# Quick Configuration Guide
# Configuring 802.1X in AOS

## Introduction

802.1X authentication allows for the capability to restrict access based on different parameters. 802.1X authentication can authenticate users on a port basis or restrict access down to the MAC Address of a device.

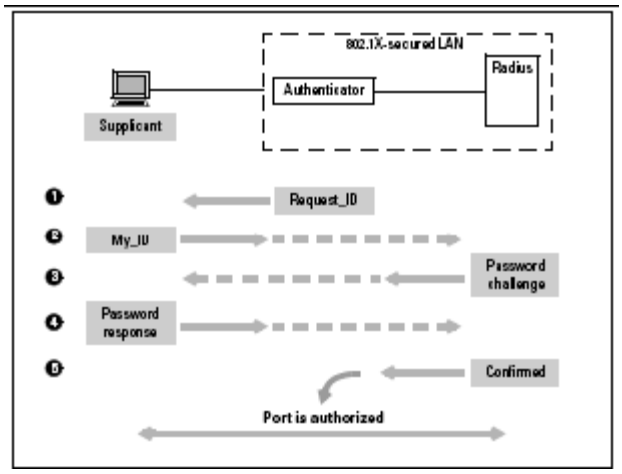
There are four parts in an 802.1X authentication connection:
• Authentication requirements
• The supplicant
• The authenticator
• The authentication server

The authentication requirements can range from a simple username and password challenge handshake to extended requirements using the extensible authentication protocol (EAP). EAP is an authentication protocol that supports multiple authentication methods, as explained in the next section. The supplicant is a client that is requesting access to the network. This client begins by establishing a limited Ethernet connection to the network.

When the authenticator detects the new connection, it begins the process of authenticating the supplicant. The authenticator uses the authentication requirements to dictate the requirements that the supplicant must satisfy. The authenticator uses an authentication server to verify the supplicant device. This is often a RADIUS server. The authenticator acts as a go-between while the RADIUS server and the supplicant negotiate authentication.

The authenticator, authentication server, and supplicant negotiate until the requirements for port access are met or denied. The RADIUS server is used to verify the supplicant device's username and password. When the supplicant has fulfilled the authentication requirements, the network port is opened, and the authenticator assigns the client an IP address. If the supplicant is unable to fulfill the authentication requirements, it is either sent to a restricted-access Virtual LAN (VLAN) or its connection to the network is severed.

The figure below shows the process of an 802.1X client supplicating the authenticator for network access.




There are several different types of authentication procedures. Often a network will only require authentication of a supplicant's pre-shared username and password. However, 802.1X networks can also expand those authentication requirements using different forms of EAP. Some examples include:

• EAP-TLS, which requires the use of certificates to authenticate the supplicant
• Limited EAP (LEAP), which uses a pre-shared key and CHAP
• Protected EAP (PEAP), which uses a certificate to allow the RADIUS server to authenticate the supplicant and then establishes a secure link to exchange credentials

Besides requiring authentication, EAP may also include some policy requirements that specify the presence or absence of certain kinds of software on the supplicant device. These requirements often include the presence of antivirus and security software and appropriate software security patches. The EAP policy may also specify the absence of malware and viruses. The authentication methods are configured on the authenticator and the authentication server.

## Hardware/Software Requirements

802.1X Authentication Mode was added in AOS 10.01.00. The Supplicant Authentication Mode is available in the following AOS products: NetVanta 1224 Series, NetVanta 1335, and NetVanta 1355/6355. This feature was also added to the NetVanta 3448 in AOS Version 16.01.00

## CLI Configuration

For brevity, RADIUS will not be covered in depth in this section. Below is a sample RADIUS configuration that will enable AAA services and specify a RADIUS server:

```
Router(config)#aaa on
Router(config)#radius-server 10.100.13.240 key adtran
```

After specifying the radius server (10.100.13.240) that will authenticate 802.1x peers, it is now necessary to specify port-authentication to use Radius:

```
Router(config)#aaa authentication port-auth default group radius none
```

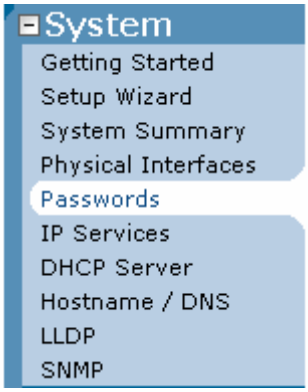
Once the AAA configuration has been completed, it is then necessary to configure each port for 802.1X. To enable 802.1X authentication on a port, use the following command from the Switchport Interface Configuration Mode Context:

Switch(config-swx 0/8)#port-auth port-control auto

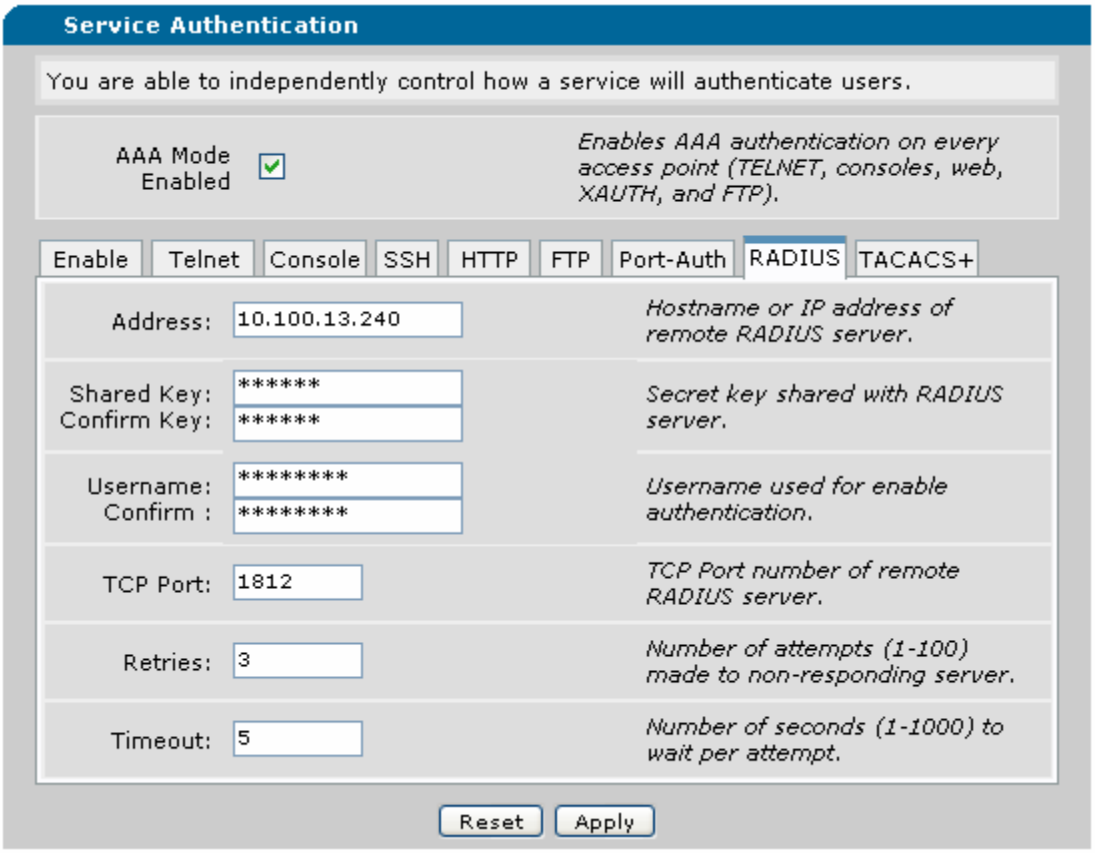
Once this is done, end units should now be authenticated using 802.1X.

