m

Avaya Solution & Interoperability Test Lab

Configuring 802.1X Protocol on HP ProCurve Switch for an Avaya IP Telephone 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 and of preventing access to that port in cases where the authentication process fails. HP ProCurve switch supports 802.1X as authenticators and Avaya IP Telephones support 802.1X as supplicants. These Application Notes provides the steps necessary to configure 802.1X on the HP ProCurve switch for an Avaya IP Telephone with an attached PC. Microsoft Internet Authentication Service is used as the authentication server.

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 machine 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 be 802.1X supplicants.

- Authenticator – a PAE that facilities the authentication of the supplicant. The HP ProCurve 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 Extensible Authentication Protocol (EAP) messages**.** The protocol 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 EAP received in 802.1X packets to an authentication server by using the RADIUS format to carry the EAP information.

The Avaya IP Telephones support EAP-MD5 authentication. The following shows typical EAP-MD5 message exchanges for the 802.1X protocol. The authenticator or the supplicant can initiate authentication. When the switch detects the port link state transitions 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 flows for the Avaya IP Telephone, the HP ProCurve switch and an authentication server using the EAP-MD5 authentication.

Avaya IP Telephones can prompt the user for a username and password, and the username and password can be stored. 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 RADIUS server rejects the current username and password. The default username is the phone's MAC address. 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.

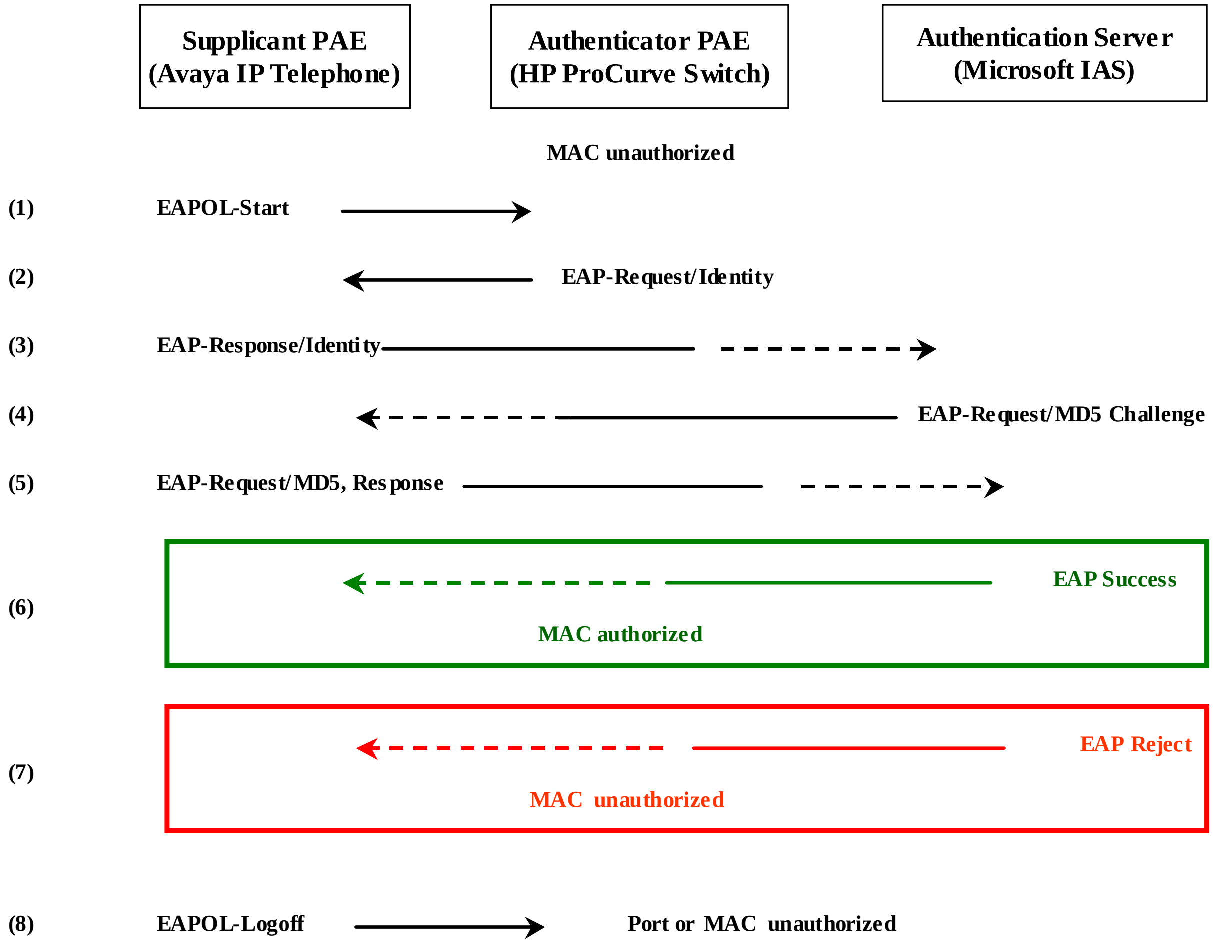


Figure 1: 802.1X Message Exchanges

The following describes the 802.1X flows in **Figure 1**:

1. The supplicant (the Avaya IP Telephone) sends an “EAPOL Start” packet to the authenticator (the HP ProCurve Switch). The IP Telephone will ignore the EAP-request/identity frames from the 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. The authenticator strips the EAP Ethernet header and encapsulates the remaining EAP frame in the RADIUS format, and then sends it to the authentication server.

4. The authentication server recognizes the packet as an EAP-MD5 type and sends back a challenge message to the authenticator. The authenticator removes the authentication server’s frame header and encapsulates the remaining EAP frame into the EAPOL format and then sends it to the supplicant.

5. The supplicant responds to the challenge and the authenticator passes the response onto the authentication server.

6. If the supplicant provides proper identity, the authentication server responds with a success message. The authenticator passes the message onto the supplicant and allows access to the LAN.

7. If the supplicant does not provide proper identity, the authentication server responds with a reject message. The authenticator passes the message onto the supplicant 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.

Figure 2 shows the network diagram used in these Application Notes. The PCs attached to the Avaya IP Telephones are installed with the Funk Odyssey client software (802.1X client software). The EAP-MD5 authentication is configured for the IP Telephone and the attached PC in these Application Notes.

