

## **Tech Note 150**

# **Configuring a Microsemi Midspan With Cisco ACS RADIUS Server (v4.2)**

Revision 1.2  
Catalog Number 06-0034-081

# Introduction

This paper describes the procedures to be followed when using a Cisco ACS RADIUS server (v4.2) to configure access to a Midspan device. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access management for computers to connect to and use Midspan devices.

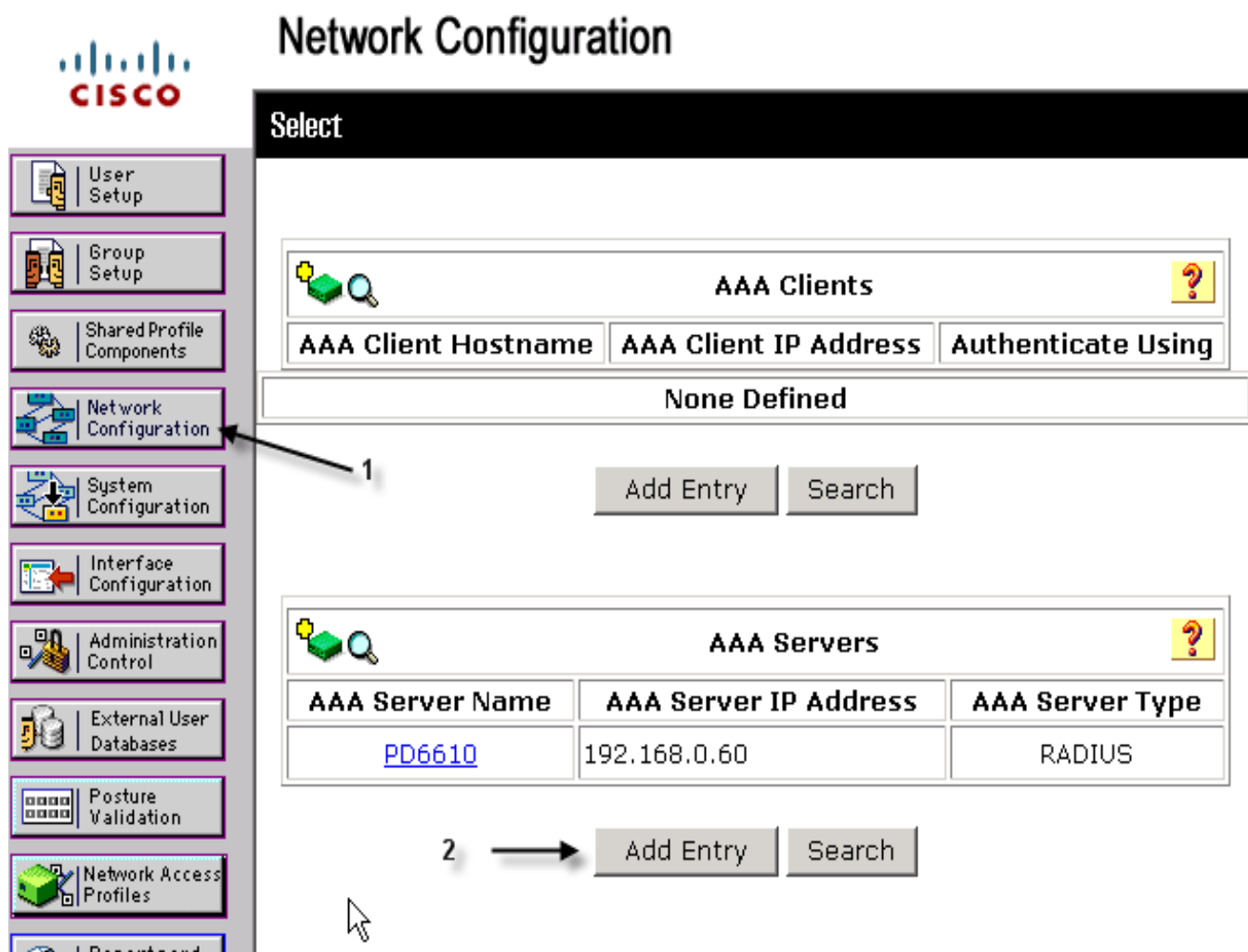
Configuration consists of:

- **Error! Reference source not found.**
- Defining the RADIUS AAA Client
- Defining the User Access Level
- **Error! Reference source not found.**

## Defining the Radius AAA Server

All servers must be added to Cisco ACS AAA Servers list

1. In the ACS RADIUS software, click **Network Configuration**.
2. Select an AAA Server.
3. Click Add Entry.
4. The AAA Server Setup dialog box appears.



