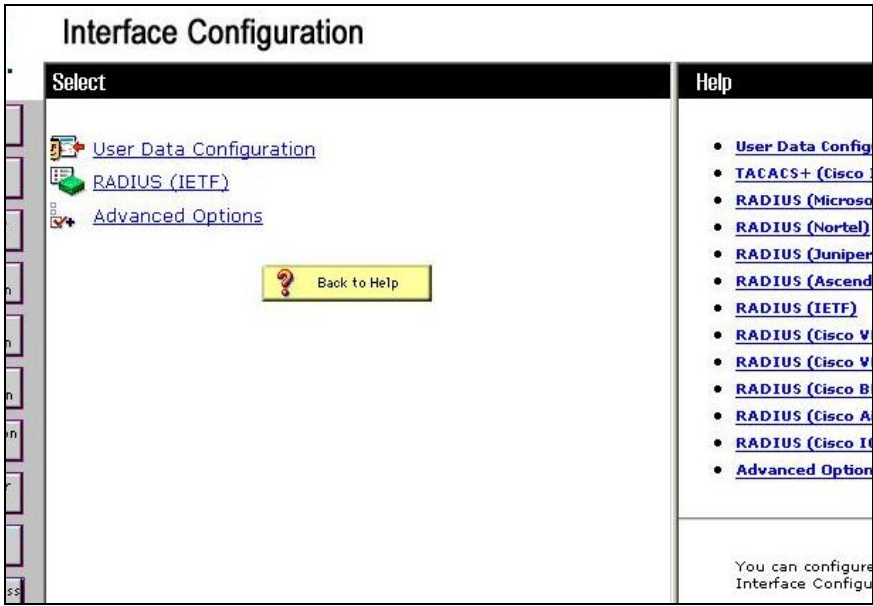
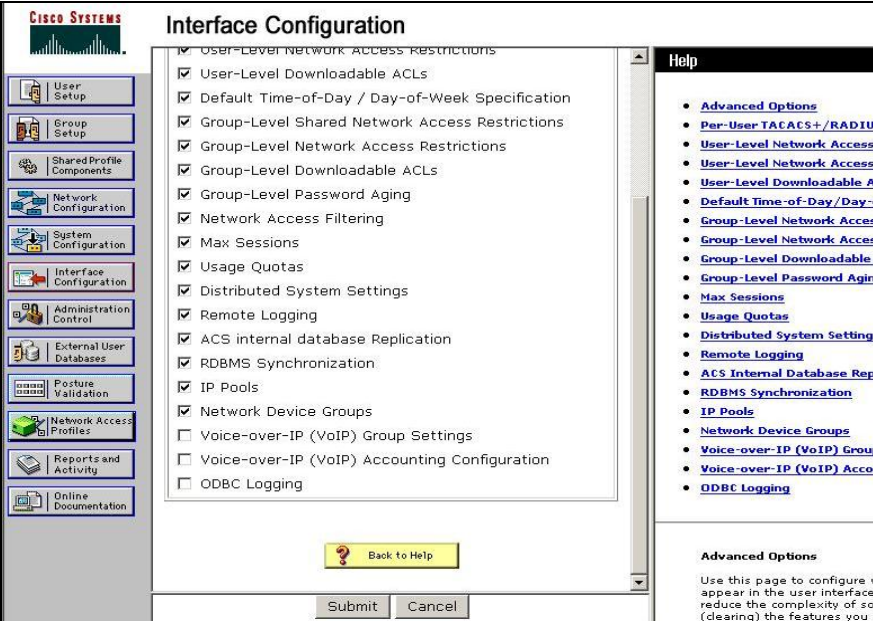
By default, re-authentication is not enabled. It is recommended to enable re-authentication for high security. The default re-authentication period is 1 hour. Re-authentication does not have any impact on the phone's operation as long as the phone can provide the correct credentials.

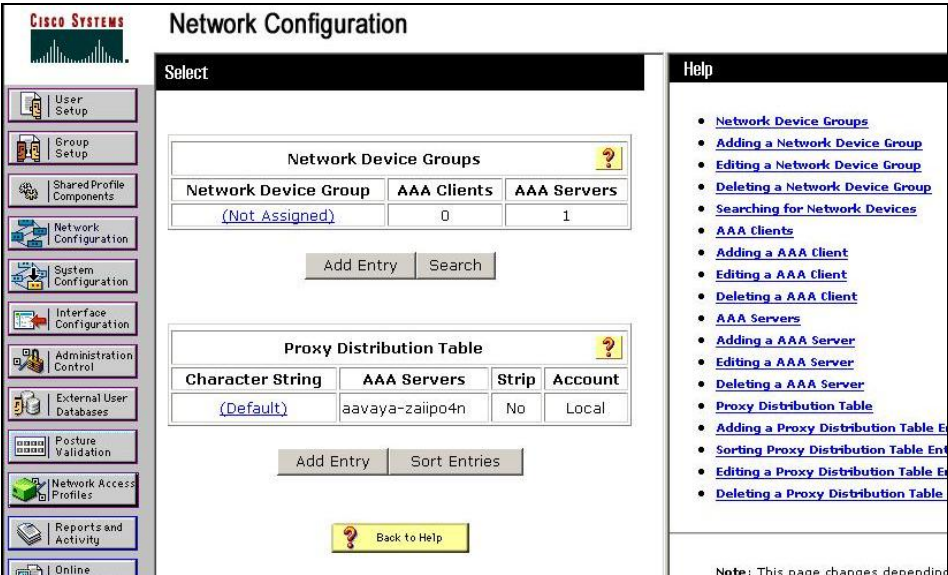
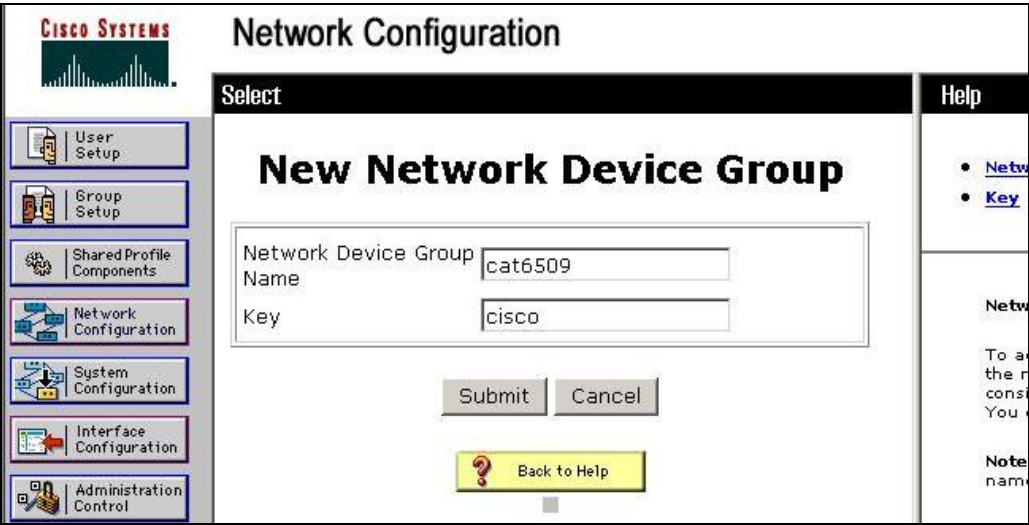
```
Console> (enable) set port dot1x 7/1-2 re-authentication enable
Ports 7/1-2 Dot1x re-authentication enabled
```