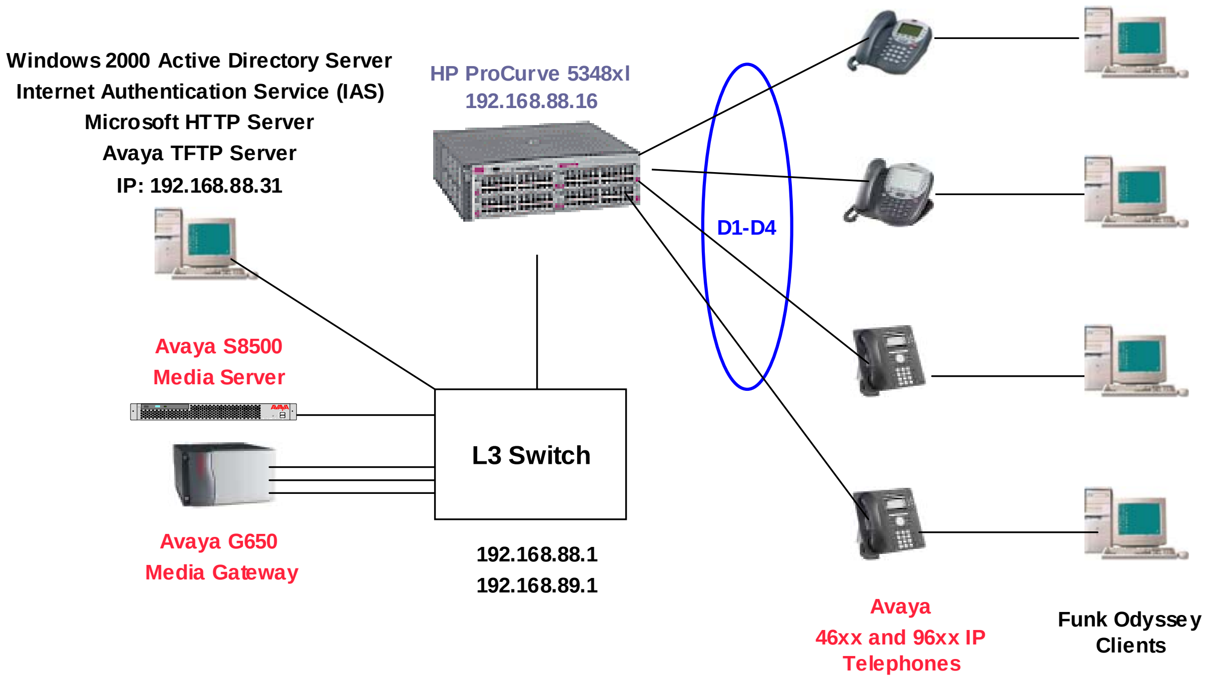


Figure 2 – 802.1X Configuration With Avaya IP Telephones

2 Equipment and Software Validated

Table 1 below shows the versions verified in these Application Notes.

Equipment	Software
Avaya S8500 Media Server	Avaya Communication Manager 3.1.1 (load 628.7)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MEDPRO (TN2302AP)	 HW12 FW030 HW01 FW017 HW11 FW108
Avaya 9610 IP Telephone	1.2 H.323
Avaya 9620 IP Telephone	1.2 H.323
Avaya 9630 IP Telephone	1.2 H.323
Avaya 9630G IP Telephone	1.2 H.323
Avaya 9640 IP Telephone	1.2 H.323
Avaya 9650 IP Telephone	1.2 H.323
Avaya 4610SW IP Telephone	2.6
Avaya 4620SW IP Telephone	2.6
Avaya 4621SW IP Telephone	2.6
Avaya 4622SW IP Telephone	2.6
HP ProCurve 5348xl Switch	E.10.44
Apache HTTP Server (for 96xx phones)	2.0.54
Avaya TFTP Server (for 46xx phones)	3.6.1
Microsoft Internet Authentication Service (IAS)	Microsoft Windows 2000 Advanced Server
Microsoft DHCP Server	Microsoft Windows 2000 Advanced Server
Funk Odyssey Client	4.30

Table 1: Equipment and Software Validated

3 Configurations

The HP ProCurve switch supports Client-Based Authentication. Multiple clients on the same port can be authenticated individually. An Avaya IP Telephone with an attached PC can be independently authenticated in different VLANs when connected to the HP ProCurve Switch.

Avaya IP Telephones support three 802.1X operational modes. The operational mode can be changed by pressing “mute80219#” (“mute8021x”) on the Avaya 46xx IP Telephones or by pressing the Craft Access Code (the default is “mutecraft#” or “mute27283#”) on the Avaya 96xx IP Telephones.

- **Pass-thru Mode –** Unicast supplicant operation for the IP Telephone itself, with PAE multicast pass-through for the attached PC, but without proxy Logoff (default).

- **Pass-thru with logoff Mode (p –t w/Logoff) –** Unicast supplicant operation for the IP Telephone itself, with PAE multicast pass-through and proxy Logoff for the attached PC. When the attached PC is physically disconnected from the IP Telephone, the phone will send an EAPOL-Logoff for the attached PC.

- **Supplicant Mode –** Unicast or multicast supplicant operation for the IP Telephone itself, without PAE multicast pass-through or proxy Logoff for the attached PC.

Since most 802.1X clients use the Multicast MAC address for the EAPOL messages, the IP Telephone must be configured to the **pass-thru** or **p-t w/Logoff** mode to pass-through these Multicast messages. It is recommended to use the **p-t w/Logoff** mode. When the phone is in the **p-t w/Logoff** mode, the phone will do proxy logoff for the attached PC when the PC is physically disconnected. When the HP ProCurve switch receives the logoff message, the PC will be removed from the authorized MAC list.

3.1 Configuring 802.1X on the HP ProCurve Switch

The following shows the annotated global 802.1X configuration. The radius authentication secret must match the configuration on the Microsoft Internet Authentication Server.

```
! --- Configure the switch for 802.1X authentication for the port access
aaa authentication port-access eap-radius

! --- Configure the radius server to the IAS
radius-server host 192.168.88.31 key 1234567890123
```

By default, all ports are configured in the **auto** mode. The command **aaa port-access authenticator <port #> control** can be used to configure a port in the **authorized**, **auto** or **unauthorized** mode.

```
HP(config)# aaa port-access authenticator D1-D4 control
 authorized             Force authorized.
 auto                   Auto.
 unauthorized           Force unauthorized.
```

The following screen configures ports D1 to D4 to the 802.1X authenticator ports and the control mode to auto.

```
aaa port-access authenticator D1-D4

aaa port-access authenticator D1-D4 control auto
```

Use the command **aaa port-access authenticator active** to enable 802.1X authentication on the switch. This command will activate 802.1X port-access on the configured ports as authenticators.

```
aaa port-access authenticator active
```

The following screen shows the VLAN and ports configuration. To put an IP Telephone and the attached PC into different VLANs, configure a port with an untagged VLAN for the attached PC and a tagged VLAN for the Avaya IP Telephone. Ports D1-D4 are configured with untagged VLAN 89 and tagged VLAN 88. Port D24, which is connected to the L3 switch, is configured with tagged VLANs 88 and 89.

```
vlan 89
   name "VLAN89"
   untagged D1-D4
   tagged D24
   voice
   exit
vlan 88
   name "VLAN88"
   ip address 192.168.88.16 255.255.255.0
   tagged D1-D4,D24
   exit
```

Use the command **primary-vlan <VLAN ID>** to configure a primary VLAN on the switch. The primary VLAN IP address will be used as the network access server (NAS) IP address to access the Radius Server (see **Section 3.4**). The primary VLAN is configured to VLAN 88 in these Application Notes. The VLAN 88 IP address 192.168.88.16 will be used as the NAS-IP-address.

By default, 802.1X re-authentication is not enabled. It is recommended to enable re-authentication for high security. In the sample configuration, the re-authentication period is configured to 3600 seconds. The HP ProCurve switch also supports client limits for 802.1X authentication. It must be configured to 3 (3 MACs) if the phone with the attached PC needs to be supported. When the phone is reset from the manufacturer's default, the phone will boot from the native VLAN and then switch to the voice VLAN. The HP ProCurve Switch will detect two MAC addresses for the phone (one MAC on the native VLAN and another on the voice VLAN). Use the command **port-security <port#> learn-mode port-access** to allow only the number of 802.1X devices specified by the client-limit option.

```
aaa port-access authenticator D1-D4 reauth-period 3600
aaa port-access authenticator D1-D4 client-limit 3
port-security D1-D4 learn-mode port-access
```

Refer to [1] for detailed security configuration guide on the HP ProCurve switch.

3.2 DHCP Configuration for Avaya IP Telephones

Table 2 summarizes the Dynamic Host Configuration Protocol (DHCP) configuration on the Microsoft DHCP Server. The following describes how the Avaya IP Telephones work with the DHCP server after the 802.1X authentication succeeds.

Consider the example of IP Telephones and computers configured for DHCP in **Figure 2**. If the IP Telephone is set to the manufacturer's default configuration, the IP Telephone will initially send a clear DHCP request. The HP ProCurve port connected to the Avaya IP Telephone is configured with both untagged VLAN 89 and tagged VLAN 88. The clear DHCP request will be associated with the untagged VLAN 89 on the port. When the L3 switch 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 Options 176 and 242 strings, instructing the IP Telephone to enable 802.1Q tagging with VLAN ID 88. The IP Telephone receiving this reply will release the supplied IP address and issue a new DHCP request with VLAN ID 88. 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 Options 176 and 242.

When the attached PC issues a DHCP request, it will send a clear DHCP request after its successful authentication. This request will be served in the same way as the initial request from the phone. However, the computer will ignore Options 176 and 242 values specifying a new VLAN. Therefore, no new DHCP request is issued.

By default, the Avaya 46xx IP Telephones use Option 176 and the Avaya 96xx IP Telephones use Option 242. Avaya 46xx IP Telephones use the TFTP server and the Avaya 96xx IP Telephones use the HTTP server.

DHCP Scope	**Option 3 Router**	**Option 176 Option 242**
192.168.88.0	192.168.88.1	Option 176: MCIPADD=192.168.88.22,TFTPSRVR=192.168.88.31 Option 242: MCIPADD=192.168.88.22,HTTPSRVR=192.168.88.31
192.168.89.0	192.168.89.1	Option 176: L2QVLAN=88 Option 242: L2QVLAN=88

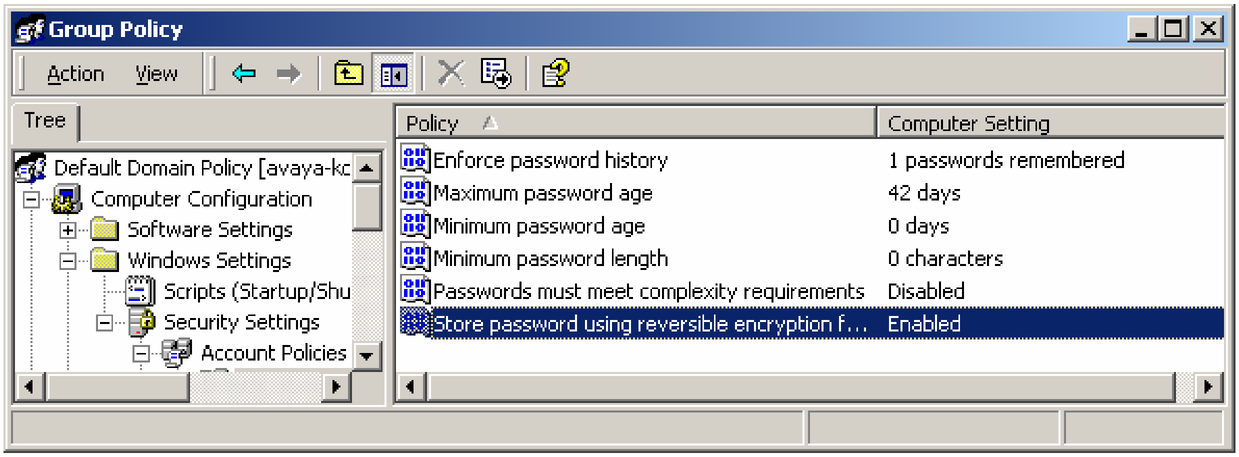
Table 2 – DHCP Configuration Summary

3.3 Configuring the Active Directory Server

In the sample configuration, the Microsoft IAS and the active directory run on the same Microsoft Advanced 2000 Server. The intent of this section is to illustrate relevant aspects of the configuration used for the testing.

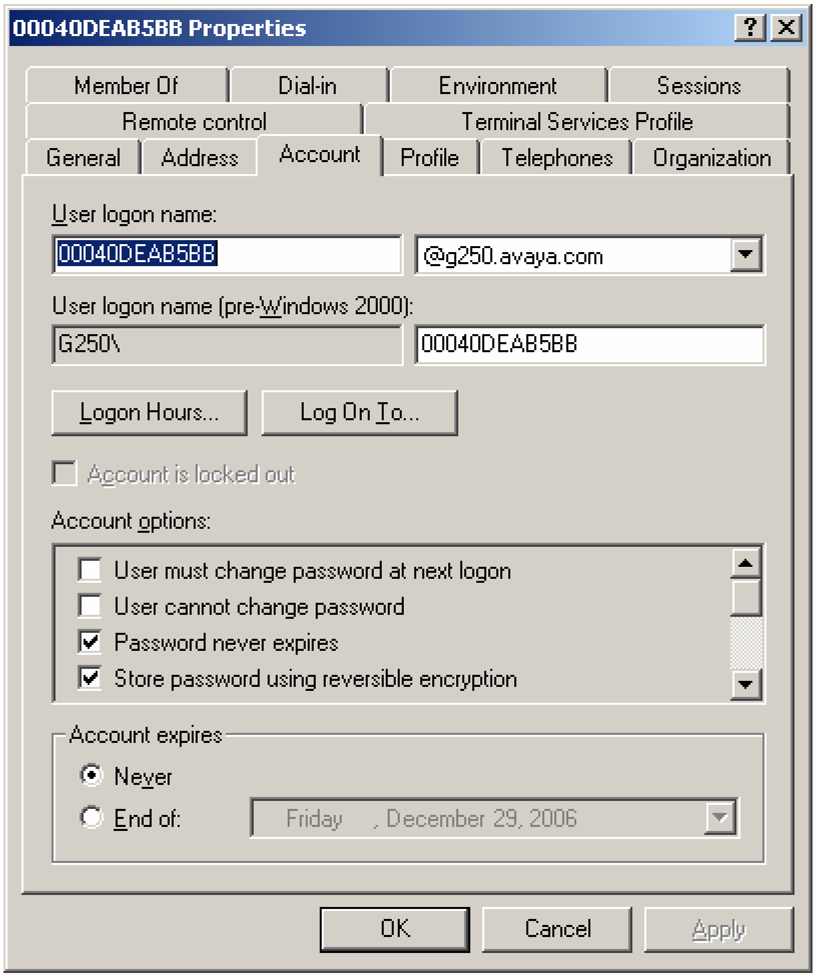
Configure passwords to be stored using reversible format to support EAP-MD5. This step is required for MD5.

- From the **Active Directory Users and Computers** screen, right-click the Active Directory domain and select **Properties** (not shown)..
- Select **Group Policy,** highlight **Default Domain Policy** and click the **Edit** button (not shown).
- Set **Store password using reversible encryption** to be **Enabled** for the password policy under Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy tree.



Policy	Computer Setting
Enforce password history	1 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption f…	Enabled

Create user names and passwords for the phones and PCs. Configure the phone's MAC as its user name. The default user name for the phone is its MAC address (without colons) with upper case letters. To store password using reversible encryption, check **Store password using reversible encryption** under the **Account** tab. Note that user names are not case sensitive on the Microsoft IAS. Use default for the rest.


00040DEAB5BB Properties

User logon name: 00040DEAB5BB @g250.avaya.com

User logon name (pre-Windows 2000): G250\ 00040DEAB5BB

□ Account is locked out

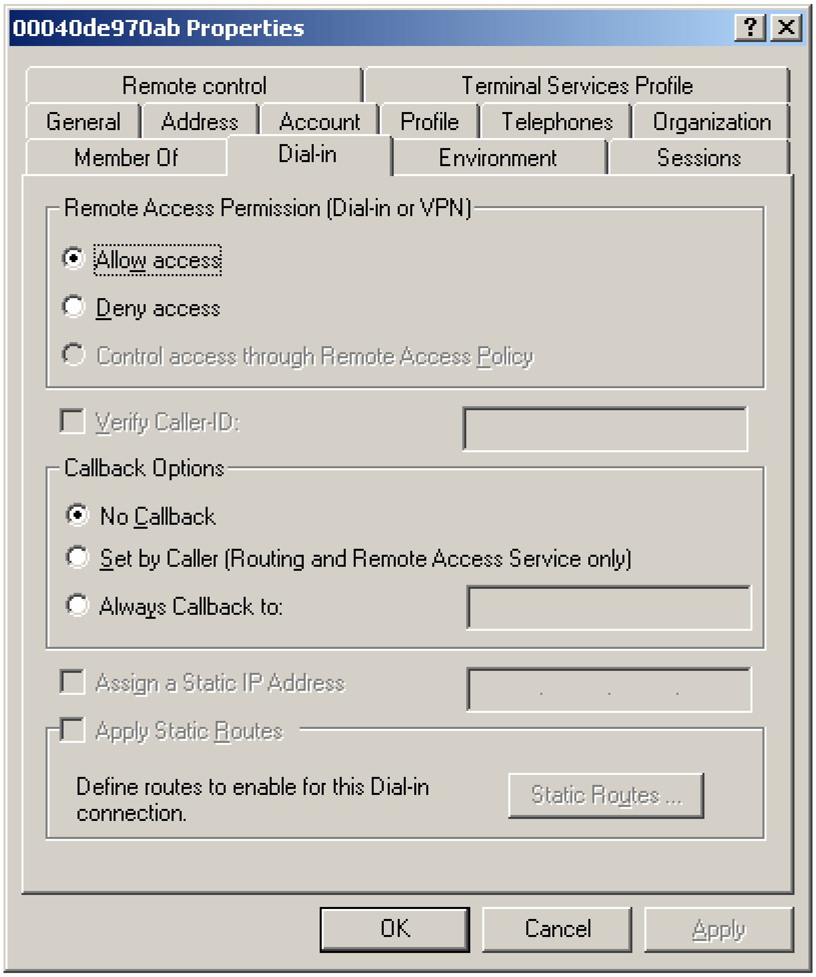
Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
☑ Store password using reversible encryption

Account expires

● Never
○ End of: Friday , December 29, 2006

To enable remote access for a user, from a user account **Properties**; select **Allow access** for **Remote Access Permission** under the **Dial-in** tab. Click **OK**.



00040de970ab Properties

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

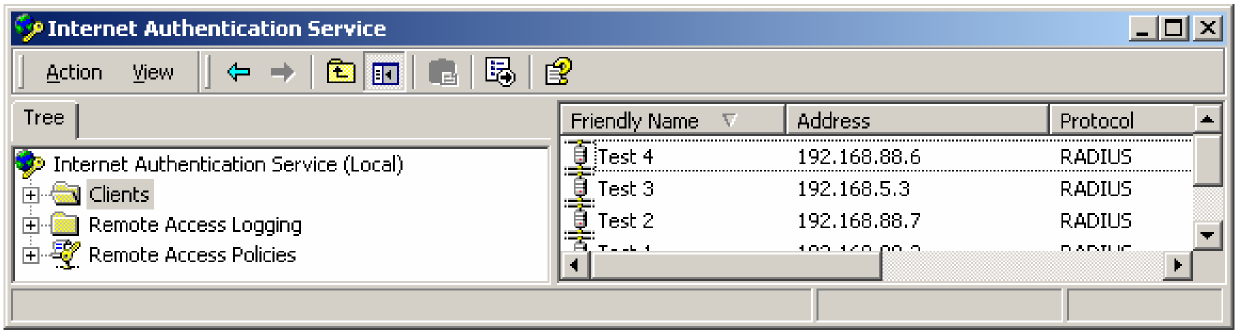
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