## Web GUI Configuration

To use 802.1X, it is first important to configure the AAA service to run. To turn AAA on, go to the Passwords page as shown below:

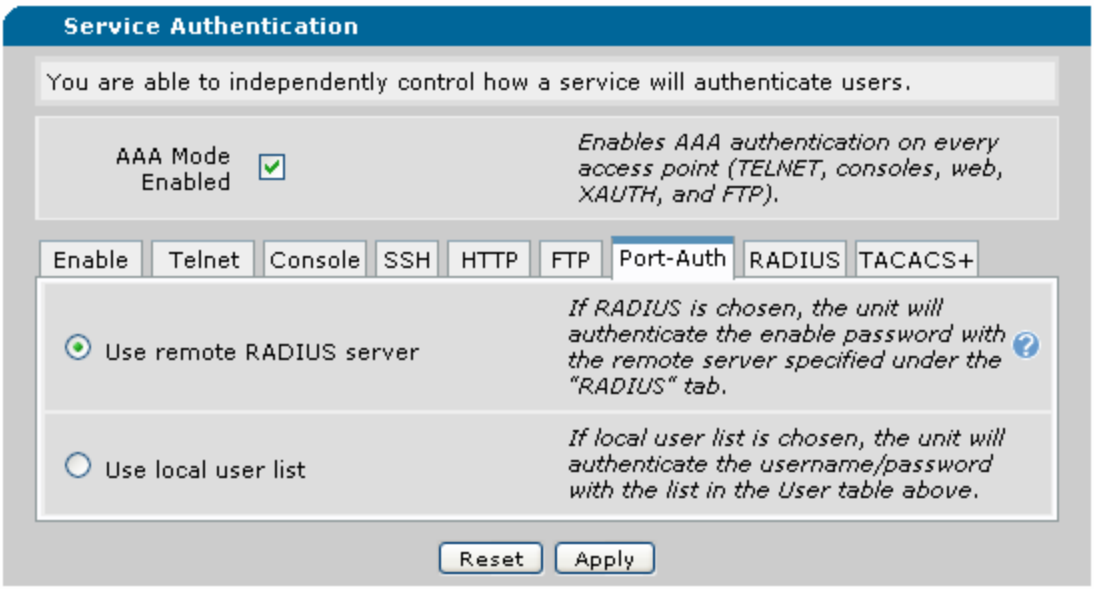



Turn on AAA Services by clicking the AAA Mode Enabled checkbox under Service Authentication.



