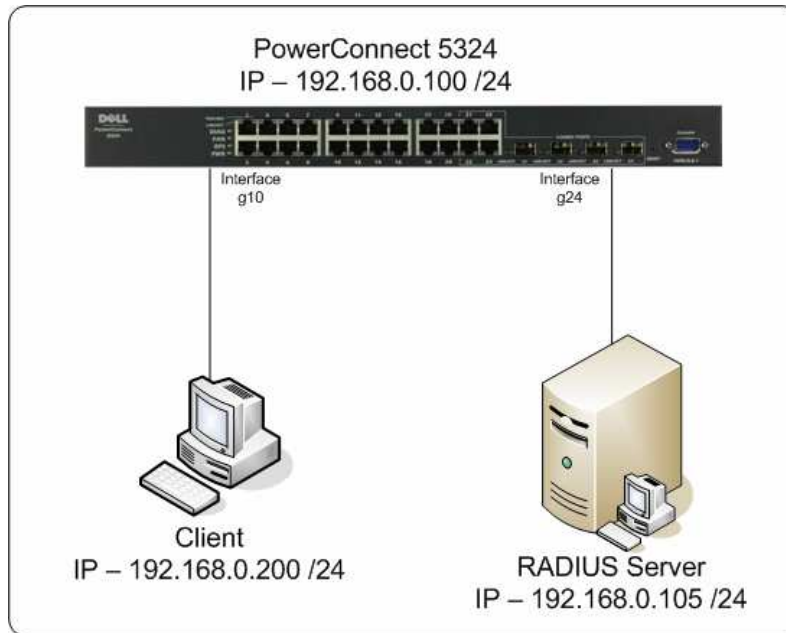


Configuring 802.1x authentication on a PowerConnect 5324 using the Aegis client and Steel Belted Radius

Written by: Greg Gibbs 12/2/2004

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
```

Enable 802.1x globally:

```
console(config)# dot1x system-auth-control
```

Configure the default authentication for dot1x to use the RADIUS server:

```
console(config)# aaa authentication dot1x default radius
```

Set the authorization state of the client port to auto:
console(config)# interface ethernet g10
console(config-if)# dot1x port-control auto

Step 2 – Installing and Configuring the RADIUS server

Install Steel Belted Radius. A demo version can be downloaded from Funk Software at the following link:

http://www.funk.com/radius/enterprise/enterprise_radius.asp

**EAP is not enabled on the RADIUS server by default. To enable the proper EAP support, you must edit the %ROOT\Radius\Service\eap.ini file. Under the [Native-user] section, uncomment (remove the preceding semicolon) the following lines:

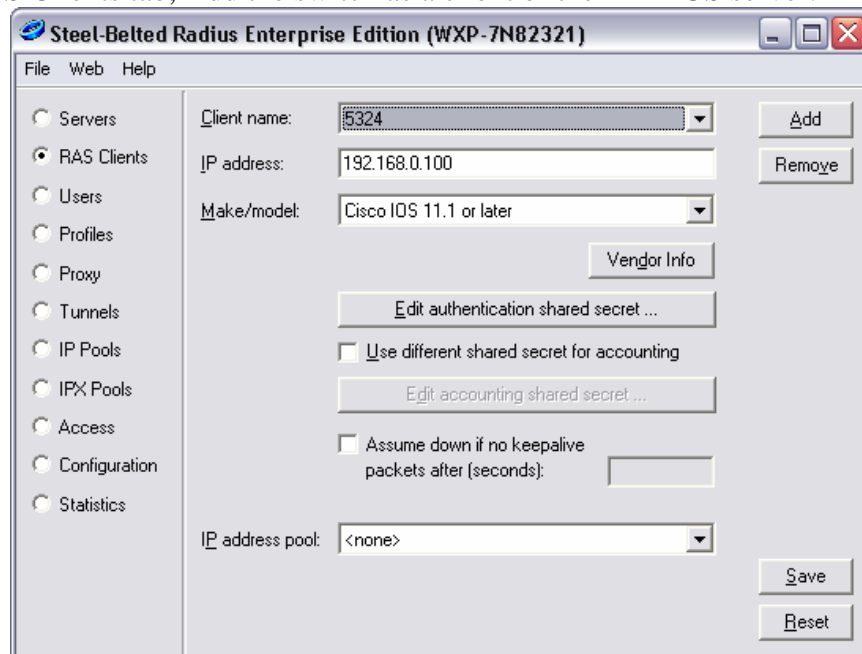
EAP-Only = 0
EAP-Type = MD5-Challenge
First-Handle-via-Auto-EAP = 1

Save the changes to the file. Open the Windows Services snap-in and restart the Steel-Belted Radius service.

Verify that the Local radio button is selected and click the Connect button.

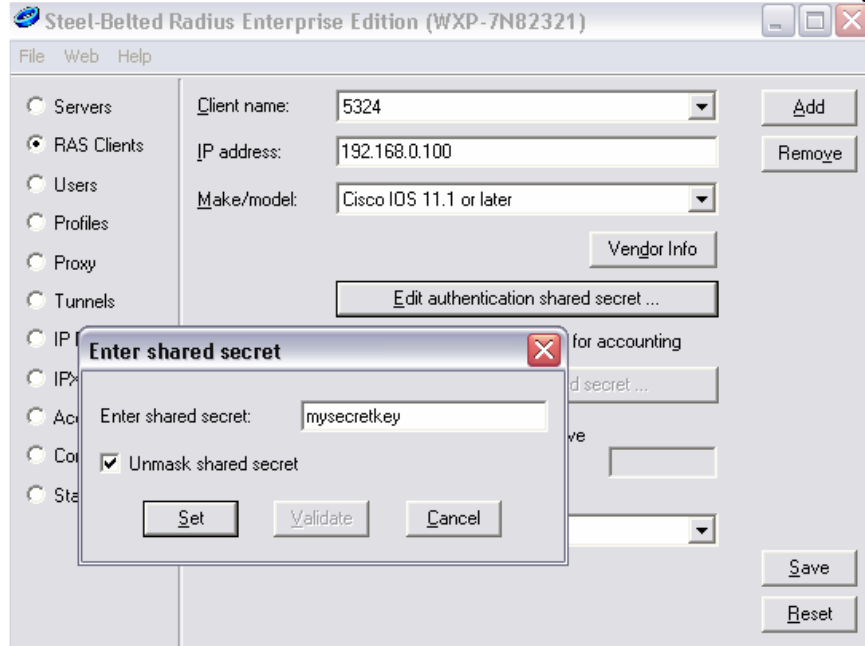
**Note: The PowerConnect 5324 only support EAP using MD5 Challenges. The use of Digital Certificates is not supported.

On the RAS Clients tab, Add the switch as a client of the RADIUS server:



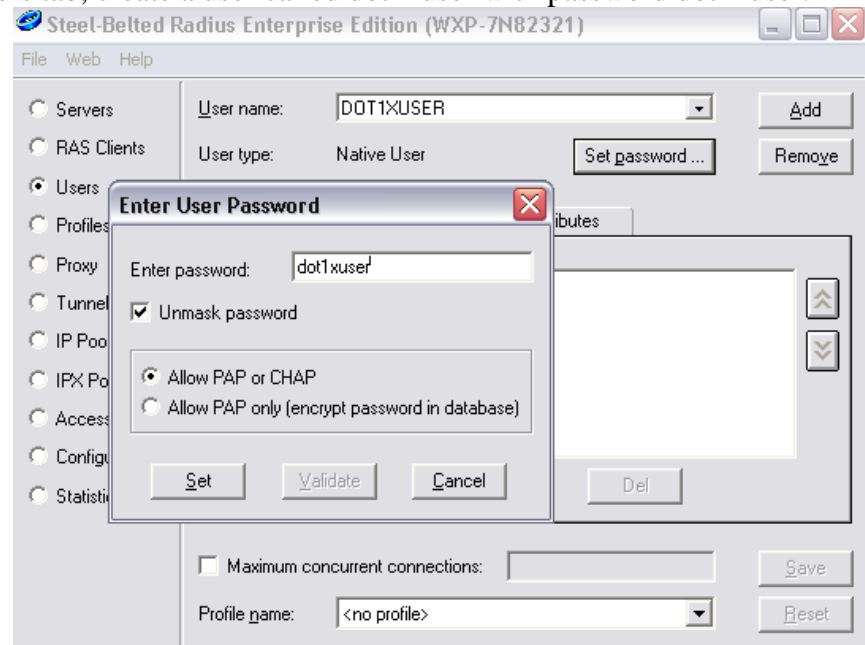
** Note: Be sure the Make/model is configured for Cisco IOS **

Click the Edit authentication shared secret button to enter the shared secret key:



Save the RAS Client configuration

On the Users tab, create a user called dot1xuser with password dot1xuser.