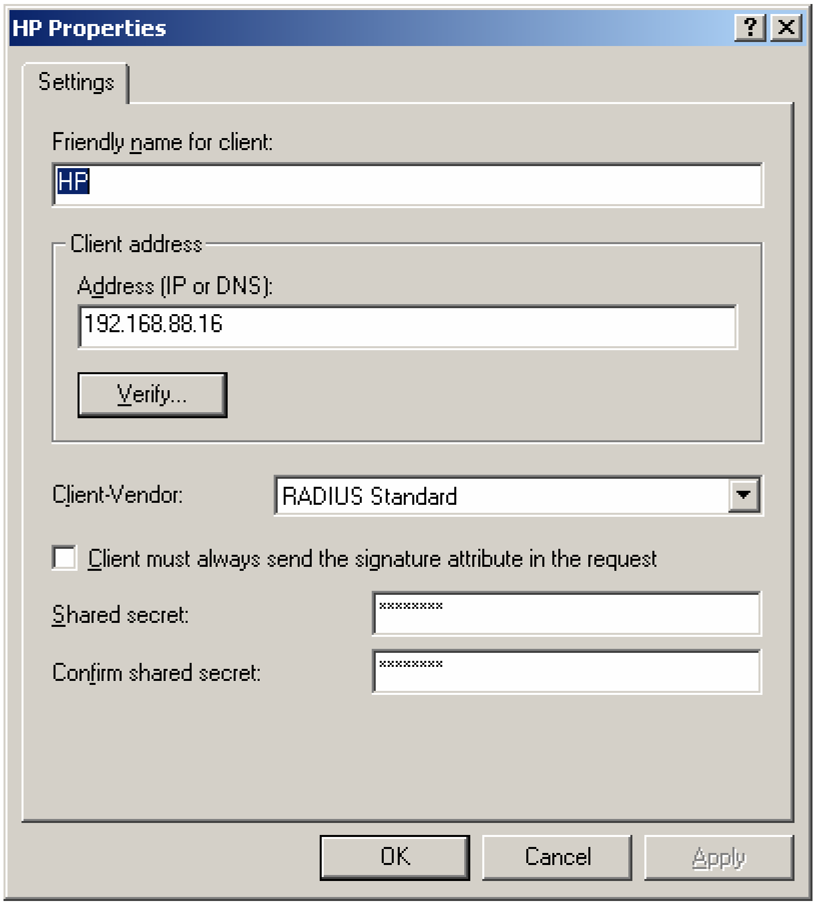
3.4 Configuring the Microsoft IAS

Open the Microsoft IAS by navigating to **Start → Programs → Administrative Tools → Internet Authentication Service.** Right click **Clients** and select **New Client** to add a new client**.**


Internet Authentication Service
Action
View
Tree
Internet Authentication Service (Local)
Clients
Remote Access Logging
Remote Access Policies

Friendly Name	Address	Protocol
Test 4	192.168.88.6	RADIUS
Test 3	192.168.5.3	RADIUS
Test 2	192.168.88.7	RADIUS

The following shows the client configuration for the HP ProCurve switch. The **Client address** and **Shared secret** must match the configuration on the HP ProCurve switch in **Section 3.1**. Use default for the rest. Click **OK**.



Friendly name for client: HP

Address (IP or DNS): 192.168.88.16

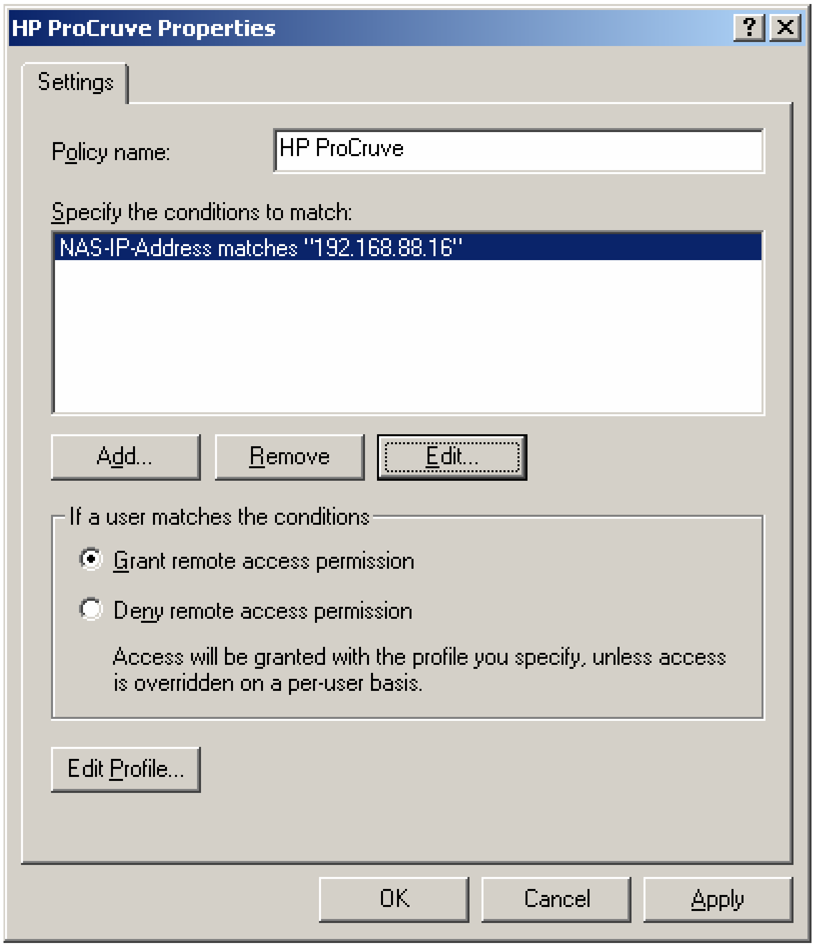
Client-Vendor: RADIUS Standard

□ Client must always send the signature attribute in the request

Shared secret: ********

Confirm shared secret: ********

Right click **Remote Access Policies** and select **New Remote Access Policy** to add a new Remote Access Policy. The following shows the remote access policy configuration for the HP ProCurve switch. The **Specify the conditions to match** is configured to match the NAS-IP-Address. The NAS-IP-Address must be configured to the primary IP address of the HP ProCurve switch (192.168.88.16). Select **Grant remote access permission** under **If a user matches the conditions**. Click **OK**.



HP ProCruve Properties

Policy name: HP ProCruve

Specify the conditions to match:

NAS-IP-Address matches "192.168.88.16"