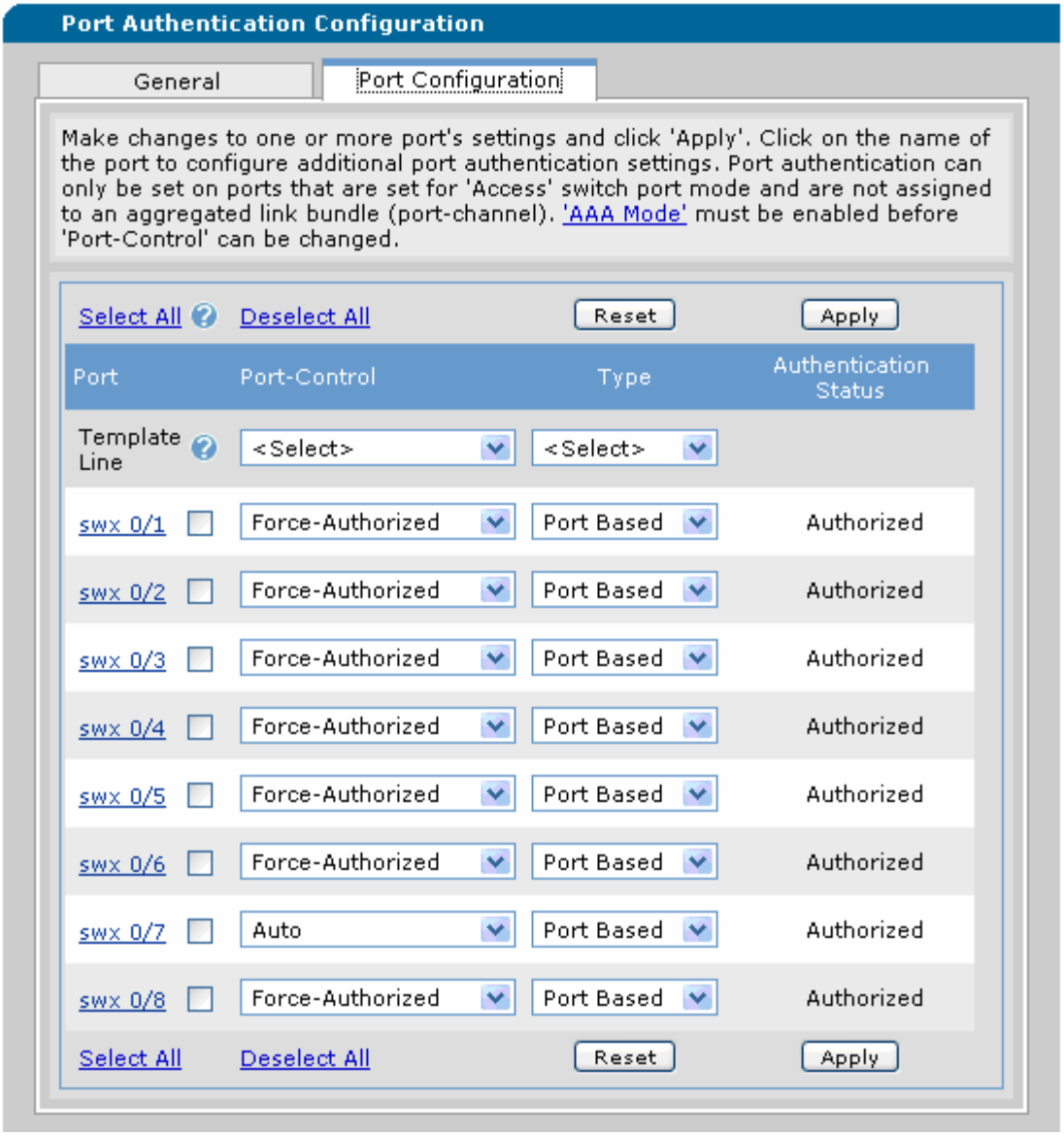

After enabling AAA, it is then necessary to configure a RADIUS server to authenticate to. To do this, click on the appropriate tab and list the KEY information as well as the Address where the given server was located. In this example, the 3448 sends credentials to a RADIUS server at 10.100.13.240. The key is a string that both the server and the NetVanta router much match in order for authentication to work properly. The Username below the Shared Key is shown, however is omitted since this refers to login credentials for the NetVanta router instead of network access. After setting configuring the Radius parameters, click Apply to commit the changes to the configuration.

Once a server has been configured, it is then necessary to configure the type of authentication. It is possible to configure the NetVanta router to use Local authentication, however, in most situations it is recommended to use Radius. After selecting “use remote RADIUS server, click Apply to commit changes to configuration. Below is an example of the Port-Auth tab and selecting Radius authentication.




Port Authentication (802.1X) can then be set. Click the Port Authentication tab under the Switch menu on the left-hand side of the page.


From this menu, navigate to the tab labeled Port Configurations to configure ports for 802.1X.



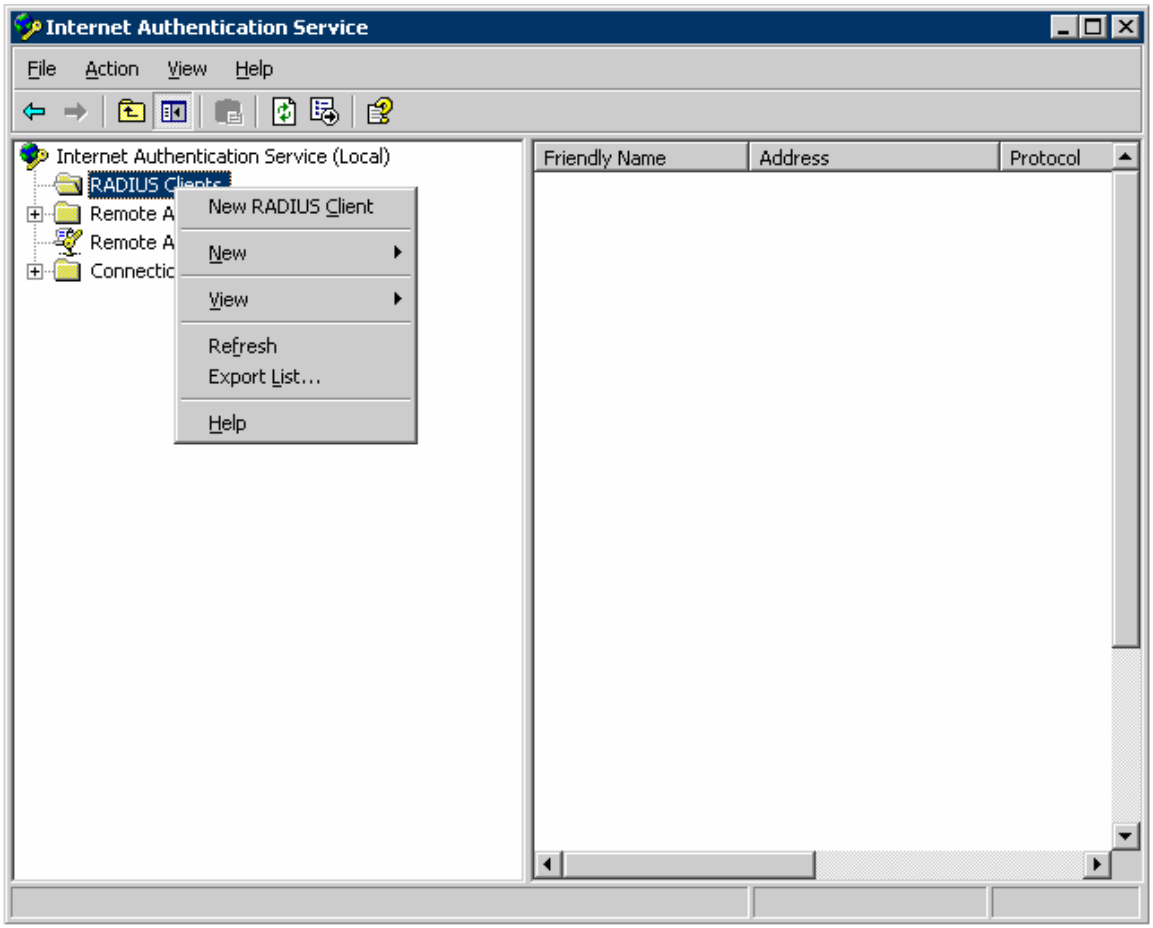

There are three different types of Port-Control. One is Force-Authorized (everyone gets access with no credentials), Force-Unauthorized (No one should be allowed to access port), and Auto (Use 802.1X authentication). It is also possible to select the Type of Port-Authentication. The two different selections are Port-Based (the port is open to traffic if Authorized) and MAC Based (the port is open for the specific MAC Address that is Authorized).

In the example above, the only port using port-auth is Switchport 0/7, this is shown because it is set to Auto which states that the port will only become authorized if it passes 802.1X authentication. After setting the ports for authentication, click Apply and the ports should be set for authentication.

