Ethernet Switch 470

Ethernet Routing Switch

2500, 4500, 5500 and 8300

Engineering

Authentication for non-EAPOL MAC Clients for ES and ERS Technical Brief

Enterprise Solutions Engineering

Document Date: July, 2010

Document Number: NN48500-552

Document Version: 2.1

© 2010 Avaya Inc.
All Rights Reserved.

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support.

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This Technical Brief provides a brief summary for authenticating non-EAPOL MAC clients for all supported releases of the Avaya Ethernet Switch (ES) 470, Ethernet Routing Switch (ERS) 2500, 4500, 5500 and 8300. This document replaces the previously released document titled “Technical Brief for RADIUS Authentication for non-EAPOL MAC Clients”.

Table of Contents

Document Updates

July 30, 2010

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Avaya devices are displayed in a Lucida Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

1. Overview: Non-EAP-MAC (NEAP)

1.1 MAC Authentication

If a port is configured for Multiple Host Multiple Authentication (MHMA), by default only multiple EAP Supplicants are allowed on this port. All traffic from non-EAP MAC addresses will be discarded. To allow non-EAP MAC (NEAP) addresses on a port, the Switch non-eap-mac (NEAP) feature must be enabled. The NEAP MAC address or addresses can be statically configured on the switch. If a NEAP MAC connects to the switch, its MAC address will be checked against the NEAP table and if present, the port will forward traffic for this particular MAC address.

As an alternative to configuring the NEAP MAC statically on the switch, the NEAP MAC can be authenticated via RADIUS. Upon detecting a NEAP MAC, the switch will first check to see if the NEAP MAC is located in the NEAP table. If not, and if the Radius authentication of non-eap clients is enabled, the switch will forward an Access-Request to the Radius server. The Access-Request will contain the non-EAP MAC address as the user name and one or any combination of IP address, MAC address, and/or port number for the password.

The number of EAP and non-EAP addresses is configurable.

EAP Guest VLAN cannot be enabled with NEAP.

1.2 Enhanced MHMA Feature: Non-EAP Avaya IP Deskphone Client

This feature allows an Avaya IP Deskphone and an EAP Supplicant to co-exist on an EAP enabled port. The IP Deskphone is not required to use EAP and instead is authenticated by the switch using a DHCP Signature from the Avaya IP Deskphone while the PC, if connected on the same interface, is authenticated by EAP. At this time, only Avaya IP Deskphone sets are supported with this feature.

Do not enable EAP Guest VLAN. Do no enable EAP on the IP Deskphone. If EAP authentication is required on the phone, do not enable this feature. Do not enable any other non-eap feature on the same port.

1.3 EAP Support on Avaya Switches

Table 1 shown below displays the various EAP features supported on the Avaya switches used for this technical brief.

Table 1: EAP Support on Avaya Switches

Authentication Feature	Switch				
	Ethernet Switch 470	Ethernet Routing Switch 2500	Ethernet Routing Switch 4500	Ethernet Routing Switch 5500	Ethernet Routing Switch 8300

Local MAC Security	Yes	Yes	Yes	Yes	Yes
Non EAP (Centralized MAC) Security	Yes	Yes	Yes	Yes	Yes
*Guest VLAN	Yes	Yes	Yes	Yes	Yes
Single Host Single Authentication (SHSA) – 802.1x	Yes	Yes	Yes	Yes	Yes
Multiple Host Single Authentication (MHSA) – 802.1x	Yes	Yes	Yes	Yes	Yes
Multiple Host Multiple Authentication (MHMA) – 802.1x	Yes (3.7)	Yes	Yes	Yes	Yes
SHSA with Guest VLAN	Yes	Yes	Yes	Yes	Yes
*MHSA with Guest VLAN	Yes	Yes	Yes	Yes	Future
*MHMA with Guest VLAN	Yes	Yes	Yes	Yes	Yes
EAP with Dynamic RADIUS VLAN Assignment	Yes, with SHSA	Yes, with SHSA and MHMA	Yes, with SHSA and MHMA	Yes, with SHSA and MHMA[1]	Yes, with SHSA
Non-EAP Phone	No	No	Yes	Yes	No
Policy Support	No	No	No	Yes	No
Tagged/Untagged					
Per VLAN Egress Tagging	Yes	Yes	Yes	Yes	Yes
Tagged and untagged per port	Yes	Yes	Yes	Yes	Yes
Tagging with EAP	Yes	Yes	Yes	Yes	**Yes

* **Please note** that a device is only put into the Guest VLAN providing another user has not already passed EAP authentication. For example, on a switch port configured for MHMA with Guest VLAN, once an EAP supplicant has passed EAP authentication, any existing client or any new client that either fails EAP or does not support EAP will be removed from the Guest VLAN. You cannot enable Guest VLAN and non-EAP on the same port.

[1]Requires software release 5.1. Not supported for NEAP (centralized MAC authentication)

**The Ethernet Routing Switch 8300 supports tagging with 802.1x in software release 2.2.2.0. Please see software release notes. Tagging with EAP is not supported in release 2.3, but is reintroduced in release 2.3.1.

2. Base Scenario

This configuration covers configuration examples only pertaining to authentication via a RADIUS server for non-EAPOL MAC and non-EAP IP Deskphone clients only.

2.1 Assumptions

It is assumed that general knowledge of EAPOL and basic VLAN configuration on Avaya switches is understood.

2.2 Non-EAP Configuration

The following command is used to define what the MAC user's password string will consist of:

- 5530g(config)#***eapol multihost non-eap-pwd-fmt ?***

```
ip-addr
mac-addr
port-number
```

The non-EAPOL password attribute on the RADIUS server can be a combination of the MAC address, Switch IP, Unit and Port number. You can select one of the single items shown above or a combination. For example, if you wish to configure non-EAP authentication with MAC address and unit/port-number, enter the following command:

- 5530g(config)#***eapol multihost non-eap-pwd-fmt mac-addr port-number***

The default setting for the non-EAP password string is *IpAddr.MACAddr.PortNumber*. If you do not wish to use this format, remove the default setting using the command '*no eapol multihost non-eap-pwd-fmt'*. Thereafter, enter the non-EAP password format of your liking.