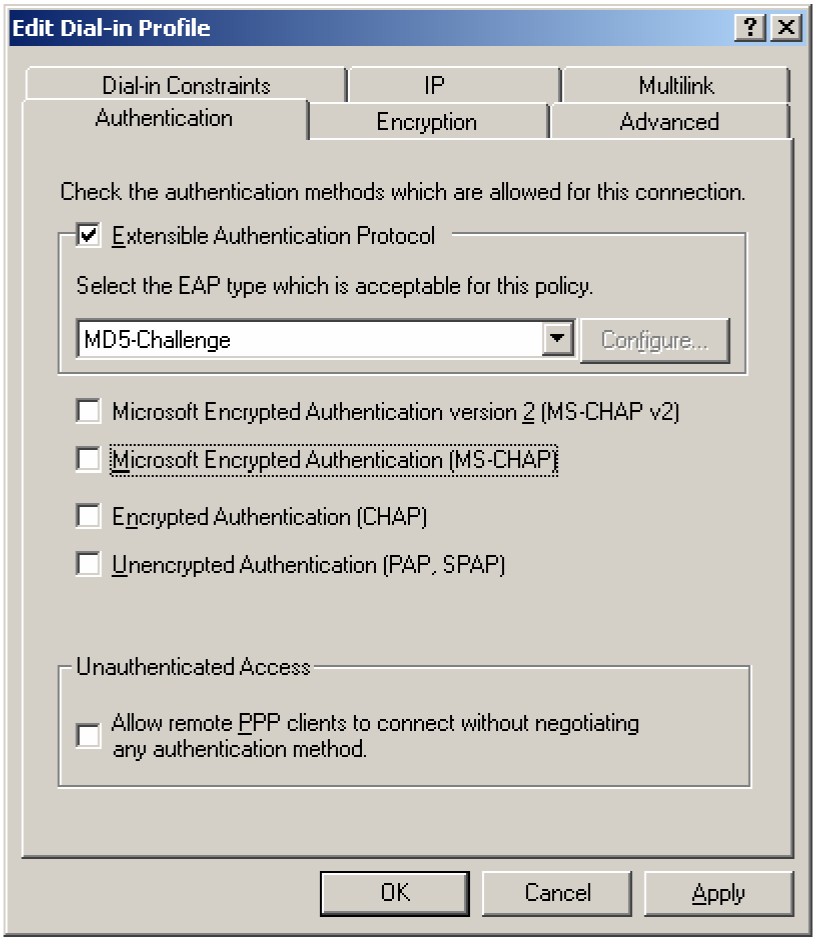
If a user matches the conditions

● Grant remote access permission

○ Deny remote access permission

Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

Click the **Edit Profile…** button and select the **Authentication** tab. Check the **Extensible Authentication Protocol** and select **MD5-Challenge** under **Select the EAP type which is acceptable for this policy**. Click **OK**.



Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

MD5-Challenge

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

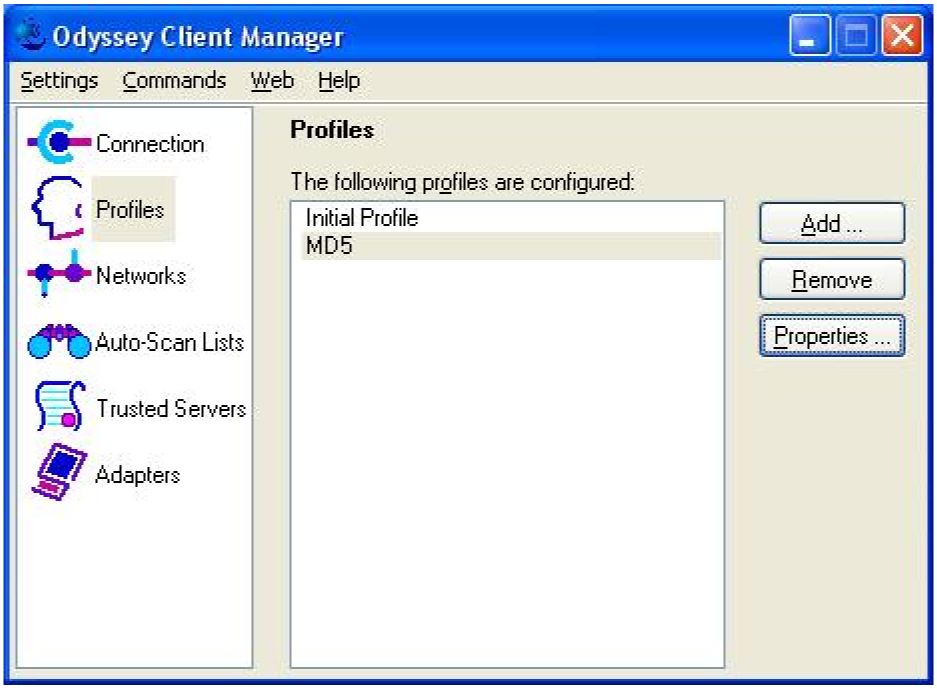
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

3.5 Configuring the Odyssey Client

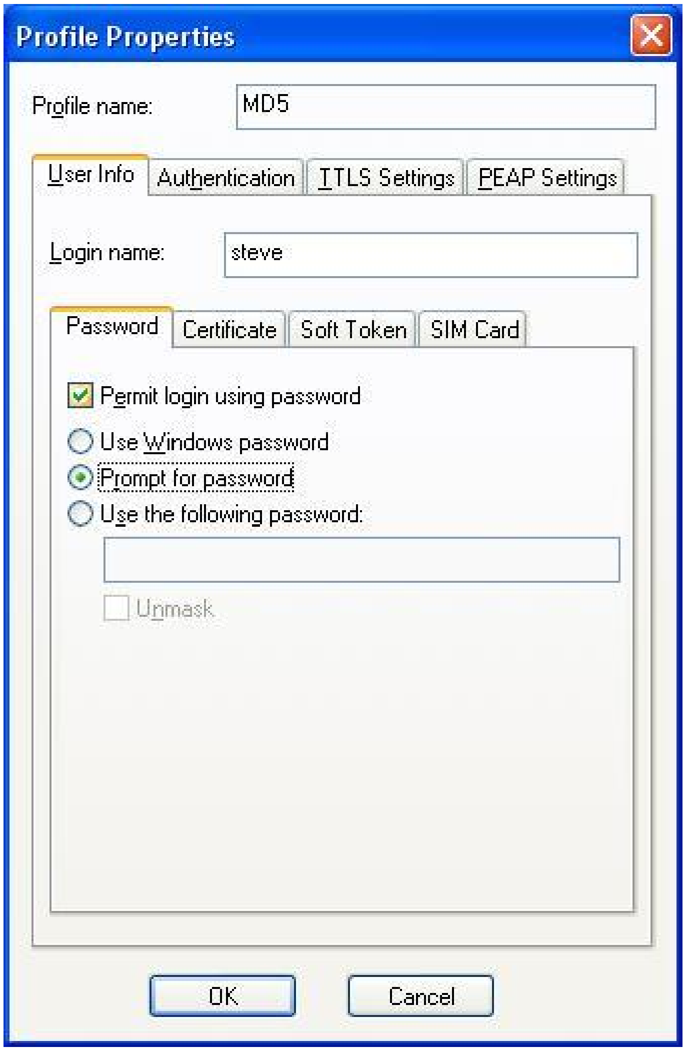
After the Funk Odyssey Client Software is installed on a client PC, start the Funk Odyssey Client Manager by navigating to **Start** → **Programs** → **Funk Software** → **Odyssey Client** → **Odyssey Client Manager**. The following shows the Funk Odyssey Client Manager. Click **Profiles** and then click **Add** or highlight the existing profile and press **Properties**.