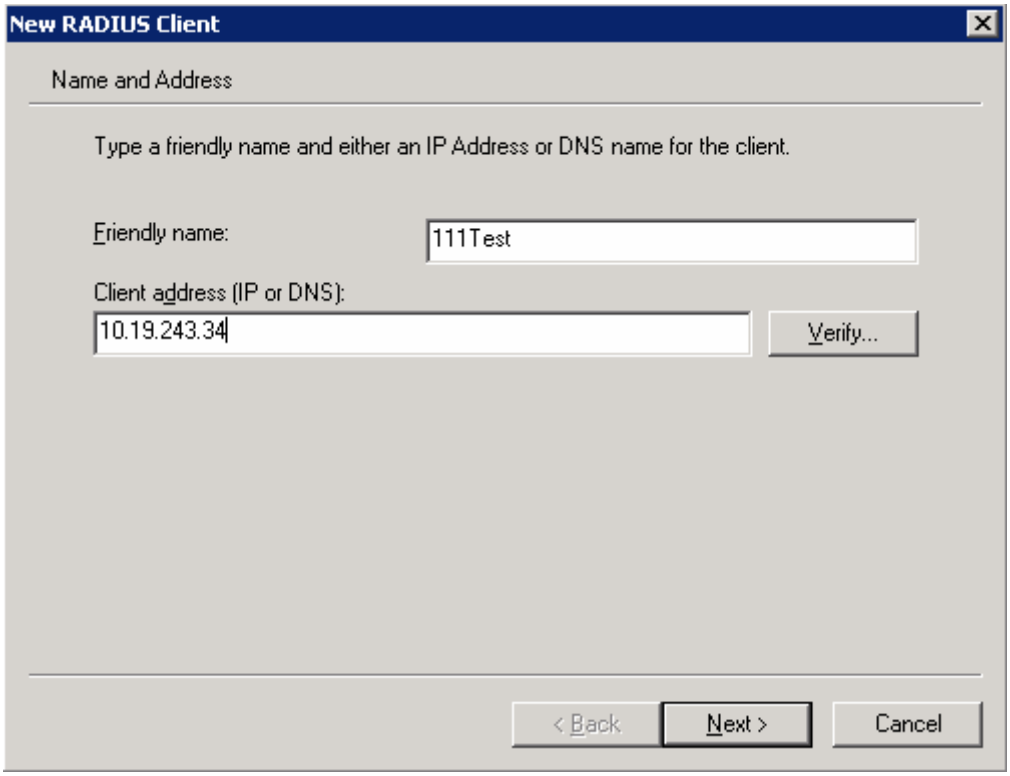
## RADIUS Server Configuration for Microsoft IAS

To configure RADIUS Authentication on a Microsoft Server using IAS, first, go to Control Panel and open the Internet Authentication Service and right click on RADIUS Clients. Go to New

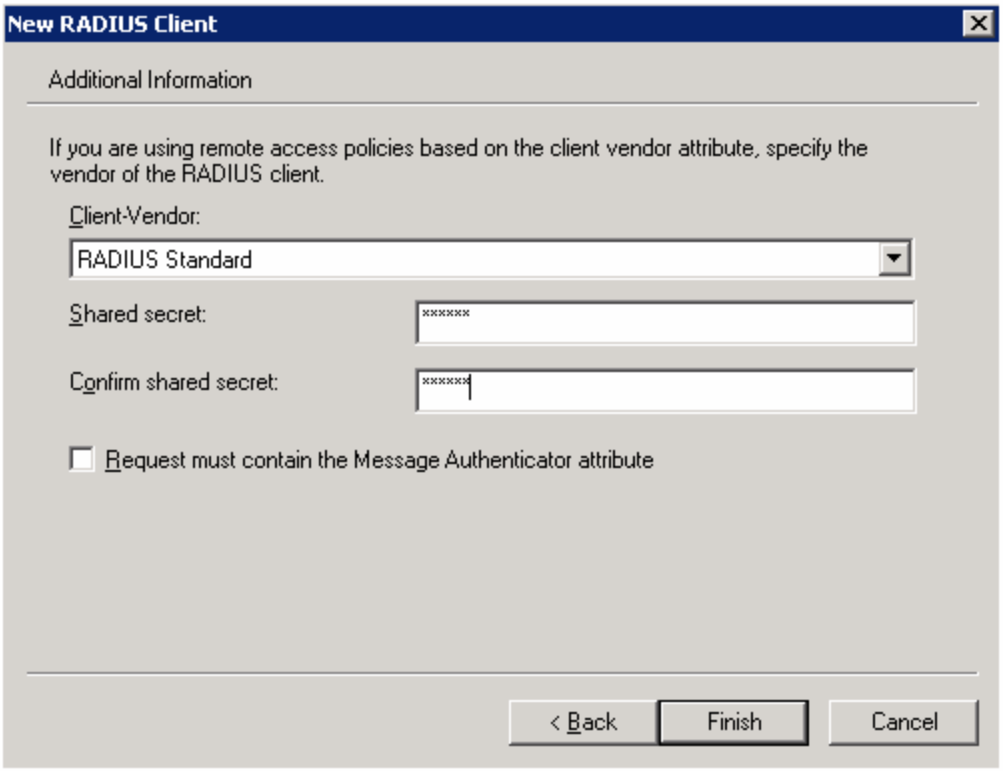
RADIUS Client to create a new client. Again, this is not a full tutorial on setting up IAS, this assumes RADIUS is already configured on the Server and only steps through what needs to be done for 802.1X Authentication to NetVanta.




On the next screen, create a useful Friendly Name for the Client (or the NetVanta Router) and also supply the IP address of the Client. In this situation, the IP address of the Router is 10.19.243.34.

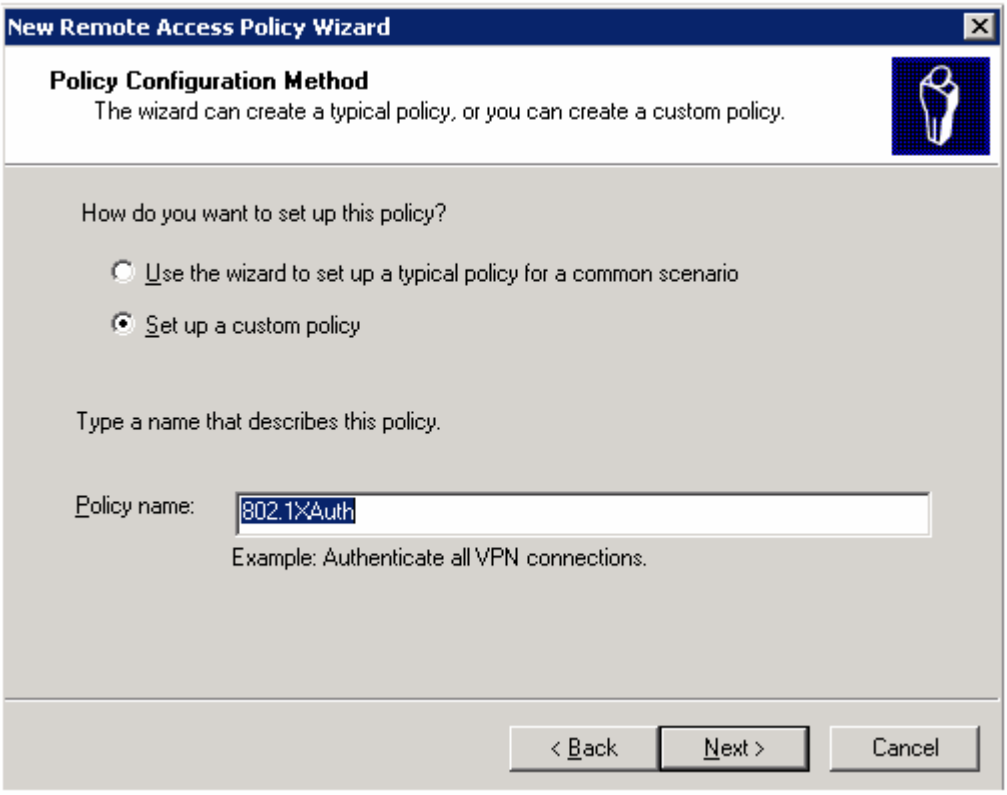



After setting the IP address, click Next. On the Next Screen, leave the Client/Vendor as RADIUS Standard. Set a Shared Secret (KEY) for the RADIUS Server. This should correspond with the Key set earlier on the NetVanta router for the RADIUS server.

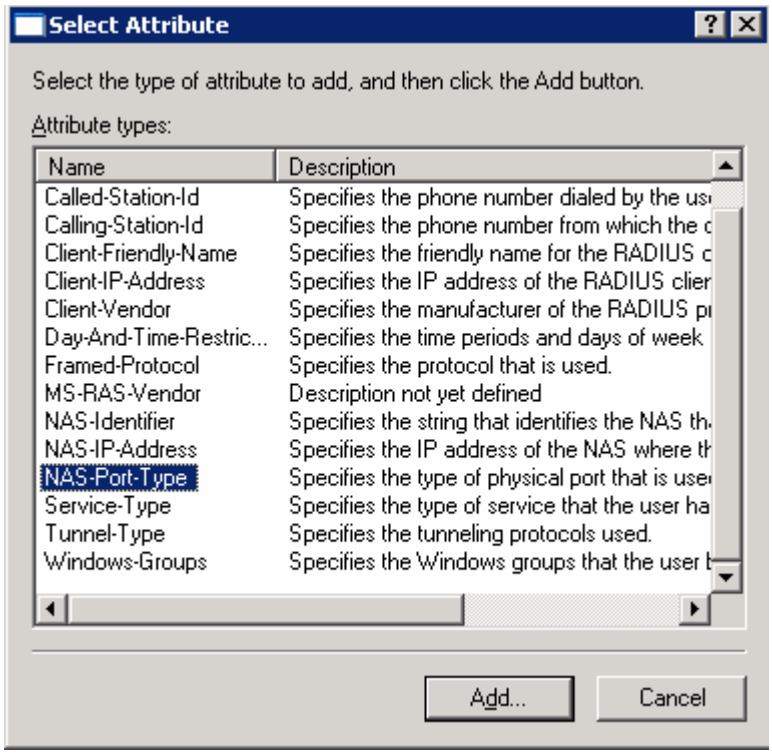



After setting the Shared secret, click Finish.

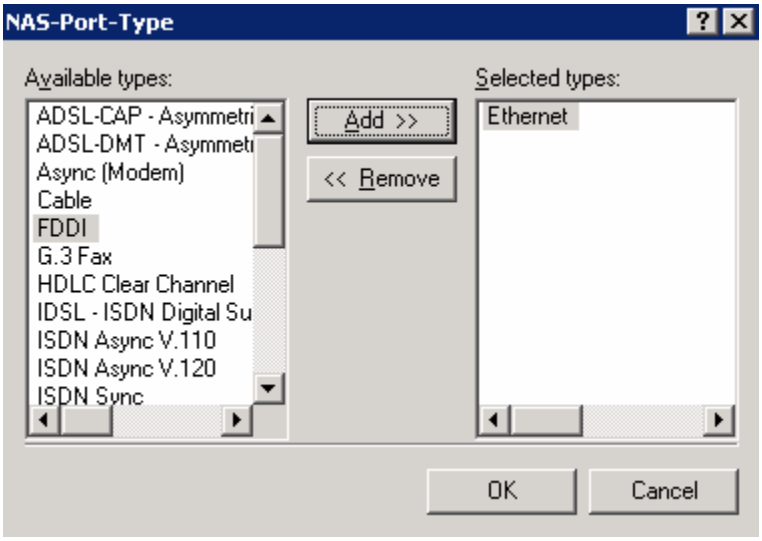
Once the Client has been configured, right click on Remote Access Policies and click on New Remote Access Policy. On the Wizard, name the Remote Access Policy and select Set Up Custom Policy from the Menu.



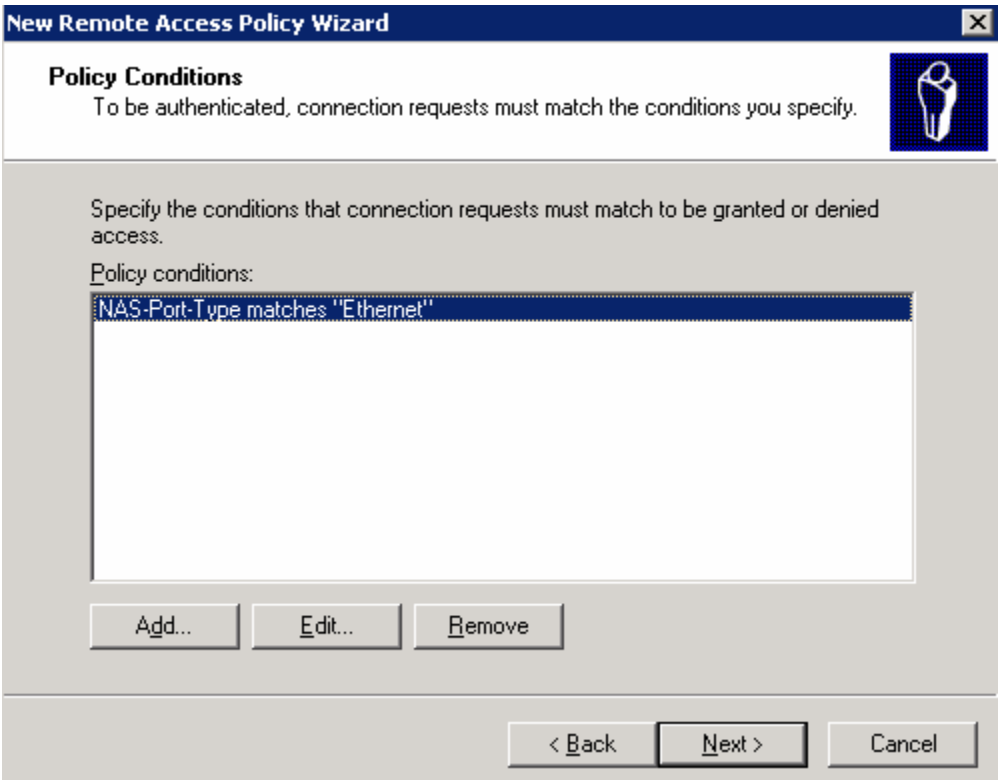

After clicking Next, select Add from the Policy Conditions. Although it is possible to select different criteria, this example will stay general. Click "Add" on the Policy Conditions. Under Attributes, select NAS-Port-Type and again click Add.



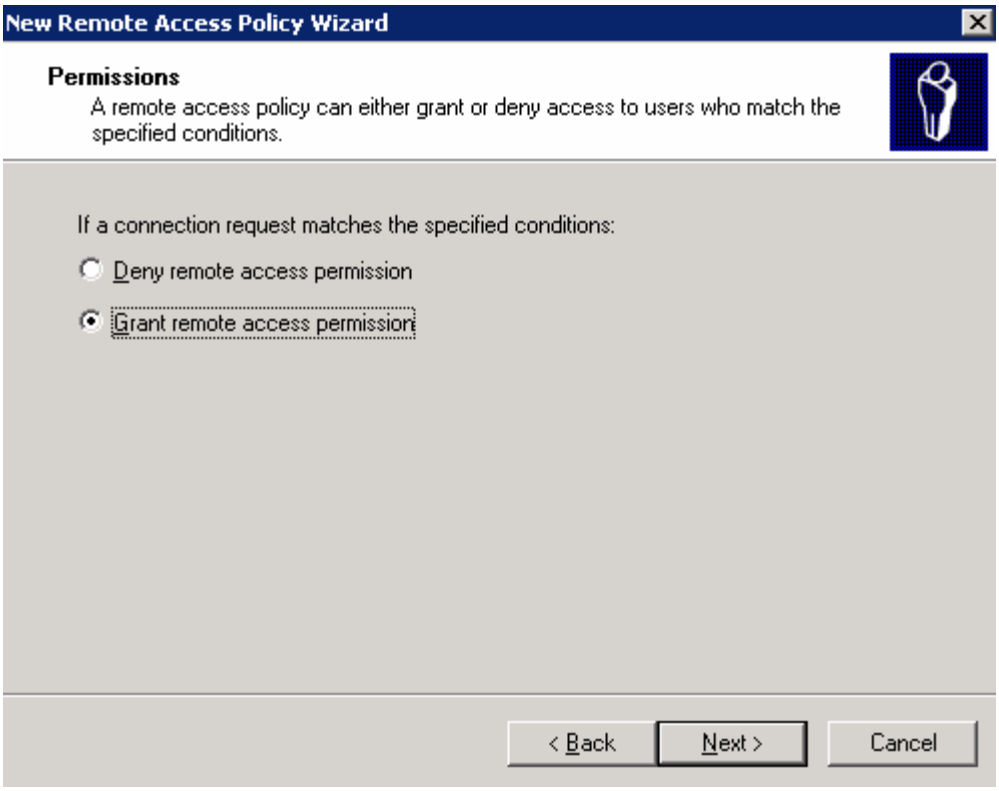
A large selection of NAS Port Types should appear. In this grouping, select Ethernet as that will be the Medium Authenticated:



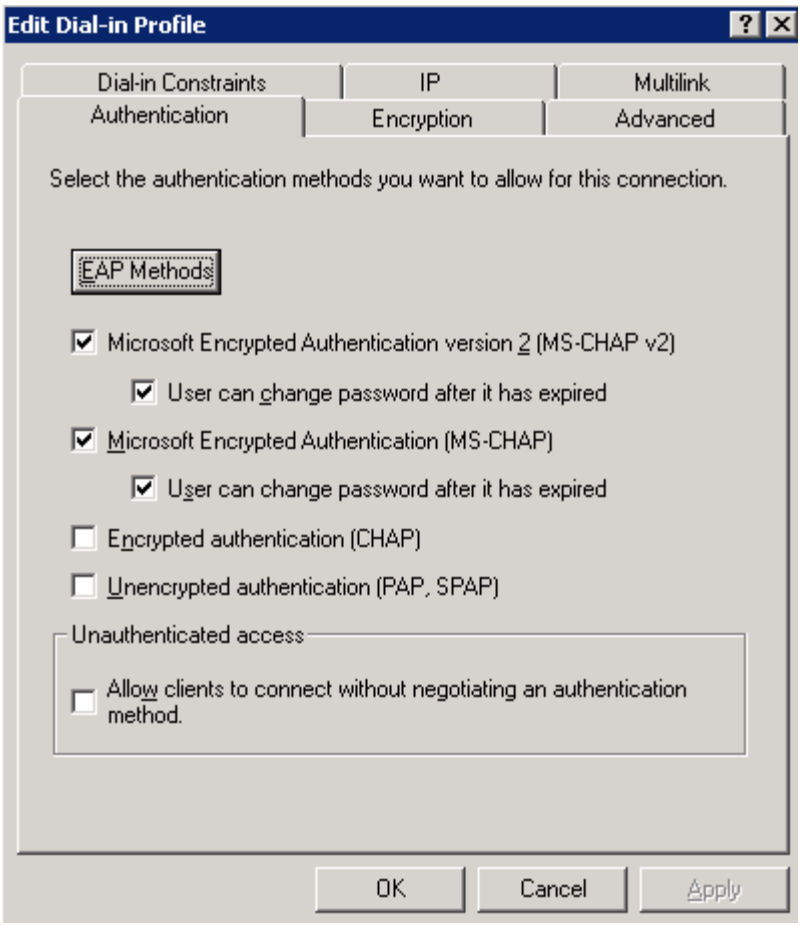

After selecting Ethernet, click Add. Once Ethernet has been Added as shown above, click OK. Once back to the Policy Conditions, it should now show what is displayed below. Click Next to move to the next part.



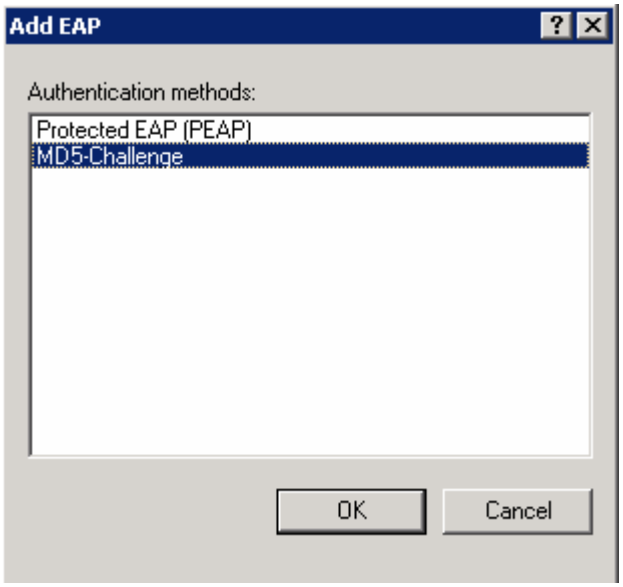

On the next screen, set the Policy to Grant remote access permission if matched and click Next as shown below:



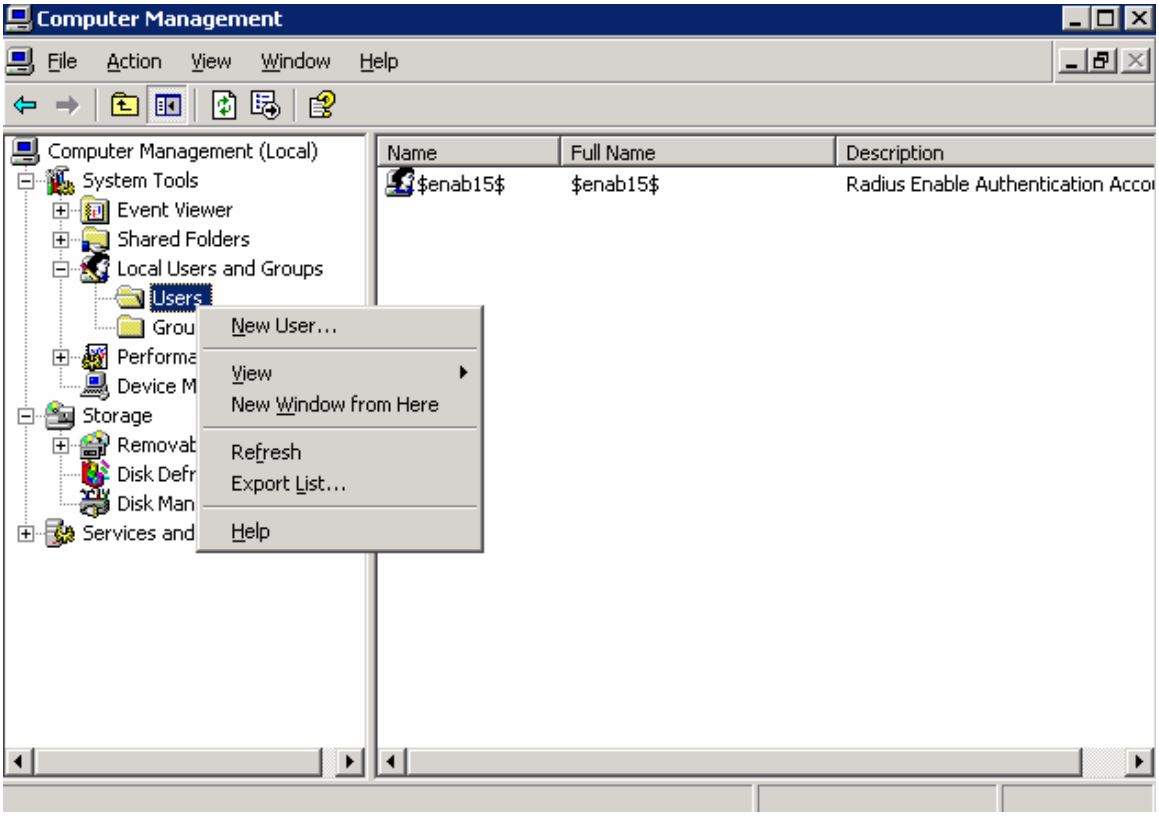

On the next screen, click Edit Profile and then click on the Authentication Tab as shown below:




Click on EAP Methods as MD5 Challenge will be needed to allow NetVanta Routers to work with IAS. For the EAP types, click Add at the bottom of the Box and then select MD5-Challenge from the Next Window that opens as shown below:

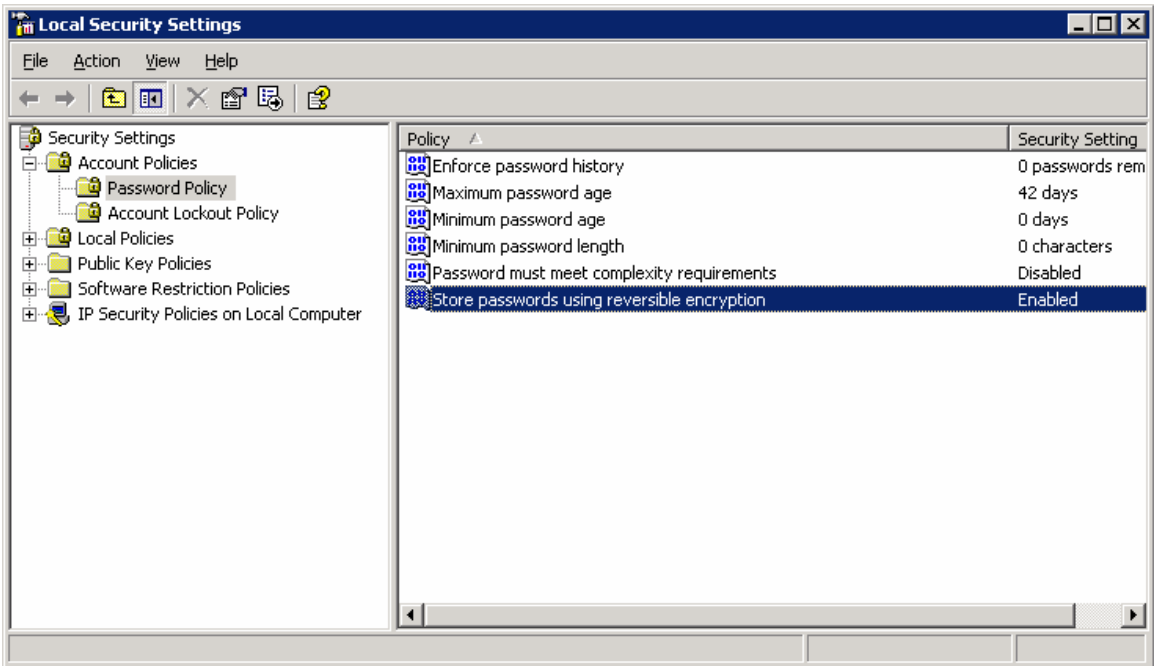


After selecting MD5-Challenge, click OK. Then Click OK on the Next Window Down (Select EAP Providers). Click Apply on the Edit Dial-In Profile. Click OK and then click Next and Finish to finish the Wizard. Next, Navigate to the Computer Management under Administrative Tools in the Control Panel. Once this is done, expand the Section: "Local Users and Groups." Once here, right click on the Users Folder and Add New User as shown below:




In the New User window that opens, fill out the profile including User Name and Full Name and Password. Remember, this will be the credentials the End User will use to log on to the Network. Once the information is filled in, click Create, then Close. The User should show up on the right side of the screen.

After doing this, go back to the Administrative Tools under the Control Panel and Open the Local Security Policy MMC. On this, navigate to Password Policy. The folders to navigate through are shown in figure below:

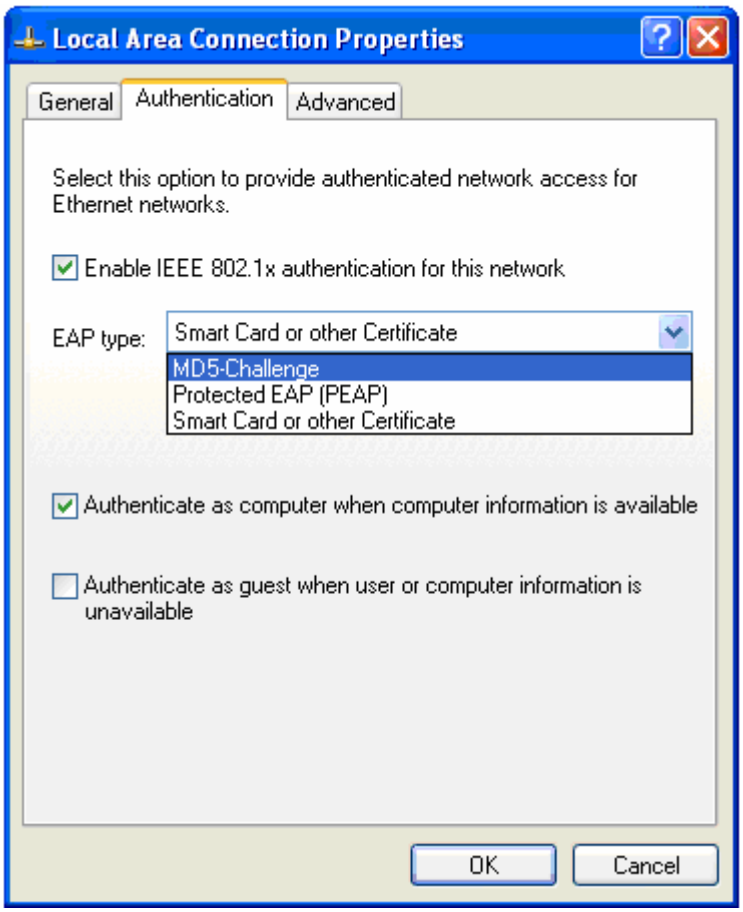



Make sure the "Store passwords using reversible encryption is Enabled. If it isn't, click on the property and change accordingly. After doing this, the IAS Server should now be configured to accept 802.1X authentication requests.

## Configuring Windows Supplicant

To configure the Windows Supplicant, begin by opening up the Network Connection properties. The easiest way to reach this menu is to double-click on the Network Icon in the lower right corner of the screen of the Windows device as shown below:


After double-clicking on the Network Icon, click properties under the Local Area Connection Status. After opening the properties, click the Authentication tab. Below is an example of this menu.




As shown above, select Enable IEEE 802.1x authentication for this network. Also change the EAP type from the drop down menu to MD5-Challenge. After changing this, click OK. At this point, the Supplicant has been configured to use 802.1x.

## Troubleshooting

There are a few different commands that can be used to debug port-auth. A very important command that displays the authentication of a user is "**debug port-auth**." Below is the output from a successful logon:

Switch#debug port-auth
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.PACKET RX Rcvd EAP Resp for sess 11 on int swx 0/1
1
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in RESPONSE state
2007.09.11 11:55:30 PORT_AUTH.GENERAL Init auth with server for sess 11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Sent EAP Resp/Id to AuthServer for sess 11
on int swx 0/11
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.GENERAL Rcvd response from server for sess 11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in SUCCESS state
2007.09.11 11:55:30 PORT_AUTH.PACKET TX Sent EAP Success for sess 11 on int swx

0/11
2007.09.11 11:55:30 PORT_AUTH.BKENDSM Int swx 0/11 sess 11 in IDLE state
2007.09.11 11:55:30 PORT_AUTH.REAUTHSM Int swx 0/11 sess 11 in INITIALIZE state
2007.09.11 11:55:30 PORT_AUTH.AUTHSM Int swx 0/11 sess 11 in AUTHENTICATED state
; sess is authorized

Using the **show port-auth interface switchport 0/11** command can show the status of 802.1X on a certain port. In this case, it shows that a PC with a MAC Address of 00:D0:59:23:D6:03 has been authorized to connect to the network.

```
Switch# sh port-auth interface switchport 0/11
  Port-Authentication is enabled on swx 0/11
    Status                authorized
    Auth Mode             port-based
    Port-Control          auto
    Multiple Hosts Allowed   disabled
    Supplicant MAC        00:d0:59:23:d6:03
    Current Identifier    3
```