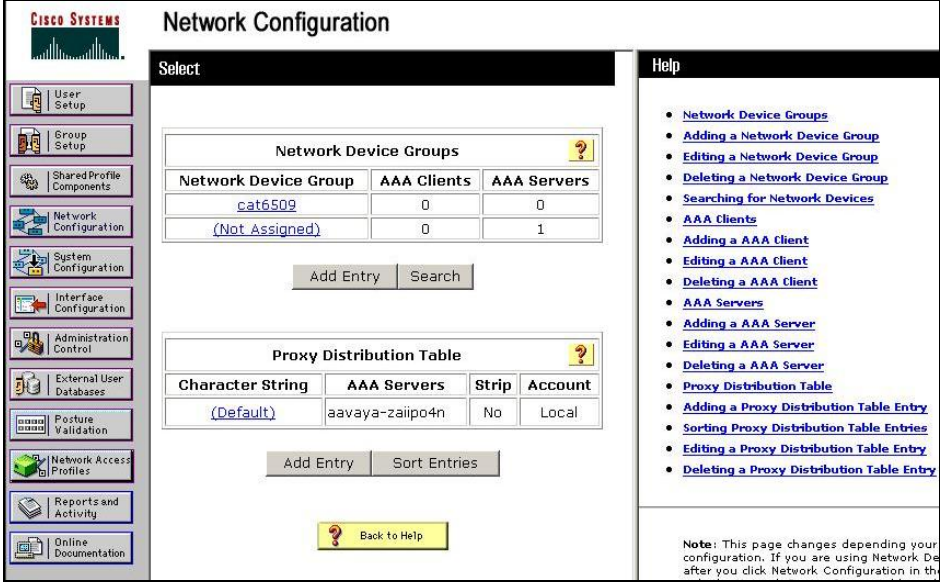
5 Configure the Cisco Secure ACS

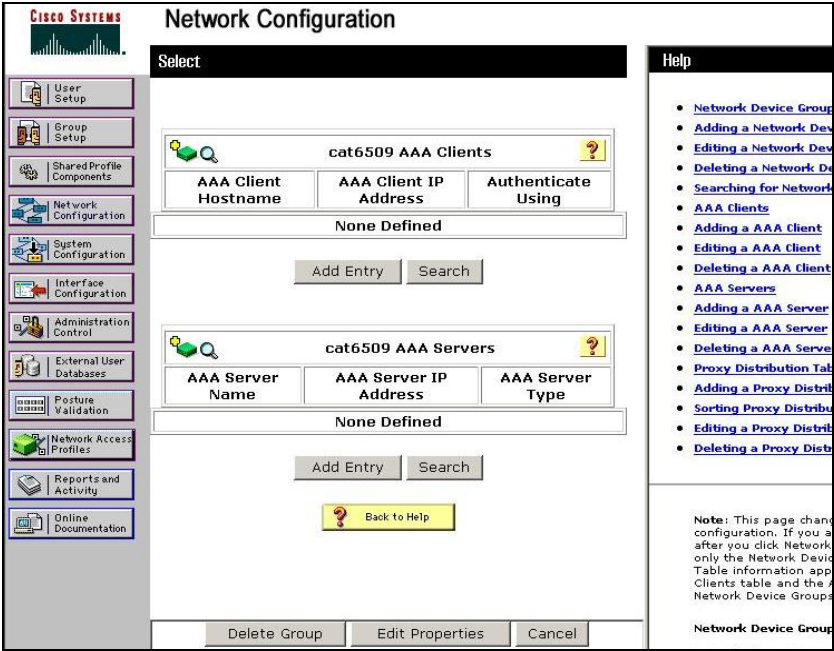
This section describes the steps for configuring the Cisco Secure ACS to accept the Cisco Catalyst 6509 switch as an AAA client and the Avaya 9620 IP Telephones as users requesting authentication. For additional configuration information, see [5].

Step	Description
1.	<p>Launch the Cisco Secure ACS browser-based administration tool. The following screen appears.</p> 

Step	Description
2.	<p>From the left panel, select Interface Configuration. The following screen appears.</p> 
3.	<p>In the center (Select) panel, select the Advanced Options link. Scroll down in the left pane to verify that all options are checked except the last three (Voice-over-IP (VoIP) Group Setting, Voice-over-IP (VoIP) Accounting Configuration, ODBC Logging). Click Submit.</p> 

Step	Description
4.	<p>From the left panel, select Network Configuration. The following screen appears.</p> 
5.	<p>Under the Network Device Groups table, select Add Entry. The New Network Device Group form appears, as shown below. Enter a name for the Network Device Group (in this example, “cat6509” is used) and a shared key that must match the RADIUS authentication secret set in the Cisco Catalyst 6509 switch in Section 4 (in this example, “cisco” is used). Click Submit.</p> 