Verify that the Check list attributes and Return list attributes tabs are blank.

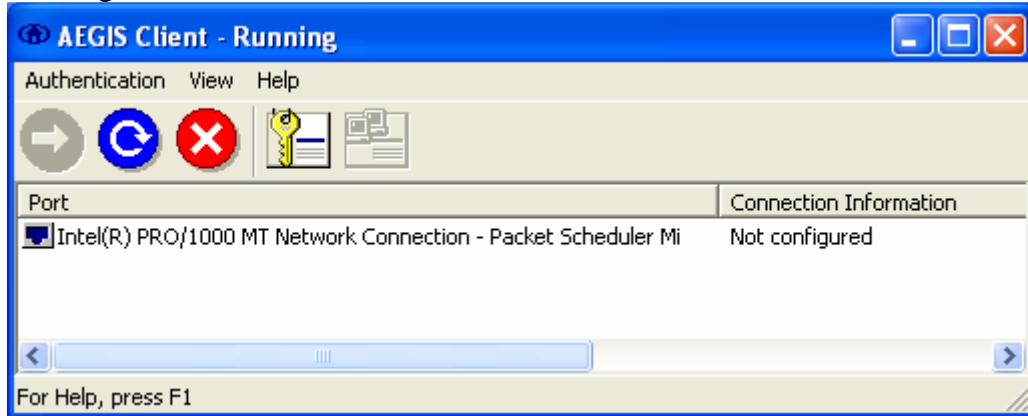
Save the changes to the Users tab.

Step 3 – Installing and Configuring the Aegis client

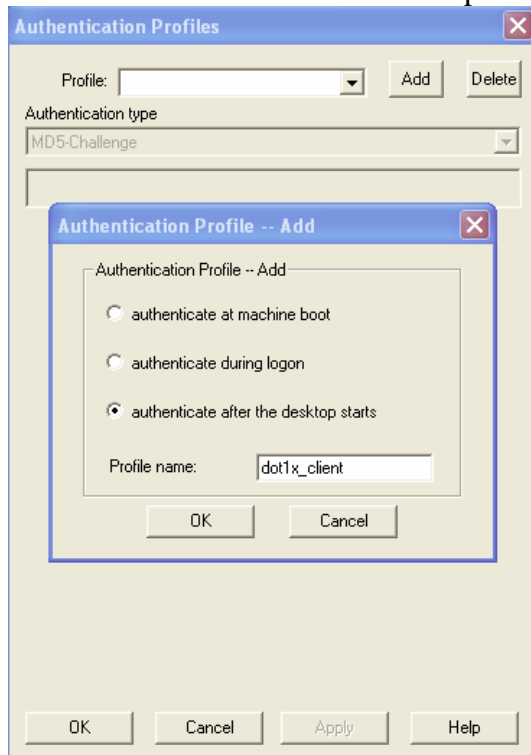
Install the Aegis client. A demo version can be downloaded from Meetinghouse Data Communications at the following link:

<http://www.mtghouse.com/products/aegisclient/index.shtml>

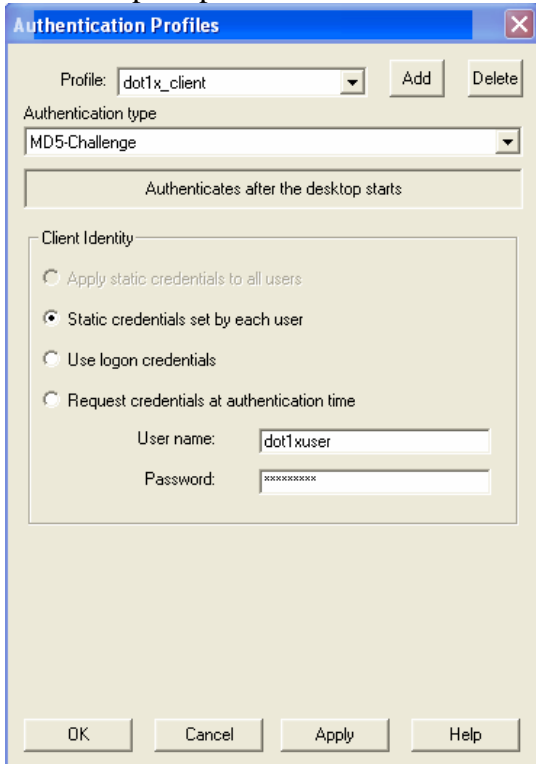
Start the Aegis client:



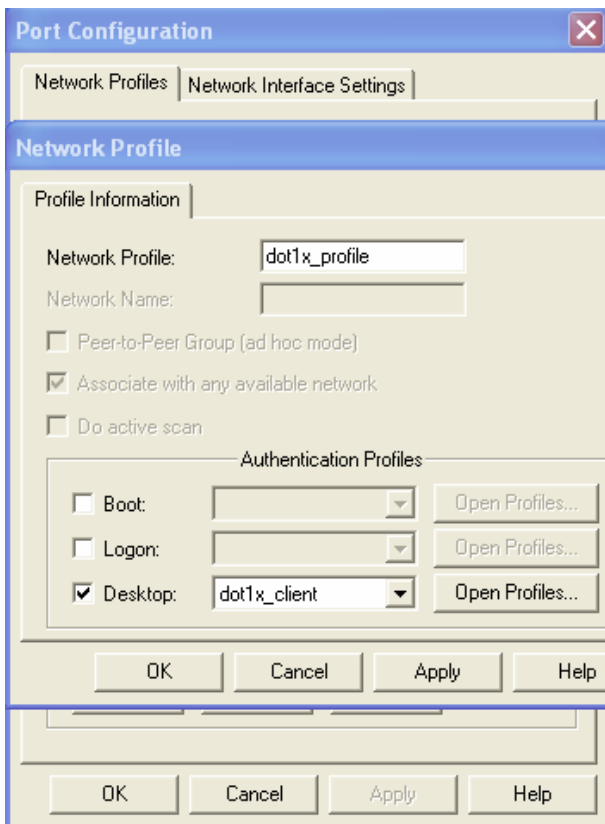
Select the Authentication Profiles option and add a new profile called dot1x_client:



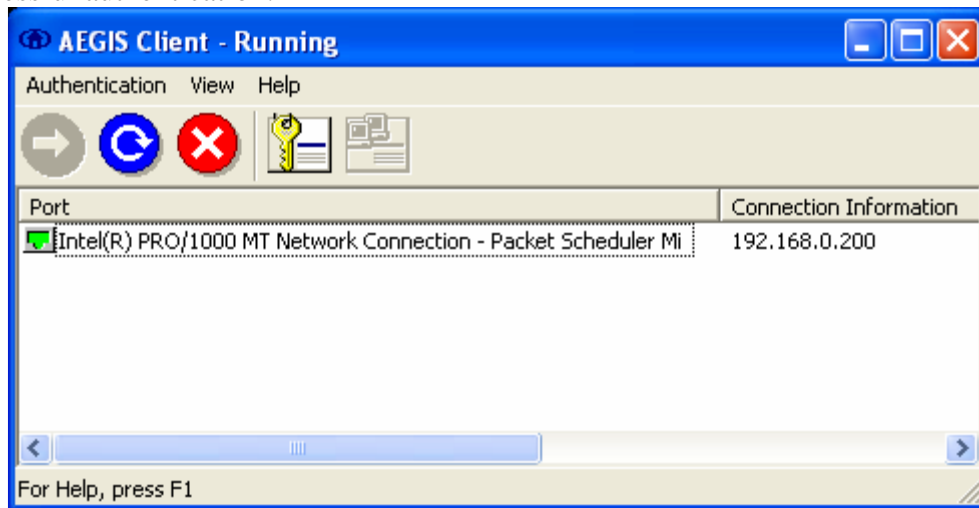
Verify that the Authentication type is configured for MD5-Challenge. For this example, we are using static authentication credentials. You can also use logon credentials or have the client prompt for authentication:



Highlight the network adapter, and click the Network profiles toolbar button. Add a network profile called dot1x_profile, select the Desktop check box, and select the dot1x_client profile from the dropdown:



Restart or Stop/Start the Aegis client. If everything is configured properly, you should get a successful authentication:



Once the port is authenticated, the client should be able to communicate with the rest of the network.

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:

