Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Telephony Infrastructure in a Converged VoIP and Data Network using HP Networking Switches configured with 802.1X Authentication - Issue 1.0

Abstract

The IEEE 802.1X standard defines a client-server based network access control (NAC) 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 Networking switches support 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 Networking switches for an Avaya IP Telephone with an attached PC.

1. Introduction

The 802.1X protocol is an IEEE standard for media-level network access control (NAC), 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 Networking 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 Networking 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 *and there is no default password*. 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.

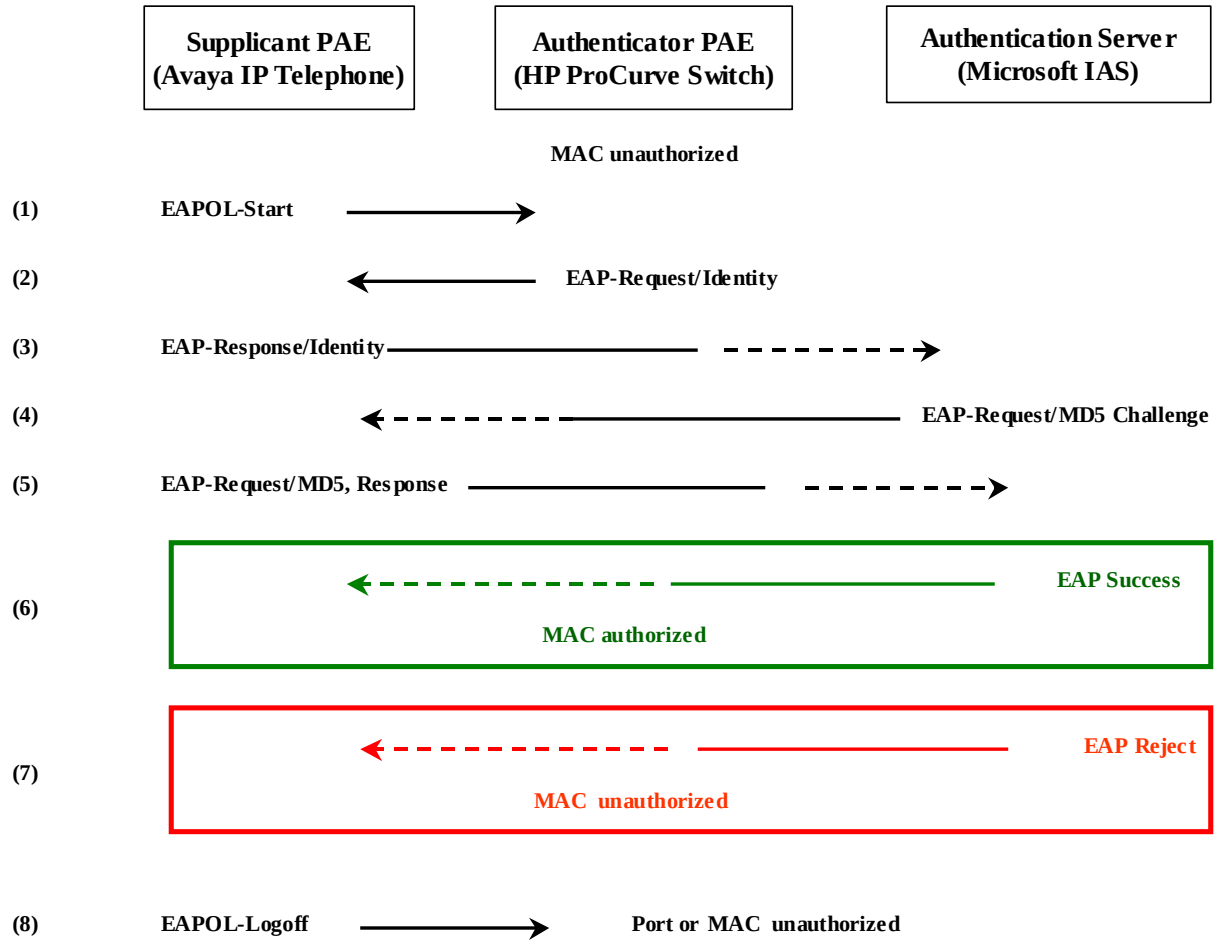


Figure 1: 802.1X Message Exchanges

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 Networking 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 Windows 7 Clients with native 802.1X client software installed. The EAP-MD5 authentication is configured for the IP Telephone and the attached PC is using Microsoft Protected EAP (PEAP-TLS) in these Application Notes.

