



Avaya Solution & Interoperability Test Lab

802.1x Configuration of Avaya Ethernet Routing Switches (ERS), with Avaya one-X® 9600 Series IP Deskphones and Avaya 1600 Series IP Deskphones - Issue 1.0

Abstract

These Application Notes describe the configuration of Multiple Host Multiple Authentication (MHMA) on Avaya Ethernet Routing Switches (ERS) 5520 and 4548. This will support 802.1x authentication with Avaya one-X® 9600 Series and Avaya 1600 Series IP Deskphones. 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. In this configuration, the IP telephone and a PC attached to the phone are authenticated separately.

1. Introduction

The sample network outlined in these Application Notes consists of Avaya ERS 5520-48T-PWR and 4548GT-PWR switches, serving as the connection point for the Avaya IP phones to connect into the network. The Ethernet switch ports are configured to support 2 VLANs, one for voice and one for data. The voice VLAN supports Avaya IP phone traffic and the data VLAN supports PC traffic. Multiple Host Multiple Authentication (MHMA) is enabled on these Ethernet ports to support 802.1x authentication of the phone and PC separately. The FreeRADIUS server is configured to supply VLAN information to the IP phones. **Figure 1** illustrates the configuration used in these Application Notes.

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

- **Supplicant** – Client device requesting network access (e.g. IP phones and attached PCs).
- **Authenticator** – Network device that facilitates the Supplicant authorization requests (e.g. Avaya ERS 5520).
- **Authentication Server** – A Remote Authentication Dial-in User Server (RADIUS) which provides the authentication service (e.g. FreeRADIUS server).

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

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

In a Multiple Host Multiple Authentication configuration the IP telephone and the attached PC must independently request access to the network by specifying a username and password. Therefore there are separate entries for each Supplicant device configured on the RADIUS server (see **Section 4.2**).

The Avaya IP telephones support 802.1x except for the A175 on its wired ports at the time of this interoperability testing. These phones use their MAC addresses as their username by default and there is no default password.

The Avaya IP telephones support three 802.1x Pass-Thru modes for attached PCs. The name of the modes can vary between the telephone models.

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

There are also three Supplicant modes that the IP telephone can operate in. The name of the modes can vary between the telephone models.

- **Enabled or Unicast-Only** -The Phone will operate as a Supplicant using Unicast.
- **Enabled with Multicast** - The Phone will operate as a Supplicant using Unicast and Multicast.
- **Disabled** - The Phone will not operate as a Supplicant. This mode should not be used in a Multiple Host Multiple Authentication (MHMA) configuration.

The Authenticator device may require information from the RADIUS called attributes. Attributes specify additional authorization information such as whether access to a particular VLAN is allowed for a Supplicant. In this reference configuration the FreeRADIUS server is configured to tell the ERS Switches that a Supplicant (IP telephone) is allowed on the voice VLAN (see **Section 4.2**).

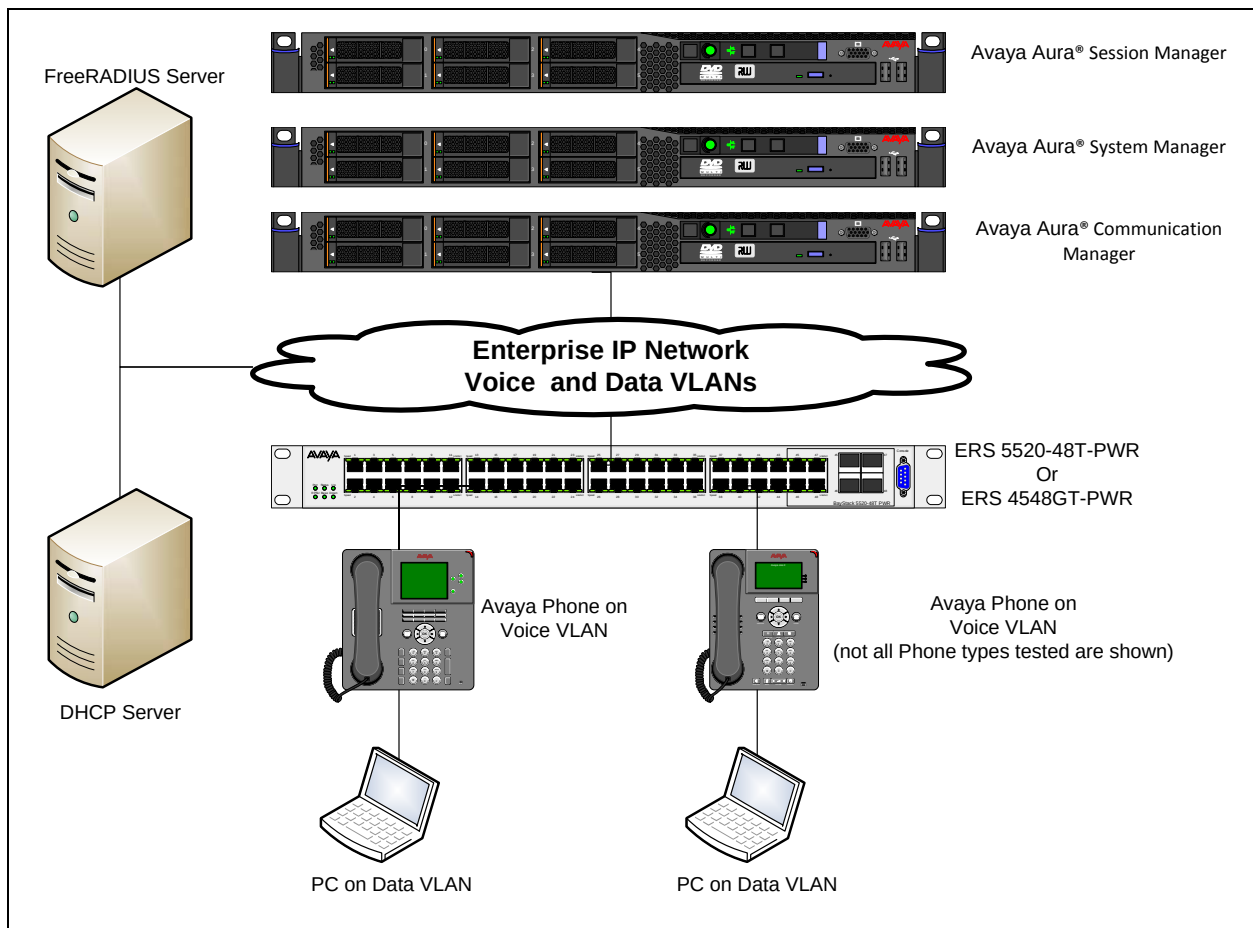


Figure 1: Avaya Interoperability Test Lab Reference Configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:
All of the telephone firmware versions used for this sample configuration are generally available with the exception of the Avaya A175.

Equipment	Software/Firmware
Avaya S8800 Server	Avaya Aura® System Manager 6.1.0 Build No. - 6.1.0.0.7345-6.1.5.9
Avaya S8800 Server	Avaya Aura® Communication Manager 6.1.0 Build No. - 6.1.0.5.7420-6.1.5.2
Avaya S8800 Server	Avaya Aura® Session Manager 6.1.1 Build No. - 6.1.1.0.611004-6.1.1.611017
Avaya Ethernet Routing Switch 4548GT-PWR	FW: 5.3.0.3 SW: V5.5.0.002
Avaya Ethernet Routing Switch 5520-48T-PWR	FW: 6.0.0.13 SW: V6.2.2.022
Avaya 1608-I Deskphone (H323)	ha1608ua1_300B.bin hb1608ua1_300B.bin
Avaya one-X® 9621 Deskphone (H323)	S9621_41HALBR6_0_16T_V452.tar S96x1_UKR_V7_V7.tar
Avaya one-X® 9670G Deskphone (H323)	ha9670ua3_1_02_S.bin hb9670ua3_1_02_S.bin
Avaya one-X® 9608 Deskphone (SIP)	S96X1_SALBR6_0_1_V452.tar S96x1_UKR_V4_V4.tar
Avaya one-X® 9650C Deskphone (SIP)	SIP96xx_2_6_4_0.bin hb96xxua3_00.bin
Avaya one-X® 9611G Deskphone (H323)	S9608_11HALBR6_0_16T_V452.tar S96x1_UKR_V7_V7.tar
Avaya one-X® 9620L Deskphone (H323)	Ha96xxua3_1_02_S.bin Hb96xxua3_1_02_S.bin
Avaya one-X® 9621G Deskphone (SIP)	S96x1_SALBR6_0_1_V452.tar S96x1_UKR_V4_V4.tar
Avaya A175 Desktop Video Device with the Avaya Flare® Experience	System Image: SIP_A175_1_1_0_007001.tar Kernel: 2.6.31.6-17.1.moblin2-mojo
Ubuntu Server	11.04
FreeRADIUS Server	2.1.11

Table 1: Equipment List

3. Configure the Avaya ERS 5520 or 4548

This section describes the configuration for Avaya ERS 5520 and 4548 switches as shown in **Figure 1** using the Avaya Command Line Interface (ACLI). In this example the data VLAN is 7 and the voice VLAN is 8. Port 48 is used as the uplink trunk port to the LAN and is configured for tagging.

1. Log into the Avaya ERS switch and enter **enable** mode.
2. Enter into configuration mode by typing **configure terminal**.
3. Configure the voice and data VLANs with the commands shown in **Figure 2**.

```
4548GT-PWR(config)#vlan configcontrol autopvid
4548GT-PWR(config)#vlan create 8 name voice type port
4548GT-PWR(config)#vlan create 7 name data type port
4548GT-PWR(config)#vlan members add 8 all
4548GT-PWR(config)#vlan members add 7 all
4548GT-PWR(config)#vlan members remove 1 all
4548GT-PWR(config)#auto-pvid
4548GT-PWR(config)#vlan ports 48 tagging tagall
```

Figure 2: ACLI Commands for VLAN Configuration

4. Configure the ERS Switch for Multiple Host Multiple Authentication (MHMA) with the commands shown in **Figure 3**. This will configure the ERS ports to require attached devices to authenticate before they can access the network.

```
4548GT-PWR(config)#radius-server host 10.10.97.249 key thepwd
→thepwd is the Password sent to the RADIUS server at IP 10.10.97.249
4548GT-PWR(config)#eapol multihost use-radius-assigned-vlan
4548GT-PWR(config)#eapol multihost multivlan enable
4548GT-PWR(config)#eapol multihost voip-vlan 1 vid 8
→This sets VLAN 8 for VoIP
4548GT-PWR(config)#eapol enable
4548GT-PWR(config)#
4548GT-PWR(config)#interface fastEthernet all
4548GT-PWR(config-if)#eapol port 1-10 status auto
4548GT-PWR(config-if)#eapol multihost port 1-10 use-radius-assigned-vlan
4548GT-PWR(config-if)#eapol multihost port 1-10 eap-mac-max 2
→Only 2 MAC addresses can authenticate on each port from 1 to 10
4548GT-PWR(config-if)#eapol multihost port 1-10 enable
```

Figure 3: ACLI Commands for MHMA Configuration

4. FreeRADIUS Configuration

The configuration in this section is for FreeRADIUS 2.1.11 running on Ubuntu Server 11.04.

4.1. Define the Avaya ERS Switches as Clients

The ERS 5520 and 4548 Switches must be configured in FreeRADIUS as clients. This is done by adding client configuration to file `clients.conf` located at `/etc/freeradius`. The secret value below must match the key value configured on the ERS Switches in **Section 3**.

1. From the FreeRADIUS console change to directory `freeradius` with the command **`cd /etc/freeradius`**.
2. Open the file `clients.conf` for editing. The vim editor can be used by entering the command **`sudo vim clients.conf`**.
3. Go to the end of the file and add the required client configuration. The following figure shows an example of a configuration for two clients.

```
client 10.10.97.250 {  
    secret      = thepwd  
    shortname   = ERS5520  
}  
client 10.10.97.251 {  
    secret      = thepwd  
    shortname   = ERS4548  
}
```

→Management IP of the ERS5520
→Authentication key
→Name of client

Figure 4: FreeRADIUS Client configuration

4. Save and close the file.

4.2. Define the Avaya Telephones and PCs as Users

Every telephone and PC that will be authenticated must be defined as users in FreeRADIUS. This is done by adding configuration to file “users” located at /etc/freeradius.