**Network Configuration**

**Select**

**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry Search

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">PD6610</a>	192.168.0.60	RADIUS

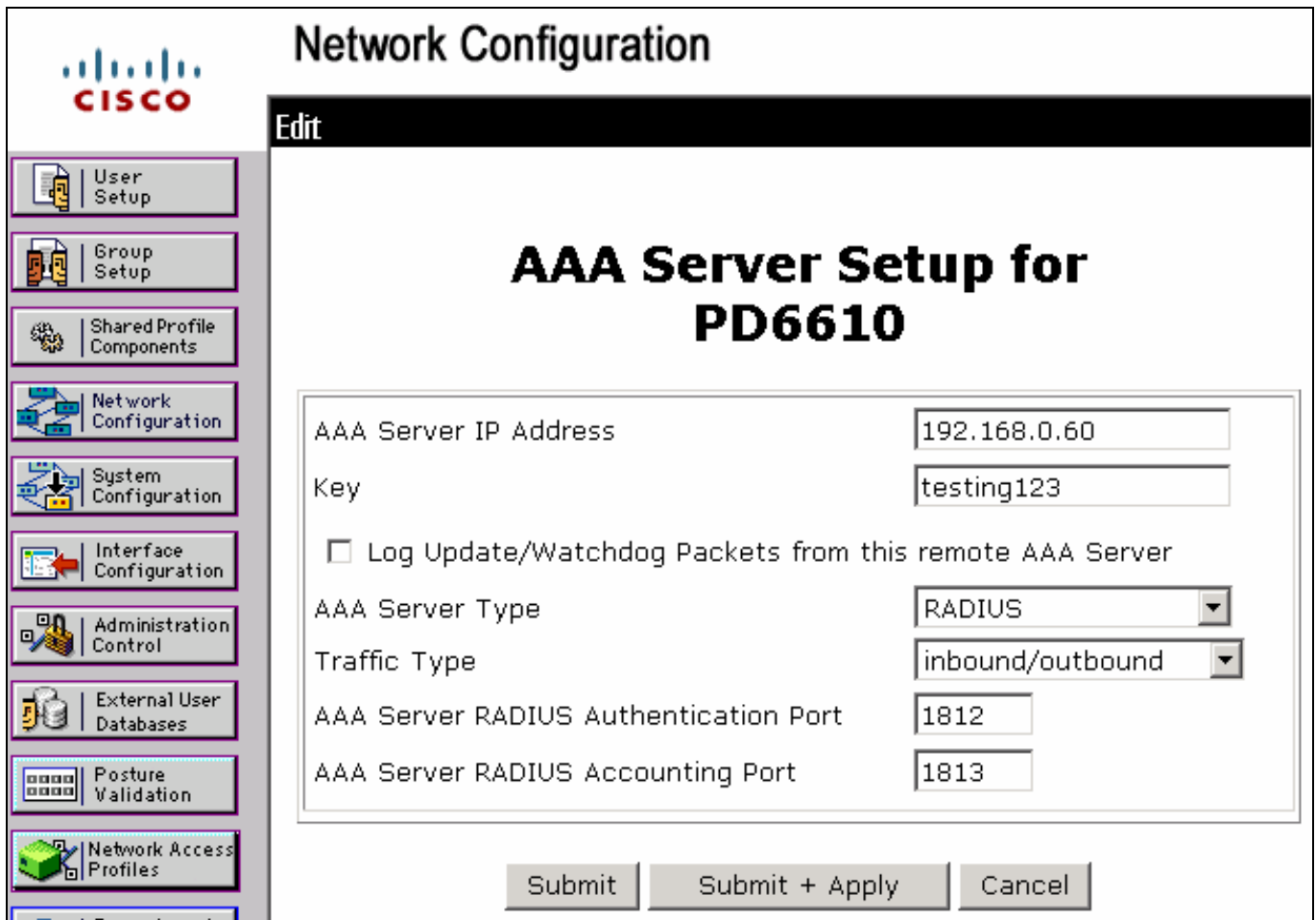
Add Entry Search

5. Enter the following Radius Server information:

- **AAA Server IP Address:** Radius Server IP address.
- **Key:** Shared Secret string. This string must match Midspan shared secret string.
- **AAA Server Type:** RADIUS.
- **Traffic Type:** Select inbound/outbound from the drop-down list.
- **AAA Server RADIUS Authentication Port:** Type **1812**. This number must match the Midspan Authentication UDP port.
- **AAA Server RADIUS Accounting Port:** Type **1813**. This number must match the Midspan Accounting UDP port.