2. General Test Approach and Test Results

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the following after verifying successful 802.1X authentication:

All test cases were performed manually.

- LAN connectivity between the Avaya and HP Networking products.
- Registration of Avaya H.323 endpoints with Communication Manager.
- Registration of Avaya SIP endpoints with Session Manager.
- VoIP calls, including, hold, transfer and conferencing.
- Configuration of QoS parameters using LLDP
- Configuration of Voice VLAN using LLDP
- Communication Manager Messaging voicemail and MWI works properly.

Compliance testing focused on the 802.1X implementation in the Avaya/HP Networking configuration using "client-based" authentication. Specifically, compliance testing verified proper behavior when 802.1X was enabled and disabled.

2.2. Test Results

The test objectives listed in **Section 2.1** were verified. 802.1X testing was verified by making voice calls and sending data from PC's connected to the Avaya Telephones after verifying successful 802.1X authentication.

Serviceability testing was conducted to verify the ability of the Avaya/HP Networking VoIP solution to recover from adverse conditions, such as power cycling network devices and disconnecting/reconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized was verified.

All of HP Networking products used in the compliance testing successfully passed.

2.3. Support

For technical support on HP Networking products, consult the following support pages by contacting HP Networking customer support at:

- Contact us: http://h17007.www1.hp.com/us/en/contact
- Website Support: http://h17007.www1.hp.com/us/en/support/converter/index.aspx
- Website Product Information: http://h17007.www1.hp.com/us/en/index.aspx

3. Reference Configuration

Figure 2 illustrates the configuration used for compliance testing. The network consisted of Avaya Aura® Communication Manager Server running on an S8300D card that was installed in the G450 Media gateway, Avaya Aura® Session Manager, and IP endpoints including, Avaya IP Telephones, with connected PC's. All Avaya components were connected to the HP Networking switches and voice and data traffic was carried across this infrastructure. To better manage the different traffic types, the voice and data traffic were separated onto different VLANs.