2.2.1 RADIUS Server User Account Setup

When setting up a non-EAPOL user account on the RADIUS server, the user name is always the clients MAC address while the user's password string can include up to three parts (IP Address of switch, MAC address, Unit/Port).

- **Username:** Non-EAPOL MAC Address in a string format, i.e. 0002a5e90028
- **Password:** A combination of the MAC address, Switch IP, Unit and Port to generate a string

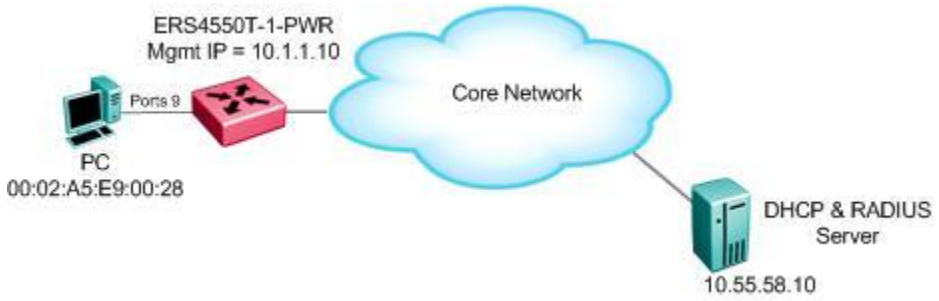
The password string can be configured to include any of the three parts or none. For example, assuming the ERS55xx switch has a management IP address of 10.1.1.10, the non-EAPOL client has a MAC address of 00:02:a5:e9:00:28 and the client is connected on a switch stack via unit 3 port 25, the non-EAPOL RADIUS password can consist of the following:

RADIUS Password String	Type
..	No IP, MAC or unit/port included
.0002a5e90028.	Just MAC included
010001001010..	Just IP included
010001001010. 0002a5e90028	IP and MAC included
010001001010. 0002a5e90028.0325	IP, MAC, and unit/port included

- If only MAC address is used, a period must be inserted before and after the MAC address
- If only the switch IP address is used, 2 periods must be inserted after the IP address.
- If you plan to use unit/port number, on a standalone switch the unit number is always expressed at ‘00’. For example, if the non-EAPOL client is connected to port 25 on a standalone switch, this will be expressed as ‘0025’.

3. Non-EAP Configuration

3.1 Non-EAP Configuration Example: MAC Only Using ERS4500



Assuming we wish to provide RADIUS authentication using the non-EAP clients MAC addresses password via port 9 of ERS4550T-1-PWR, please follow the following configuration steps.

Via the RADIUIS server, the user name is entered as '0002a5e90028' while the password is entered as '.0002a5e90028.'. Please note that the user name is simply the clients MAC address while the password is the clients MAC address with a period added before and after the MAC address.

Via the RADIUS server profile for the non-EAP clients, the authentication method must be configured as 'PAP'.

3.1.1 ERS4550T-1-PWR Configuration

3.1.1.1 Configure RADIUS Server

ERS4550T-1-PWR Step 1 – 1. Enable RADIUS Sever assuming the shared key is "nortel"

```
4550T-1-PWR(config)#radius-server host 10.55.58.10 key
Enter key: nortel
Confirm key: nortel
```

3.1.1.2 Enable EAP at Interface Level

ERS4550T-1-PWR Step 1 – Enable EAP on port 9

```
4550T-1-PWR(config)#interface fastEthernet 9
4550T-1-PWR(config-if)#eapol status auto
4550T-1-PWR(config-if)#eapol multihost allow-non-eap-enable
4550T-1-PWR(config-if)# eap multihost non-eap-mac-max 1
4550T-1-PWR(config-if)#eapol multihost radius-non-eap-enable
4550T-1-PWR(config-if)#eapol multihost enable
```

```
4550T-1-PWR(config-if)#exit
```

3.1.1.3 Enable EAP Globally

ERS4550T-1-PWR Step 1 – Enable EAP globally

```
4550T-1-PWR(config)#eapol multihost allow-non-eap-enable
4550T-1-PWR(config)#eapol multihost radius-non-eap-enable
4550T-1-PWR (config)#no eapol multihost non-eap-pwd-fmt
4550T-1-PWR(config)#eapol multihost non-eap-pwd-fmt mac-addr
4550T-1-PWR(config)#eapol enable
```

Please note that by default the non-EAP password format is *IpAddr.MACAddr.PortNumber*. Hence, the reason we enter the command 'no eapol multihost non-eap-pwd-fmt' to remove the default setting.

3.2 Verify Operations

3.2.1 ERS4550T-1-PWR

3.2.1.1 Verify the non-EAP Global Configuration

Step 1 – Verify the non-EAP configuration using the following command:

```
4550T-1-PWR#show eapol multihost
```

Result:

```
      Allow Non-EAPOL Clients:  Enabled
      Use RADIUS To Authenticate Non-EAPOL Clients:  Enabled
      Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
      Allow Non-EAPOL VoIP Phone Clients:  Disabled
      EAPOL Request Packet Generation Mode:  Multicast
      Allow Use of RADIUS Assigned VLANs:  Enabled
      EAPOL Reauthentication Security Mode:  Fail on RADIUS Timeout
      Non-EAPOL RADIUS Password Attribute Format:  .MACAddr.
```

Via ERS4550T-1-PWR, verify the following information:

Option	Verify
Allow Non-EAPOL Clients:	Verify that non-EAPOL clients are ***Enabled*** globally.
Use RADIUS To Authenticate Non-	Verify that non-EAPOL RADIUS authentication is ***Enabled*** globally.

