Ethernet Routing Switch

8600/8800

Engineering

> EAPoL Technical Configuration Guide

Avaya Data Solutions

Document Date: June 2013

Document Number: NN48500-608

Document Version: 2.0

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 document provides an overview on how to configure EAPoL on the Ethernet Routing Switch 8000.

Revision Control

No	Date	Version	Revised By	Remarks
1	10/22/2004	1.0	JVE	Initial Draft
2	12/22/2010	1.1	K. Marshall	Rebranded Avaya
3	06/13/2013	2.0	JVE	Updated to include ACLI and text in configuration example

Table of Contents

Figures

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 sys-info

Operation Mode:          Switch
MAC Address:             00-12-83-93-B0-00
PoE Module FW:           6370.4
Reset Count:             83
Last Reset Type:         Management Factory Reset
Power Status:            Primary Power
Autotopology:            Enabled
Pluggable Port 45:       None
Pluggable Port 46:       None
Pluggable Port 47:       None
Pluggable Port 48:       None
Base Unit Selection:     Non-base unit using rear-panel switch
sysDescr:                Ethernet Routing Switch 5520-48T-PWR
                         HW:02       FW:6.0.0.10  SW:v6.2.0.009
                         Mfg Date:12042004    HW Dev:H/W rev.02
```

1. Overview

Extensible Authentication Protocol over LAN is a port-based network access control protocol. EAPoL provides a method for performing authentication at the edge of the network in order to obtain network access based on the IEEE 802.1X standard.

802.1X specifies a protocol used between devices (EAP Supplicants) that desire access to the network and devices providing access to the network (EAP Authenticator). It also specifies the requirements for the protocol used between the EAP Authenticator and the Authentication server, i.e. RADIUS. The following are some of the 802.1X definitions:

- ***Authenticator:*** The entity that requires the entity on the other end of the link to be authenticated. Authenticator passes authentication exchanges between supplicant and authentication server.
- ***Supplicant:*** The entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.
- ***Port Access Entity (PAE):*** The protocol entity associated with a port. May support functionality of Authenticator, Supplicant or both.
- ***Authentication Server:*** An entity providing authentication service to the Authenticator. Maybe co-located with Authenticator, but most likely an external server.

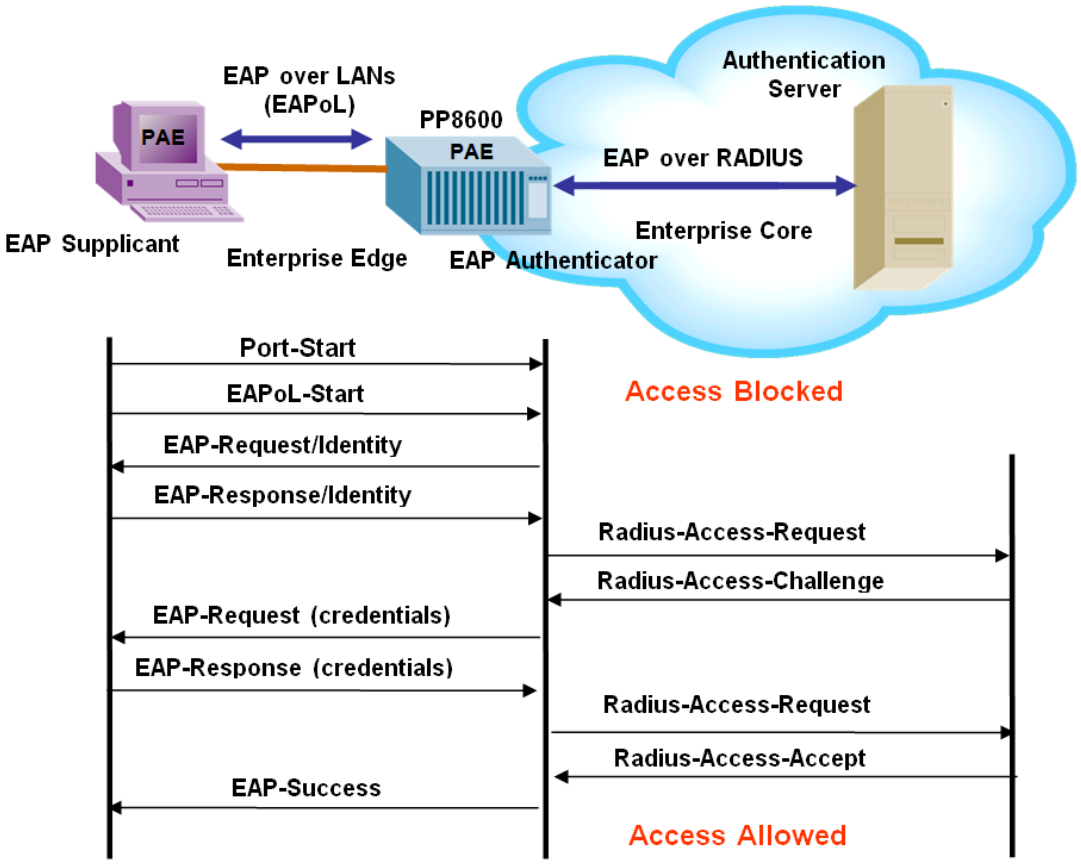
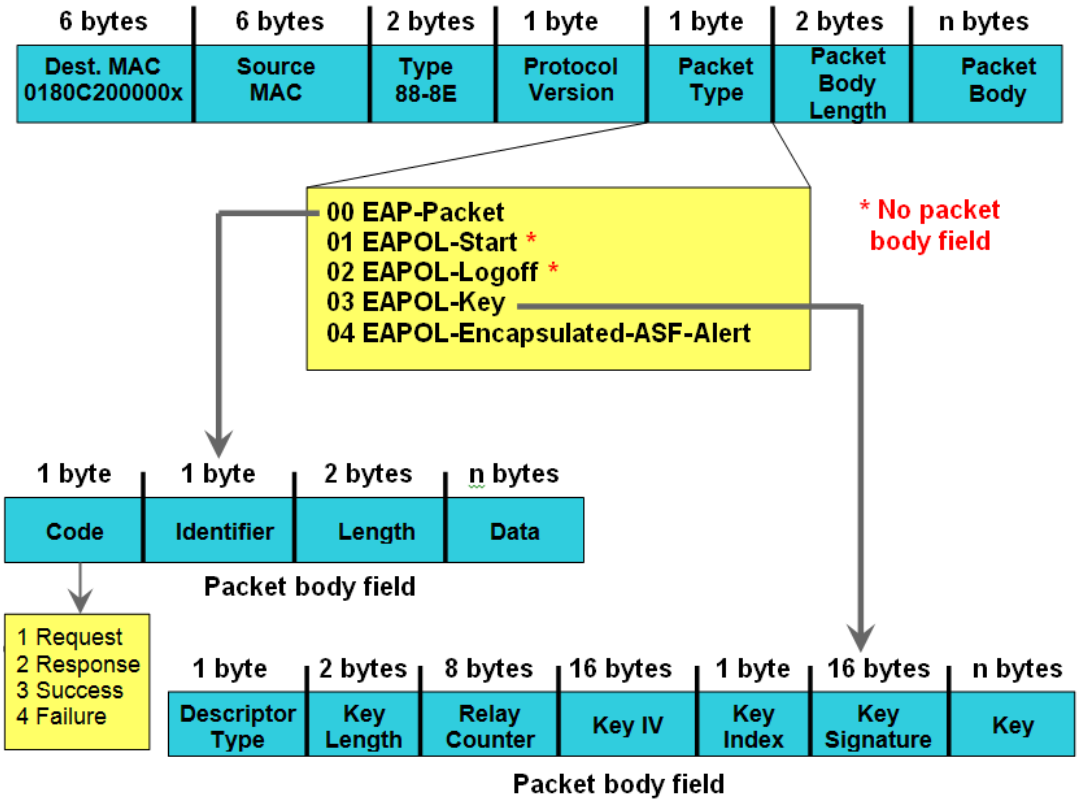


Figure 1 – EAP Authentication



EAP Request and Response Code Types

- Type code 1: Identity
- Type code 2: Notification
- Type code 3: NAK
- Type code 4: MD-5 Challenge
- Type code 5: One-time password (OTP)
- Type code 6: Generic Token Card
- Type code 13: TLS

EAP and RADIUS related RFCs

- RFC2284 – PPP Extensible Authentication Protocol
- RFC2716 – PPP EAP Transport Level Security (TLS) Authentication Protocol
- RFC2865 (Obsoletes RFC2138) – RADIUS
- RFC2548 – Microsoft Vendor specific RADIUS Attributes

Figure 2 – 802.1X Ethernet Frame

1.1 ERS 8000 EAP Flow Diagram

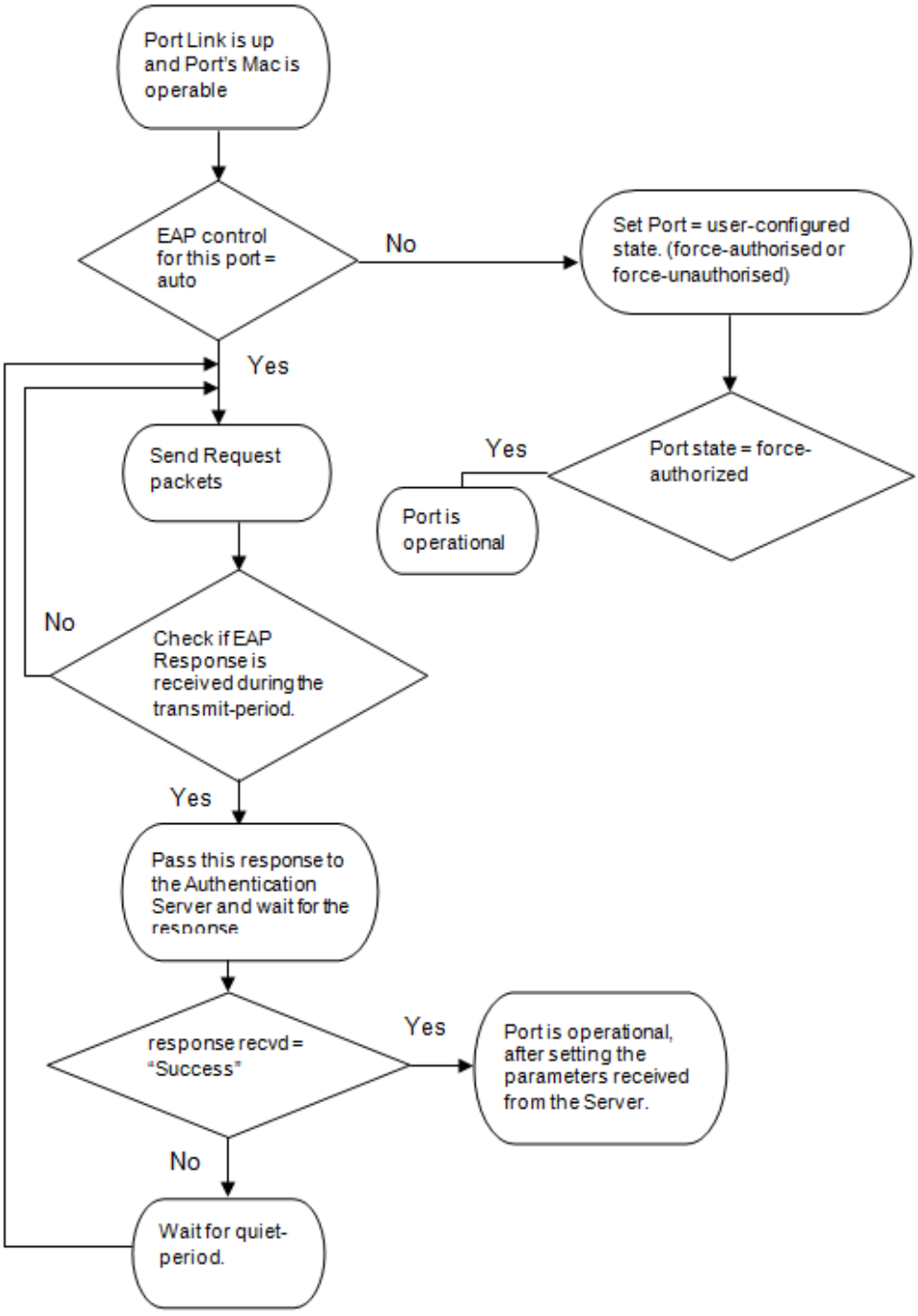


Figure 3 – EAP Flow Chart

1.2 Configuring EAP on the ERS 8000

The following steps are the basic steps to get EAPoL configured on the Ethernet Routing Switch 8000. The next section will cover all the various EAPoL port parameters available.

1	Enable EAP Globally

```
CLI

config sys set eapol <enable|disable>

ACLI

eapol enable
```

2	Set the EAPoL Authentication Status

```
CLI

config ethernet <slot/port> eapol admin-status <auto|force-unauthorized|force-
authorized>

ACLI

interface gigabitEthernet <slot/port>

eapol status <authorized|auto|unauthorized>

exit
```

For example, to enable EAP on Ethernet port 1/1, enter the following command:

```
ERS8600:5# config ethernet 1/1 eapol admin-status auto
```

EAP Auth State	Definition
Auto	Port authorization depends on the results of the EAPoL authentication by the RADIUS server.
Force-authorized Authorized	The port is always authorized.
Force-unauthorized Unauthforized	The port is always unauthorized.

3	Enable RADIUS Globally

```
CLI

config radius enable <true|false>

ACLI

radius enable
```

```
ERS8600:5# config radius enable true
```

4	Add Radius Server

```
CLI

config radius server create <IP address> secret [Word<0-32>] useby eapol

ACLI

radius server host <IP address> key [Word<0-32>] used-by eapol
```

By default, the Ethernet Routing Switch 8000 uses RADIUS UDP ports 1812 and 1813. You can change the port number or other RADIUS server options. List below are all the available options:

```
ERS8600:5# config radius server ?

Sub-Context:

Current Context:


    create <ipaddress/ipv6address> secret <value> [usedby <value>] [port <value>] [priority
<value>] [retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable
<value>] [source-ip <value>]

    delete <ipaddress/ipv6address> usedby <value>

    info

    set <ipaddress/ipv6address> usedby <value> [secret <value>] [port <value>] [priority <value>]
[retry <value>] [timeout <value>] [enable <value>] [acct-port <value>] [acct-enable <value>]
[source-ip <value>]
```

When a port is configured for EAP, i.e. EAP Status of auto, only one Supplicate is allowed on this port. In other words, multiple EAP Supplicants are not allowed on the same physical Ethernet Routing Switch 8000 port.

1.3 Other EAP Port Configuration Options

Listed below are all the port options available when configuring EAPoL.

1	Maximum Requests

You can set the maximum number of times to retry sending packets to the Supplicant by using the following command. The allowed range is 1 to 10, and the default is 2.

```
CLI

config ethernet <slot/port> eapol max-req <1…10>

ACLI

interface gigabitEthernet <slot/port>

eapol max-request <1…10>

exit
```

2	Port Re-authenticate
Re-authenticates the Supplicant connected to this port immediately. You must first enable re-authentication.	

```
CLI
config ethernet <slot/port> eapol reauthentication true
config ethernet <slot/port> eapol reauthenticate-now true
ACLI
interface gigabitEthernet <slot/port>
eapol re-authentication enable
eapol re-authentication
exit
```

4	Quiet Period
Sets the time interval (in seconds) between authentication failure and the start of a new authentication. The allowed range is 1 to 65535, and the default is 60.	

```
CLI
config ethernet <slot/port> eapol quiet-period <1-65535>
ACLI
interface gigabitEthernet <slot/port>
eapol quiet-interval <1-65535>
exit
```

5	Tx Period
Sets the time (in seconds) to wait for a response from a Supplicant for EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.	

```
CLI
config ethernet <slot/port> eapol transmit-period <1-65535>
ACLI
interface gigabitEthernet <slot/port>
eapol transmit-interval <1-65535>
exit
```

6	Supplicant Timeout
Sets the time (in seconds) to wait for a response from a Supplicant for all EAP packets except EAP Request/Identity packets. The allowed range is 1 to 65535, and the default is 30.	

```
CLI
config ethernet <slot/port> eapol supplicant-timeout <1-65535>
ACLI
interface gigabitEthernet <slot/port>
eapol supplicant-timeout <1-65535>
exit
```

7	**Server Timeout**

Sets the time (in seconds) to wait for a response from the RADIUS server. The allowed range is 1 to 65535, and the default is 30.

```
CLI
config ethernet <slot/port> eapol server-timeout <1-65535>
ACLI
interface gigabitEthernet <slot/port>
eapol server-timeout <1-65535>
exit
```

8	**Re-authentication Period**

Sets the time interval (in seconds) between successive re-authentications (refer to ReAuthEnabled). The allowed range is 1 to 2147483647, and the default is 3600 (1 hour).

```
CLI
config ethernet <slot/port> eapol reauthentication-period <1-2147483647>
ACLI
interface gigabitEthernet <slot/port>
eapol re-authentication-period <1-2147483647>
exit
```

The RADIUS server idle disconnect if enabled will override the Ethernet Routing Switch 8000 EAP reauthentication-period setting. For example, on a Windows IAS server, by default, idle disconnects is enabled and set for one minute. To disable IAS idle disconnect, edit your IAS profile, and remove the check box in the ***Disconnect if idle for:*** box in the ***Edit Dial-in Profile*** window.

1.4 EAP Show Commands

1	**To view the EAP global status, enter the following command:**

```
CLI
```

```
show sys eapol
ACLI
show eapol system
```

2	To view the RADIUS settings:

```
CLI
show radius info
show radius show-all
show radius server stat
show radius server config
ACLI
show radius
show radius-server statistics
show radius-server
```

3	To view various EAP port settings and status:

```
CLI
show ports info eapol ?
  auth-diags     show port eap authenticator diagnostics
  auth-stats     show port eap authenticator statistics
  config         show port eap config information
  oper-stats     show port eap operation statistics
  sess-manage    show port eap managed session
  session-stats  show port eap authenticator session stats
ACLI
show eapol ?
  auth-diags               Show port eap authenticator diagnostics
  auth-stats               Show port eap authenticator statistics
  multihost-session-stats  Show manage mode parameters specific to ops
  port                     Port
  session-stats            Show port eap authenticator session stats
  status                   Show port eap operation statistics
  system                   Show EAPOL setting
show eapol port <slot|port>
```

For example, to view the EAP operating status on Ethernet ports 1/24 and 1/25 enter the following command:

```
ERS8600:5# show ports info eapol oper-stats 1/24-1/25

================================================================
                        Eap Oper Stats
================================================================
PORT  CTRL   PORT          PAE               BKEND
      DIR    STATUS        STATUS            STATUS
----------------------------------------------------------------
1/24  both   authorized init          idle
1/25  both   authorized authorized    idle
----------------------------------------------------------------
```

Example: To view the EAP authenticator statistics on Ethernet ports 1/15, enter the following command:

```
ERS8600:5# show ports info eapol auth-stats 1/15

================================================================================
                                    Eap Authenticator Statistics
================================================================================
PORT  TOTAL TOTAL START LOGOFF RESP_ID RESP REQ-ID REQ INVALID LENGTH FRAME LAST-SRC
      RX    TX    RCVD  RCVD   RCVD    RCVD TX     TX  FRAMES  ERROR  VER   MAC
--------------------------------------------------------------------------------
1/15  121   3233  34    9      45      33   2374   859 0       0      1     00:d0:a8:00:61:3e
--------------------------------------------------------------------------------
```

Example: To view the EAP session statistic on port 1/45, enter the following command:

```
ERS8600:5# show ports info eapol session-stats 1/45

================================================================================
                                  Eap Authenticator Session Statistics
================================================================================
      TOTAL    TOTAL    TOTAL    TOTAL
      OCTETS   OCTETS   FRAMES   FRAMES  SESSION   AUTHENTIC SESSION              TERMINATE       USER
PORT  RCVD     TXMT     RCVD     TXMT    ID        METHOD    TIME                 CAUSE           NAME
--------------------------------------------------------------------------------
1/45  23179    17302    121       118    23000015  remote-server 0 day(s), 00:02:42 not-terminated  test
--------------------------------------------------------------------------------
```

1.5 RADIUS Return Attributes

The Ethernet Routing Switch 8000 uses the RADIUS tunnel attributes to place a port into a particular VLAN. This allows the Ethernet Routing Switch 8000 to support dynamic VLAN switching based on authentication.

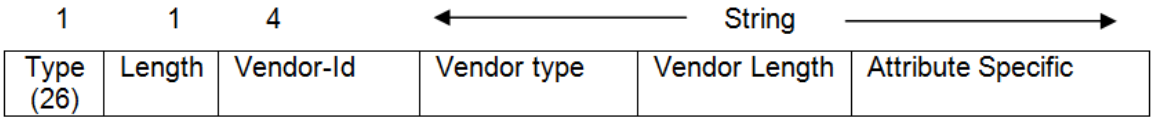
The RADIUS server indicated the desired VLAN by including the tunnel attribute within the Access-Accept message. The following tunnel attributes are used

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLAN ID

The VLAN ID is 12-bits, using a value from 1 to 4096 and is encoded as a string.

In addition, the RADIUS server can be setup to send a vendor-specific attribute to configure port priority. The Ethernet Routing Switch 8000 supplicant port can be assigned a QoS value from 0 to 7.

RADIUS Vendor-Specific frame format:



Ethernet Routing Switch 8600 Port Priority frame format:

- Vendor specific type = 26
- length = 12
- vendor-id = 0562
- string = vendor type = 1 + vendor length = 6 + attribute specific = priority

26	12	0562	01	06	(0 .. 7)

Figure 4 – RADIUS Frame Formats

2. Configuration Examples

2.1 EAPoL via L2

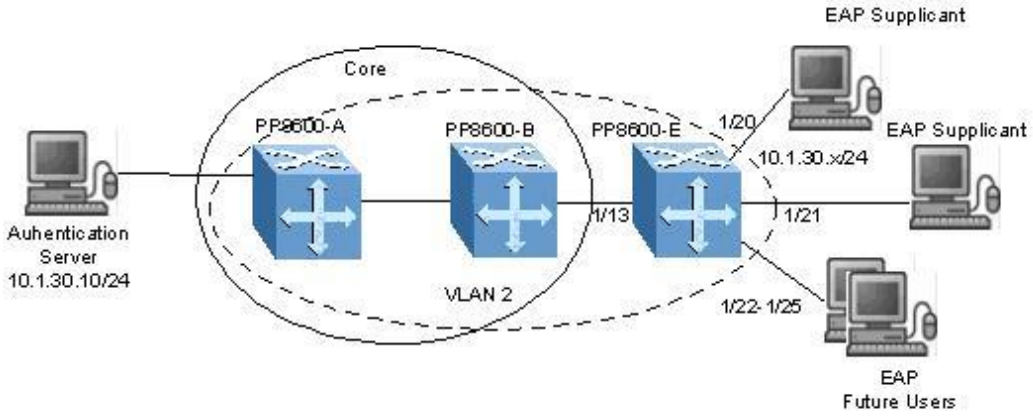


Figure 5 – Configuration Example 2.1, EAPoL via L2

For this configuration example, in reference to PP8600E only, VLAN 2 will be used for the EAP Supplicants using ports 1/20-1/25 and 1/13. We will assume only ports 1/20 and 1/21 are ready for EAPoL users. The other EAP Supplicant ports, ports 1/22-1/25, are for future EAPoL use and we do not wish to allow any possible EAP users on these port. In summary, we wish to accomplish the following on PP8600E:

- Create VLAN 2 for EAPoL with ports 1/13 and port 1/20-1/25
- Use IP address of 10.1.30.2/24 on VLAN 2
- Configure Ports 1/20 and 1/21 for EAPoL auto
- Configure ports 1/22-1/25 for EAPoL force-unauthentized
- Configure RADIUS-server on the PP8600E pointing to the Authentication Server

To accomplish the above, please follow the steps below:

1	**create VLAN 2 as a port-based VLAN using STG 1:**
ERS8600:5# ***config vlan 2 create byport 1***	
2	**If required, enabled VLAN tagging on port 1/13 and remove 1/13 from the default VLAN:**
ERS8600:5# ***config ethernet 1/13 perform-tagging enable*** ERS8600:5# ***config vlan 1 ports remove 1/13***	

3	**Add VLAN members:**
ERS8600:5# ***config vlan 2 ports add 1/13,1/20-1/25***	
4	**Add IP address to VLAN 2:**
ERS8600:5# ***config vlan 2 ip create 10.1.30.2/24***	
5	**Enable EAP Globally:**
ERS8600:5# ***config sys set eapol enable***	
6	**Enable EAPoL on ports 1/20 and 1/21:**
ERS8600:5# ***config ethernet 1/20-1/21 eapol admin-status auto***	
7	**Set Ports 1/22-1/25 to EAPoL unauthorized**
ERS8600:5# ***config ethernet 1/22-1/25 eapol admin-status force-unauthorized***	
8	**Enable RADIUS Globally:**
ERS8600:5# ***config radius enable true***	
9	**Add the RADIUS server, assuming the RADIUS key = eap8600:**
ERS8600:5# ***config radius server create 10.1.30.10 secret eap8600 usedby eap***	

2.2 EAPoL via L3

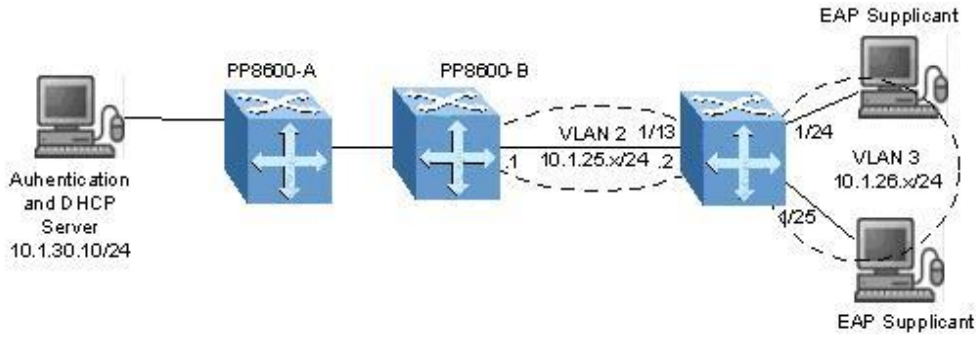


Figure 6 – Configuration Example 2.2, EAPoL via L3

For this configuration example, Ethernet Routing Switch 8600E is connected to a routed OSPF core. In summary, we wish to accomplish the following on PP8600E:

- Create VLAN 2 with port1/13 and IP address of 10.1.25.2/24 to be used to connect to the Core Network
- Create VLAN 3 with ports 1/24 and 1/25 and IP address of 10.1.26.1/24 to be used for the EAP Supplicants
- Enable OSPF on VLAN 2 and enable OSPF with interface type of passive on VLAN 3
- Enable DHCP relay on VLAN 3
- Configure RADIUS-server pointing to the Authentication Server

To accomplish the above, please follow the step below.

1	**Remove Ports from Default VLAN:**
`ERS8600:5#` ***`config vlan 1 ports remove 1/13,1/24-1/25`***	
2	**Create VLAN 2 as a port-based VLAN using STG 1:**
`ERS8600:5#` ***`config vlan 2 create byport 1`***	
3	**If required, enabled VLAN tagging on port 1/13:**
`ERS8600:5#` ***`config ethernet 1/13 perform-tagging enable`***	
4	**Add VLAN 2 members:**
`ERS8600:5#` ***`config vlan 2 ports add 1/13`***	
5	**Add IP address to VLAN 2:**
`ERS8600:5#` ***`config vlan 2 ip create 10.1.25.2/24`***	

If desired, disable spanning on port 1/13 if it is not required. Also, port 1/13 could also be configured as a brouter port instead of a VLAN member.

6	**Create VLAN 3 as a port-based VLAN using STG 1:**
ERS8600:5# ***config vlan 3 create byport 1***	
7	**Add VLAN 3 members:**
ERS8600:5# ***config vlan 3 ports add 1/24-1/25***	
8	**Add IP address to VLAN 3:**