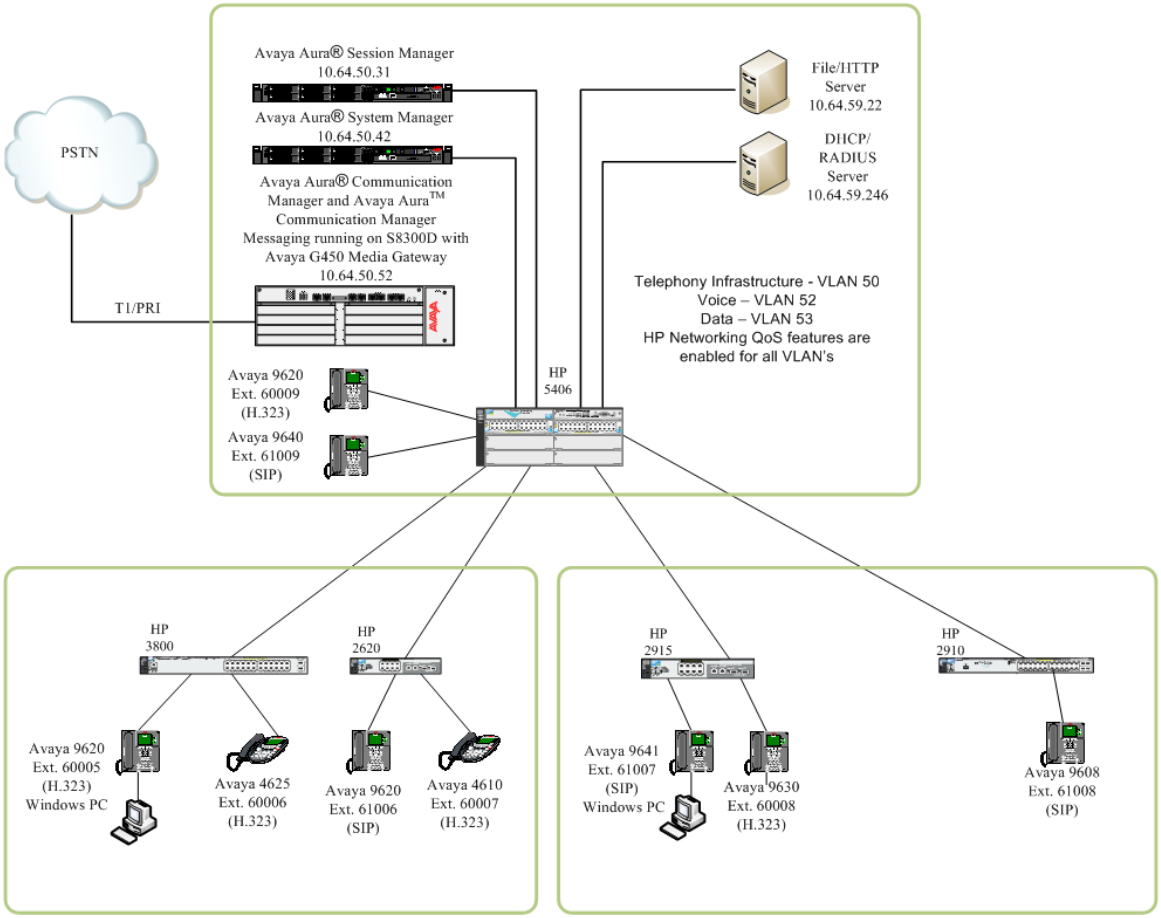


Figure 2: Network Configuration

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300D Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0.1 with SP5.0.1(Patch 19303)
Avaya G450 Media Gateway MGP MM710 T1 Module MM711 Analog Module MM712 DCP Media Module MP80 VoIP-DSP	HW 2 FW 31.20.0 HW 5 FW 22 HW 23 FW 73 HW 7 FW 14 HW 6 FW 67
Avaya Aura® Session Manager	
Avaya Aura® Session Manager HP Proliant DL360 G7	6.1 with SP5
Avaya Aura® System Manager HP Proliant DL360 G7	6.1 with SP5
Avaya Messaging (Voice Mail) Products	
Avaya Aura® Communication Manager Messaging (CMM)	6.0
Avaya Endpoints	
Avaya 96xx Series IP Telephones	(H.323 3.1SP2), (SIP 2.6.6.0)
Avaya 96x1 Series IP Telephones	(H.323 S6.010f), (SIP 6.0.3)
Avaya 46xx Series IP Telephones	2_9_1
Linux FreeRADIUS	
DELL PowerEdge 850	FreeRADIUS Version 2.1.10
Windows 7 Clients	
Lenovo ThinkStation S20	Windows 7 Enterprise Service Pack 1
HP Networking Products	
HP 3800	https://h10145.www1.hp.com/downloads/SoftwareReleases.aspx?ProductNumber=J9573A KA.15.03.3006
HP 2620	https://h10145.www1.hp.com/downloads/SoftwareReleases.aspx?ProductNumber=J9623A RA.15.06.0009
HP 2915	https://h10145.www1.hp.com/downloads/SoftwareReleases.aspx?ProductNumber=J9562A A.14.15

Equipment	Software/Firmware
HP 2910	https://h10145.www1.hp.com/downloads/SoftwareReleases.aspx?ProductNumber=J9145A W.14.70
HP 5406	https://h10145.www1.hp.com/downloads/SoftwareReleases.aspx?ProductNumber=J9532A K.15.07.0008

5. 802.1X Configurations

The HP Networking switches support "Client-Based" authentication to ensure multiple clients sharing the same port are authenticated individually. This is a required to support secure authentication of both the Avaya IP Telephone with an attached PC to be independently authenticated and provisioned in different VLANs when connected to HP Networking switches.

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 "<mute>craft#" or "<mute>27283#") 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 (**recommended mode**).

- **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 special PAE group 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 for improved security. This is because when the phone is in the **p-t w/Logoff** mode, the phone will do a proxy logoff on behalf of the attached PC when the PC is physically disconnected. When the HP Networking switches receive the EAPOL logoff message, it will immediately remove the PC from the authorized MAC list.

When proxy logoff is not enabled, the HP Networking switch is unable to detect a link loss when the PC is disconnected from the phone and will defer cleanup of the authorized MAC list until no more packets with the PC MAC address have been seen for a duration specified by the 'logoff-period' (default timeout is 5 min).

NOTE: it is strongly recommended to not use "port-based" 802.1X authentication on ports connected to IP phones, since this mode only authenticates the first client device that connects. As long as the port has been opened by an authenticated device, the port will remain opened until that device disconnects or the authentication session expires. Thus, once an IP phone is authenticated, any device plugged into the back of the phone would have full access to the network without needing to authenticate and effectively bypassing Network Access Control.

5.1. Configuring 802.1X on the HP Networking 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
HP-E2620-24-PoEP(config)# aaa authentication port-access eap-radius

! --- Configure the radius server to the IAS
HP-E2620-24-PoEP(config)# radius-server host 10.64.59.246 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-E2620-24-PoEP(config)# aaa port-access authenticator 1-3 control
 authorized        Force authorized.
 auto              Auto.
 unauthorized      Force unauthorized.
```

The following commands configure ports 1 through 3 to the 802.1X authenticator ports and the control mode to auto.

```
HP-E2620-24-PoEP(config)# aaa port-access authenticator 1-3

HP-E2620-24-PoEP(config)# aaa port-access authenticator 1-3 control auto
```

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

```
HP-E2620-24-PoEP(config)# 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 1-3 are configured with untagged VLAN 53 and tagged VLAN 52. Port 26, which is connected to the L3 switch, is configured with tagged VLAN 53 and 52.

```
vlan 53
   name "Data"
   untagged 1-3,23
   ip address 10.64.53.65 255.255.255.0
   tagged 26
   exit
vlan 52
   name "Voice"
   tagged 1-3,26
   no ip address
   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. The primary VLAN is configured to VLAN 53 in these Application Notes. The VLAN 53 IP address 10.64.53.65 will be used as the NAS-IP-address.

```
HP-E2620-24-PoEP(config)# primary-vlan 53
```

By default, 802.1X re-authentication is not enabled on HP Networking switches. It is recommended to enable re-authentication for improved security. In the sample configuration, the re-authentication period is configured to 3600 seconds to force a re-authentication once an hour.

The HP Networking switches also support client limits for 802.1X authentication, which enables the "client-based" mode and also limits the maximum number of endpoints that can be simultaneously authenticated on a given port.

For proper security, it is strongly recommended to change the 802.1X mode from "port-based" (default) to "client-based" for ports directly connected to IP phones. This is done by setting the client-limit parameter to at least one, and also to match the number of endpoints expected on a port. For typical IP phone deployments, the client-limit should be configured to 2, when an Avaya phone with attached PC needs to be supported.