EAPOL Clients:	
Non-EAPOL RADIUS Password Attribute Format:	Verify the non-EAP RADIUS password attribute format is configured as ***.MACAddr.***

3.2.1.2 Verify the non-EAP Interface Configuration

Step 1 – Verify the non-EAP configuration for port 9 used in this configuration example:

```
4550T-1-PWR#show eapol multihost interface 9
```

Result:

```
      Port:  9
          MultiHost Status:  Enabled
          Max Eap Clients:  1
          Allow Non-EAP Clients:  Enabled
          Max Non-EAP Client MACs:  1
          Use RADIUS To Auth Non-EAP MACs:  Enabled
          Allow Auto Non-EAP MHSA:  Disabled
          Allow Non-EAP Phones:  Disabled
          RADIUS Req Pkt Send Mode:  Multicast
          Allow RADIUS VLANs:  Disabled
          RADIUS Timeout Mode:  Fail
```

Via ERS4550T-1-PWR, verify the following information for port 9:

Option	Verify
MultiHost Status:	Verify that MultiHost status is ***Enabled*** on port 9
Max Non-EAP Client MACs:	Verify that non-EAPOL maximum client setting is ***1*** as this is the setting used for this configuration example
Use RADIUS To Auth Non-EAP MACs:	Verify that non-EAP use RADIUS to authenticate MAC's is ***Enabled*** on port 9

3.2.1.3 Verify Non-EAPOL Client

Assuming the non-EAP client has successfully authenticated via RADIUS, use the following command for verification.

Step 1 – Verify the non-EAP client status using the following command:

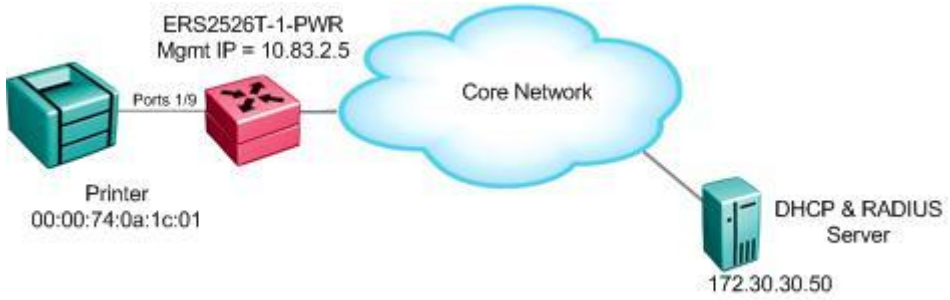
```
4550T-1-PWR#show eapol multihost non-eap-mac status 9
```

Result:
Port Client MAC Address State ---- ------------------ ------------------------------ 9 **00:02:A5:E9:00:28 Authenticated By RADIUS**

Via ERS4550T-1-PWR, verify the following information:

Option	**Verify**
Client MAC:	If the non-EAP client has successfully been authenticated using RADIUS, its MAC address will be displayed.
State:	If the non-EAP client has successfully been authenticated using RADIUS, the state ***Authenticated By RADIUS*** will be displayed.

3.3 Non-EAP Configuration Example: MAC, IP, and Port Using ERS2500



Assuming we wish to provide RADIUS authentication using the non-EAP clients MAC addresses via port 1/9 of the ERS2526T-1-PWR stack. In this example, we will assume the NEAP client will not be mobile, i.e. a printer, such that it has a static IP address and is permanently connected to port 1/9. This will allow us to use a NEAP password consisting of the client MAC address, IP address, and switch port number.

Via the RADIUIS server, for this example, the user name is entered as '0000740a1c01' while the password is entered as '010083002005.0000740a1c01.0109'. Please note that the user name is simply the clients MAC address while the password is the clients IP address, MAC address, and switch port number with a period added after the IP address, the MAC address, and port number.

Via the RADIUS server profile for the non-EAP clients, the authentication method must be configured as 'PAP'.

3.3.1 ERS2526T-1-PWR Configuration

3.3.1.1 Configure RADIUS Server

ERS2526T-1-PWR Step 1 – 1. Enable RADIUS Sever assuming the shared key is "nortel"

```
2526T-1-PWR(config)#radius-server host 172.30.30.50 key
Enter key: nortel
Confirm key: nortel
```

3.3.1.2 Enable EAP at Interface Level

ERS2526T-1-PWR Step 1 – Enable EAP on port 1/9

```
2526T-1-PWR(config)#interface fastEthernet 1/9
2526T-1-PWR(config-if)#eapol status auto
2526T-1-PWR(config-if)#eapol multihost allow-non-eap-enable
2526T-1-PWR(config-if)# eap multihost non-eap-mac-max 1
2526T-1-PWR(config-if)#eapol multihost radius-non-eap-enable
```

```
2526T-1-PWR(config-if)#eapol multihost enable
2526T-1-PWR(config-if)#exit
```

3.3.1.3 Enable EAP Globally

ERS2526T-1-PWR Step 1 – Enable EAP globally

```
2526T-1-PWR(config)#eapol multihost allow-non-eap-enable
2526T-1-PWR(config)#eapol multihost radius-non-eap-enable
2526T-1-PWR(config)#eapol enable
```

Please note that by default the non-EAP password format is *IpAddr.MACAddr.PortNumber*. Hence, we did not have to enter the CLI command '*eap multihost non-eap-pwd-fmt ip-addr mac-addr port-number'*. You can check the setting by using the CLI command '*show eapol multihost*'.

3.4 Verify Operations

3.4.1 ERS2526T-1-PWR

3.4.1.1 Verify the non-EAP Global Configuration

Step 1 – Verify the non-EAP configuration using the following command:

```
2526T-1-PWR#show eapol multihost
```

Result:

```
      Allow Non-EAPOL Clients:  Enabled
      Use RADIUS To Authenticate Non-EAPOL Clients:  Enabled
      Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
      Allow Use of RADIUS Assigned VLANs:  Disabled
      Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
```

Via ERS2526T-1-PWR, verify the following information:

Option	Verify
Allow Non-EAPOL Clients:	Verify that non-EAPOL clients are ***Enabled*** globally.
Use RADIUS To Authenticate Non-EAPOL Clients:	Verify that non-EAPOL RADIUS authentication is ***Enabled*** globally.
Non-EAPOL RADIUS Password Attribute Format:	Verify the non-EAP RADIUS password attribute format is configured as ***IpAddr.MACAddr.PortNumber.***