The following profiles are configured:

Initial Profile
MD5

The profile named **MD5** has been created. Double-click the **MD5** profile to show the configuration. Click the **User Info** tab in the following screen and enter a **Login name** as configured on the Microsoft IAS. Check **Permit login using password**. Select **Prompt for password** or **Use the following password**. When **Prompt for password** is selected, a window will pop up on the client to request a password when a new connection is made, or the current password fails the authentication.



Profile name: MD5

Login name: steve

☑ Permit login using password

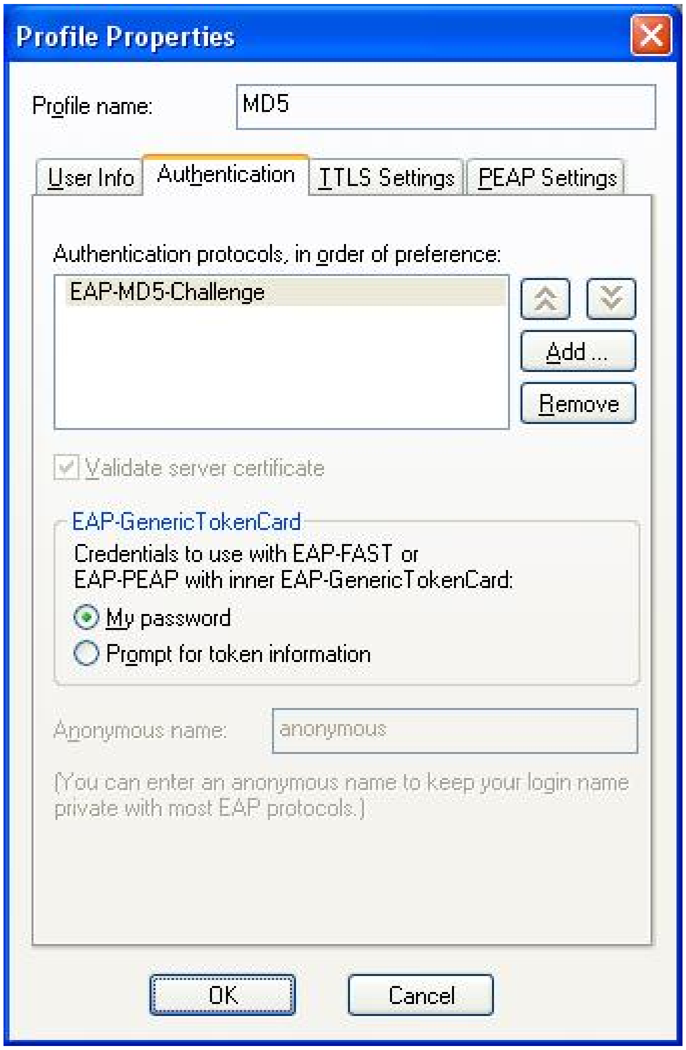
○ Use Windows password

● Prompt for password

○ Use the following password:

□ Unmask

Click the **Authentication** tab from the profile screen and add **EAP-MD5-Challenge** as an authentication protocol. Ignore the **TTLS Settings** and **PEAP Settings** tabs, which are not related to EAP-MD5. Click **OK**.



Profile Properties

Profile name: MD5

Authentication protocols, in order of preference: EAP-MD5-Challenge

☑ Validate server certificate

EAP-GenericTokenCard

Credentials to use with EAP-FAST or EAP-PEAP with inner EAP-GenericTokenCard:

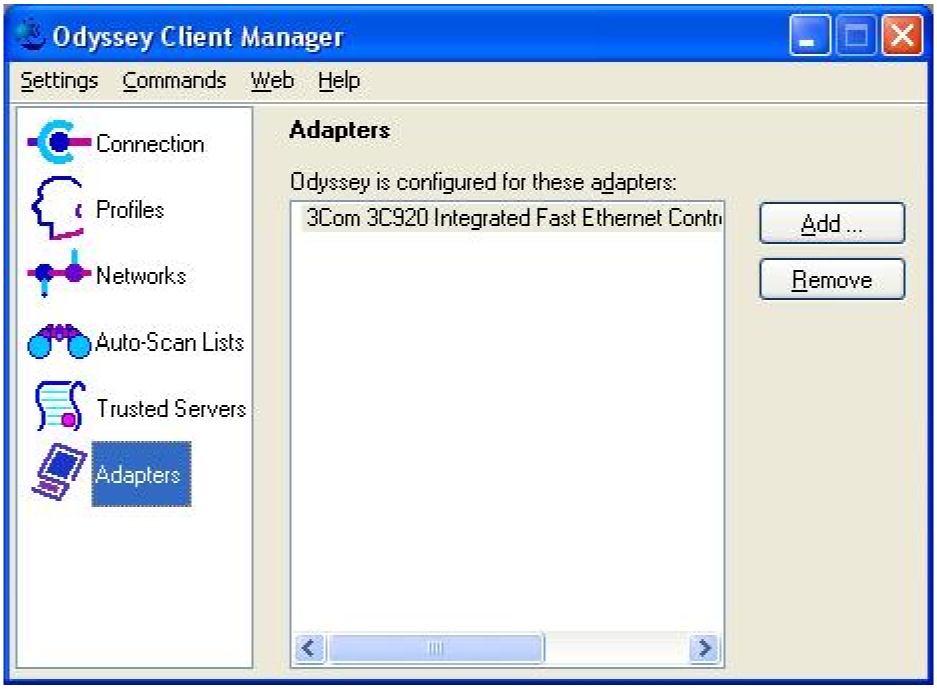
● My password

○ Prompt for token information

Anonymous name: anonymous

(You can enter an anonymous name to keep your login name private with most EAP protocols.)

Click the **Adapters** icon from **Odyssey Client Manager,** and add the wired Ethernet adapter (not shown). The following screen shows the adapter configured for the Odyssey.

