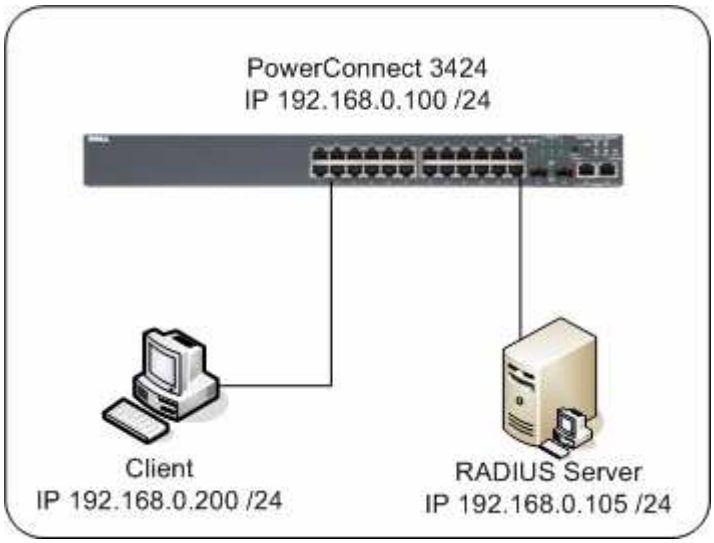
# Configuring RADIUS authentication on a PowerConnect 3424 using Microsoft Internet Authentication Server

Written by: Greg Gibbs
9/30/2005

The configuration listed in this document is based on the following topology:




**Step 1 – Configuring the switch (from defaults)**

Configure the IP address for VLAN 1:

*console# config*
*console(config)# interface vlan 1*
*console(config-if)# ip address 192.168.0.100 /24*

Configure a local user named user1 with password user1 and level 15 privilege:

*console(config)# username user1 password user1 level 15*

Define the RADIUS server and specify the shared secret key "mysecretkey"

*console(config)# radius-server host 192.168.0.105*
*console(config)# radius-server key mysecretkey*

Create an authentication method called radius_local that will attempt to authenticate via RADIUS, then use the local database if communication to the radius server cannot be established:

*console(config)# aaa authentication login radius_local radius local*

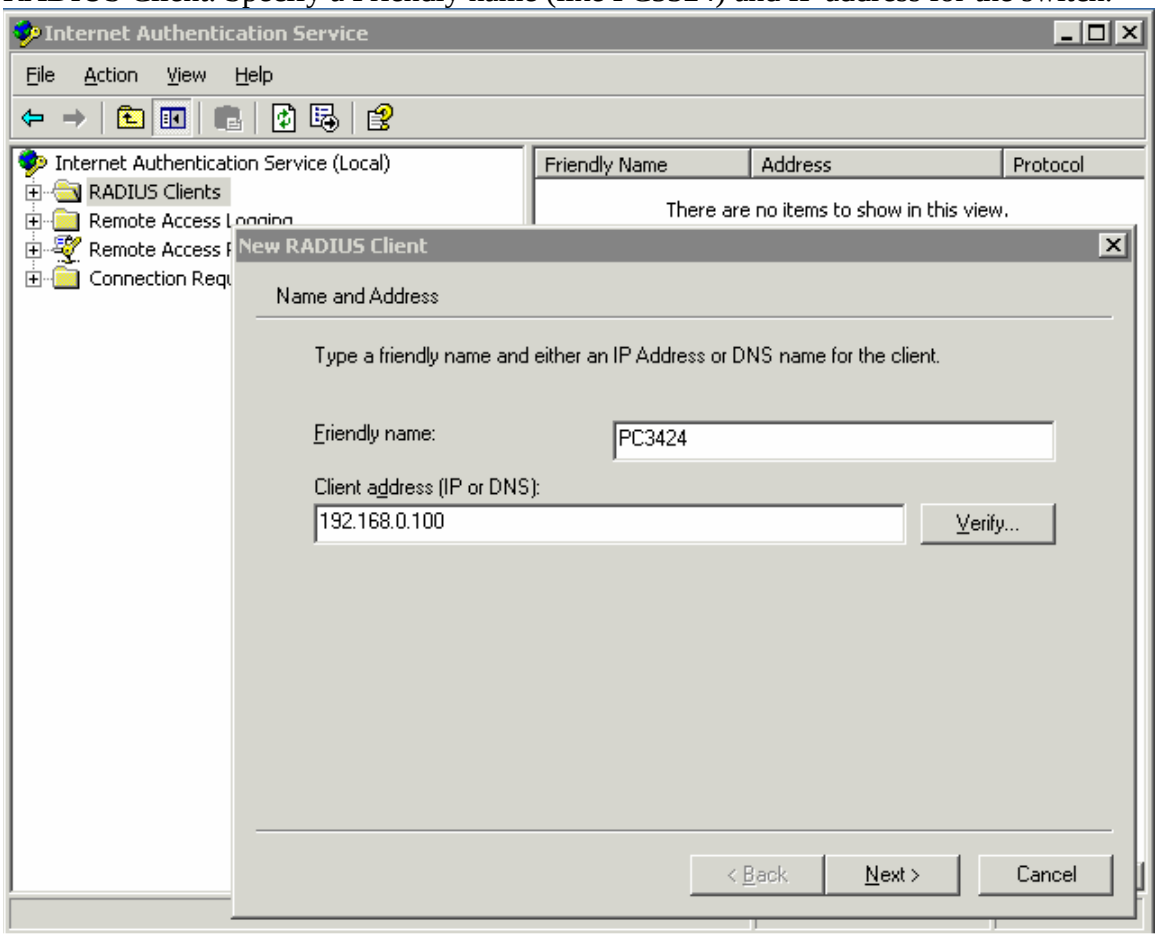
Bind this authentication method list to the telnet line:

*console(config)# line telnet*
*console(config-line)# login authentication radius_local*

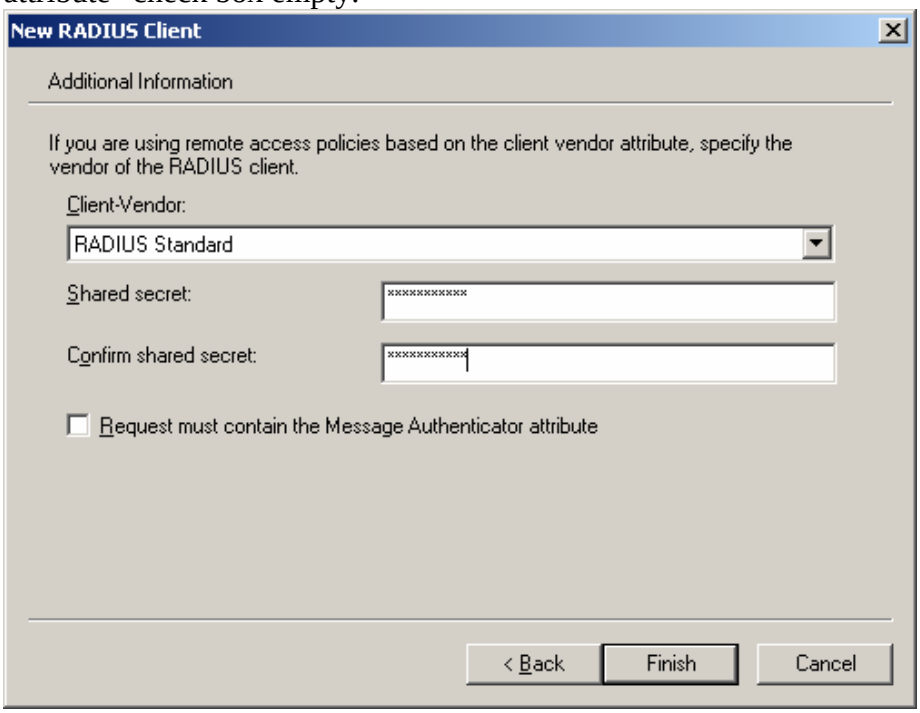
**Step 2 – Installing and Configuring the RADIUS server for Windows Server 2003**

Install the Internet Authentication Service. To do so, open the Add or Remove Programs applet and select Add/Remove Windows Components. Highlight the Networking Services option and click the Details button. Check the box for Internet Authentication Service.