6. Click **Submit + Apply**.

The server is defined



The screenshot shows the Cisco Network Configuration interface. On the left is a sidebar with icons and labels for various configuration sections: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, and Network Access Profiles. The main area is titled "Network Configuration" and "Edit". Below this is the heading "AAA Server Setup for PD6610". The configuration fields are as follows:

AAA Server IP Address	192.168.0.60
Key	testing123
<input type="checkbox"/> Log Update/Watchdog Packets from this remote AAA Server	
AAA Server Type	RADIUS
Traffic Type	inbound/outbound
AAA Server RADIUS Authentication Port	1812
AAA Server RADIUS Accounting Port	1813

At the bottom of the form are three buttons: "Submit", "Submit + Apply", and "Cancel".


## Defining the RADIUS AAA Client

All Midspan devices which were configured to use Radius Authentication must be added to Cisco ACS AAA Clients list

1. In the ACS RADIUS software, type the following AAA Client information:
  - **AAA Client Hostname:** Any string which describes your client type.
  - **AAA Client IP Address:** \*.\*.\* Enables handling all Midspan devices via a single AAA client.
  - **Shared Secret:** Must match Midspan shared secret string.
2. Click **Submit + Apply**.

The client is defined

### Add AAA Client

AAA Client Hostname	<input type="text" value="Midspan"/>
AAA Client IP Address	<input type="text" value="*,*,*,*"/> 
Shared Secret	<input type="text" value="testing123"/>

---

**RADIUS Key Wrap**

Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal

---

Authenticate Using

- ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- ☐ Log Update/Watchdog Packets from this AAA Client
- ☐ Log RADIUS Tunneling Packets from this AAA Client
- ☐ Replace RADIUS Port info with Username from this AAA Client
- ☐ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

## User Access Level

A remote user can have one of two access levels:

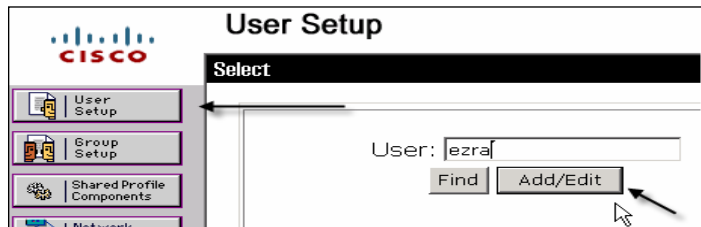
- View access level
- Configuration access level

### Defining a Remote User with View Access Level

This procedure defines how to configure View access level. A remote user with View access level can only view sections under Telnet/SSH/Web (as view-status Web Page).

1. Click **User-Setup**.
2. In the User field, type the user name.
3. Click **Add/Edit**.

The User Setup dialog box appears.



**User Setup**

Select

User: ezra

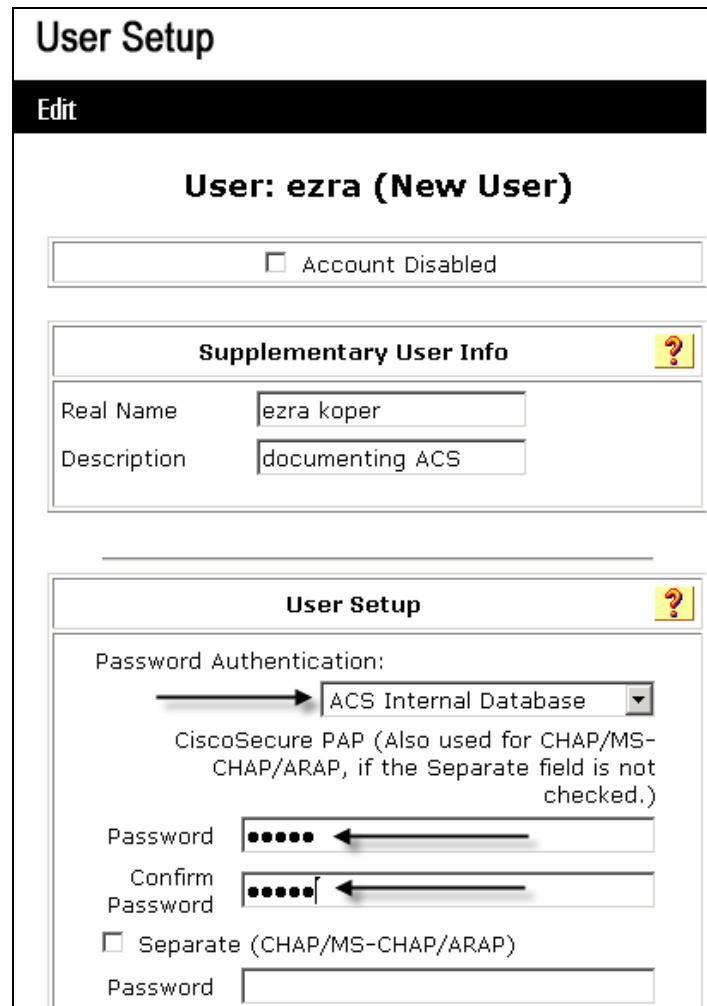
Find Add/Edit

4. Enter the following information:
  - **Real Name:** Type any string.
  - **Description:** Type any string.
  - **Password Authentication:** Select ACS Internal Database from the drop down list.

**Note:** This step is only done where no external data base is in use.

- **Password:** Type the remote user password.
  - **Confirm Password:** Type the remote user password.
5. Click **Submit**.

The user has been defined as having view access level only.



**User Setup**

Edit

**User: ezra (New User)**

☐ Account Disabled

**Supplementary User Info**

Real Name: ezra koper

Description: documenting ACS

**User Setup**

Password Authentication: ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: .....

Confirm Password: .....

☐ Separate (CHAP/MS-CHAP/ARAP)

Password: .....

## Defining a Remote User with Configuration Access Level

A remote user with Configuration access level has full access to all Telnet/SSH/Web sections.

1. Click **User-Setup**.
2. In the User field, type the user name.
3. Click **Add/Edit**.
4. Enter the following information:
  - **Real Name:** Free text.
  - **Description:** Free text.
  - **Password Authentication:** Select **ACS Internal Database** from the drop down list (in case no external data base is in use).
  - **Password:** Type the remote user password.
  - **Confirm Password:** Type the remote user password
5. Under Callback, select **Callback using this number**.
6. In the field below, type *admin* as the callback number.
7. Click Submit.

The user has been defined as having configuration access level.

User Setup

Edit

User: ezra1 (New User)

☐ Account Disabled

Supplementary User Info

Real Name

ezra as administrator

Description

full access

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

.....

Confirm Password

.....

☐ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Default Group

Callback

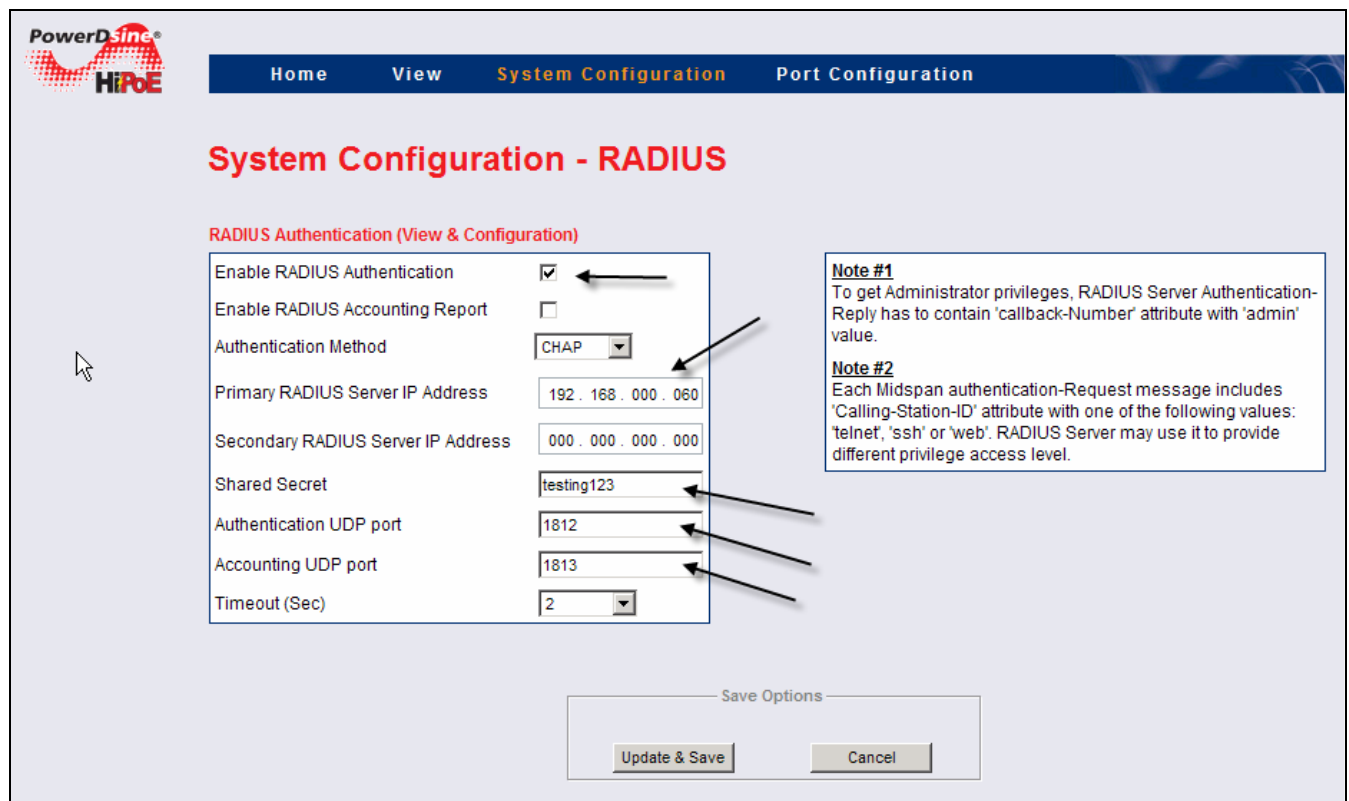
☐ Use group setting
 ☐ No callback allowed
 ☒ Callback using this number
 

admin

☐ Dialup client specifies callback number
 ☐ Use Windows Database callback settings

# Enabling Midspan Radius Authentication

1. In a web browser, type the device IP address to access the Midspan Radius Configuration Web page.
2. Fill in the following fields:
  - **Mark** Enable Radius Authentication.
  - **Authentication Method:** CHAP.
  - **Primary Radius Server IP Address:** Cisco ACS Server IP Address.
  - **Shared Secret:** Must match the same shared secret as defined in Cisco ACS Server (see Step #1 and Step #2).
  - **Authentication UDP Port:** Must match the Authentication UDP port entered in Step #1.
  - **Accounting UDP Port:** Must match the Accounting UDP ports entered in Step #1.
3. Click **Update & Save**.



**PowerDsinc® HiPoE**

Home View **System Configuration** Port Configuration

### System Configuration - RADIUS

**RADIUS Authentication (View & Configuration)**

Enable RADIUS Authentication	<input checked="" type="checkbox"/>
Enable RADIUS Accounting Report	<input type="checkbox"/>
Authentication Method	CHAP
Primary RADIUS Server IP Address	192 . 168 . 000 . 060
Secondary RADIUS Server IP Address	000 . 000 . 000 . 000
Shared Secret	testing123
Authentication UDP port	1812
Accounting UDP port	1813
Timeout (Sec)	2

**Note #1**  
To get Administrator privileges, RADIUS Server Authentication-Reply has to contain 'callback-Number' attribute with 'admin' value.

**Note #2**  
Each Midspan authentication-Request message includes 'Calling-Station-ID' attribute with one of the following values: 'telnet', 'ssh' or 'web'. RADIUS Server may use it to provide different privilege access level.

Save Options

Update & Save Cancel



## Configuring a Microsemi Midspan

*The information contained in the document is PROPRIETARY AND CONFIDENTIAL information of Microsemi and cannot be copied, published, uploaded, posted, transmitted, distributed or disclosed or used without the express duly signed written consent of Microsemi. If the recipient of this document has entered into a disclosure agreement with Microsemi, then the terms of such Agreement will also apply. This document and the information contained herein may not be modified, by any person other than authorized personnel of Microsemi. No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the information, either expressly, by implication, inducement, estoppel or otherwise. Any license under such intellectual property rights must be express and approved by Microsemi in writing signed by an officer of Microsemi.*

*Microsemi reserves the right to change the configuration, functionality and performance of its products at anytime without any notice. This product has been subject to limited testing and should not be used in conjunction with life-support or other mission-critical equipment or applications. Microsemi assumes no liability whatsoever, and Microsemi disclaims any express or implied warranty, relating to sale and/or use of Microsemi products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. The product is subject to other terms and conditions which can be located on the web at <http://www.microsemi.com/company/terms-and-conditions>*

### Revision History

Revision Level / Date	Para. Affected	Description
Rev 1.1 / 4-Nov-11	Entire Document	Formatting
Rev 1.2 /24-May-16		Replace "Powerdsine" by "Microsemi"

© 2011 Microsemi Corp.

All rights reserved.

For support contact: [PoEsupport@microsemi.com](mailto:PoEsupport@microsemi.com)

Visit our web site at: [www.microsemi.com/products/poe-systems/poe-systems](http://www.microsemi.com/products/poe-systems/poe-systems)

Catalog Number: 06-0034-081