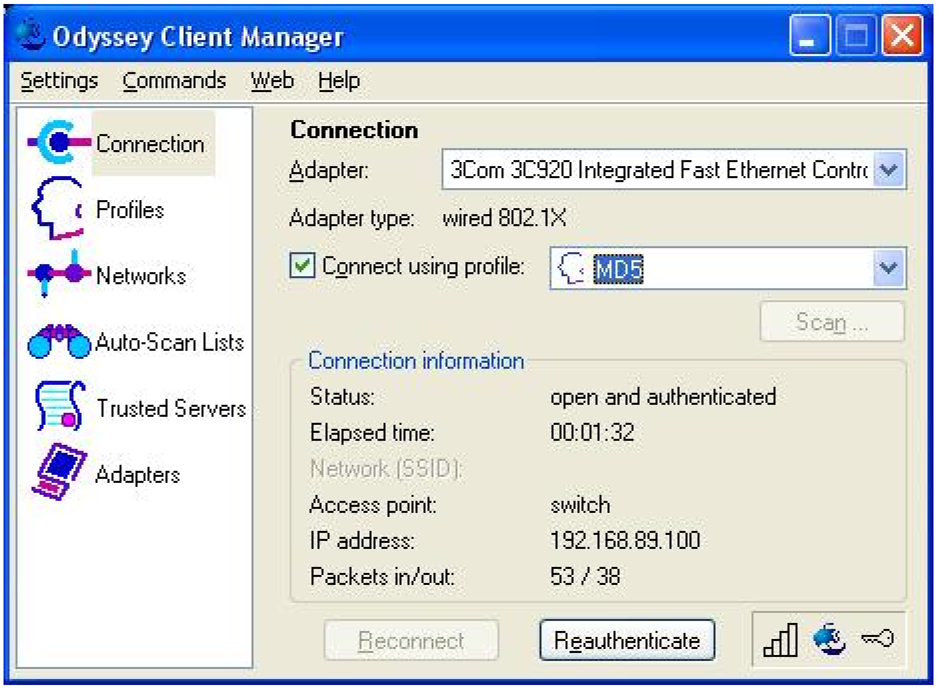


Adapters

Odyssey is configured for these adapters:

3Com 3C920 Integrated Fast Ethernet Contr

Click the **Connection** icon from the **Odyssey Client Manager**. Select the Ethernet adapter in the **Adapter** field. Check the **Connect using profile** box and select the **MD5** as the profile. If the client is authenticated, the **Status** for the **Connection information** should be **open and authenticated**.



Connection

Adapter: 3Com 3C920 Integrated Fast Ethernet Contro

Adapter type: wired 802.1X

☑ Connect using profile: MD5

Connection information

Status: open and authenticated

Elapsed time: 00:01:32

Network (SSID):

Access point: switch

IP address: 192.168.89.100

Packets in/out: 53 / 38

4 Verification

4.1 Verify 802.1X on the HP ProCurve Switch

Use the command **show authentication** to verify that **Port-Access** is enabled with the **EapRadius**.

```
HP# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Local      None       Local      None
  Port-Access | EapRadius
  Webui       | Local      None       Local      None
  SSH         | Local      None       Local      None
  Web-Auth    | ChapRadius
  MAC-Auth    | ChapRadius
```

Use the command **show radius authentication** to display authentication information.

```
HP# show radius authentication

 Status and Counters - RADIUS Authentication Information

  NAS Identifier : HP
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port  Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ----- ---------- ---------- ---------- ---------- --------
  192.168.88.31   1812  5          14         5          5          0
```

Use the command **show port-access authenticator config** to display the port-access configuration. The following screen shows that port-access authenticator is activated on the switch and ports D1 to D4 are configured with the auto mode with the re-authentication period 3600 seconds.

```
HP# show port-access authenticator config

 Port Access Authenticator Configuration

  Port-access authenticator activated [No] : Yes

       | Re-auth Access   Max   Quiet   TX       Supplicant Server   Cntrl
  Port | Period  Control  Reqs  Period  Timeout  Timeout    Timeout  Dir
  ---- + ------- -------- ----- ------- -------- ---------- -------- -----
  D1   | 3600    Auto     2     60      30       30         30       both
  D2   | 3600    Auto     2     60      30       30         30       both
  D3   | 3600    Auto     2     60      30       30         30       both
  D4   | 3600    Auto     2     60      30       30         30       both
```

Use the command **show port-access authenticator** to display the 802.1X status. The **Status Open** indicates that there is an 802.1X client successfully authenticated on a port. The **Status Closed** indicates that there is no 802.1X client successfully authenticated on the port.

```
HP# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes

              Current  Current     % Curr. Rate   RADIUS ACL
  Port Status VLAN ID  Port COS    Limit Inbound  Applied?
  ---- ------ -------- ----------- -------------- -----------
  D1   Open   89       No-override No-override    No
  D2   Open   89       No-override No-override    No
  D3   Open   89       No-override No-override    No
  D4   Open   89       No-override No-override    No
```

Use the command **show mac-address <port#>** to list the authorized MACs on the specified ports. The following screen shows that two MACs are authorized on port D1. One MAC responds to the IP Telephone and the other MAC to the attached PC.

```
HP# show mac-address D1-D4

Status and Counters - Port Address Table - D1

  MAC Address
  -------------
  00040d-9d6471
  001111-28d03b


 Status and Counters - Port Address Table - D2

  MAC Address
  -------------
  00096e-0e57f5


 Status and Counters - Port Address Table - D3

  MAC Address
  -------------
  00040d-eab5ca


 Status and Counters - Port Address Table - D4

  MAC Address
  -------------
  00040d-eab9f9
```

Use the command **show mac-address vlan <VLAN ID>** to list the MAC address for a VLAN. The following screen shows that MAC **001111-28d03b** on port D1 is on VLAN 89. This is the MAC address for the attached PC.

```
HP# show mac-address vlan 89

 Status and Counters - Address Table - VLAN 89

  MAC Address   Located on Port
  ------------- ---------------

  000197-29d3ff D24
  001111-28d03b D1
  00d0c0-ced954 D24
```

The following screen shows the MACs on VLAN 88. The MACs on ports D1 to D4 correspond to the MACs of the phones.

```
HP# show mac-address vlan 88

 Status and Counters - Address Table - VLAN 88

  MAC Address   Located on Port
  ------------- ---------------
  00040d-9d6471 D1
  00040d-eab5ca D3
  00040d-eab9f9 D4
  00096e-0e57f5 D2
  00123f-7910c2 D24
  00d0c0-ced954 D24
```

5 Verify the Avaya IP Telephone Operation

Reset the IP Telephones to the manufacturer's default. Enter the correct password using the default user name (the phone's MAC address) when the phone is prompted for user name and password. Verify that the phone resets and uses Voice VLAN 88 after successful authentication. Verify that the phone can register to Avaya Communication Manager with its extension and password. Verify that calls can be made.

Reset the phone with the current configuration. Verify that the phone can register to Avaya Communication Manager with its extension and password. Verify that calls can be made.

6 Conclusion

As illustrated in these Application Notes, Avaya IP Telephones can be configured as 802.1X supplicants and the HP ProCurve switch can be configured as an 802.1X authenticator. The Avaya IP Telephone and the attached PC can be authenticated individually in different VLANs.

7 Additional References

The following document can be found at http://www.hp.com

[1] *Access Security Guide for the ProCurve Series 6400cl/5300xl/4200vl/3400cl Switches (October 2006)*

The following Application Notes can be found at http://www.avaya.com.

[2] *Configuring 802.1X Protocol On Avaya G250 and G350 Media Gateways For an Avaya IP Telephone With an Attached PC*

[3] *Configuring Link Layer Discovery Protocol (LLDP) and 802.1X Protocol on Extreme Networks BlackDiamond 8810 for an Avaya IP Telephone with an Attached PC*

[4] *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*

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