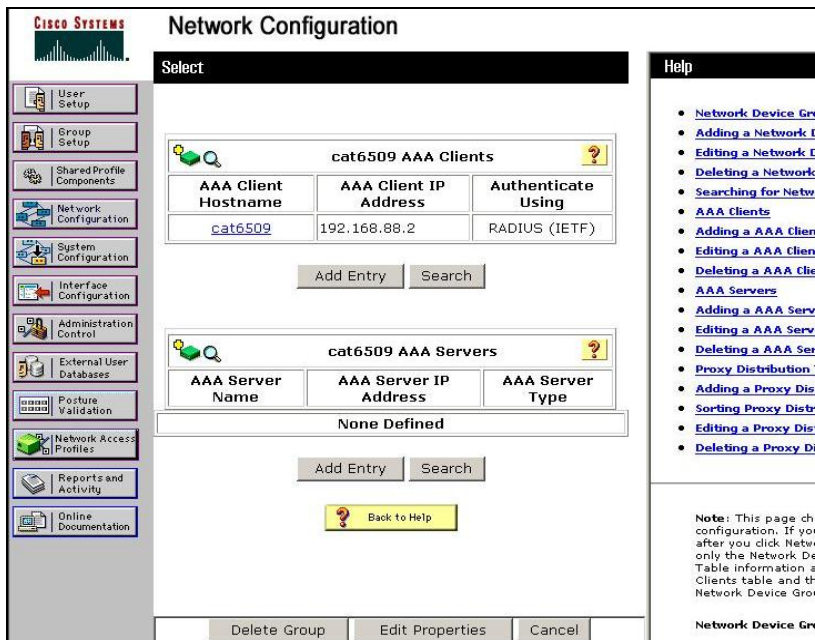
Step	Description
6.	<p>The Network Device Group now appears on the Network Configuration screen, as shown below.</p>  <p>The screenshot shows the 'Network Configuration' page with a sidebar on the left containing various configuration options like 'User Setup', 'Group Setup', and 'Network Configuration'. The main content area is divided into two sections: 'Network Device Groups' and 'Proxy Distribution Table'. The 'Network Device Groups' table has columns for 'Network Device Group', 'AAA Clients', and 'AAA Servers'. The 'Proxy Distribution Table' has columns for 'Character String', 'AAA Servers', 'Strip', and 'Account'. A 'Help' sidebar on the right lists various actions like 'Adding a Network Device Group' and 'Deleting a Network Device Group'. A 'Back to Help' button is located at the bottom of the main content area.</p>

7.	<p>Click on the name of the newly added Network Device Group. The AAA Clients table and AAA Servers table for this Network Device group appears.</p>  <p>The screenshot shows the 'Network Configuration' page with the 'cat6509' Network Device Group selected. The main content area now displays two tables: 'cat6509 AAA Clients' and 'cat6509 AAA Servers'. The 'AAA Clients' table has columns for 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. The 'AAA Servers' table has columns for 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type'. Both tables show 'None Defined' entries. The 'Help' sidebar on the right is updated to show actions related to the selected group, such as 'Adding a Network Device Group' and 'Deleting a Network Device Group'. At the bottom of the main content area, there are buttons for 'Delete Group', 'Edit Properties', and 'Cancel'.</p>
----	--

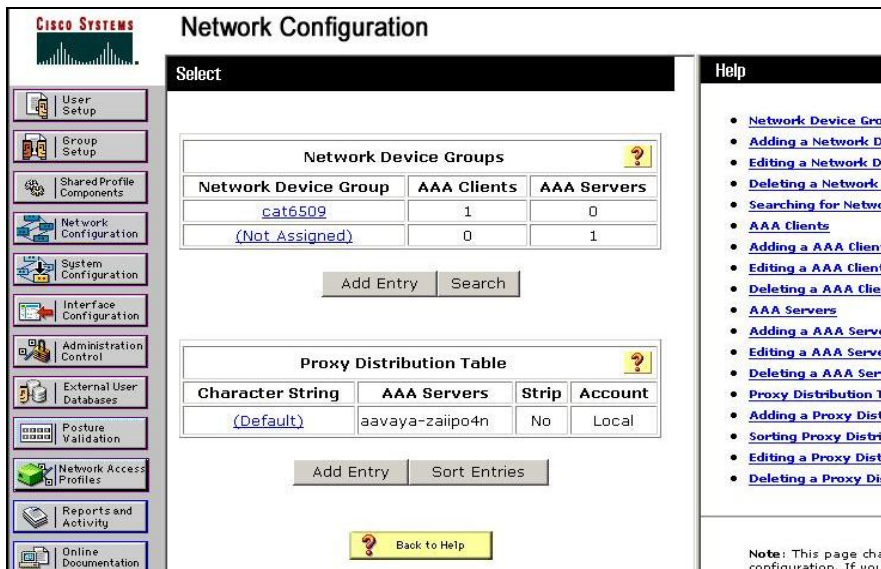
Step	Description
8.	<p>Under the AAA Clients table, click the Add Entry button. The Add AAA Client form appears. Enter the following values:</p> <ul style="list-style-type: none"> • AAA Client Hostname: Provide a descriptive name (in this example, “cat6509” is used) • AAA Client IP Address: Enter the IP address of the AAA client (in this example, 192.168.88.2) • Key: Enter a value to be used as a shared key (in this example “cisco” is used) • Network Device Group: Leave this field unchanged (it should already be set to the name of the newly added Network Device Group) • Authenticate Using: Select RADIUS (IETF) from the drop-down list. <p>The completed form should appear as shown below. Click Submit + Apply.</p>

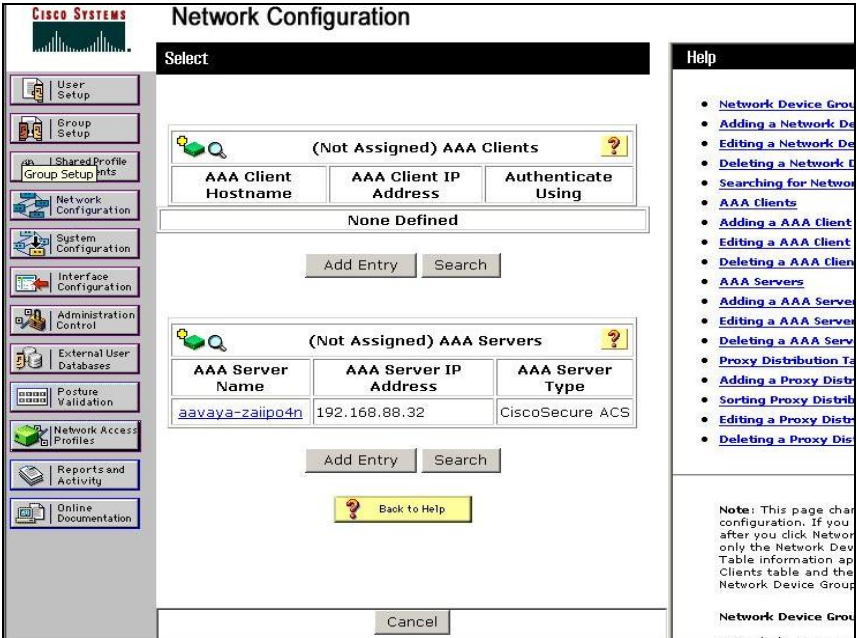
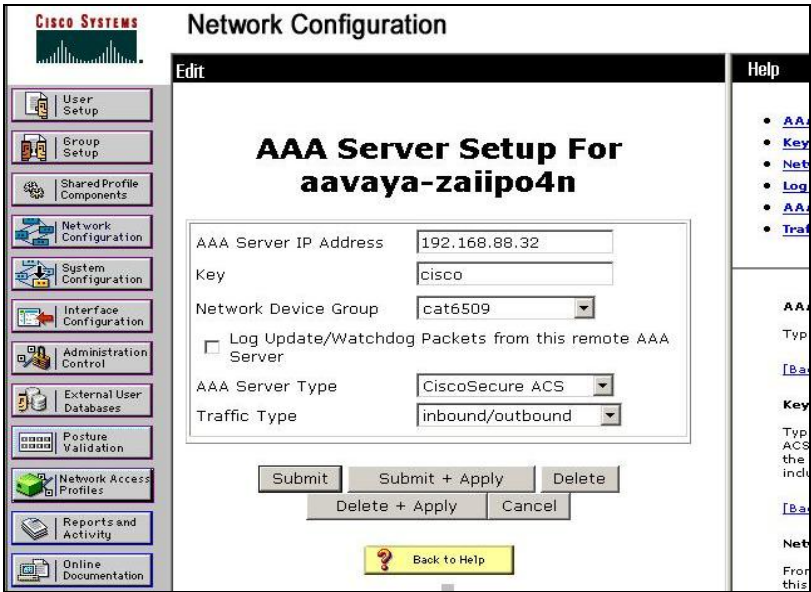
Step	Description
------	-------------

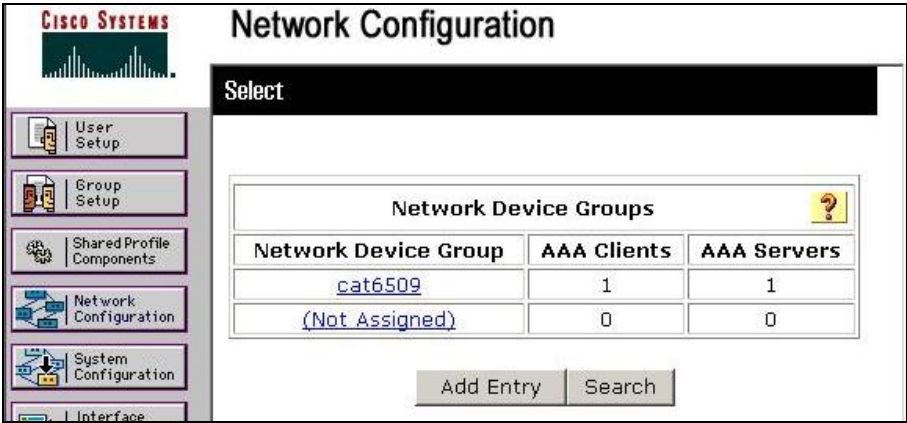
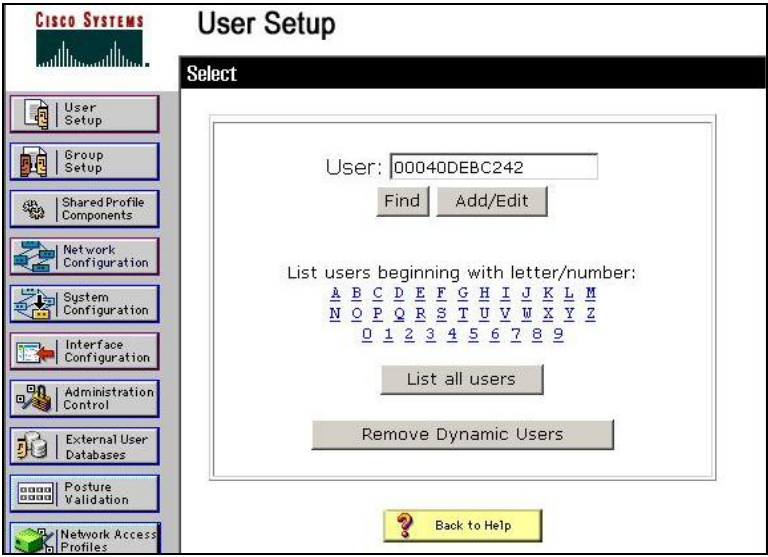
9. The newly added AAA Client appears in the Network Device Group's AAA Clients table, as shown below.



10. From the left panel, select **Network Configuration**. In the **Network Device Groups** table (see below), click the **(Not Assigned)** group name.



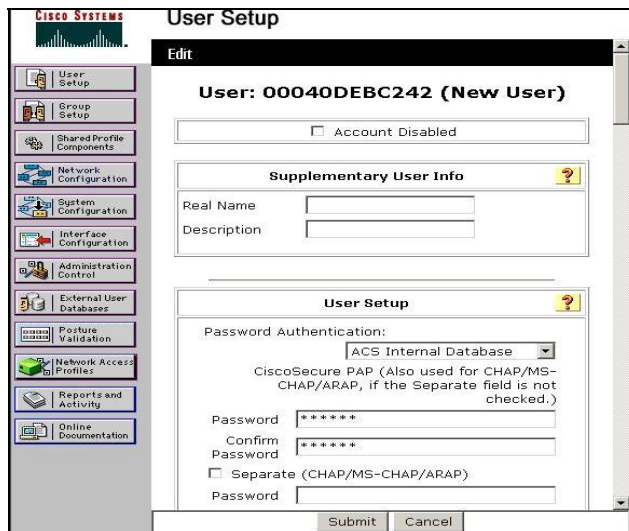
Step	Description
<p>11.</p>	<p>In the list of (Not Assigned) AAA Servers (see below), click on the name of the local machine (in this example, “aavaya-zaiipo4n”).</p>  <p>The screenshot shows the 'Network Configuration' interface with the 'Select' tab active. It displays two tables: '(Not Assigned) AAA Clients' (empty) and '(Not Assigned) AAA Servers'. The AAA Servers table contains one entry: 'aavaya-zaiipo4n' with IP '192.168.88.32' and Type 'CiscoSecure ACS'. A 'Back to Help' button is visible below the table.</p>
<p>12.</p>	<p>In the AAA Server Setup form (see below), select the newly added Network Device Group from the Network Device Group drop-down list, then click Submit + Apply.</p>  <p>The screenshot shows the 'AAA Server Setup For aavaya-zaiipo4n' form. The 'Network Device Group' dropdown menu is open, showing 'cat6509' selected. Other fields include 'AAA Server IP Address' (192.168.88.32), 'Key' (cisco), 'AAA Server Type' (CiscoSecure ACS), and 'Traffic Type' (inbound/outbound). The 'Submit + Apply' button is highlighted.</p>

Step	Description
<p>13.</p>	<p>From the left panel, select Network Configuration. The entry in the Network Device Groups table for the newly added Network Device Group (in this example, cat6509) shows one AAA Server as a member in addition to the previously added AAA Client (see below).</p> 
<p>14.</p>	<p>From the left panel, click User Setup.</p>  <p>Type into the User field the username corresponding to the Avaya 9620 IP Telephone to be registered with Avaya Communication Manager. As described in Section 1, the default username provided by the Avaya 9620 IP Telephone is its MAC address (in this example, 00040DEBC242). See Section 6.2 for details on how to use a username other than the default.</p> <p>Click Add/Edit.</p>

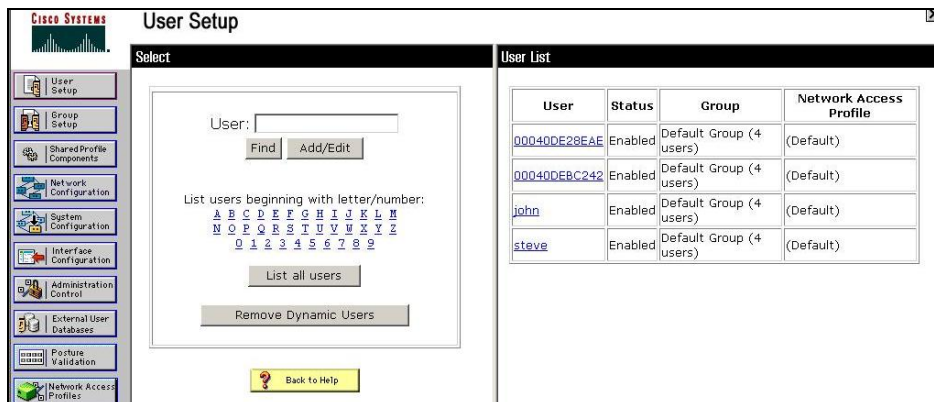
Step	Description
------	-------------

- 15.** On the **User Setup Edit** form (see below), enter the following values:
- **Password Authentication:** Select ACS Internal Database from the drop-down list.
 - **Password:** Enter a password corresponding to the Security Code on Avaya Communication Manager’s Station Administration form for this Avaya 9620 IP Telephone (see [2] for details).
 - **Confirm Password:** Re-enter the above password.

Click **Submit**.



- 16.** Repeat **Steps 14 and 15** to add additional users as needed. From the **User Setup** screen, click **List All Users**. The screen below lists two Avaya IP Telephones (identified by MAC address) and two PCs (given names “john” and “steve”) as users. Note that the password entered by a PC user via an 802.1X authentication client application must match the password stored for that user in the Cisco Secure ACS.



6 Configure the Avaya 9620 IP Telephone

This section describes the procedures to configure a new, “out-of-the-box” Avaya 9620 IP Telephone for the various options referenced in these Application Notes. See [3] for details on configuring an Avaya 9620 IP Telephone that is already connected to an enterprise network.

Avaya 9620 IP Telephones support three 802.1X operational modes, as described below. See **Section 6.1** for details on how to configure the operational mode.

- **Supplicant Mode** – Unicast or Multicast supplicant operation for the Avaya 9620 IP Telephone itself, without PAE Multicast pass-through or proxy Logoff for the attached PC.
- **Pass-thru Mode** – Unicast supplicant operation for the Avaya 9620 IP Telephone itself, with PAE Multicast pass-through for the attached PC, but without proxy Logoff. This is the default setting.
- **Pass-thru Mode with Proxy Logoff** – Unicast supplicant operation for the Avaya 9620 IP Telephone itself, with PAE Multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected from the Avaya 9620 IP Telephone, the phone will send an EAPOL-Logoff for the attached PC.

Since the Cisco Catalyst 6509 switch only supports Multicast operation when Single host or Multi-host authentication mode is used, the Avaya 9620 IP Telephone must be configured in Supplicant Mode if it is to be used to authenticate a port. If an attached PC will be requesting authentication, then the Avaya IP 9620 IP Telephone must be configured to use one of the two forms of Pass-thru Mode, which support PAE Multicast pass-through.

6.1 Set 802.1X Operational Mode

Step	Description
<p>1.</p>	<p>During the initial power-up boot sequence, press * on the Avaya 9620 IP Telephone keypad, then press # until the following set of text appears in the display.</p> <div data-bbox="683 512 1081 642" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <pre>802.1X=pass-thru mode *=change #=ok</pre> </div> <p>This is the default setting for the 802.1X parameter. Other possible values, which are displayed in turn by pressing *, are:</p> <div data-bbox="683 789 1081 919" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <pre>802.1X=Supplicant mode *=change #=ok</pre> </div> <div data-bbox="683 1010 1081 1140" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <pre>802.1X=p-t w/Logoff *=change #=ok</pre> </div>
<p>2.</p>	<p>Press * until Supplicant mode is displayed, and then press # until the following text is displayed:</p> <div data-bbox="683 1257 1081 1388" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <pre>Save new values? *=no #=yes</pre> </div> <p>Press # to save this setting</p>

NOTE: If **pass-thru mode** or **p-t w/Logoff** are used (see **Section 7.5** for an example) and a PC is not yet connected to the Avaya 9620 IP Telephone, the VLAN ID must be set manually to allow the telephone to register. See [3] for details on carrying out this provisioning.

6.2 Change 802.1X Username and Password

This procedure assumes that (1) the Avaya 9620 IP Telephone has already been configured with the necessary options for access to the enterprise network and (2) there is a user administered on the Cisco Secure ACS that matches the MAC address of the Avaya 9620 IP Telephone.

Step	Description
1.	<p>Reset the Avaya 9620 IP Telephone by entering “[MUTE]73738#” (i.e. [MUTE]RESET) on the keypad. The following set of text appears in the display.</p> <div data-bbox="683 659 1081 787" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"><pre>Reset values? *=no #=yes</pre></div> <p>Press *. The following prompt appears.</p> <div data-bbox="683 898 1081 1026" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"><pre>Restart phone? *=no #=yes</pre></div> <p>Press #.</p>
2.	<p>During the course of the restart sequence, the following display will appear.</p> <div data-bbox="683 1220 1081 1348" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"><pre>802.1X ID=00040DEBC242 #=OK New=</pre></div> <p>The default 802.1X ID, which is the MAC address of the Avaya 9620 IP Telephone (in this example, 00040DEBC242). Press #.</p>

Step	Description
3.	<p>The following display appears.</p> <div data-bbox="683 359 1081 478" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <pre> Password= #=OK </pre> </div> <p>Enter the password associated with the user entered in Step 2, and then press #. This password must match the password entered for this user in Section 5, Step 15.</p> <p>The restart sequence will continue, with the Avaya 9620 IP Telephone being authenticated successfully.</p>

7 Verification

7.1 Verify 802.1X On the Cisco Catalyst 6509

Use the command **show port dot1x** to display the dot1x configuration and 802.1X status. The following screen shows that port 7/2 is authorized. This output is as shown regardless of the type of device requesting authentication (i.e. telephone or PC).

```

Console> (enable) show port dot1x 7/2

```

Port	Auth-State	BEnd-State	Port-Control	Port-Status	
7/2	authenticated	idle	auto	authorized	

Port	Port-Mode	Re-authentication	Shutdown-timeout	Control-Mode	
				admin	oper
7/2	MultiHost	enabled	disabled	Both	Both

Port	Posture-Token	Critical Termination	action	Session-timeout
7/2	-	NO	ReAuth	-

Use the command **show port dot1x user** to display 802.1X user information. The following screen shows that username **00040DEBC242** was used to authenticate port 7/2 (where **00040DEBC242** is the MAC address of an Avaya 9620 IP Telephone) and username **john** was used to authenticate port 7/3 (where **john** is a username used by an 802.1X client application running on a PC attached to a different Avaya 9620 IP Telephone).

```

Console> (enable) show port dot1x user
Username                               Mod/Port  UserIP          VLAN
-----                               -
00040DEBC242                           7/2      0.0.0.0         89
john                                     7/3      0.0.0.0         89

```

When the port security is disabled, use the command **show cam dynamic <port#>** to verify that the Cisco Catalyst 6509 switch learns the MAC addresses of the Avaya 9620 IP Telephone and the attached PC in different VLANs. (When the port security is enabled, use the command **show cam static <port#>**.)

```

Console> (enable) show cam dynamic 7/2
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry M = Mac-Auth-Bypass Entry

VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
-----
89    00-0f-1f-23-f1-db      7/2 [ALL]
88    00-04-0d-eb-c2-42     7/2 [ALL]
Total Matching CAM Entries Displayed = 2

```

Use the command **set trace dot1x <debug levels 1-15>** to troubleshoot an 802.1X problem on the Cisco Catalyst 6509 switch.

```
Console> (enable) set trace dot1x 7

DOT1X tracing set to 7.

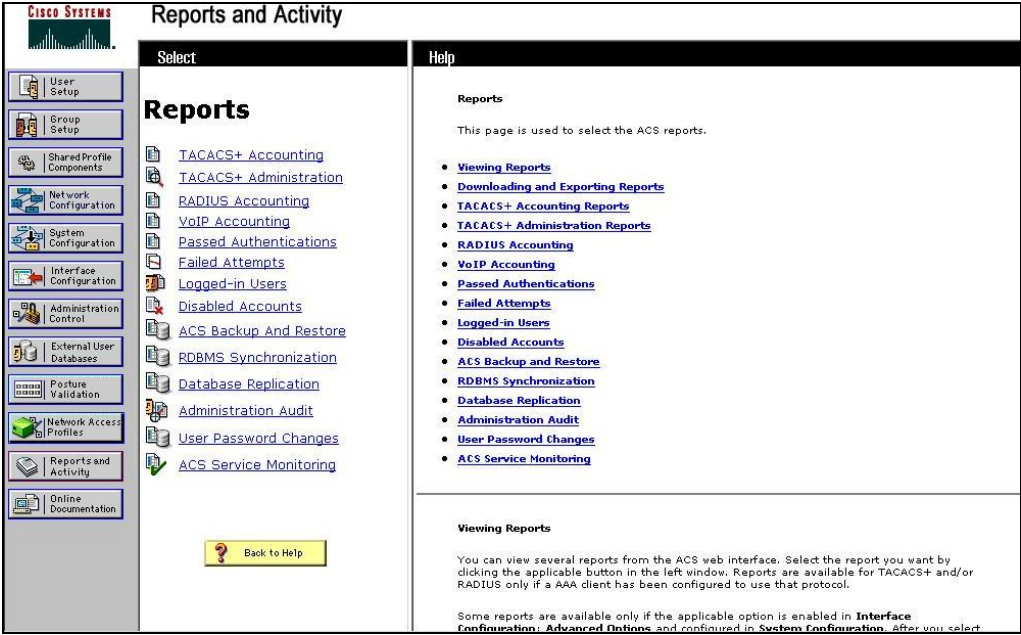
Warning!! Turning on trace may affect the operation of the system.
Use with caution.
Console> (enable) dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:43:47.210
Resp received for ID = 32006 Dec 05 06:43:47.270
dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:43:47.350
Resp received for ID = 42006 Dec 05 06:43:47.430
addPortVlanMVAP :rc = 02006 Dec 05 06:43:56.200
delPortVlanMVAP :rc = 02006 Dec 05 06:43:56.260
dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:43:56.340
Resp received for ID = 52006 Dec 05 06:43:56.400
dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:43:56.470
Resp received for ID = 62006 Dec 05 06:43:56.530
dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:43:56.740
Resp received for ID = 82006 Dec 05 06:43:56.840
addPortVlanMVAP :rc = 02006 Dec 05 06:44:10.550
dot1x_rad: Checking server and index is 12006 Dec 05 06:44:10.620
dot1x_rad: RadiusSendQuery: authport - 18122006 Dec 05 06:44:10.700
Resp received for ID = 15
Console> (enable)
Console> (enable) set trace dot1x 0
DOT1X tracing disabled.
Console> (enable)
```

7.2 Verify 802.1X On the Avaya 9620 IP Telephone

Verify that the Avaya 9620 IP Telephone is configured to the supplicant mode by pressing “[MUTE]80219#”. You will be prompted to enter a username and password if the authentication fails.

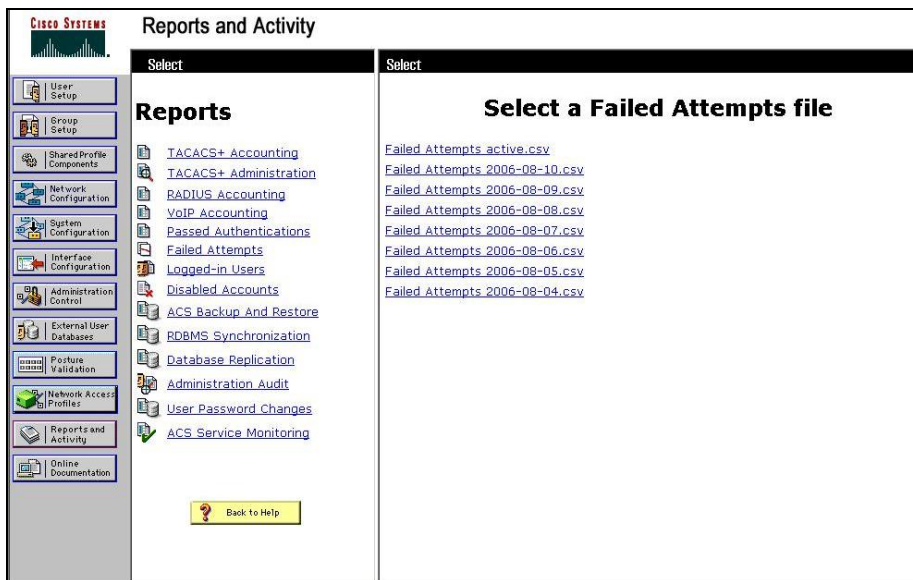
7.3 Verify 802.1X on the Cisco Secure ACS

To verify the authentication status of the Avaya 9620 IP Telephone by the Cisco Secure ACS, take the following steps:

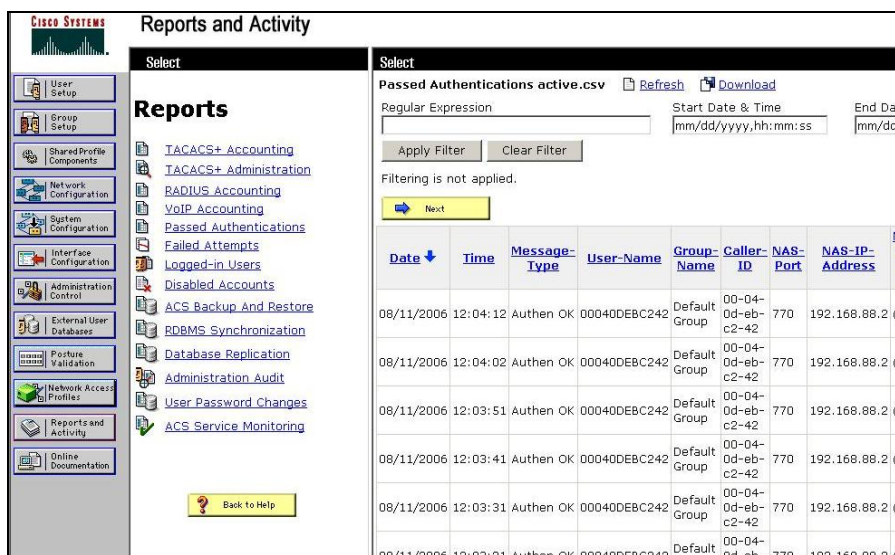
Step	Description
1.	<p>From the Cisco Secure ACS administration tool's main screen, click the Reports and Activity button in the left panel. The following screen appears.</p> 

Step	Description
------	-------------

2. From the **Reports and Activity** screen shown in **Step 1** above, select **Passed Authentications** from the set of **Reports** links in the **Select** panel. The following screen appears.

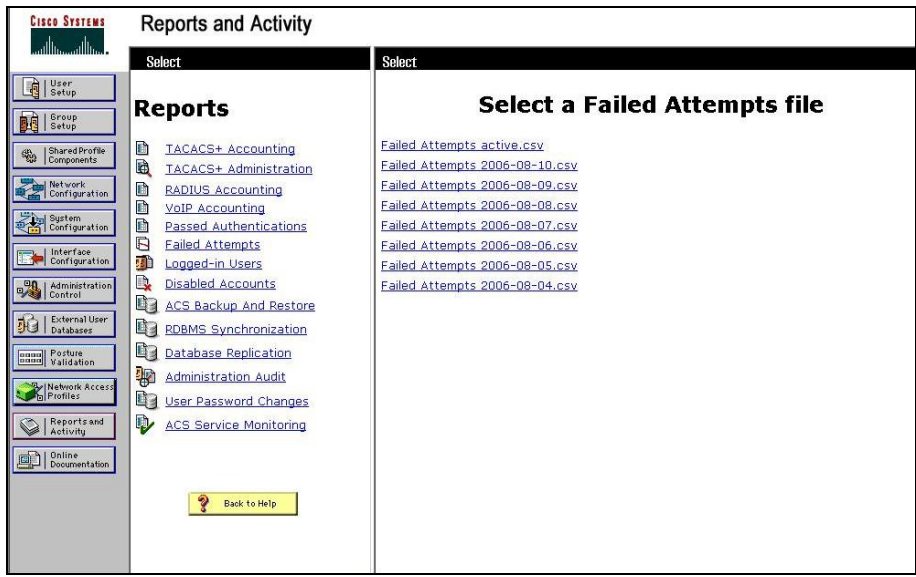


3. From the right-most panel, select a **Passed Authentications** file corresponding to the time frame to be examined. The contents of the file will appear as shown below.