3.4.1.2 Verify the non-EAP Interface Configuration

Step 1 – Verify the non-EAP configuration for port 1/9 used in this configuration example:

```
2526T-1-PWR#show eapol multihost interface 1/9
```

Result:

```
      Unit/Port:  1/9
          MultiHost Status:  Enabled
          Max Eap Clients:  1
          Allow Non-EAP Clients:  Enabled
          Max Non-EAP Client MACs:  1
          Use RADIUS To Auth Non-EAP MACs:  Enabled
          Allow Auto Non-EAP MHSA:  Disabled
          Allow RADIUS VLANs:  Disabled
```

Via ERS2526T-1-PWR, verify the following information for port 9:

Option	Verify
MultiHost Status:	Verify that MultiHost status is ***Enabled*** on port 1/9
Max Non-EAP Client MACs:	Verify that non-EAPOL maximum client setting is ***1*** as this is the setting used for this configuration example
Use RADIUS To Auth Non-EAP MACs:	Verify that non-EAP use RADIUS to authenticate MAC's is ***Enabled*** on port 1/9

3.4.1.3 Verify non-EAPOL Client

Assuming the non-EAP client has successfully authenticated via RADIUS, use the following command for verification.

Step 1 – Verify the non-EAP client status using the following command:

```
2526T-1-PWR#show eapol multihost non-eap-mac status 1/9
```

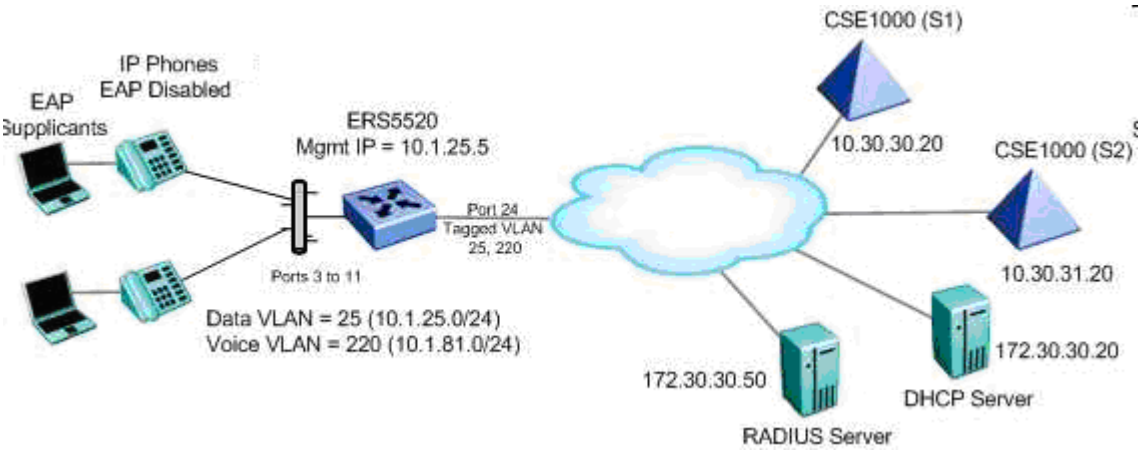
Result:

```
      Port Client MAC Address State
      ---- ----------------- ------------------------------
      1/9  00:00:74:0A:1C:01 Authenticated By RADIUS
```

Via ERS2526T-1-PWR, verify the following information:

Option	Verify
Client MAC:	If the non-EAP client has successfully been authenticated using RADIUS, its MAC address will be displayed.
State:	If the non-EAP client has successfully been authenticated using RADIUS, the state ***Authenticated By RADIUS*** will be displayed.

3.5 Non-EAP Configuration Example with User Based Policy: MAC Only with Policy Using ERS5500



For this example, we will demonstrate how to configure the Ethernet Routing Switch 5500 to allow for non-EAP (NEAP) authentication via RADIUS for the IP Deskphones. We will also demonstrate using user based policies to apply QoS for the IP Deskphones. Hence, instead of configuring filters on the switch to apply QoS for the voice traffic, we can use a policy triggered by EAP to apply QoS to the voice VLAN.

The Ethernet Routing Switch 5500 can be configured to accept both EAP and non-EAP (NEAP) on the same port. In regards to non-EAP, the switch can be configured to accept a password format using any combination of IP address and MAC address with or without port number. By default, the password format is set for IP address, MAC address, and port number.

To apply QoS for the IP Deskphone sets, you can configure the QoS filters on the switch, use ADAC, or use user based policies (UBP) and trigger the policy via RADIUS authentication. As stated above, we will use UBP for this configuration example. Once the user based policies has been configured on a switch, the RADIUS server can reference the policy by using the name given to the UBP policy. User based policies (UBP) can be used with EAP and/or NEAP.

Overall, we will configured the following

- Enable Centralized MAC for IP Deskphone set on port 3 of ERS5520 using the non-EAP password format of MAC address only – the will allow the IP Deskphone to be connected anywhere in the network
- Configure a user based policy (UBP) for non-EAP IP Deskphones named *voice* that will remark both the DSCP and p-bit values to a CoS value of Premium only for tagged Voice VLAN 220
- Configure the Ethernet Routing Switch 5520 and RADIUS server with shared key set to *nortel*
- Configure the RADIUS server NEAP policy using Avaya specific option 562 with vendor-assigned attribute number 110 and set the string value to *UROLvoice*. Please see note below.

Please note that when setting up the RADIUS server policy for the NEAP group, the string always starts with *UROL*. In our example, we configured the ERS5520 with a user based policy named *voice*. Hence the string value configured on the RADIUS server must be set to *UROLvoice*.

If you do not wish to use EAP to authenticate the phone, enable the non-eap phone feature and use ADAC to configure the QoS portion for the IP Deskphone. Please see the next configuration example.

You cannot use the EAP radius-assigned VLAN option with NEAP.

3.5.1 Configuration

3.5.1.1 Go to Configuration Mode

ERS5520-1 Step 1 - Enter configuration mode

```
5520-24T-1>enable
5520-24T-1#configure terminal
```

3.5.1.2 Create VLAN's

ERS5520-1 Step 1 – Remove port members from the default VLAN, create VLAN 25 and 220

```
5520-24T-1(config)#vlan members remove 1 ALL
5520-24T-1(config)#vlan create 25 name data type port
5520-24T-1(config)#vlan create 220 name voice type port
```

3.5.1.3 Enable VLAN Tagging

ERS5520-1 Step 1 – Enable VLAN tagging on all appropriate ports

```
5520-24T-1(config)#vlan port 24 tagging tagall
5520-24T-1(config)#vlan port 3-11 tagging untagpvidOnly
```

3.5.1.4 Add VLAN Port Members and Default VLAN ID

ERS5520-1 Step 1 – Enable VLAN tagging on all appropriate ports

```
5520-24T-1(config)#vlan members add 25 3-11,24
5520-24T-1(config)#vlan members add 220 3-11,24
5520-24T-1(config)#vlan port 3-11 pvid 25
5520-24T-1(config)#vlan mgmt 25
```

3.5.1.5 Configure Management IP Address on Switch

ERS5520-1 Step 1 – Set the IP address of the switch

```
5520-24T-1(config)#ip address 10.1.25.5 netmask 255.255.255.0
5520-24T-1(config)#ip default-gateway 10.1.25.1
```

3.5.1.6 Configure RADIUS Server

ERS5520-1 Step 1 – Add RADIUS server using key 'nortel'

```
5520-24T-1(config)#radius-server host 172.30.30.50 key
Enter key: ******
Confirm key: ******
```

3.5.1.7 Enable EAP Globally

ERS5520-1 Step 1 – Enable non-EAP (NEAP)

```
5520-24T-1(config)#eapol multihost allow-non-eap-enable
```

ERS5520-1 Step 2 – Enable multihost RADIUS authentication for NEAP

```
5520-24T-1(config)#eapol multihost radius-non-eap-enable
```

ERS5520-1 Step 3 – Remove the default NEAP password format of IpAddr.MACAddr.PortNumber

```
5520-24T-1(config)#no eapol multihost non-eap-pwd-fmt
```

ERS5520-1 Step 4 – Enable NEAP password format of MAC address only

```
5520-24T-1(config)#eapol multihost non-eap-pwd-fmt mac-addr
```

ERS5520-1 Step 5 – Enable EAP user-based Policies

```
5520-24T-1(config)#eapol user-based-policies enable
```

ERS5520-1 Step 6 – Enable EAP multihost NEAP policies

```
5520-24T-1(config)# eapol multihost non-eap-user-based-policies enable
```

ERS5520-1 Step 6 – Enable EAP globally

```
5520-24T-1(config)#eapol enable
```

3.5.1.8 Enable EAP at Interface Level

ERS5520-1 Step 1 – Enable EAP on port 3 with NEAP, set the maximum allowable EAP and NEAP client to 1, enable EAP multihost and enable RADIUS NEAP

```
5520-24T-1(config)#interface fastEthernet 3
5520-24T-1(config-if)#eapol status auto
5520-24T-1(config-if)#eapol multihost allow-non-eap-enable
5520-24T-1(config-if)#eapol multihost eap-mac-max 1
5520-24T-1(config-if)#eapol multihost non-eap-mac-max 1
```

```
5520-24T-1(config-if)#eapol multihost radius-non-eap-enable
5520-24T-1(config-if)#eapol multihost enable
5520-24T-1(config-if)#exit
```

3.5.1.9 Configure Policy

ERS5520-1 Step 1 – Configure a policy using the name 'voice' to filter on tagged VLAN 220 and remark DSCP and p-bit to Premium CoS. We will set the eval-order to 5 in case you wish to add additional filters in the future with a higher preference

```
5520-24T-1(config)#qos ubp classifier name voice vlan-min 220 vlan-max 220 vlan-tag tagged ethertype 0x0800 update-dscp 46 update-1p 6 eval-order 5
```

ERS5520-1 Step 2 – Set the default action to pass all other traffic

```
5520-24T-1(config)#qos ubp set name voice drop-nm-action enable
```

ERS5520-1 Step 3 – Enable ubp

```
5520-24T-1(config)#qos agent ubp high-security-local
```

3.5.2 Verify Operations

3.5.2.1 Verify EAP Global and Port Configuration

Step 1 – Verify that EAP has been enabled globally and the correct port members:

```
5520-24T-1# show eapol port 3
```

Result:

```
        EAPOL Administrative State:  Enabled
        EAPOL User Based Policies:  Enabled
        EAPOL User Based Policies Filter On MAC Addresses:  Disabled
             Admin          Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
        Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
        ---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
        3    Auto     No   Both  Both No     3600   60     30     30      30      2
```

On the ERS5520 verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
EAPOL User Based Policies	Verify that EAPOL policies are ***Enabled*** globally.

Admin Status	Verify that the EAP is enabled on port 3 by verifying that the Admin Status is set to ***Auto***.
Auth	The value will be ***No*** even if the IP Deskphone has successfully authenticated. Only if there a Supplicant attached to the IP Deskphone and it has successfully authenticated will this value change to Yes.

3.5.2.2 Verify EAP Multihost Configuration

Step 1 – Verify that EAP multihost has been globally configured correctly:

```
5520-24T-1#show eapol multihost
```

Result:

```
      Allow Non-EAPOL Clients:  Enabled
      Use RADIUS To Authenticate Non-EAPOL Clients:  Enabled
      Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
      Allow Non-EAPOL VoIP Phone Clients:  Disabled
      EAPOL Request Packet Generation Mode:  Multicast
      Allow Use of RADIUS Assigned VLANs:  Disabled
      Non-EAPOL RADIUS Password Attribute Format:  .MACAddr.
      Non-EAPOL User Based Policies:  Enabled
      Non-EAPOL User Based Policies Filter On MAC Addresses:  Disabled
```

On the ERS5520 verify the following information:

Option	Verify
Allow Non-EAPOL Clients:	Verify that the non-EAPOL (NEAP) is ***Enabled*** globally.
Use RADIUS To Authenticate Non-EAPOL Clients:	Verify the use RADUIS to authenticate non-EAPOL option is ***Enabled*** globally.
Non-EAPOL RADIUS Password Attribute Format:	Verify that the non-EAP password format is set for ***.MACAddr.***.
Non-EAPOL User Based Policies:	Verify that the non-EAPOL user based policies is ***Enabled***

3.5.2.3 Verify EAP Multihost Status

Step 1 – Assuming the IP Deskphone via port 3 has successfully authenticated via EAP, use the following command to view the EAP status:

```
5520-24T-1# show eapol multihost non-eap-mac status
```

Result:

```
      Port Client MAC Address State
      ---- ----------------- ----------------------------
      3    00:0A:E4:09:72:E7 Authenticated By RADIUS
```

On the ERS5520 verify the following information:

Option	Verify
Port	Verify the port number is correct, should be ***3*** for this example.
Client MAC Address	If the IP Deskphone has successfully authenticated via NEAP, its MAC address should be shown. For this example, the MAC ***00:0A:E4:09:72:E7*** will be displayed.
State	Verify that ***Authenticated By RADIUS*** is displayed

3.5.2.4 Verify EAP Policy

Step 1 – Assuming the IP Deskphone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:

```
5520-24T-1# show qos ubp classifier
```

Result:

```
      Id: 1
      Name: voice
      Block:
      Eval Order: 5
      Address Type: IPv4
      Destination Addr/Mask: Ignore
      Source Addr/Mask: Ignore
      DSCP: Ignore
      IPv4 Protocol / IPv6 Next Header: Ignore
      Destination L4 Port Min: Ignore
      Destination L4 Port Max: Ignore
      Source L4 Port Min: Ignore
```

```
        Source L4 Port Max: Ignore
        IPv6 Flow Id: Ignore
        Destination MAC Addr: Ignore
        Destination MAC Mask: Ignore
        Source MAC Addr: Ignore
        Source MAC Mask: Ignore
        VLAN: 220
        VLAN Tag: Tagged
        EtherType: 0x0800
        802.1p Priority: All
        Action Drop: No
        Action Update DSCP: 0x2E
        Action Update 802.1p Priority: Priority 6
        Action Set Drop Precedence: Low Drop
        Storage Type: NonVolatile
```

On the ERS5520 verify the following information:

Option	Verify
Name:	Verify the port number is correct, should be ***voice*** for this example.
Eval Order:	Verify the port number is correct, should be ***5*** for this example.
Address Type:	Verify the Address Type is correct, should be ***IPv4*** for this example.
VLAN:	Verify VLAN is correct, should be ***220*** for this example.
EtherType:	Verify the EtherType is correct, should be ***0x0800*** representing IP for this example.
Action Update DSCP:	Verify the DSCP value is correct, should be ***0x2e*** (decimal 46) for this example.
Action Update 802.1p Priority:	Verify the p-bit value is correct, should be ***6*** for this example.

3.5.2.5 Verify EAP Policy upon the NEAP Client Successfully Authenticating

Step 1 – Assuming the IP Deskphone via port 3 has successfully authenticated via EAP, use the following command to view the UBP Policy:
`5520-24T-1#` ***`show qos ubp interface`***
Result:

```
  Id  Unit Port Filter Set Name

_____ ____ ____ _________________
55001 1    3    voice
```

On the ERS5520 verify the following information:

Option	Verify
Port	Verify the port number is correct, should be ***3*** for this example.
Filter Set Name	If the IP Deskphone has successfully authenticated via NEAP, and if the RADIUS server has been configured correctly, the policy named ***voice*** will be displayed.

3.5.2.6 View EAP Policy Statistics

Step 1 – You can view the statistics by using the UBP reference and port number using the following command. Please note that the reference number for each port will be different.

```
5520-24T-1# show qos statistics 55001 port 3
```

Result:

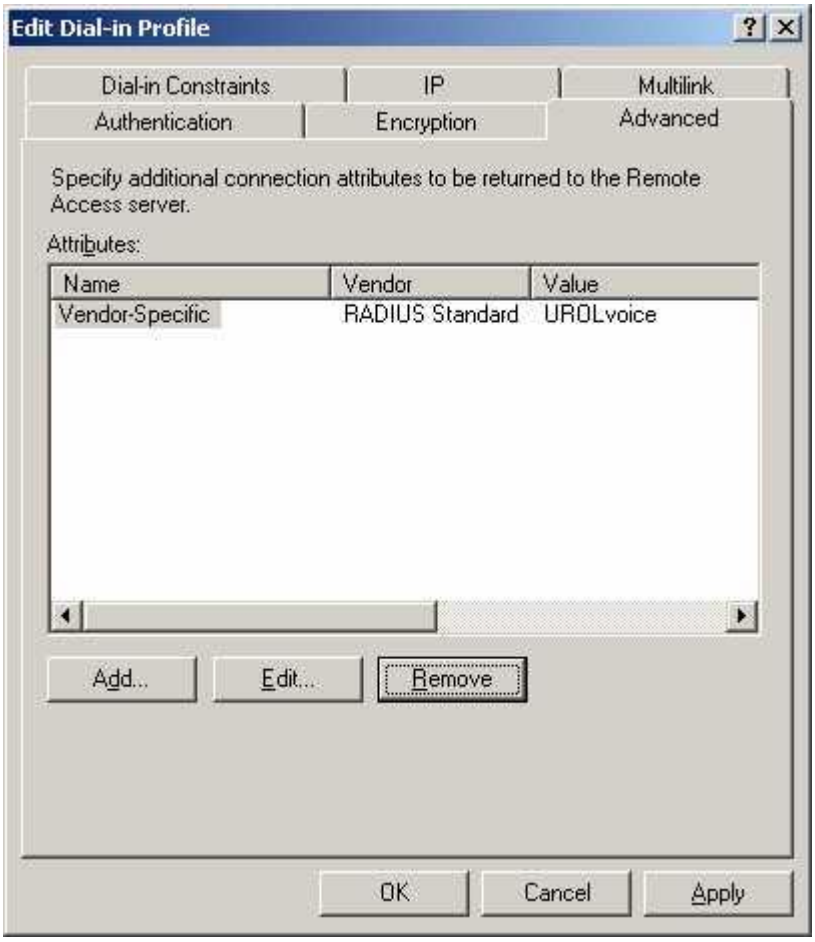
```
Id: 55001
Policy Name: UntrustedClfrs2

   Classifier     Unit/Port      In-Profile
      Name                         Packets

_________________ _________ ____________________
                  1/3       22547378
```

3.5.3 RADIUS Server – Policy Setup

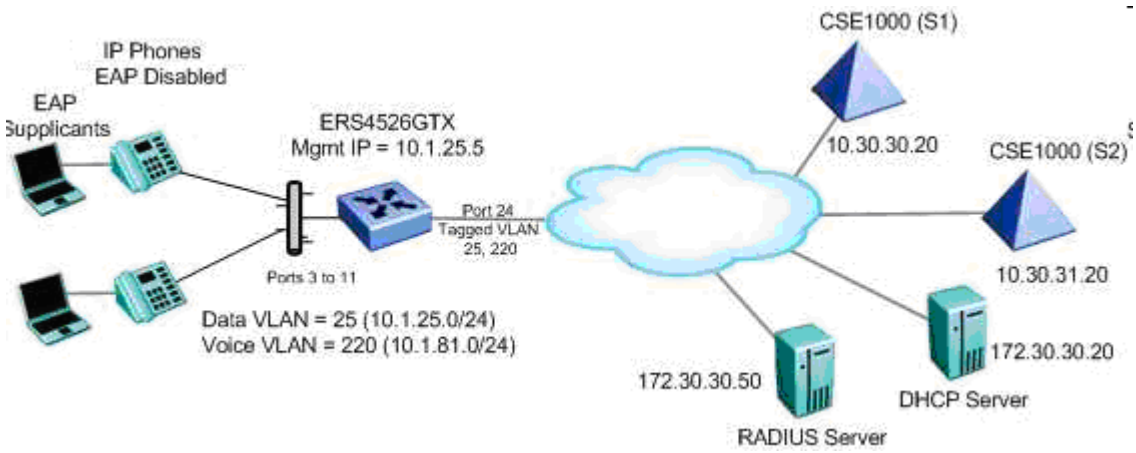
Step 1 – Assuming the RADIUS server is a Windows 2003 server, via the IAS Remote Access Policies go to your NEAP policy Advanced settings. The Vendor-Specific attribute should be setup as follows.

- Vendor Code : Avaya ; Avaya Specific Option 562
- Vendor-assigned attribute
  - Attribute number : 110
  - Attribute formate : String
  - Attribute value : UROLvoice

Result:


Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Specify additional connection attributes to be returned to the Remote Access server.
Attributes:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
UROLvoice
Add...
Edit...
Remove
OK
Cancel
Apply

3.6 Non-EAP for IP Deskphone Configuration Example: Using ADAC LLDP Detection for QOS and NEAP using ERS4500



In the 5.1 software release for the ERS4500 and ERS5500, non-EAP support for Avaya IP Deskphones was introduced. This feature allows an Avaya IP Deskphone and an EAP Supplicant to co-exist on an EAP enabled port. The IP Deskphone will not require authentication while the device attached to the IP Deskphone will have to be authenticated via EAP.

For this configuration example, we wish to accomplish the following:

- Configure ERS4526GTX with a data VLAN 25 and voice VLAN 220
- Configure the Ethernet Routing Switch with EAP multihost using options non-EAP phone on port 3 to 11
  - This will in fact allow NEAP support for the Avaya IP Deskphone sets
  - Please note that DHCP must be enabled on the Avaya IP Deskphones for non-EAP-phone to work
- Configure ERS4526GTX and RADIUS server with shared key set to ‘nortel’
- Limit the number of EAP Supplicant to only 1
- Configure ports 3 to 11 on the ERS4526GTX to untag the data VLAN 25 and use ADAC with LLDP detection for the Avaya IP Deskphone set
- The Avaya IP Deskphones will need to be setup with LLDP-MED and for DHCP

Please note the non-EAP support for IP Deskphones is only supported on Avaya IP Deskphones and requires that DHCP be enabled. The IP Deskphone is authenticated based on the DHCP signature. Do not enable EAP on the phone. Also, do not enable Guest-VLAN.

3.6.1.1 Go to Configuration Mode

ERS4526GTX-1 Step 1 - Enter configuration mode
4526GTX-1>***enable*** 4526GTX-1#***configure terminal***

3.6.1.2 Create Data VLAN

ERS4526GTX-1 Step 1 – Remove port members from the default VLAN, create VLAN 25 and 220

```
4526GTX-1(config)#vlan members remove 1 ALL
4526GTX-1(config)#vlan create 25 name data type port
```

3.6.1.3 Enable ADAC Globally

ERS4526GTX-1 Step 1 – Enable ADAC globally with port 24 as the uplink port and set the mode to tagged frames

```
4526GTX-1(config)#adac voice-vlan 220
4526GTX-1(config)#adac op-mode tagged-frames
4526GTX-1(config)#adac uplink-port 24
4526GTX-1(config)#adac enable
```

3.6.1.4 Add VLAN Port Members to Data VLAN and Enable as the Management VLAN

ERS4526GTX-1 Step 1 – Enable VLAN tagging on all appropriate ports

```
4526GTX-1(config)#vlan members add 25 3-11,24
4526GTX-1(config)#vlan mgmt 25
```

3.6.1.5 Enable ADAC at Interface Level

ERS4526GTX-1 Step 1 – Enable ADAC on ports 3 to 11

```
4526GTX-1(config)#interface fastEthernet 3-11
4526GTX-1(config-if)#no adac detection mac
4526GTX-1(config-if)#adac tagged-frames-tagging untag-pvid-only
4526GTX-1(config-if)#adac enable
4526GTX-1(config-if)#exit
```

3.6.1.6 Configure RADIUS Server

ERS4526GTX-1 Step 1 – Add RADIUS server using key 'nortel'

```
4526GTX-1(config)#radius-server host 172.30.30.20 key
Enter key: ******
Confirm key: ******
```

3.6.1.7 Enable EAP Globally

ERS4526GTX-1 Step 1 – Enable EAP non-EAP phone
4526GTX-1(config)#***eapol multihost non-eap-phone-enable***
ERS4526GTX-1 Step 2 – Enable EAP
4526GTX-1(config)#***eapol enable***

3.6.1.8 Enable EAP at Interface Level

ERS4526GTX-1 Step 1 – Enable EAP on ports 3 to 11 with non-eap-phone and use-radius-assigned-vlan enabled
4526GTX-1(config)#***interface fastEthernet 3-11***
4526GTX-1(config-if)#***eapol multihost non-eap-phone-enable***
4526GTX-1(config-if)#***eapol multihost eap-mac-max 1***
4526GTX-1(config-if)#***eapol multihost enable***
4526GTX-1(config-if)#***eapol status auto***
4526GTX-1(config-if)#***exit***

3.6.1.9 Configure Management IP Address on Switch

ERS4526GTX-1 Step 1 – Set the IP address of the switch
4526GTX-1(config)#***ip address 10.1.25.5 netmask 255.255.255.0***
4526GTX-1(config)#***ip default-gateway 10.1.25.1***

3.6.2 Verify Operations

Assuming we have an Avaya IP Deskphone with a Supplicant connected to port 8 and an Avaya IP Deskphone connected to port 6 with the following characteristics:

- Port 6: i2004 with MAC address 00-0a-e4-09-72-e7
- Port 8:
  - 1120E with MAC address 00-13-65-fe-f1-cb
  - Supplicant with MAC address 00:02:A5:E9:00:28

3.6.2.1 Verify EAP Global and Port Configuration

Step 1 – Verify that EAP has been enabled globally and the correct port members:
4526GTX-1# ***show eapol port 3-11***
Result:
EAPOL Administrative State: Enabled

```
            Admin          Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir    Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- -----  ---- ------ ------ ------ ------ ------- ------- ---
3    Auto     Yes  Both   Both No     3600   60     30     30      30      2
4    Auto     No   Both   Both No     3600   60     30     30      30      2
5    Auto     Yes  Both   Both No     3600   60     30     30      30      2
6    Auto     No   Both   Both No     3600   60     30     30      30      2
7    Auto     Yes  Both   Both No     3600   60     30     30      30      2
8    Auto     Yes  Both   Both No     3600   60     30     30      30      2
9    Auto     Yes  Both   Both No     3600   60     30     30      30      2
10   Auto     No   Both   Both No     3600   60     30     30      30      2
11   Auto     Yes  Both   Both No     3600   60     30     30      30      2
```

On the ERS4526GTX verify the following information:

Option	Verify
EAPOL Administrative State	Verify that the EAPOL is ***Enabled*** globally.
Auth	For any port that has a Supplicant which has successfully been authenticated, the Auth state should be ***Yes***

3.6.2.2 Verify EAP Multihost Configuration

Step 1 – Verify that EAP multihost has been globally configured correctly:

```
4526GTX-1#show eapol multihost
```

Result:

```
Allow Non-EAPOL Clients:  Disabled
Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
Allow Non-EAPOL VoIP Phone Clients:  Enabled
EAPOL Request Packet Generation Mode:  Multicast
Allow Use of RADIUS Assigned VLANs:  Disabled
EAPOL Reauthentication Security Mode:  Fail on RADIUS Timeout
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
```

On the ERS4526GTX verify the following information:

Option	Verify
Allow Non-EAPOL VoIP Phone Clients	Verify the allow non-EAPOL VoIP Phone Clients option is ***Enabled*** globally.

3.6.2.3 Verify EAP Multihost Port Configuration

Step 1 – Verify that EAP mulltihost configuration:

```
4526GTX-1#show eapol multihost interface 3-11
```

Result, i.e. for port 3:

```
      Port:  3
          MultiHost Status:  Enabled
          Max Eap Clients:  1
          Allow Non-EAP Clients:  Disabled
          Max Non-EAP Client MACs:  1
          Use RADIUS To Auth Non-EAP MACs:  Disabled
          Allow Auto Non-EAP MHSA:  Disabled
          Allow Non-EAP Phones:  Enabled
          RADIUS Req Pkt Send Mode:  Multicast
          Allow RADIUS VLANs:  Disabled
          RADIUS Timeout Mode:  Fail
```

On the ERS4526GTX verify the following information:

Option	Verify
MultiHost Status	Verify that the MultiHost status is ***Enabled*** on port ***3 to 11***.
Max Eap Client	Verify that the maximum EAP client is set to ***1***. If not, check your configuration
Max Non-EAP Client MACs	Verify that the maximum non-EAP client is set to ***1***. If not, check your configuration
Allow Non-EAP Phones	Verify that Allow Non-EAP Phone is set to ***Enabled***. If not, check your configuration

3.6.2.4 Verify EAP Multihost Status

Step 1 – Assuming the Supplicant via port 8 has successfully authenticated via EAP, use the following command to view the EAP status:

```
4526GTX-1#show eapol multihost status
```

Result:

```
      Port Client MAC Address Pae State      Backend Auth State
      ---- ----------------- -------------- ------------------
      8    00:02:A5:E9:00:28  Authenticated  Idle

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

      unit 0 port 6 mac 00-0a-e4-09-72-e7
      unit 0 port 8 mac 00-13-65-fe-f1-cb
```

On the ERS4526GTX verify the following information:

Option	Verify
Client MAC Address	Verify the actual Supplicant MAC. For this example, this should be ***00:02:A5:E9:00:28*** on port ***8***.
Pae State	Verify the actual Supplicant Pae State. If the Supplicant has successfully authenticated, the Pae State should be displayed as ***Authenticated***
Neap Phones	Verify the actual MAC for the Avaya IP Deskphone sets. For this example, this should be ***00-0a-e4-09-72-e7*** on port ***6*** and ***00-13-65-fe-f1-cb*** on port ***8***

4. Software Baseline

The configuration examples in this technical brief are based on software release 5.1 for the ERS 5500and ERS4500, release 3.7 for the ES470, and release 4.1.1 for the ERS2500.

5. Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

5.1 Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

5.2 Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

5.3 Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

5.4 Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.