1. From the FreeRADIUS console change to directory freeradius with the command **cd /etc/freeradius**.
2. Open the file users for editing. The vim editor can be used by entering the command **sudo vim users**
3. Go to the end of the file and add the required configuration. The following figure shows an example of a configuration for a PC and an IP Telephone. For the PC “tim” is the User name and “12345” is the MD5 password. The IP telephone uses its MAC address as the default User name. In the following example this is the “3cb15b5ed97f”. The MD5 password for the IP telephone has also been set to “12345” in the example configuration. The Tunnel commands are used to tell the ERS Switches that the IP Telephone can access the voice VLAN. A Tunnel-Type of 13 indicates VLAN. The Tunnel-Medium-Type of 6 is for 802 media plus Ethernet. Tunnel-Private-Group-ID = “voice” is used to indicate that the VLAN named voice is to be used.

```
# Config for PC
tim    Cleartext-Password := "12345"
# Config for IP Telephone
3cb15b5ed97f    Cleartext-Password := "12345"
                Tunnel-Type = 13,
                Tunnel-Medium-Type= 6,
                Tunnel-Private-Group-ID = "voice"
```

Figure 5: FreeRADIUS User Configuration

4. Save and close the file.

4.3. Applying Changes to the clients.conf and users Files

Once the clients.conf and the users files have been modified and saved, FreeRADIUS must be restarted for the changes to take effect. The following table shows commands that can be used with FreeRADIUS.

Command	Description
sudo freeradius -X	This will start FreeRADIUS in debug mode. Authentication information is displayed to the console. After the command is executed "Ready to process requests" should be displayed. <Ctrl> C can be used to stop FreeRADIUS in this mode.
sudo freeradius start	This will start FreeRADIUS as a task running in the background.
sudo /etc/init.d/freeradius stop	This will stop FreeRADIUS
ps -ef grep radius	This command can be used to determine if FreeRADIUS is currently running.

Table 2: FreeRADIUS Commands

Note: if "Error binding to port for 0.0.0.0 port 1812" is displayed after entering the command "sudo freeradius -X" it is because FreeRADIUS is already running.

5. IP Telephone Configuration

This section describes the configuration for the Avaya IP telephones. As per **Section 1** there are settings on the phones for Pass-Thru and for phones supplicant operation. For these Application Notes, all IP Telephones were tested with the Pass-Thru setting turned on (without Logoff) and the supplicant mode set to Enabled (Unicast-Only).

5.1. Configuration of 9600 Series IP Telephones

To configure the 802.1x settings on Avaya one-X® 9600 series IP Telephones the <**Mute**> **CRAFT** command can be entered on the Telephone.

1. On the IP Telephone enter <**Mute**>, **C,R,A,F,T** or (<Mute>,2,7,2,3,8). The Phone will now be in a setup menu.
2. Select **802.1x** from the menu.
3. Select **Pass-Thru** and configure it to ON (without Logoff).
4. Select **Supplicant** and configure it to Enabled or Unicast-Only.

5.2. Configuration of 1600 Series IP Telephones

The 1600 series IP Telephones use different commands to change the phone settings. To access the 802.1x configuration menu enter <**Mute**>, **8,0,2,1,X**. Then follow steps 3 and 4 from **Section 5.1**.

5.3. IP Telephone Authentication

After defining the phone's 802.1x ID and password in the RADIUS server, the ID and password must be administered on the phones. The MAC address of the phone can be used as its 802.1x ID. The Avaya IP telephones use their MAC addresses by default for the User ID; however, an 802.1x password must be provisioned. The phones 802.1x authentication values must match those specified in the FreeRadius server users file.

1. When the phone boots for the first time, or after performing Craft level "CLEAR" or "802.1x" configuration changes, the IP Telephone will display the following by default, where xxxxxxxxxxxx is the MAC address of the phone.

802.1x ID=xxxxxxxxxxxx
#=OK New=

2. Press # to accept the MAC address as the phone's 802.1x ID.
3. The Phone will then prompt for the Password as follows.

