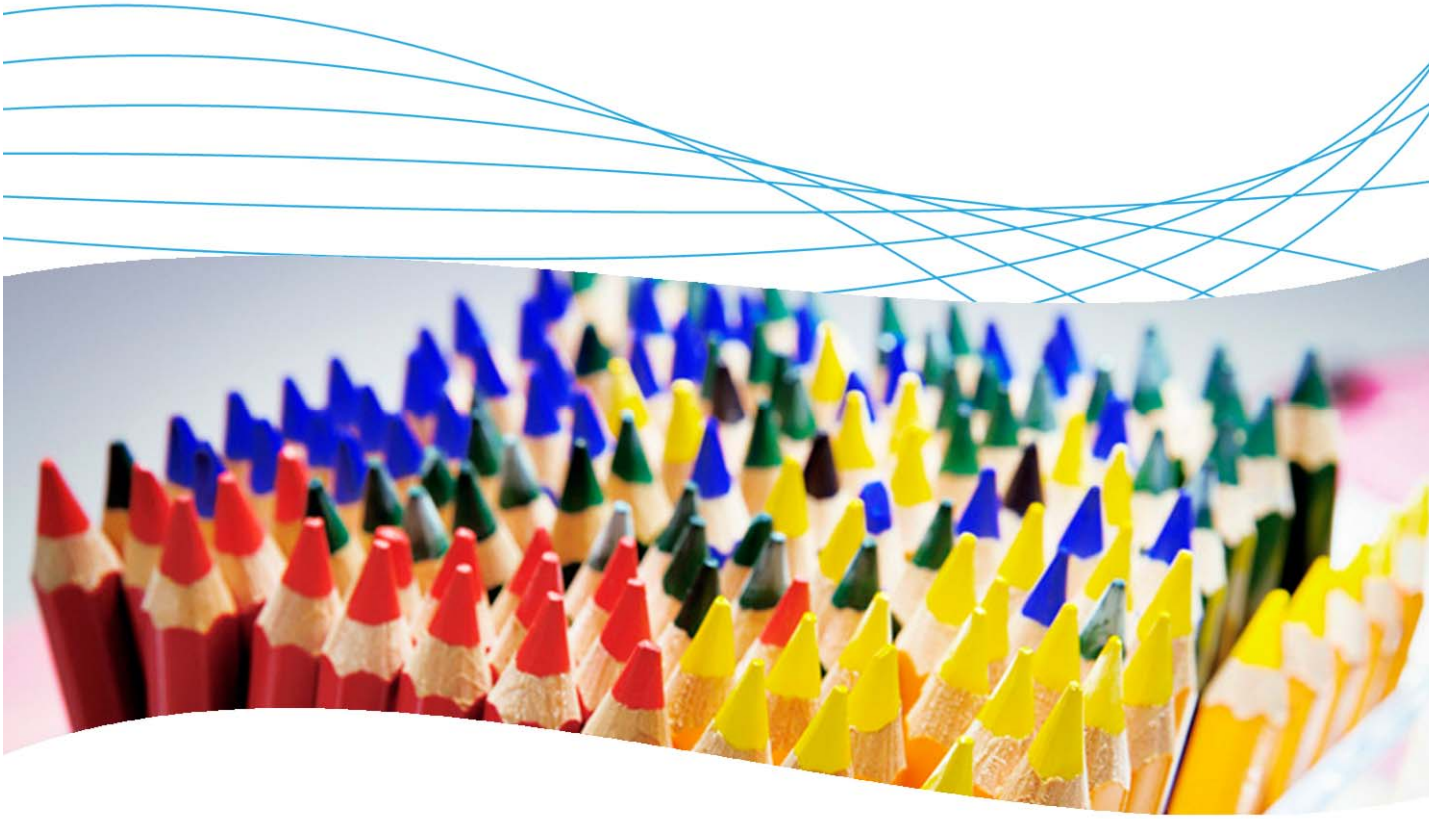
An HP ProCurve Networking Application Note

How to configure MAC authentication on a ProCurve switch



Contents

1. Introduction

This document describes how to configure MAC authentication using a ProCurve switch and a RADIUS server (Microsoft IAS). The switch used in this example is an HP ProCurve Switch 5400zl, but most ProCurve switches can be configured in the same manner.

2. Prerequisites

This procedure assumes you have an already configured RADIUS server (Microsoft IAS, on Windows Server 2003), and have created the necessary users and groups.

3. Network diagram

Figure 1 details the configuration referenced in this section.

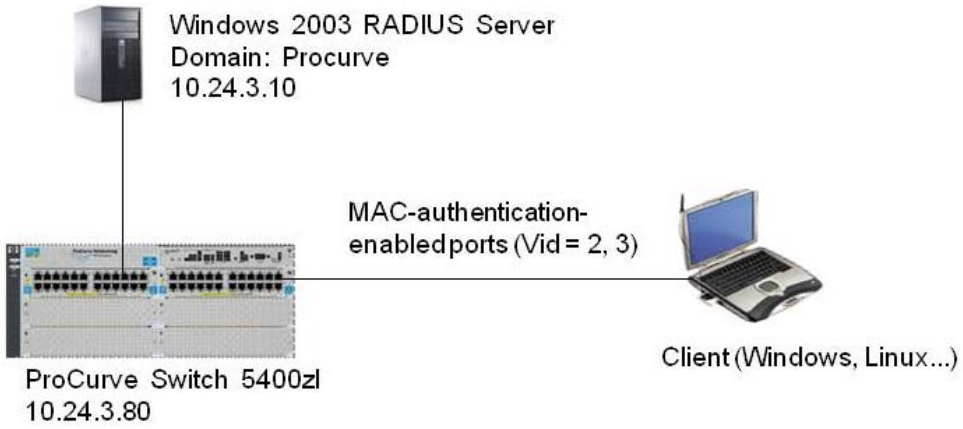


Figure 1. Setup for MAC authentication

Using this topology, you will configure the clients, switch, and RADIUS server to allow access to the network via MAC authentication. You will use two VLANs to separate traffic between authorized and unauthorized users.

4. Configuring the ProCurve Switch 5400zl

As stated in the previous section, to keep the unauthorized and authorized traffic separate and secure, you will divide them into two separate VLANs. The first VLAN, ID=2, will be used to hold the unauthorized traffic. The second VLAN, ID=3, will be used to hold the authorized traffic.

4.1 Configure the VLANs

In order to support the authorized and unauthorized VLANs on the HP ProCurve Switch 5400zl, you need to create the VLANs and assign the uplink ports to the designated VLANs.

Connect to the 5400zl switch and enter the following commands:

```
5400zl> en
5400zl# config term
5400zl(vlan-1)# vlan 2
5400zl(vlan-2)# name "unauth"
5400zl(vlan-2)# untag all
5400zl(vlan-2)# vlan 3
5400zl(vlan-3)# name "auth"
5400zl(vlan-3)# ip addr 10.24.3.80/24
```

```
5400zl(vlan-3)# exit
5400zl(config)# ip default-gateway 10.24.3.1

5400zl(config)# exit
5400zl# write mem
```

4.2 Configure access to the RADIUS server

Now that you have created the VLANs, you need to tell the HP ProCurve Switch 5400zl how to authorize clients and how to handle client traffic. Connect to the 5400zl switch and enter the following commands to tell the switch to access a RADIUS server:

```
5400zl# config term
5400zl(config)# radius-server host 10.24.3.10 key hpsecret
5400zl(conifg)# show radius

 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :

                        Auth          Acct
  Server IP Addr        Port          Port          Encryption Key
  ----------------      -----         -----         --------------------------
  10.24.3.10            1812          1813          hpsecret

5400zl(config)# exit
5400zl# write mem
5400zl# ping 10.24.3.10
10.24.3.10 is alive, time = 25 ms
5400zl#
```

4.3 Configure the ProCurve switch for MAC authentication

After the 5400zl switch knows the address of the RADIUS server, you next restrict the security on the switch and enable MAC authentication. Restricting the access to the switch and specifying secure communication to it is necessary to create a secure environment.

The following steps create local usernames, set up SSL communications, and set the MAC authentication parameters to the switch:

```
5400zl# config term
5400zl(config)# password manager user-name admin
New password for Manager: procurve
Please type new password for Manager: procurve
5400zl(config)# crypto key gen cert 1024
Installing new RSA key. If the key/entropy cache is
depleted, this could take up to a minute.
```

```
5400zl(config)# aaa port-access mac-based a5

LACP has been disabled on 'port-access' enabled port(s).

5400zl(config)# aaa port-access mac-based a5 auth-vid 3
5400zl(config)# aaa port-access mac-based a5 unauth-vid 2
5400zl(config)# exit
5400zl# write mem
```

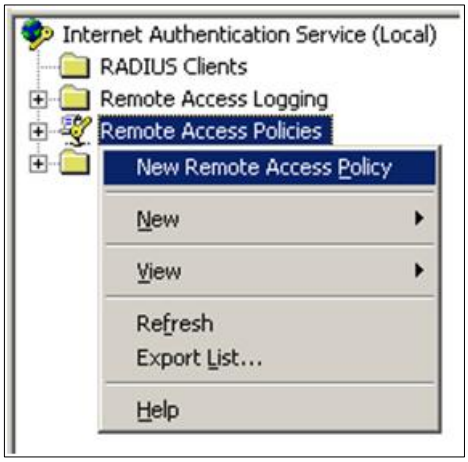
5. Configuring the RADIUS server

With the switch configured, the next step is to configure the Windows 2003 IAS RADIUS server.

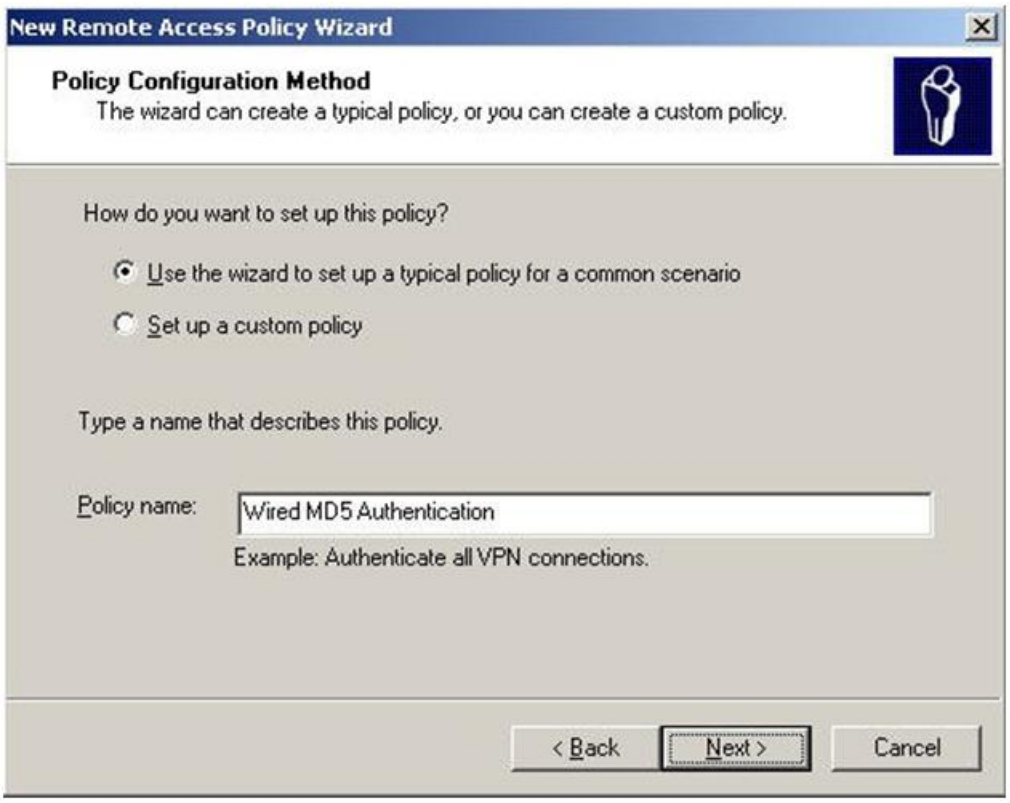
5.1 Configure the policy

You first need to define a policy to allow MAC authentication to work. To configure the policy:

1. In IAS, right click “Remote Access Policies” and choose “New Remote Access Policy”. You see the New Remote Access Policy Wizard pop up.

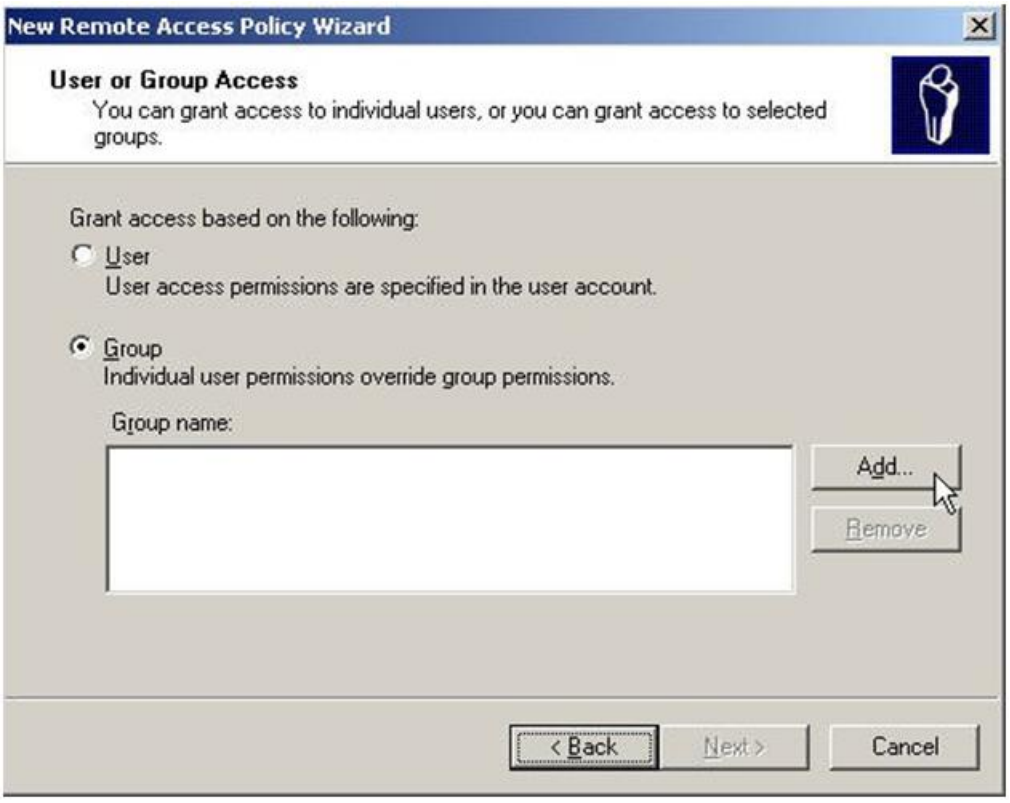


2. In the New Remote Access Policy Wizard, click Next. You see the Policy Configuration Method window:

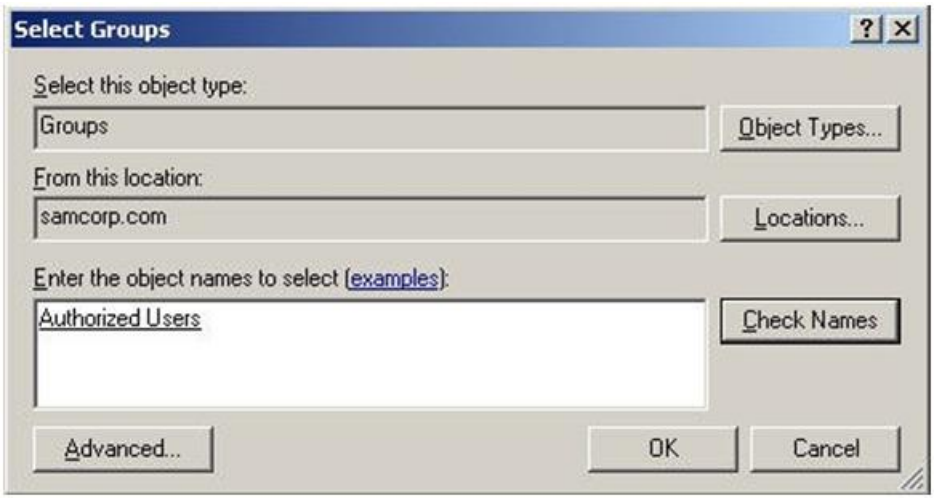


3. In the Policy Configuration Method window, select Use the wizard and provide a policy name (for example, Wired MD5 Authentication). Then click Next.

4. Select Ethernet and click Next. You see a window to choose user or group access.



5. Select Group and click the Add button. You see the Select Groups window:



6. In the Enter the object names to select text box enter Authorized Users and click the Check Names button. The group name will be validated and should show as underlined.

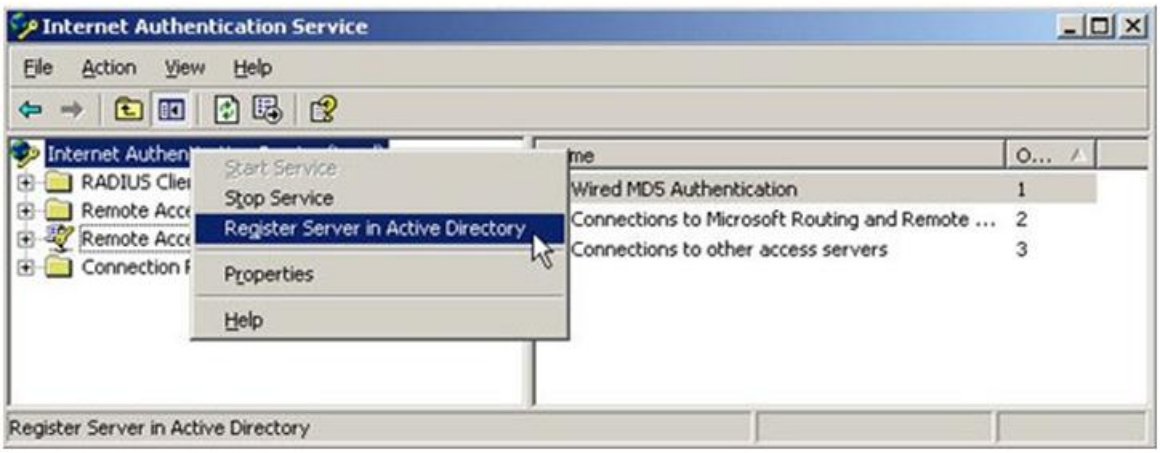
7. When the group name has been validated, click the OK button.

8. Select Next.

9. Verify MD5−Challenge is selected in the Type drop down box and press Next. You see the window for Completing the New Remote Access Policy Wizard.

10. Select Finish.

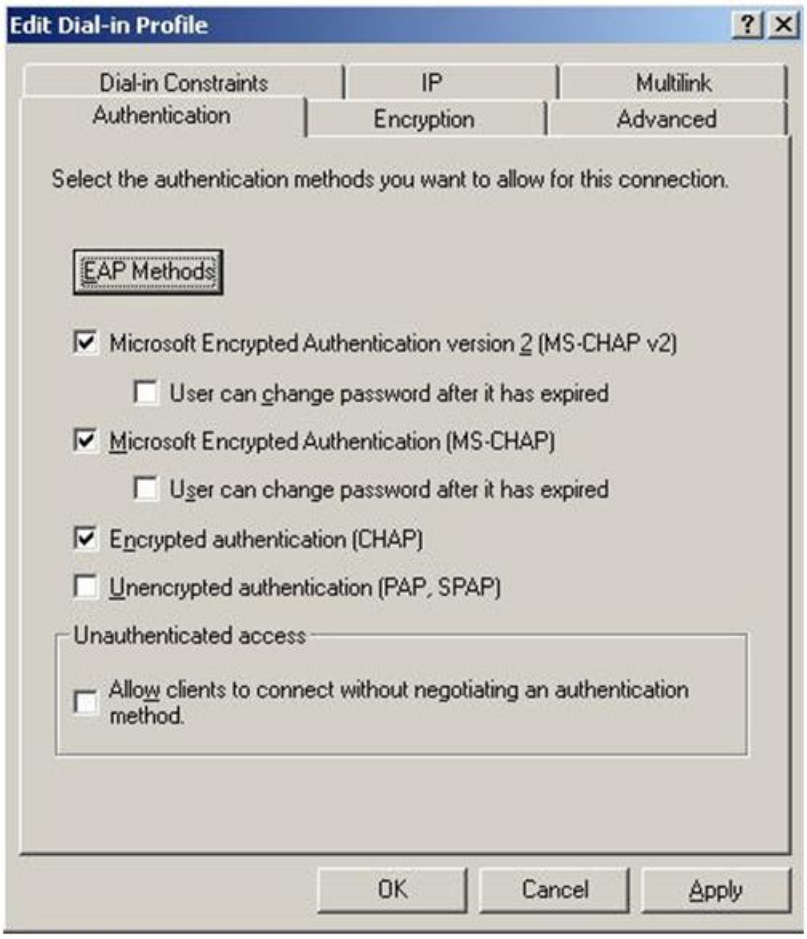
11. In the Internet Authentication Service window, right-click on Internet Authentication Service (local) and select Register Service in Active Directory.



12. Select OK at Register dialog box and on following boxes.

13. Right-click on the policy you just created, Wired MD5 Authentication, and select Properties.

14. Click the Edit Profile button, and select the Authentication tab. You see the screen with choices for authentication:



15. In the Authentication tab, select the MS−CHAP v2, MS−CHAP, and CHAP check boxes to turn on these authentication methods, and click OK.

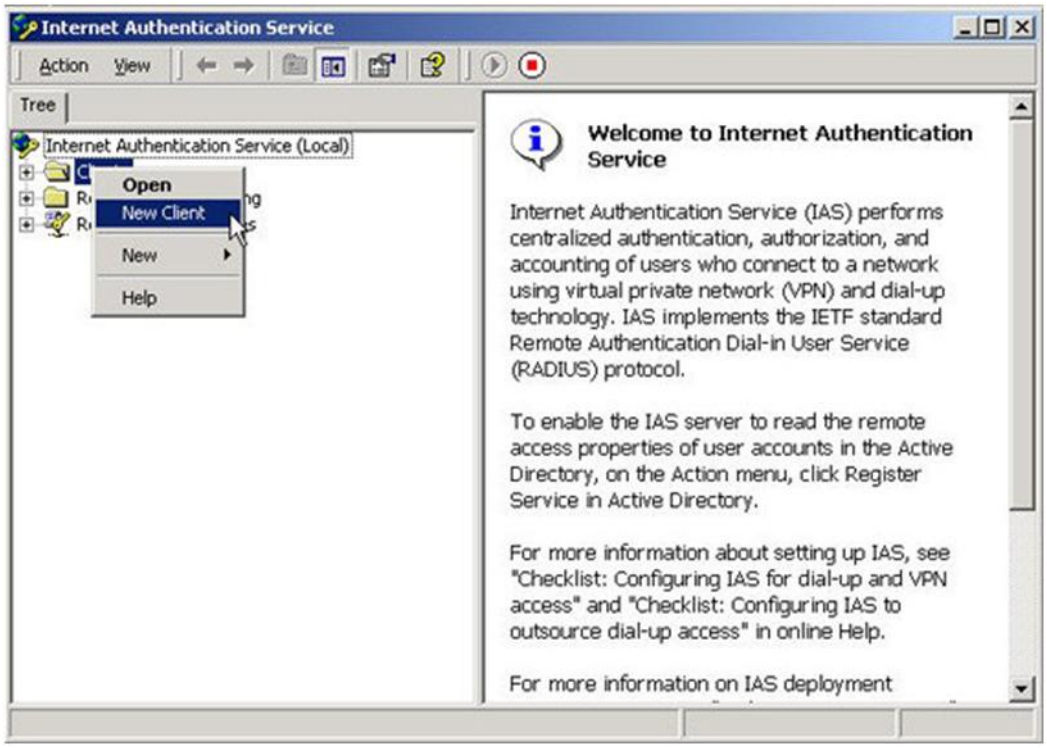
16. Select No to the Help Topic warning box.

17. Select OK at the Authentication Properties screen.

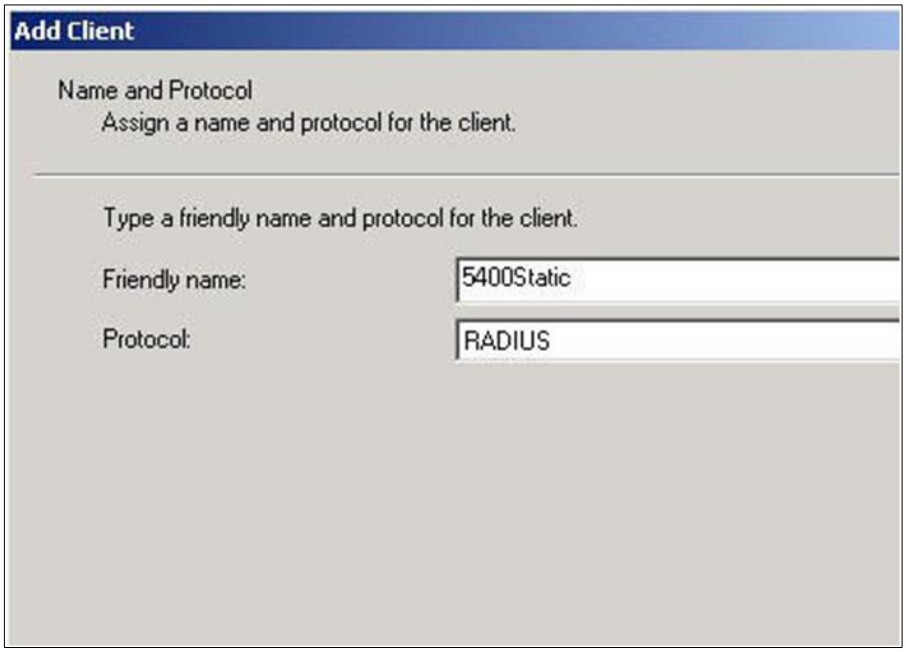
5.2 Configure IAS clients

You now need to configure the IAS server to recognize the RADIUS client and users making the requests. This means that you need to identify the ProCurve Switch 5400zl as a RADIUS client. To do this in a Windows 2003 environment, you add the switch to the IAS client table, as follows:

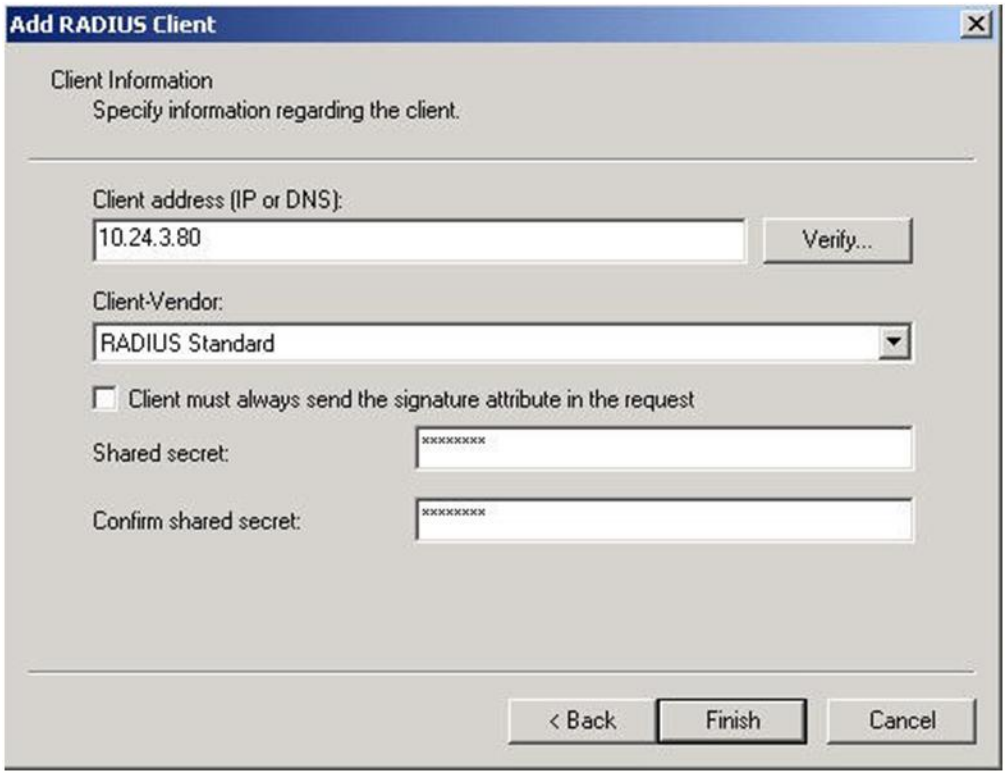
1. To load the IAS management console on the IAS server, go to Start > Programs > Administrative Tools > Internet Authentication Service. You see the Welcome page:



2. Right−click on RADIUS Clients and select New Client. You see the Add Client window:



3. In the Add Client window, enter a name for the HP ProCurve 5400zl (for example, 5400Static) in the Friendly name text box and click Next. You see the Add RADIUS Client window:



4. In the Add RADIUS Client window:
   - Enter the IP Address or DNS Name of the HP ProCurve Switch 5400zl (for example, 10.24.3.80).
   - Select RADIUS Standard as the Client−Vendor.
   - Enter a secret (for example, hpsecret) in the Shared secret field.
   - And make sure the check box next to Client must always send the signature attribute in the request is *not* selected.
5. Then click Finish to complete adding the RADIUS client.

6. Configuring users

Since the only authorization performed with MAC−Auth is verification of the MAC address, you need to define the user machine's MAC address in the user database. With IAS, the user database is Windows Active Directory. This presents a security issue, since the MAC address is listed as a user with the password matching the username.

To help prevent unwanted access by a machine spoofing a MAC address, you need to remove the user record from the Domain Users group and add it to a restricted group that has access only to needed resources.