```
HP-E2620-24-PoEP(config)# aaa port-access authenticator 1-3 reauth-period 3600
HP-E2620-24-PoEP(config)# aaa port-access authenticator 1-3 client-limit 2
```

5.2. Configuring RADIUS Server

In the sample configuration, Linux FreeRADIUS was used as the authentication server. The intent of this section is to illustrate relevant aspects of the configuration used for the testing.

For the compliance test the following entry was added to the **/etc/freeradius/clients.conf** file to support the HP Networking Switches.

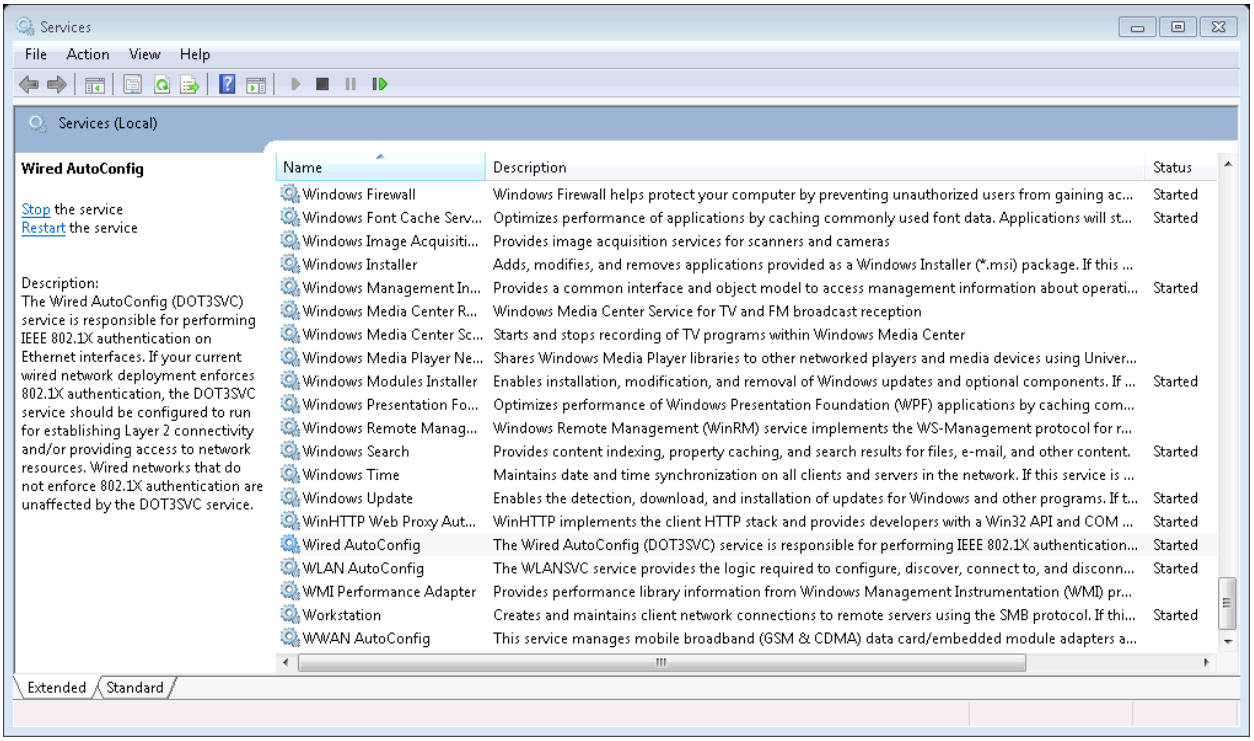
```
client 10.64.53.0/24 {
      # This is the shared secret between the Authenticator (the
      # access point) and the Authentication Server (RADIUS).
      secret          = 1234567890123
      shortname       = hp
   }
```

The following entries were added to the **/etc/freeradius/usres** file to support ther Avaya Telephones.