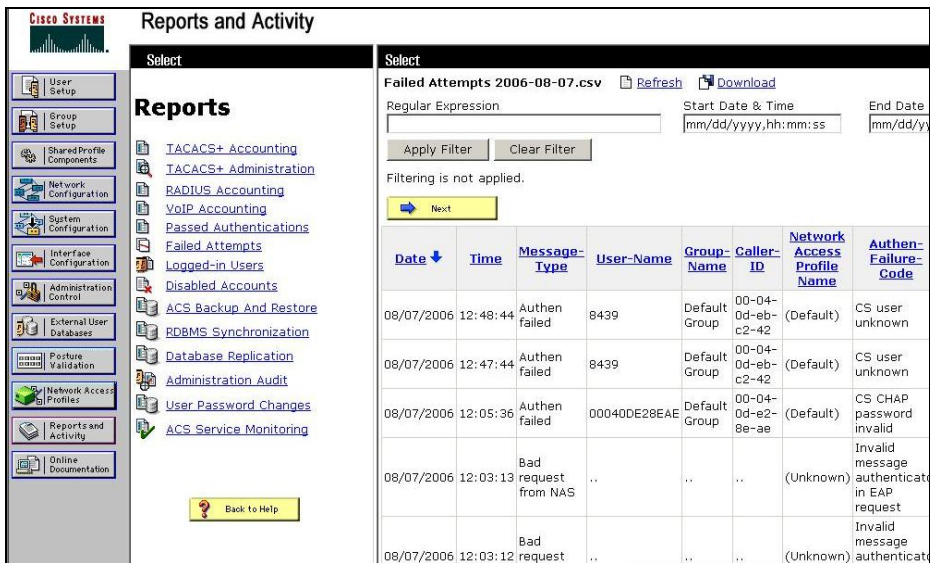


Step	Description
------	-------------

4. Similarly, details of failed authentications can be retrieved. From the set of **Reports** links in the **Select** panel, select **Failed Attempts**. The following screen appears.



5. From the right-most panel, select a **Failed Attempts** file corresponding to the time frame to be examined. The contents of the file, including information on the reason for each failed authentication attempt (**Authentication Code** column), will appear as shown below.



7.4 Verify Connectivity of Attached PC

Once the Avaya 9620 IP Telephone has been authenticated, attach a PC's Network Interface Card (NIC) to the Avaya 9620 IP Telephone's PC port. Verify that the PC can acquire an IP address from the DHCP server and can ping the network's default gateway.

Conversely, if the Avaya 9620 IP Telephone fails the authentication process, the attached PC should be unable to access the network.

7.5 Verify Authentication Behavior in Various Configurations

To understand better the authentication behavior of the network configuration described in **Figure 2**, a series of tests were conducted with the Avaya 9620 IP Telephone and Cisco Catalyst 6509 switch provisioned in a variety of combinations. In each case, 802.1X authentication of the associated switch port was established using the native VLAN (89), while connectivity from the Avaya 9620 IP Telephone to the Avaya S8500 Media Server was over the auxiliary (voice) VLAN (88). The results are described in the table below. (**NOTE:** Since changing the configuration setting for the PC port can introduce a security risk, the associated procedures are not included here. Contact an authorized Avaya representative for the details of these procedures.)

Option #	Avaya 9620 IP Telephone Settings		Cisco Catalyst 6509 Authentication Mode	Results
	802.1X Mode	PC Port		
1	Supplicant	Disabled	Single-Host	Phone authenticates port; attached PC cannot access network
2	Supplicant	Enabled	Multi-Host	Phone authenticates port; attached PC can access network without the need for authentication
3	Pass-Thru	Enabled	Multi-Host	Attached PC authenticates port (Funk Odyssey Client was used); phone can register with S8500 over voice VLAN if manually provisioned initially (see [3]) (otherwise, requires PC for authentication whenever port is enabled/re-enabled)

Based on the results in the above table, Avaya recommends that **Option 1** be used for Avaya 9620 IP Telephones placed in public areas where untrusted individuals might try to access the enterprise network by connecting a PC to the secondary physical port of the Avaya 9620 IP Telephone. **Option 2** represents the configuration implemented in these Application Notes.

Option 3 is recommended in a private office environment in which an employee's PC is required to be authenticated before being given network access.

8 Conclusion

As illustrated in these Application Notes, Avaya 9620 IP Telephones with 802.1X enabled can be authenticated when connected to a Cisco Catalyst 6509 switch configured as an 802.1X authenticator. The Cisco Catalyst 6509 switch can use the Cisco Secure ACS to authenticate the Avaya 9620 IP Telephones.

- When the Avaya 9620 IP Telephone is configured in Supplicant mode and the Cisco Catalyst 6509 switch port connected to the Avaya 9620 IP Telephone is in Multi-host mode, the Avaya 9620 IP Telephone can be used to authenticate the port so that an attached PC can get access to the network without the need for authentication. The Avaya 9620 IP Telephone can be configured to use the auxiliary (i.e. voice) VLAN on the Cisco Catalyst 6509 switch so that the Avaya 9620 IP Telephone and the attached PC are on different VLANs.
- If it is not desired to allow an attached PC to access the network, the Cisco Catalyst 6509 switch port connected to the Avaya 9620 IP Telephone can be configured in Single-host mode with the Avaya 9620 IP Telephone configured in Supplicant mode. In this case, attaching a PC to the Avaya 9620 IP Telephone would constitute a possible security violation and may cause the port (and, therefore, the Avaya 9620 IP Telephone) to be disabled.
- If the Avaya 9620 IP Telephone is configured in Pass-thru mode, an attached PC can be used for authentication of the port and the Avaya 9620 IP Telephone will gain access to the network on the auxiliary (voice) VLAN without the need for authentication.

9 Additional References

The following references can be found at the URLs indicated:

1. Application Notes: “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” (<https://enterpriseportal.avaya.com/ptlWeb/getfile?docID=Mzg3NjkxOA==>).
2. “Administrator Guide for Avaya Communication Manager,” Document ID 03-300509, May 2006 (http://support.avaya.com/elmodocs2/comm_mgr/r3_1/pdfs/03_300509_2_1.pdf).
3. “Avaya one-X Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide Release 1.0,” Document ID 16-300694, July 2006 (http://support.avaya.com/elmodocs2/one-X_Deskphone_Edition/16_300694_1.pdf).
4. “Catalyst 6500 Series Switch Software Configuration Guide – Software Release 8.5,” Text Part Number OL-7193-01, Cisco Systems, Inc. (http://www.cisco.com/application/pdf/en/us/guest/products/ps708/c2001/ccmigration_09186a00806a4eb4.pdf).
5. “User Guide for Cisco Secure ACS for Windows – Version 4.0,” Text Part Number 78-16992-02, Cisco Systems, Inc. (http://www.cisco.com/application/pdf/en/us/guest/products/ps6439/c2001/ccmigration_09186a008053d5e4.pdf).

©2006 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