Password=
#=OK

4. Enter the password configured in the FreeRADIUS user file in **Section 4.2** for this phone and then press #. The phone will now authenticate with FreeRADIUS and be assigned to the voice VLAN. Next the phone will receive an IP address from the DHCP server on the Voice Subnet and will then register.

6. Windows XP Configuration for 802.1x

When Multiple Host Multiple Authentication (MHMA) is configured on the ERS Switches, a PC connected to an Avaya IP Telephone PC port must authenticate separately from the telephone. The PC must be configured to provide 802.1x credentials. Windows XP provides an embedded 802.1x Supplicant client. Add-on 802.1x client programs are also available. These Application Notes refer to the Windows XP embedded 802.1x authentication process.

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

1. Before connecting the PC to the Avaya IP telephone, go to **Start → Control Panel → Network Connections** (in the “Classic View”). Select the appropriate network interface; right click on it and Select Properties.

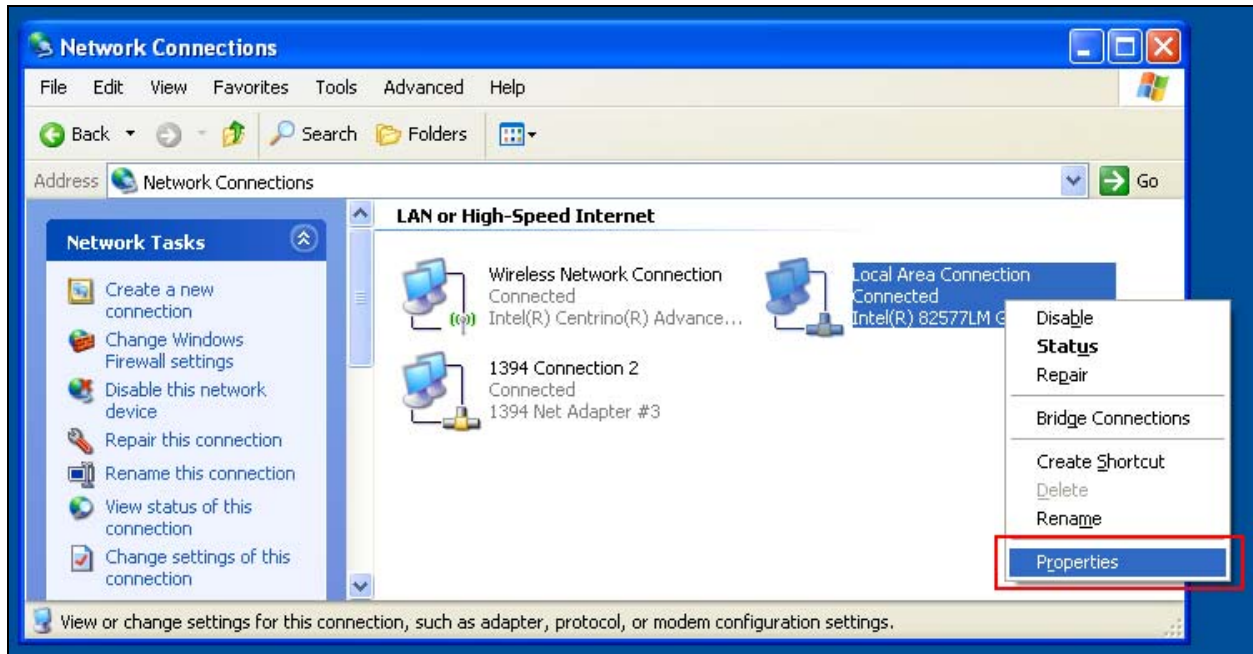


Figure 6: Network Connection Properties

2. Select the Authentication tab as in **Figure 7**.

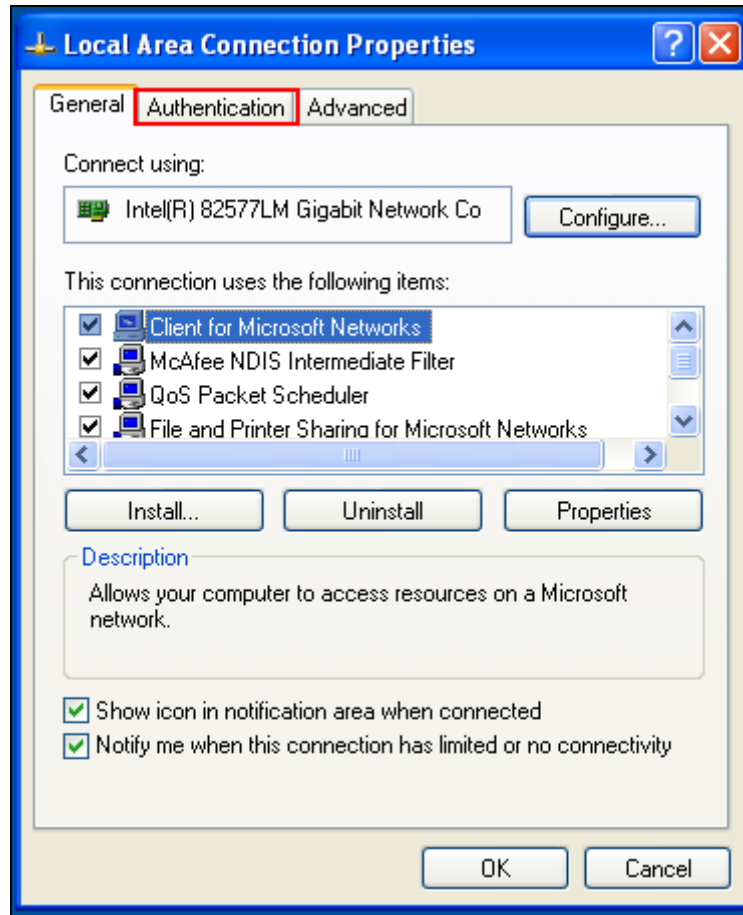


Figure 7: Authentication Tab

Note: If the Authentication tab as shown in **Figure 7** is missing, the Local Service “Wired AutoConfig” is not running. If required, it can be started as follows:

- a. Click **Start**, and then click **Run**.
- b. In the **Open** box, type **services.msc**, and then press **ENTER**.
- c. Locate the **Wired AutoConfig** service, right-click it, and then click **Start**.

3. From the Authentication window, check the **Enable IEEE 802.1X authentication** box and set the EAP type to **MD5-Challenge**. Click on **OK** when finished.

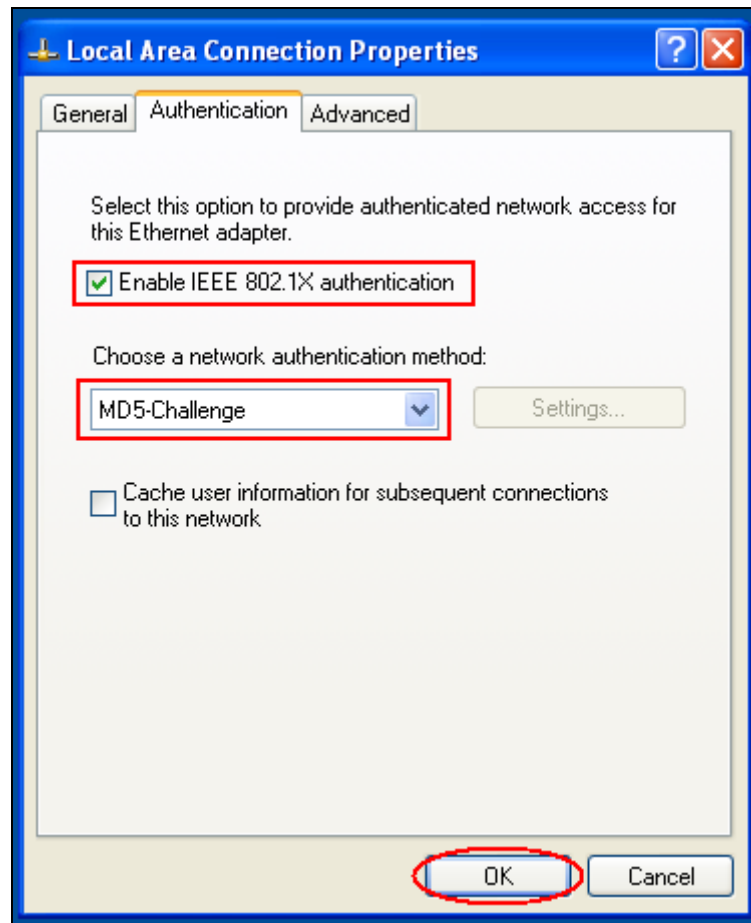


Figure 8: Enable 802.1x

4. Connect the PC to the PC port on the Avaya telephone. After the connection is made, the network Icon in the System Tray should be animated with a moving yellow ball. **Click on the icon** as shown in **Figure 9**.



Figure 9: Network Connection Icon in System Tray

5. After clicking on the icons the “Enter Credentials” window will open. Enter the **User Name** and **Password** that were configured in the FreeRADIUS users file for the PC. Then Click on **OK**.



Figure 10: Credentials Window

7. Observations

All of the IP phones tested for interoperability with the ERS 5520 and 4548 switches as listed in **Section 2** were able to Authenticate and join the voice VLAN with the exception of the A175. At the time of this interoperability testing the A175 did not support 802.1x on its wired ports.

8. Verification Steps

The following steps may be used to verify the configuration:

1. Use the **show radius-server** Avaya Command Line Interface (ACLI) command on the ERS Switches to verify the configuration for the connection to the FreeRADIUS server.

```
4548GT-PWR(config)#show radius-server
RADIUS Global Server
```

```
-----
Primary Host      : 10.10.97.249
Secondary Host    : 0.0.0.0
Port              : 1812
Time-out          : 2
Key               : thepwd
Radius Accounting : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
```

```
RADIUS EAP Server
```

```
-----
Primary Host      : 0.0.0.0
Secondary Host    : 0.0.0.0
Port              : 1812
Time-out          : 2
Key               :
Radius Accounting : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
```

```
RADIUS Non-EAP Server
```

```
-----
Primary Host      : 0.0.0.0
Secondary Host    : 0.0.0.0
Port              : 1812
Time-out          : 2
Key               :
Radius Accounting : Disabled
Radius Accounting Port : 1813
Radius Retry Limit : 3
```

```
Other Settings
```

```
-----
Password Fallback : Disabled
```

Figure 11: Verify RADIUS Server Configuration

2. Use the **show eapol multihost status** CLI command to verify that the IP Telephones and PCs have been authenticated and are using the correct VLANs. The VLANs are under the Vid heading.

```
4548GT-PWR#show eapol multihost status
Port Client MAC Address Pae State      Backend Auth State Vid  Pri
-----
1      B4:B0:17:96:71:D7  Authenticated Idle           8    0
1      F0:DE:F1:35:8C:13  Authenticated Idle           7    0

=====Neap Phones=====

Total number of authenticated clients: 2
```

Figure 12: Verify Authenticated Devices

9. Conclusion

These Application Notes have described the administration steps required to configure the Avaya Ethernet Routing Switches ERS5520 and ERS4548 to support 802.1x authentication with Avaya IP Telephones and a FreeRADIUS server. The FreeRADIUS server was also used to assign the Avaya one-X® 9600 and 1600 series IP Deskphones to the voice VLAN.

10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

[1] *Avaya IP Telephony Deployment Technical Configuration Guide*, Doc # NN48500-517, Version: 7.1, January 2011

[2] *Avaya one-X Deskphone H.323 Installation and Maintenance Guide Release 6.1 for 9608, 9611G, 9621G, and 9641G Deskphones*, Doc # 16-603603 Issue 2, May 2011

[3] *Avaya one-X™ Deskphone SIP Installation and Maintenance Guide Release 6.1 for 9601IP Deskphones*, Doc # 16-603843 Issue 1, December 2010

[4] *Avaya 1600 Series IP Deskphones Installation and Maintenance Guide Release 1.2.x*, Doc # 16-601438 Issue 4, February 2010

[5] *Configuration - System Avaya Ethernet Routing Switch 5000 Series, Release 6.2*, Doc # NN47200-500, December 2010

Documentation for FreeRADIUS may be found at <http://freeradius.org/>.

©2011 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