```
#9620-1
00040DEBCE4A    Cleartext-Password := "123456"
#9620-2
00040DEC4F94    Cleartext-Password := "123456"
#1616-1
00073B93158F    Cleartext-Password := "123456"
#9641-2
3CB15B5FB107    Cleartext-Password := "123456"
#9630-1
00040DEC520A    Cleartext-Password := "123456"
#4610
00096E11814A    Cleartext-Password := "123456"
#4625
00040D9B5F08    Cleartext-Password := "123456"
#9608-1
B4B017801378    Cleartext-Password := "123456"
#9620-3
00073BC4F52B    Cleartext-Password := "123456"
#9620-4
00073BC4F4BE    Cleartext-Password := "123456"
#9640-1
001B4F29F94C    Cleartext-Password := "123456"
#PC Users
interop         Cleartext-Password := "123456"
```

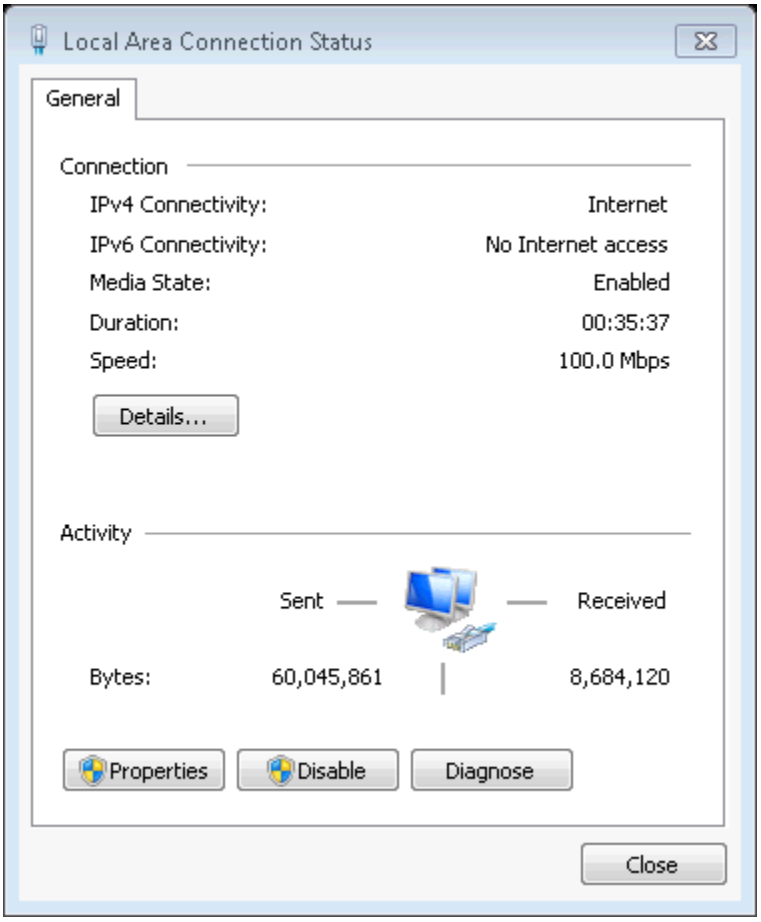
6. Configuring 802.1X Windows 7 Client

Click the Windows Start button and then enter **services** in the search box (Not Shown) to open the Services window. Scroll to the bottom of the list and enable the **Wired AutoConfig** service.

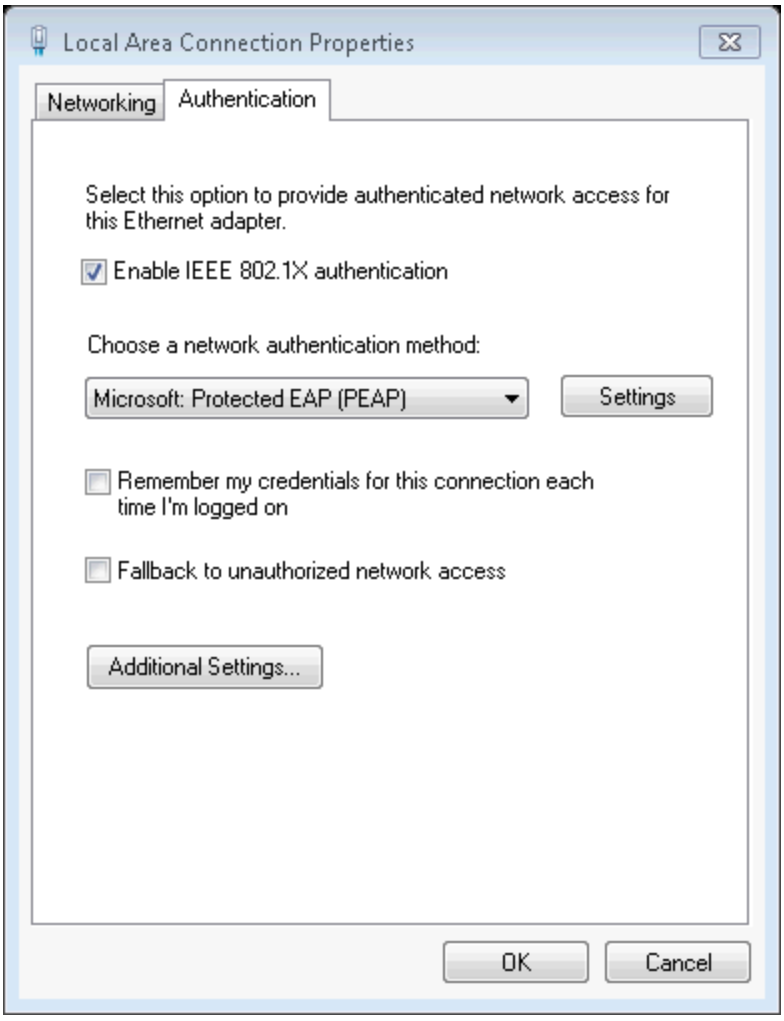