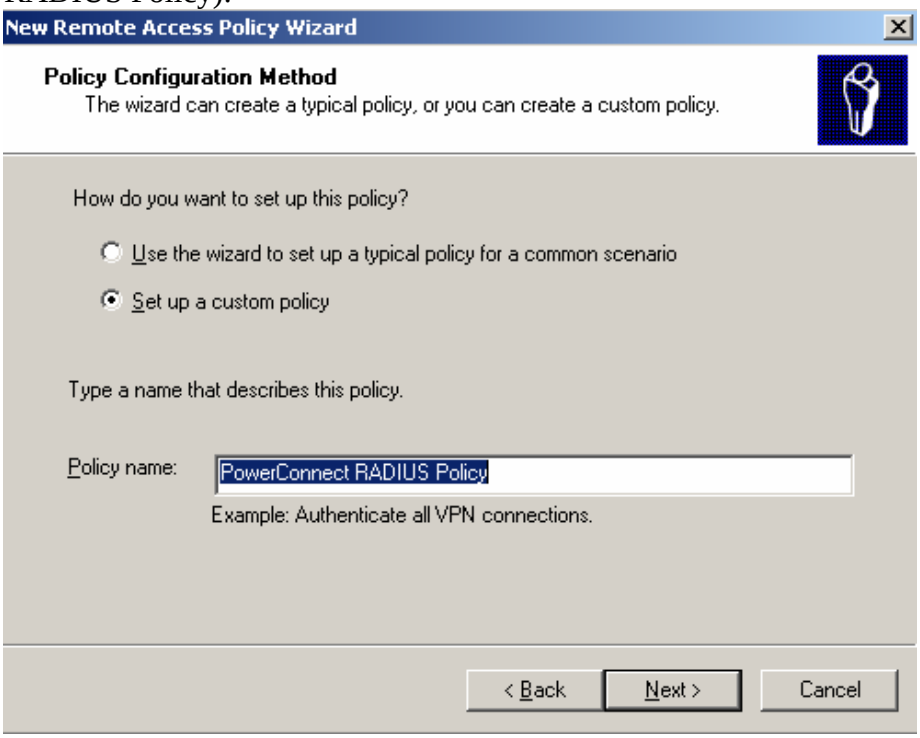
From the IAS snap-in window, Highlight the RADIUS Clients section and select New RADIUS Client. Specify a Friendly name (like PC5324) and IP address for the switch.



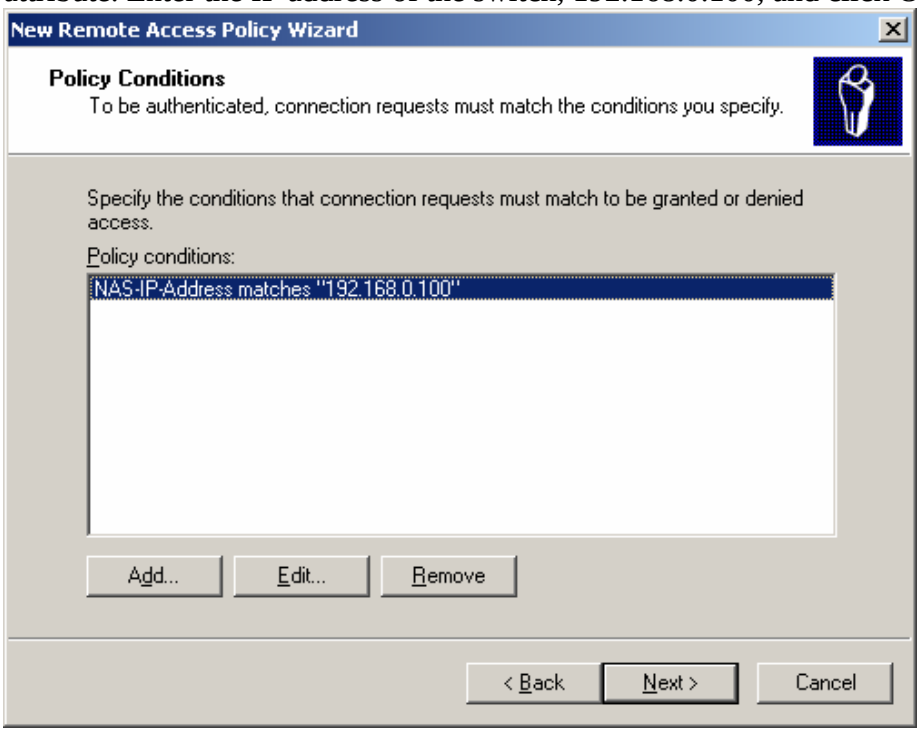
Select RADIUS Standard from the Client-Vendor drop-down box and enter mysecretkey for the Shared secret. Leave the “Request must contain the Message Authenticator attribute” check box empty.




Highlight the Remote Access Policies option and select New Remote Access Policy. Choose the option to Set up a custom policy and give it a name (ex. PowerConnect RADIUS Policy).