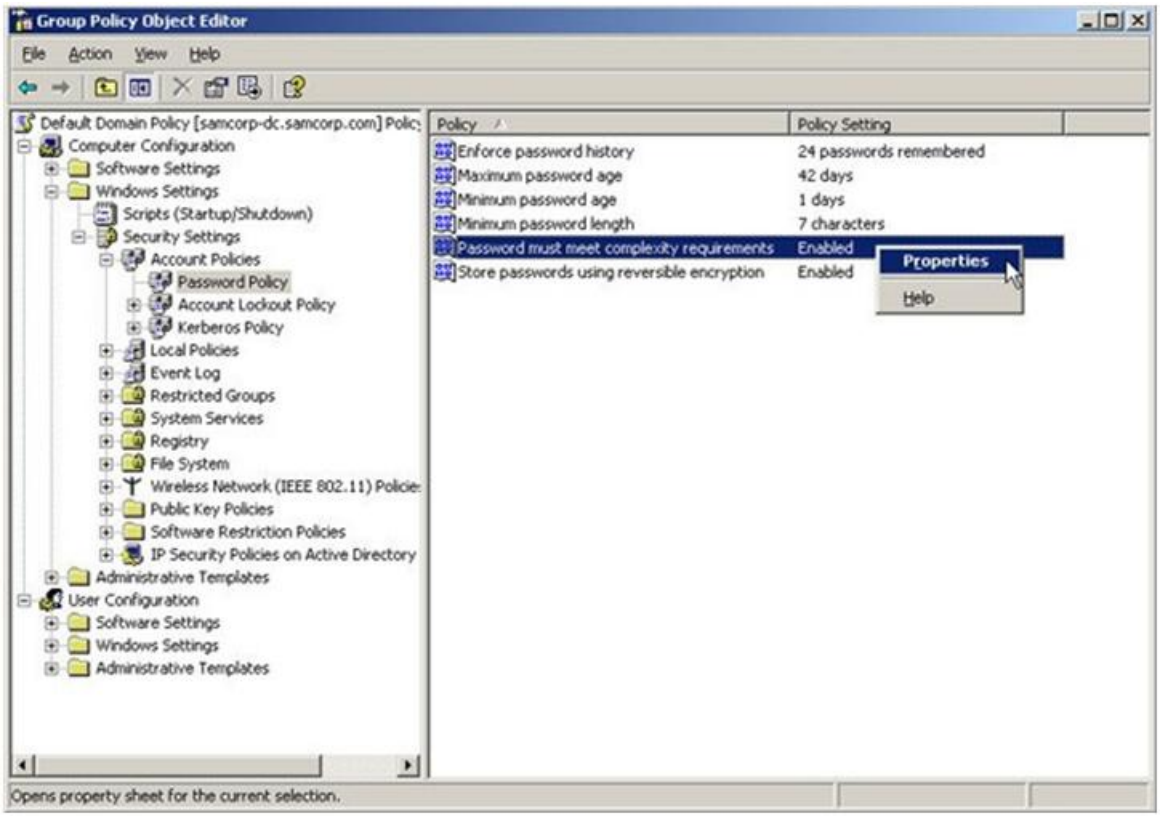
In addition to adding the MAC address as the username and password, you will need to adjust the password policy requirements for the domain. When Windows 20003 Enterprise Server Active Directory is installed, it has a set of policies for user passwords, and one of these can be that the password must meet complexity requirements. Unfortunately, with MAC authentication you need to turn off complexity requirements for passwords. This reduces the security of your passwords by disabling any password restrictions other than password length, password history, and password age.

The following steps explain how to add a new MAC-authenticated user, configure passwords, and add the user to a restricted group.

6.1 Modify the password policy

To allow MAC authentication you need to first modify the password policy in Active Directory:

1. Open the Users and Computers Manager (Start | Administrative Tools | Active Directory Users and Computers).
2. Right−click on your domain and select Properties.
3. Select the Group Policy tab and press the Edit button.
4. Under the Computer Configuration tree, open the Windows Settings folder.
5. Open the Security Settings tree.
6. Open the Account Policies tree.
7. Click on Password Policy. You see the Group Policy Object Editor.



8. Right−click on Password must meet complexity requirements in the Policy pane and select Properties.
9. Select the Disabled radio button and click the OK button.
10. Press Alt−F4 to close the Group Policy Object Editor.
11. At the domain Properties window, select the OK button.

6.2 Manually update Group Policy

Now you force Windows Active Directory to update Group Policy.

1. Open a command prompt window (Start | Run, type cmd and press OK).

2. At the command prompt type gpupdate and hit Return.

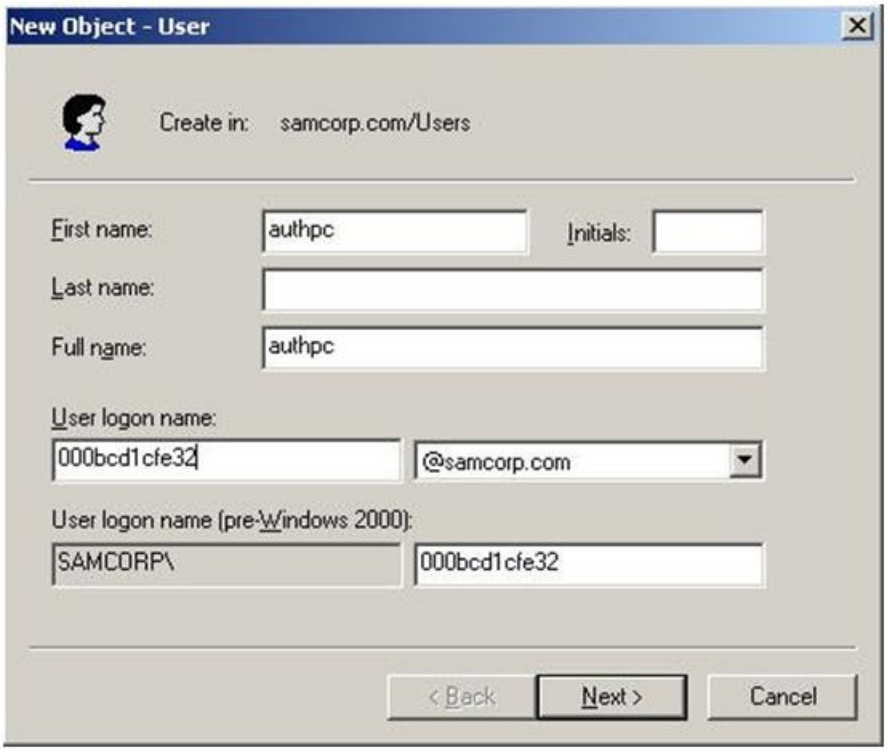
3. At the command prompt type exit and hit Return to close the command window.

6.3 Add the new MAC user

Now you can add the new MAC user to Windows Active Directory:

1. Under the domain, Select the Users organizational unit.

2. In the toolbar, click on the New User icon to create a new user. You see the first page of the New Object - User wizard.



3. In the New Object - User first page:
   - Enter the machine name (for example, authpc) in the First Name field.
   - Enter the machine's MAC address in the User logon name field.

   Then click the Next button. You see the second page of the New Object - User wizard.

4. In the second page:
   - Deselect the User must change password at next logon check box.
   - Check the Password never expires check box.
   - Enter the MAC Address of the client (for example, 000bcd1cfe32) in the Password and Confirm password text boxes.

   Then click the Next button.

5. Click the Finish button.

6.4 Create a new group for the user

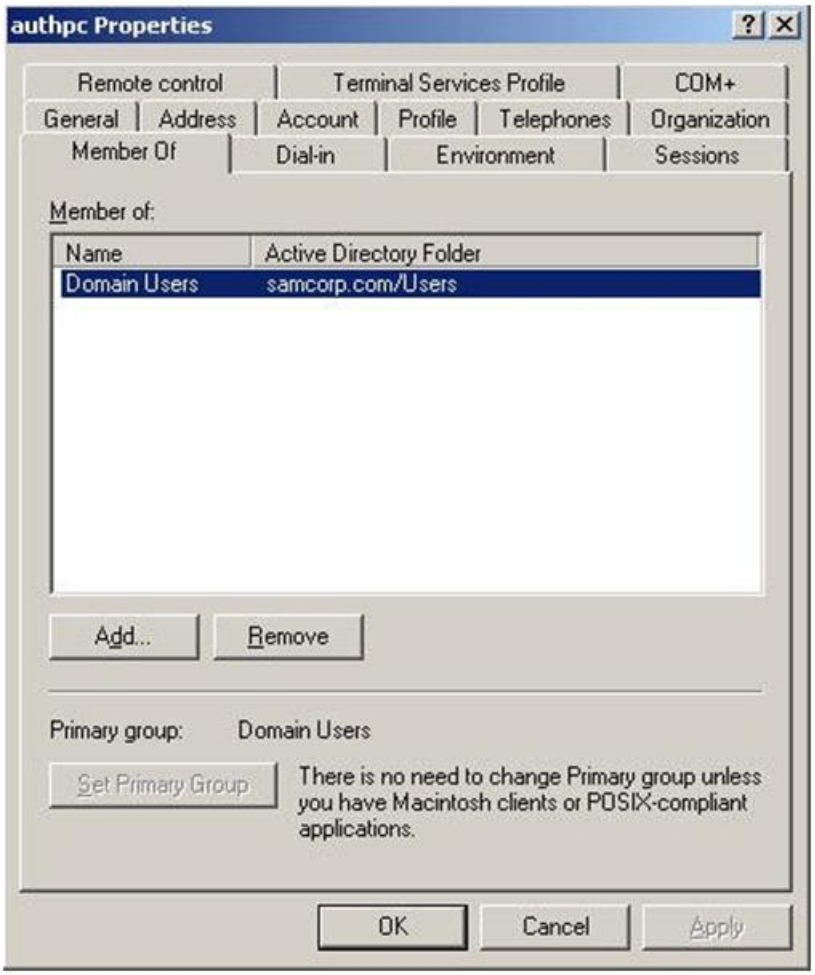
Next, you create a new restricted group:

1. Click on the New Group icon in the toolbar to create a new group.

2. Enter Restricted Users in the Group name field. In addition:
   - Make sure Global is chosen for the Group scope.
   - Make sure Security is chosen for the Group type.

   Then click the OK button.

3. Double-click on the user you just created (authpc) to see the Properties tabs for this user, and select the Member Of tab.



4. Select the Add button.

5. In the Enter the object names to select, type Authorized Users and press the Check Names button.

6. Select the OK button.

7. Click once on the Authorized Users group and select the Set Primary Group button.

8. Highlight Domain Users in the Member of list and select the Remove button. This step removes the user from the Domain Users group.

9. Select Yes to the Remove user from group message box.

10. Select the Account tab, and select the Store password using reversible encryption check box in the Account options scroll box.

11. Select the Dial−In tab, and select the Allow access radio button in the Remote Access Permission (Dial−in or VPN) group box.

12. Select the OK button to save your changes.

Remember to add the Authorized Users group to all resources you want this machine to have access to.

7. Reference documents

This concludes the procedure for configuring MAC authentication.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
  http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

- For PCM+ and IDM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm

For further information, please visit www.procurve.eu

4AA2-1530EEE, July 2008