Click the Windows Start button and then enter **ncpa.cpl** in the search box (Not Shown) to open the Network Connections window.

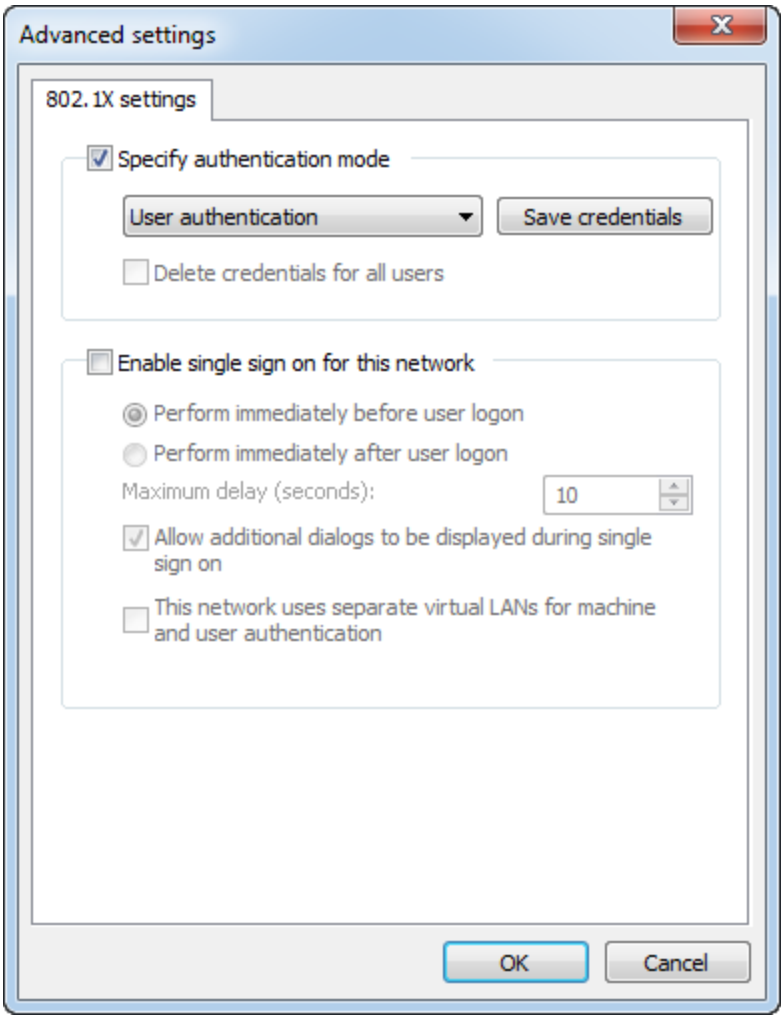
Double click the LAN connection (Not Shown) and then click the **Properties** button.

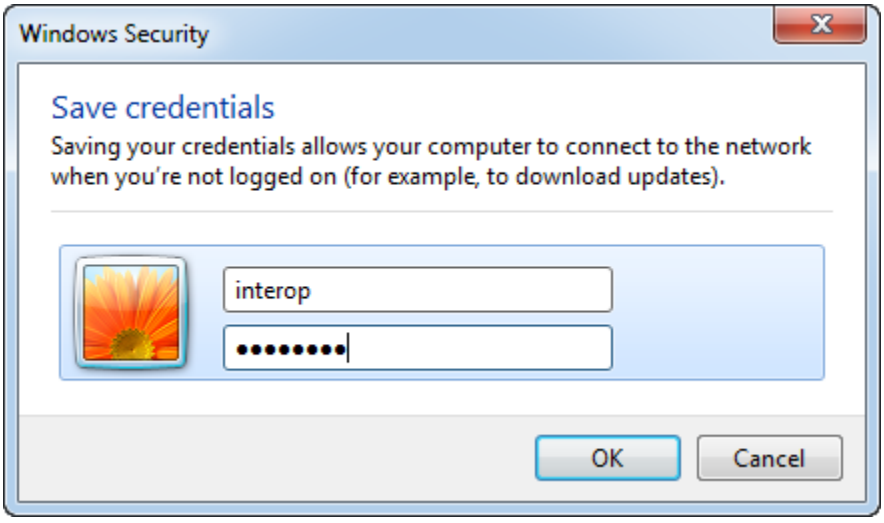


From the Local Area Connection Properties window click the **Authentication** Tab and check **Enable IEEE 802.1X authentication** box. Continue by clicking the **Additional Settings** button.



From this window check the **Specify Authentication Mode** box and select the appropriate authentication mode from the pull-down box. The compliance test used **User Authentication** and required adding the user credentials by clicking the **Save Credentials** button and adding the credentials.





Once completed click the **OK** buttons on each of the open windows and the LAN connection should be successfully authenticated and become active.

7. Verification Steps

7.1. Verify 802.1X on the HP ProCurve Switch

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

```
HP-E2620-24-PoEP# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

             | Login      Login        Login
  Access Task | Primary    Server Group Secondary
  ----------- + ---------- ------------ ----------
  Console     | Local                   None
  Telnet      | Local                   None
  Port-Access | EapRadius  radius       None
  Webui       | Local                   None
  SSH         | Local                   None
  Web-Auth    | ChapRadius radius       None
  MAC-Auth    | ChapRadius radius       None
  SNMP        | Local                   None

             | Enable     Enable       Enable
  Access Task | Primary    Server Group Secondary
  ----------- + ---------- ------------ ----------
  Console     | Local                   None
  Telnet      | Local                   None
  Webui       | Local                   None
  SSH         | Local                   None
```

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

```
HP-E2620-24-PoEP# show radius authentication

 Status and Counters - RADIUS Authentication Information

  NAS Identifier : HP-E2620-24-PoEP
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ---- ---------- ---------- ---------- ---------- --------
  10.64.59.246    1812 0          183        92         88         3
```

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 1 to 3 are configured with the auto mode with the re-authentication period 3600 seconds.

```
HP-E2620-24-PoEP# show port-access authenticator config

 Port Access Authenticator Configuration

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       | Re-auth   Access  Max  Quiet  TX      Supplicant Server  Cntrl
  Port | Period    Control Reqs Period Timeout Timeout    Timeout Dir
  ---- + --------- ------- ---- ------ ------- ---------- ------- -----
  1    | 3600      Auto    2    60     30      30         300     both
  2    | 3600      Auto    2    60     30      30         300     both
  3    | 3600      Auto    2    60     30      30         300     both
```

Use the command **show port-access authenticator clients** to display the 802.1X status. The **Client Status** indicates that there is an 802.1X client successfully authenticated on a port.

```
HP-E2620-24-PoEP# show port-access authenticator clients

 Port Access Authenticator Client Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

  Port Client Name           MAC Address   IP Address      Client Status
  ---- --------------------- ------------- --------------- ----------------
  1    00073B93158F          00073b-93158f n/a             Authenticated
  2    00040DEC4F94          00040d-ec4f94 n/a             Authenticated
  2    interop               cc52af-3d7c9b n/a             Authenticated
```

7.2. 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 phones are prompted for user name and password. Verify that they reset and use Voice VLAN 52 after successful authentication. Verify that the H.323 phones can register to Communication Manager and the SIP phones to Session Manager. Verify that calls can be made.

8. Conclusion

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Telephony Infrastructure connected to HP Networking Switches. The HP Networking Switches implemented 802.1X authentication for Avaya IP Telephones and PC's connected to those phones. HP Networking successfully passed the compliance test. Refer to **Section 2.2** for more details and listed observations.

9. Additional References

The documents referenced below were used for additional support and configuration information.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya* Aura® *Communication Manager*, June 2010, Release 6.0, Issue 6.0, Document Number 03-300509, available at http://support.avaya.com.

[2] *Administering Avaya* Aura® *Session Manager*, October 2010, Issue 1.1, Release 6.1, Document Number 03-603324, available at http://support.avaya.com.

[3] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1*, November 2009, Document Number 16-300698.

Product information for the HP Networking Switches may be found at http://h17007.www1.hp.com/us/en/products/switches/index.aspx

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