ERS8600:5# ***config vlan 3 ip create 10.1.26.1/24***	
9	**Enable OSPF interface type as passive for VLAN 3:**
ERS8600:5# ***config vlan 3 ip ospf interface-type passive***	
10	**Enable OSPF on VLAN 3:**
ERS8600:5# ***config vlan 3 ip ospf enable***	
11	**Enable DHCP relay on VLAN 3:**
ERS8600:5# ***config vlan 3 ip dhcp-relay enable*** ERS8600:5# ***config vlan 3 ip dhcp-relay mode dhcp***	
12	**Globally enable OSPF:**
ERS8600:5# ***config ip ospf enable***	
13	**Globally enable DHCP agent:**
ERS8600:5# ***config ip dhcp-relay create-fwd-path agent 10.1.26.1 server 10.1.30.10 mode dhcp state enable***	
14	**Enable EAP Globally:**
ERS8600:5# ***config sys set eapol enable***	
15	**Enable EAPoL on ports 1/24 and 1/25:**
ERS8600:5# ***config ethernet 1/24-1/25 eapol admin-status auto***	

16	**Enable RADIUS Globally:**
ERS8600:5# ***config radius enable true***	
17	**Add the RADIUS server, assuming the RADIUS key = eap8600:**
ERS8600:5# ***config radius server create 10.1.30.10 secret eap8600 usedby eap***	

2.3 Dynamic VLAN with Port Priority

The Ethernet Routing Switch 8600/8800 supports Dynamic VLAN switching allowing for dynamic VLAN assignment tied to EAP supplicant authentication. This feature allows administrators to automatically place an EAP supplicant (such as an end station PC) into a specific VLAN depending on EAP supplicant login credentials, following a successful authentication. For failed authentication, EAP port will be in blocking state and all the traffic received on this port will be dropped.

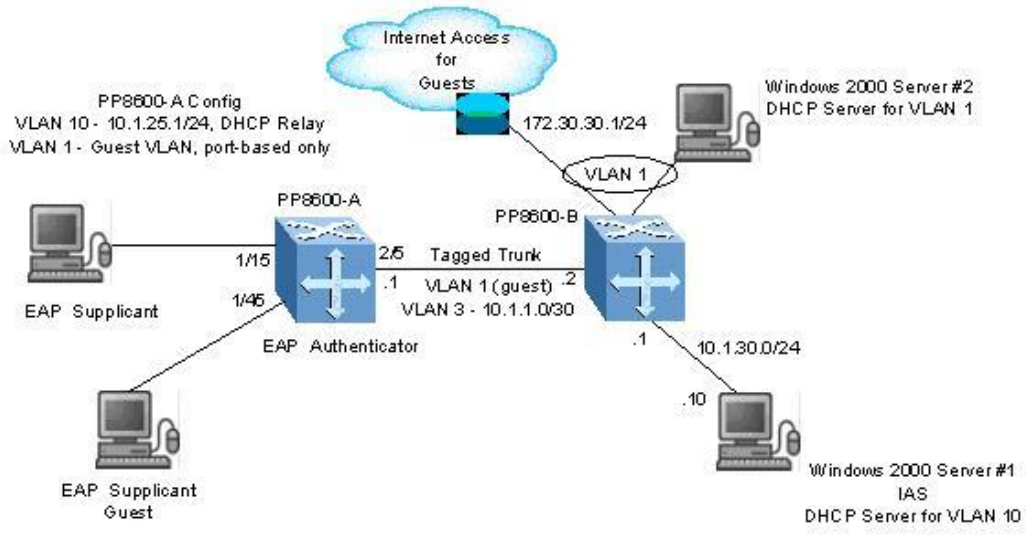


Figure 7 – Configuration Example 3, Dynamic VLAN with Port Priority

In this configuration example, we wish to accomplish the following in reference to PP8600-A:

- Place successfully EAP user supplicant into the working VLAN 10 and assign the port a QoS level of 5
- Place successfully authenticated guest EAP supplicant into the default VLAN 1 and leave the port with the default QoS level of 1
- In this configuration example, we wish to accomplish the following in reference to PP8600-A, OSPF is used for the working network. VLAN 10 will be configured as a passive OSPF interface with DHCP relay
- The default VLAN 1 will be left as-is as a port-based VLAN so that users in the default VLAN cannot have access to the working VLAN and only access to the Guest Internet router
- A separate DHCP Server, Server #2, will be used to assign an IP address in the 172.30.30.x/24 space for all guests.
- Server #1, a Windows 2000 server, is configured as an IAS (Internet Authentication Server) and as a DHCP Relay server only for the working VLAN 10

To accomplish the above, please follow the steps below.

2.3.1 PP8600-A Configuration

1	**Enable VLAN tagging on the Core Port 2/5. VLAN 1 and 3 will be added as port members for port 2/5:**
ERS8600:5# ***config ethernet 2/5 perform-tagging enable***	
2	**Remove all Ports from Default VLAN except 2/5:**
ERS8600:5# ***config vlan 1 ports remove 1/1-1/48,2/1-2/4,2/6-2/8***	
3	**Create VLAN 3 as a port-based VLAN using STG 1:**
ERS8600:5# ***config vlan 3 create byport 1***	
4	**Add VLAN 3 members:**
ERS8600:5# ***config vlan 3 ports add 2/5***	
5	**Add IP address to VLAN 3:**
ERS8600:5# ***config vlan 3 ip create 10.1.1.1/30***	
6	**Enable OSPF on VLAN 3:**
ERS8600:5# ***config vlan 3 ip ospf enable***	
7	**Create VLAN 10 as a port-based VLAN using STG 1. Note that no EAP supplicant port members are added as this will be decided upon a successful or unsuccessful EAP authentication:**
ERS8600:5# ***config vlan 10 create byport 1***	
8	**Add IP address to VLAN 10:**
ERS8600:5# ***config vlan 10 ip create 10.1.25.1/24***	
9	**Enable OSPF interface type as passive for VLAN 10:**
ERS8600:5# ***config vlan 10 ip ospf interface-type passive***	
10	**Enable OSPF for VLAN 10:**
ERS8600:5# ***config vlan 10 ip ospf enable***	

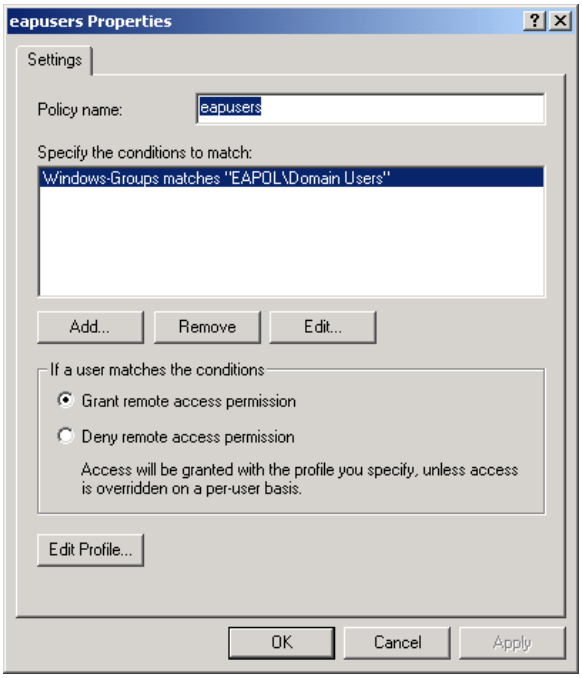
11	**Enable DHCP relay for VLAN 10:**
ERS8600:5# ***config vlan 10 ip dhcp-relay enable*** ERS8600:5# ***config vlan 10 ip dhcp-relay mode dhcp***	
12	**Globally enable OSPF:**
ERS8600:5# ***config ip ospf enable***	
13	**Globally enable DHCP agent:**
ERS8600:5# ***config ip dhcp-relay create-fwd-path agent 10.1.26.1 server 10.1.30.10 mode dhcp state enable***	
14	**Enable EAP Globally:**
ERS8600:5# ***config sys set eapol enable***	
15	**Enable EAPoL on ports 1/15 and 1/45:**
ERS8600:5# ***config ethernet 1/15,1/45 eapol admin-status auto***	
16	**Enable RADIUS Globally:**
ERS8600:5# ***config radius enable true***	
17	**Add the RADIUS server, assuming the RADIUS key = eap8600:**
ERS8600:5# ***config radius server create 10.1.30.10 secret eap8600 usedby eap***	

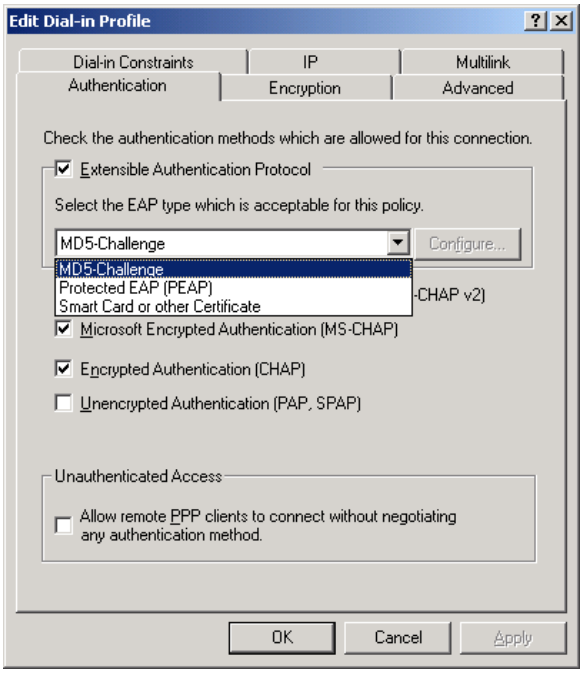
2.3.2 IAS Server Configuration

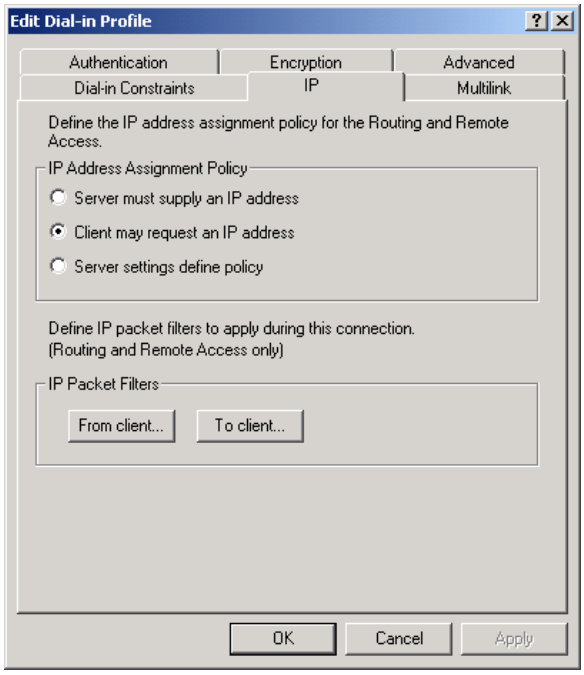
The Windows 2000 IAS server will require two Remote Access Policies, one for the working VLAN 10 and one for the guest default VLAN 1. We will create one policy named ***eapusers*** and assign Domain Users to the attribute Windows-Group. The other policy we will name ***eapdefault*** for EAP guest login and assign Domain Guests to the attribute Windows-Groups.

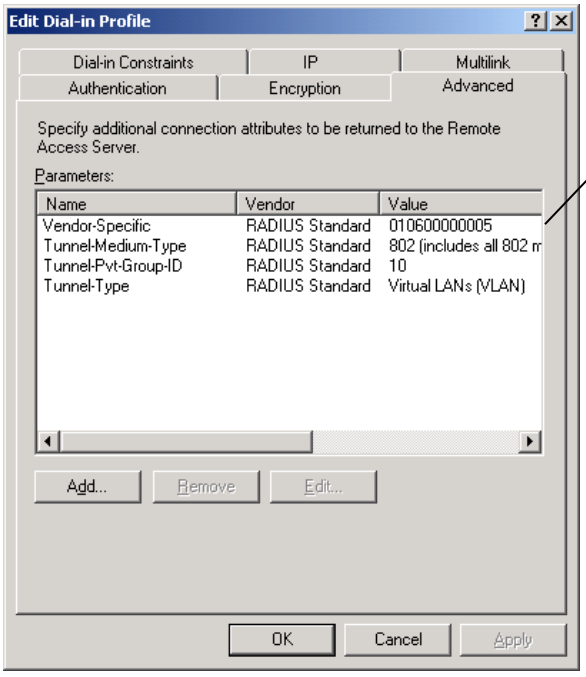
2.3.2.1 Configure Client Policy eapusers

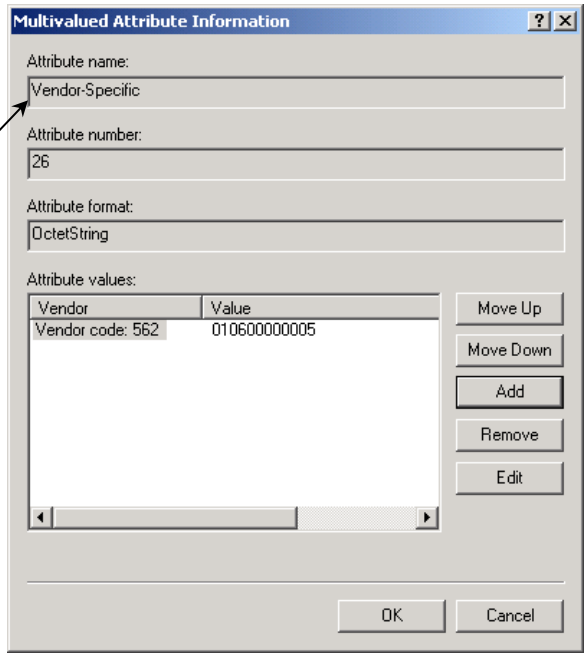
1	Go to IAS and then right-click on ***Remote Access Policies*** and select ***New Remote Access Policy***.
2	In the ***Add Remote Access Policy*** window, enter ***eapusers*** in the ***Policy friendly name*** window then click on ***next***.
3	In the next ***Conditions*** window, click on ***Add*** and select ***Windows-Groups*** in the ***Attribute types*** window then click on ***Add***.
4	In the next ***Groups*** window, click on ***Add*** and select ***Domain Users*** in the ***Select Groups*** window and then click on ***Add*** and ***OK***.
5	In the Permissions window, select ***Grant Remote Access Permission*** and then click on ***Next***.
6	Next you will need to edit the profile as shown below.




Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Check the authentication methods which are allowed for this connection.
Extensible Authentication Protocol
Select the EAP type which is acceptable for this policy.
MD5-Challenge
Configure...
MD5-Challenge
Protected EAP (PEAP)
Smart Card or other Certificate
-CHAP v2)
Microsoft Encrypted Authentication (MS-CHAP)
Encrypted Authentication (CHAP)
Unencrypted Authentication (PAP, SPAP)
Unauthenticated Access
Allow remote PPP clients to connect without negotiating any authentication method.
OK
Cancel
Apply

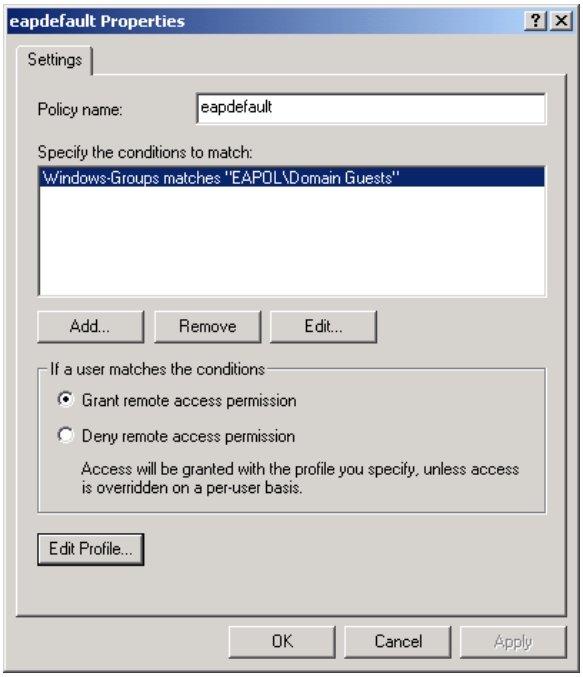

Edit Dial-in Profile
Authentication
Encryption
Advanced
Dial-in Constraints
IP
Multilink
Define the IP address assignment policy for the Routing and Remote Access.
IP Address Assignment Policy
Server must supply an IP address
Client may request an IP address
Server settings define policy
Define IP packet filters to apply during this connection.
(Routing and Remote Access only)
IP Packet Filters
From client...
To client...
OK
Cancel
Apply

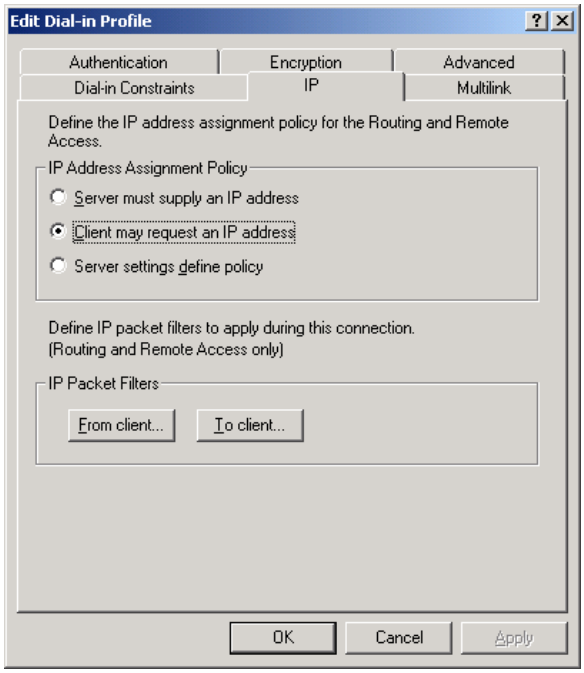

Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Specify additional connection attributes to be returned to the Remote Access Server.
Parameters:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
010600000005
Tunnel-Medium-Type
RADIUS Standard
802 (includes all 802 m
Tunnel-Pvt-Group-ID
RADIUS Standard
10
Tunnel-Type
RADIUS Standard
Virtual LANs (VLAN)
Add...
Remove
Edit...
OK
Cancel
Apply

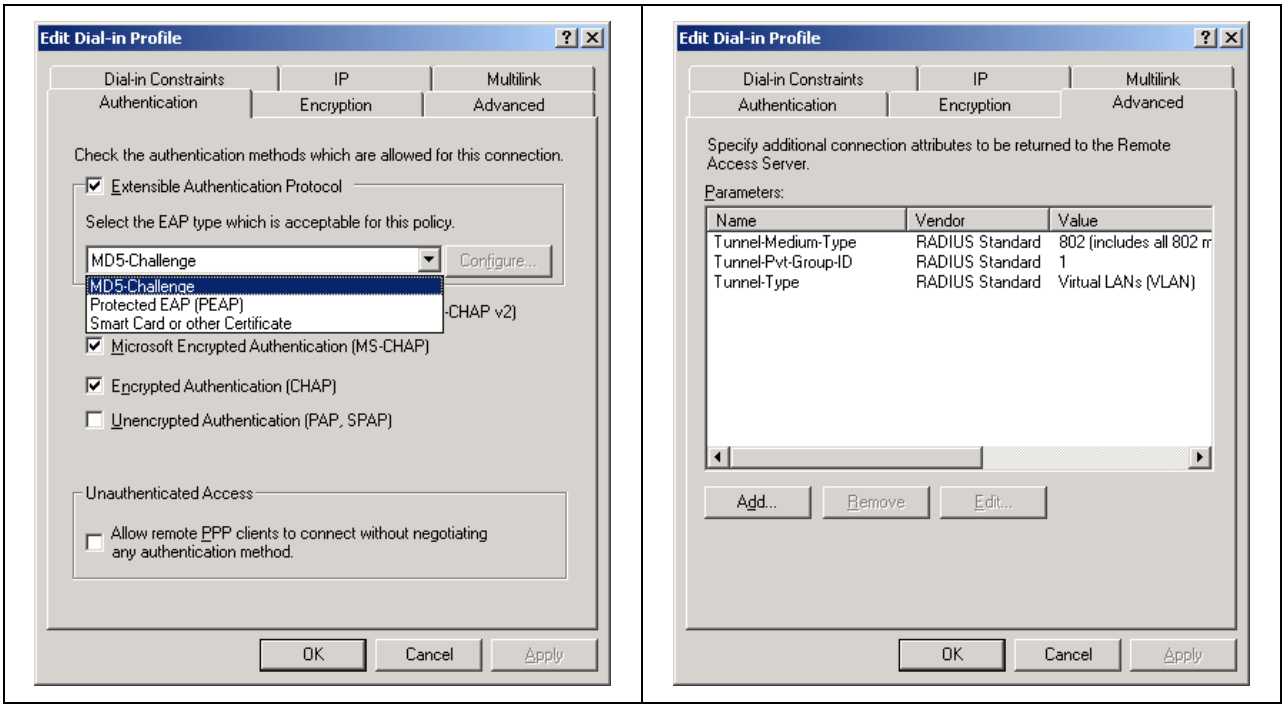

Multivalued Attribute Information
Attribute name:
Vendor-Specific
Attribute number:
26
Attribute format:
OctetString
Attribute values:
Vendor
Value
Vendor code: 562
010600000005
Move Up
Move Down
Add
Remove
Edit
OK
Cancel

2.3.2.2 Configure Client Policy eapdefault

1	Go to IAS and then right-click on ***Remote Access Policies*** and select ***New Remote Access Policy***.
2	In the ***Add Remote Access Policy*** window, enter **eapdefault** in the ***Policy friendly*** name window then click on ***next***.
3	In the next Conditions window, click on ***Add*** and select ***Windows-Groups*** in the ***Attribute types*** window then click on ***Add***.
4	In the next ***Groups*** window, click on ***Add*** and select ***Domain Guests*** in the ***Select Groups*** window and then click on ***Add*** and ***OK***.
5	In the ***Permissions*** window, select ***Grant Remote Access Permission*** and then click on ***Next***.
6	Next you will need to edit the profile as shown below.







2.3.2.3 Add Users to Active Directory

Next you will need to add user accounts the Microsoft Active Directory. All the working VLAN users should be a member of the Domain Users while the guest user must be a member of only the Domain Guests.

Make sure the check the following in the user properties:

- Check Store pass using reversible encryption in the Account tab
- Check Control access through Remote Access Policy in the Dial-in tab
- Members of Domain Users and RAS and IAS servers in the Member of tab

3. Reference Documentation

Publication Number	Document Title
Part No. 313197-D Rev 00	Network Design Guidelines
317177-A Rev 00	Release Notes for the Passport 8000 Series Switch Software Release 3.7
314724-C Rev 00	Configuring and Managing Security