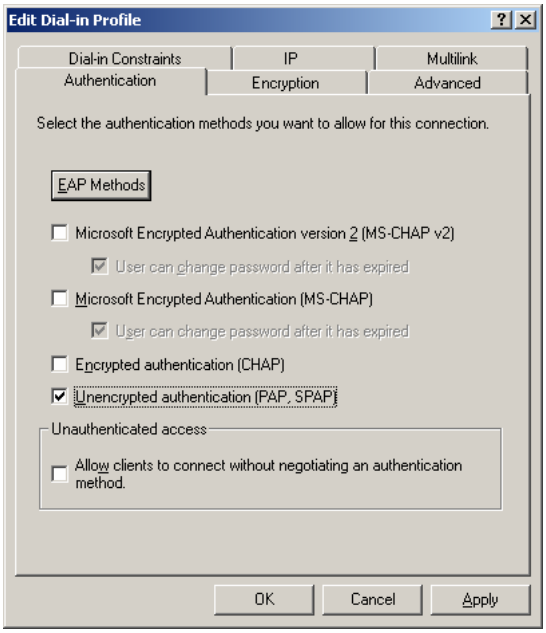
On the Policy Conditions page, click the Add button and select the NAS-IP-Address attribute. Enter the IP address of the switch, 192.168.0.100, and click OK.



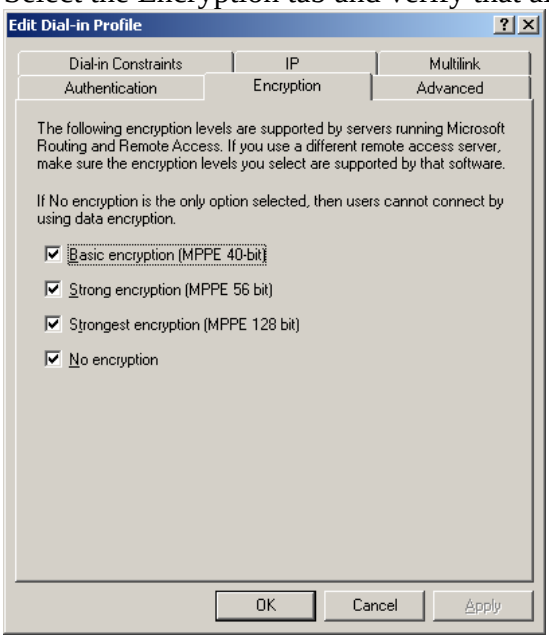

**Note: Other Policy Conditions can be used. The NAS-IP-Address attribute is used in this example for simplicity

On the Permissions page, select the radio button for Grant remote access permission

On the Profile page, select Edit Profile. Select the Authentication tab. Check the Unencrypted authentication (PAP, SPAP) option and remove all other authentication methods.

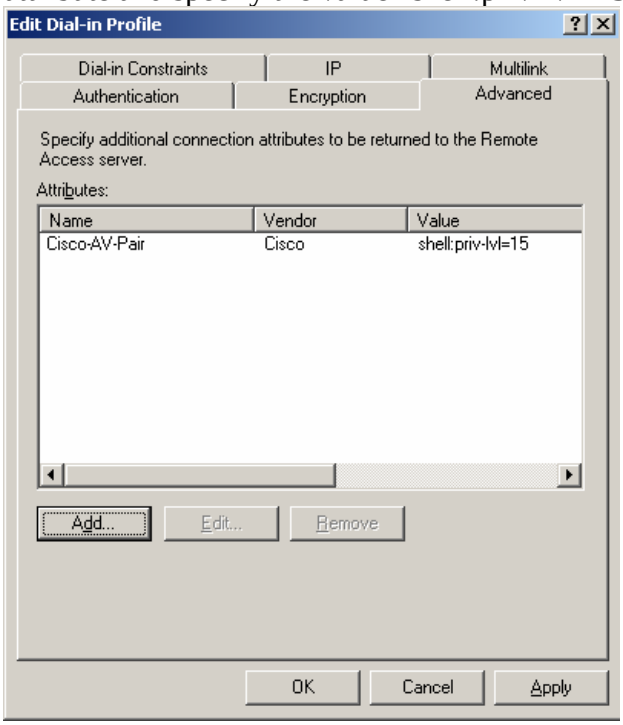


Select the Encryption tab and verify that all encryption options are checked:




**Note: If all options are not checked, IAS will send MPPE attributes {MS MPPE Encryption Policy (7) & MS MPPE Encryption Type (8)} in the RADIUS Accept message. PowerConnect switches prior to the 3400 series may not recognize these attributes and may disconnect the session.

Select the Advanced tab and remove all default attributes. Add the Cisco-AV-Pair attribute and specify the value “shell:priv-lvl=15”.




**Note: For a user with admin level access, use priv-lvl=15. For a user with guest level access, use priv-lvl=1

Finally, telnet from the client to the switch using the credentials of a valid user configured on the server.

You can use Ethereal to sniff traffic and look at the authentication process. Ethereal can be downloaded from the following link: http://www.ethereal.com

A successful authentication capture will show the following: