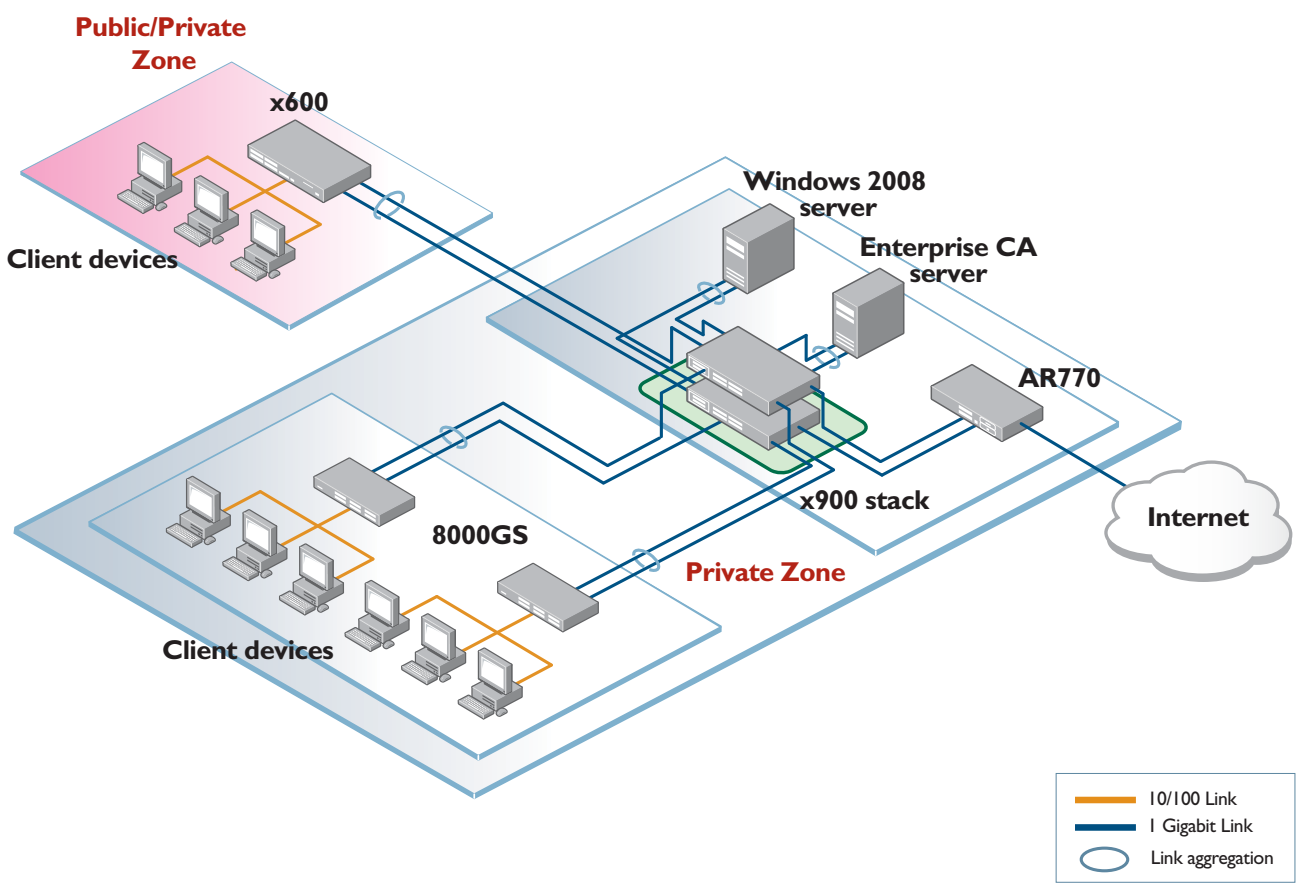
Tested Solution: LAN Client Authentication



Introduction

The key to strong LAN security, and seamless mobility within an Enterprise network, is to **identity** and **authenticate** the user at their point of connection to the network.

Authentication is necessary to safeguard valuable network resources from intruders. Identification is necessary in order to give users a consistent level of network access regardless of their physical location within the network.

Moreover, identification and authentication are integral to the client health-check process that is a core component of a NAC solution.

This solution will explain how to:

- Configure Allied Telesis switches to ensure that ALL devices connecting to the network can be authenticated and identified.
- Configure Microsoft Windows 2008 Server as the authentication server within the network.
- Use the highly secure certificate-based method of user authentication

Contents

Network scenario

The solution is based upon the network illustrated on page 1. There are two zones within the network:

- A fully private zone in which only registered users (i.e., users registered in the Active Directory hosted on the Windows Server) may connect.
- A private/public zone in which registered users, unknown guests, and trusted (but unregistered) users from other branches of the same company may connect.

Solution description

The guiding principles in the design of this network are **resiliency** and **security**.

The **core** of the network is an x900 Virtual Chassis Stack. Aggregated Gigabit links radiate from this stack to the access switches and the servers.

In the **Private Zone**, the access switches are AT-8000GS switches. These Layer 2 switches are configured for 802.1x and MAC-based authentication on all their edge-facing ports. The only devices that are connected to these ports are registered client PCs (configured for 802.1x authentication) and printers, scanners. The printers and scanners do not include 802.1x clients, so the ports to which they are connected fall back to MAC-based authentication.

The switch in the **Public/Private Zone** is an x600 Layer 3 switch. The edge-facing ports on this switch are configured for triple authentication. Therefore, all the ports are capable of performing 802.1x, MAC-based and Web-based authentication. So, registered users will be authenticated by 802.1x, and any printers or scanners installed in that zone are MAC authenticated.

The **trusted visitors** who are visiting from another office, who are not registered in the local central user database, will be given a special username/password that they can use with WEB-auth to obtain Internet access, and some intranet access. Their user accounts will be created on the Local Radius server in the x600. These user accounts will be associated with the group `otheroffices`, so those users will be dynamically allocated to VLAN40 when they have been authenticated.

The **external guests** will be given a different username/password for a user account in the local RADIUS server that is associated with the group `externalvisitors`, so these users will be dynamically allocated to VLAN50 when they have been authenticated.

The x600 switch will use Layer 3 to switch data to the core. This places a Layer 3 boundary between the Public/Private zone and the core, which makes it easier to control what traffic may leave the Public/Private Zone. It does mean that a set of IP subnets need to be provisioned specifically for the Public/Private zone, but that is a simple matter to configure on the DHCP server.

Switch Configurations

x600

This is the switch in the Private/Public Zone. Its edge ports are configured for triple authentication. Therefore, 802.1x, MAC-based, and Web-based authentication are enabled on those ports.

The switch uses three different RADIUS servers.

The Network Policy Server within the windows 2008 server at 192.168.2.254 is the RADIUS server for 802.1x requests.

So that the authentication of visitors from other offices is entirely self-contained within the Private/Public Zone, the x600 uses its own internal RADIUS database for the authentication of Web-based authentication requests. This way, a specific username/password can be created for each such visitor as they arrive, and entered into the RADIUS database of the x600, without any changes having to be made to the central Network Policy Server. These entries can be removed from the x600 RADIUS database again when the visitor departs.

MAC-based authentication requests are forwarded to yet a different RADIUS server. This is because the default strong password requirements on the Microsoft Active Directory will not accept users whose username and password is a MAC address (as MAC authentication requires). So the MAC-based authentication requests are passed to a RADIUS server hosted in the virtual chassis stack at the core of the network.

The switch is also configured with a DHCP service specifically for the Guest VLAN. This is because the visiting users will initially be placed into the Guest VLAN when they first connect, as they will fail authentication. The DHCP service on the switch will allocate IP addresses to users in the Guest VLAN. Those PCs can then use that IP address as their source address for their Web authentication session. To perform Web authentication, those users will need to browse to 192.168.160.10 (the switch's IP address in the Guest VLAN) or to any address outside the 192.168.160.0/24 subnet. Their Web browser will then be presented with a login page, into which they can enter the username/password they have been given for accessing the network.

Once successfully authenticated (by entering the correct username/password into this login page), they will be re-allocated to their appropriate VLAN - which is VLAN40 for visitors from other offices, and VLAN50 for external guests. Once they are re-allocated to this VLAN, they need an IP address that belongs to the subnet for that VLAN. This is where the brief lease-time on the DHCP leases provided by the switch comes in.

Because the PC's link to the switch does not go down at the completion of the authentication, the PC will not necessarily attempt to renew its DHCP lease at that moment. By defining a very brief lease time on the DHCP lease that is allocated to the PC while it is in the Guest VLAN, we ensure that the PC will have to renew its lease within 30 seconds of the completion of the authentication. As the PC has been put into a new VLAN when the authentication is completed, its first DHCP renewal after the authentication will provide it with a lease for an IP address in the subnet used on that new VLAN. Note that all the VLANs except the Guest VLAN have been configured to relay DHCP requests to another DHCP server.

```
hostname Triple-Auth

radius-server host 192.168.2.254 key MS-IAS
aaa group server radius NPS
 server 192.168.2.254
aaa authentication dot1x default group NPS

radius-server host 192.168.2.252 key MAC-AUTH
aaa group server radius MAC-Auth
 server 192.168.2.252
aaa authentication auth-mac default group MAC-Auth

radius-server host 127.0.0.1 key awplus-local-radius-server
aaa group server radius Internal
 server 127.0.0.1
aaa authentication auth-Web default group Internal

aaa authentication login default group NPS local
```

The Network Policy server in the windows 2008 server is used for validation of 802.1x authentication requests

A separate RADIUS server, that accepts MAC users that have a MAC address as both username and password, is used for validation of MAC-based authentication requests

The validation of Web-based authentication requests is performed within the switch's own RADIUS server

Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server. If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request

Set up the Local RADIUS server.
The only NAS configured for the server is 127.0.0.1, so it will only accept internally-generated requests.
It is configured with username/password set up for visitors from other offices, who will be dynamically allocated VLAN 40; and for external visitors, who will be dynamically allocated to VLAN50

```
crypto pki trustpoint local
crypto pki enroll local
radius-server local
 server enable
 nas 127.0.0.1 key awplus-local-radius-server
 group otheroffices
  vlan 40
group externalvisitors
  vlan 50
user InternalVisitor password ikiG4JcsKEwFlhL
group otheroffices
user ExternalVisitor password ikiG4JcsKEwFlhL
group externalvisitors
```

The switch is configured with one static VLAN (VLAN 2) that is used for communication with the rest of the network. The other 5 VLANs are used for dynamic allocation to users

```
vlan database
 vlan 2 name uplink
 vlan 10 name Accounting
 vlan 20 name Engineering
 vlan 30 name Marketing
 vlan 40 name OtherOffices
 vlan 50 name ExternalGuests
 vlan 60 name GuestsVLAN
```

The first 22 ports on the switch are available for users to connect to. They are all configured with triple authentication with dynamic VLAN assignment and VLAN60 as the guest VLAN. The ports are configured to support multiple supplicants on a single port, in case a hub or EAP-forwarding L2 switch is attached to one of the ports, to enable multiple users to share that port

```
interface port1.0.1-1.0.22
 auth-mac enable
 auth-Web enable
 dot1x port-control auto
 auth host-mode multi-supplicant
 auth guest-vlan 60
 auth dynamic-vlan-creation type multi
 spanning-tree portfast
 spanning-tree portfast bpdu-guard enable
```

Ports 23 and 24 are configured as a link aggregration group to connect the switch to the virtual chassis stack in the core

```
interface port1.0.23-1.0.24
switchport access vlan 2
static-channel-group 1
```

Set up a DHCP server on the switch that is used specifically for the Web-Auth users to have an IP address for a brief time whilst they authenticate via HTTP. The leasetime is set to 30 seconds, so the DHCP lease will be re-newed very quickly after the authentication has been completed

```
ip dhcp pool Temporary
 network 192.168.160.0 255.255.255.0
 range 192.168.160.20 192.168.160.40
 default-router 192.168.160.10
 lease 0 0 0 30
 subnet-mask 255.255.255.0
service dhcp-server
```

IP addresses are configured on all the VLANs. All the client VLANs are configured to relay DHCP requests to the DCHP server in the network core

```
interface vlan2
 ip address 192.168.2.10/24
interface vlan10
 ip address 192.168.110.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan20
 ip address 192.168.120.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan30
 ip address 192.168.130.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan40
 ip address 192.168.140.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan50
 ip address 192.168.150.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan60
 ip address 192.168.160.10/24
```

The default route is via the x900 VCStack	ip route 0.0.0.0/0 192.168.2.252
All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself	log buffered level errors log host 192.168.2.254 log host 192.168.2.254 level debugging
Allow read-only SNMP monitoring from one management station	access-list 1 permit 192.168.2.253 snmp-server enable trap auth nsm snmp-server community public ro 1 snmp-server host 192.168.2.253 version 2c public
Configure NTP (Network Time Protocol) with the IP address of the NTP server	ntp server 192.168.2.252

8000S

Enable 802.1x globally	dot1x system-auth-control
The switch cannot configure separate RADIUS servers for 802.1x authentication and MAC-based authentication. So, it will forward all authentication requests to the Network Policy Server running on the Windows 2008 server at 192.168.2.254. The Network Policy Server will process 802.1x requests itself. For the MAC-based authentication requests, it acts as a RADIUS proxy, and forwards the requests to the RADIUS server running within the core VCStack	radius-server host 192.168.2.254 key MS-IAS aaa authentication dot1x default radius
Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server. If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request	aaa authentication login default radius local
The switch is configured with one static VLAN (VLAN 2) that is used for communication with the rest of the network. The other 4 VLANs are used for dynamic allocation to users	vlan database vlan 2,10,20,30,50
vlan50 is designated as the guest VLAN for the switch	interface vlan 50 dot1x guest-vlan exit
The 24 10/100 ports are configured for MAC-based and 802.1x authentication. They accept dynamic VLAN allocation, and will put unauthenticated users into the guest VLAN	interface range ethernet 1/e(1-24) dot1x re-authentication dot1x mac-authentication mac-and-802.1x dot1x guest-vlan enable dot1x radius-attributes vlan dot1x port-control auto spanning-tree portfast spanning-tree guard root exit

Two gigabit ports, one from each stack member, are aggregated together to create a resilient link to the network core. These ports are tagged in all the VLANs on the switch

```
interface range ethernet 1/g1,2/g1
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 10
switchport trunk allowed vlan add 20
switchport trunk allowed vlan add 30
switchport trunk allowed vlan add 50
channel-group 1 mode on
exit

interface vlan 2
ip address 192.168.2.11 255.255.255.0
exit
```

DHCP snooping guards against rogue server and server exhaustion attacks

```
ip dhcp snooping
ip dhcp snooping vlan 10
ip dhcp snooping vlan 20
ip dhcp snooping vlan 30
ip dhcp snooping vlan 50

interface port-channel 1
ip dhcp snooping trust
exit
```

Allow read-only SNMP monitoring from one management station. Send traps to that same management station

```
snmp-server community public ro 192.168.2.253 view Default
snmp-server host 192.168.2.253 public traps 2
```

System time is provided from an SNTP server

```
sntp client enable vlan 2
clock source sntp
sntp unicast client enable
sntp server 192.168.2.252
```

All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself

```
logging 192.168.10.11
logging buffered errors
```

x900 Stack

All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself

```
log buffered level errors
log host 192.168.2.254
log host 192.168.10.11 level debugging
```

Allow read-only SNMP monitoring from one management station

```
access-list 1 permit 192.168.10.13
snmp-server enable trap auth nsm
snmp-server community public ro 1
snmp-server host 192.168.10.13 version 2c public
```

A resiliency link backs up the dedicated stacking link. If the stacking link fails, communication is maintained to allow graceful reconfiguration

```
stack resiliencylink eth0
```

Use priority to pre-elect the VCStack master switch

```
stack 1 priority 1
```

Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server. If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request

```
radius-server host 192.168.2.254 key MS-IAS

aaa authentication login default group Radius local
```

The switch is configured with 8 VLANs

```
vlan database
 vlan 2 name core
 vlan 10 name Accounting
 vlan 20 name Engineering
 vlan 30 name Marketing
 vlan 40 name OtherOffices
 vlan 50 name ExternalGuests
```

Create ACLs that will control where the various categories of users will be able to access

All DHCP will be allowed through

```
access-list 3001 permit udp any range 67 68 any range 67 68
```

External visitors' traffic (apart from DHCP) cannot go to any internal addresses

```
access-list 3002 deny ip 192.168.150.0/24 192.168.0.0/16
access-list 3003 deny ip 192.168.150.0/24 172.16.0.0/12
access-list 3004 deny ip 192.168.150.0/24 10.0.0.0/8
```

Visitors from other offices' traffic (apart from DHCP) cannot go to local internal addresses, but can go out onto the corporate WAN

```
access-list 3005 deny ip 192.168.140.0/24 192.168.0.0/16
```

The final ACL allows through all the traffic that has not been explicitly blocked by the previous ACLs

```
access-list 3006 allow ip any any
```

Create link aggregation groups across the VCStack members for resiliency

The ports that connect to the x600 are untagged in VLAN 2

```
interface port1.0.1
switchport access vlan 2
static-channel-group 1
ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006

interface port2.0.1
switchport access vlan 2
static-channel-group 1
ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006
```

The ports that connect to the 8000S switches are tagged in all VLANs except the InternalVisitors VLAN

```
interface port1.0.2
switchport mode trunk
switchport trunk allowed vlan add 2,10,20,30,50
static-channel-group 2

ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006

interface port2.0.2
switchport mode trunk
switchport trunk allowed vlan add 2,10,20,30,50
static-channel-group 2
ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006

interface port1.0.3
switchport mode trunk
switchport trunk allowed vlan add 2,10,20,30,50
static-channel-group 3
ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006

interface port2.0.3
switchport mode trunk
switchport trunk allowed vlan add 2,10,20,30,50
static-channel-group 3
ip access-group 3001
ip access-group 3002
ip access-group 3003
ip access-group 3004
ip access-group 3005
ip access-group 3006
```

Other ports are untagged in VLAN2, for connection to servers and a router

```
interface port1.0.10-1.0.12
switchport access vlan 2
spanning-tree portfast
spanning-tree portfast bpdu-guard enable

interface port2.0.10-2.0.12
switchport access vlan 2
spanning-tree portfast
spanning-tree portfast bpdu-guard enable
```

IP addresses are configured on all the VLANs. All the client VLANs are configured to relay DHCP requests to the DCHP server in the network core

```
interface vlan2
 ip address 192.168.2.252/24
interface vlan10
 ip address 192.168.10.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan20
 ip address 192.168.20.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan30
 ip address 192.168.30.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan40
 ip address 192.168.40.10/24
 ip dhcp-relay server-address 192.168.2.254
interface vlan50
 ip address 192.168.50.10/24
 ip dhcp-relay server-address 192.168.2.254
```

Create routes to the subnets in the Public/Private Zone

```
ip route 192.168.110.0/24 192.168.2.10
ip route 192.168.120.0/24 192.168.2.10
ip route 192.168.130.0/24 192.168.2.10
ip route 192.168.140.0/24 192.168.2.10
ip route 192.168.150.0/24 192.168.2.10
```

The stack will also require a local RADIUS server configuration, which is described in the section "**Setting up MAC-based authentication**" (page 54).

Additionally, it could be configured as a DHCP server, as described in the section "**Setting up the x900 VCStack as a DHCP server**" (page 61).

Setting up the Windows 2008 Server

This solution uses two roles of the windows 2008 server:

- Active Directory Domain Controller
- Network Policy Server

The description that follows describes all the steps required to take the server from a fresh install of Windows Server 2008 through to the state whereby it is able to play its required role in the authentication solution.

Configuring IP interface(s)

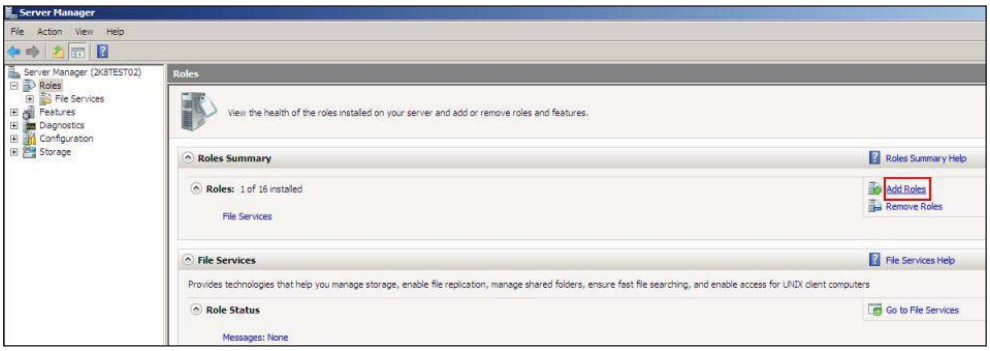
It is advisable to have at least one IP interface configured on the server before embarking on installing Active Directory and Network Policy Server. These applications assume that the server has IP connectivity.

For the purposes of the solution example, the main LAN interface of the server has been given IP address 192.168.2.254.

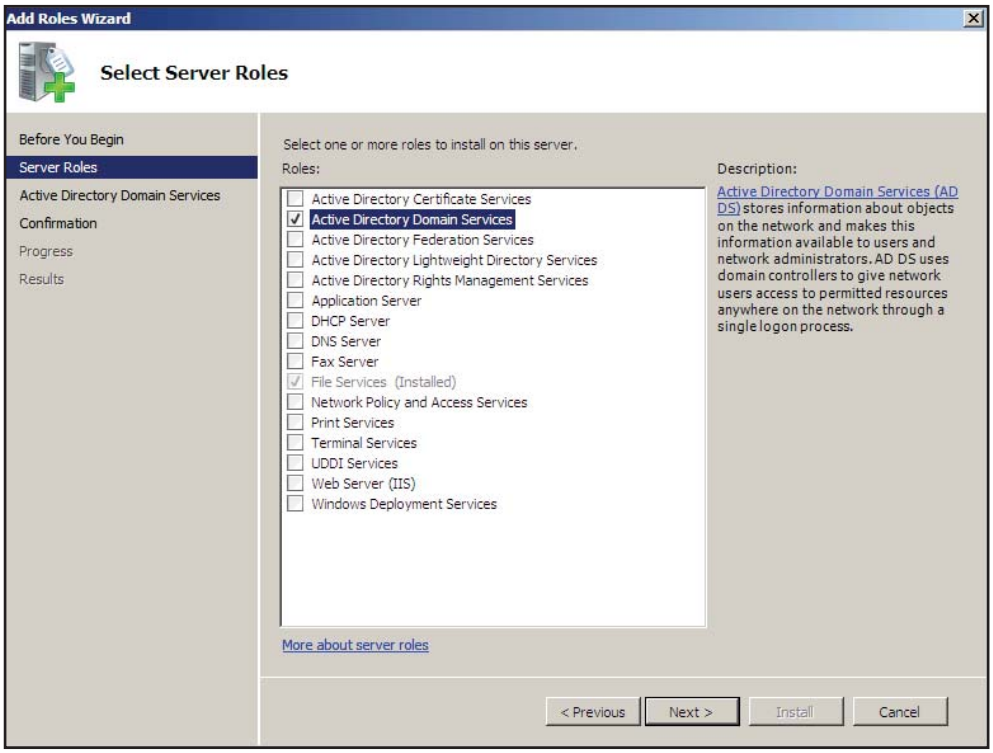
Installing Active Directory

To install Active Directory:

- Run the **Server Manager** - which is found in the **Administrative Tools** section of the **Start** menu.
- Select **Add Roles**.This will open the **Add Roles Wizard**.

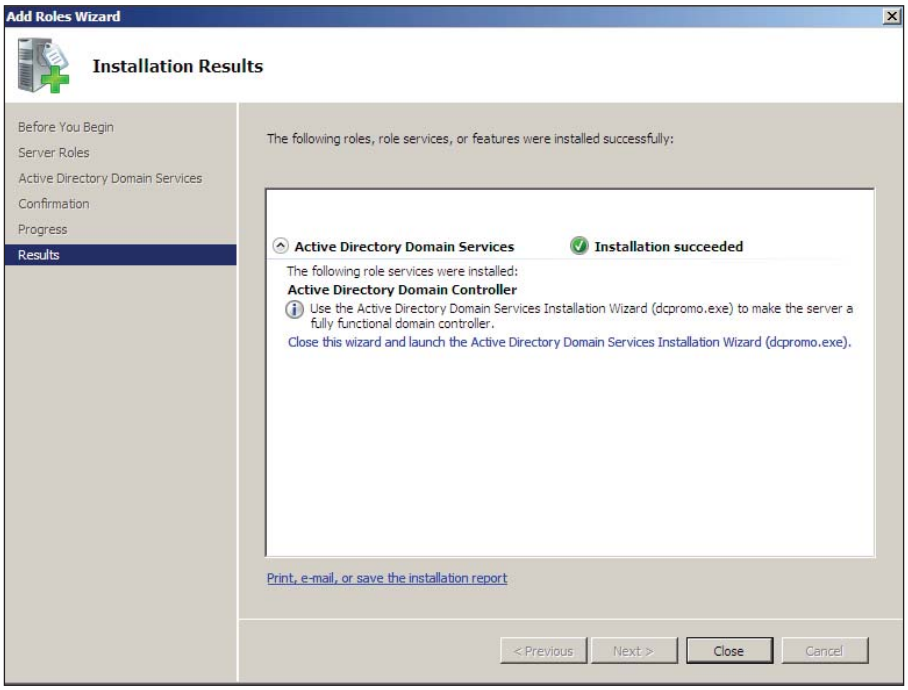


- In the **Before You Begin** window, choose **Server Roles** from the left side, and select **Active Directory Domain Services** from the list of **Roles**.

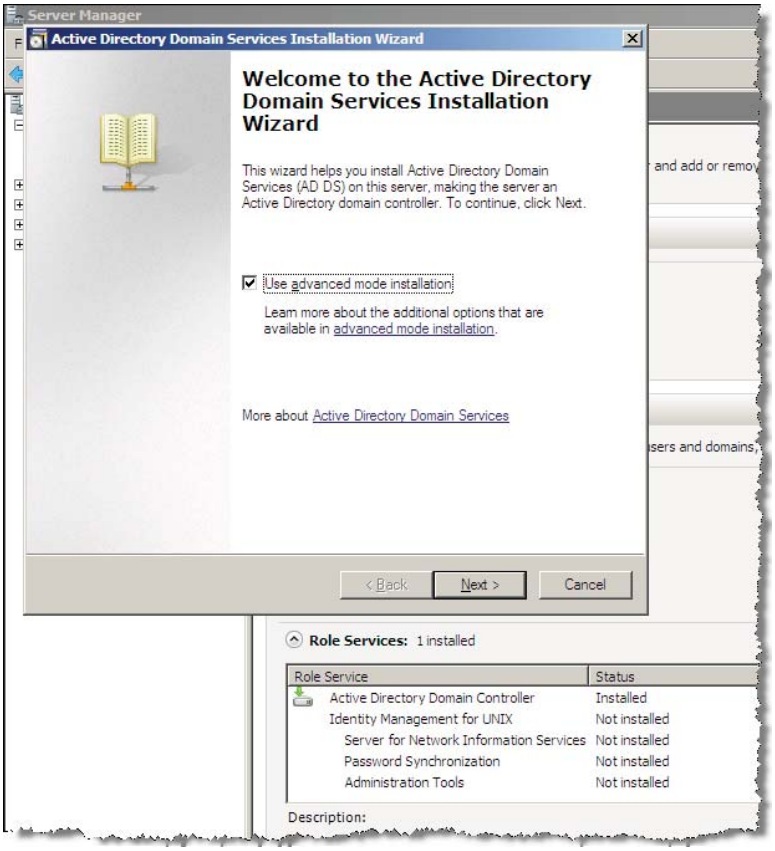


- Click **Next**.

Follow the instructions in the succeeding windows, there are no decisions that need to be made. The service will be installed, and you will reach the completion window.

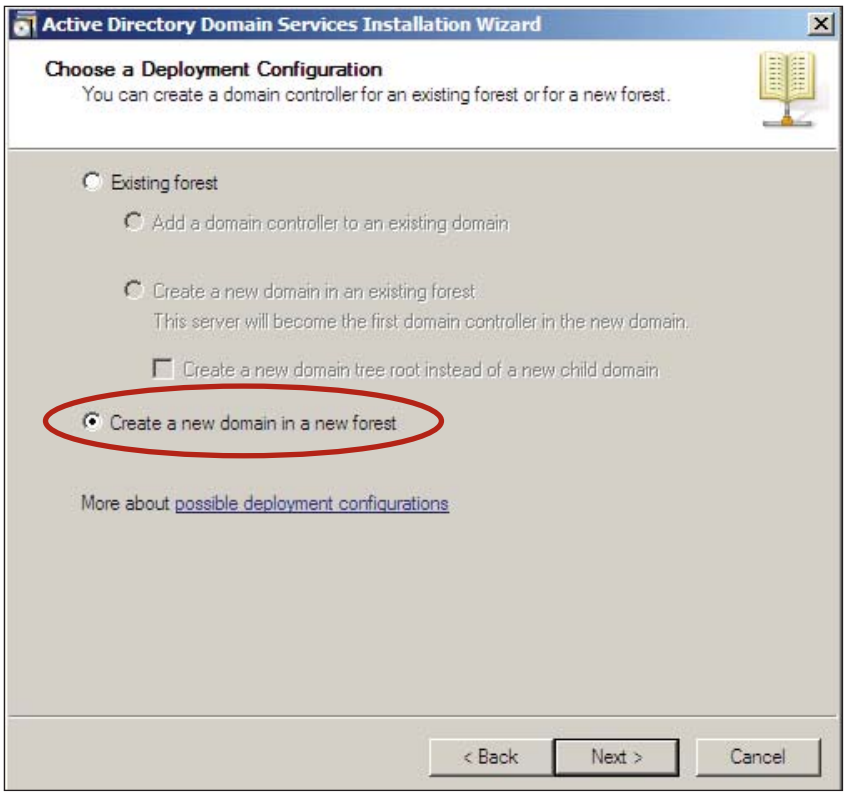


- Click **Close**, and you are taken to another wizard that takes you through some configuration tasks on the **Active Directory Domain Services** (despite being called the installation wizard, it is really a configuration wizard).

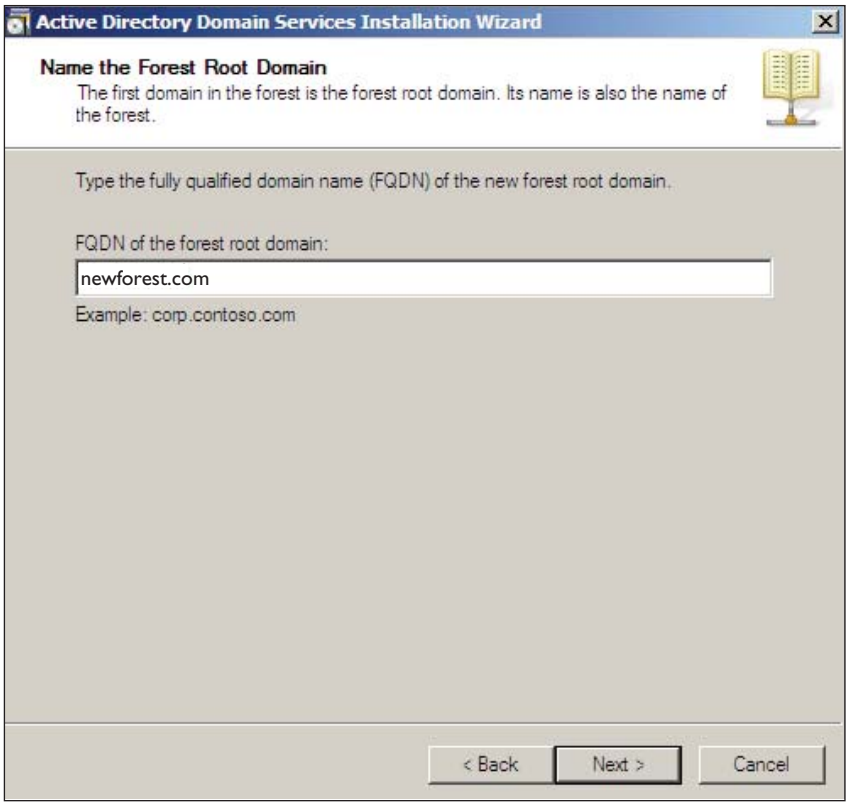


Continue through the wizard to the **Choose a Deployment Configuration** window.

- Choose the option that matches your deployment. In our example, the domain server is being created in a **new forest**.

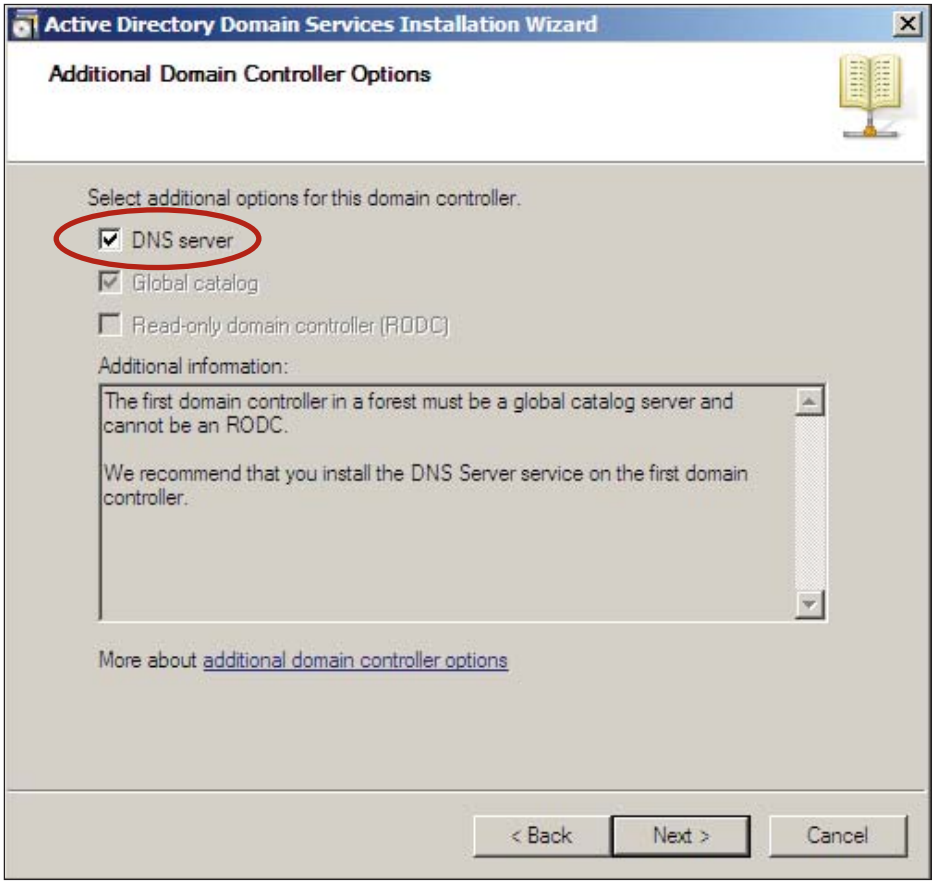


- Click **Next**.
- In the next window, type in a domain name for the forest:
- Choose the defaults in the next few windows.



- Click **Next**.

When you come to the **Additional Domain Controller Options** window, you might choose to set the server up as a DNS server, if the network does not already have a DNS server.



- Click **Next**.

The remaining windows in the wizard are straight-forward.

Upon completion of the wizard, the Active Directory Domain Services are fully installed and configured.

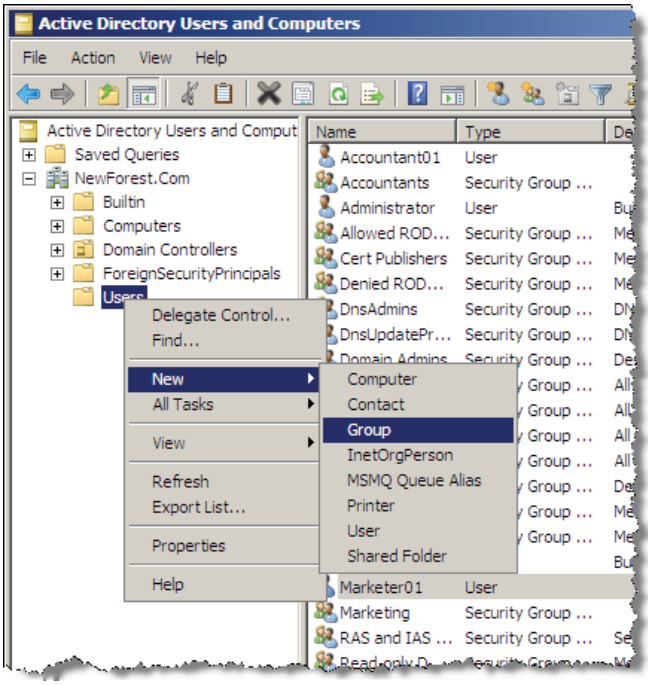
Adding users and groups to Active Directory

Users need to be added to **Active Directory**, as this is the store of user credentials that will be used for the 802.1x authentication.

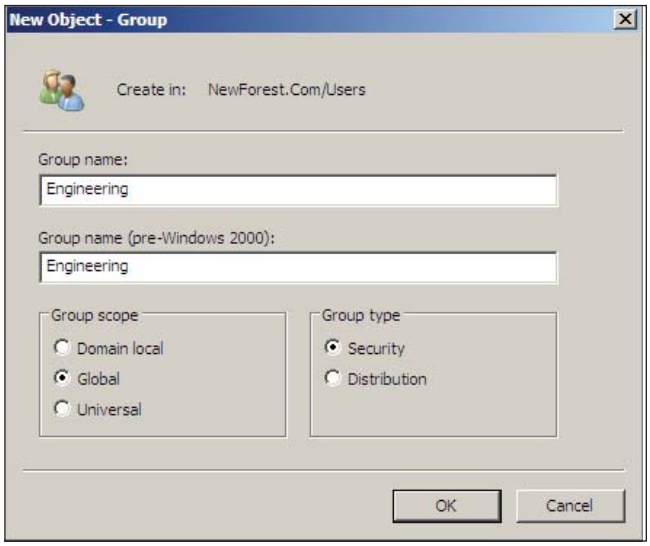
In this solution example, three groups of users are created – Accountants, Engineers, and Marketers. Let us follow through the steps of creating the Engineers group, and then creating a user member of that group.

To add users and groups to Active Directory:

- Open **Active Directory Users and Computers** - which is found in the **Administrative Tools** section of the **Start** menu.
- Open up the items below the domain's name in the left-hand pane (NewForest.com).
- Right-click on **Users**, then choose **New** > **Group**.



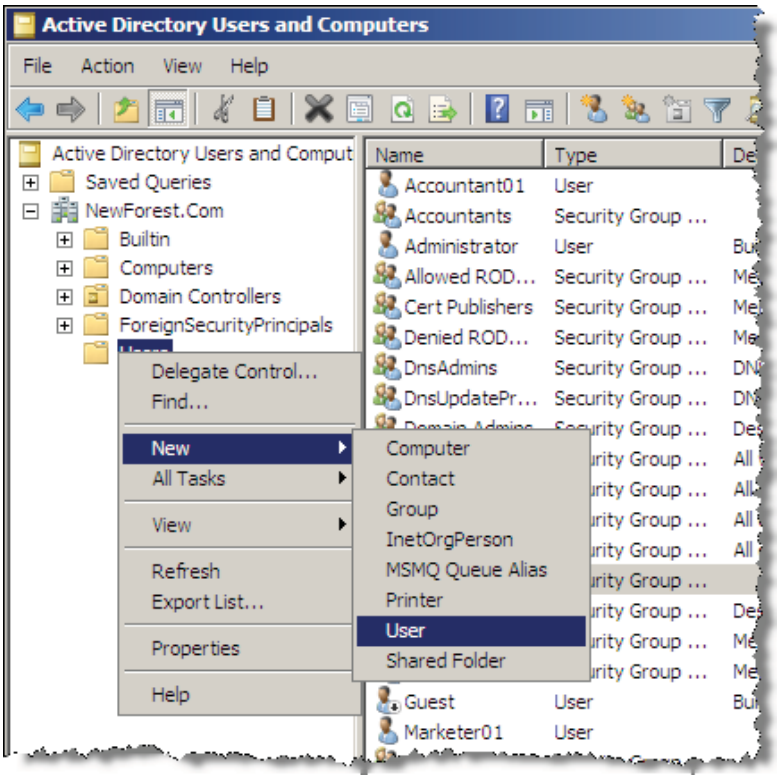
- Type in a **Group Name**.



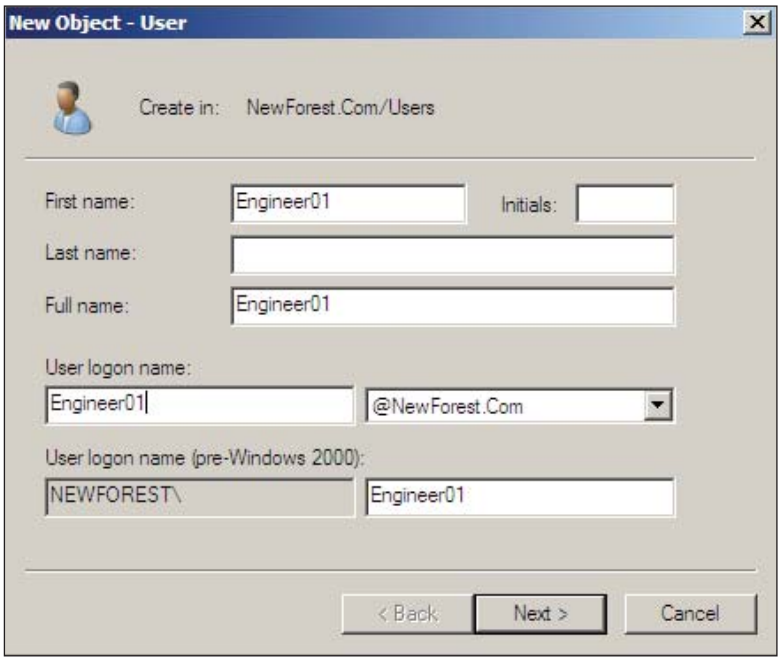
- Click **OK** and the group is created.

Now, you can create users to go into the group.

- Right-click on **Users** in the left-hand pane. This time choose **New** > **User**.



- Type in the user details.



- Click **Next**.

- Type in the user **Password**.

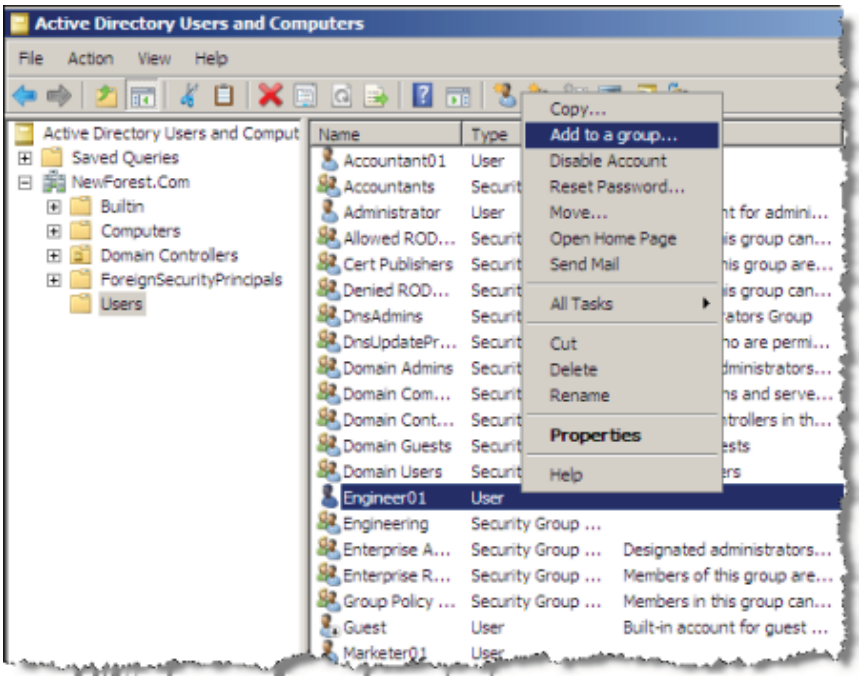
- Click **Next**.

The user is then successfully created.

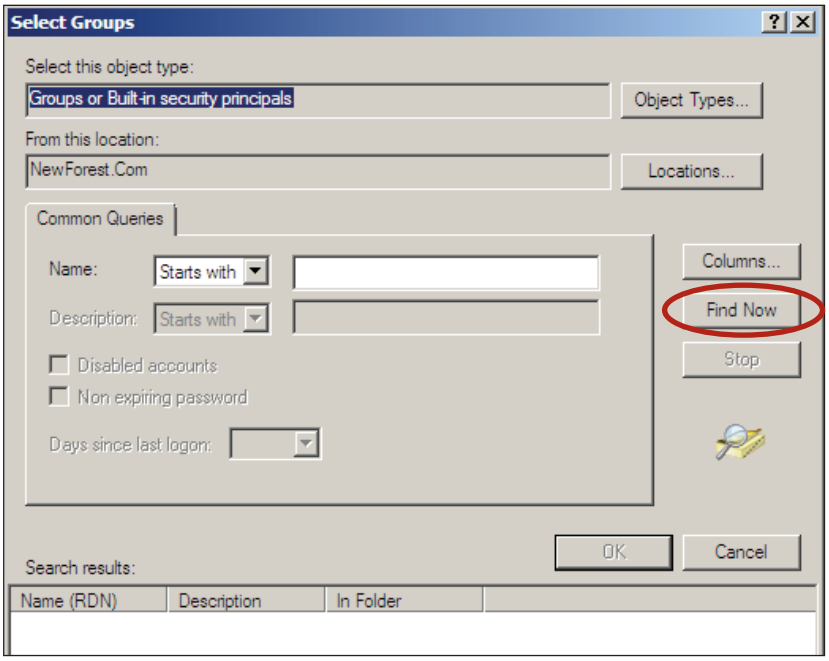
To add the user to a Group:

The final step is to add the user Engineer01 to the **Group** Engineers.

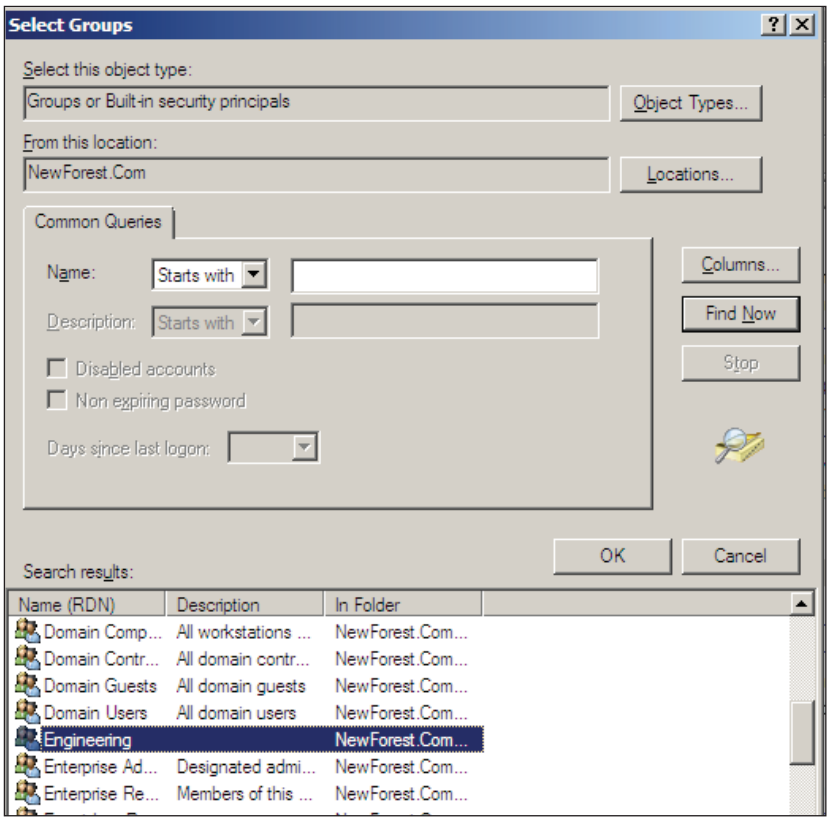
- Right-click on the new user's name Engineer01 in the list of users, then choose **Add to a group...**



- Click the **Advanced...** button on the resulting window, to go to the advanced form of the **Select Groups** window:



- Click **Find Now** to get a list of the available groups.
- Choose the desired group, click **OK**, and the new user is added to the chosen group.



In this way, entries can be created in Active Directory for all the users who are to be authenticated on the network, and they can be collected into groups to whom common attributes will be assigned after authentication. In the case of this solution example, all the users in the same group will be assigned the same **VLAN ID** upon authentication.

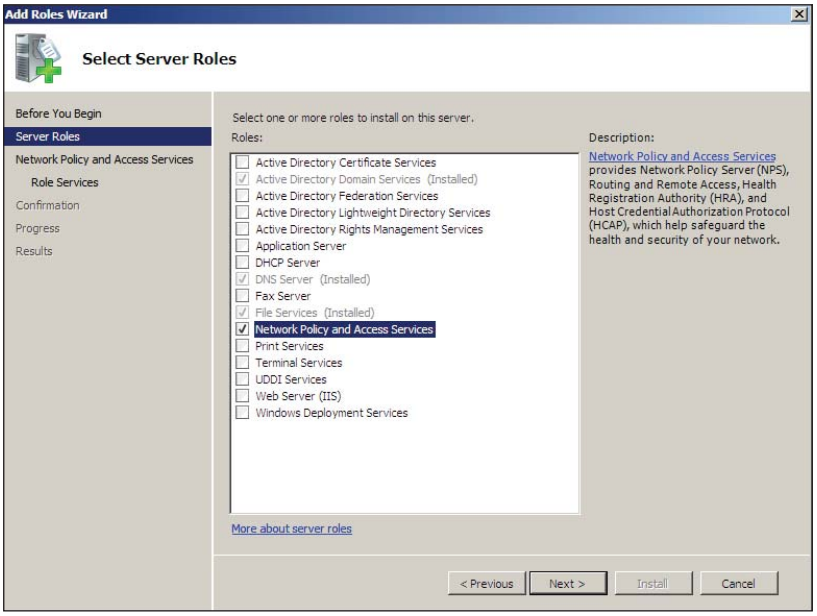
Installing Network Policy Server

In Windows Server 2008, the old IAS server has been replaced by the Network Policy Server. This server expands upon the IAS functionality by adding NAC capability. In this solution example, we will use the Network Policy Server as a RADIUS server.

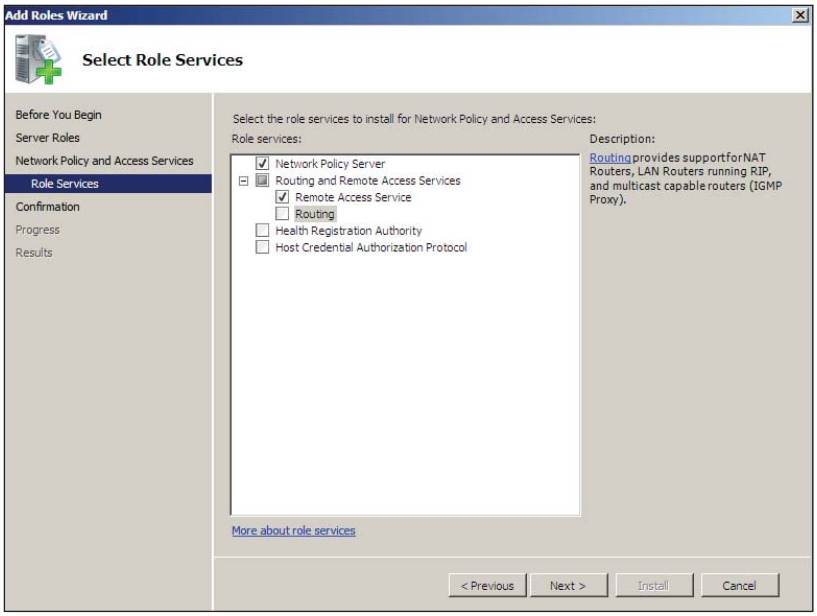
To install the Network Policy Server:

Start again with the **Add Roles** link in the Server Manager.

- In the **Select Server Roles** window, select **Network Policy and Access Services**:

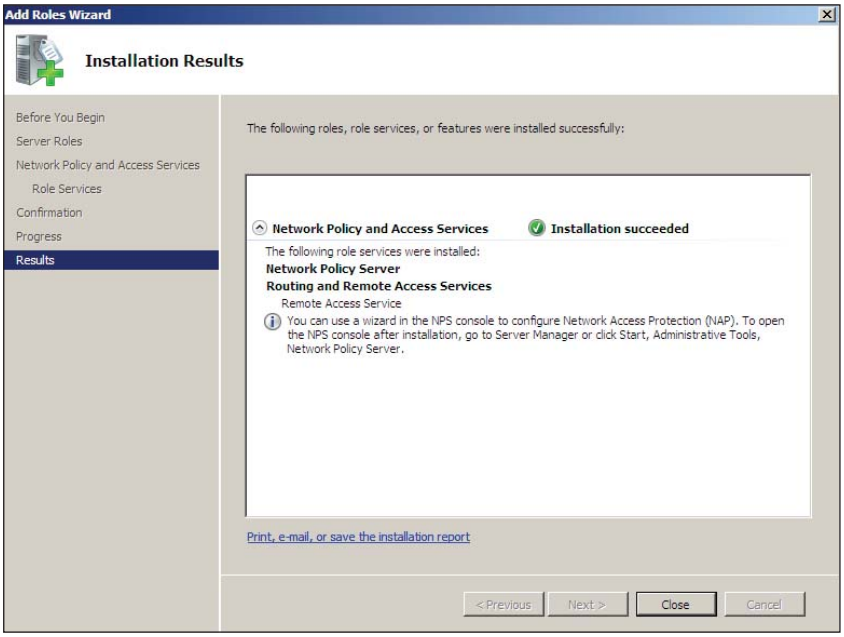


- Click **Next** until you get to the **Select Role Services** window.



- Select the role services to install. (Not all the role services need to be installed).
- Click **Next**.

- Click through the succeeding windows; the role will be installed, and the completion window is displayed.

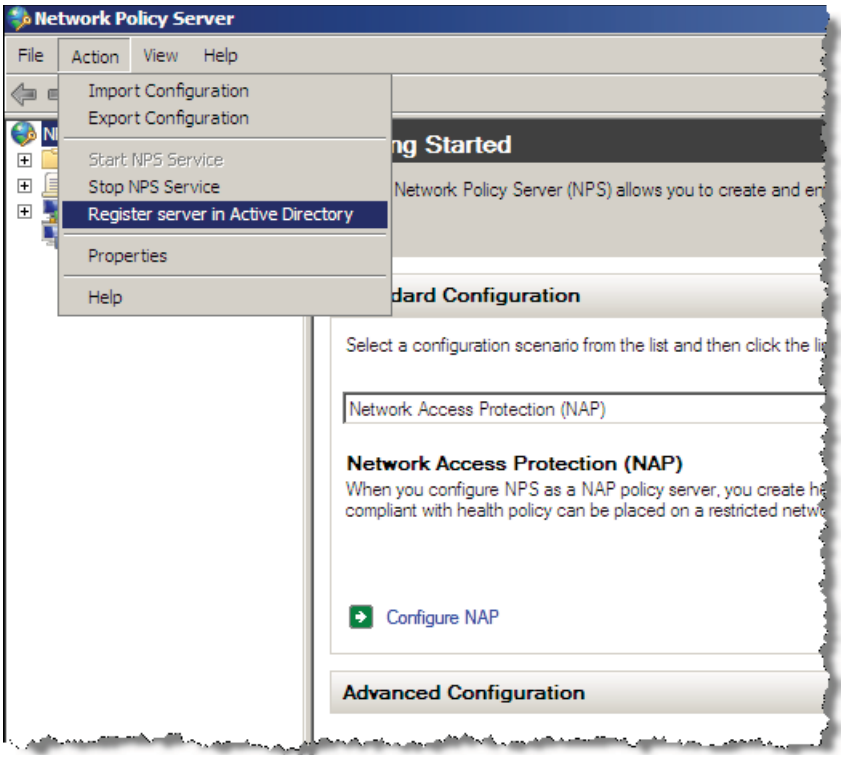


Registering NPS with Active Directory

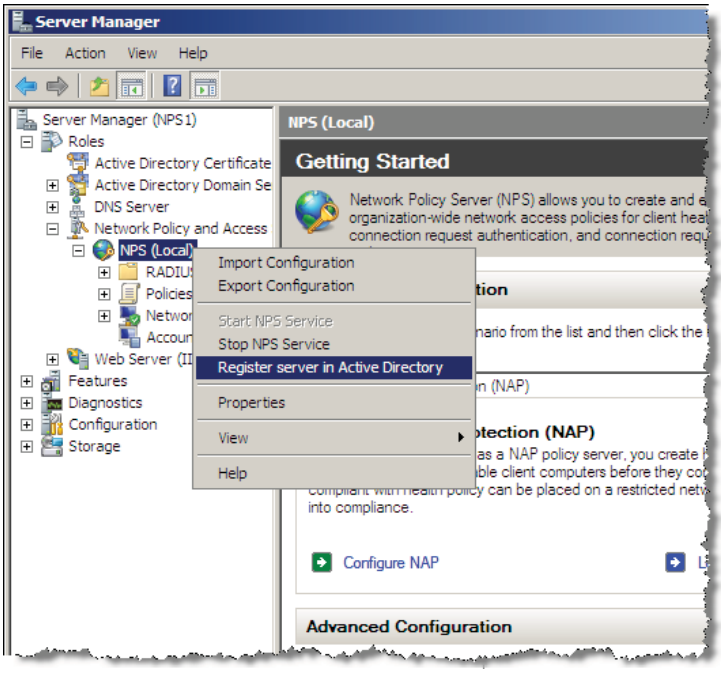
In order for NPS to be able to request user credentials from Active Directory, it must be registered with Active Directory.

To register NPS with Active Directory:

- Open the **Network Policy Server Manager**, by choosing **Network Policy ...** from the **Administrative Tools** section of the **Start** menu.
- Select **Action** > **Register server in Active Directory**.



Or, in the **Server Manager**, select **Network Policies and Access...**, then right-click **NPS (Local)** > **Register Server in Active Directory**.



Obtaining a server certificate for the server that is running NPS

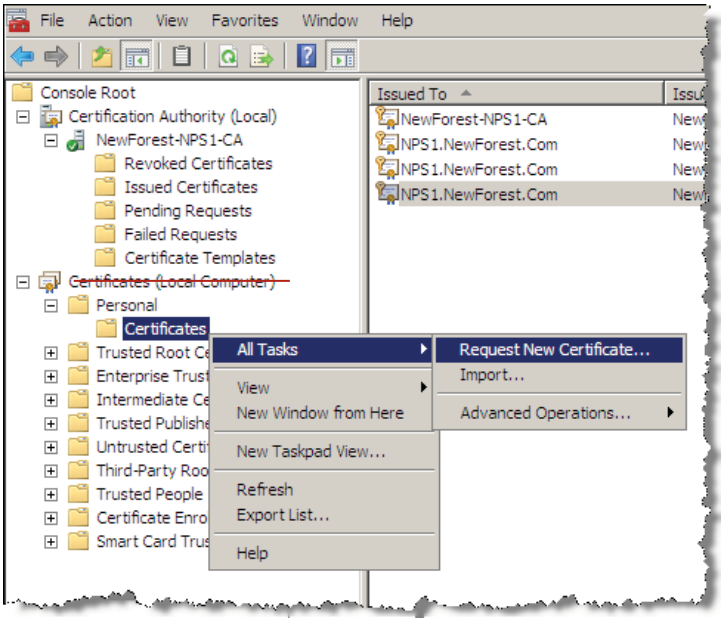
The server running NPS must have a certificate if it is to perform 802.1 x authentications using PEAP/TLS; even if the supplicants are using username/password (rather than certificates) to identify themselves.

The server must **obtain a certificate** that can be used for this purpose. It requests the certificate from the Domain's Certificate Authority.

For the purposes of this example, we will assume that another server has been configured as a Root CA for the domain, and has been joined to the **NewForest** domain.

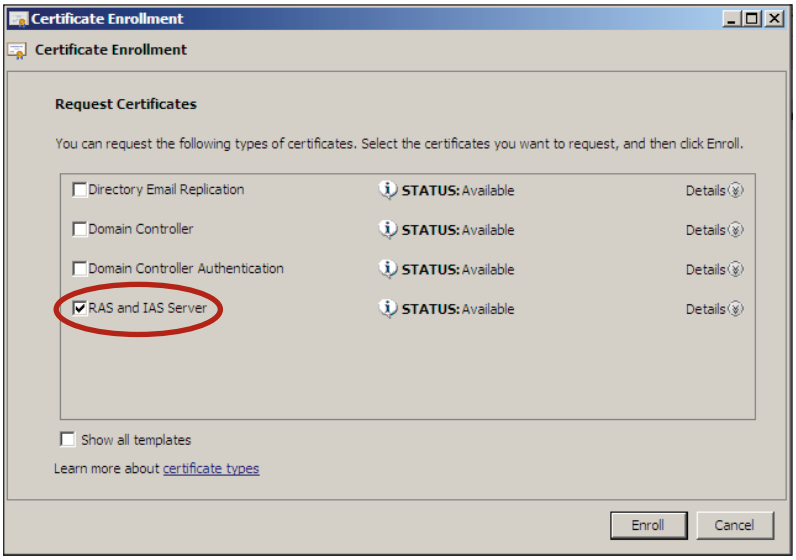
To obtain a server certificate:

- To obtain a certificate from this server, use the **Certificates** snap-in in the Console.
- Open up the topics under **Certificates (Local Computer)**, then right click on **Certificates** and select **All Tasks** > **Request New Certificate...**



This will open a window showing the certificates that are offered by the Certificate Authority in the domain. If the CA is offering the type **RAS and IAS Server** then that would be the best type to choose. But a certificate of type **Computer** or of type **Domain Controller** would also be OK.

- Select the type of certificate you want, and click **Enroll**.



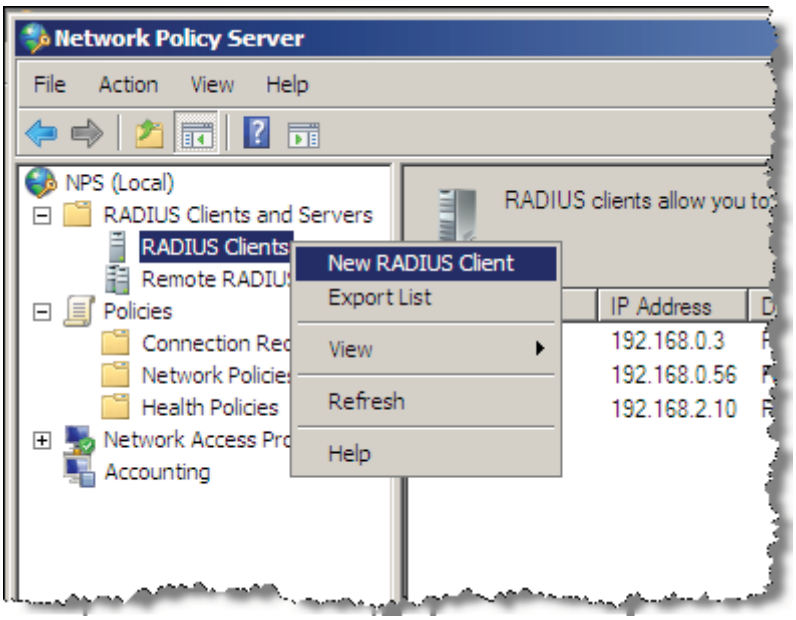
The certificate will be created, and automatically installed into the certificate store on the server.

Adding RADIUS clients to the Network Policy Server

The RADIUS clients are the LAN switches that act as 802.1x, MAC-based or Web-based authenticators to the end-user devices, and use the Network Policy Server as the RADIUS server for those authentications.

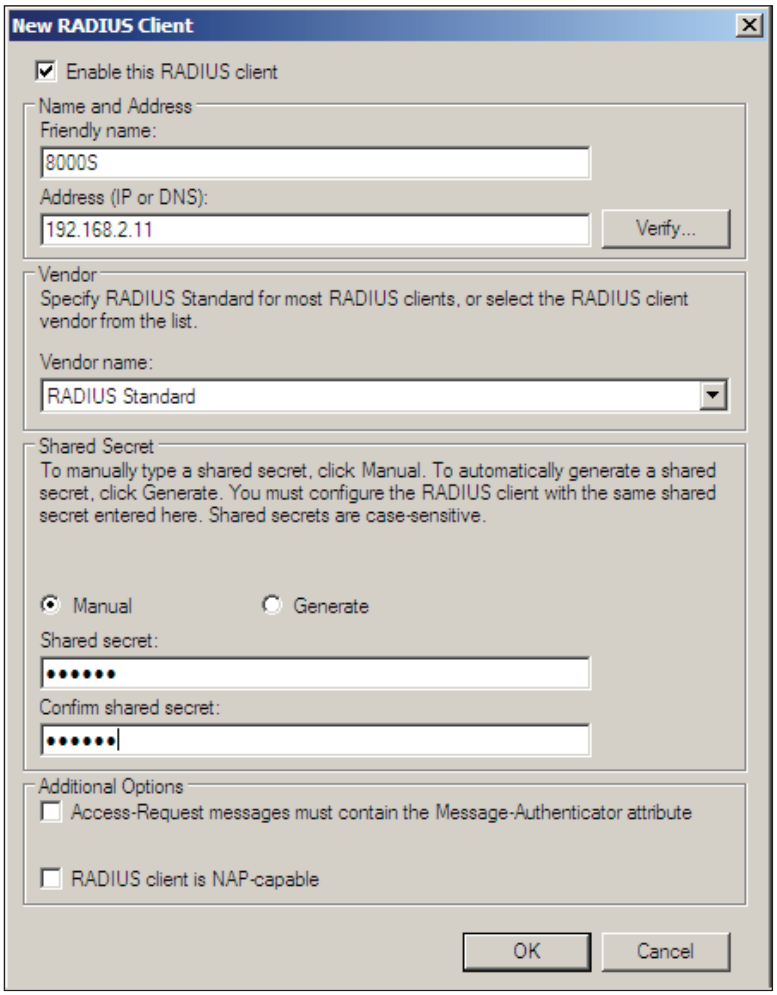
To add a RADIUS client:

- Open the **Network Policy Server Manager**, by choosing **Network Policy ...** from the **Administrative Tools** section of the **Start** menu.
- In the **Network Policy Server** manager, select **RADIUS Clients and Servers**.
- Right-click on **RADIUS Clients**, then select **New RADIUS Client**.



The **New RADIUS client** window opens.

- Fill in the details of the RADIUS client:



- Click **OK**, and the client will be added.
- Add RADIUS client entries for all the switches in the network that will be acting as 802.1x authenticators.

Setting up a Connection Request Policy

Within the Network Policy Server, there are two levels of policies – **Connection Request** and **Network**.

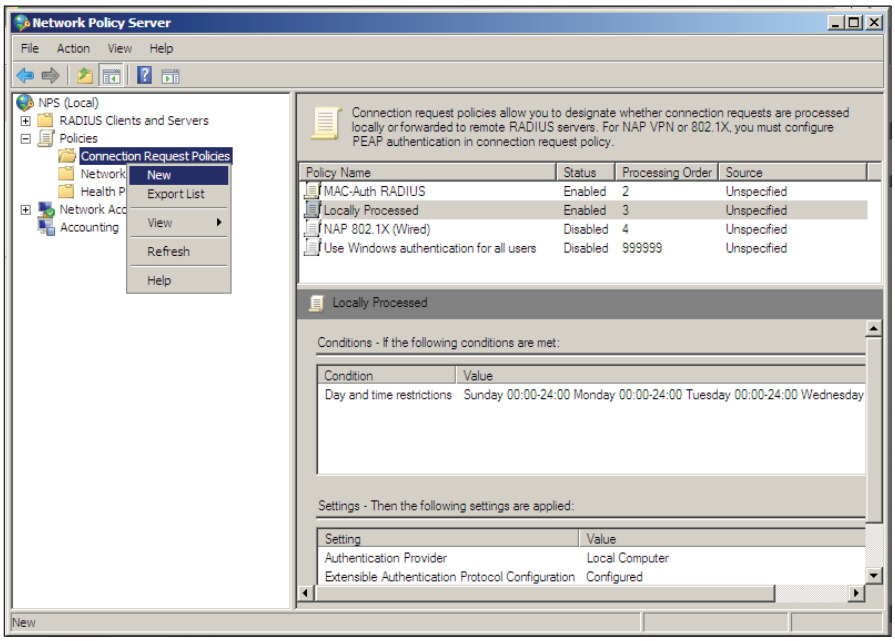
Incoming RADIUS requests are first run through the list of **Connection Request Policies**. This gives the Network Policy Server the ability to operate as a RADIUS proxy, as the Connection Request Policies provide options to process RADIUS requests locally or forward the request to another RADIUS server.

Those RADIUS requests that match the conditions of a **Connection Request Policy**, that specifies local processing, are then passed on to the list of **Network Policies**. The Network Policies specify the authentication method that will be used on requests, and the RADIUS attributes that will be sent out in RADIUS-Accept messages in reply to successful access requests.

In our example, we will create a Connection Request Policy that specifies the local processing of requests.

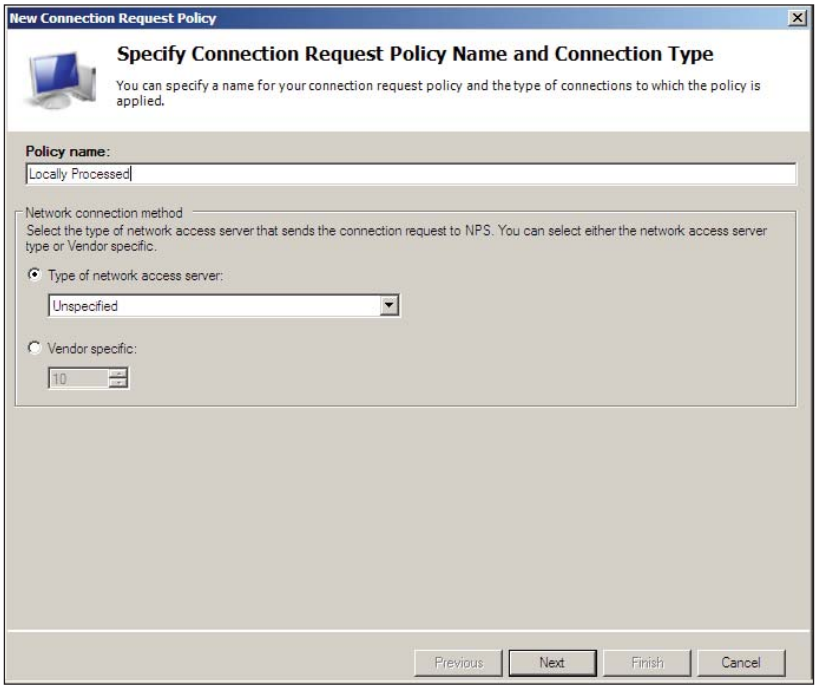
To create a Connection Request Policy:

- Open the **Network Policy Server Manager**, by choosing **Network Policy ...** from the **Administrative Tools** section of the **Start** menu.
- In the **Network Policy Server** select **Policies**, then right-click on **Connection Request Policies** the select **New**.



This will open up the **New Connection Request Policy** wizard. In the opening window of the wizard, type in a **Policy name**.

:



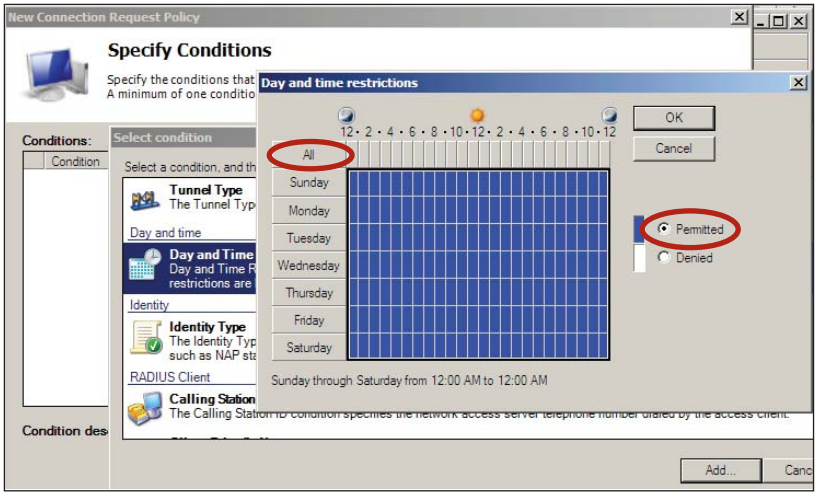
- Click **Next** to move along to the **Specify Conditions** window.

There are actually no specific conditions you need to match with this Connection Request Policy, as this policy will match all requests that reach it. However, the server requires that you specify at least **one** condition.

- Set the **Day and Time Restrictions** condition, to allow the policy to be used all day every day.
- In the **Specify Conditions** window, click **Add…** to open the **Select condition** window. In this window, highlight **Day and Time Restrictions** and click **Add....**

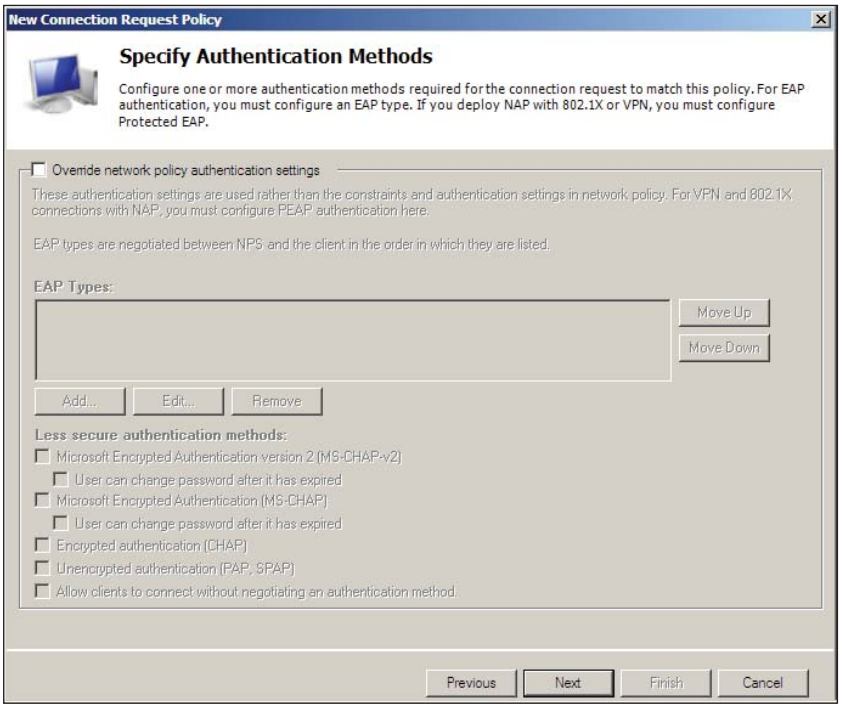
This will open the **Day and time restrictions** window.

- Select **Permitted** then click **All** in the top-left of the Day and Hour table. This should colour all the cells of the table blue.

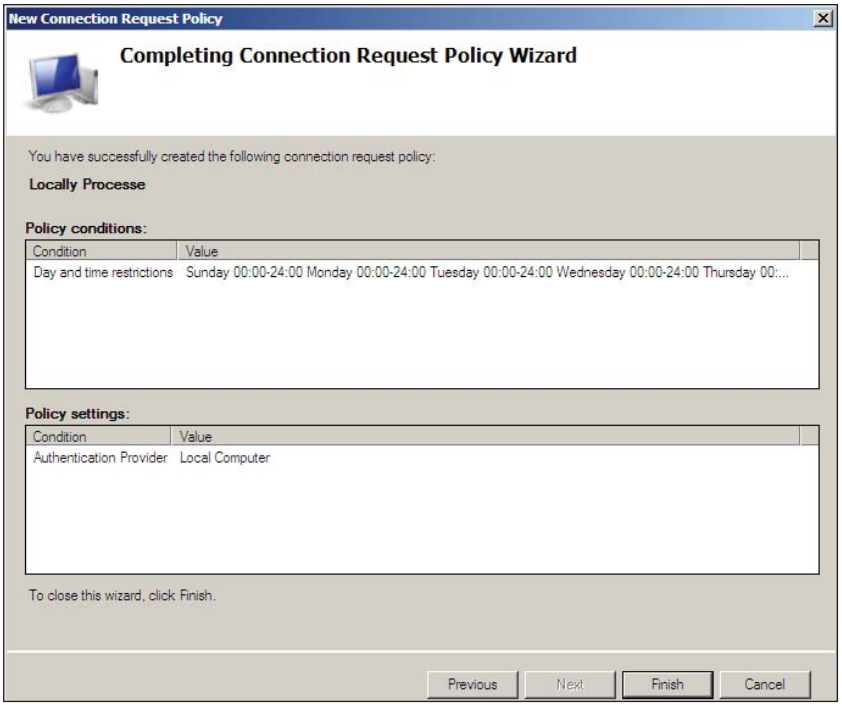


- Click **OK**, and go back to the **Specify Conditions** window.
- Click **Next** twice to move through to the **Specify Authentication Methods** window.

Leave this window in its default, greyed out, state:



- Click **Next** through the remaining windows of the wizard, to complete the new **Connection Request Policy**.



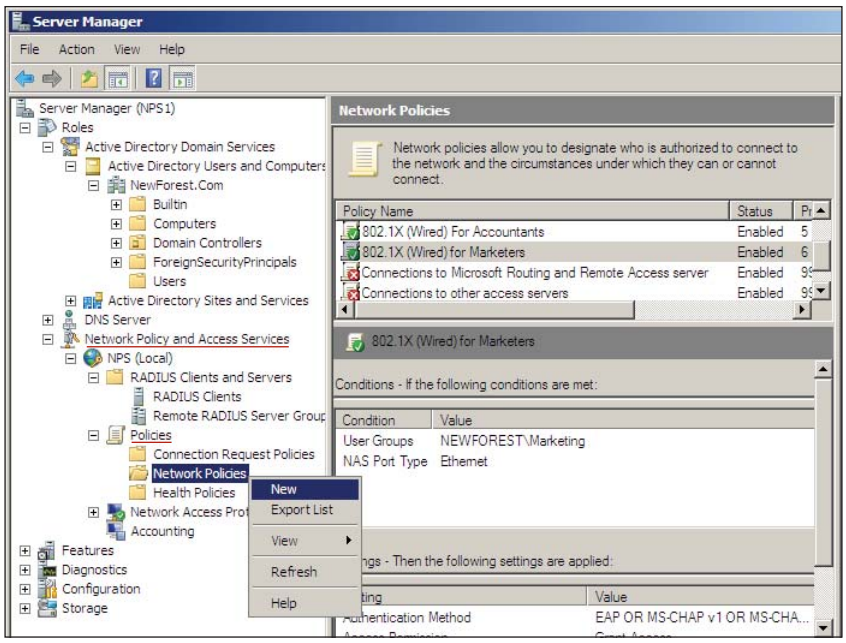
Setting up Network Policies

A network policy is used to identify specific sets of connections to which specific RADIUS attributes will be assigned.

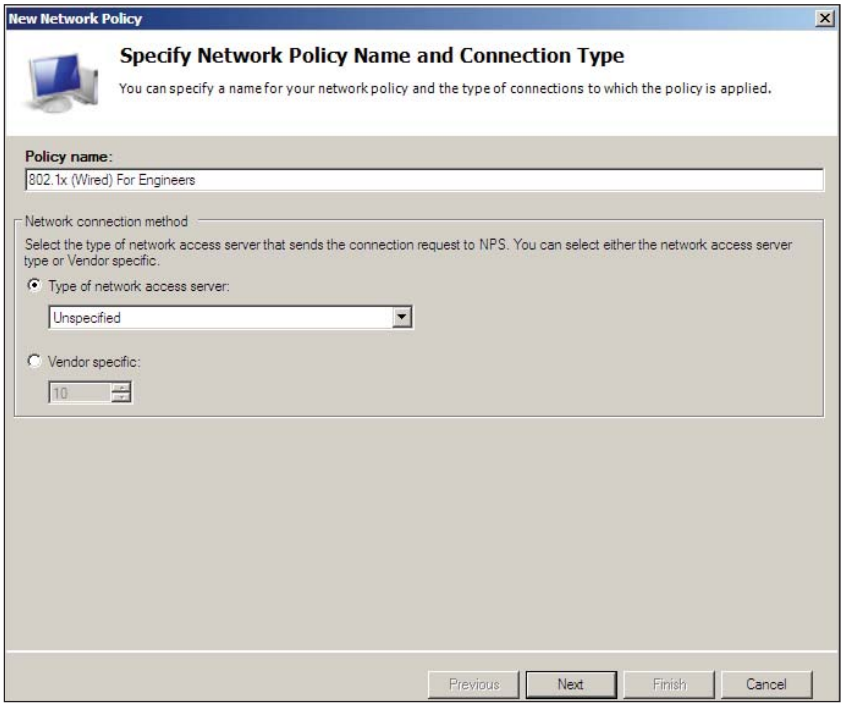
In the example below, we will create a Network Policy for the Engineer users, which will ensure that VLAN ID 20 will be allocated to these users.

To create a Network Policy:

- Select **Network Policies and Access Services** > **Policies** > **Network Policies**, right click and select **New.**



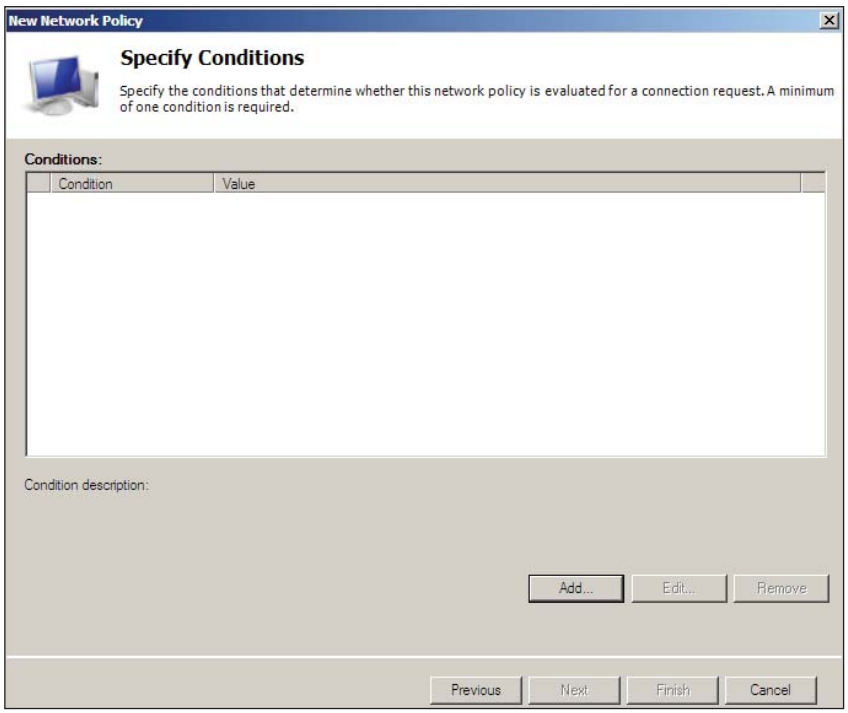
- In the first window of the New Network Policy wizard, type in a **Policy name**, and leave the **Type of network access server** left at **Unspecified**.



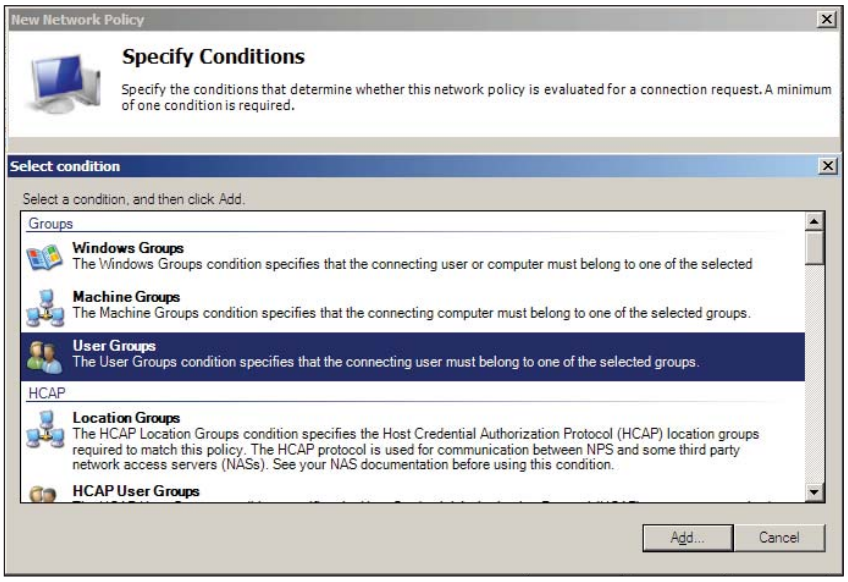
- Click **Next**.

In the **Specify Conditions** window:

- Click **Add...**

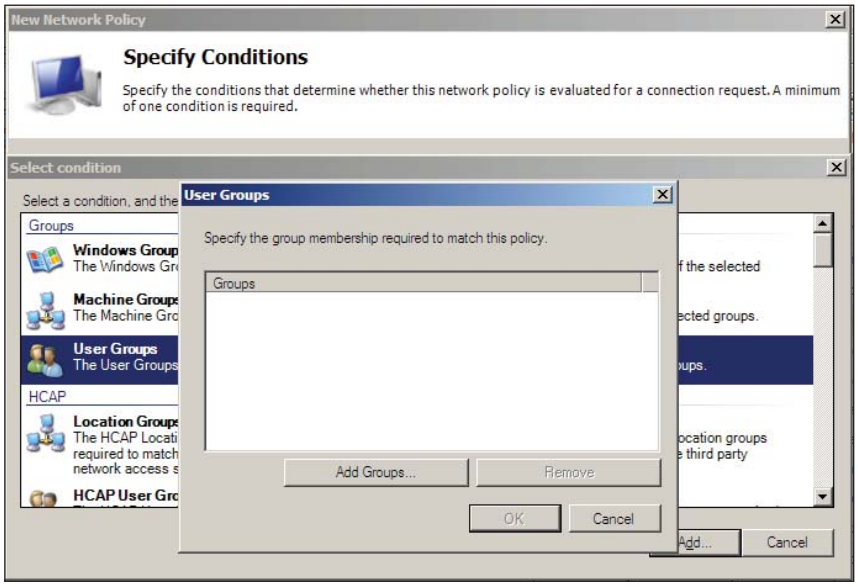


- Select **User Groups**, and click **Add...**



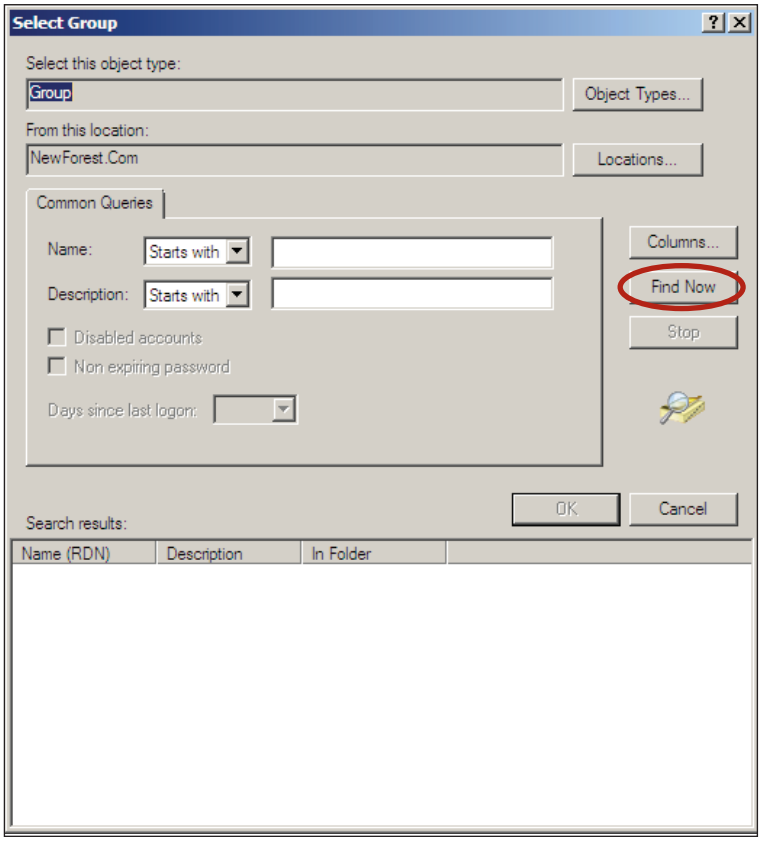
This will open another window into which you can list the groups to add.

- In this window, click **Add Groups...**



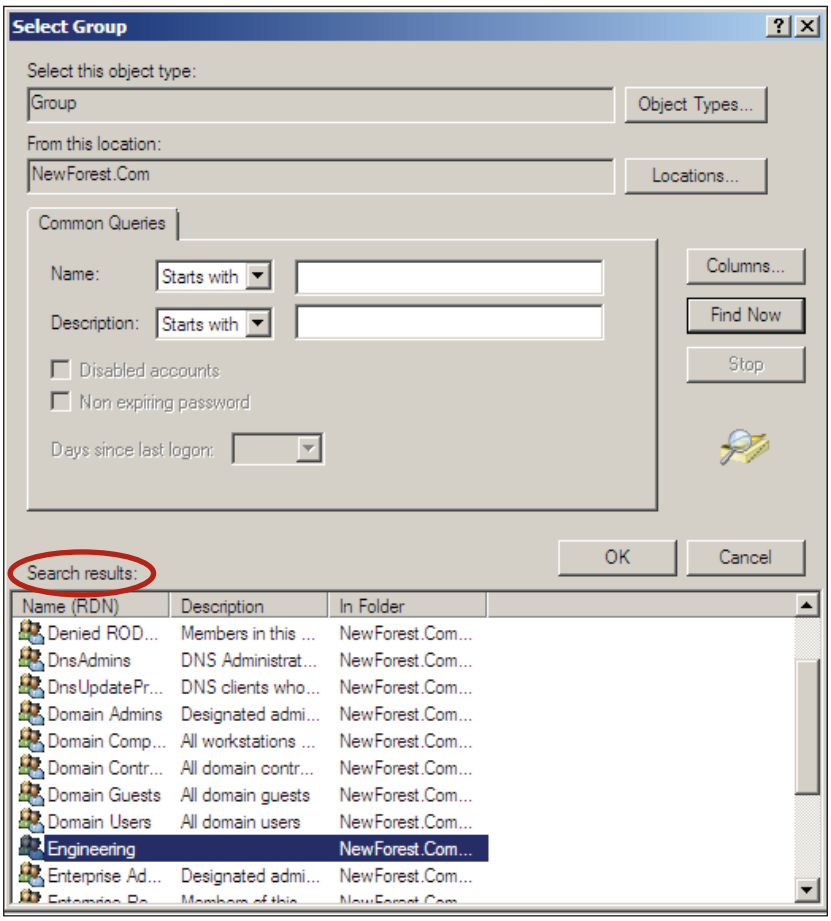
This will open the **Select Group** window.

- Click **Advanced...** to change it to the advanced form, which enables searching for a **Group**.

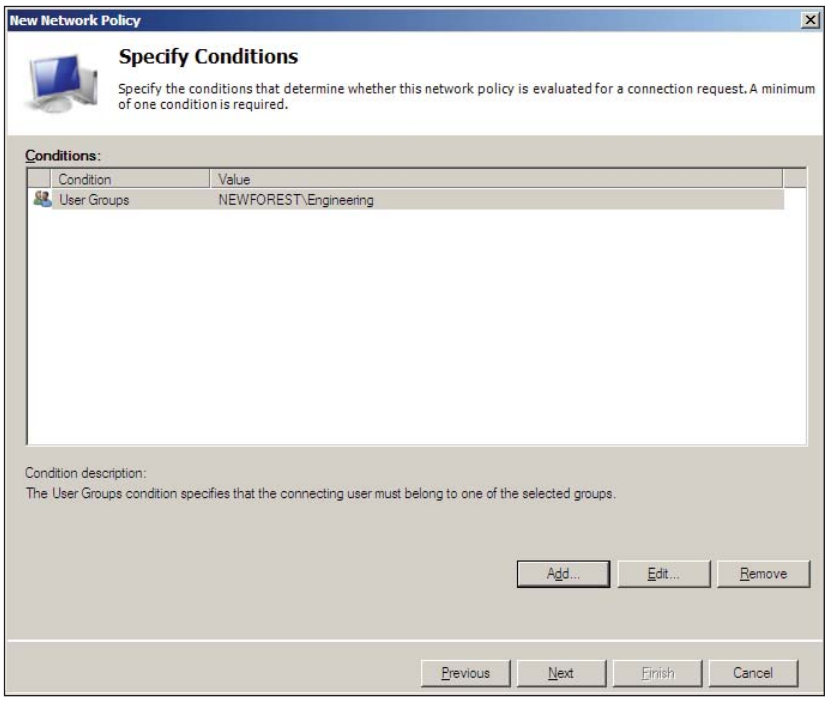


- Click **Find Now**.

- Select **Engineers** from the **Search results:**

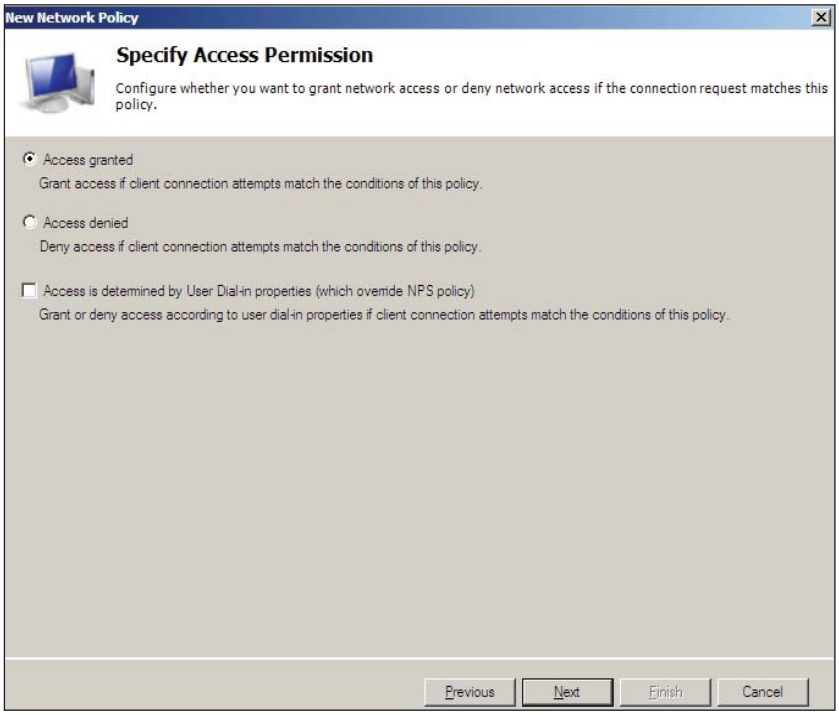


Click **OK** back through the stack of open windows, until you are back at the **Specify Conditions** window of the **New Network Policy** wizard. The newly added condition is displayed. This condition, of course, ensures that the policy will apply only to users who are members of the Engineering group.

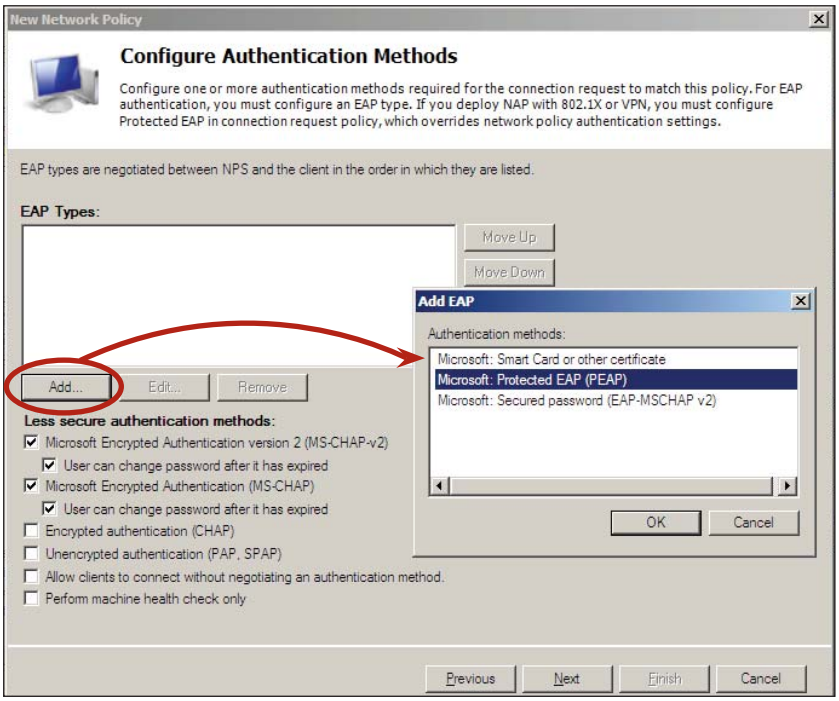


- Click **Next** and move along to the next window in the wizard, where you specify the type of permission that this policy will apply.

In this case, the policy grants access to authenticated users.



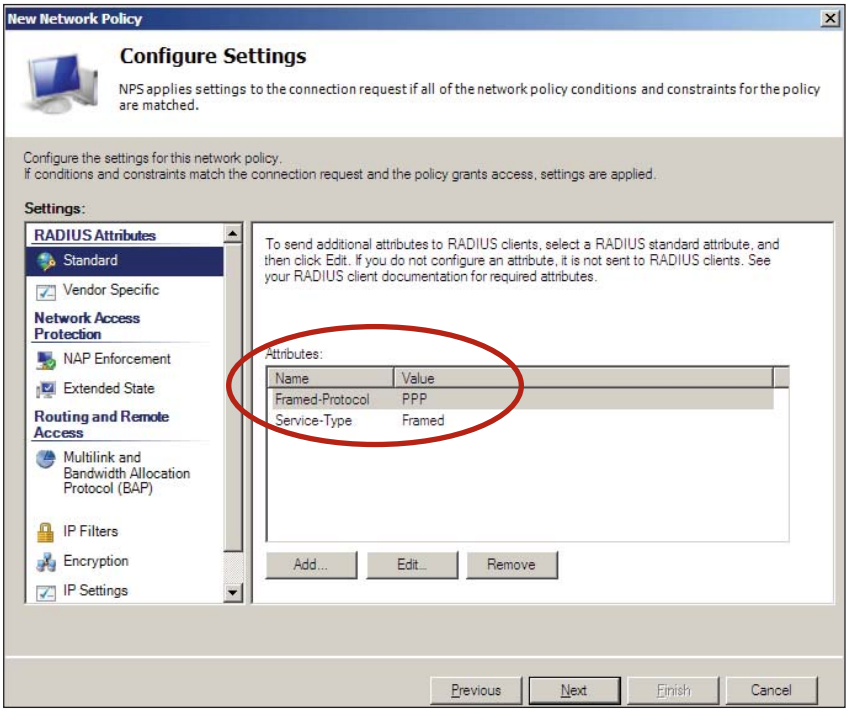
- Click **Next,** to open the **Configure Authentication Methods** window.
- Click **Add...** and choose **Microsoft: Protected EAP (PEAP)** from the list of Authentication methods.



- Click **OK**.
- Click through the **Configure Constraints** window to the **Configure Settings** window.

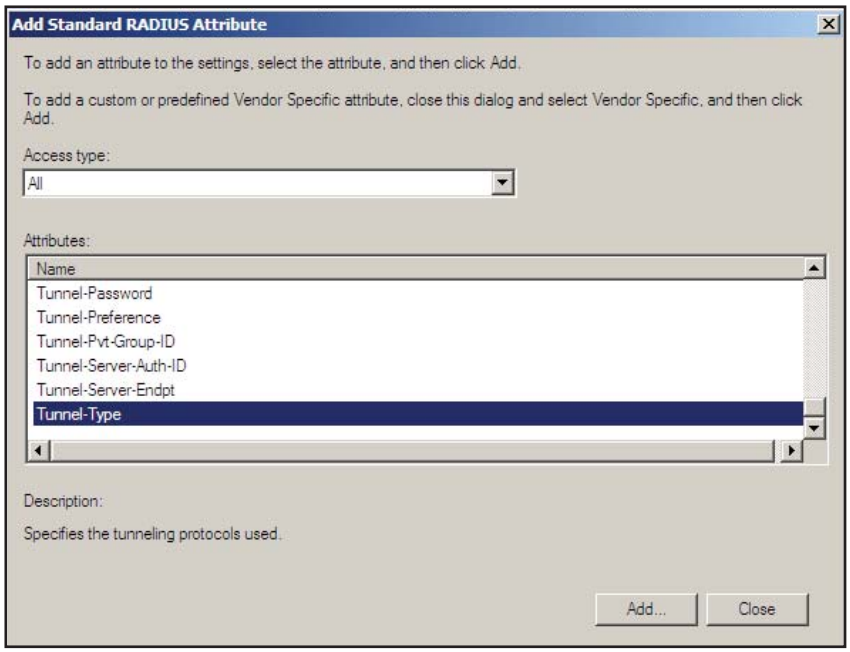
In this window, we will configure the RADIUS attributes that will be sent to authenticated users.

- Select **Standard** under **Radius Attributes** in the left-hand pane.
- Remove the existing, **Service-Type** and **Framed-Protocol**, attributes.



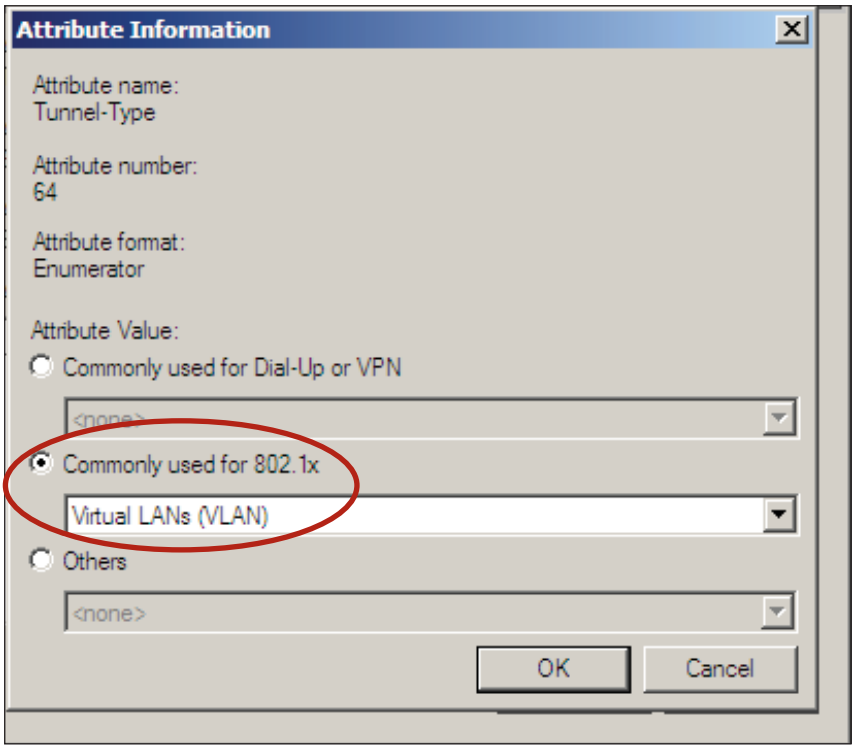
Then proceed to adding new attributes. The first to add is **Tunnel Type**.

- Click **Add...**
- Select **Tunnel-Type** from the list of available attributes.

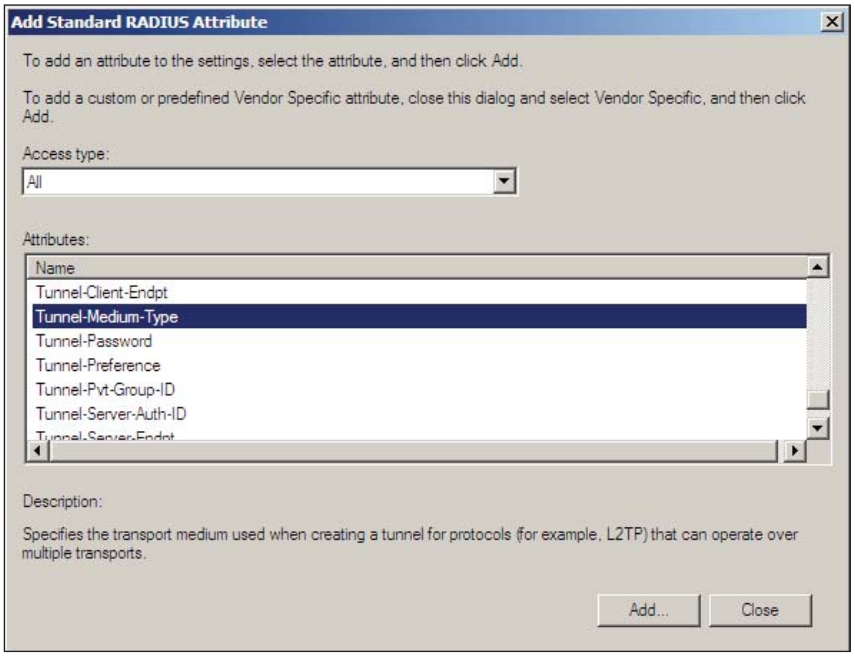


- Click **Add...** the **Attribute Information** window will open.

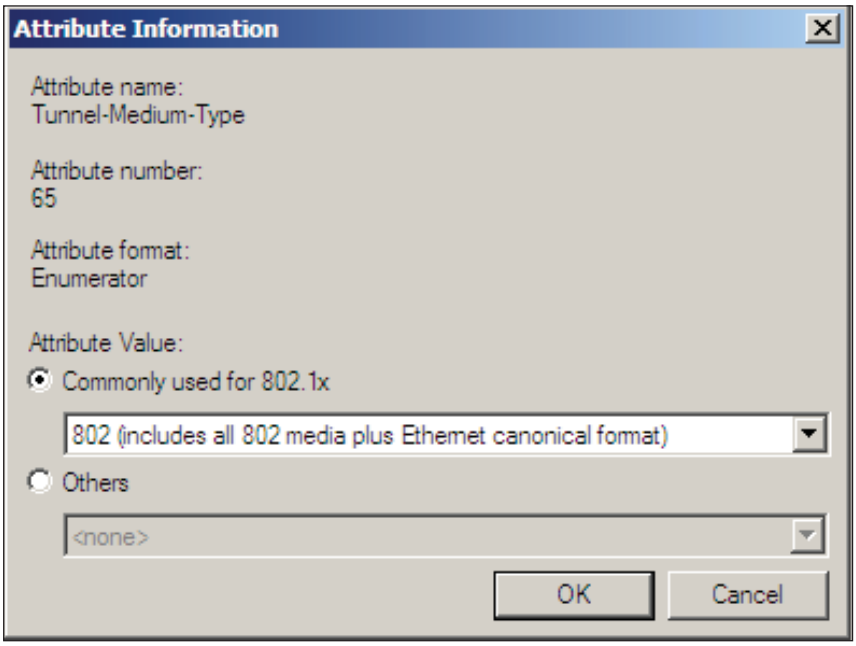
- Click **Add...** in that window to open the window in which you can choose a tunnel type.
- Choose **Virtual LANs (VLAN)**.



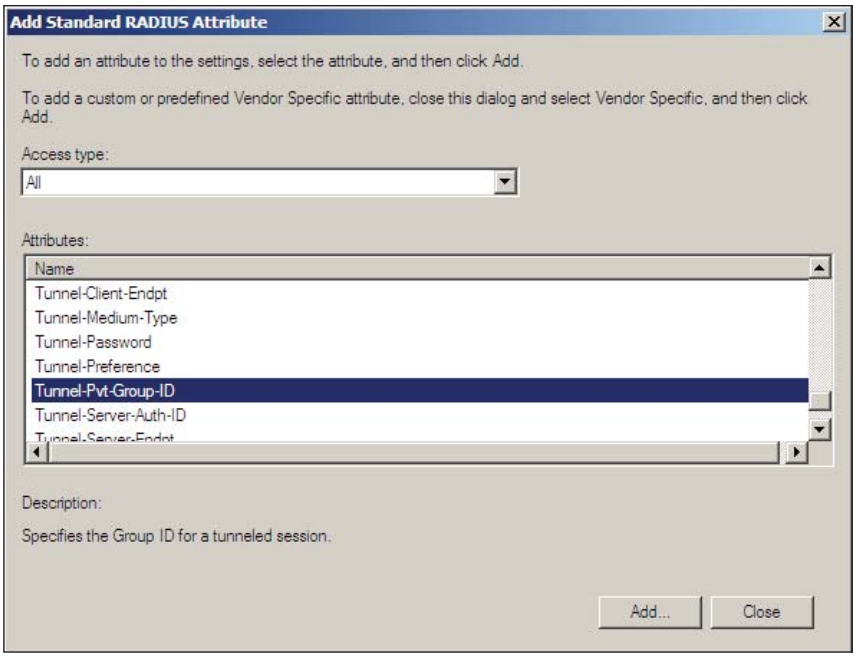
- Click **OK** twice to get back to the **Add Standard RADIUS Attribute** window.
- Click **Add...**
- This time, choose to add the attribute **Tunnel-Medium-Type**.



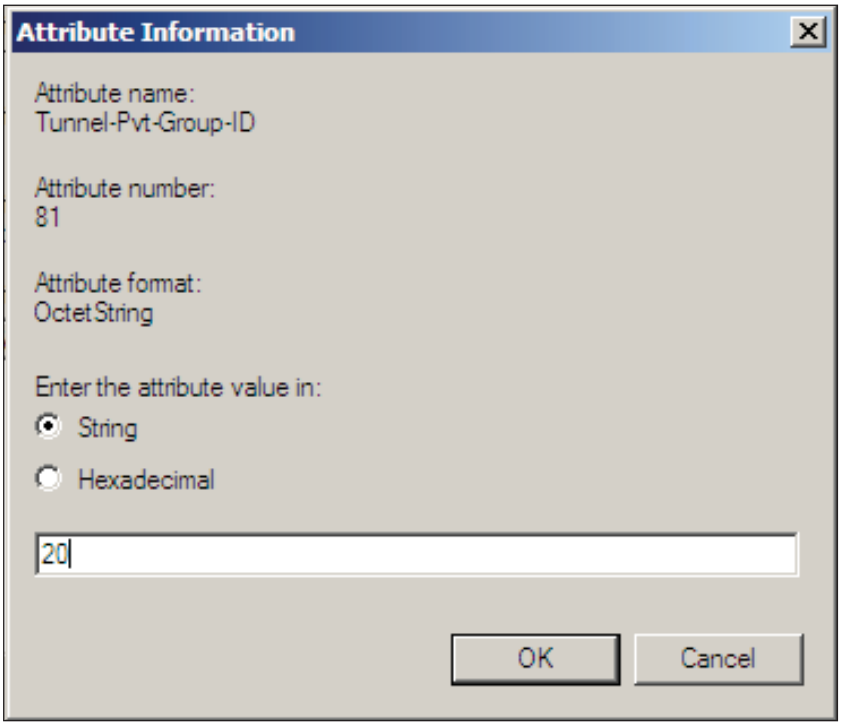
- For this attribute, choose the value **802 (including all 802 media plus Ethernet canonical format)**.



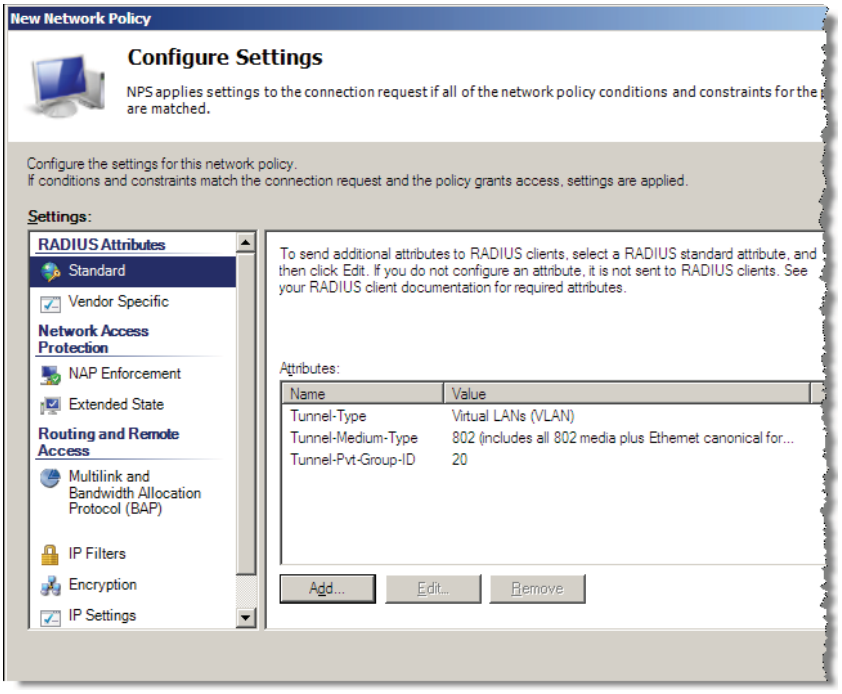
- Click **OK** twice to get back to the **Add Standard RADIUS Attribute** window.
- Click **Add...**
- This time, choose to add the attribute **Tunnel-Pvt-Group-ID**:



- Specify this attribute value as a **String** whose content is the VLAN ID 20.



The RADIUS attributes to send to authenticated users have now been configured.



- Click through the remaining window of the Wizard, and the Network Policy will be added to the Network Policy Server.

With three Network Policies in place – one for Accountants (allocating VLAN ID **10**), one for Engineers (allocating VLAN ID **20**) and one for Marketers (allocating VLAN ID **30**), the Network Policy Server is now ready to authenticate 802.1x supplicants on the LAN.

Setting up Client PCs to perform 802.1x authentication

There are two steps to setting up the Client PCs:

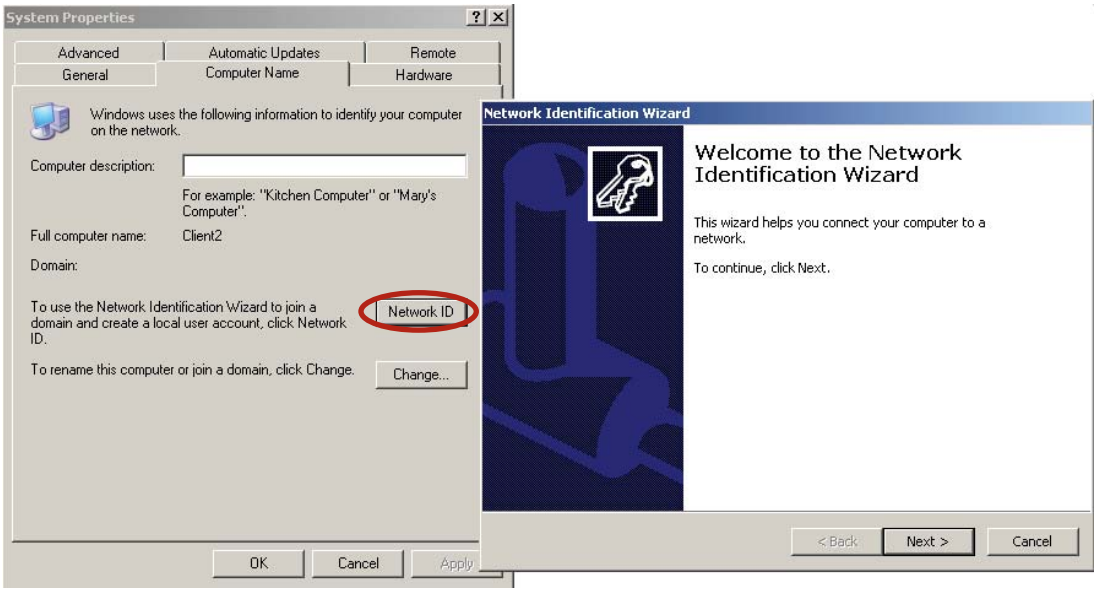
- Join the PCs to the Domain
- Configure the PCs as 802.1x supplicants

Joining the PCs to the domain

This process requires the Client PC to have IP connectivity to the server running Active Directory. Given that the PC is not yet fully configured for 802.1x authentication, this connectivity cannot be provided by an authenticating port on one of the access switches. This process needs to be carried out by connecting the PC to a non-authenticating port somewhere in the network, prior to the deployment of the PC.

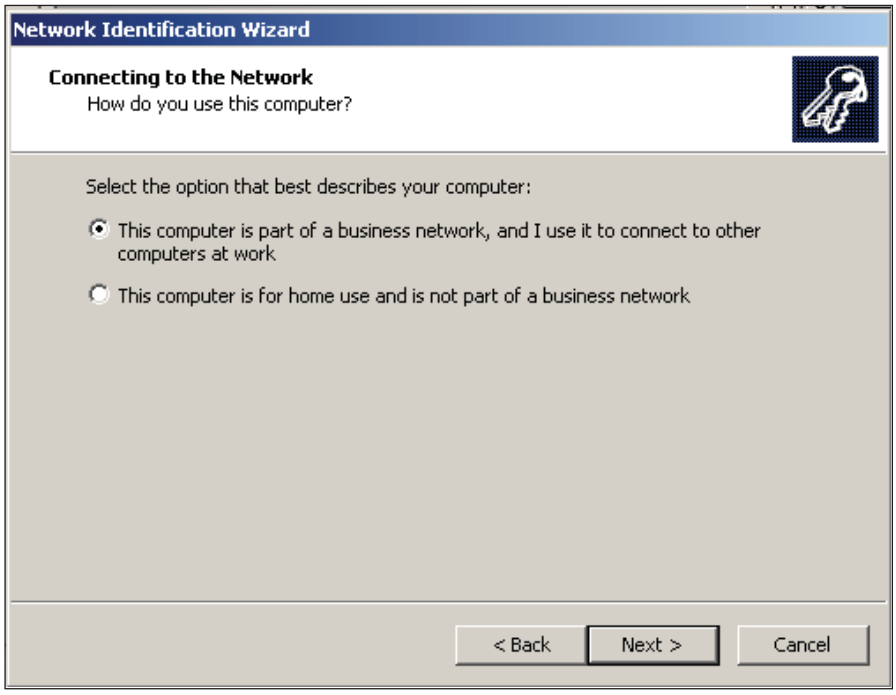
To register a PC on the domain:

- Open **Control Panel** > **System Properties**. In the **System Properties** window, select the **Computer Name** tab.
- Click **Network ID**, to start up the Network Identification Wizard.

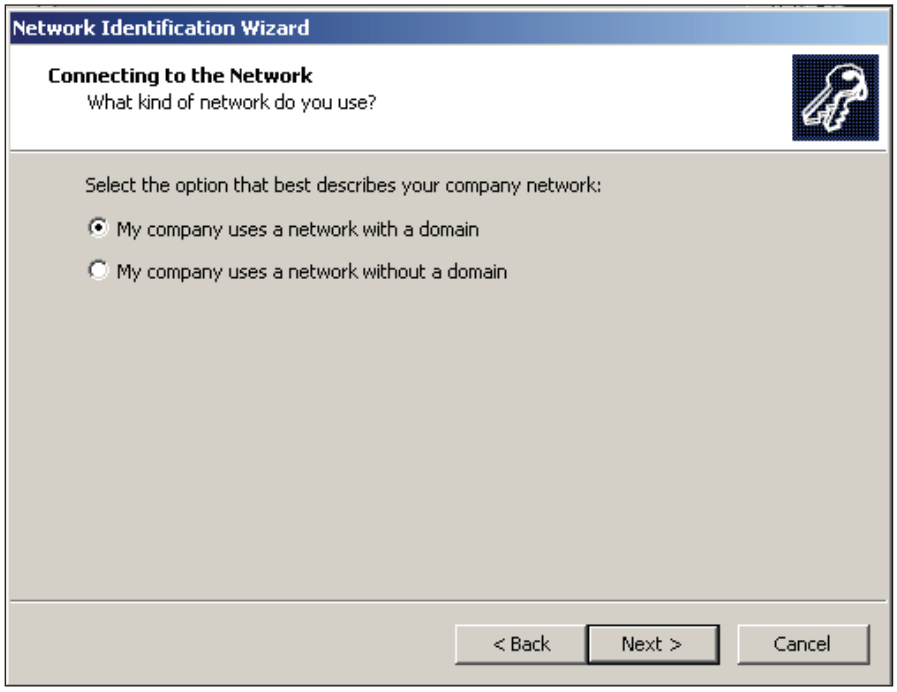


- Click **Next** to open the **Connecting to the Network** window.

- In this window, select **This computer is part of a business network, ...**

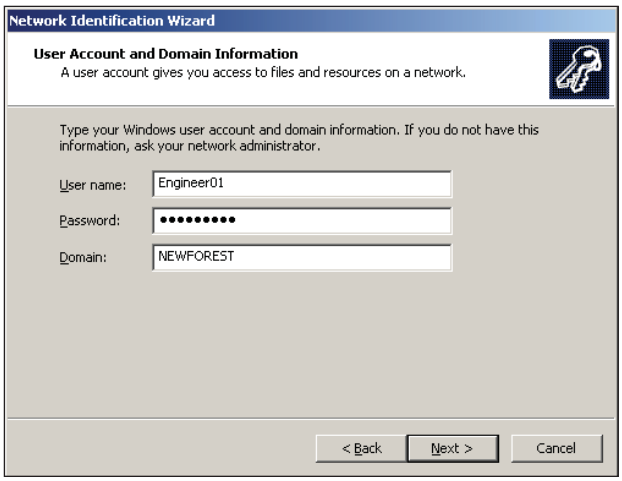


- Click **Next**.
- In the next window, choose **My company uses a network with a domain**.



- Click **Next**.

- In the next window, enter the **User name** and **Password** of the user under which you are logged into the client PC. And specify the name of the Domain you are wishing for the PC to join.



- Click **Next**.

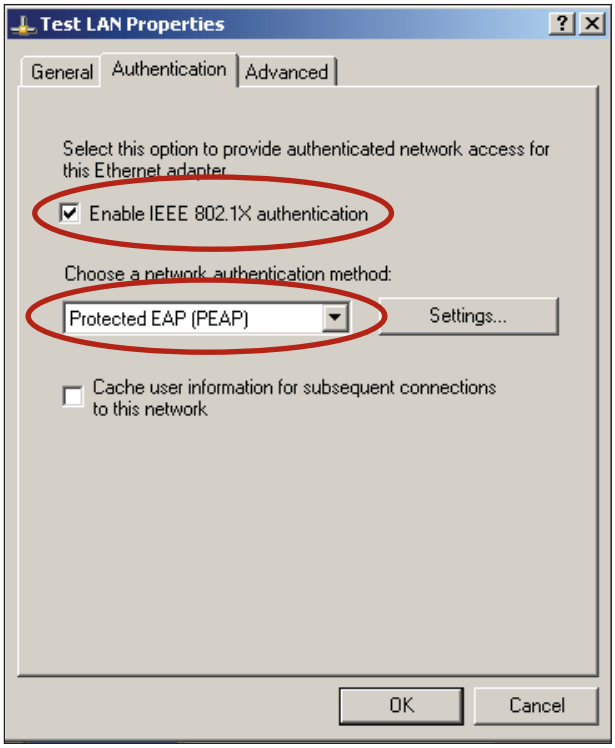
The PC will then proceed to register with the domain, and prompt you to reboot in order to complete the process.

Configuring the PC as an 802.1x supplicant

To set up a PC to operate as an 802.1x supplicant, you need to configure the properties of the NIC card via which it connects to the network.

To configure the PC as an 802.1x supplicant:

- Open the **Properties** window of the NIC card in question.
- Click on the **Authentication** tab in the **Properties** window box.
- Tick the check box labelled **Enable IEEE 802.1X authentication**.
- In the **Choose a network authentication method** combo box, select **Protected EAP (PEAP)**.
- Click **Settings...** to open the **Protected EAP Properties** window.



- In this window, untick the check box beside **Validate Server Certificate** (we will discuss the validation of the server certificate later, when considering certificate-based authentication).
- In the **Select Authentication Method** combo box, choose **Secured Pasword (EAP-MSCHAP v2)**.
- Click **Configure...**beside that Combo box. In the resulting **EAP MSCHAPv2 Properties** window, ensure that the check box is ticked.

With this check box ticked, the PC will not need any user intervention in order to carry out 802.1x authentication. If the check box is not ticked, the PC will open a window asking for a username/password every time it needs to perform 802.1 x authentications. This is a particular problem at the time when the PC is logging into the network. It cannot log into the network until the network connection has been authenticated, but if it needs user input to authenticate the connection, it cannot proceed at login time, as the request for user input cannot be popped up at login time.

- Click **OK** on all the open windows, and the configuration is complete.

Performing 802.1x authentication

With the switch, server, and the client PC all configured as described above, 802.1x authentication should now proceed successfully. As the PC connects to the switch, the switch will request 802.1x authentication credentials from the PC by EAPOL, and pass them through to the NPS server by RADIUS. If the credentials match a username/password (in an appropriate Group) stored in the Active Directory user database, then the NPS server will indicate that the user is accepted, via a RADIUS accept message. The RADIUS accept message will also include the attributes (configured on the NPS Network Policy) that inform the switch which VLAN ID to dynamically configure on the port where the client PC has connected.

The switches provide commands that enable you to see that authentication has succeeded.

On the **x600**, the command is **show dot1x supplicant interface <port name>** which provides output like:

```
Triple-Auth#show dot1x supplicant int port1.0.13
Interface port1.0.13
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    WebBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

  Supplicant name: Engineer01
  Supplicant address: 0002.b363.319f
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 9
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 8
    CD: adminControlledDirections: both - operControlledDirections: both
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 20
```

Also the command **show VLAN <VID>** will show that the supplicant's port has been dynamically added to the correct VLAN.

```
Triple-Auth#show vlan 20

VLAN ID  Name             Type    State   Member ports
                                          (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ===================================
20       Engineering      STATIC  ACTIVE  port1.0.13(u)
```

On the 8000S, the commands are **show dot1x ethernet<port name>** and **show vlan**

```
console# show dot1x ethernet 1/e1
```

802.1x is enabled

```
         Admin              Oper          Reauth   Reauth     Username
Port     Mode               Mode          Control  Period
-------- ------------------ ------------- -------- ---------- -----------------
1/e1     Auto               Authorized    Disabled 3600       NEWFOREST\Engineer01


Quiet period:            60 Seconds
Tx period:               30 Seconds
Max req:                 2
Supplicant timeout:      30 Seconds
Server timeout:          30 Seconds
Session Time (HH:MM:SS): 00:00:27
MAC Address:             00:02:b3:63:31:9f
Authentication Method:   Remote

Termination Cause:       Not terminated yet

Authenticator State Machine
State:                   AUTHENTICATED

Backend State Machine
State:                   IDLE
Authentication success:  11
Authentication fails:    7


console# sh vlan

Vlan       Name                 Ports                Type     Authorization

---- ---------------- -------------------------- ------------ -------------
 1           1         1/e(2-5,7-48),1/g(1-4),       other       Required
                       2/e(1-48),2/g(1-4),
                       3/e(1-48),3/g(1-4),
                       4/e(1-48),4/g(1-4),
                       5/e(1-48),5/g(1-4),
                       6/e(1-48),6/g(1-4),ch(1-8)
 2           2                1/e(23-24)         permanent     Required
 10         10                1/e(23-24)         permanent     Required
 20         20               1/e(1,23-24)        permanent     Required
 30         30                1/e(23-24)         permanent     Required
 40         40                1/e(23-24)         permanent     Required
 50         50                1/e(23-24)         permanent     Required
```

802.1x Authentication with Certificates

Up until now, we have considered authentication using Username and Password. However, even more secure authentication can be achieved using digital certificates.

To enable the authentication to be carried out using certificates, three steps need to be carried out:

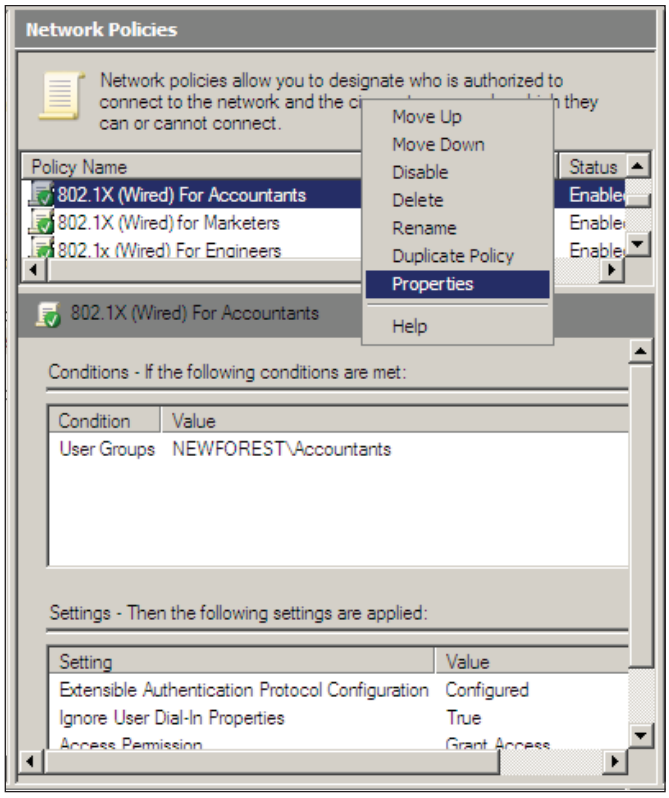
- The users on the network need to obtain certificates.
- The 802.1x configuration on the end devices needs to be changed to use cetificate authentication.
- The Network Policies on the Network Policy Server need to be altered to accept certificate authentication.

Configuring Policies on the Network Policy Server to use certificates

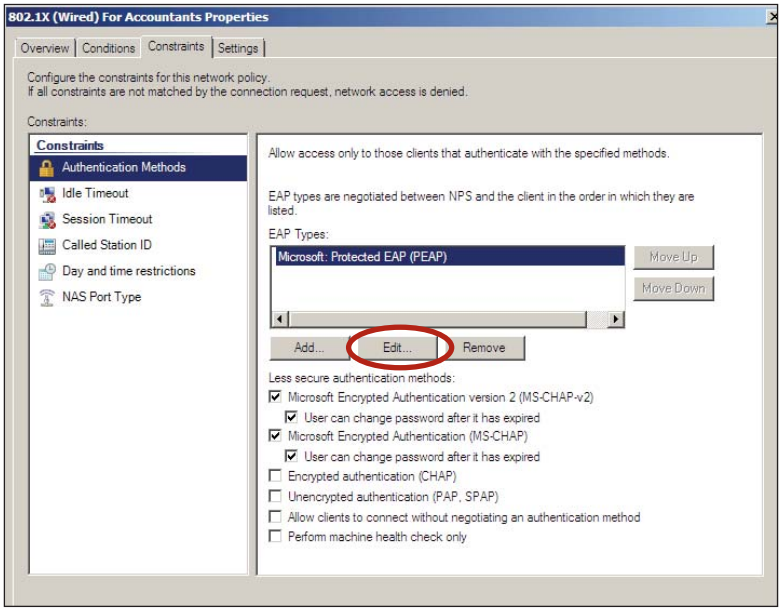
The Network Policies defined within the Network Policy server need to be edited to accept authentication by Certificates.

In the example below, we will edit the **Accountants** Network Policy.

In the **Server Manager** window, right-click on the policy, and choose **Properties**.



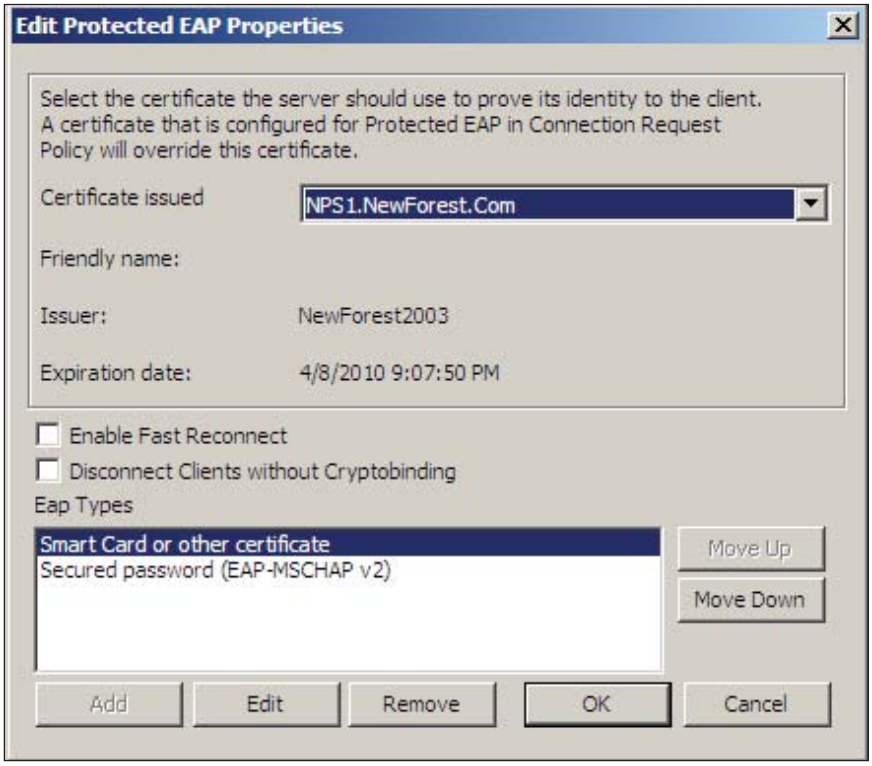
- In the **Properties** window, open the **Constraints** tab.
- Select **Authentication Methods**
- In the **EAP Types** list, select **Microsoft: Protected EAP (PEAP)** and click **Edit...**



The **Edit Protected EAP Properties** window opens.

- Click **Add** and choose **Smart Card or other certificates** from the **EAP Types** list.
- Then, move this option to the top of the list using the **Move Up** button.

Note that the **Certificate issued** listed in the upper half of this window is the Server Certificate that has been issued to this server, **NPS1.NewForest.Com**.



For flexibility, you can leave the option Secured password (EAP-MSCHAP v2) in the list, as that will enable the Connection Request Policy to accept connections from client PCs using Certificates or from client PCs using username/password. However, if you want to enforce a policy whereby client PCs *must* use certificates, then remove the Secured password (EAP-MSCHAP v2) option from the Eap Types list.

Setting up the client PC to perform Certificate Authentication

There are three steps required to set up the client PCs to perform Certificate Authentication

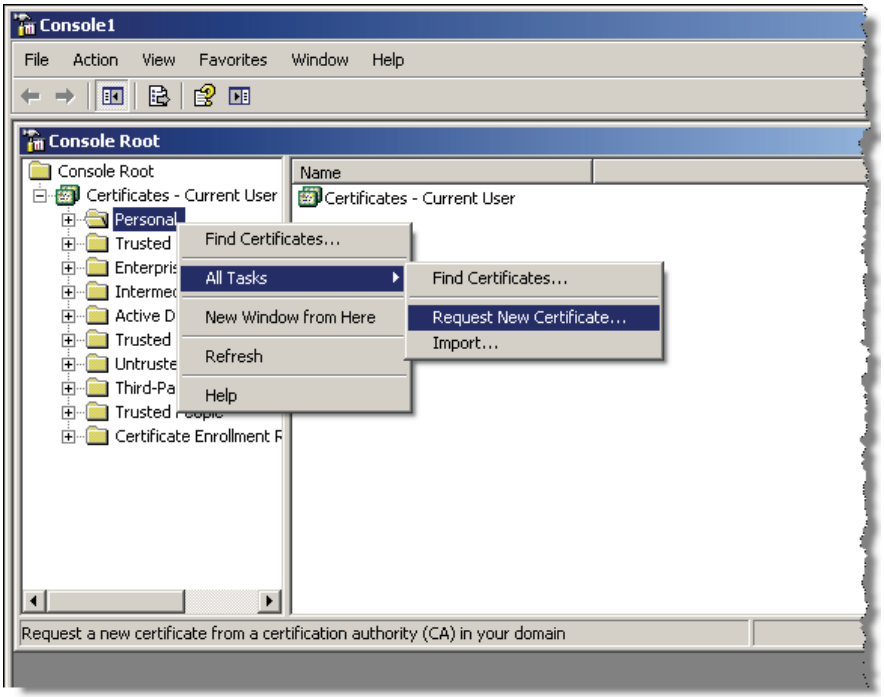
- Obtain user certificates
- Download the Certificate Authority server's Root certificate
- Set up the NIC card to perform authentication by certificate

Obtain user certificates

All users who will use the PC need certificates that can be used for authentication.

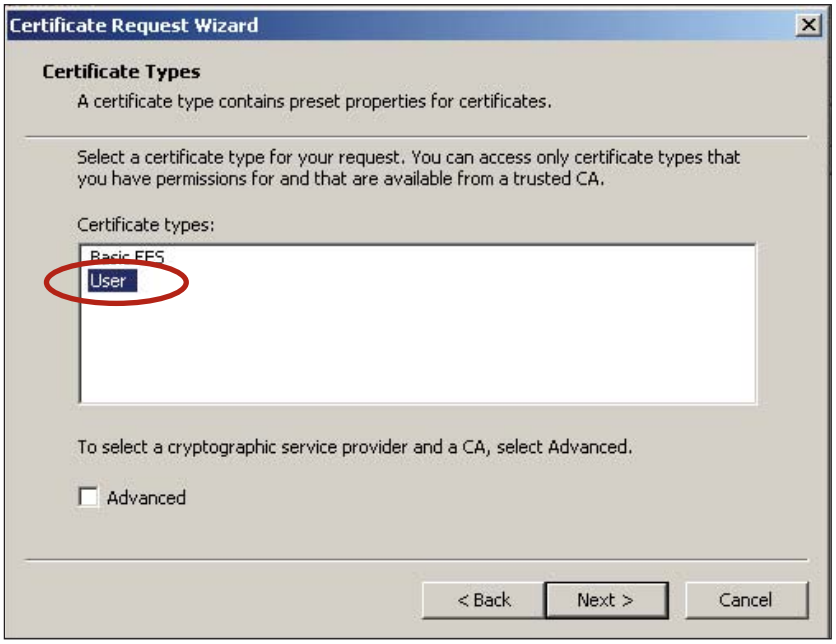
To obtain a user certificate from the Certificate Authority:

- Open the console on the client PC (by running mmc). Add the Certificates Snap-in to the console. Select **Certificates – Current User > Personal**, right-click and select **All Tasks > Request New Certificate...**

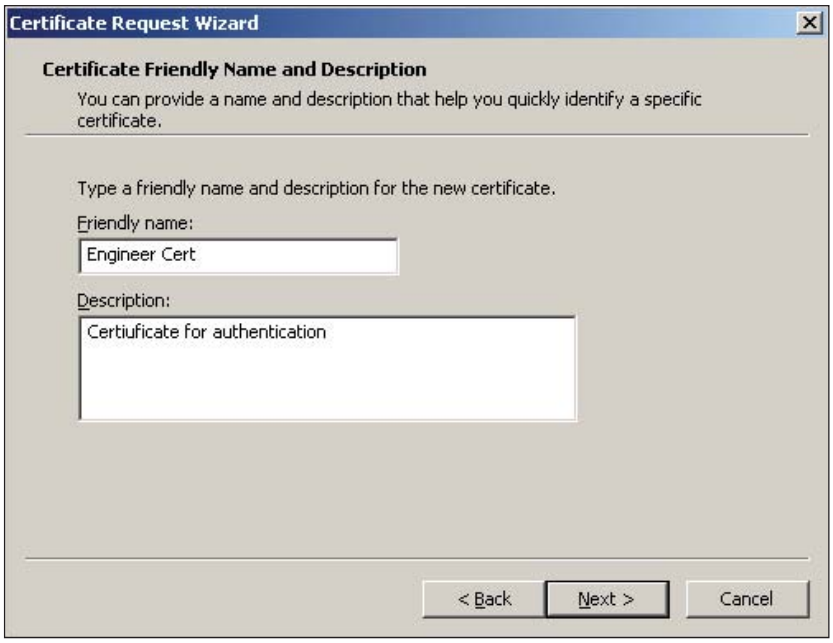


This will open the Certificate Request Wizard:

- Click **Next >** to open the **Certificate Types** window.
- In this window, choose **User**.



- Click **Next >** to open the **Certificate Friendly Name and Description** window.
- Type in an appropriate **Friendly Name** and **Description**:



- Click through the remaining windows of the wizard, the certificate will be created and installed.

Download the Certificate Authority server's Root certificate

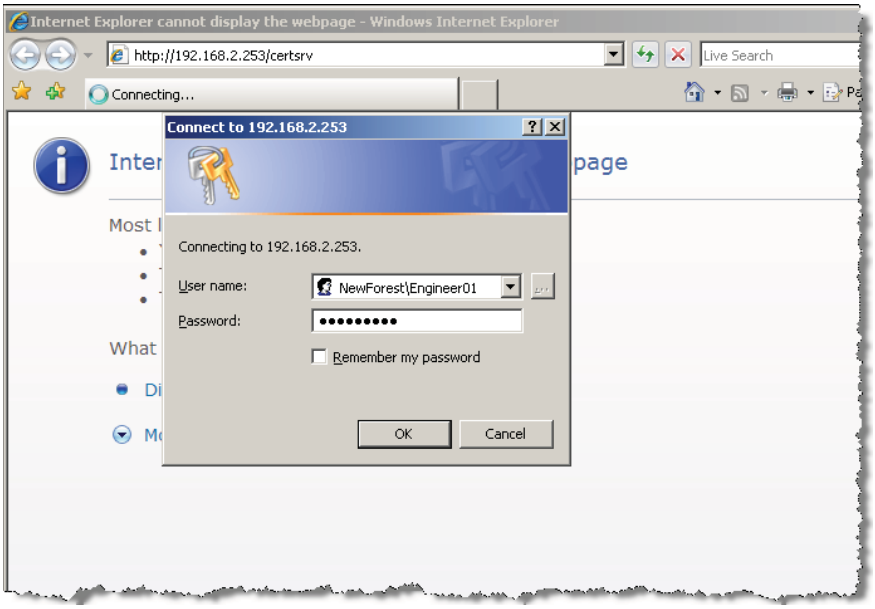
This step is only necessary if you wish to enable the option whereby the Client PC validates the server's certificate (this is described below in the section "Set up the NIC card to perform authentication by certificate" (page 49)). It is advisable to **enable** this option, as it increases the security of the overall solution with very little overhead.

The reason that the Certificate Authority's certificate is required for this option is that the NPS server was issued its certificate by the Certificate Authority. In order for the client PC to validate the server's certificate, it must trust the entity that issued the certificate. One way to enable the client PC to trust the Certificate Authority is for the client PC to have a copy of the Certificate Authority's own root certificate.

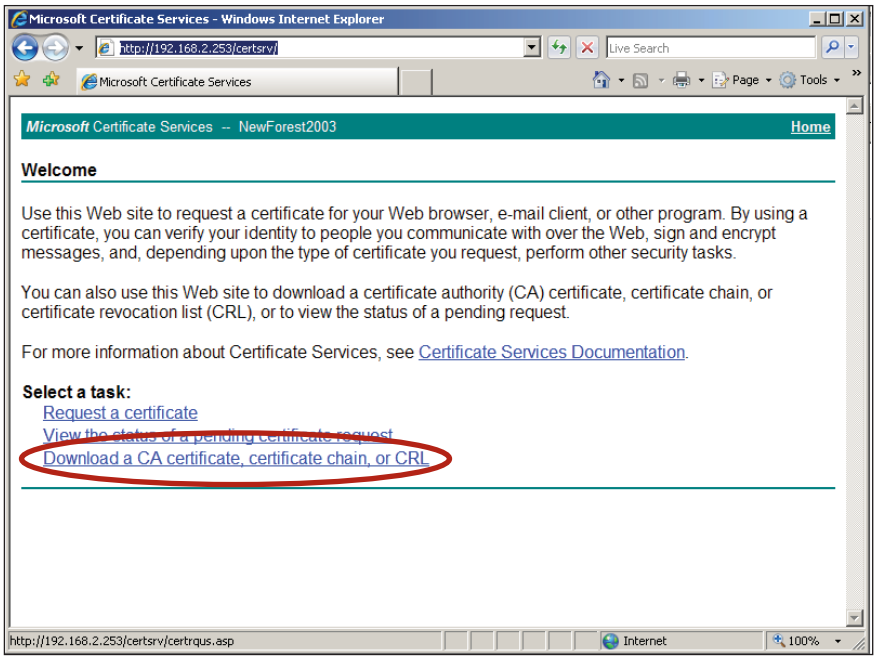
Probably the most convenient way to obtain the Certificate Authority's root certificate is to use the Certificate Authority's Web interface.

- On the client PC, browse to ***http:/<certificate authority's IP address>/certsrv***

You will be challenged for a username and password to log into the certificate server. Provide the same username and password as you are currently logged into the client PC with. Note that you may need to prefix the username with the name of the windows domain (**NewForest** in this case).

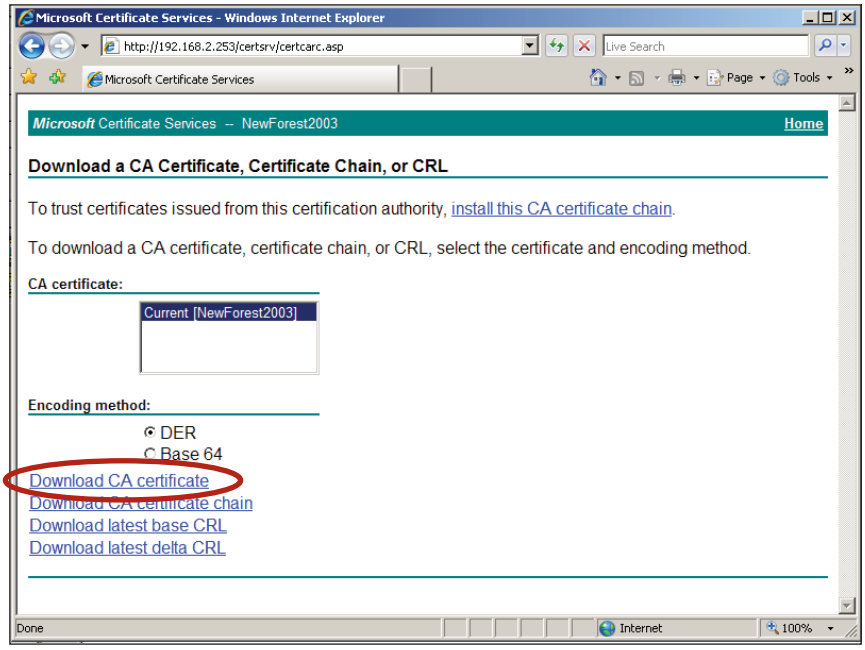


- Having logged in, you will be presented with the opening page of the certificate server. In this page, click on the link **Download a CA certificate, certificate chain, or CRL**.

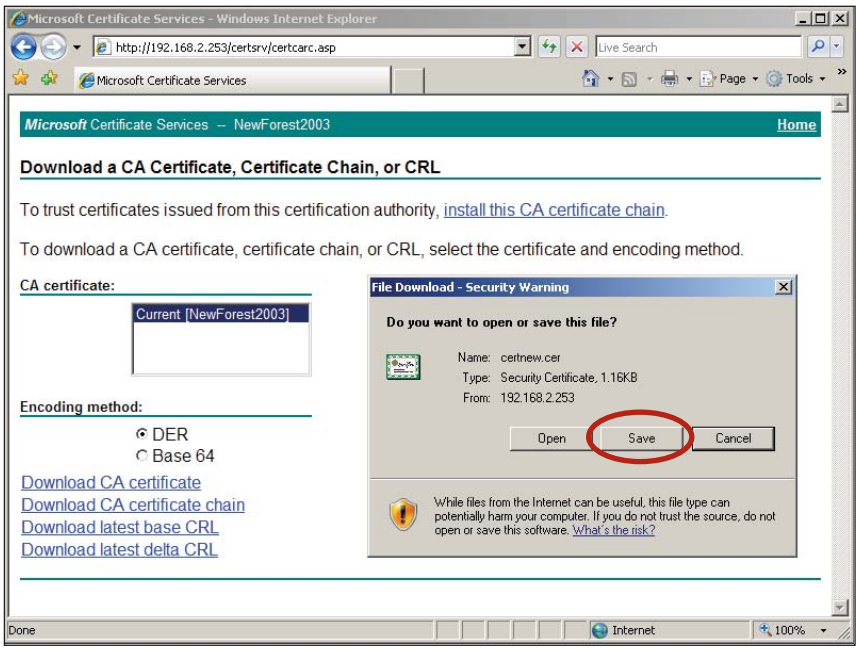


That will take you to the **Download a CA certificate, certificate chain or CRL** page.

- Click the link **Download CA certificate**

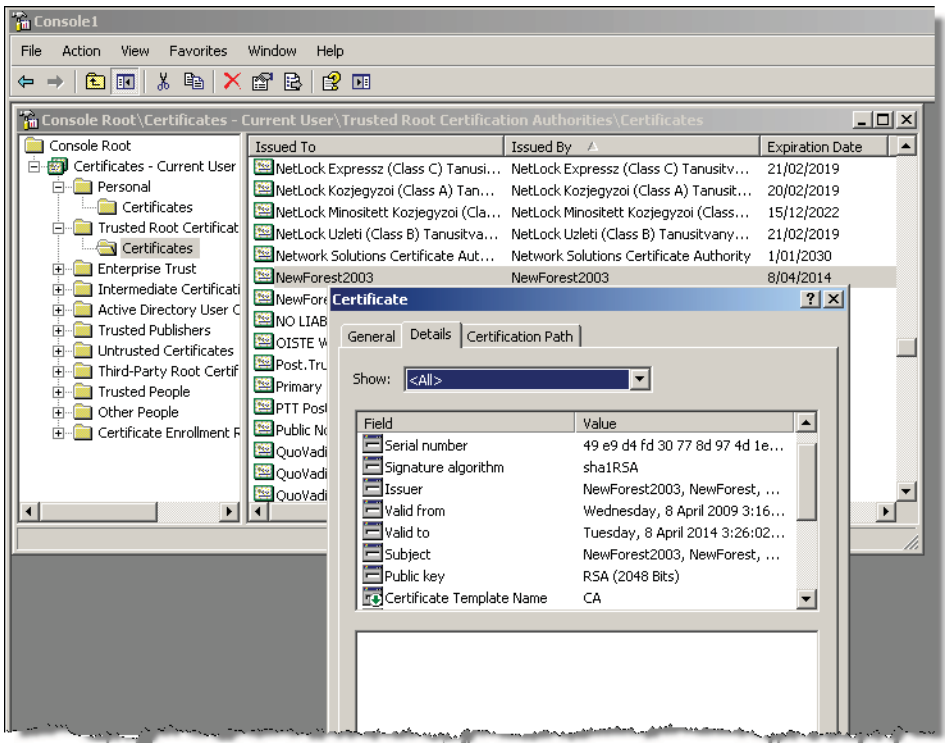


- You will then be offered the opportunity to open or save the certificate. Choose to **Save** it.



- Click **Yes** on the next question.

The Certificate will then be saved, and you will be able to view it under **Trusted Root Certificates** in the Certificates snap-in of the Windows Console.

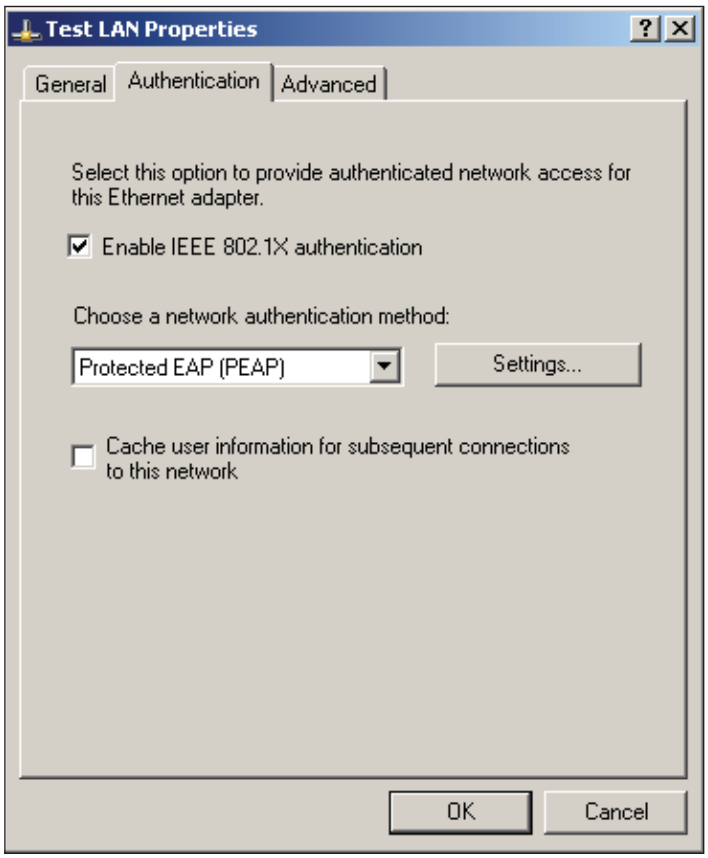


Set up the NIC card to perform authentication by certificate

To setup the NIC card:

- Open the **Properties** window for the NIC card in question.
- Click on the **Authentication** tab.

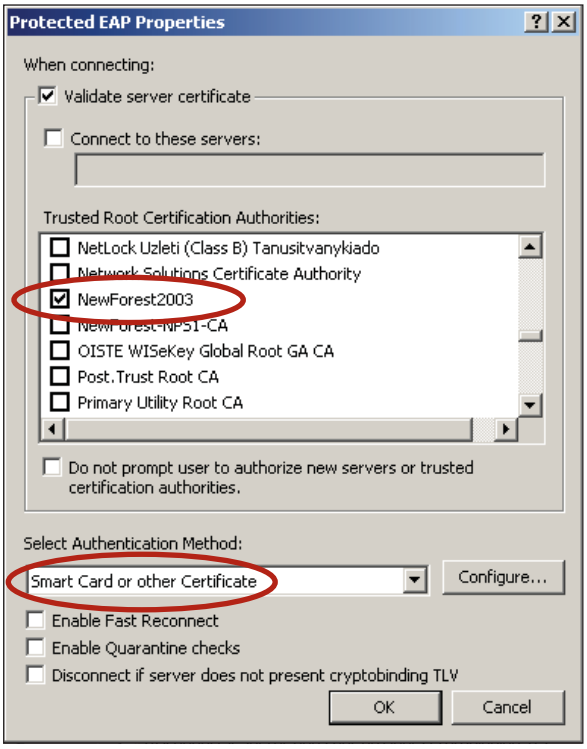
The settings described earlier in the section **Configuring the PC as an 802.1x supplicant** (page 38) will be displayed as shown below:



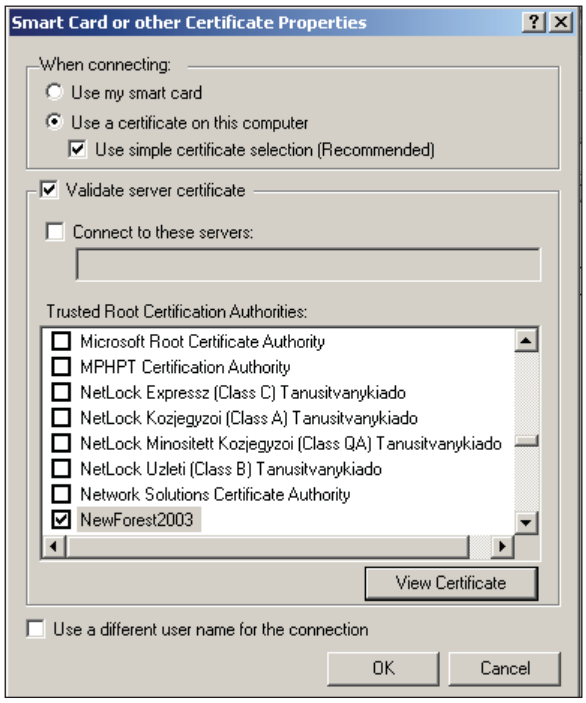
- Click on the **Settings...** button beside **Protected EAP (PEAP)**. This will open the **Protected EAP Properties** window.

In this window

- Tick the **Validate Server Certificate** check box
- In the **Trusted Root Certification Authorities** ListBox, scroll down until you find the name of your Windows domain's Certificate Authority Server (in this case NewForest2003). This Certificate Authority will appear in the list only if you have carried out the process described above in **Download the Certificate Authority server's Root certificate**. Tick the Check box beside this Certificate Authority.
- In the **Select Authentication Method** combo box, choose **Smart Card or Other Certificate**



- Click **Configure...**



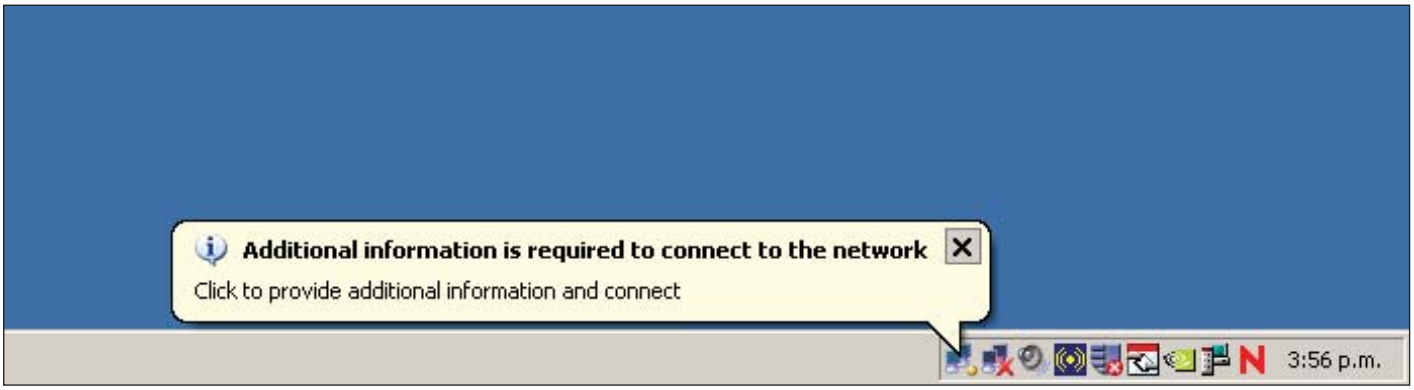
- In the **Smart Card or other Certificate Properties** window select:
  - **Use a certificate on this computer**
  - **Use simple certificate selection**
  - **Validate server certificate**

Once again, tick the check box beside the CA of your Windows domain in the list of Trusted CAs. (NewForest2003, in our example).

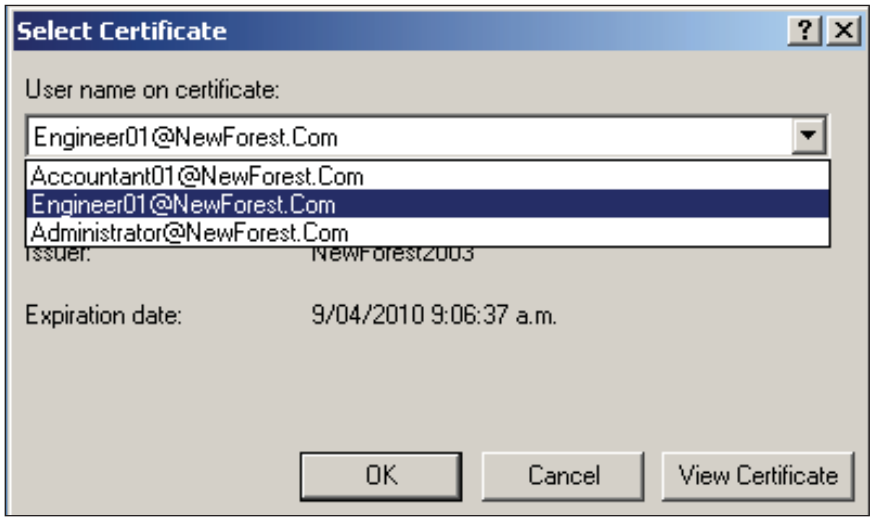
- Click **OK** on all the open windows, and the PC will now be ready to perform 802.1x authentication using Certificates.

Certificate-based authentication will now proceed when the client PC is attached to an authenticating port on one of the access switches. Note that if the PC has enrolled more than one user certificate, it will not be able to automatically choose which certificate to use, but will require user intervention to choose a certificate.

As the PC is connected to the switch, a message bubble stating **Additional information required to connect to the network** will appear.



- Click on the bubble, and you will be able to choose the desired certificate from a combo box that lists all the user certificates currently enrolled on the PC.



This actually can cause a bit of a problem at login time. As the PC boots up and tries to log into the network, it cannot automatically choose which certificate to use in its 802.1x authentication. Given that user intervention to choose which certificate to use is not possible at login time, the 802.1x authentication fails, and the PC does not log into the domain. Subsequent disabling and re-enabling of the NIC card is required, after the user has access to the desktop, in order to perform successful authentication (with user intervention to select the certificate). So, unless multiple users will use a given PC, it is recommended to store no more than **one** user certificate on the PC at any time.

Verifying the authentication from the switch command-line

The x600 switch is able to extract the supplicant name from the Certificate Authentication process, and will display it in response to the **show dot1x supplicant** command. It will likely display the name as an email address in the form **<supplicant name>@ domain-name>**

```
Interface port1.0.13
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    WebBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0


  Supplicant name: Engineer01@NewForest.Com
  Supplicant address: 0002.b363.319f
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 22
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 21
    CD: adminControlledDirections: both - operControlledDirections: both
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 20
```

Multiple supplicants on the same x600 port, assigned to different VLANs

The x600 switch supports the ability to assign different VLAN IDs to different supplicants downstream of the same port. If an EAP-forwarding L2 switch or hub is connected to an authenticating port of the x600 switch, and multiple client devices are connected to that L2 switch or hub, then those client devices can each be separately authenticated, provided the authenticating port of the x600 has been configured with:

```
(config-if)# auth host-mode multi-supplicant
```

If the x600 port is also configured with the command

```
(config-if)#auth dynamic-vlan-creation type multi
```

then it will not only authenticate multiple devices downstream of the same port, but it will dynamically allocate them to different VLANs if the RADIUS server sends back different VIDs for different supplicants.

If two supplicant devices are attached downstream of the same port, and one is authenticated with credentials for a user in the Accountants group, and one is authenticated with credentials for a user in the Engineers group, then the port will report two separate supplicants, allocated different VLAN IDs.

```
show dot1x supplicant interface port1.0.13
Interface port1.0.13
  authenticationMethod: dot1x

…
…

  Supplicant name: NEWFOREST\Accountant01
  Supplicant address: 000e.2e5f.a7fc
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 9

…
…
```

```
    dynamicVlanId: 10
  Supplicant name: NEWFOREST\Engineer01
  Supplicant address: 0002.b363.319f
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 9

…
…

    dynamicVlanId: 20
```

The authenticating port will appear as an untagged port in both VLAN 10 and VLAN 20:

```
show vlan 10

VLAN ID  Name            Type     State  Member ports
                                        (u)-Untagged,    (t)-Tagged
======= ================ ======= ======= ===================================
10       Accounting       STATIC  ACTIVE  port1.0.11(u)    port1.0.13(u)



show vlan 20

VLAN ID Name             Type    State   Member ports
                                         (u)-Untagged,    (t)-Tagged
======= ================ ======= ======= ===================================
20       Engineering      STATIC  ACTIVE  port1.0.13(u)
```

In effect, the x600 is treating this port as being a MAC-based member of VLANs 10 and 20. This is illustrated by looking at the hardware VLAN table. The switch is associating packets from MAC address 0002.b363.319f, arriving into port1.0.13, as belonging to VLAN 20, and packets from MAC address 000e.2e5f.a7fc arriving into port1.0.13, as belonging to VLAN 10.

```
show platform table vlan

[Instance 1.0]
VLAN table
---------------

…
…

Mac Based Vlan Information:
Index Mac               Vid   Prio
-------------------------------------------------------------------------------
212   0002.b363.319f    20    0
996   000e.2e5f.a7fc    10    0
```

Similarly, the ARP table shows the ARP entries for the IP addresses of the two hosts as being associated with different VLANs.

```
Show arp
IP  Address          MAC Address    Interface    Port         Type
192.168.2.253        00e0.1867.c69a vlan2        port1.0.4    dynamic
192.168.2.254        000b.6af0.35f4 vlan2        port1.0.23   dynamic
192.168.10.20        000e.2e5f.a7fc vlan10       port1.0.13   dynamic
192.168.20.20        0002.b363.319f vlan20       port1.0.13   dynamic
```

Setting up MAC-based authentication

The way that MAC-based authentication works is that when the supplicant device starts sending packets, the Authenticating switch will extract the source MAC address from the packets, and send a RADIUS request that uses this MAC address as the username and password in the request.

The RADIUS server needs to be configured with a User whose username **and** password are **both** the MAC address of this device that is to be authenticated.

By default, Microsoft Windows servers enforce strong password requirements that actually disallow having a username and password that are both equal to a MAC-address string.

This strict password requirement can be disabled on the servers, but Microsoft warns against disabling it, as this undermines the security of the network.

A convenient solution to this problem is to use the x900 VCStack as the RADIUS server for the MAC-based authentication. Whilst it is a little inconvenient to use a separate RADIUS server for the MAC-based authentication, it is distinctly preferable to disabling the strong password requirement on the Windows servers.

Also, the configuration of the RADIUS server feature on the x900 is simple, and the configuration will likely not need to be changed often, as printers and scanners tend to stay in place for long periods once installed.

There is one other matter that needs to be considered in relation to MAC-based authentication – namely that the 8000S and x600 operate slightly differently in two ways:

(i) The RADIUS requests, that the 8000S creates for MAC-authentication, uses a username and password that contain only the hex digits of the supplicant device. The RADIUS requests that the x600 creates for MAC-authentication, uses a username and password that contain pairs of hex digits separated by dashes. So, for a supplicant with MAC address 0002.4e2a.80b4, the usernames/passwords in the RADIUS requests created by these two switch models would be:

8000S : username = 00024e2a80b4 password = 00024e2a80b4

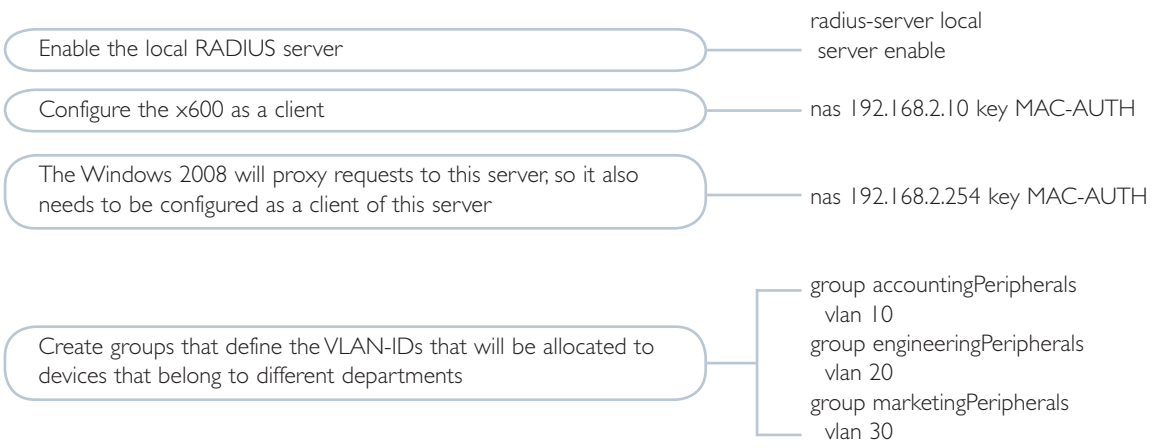
x600 : username = 00-02-4e-2a-80-b4 password = 00-02-4e-2a-80-b4

(ii) The x600 can be configured with different RADIUS servers for 802.1x and MAC-based authentication, whereas the 8000S must use the same RADIUS server for both types of authentication.

The solution to difference (i) above, is simple: two entries need to be created in the RADIUS database for any device that might need to be MAC authenticated.

The solution to difference (ii) above is a little more involved. Given that the 8000S must use the Windows 2008 server for its 802.1x authentication, it must also send its MAC authentication requests to that same server. The solution is to configure the Windows 2008 server as a **proxy RADIUS server** for the MAC-based authentication requests, so that it forwards those on to the core VCStack that is acting as the RADIUS server for MAC authentication.

The configuration of RADIUS proxy on the Network Policy Server is described below, but first let us look at the RADIUS configuration required on the VCStack:



Create 2 entries for each device that needs to be authenticated

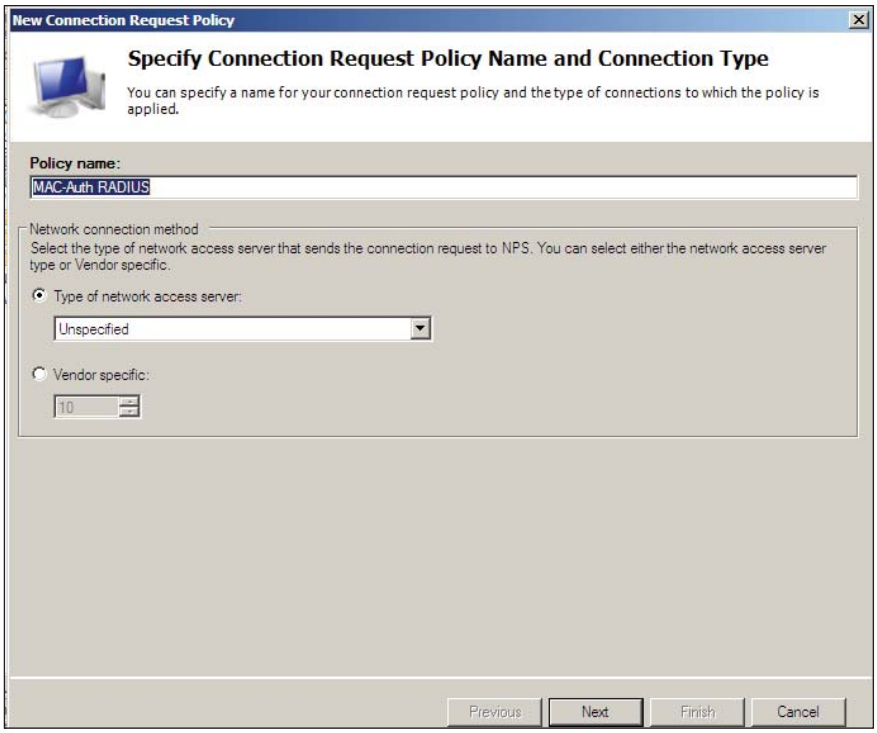
```
user 00-02-b3-63-31-9f password 00-02-b3-63-31-9f group engineeringPeripherals
user 0002b363319f password 0002b363319f group engineeringPeripherals
user 00-00-65-a3-83-e4 password 00-00-65-a3-83-e4 group accountingPeripherals
user 000065a383e4 password 000065a383e4 group accountingPeripherals
user 00-40-dd-9e-e1-b7 password 00-40-dd-9e-e1-b7 group accountingPeripherals
user 0040dd9ee1b7 password 0040dd9ee1b7 group accountingPeripherals
```

Configuring the Network Policy server to Proxy MAC-based RADIUS requests to the VCStack RADIUS server

The key to configuring RADIUS proxy on the Network Policy server is to create a new Connection Request Policy.

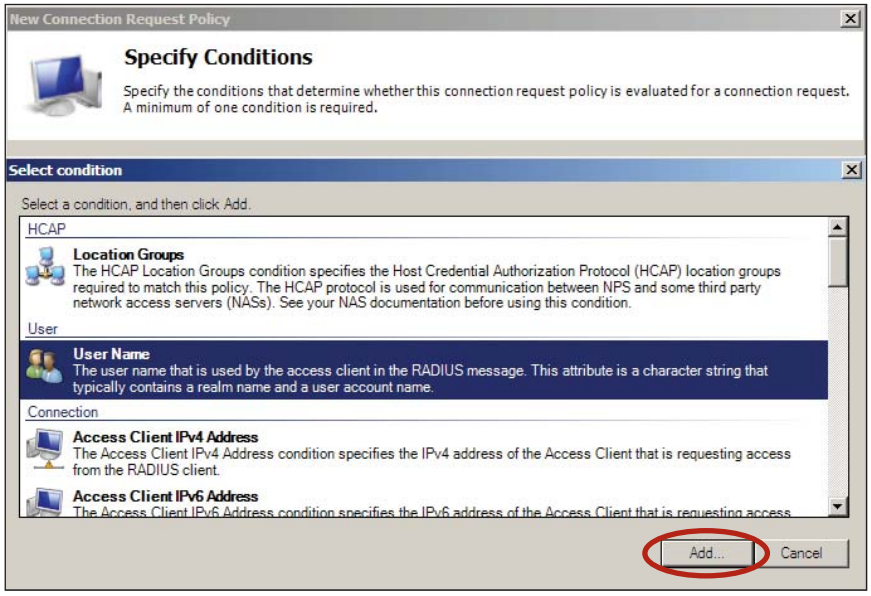
To create a new Connection Request policy:

- In the main menu of the Windows 2008 server, choose **Administrative Tools** > **Network Policy Server**, to open the **Network Policy Server manager**.
- In the left-hand pane of the **Network Policy Server manager**, expand the **Policies** section, then right-click on **Connection Request Policies** and choose **New**.
- This will open the **New Connection Request Policy** wizard. In the opening window of the wizard, type in a **Policy name**:

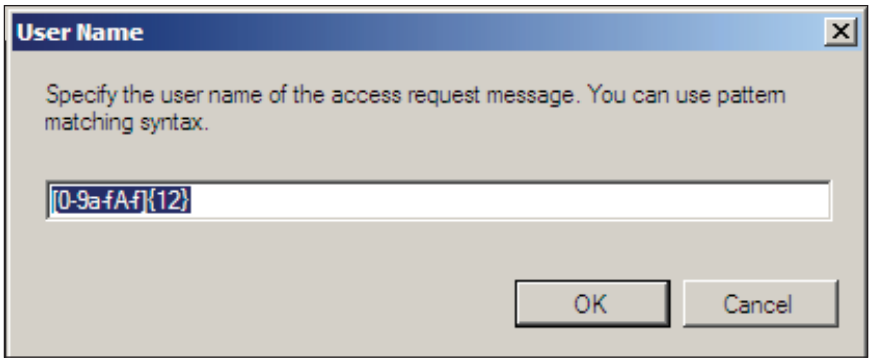


- Click **Next** to move to the **Specify Conditions** window.

- In this window, click **Add...** to open up the **Select condition** window.
- Within the **Select condition** window, select **User Name**, and click **Add...**

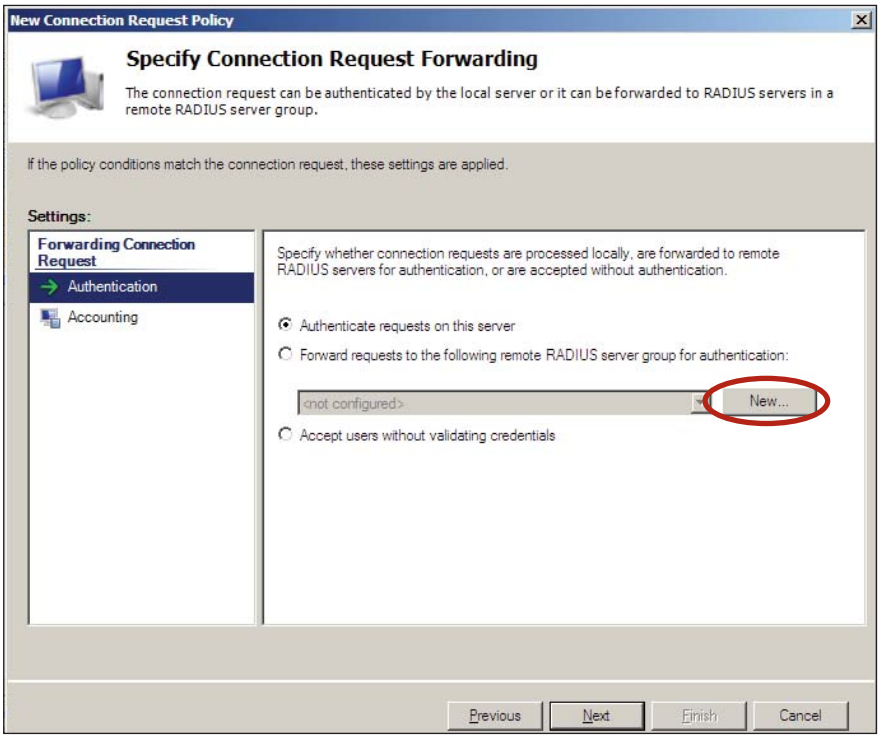


- For the **User Name**, specify the Regular Expression that represents 12 hex digits – [0-9a-fA-F]{12}. This will match **any** MAC address in the form that they are sent in MAC-Authentication RADIUS requests from the 8000S:



- Click **OK** in the **User Name** window, and close the **Select condition** window.

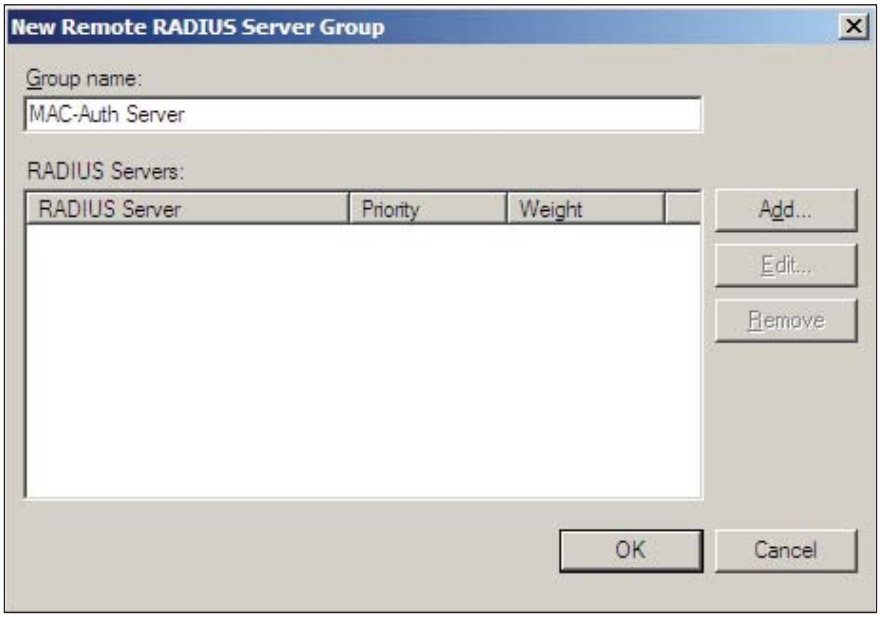
- Click **Next** in the **Specify Conditions** window, to move on to the **Specify Connection Request Forwarding** window:



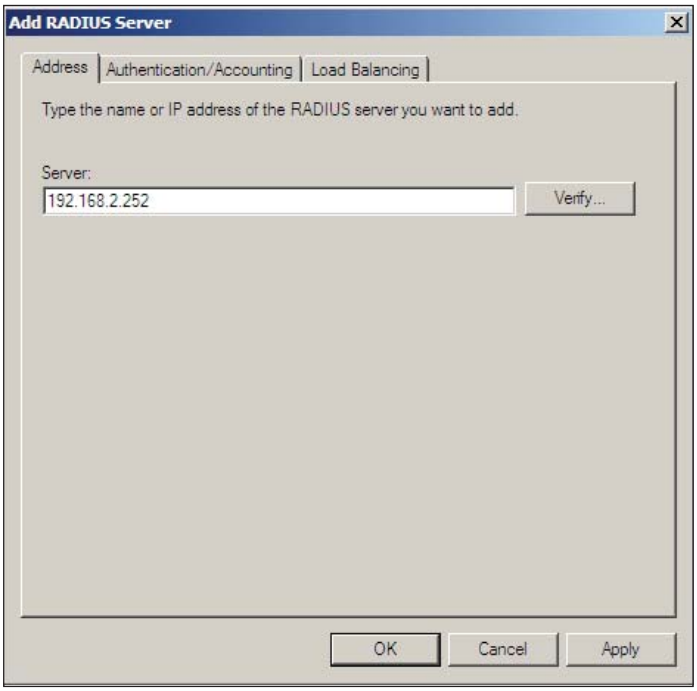
- In this window, click **New...** in order to define the RADIUS server to which the Network Policy Server will proxy-forward requests.

This opens the **New Remote RADIUS Server Group** window.

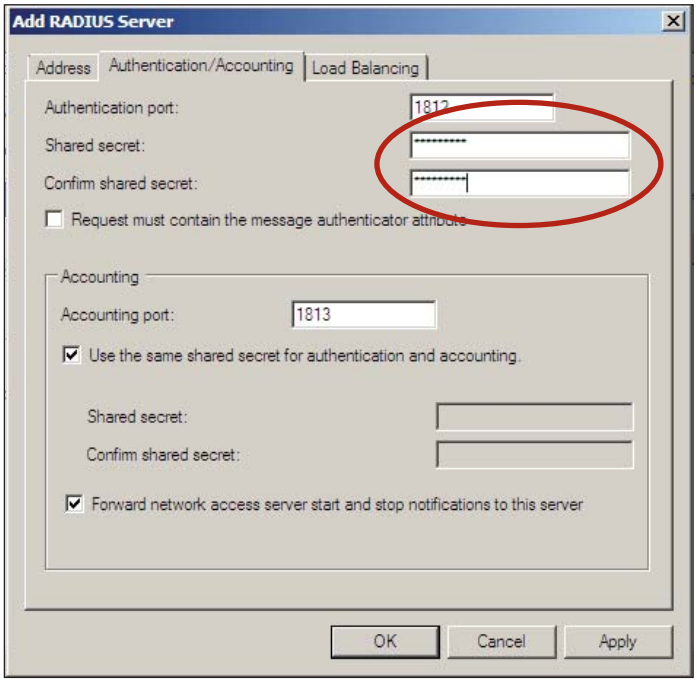
- In this window, type in a **Group name** (MAC-Auth Server in our example), and click **Add...** to add the details of the server.



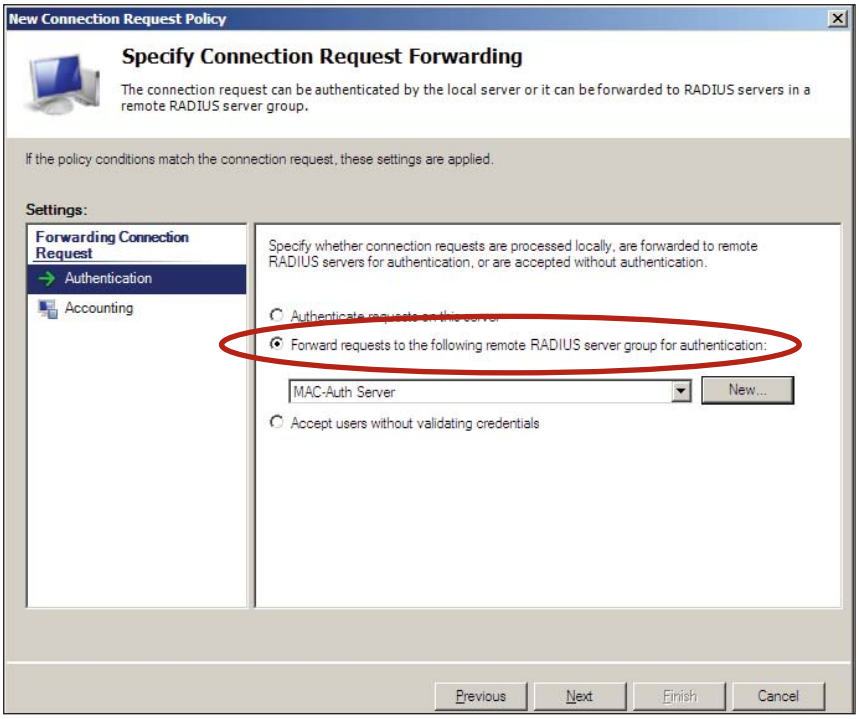
- In the **Address** tab of the **Add RADIUS Server** window, enter the IP address of the VCStack.



- In the **Authentication/Accounting** tab, enter the **Shared secret** that the VCStack expects to receive from the Network Policy Server (MAC-AUTH).

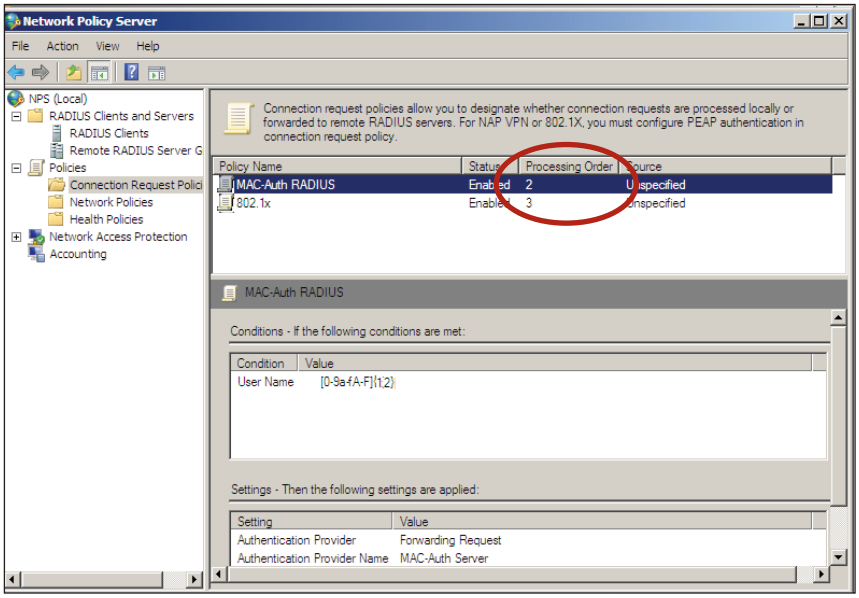


- Then click **OK** twice to get back to the **Specify Connection Request Forwarding** window.
- In this window, select **Forward requests to the following remote RADIUS...**, and in the combo box below that, choose the RADIUS group you have just defined (MAC-Auth Server):



- Click **Next** - through the rest of the windows in the wizard, and the new connection request policy is created.
- In the **Network Policy Server** manager, move this policy to the top of the list of Connection Request policies, to ensure that incoming RADIUS requests are compared to this policy first. This is done by right clicking on an entry in the list of policies, and choosing **Move Up** or **Move Down** in the resulting pop-up menu.

That will mean that MAC authentication requests will match this policy, and be proxy forwarded to the VCStack, and 802.1x requests (that do not match the conditions of this policy) will fall through to the next policy, and be processed within the Network Policy Server itself.



Creating MAC address entries in the Active Directory User database

The final step to enabling successful proxying of these RADIUS requests is to create entries in the Active Directory User database for each of the MAC addresses that are to be authenticated. The Network Policy Server will not proxy forward the RADIUS requests unless it can find the user name in the Active Directory User database.

At this point, it might seem we have gone around in a circle. The whole reason for moving the MAC authentication database off to a different RADIUS database is that Active Directory would not accept users whose username and password were both a MAC address. That is true, but the important difference is that in the case of the user entries we have to create to enable the Proxy forwarding to work, the password is not constrained. You can use whatever string you like for the password – it will not be checked. The Network Policy Server simply checks that the Active Directory User database contains a user whose name corresponds to the name in the RADIUS request it is about to proxy forward. It does not check whether the password in the RADIUS request matches the password in that Active Directory user entry.

Create a set of Active Directory User entries for the MAC addresses that are to be authenticated, and give the users whatever password you like. It is advisable to add these entries to a user group to whom no privileges are granted.

Appendix 1 – Setting up a DHCP server

In an environment where VLANs are dynamically allocated to user ports, it is very likely that the client PCs will be configured to obtain their IP addresses by DHCP, rather than being set up with static IP addresses. Hence, the network will need a DHCP server.

There are two obvious choices of which device to use as the DHCP server – the **core x900 VCStack**, or the **Windows 2008 server**.

The sections below describe how to set up either of these choices as a DHCP server.

Setting up the x900 VCStack as a DHCP server

The first step is to enable the DHCP service. This uses a command in global configuration mode:

service dhcp-server

Then you need create a set of IP address Pools from which the server can allocate IP addresses to hosts in the various subnets in the LAN. An IP address Pool is required for each subnet.

Each pool requires a:

- name
- definition of the subnet which it applies to
- definition of the range of addresses within that network that can be allocated to hosts
- lease time
- set of options (subnet mask, DNS server, gateway address, etc)

For the network in this example, the DHCP server will need to define eight pools:

- Two for Accountants (one for when connected in the private zone, and one for when connected in the public/private zone)
- Two for Engineers (one for when connected in the private zone, and one for when connected in the public/private zone)
- Two for Marketers (one for when connected in the private zone, and one for when connected in the public/private zone)
- One for Guests from Other offices
- One for External guests

The full configuration is:

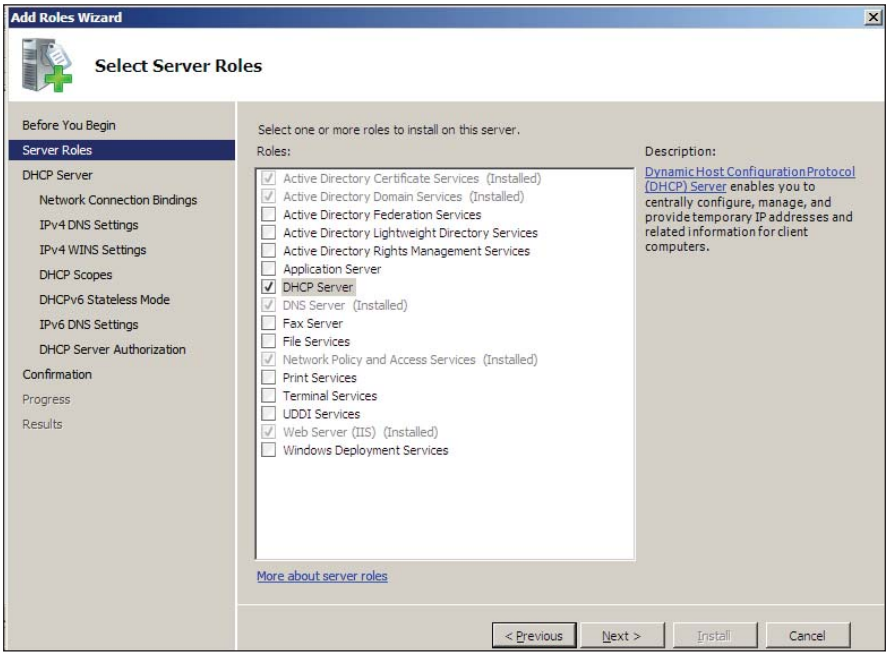
```
service dhcp-server
ip dhcp pool Accounting-private
network 192.168.10.0 255.255.255.0
range 192.168.10.20 192.168.10.210
dns-server 192.168.2.254
default-router 192.168.10.10
lease 30 1 1
subnet-mask 255.255.255.0
ip dhcp pool Accounting-publicPrivate
network 192.168.110.0 255.255.255.0
range 192.168.110.20 192.168.110.210
dns-server 192.168.2.254
default-router 192.168.110.10
lease 30 1 1
subnet-mask 255.255.255.0
```

```
ip dhcp pool Engineeering-private
network 192.168.20.0 255.255.255.0
range 192.168.20.20 192.168.20.210
dns-server 192.168.2.254
default-router 192.168.20.10
lease 30 1 1
subnet-mask 255.255.255.0

ip dhcp pool Engineeering-publicPrivate
network 192.168.120.0 255.255.255.0
range 192.168.120.20 192.168.120.210
dns-server 192.168.2.254
default-router 192.168.120.10
lease 30 1 1
subnet-mask 255.255.255.0

ip dhcp pool Marketing-private
network 192.168.30.0 255.255.255.0
range 192.168.30.20 192.168.30.210
dns-server 192.168.2.254
default-router 192.168.30.10
lease 30 1 1
subnet-mask 255.255.255.0

ip dhcp pool Marketing-publicPrivate
network 192.168.130.0 255.255.255.0
range 192.168.130.20 192.168.130.210
dns-server 192.168.2.254
default-router 192.168.130.10
lease 30 1 1
subnet-mask 255.255.255.0

ip dhcp pool InternalVisitors
network 192.168.40.0 255.255.255.0
range 192.168.40.20 192.168.40.210
dns-server 192.168.2.254
default-router 192.168.40.10
lease 30 1 1
subnet-mask 255.255.255.0

ip dhcp pool ExternalVisitors
network 192.168.50.0 255.255.255.0
range 192.168.50.20 192.168.50.210
dns-server 192.168.2.254
default-router 192.168.50.10
lease 30 1 1
subnet-mask 255.255.255.0
```

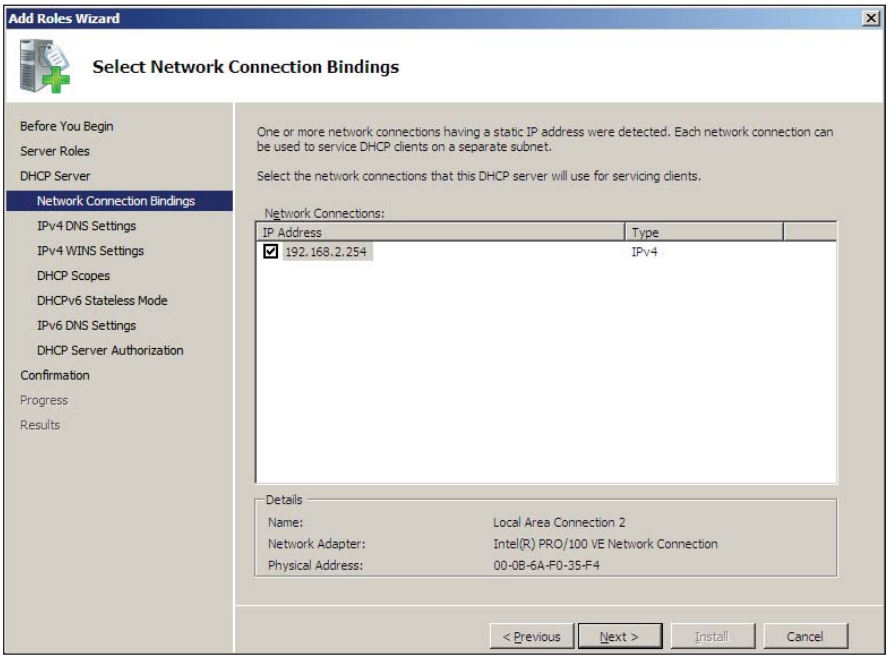
To set up the Windows 2008 server as the DHCP server

To install the DHCP server on the Windows 2008 server

- Right-click on **Roles** in the Server Manager, and choose **Add Roles** from the resulting menu.
- In the **Add Roles Wizard** select **Server Roles** and then select **DHCP Server**.

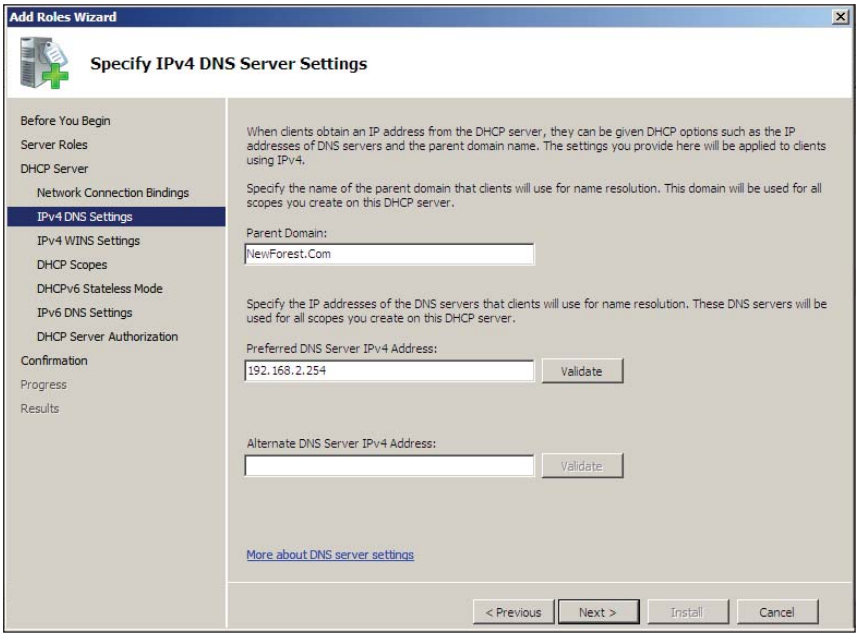


- Click **Next**.
- In the **Select Network Connection Bindings** window, select the one or more interfaces of the server which will accept DHCP requests.

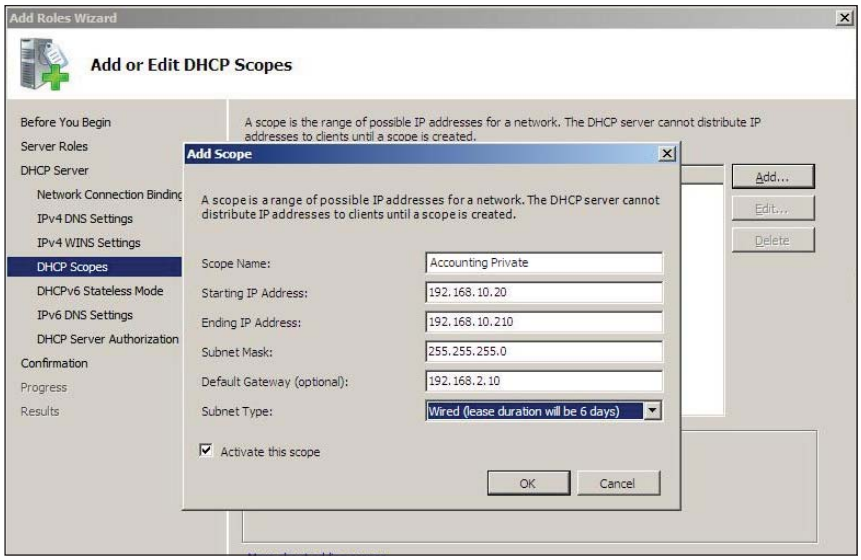


- Click **Next**.

- In the next window, specify the **Parent Domain**, and the **Preferred DNS Server IPv4 Address**.

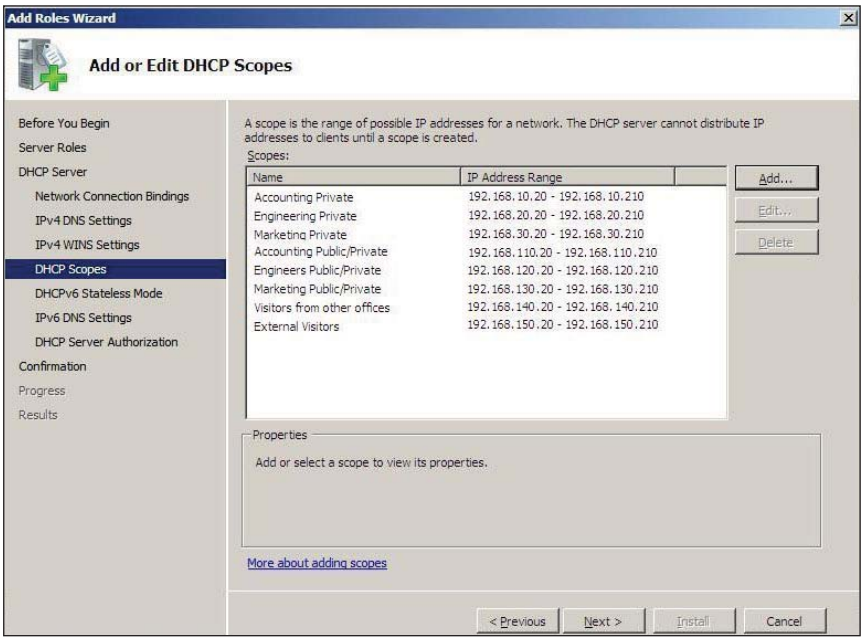


- Click **Next** until you see the **Add or Edit DHCP Scopes** window. This is where the IP address pools (referred to as **scopes** in Microsoft Windows) are created.
- Click **Add...** to add an address pool, and fill in the details of the pool.

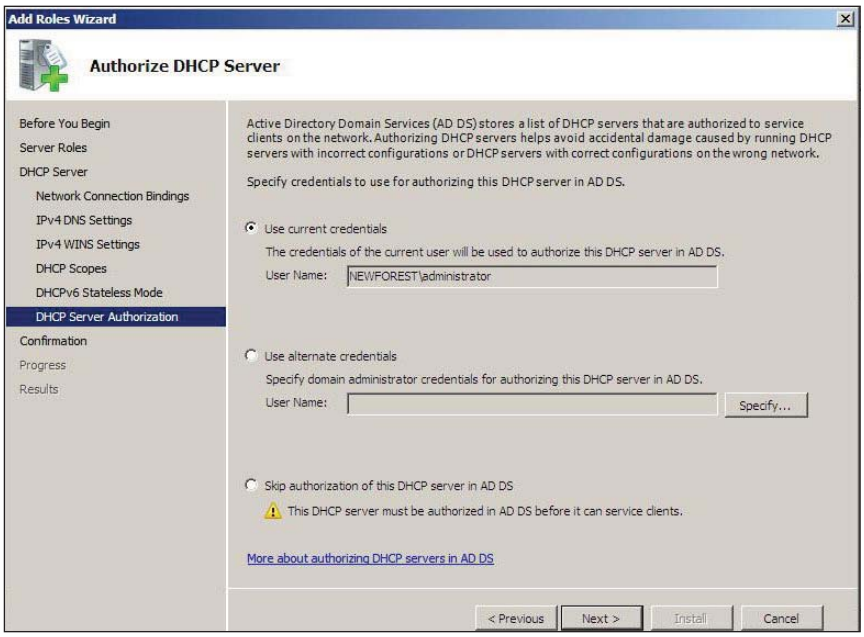


- Click **OK**.

- Continue on to create all eight pools.



- Then, move on to specify the credentials for authorizing the DHCP server with Active Directory.



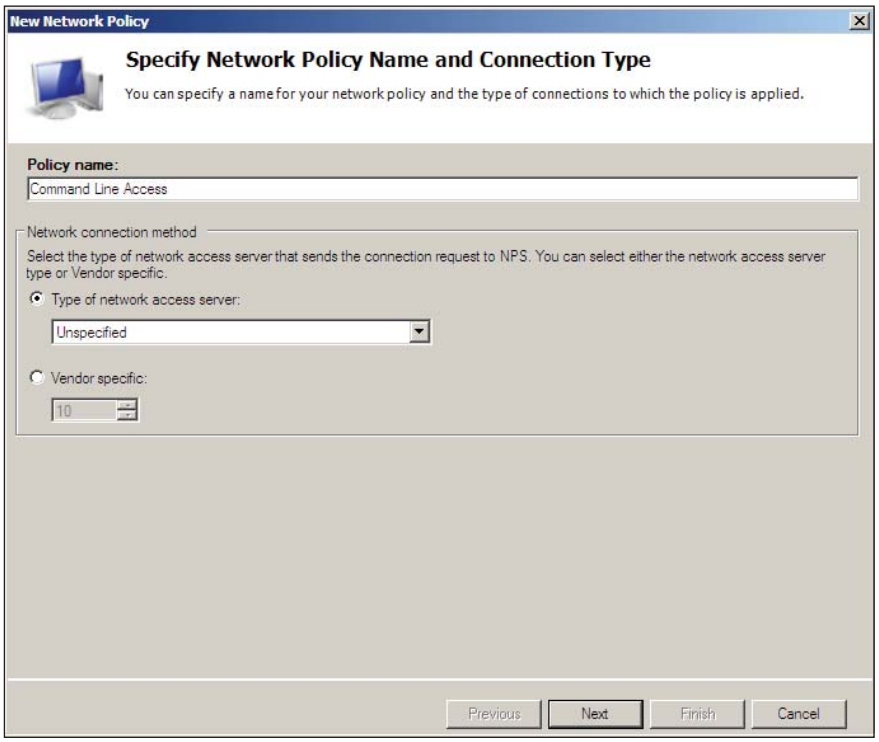
- From there, click through the rest of the windows in the wizard, and the DHCP server will be installed, and ready to service DHCP requests.

Appendix 2 – Setting up the Windows 2008 Network Policy Server to authenticate Management access to the switches

You will have seen in the configuration scripts of the switches, that the switches have been set up to use the Windows 2008 NPS server to authenticate login sessions. To enable the NPS to authenticate these sessions, we need to create another **Network Policy**.

To create a Network Policy:

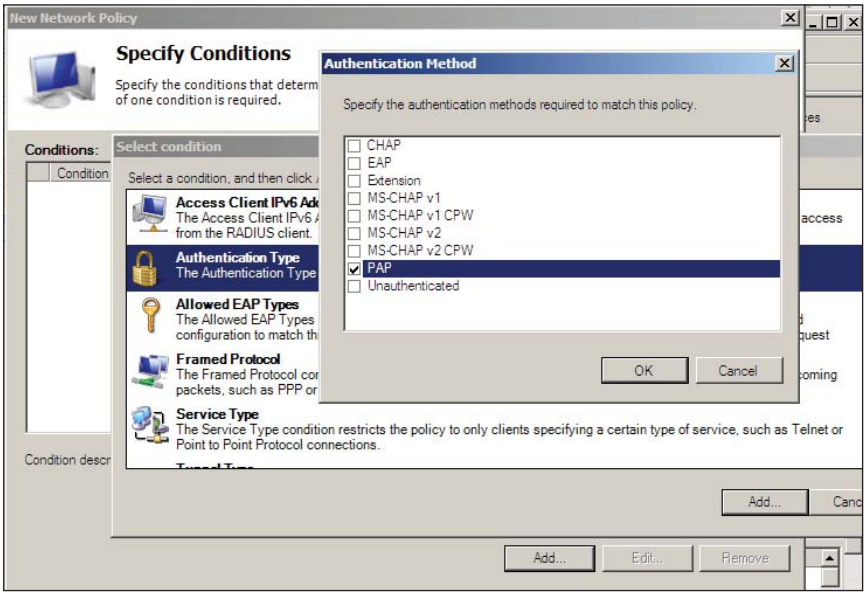
- Within the **Network Policy Server** manager, left-click on **Network Policy** in the left-hand pane, and choose **New** from the resulting pop-up menu. This will open the **New Network Policy** wizard.
- In the first window of the wizard, type in a **Policy name**.



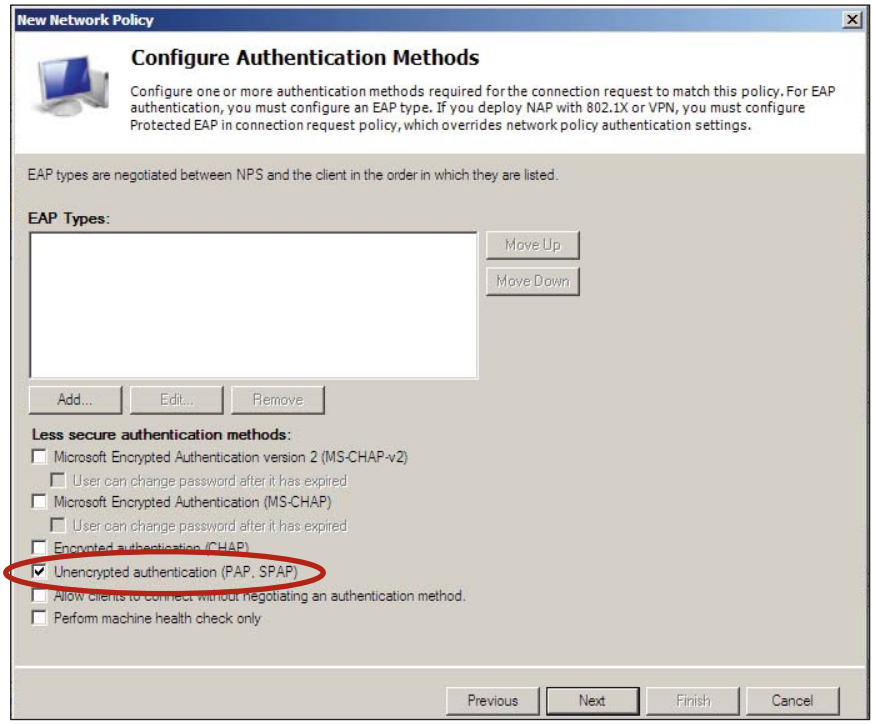
- Click **Next** to move along to the **Specify Conditions** window.
- Within this window, click **Add…,** to open the **Select Condition** window.
- Within the **Select Condition** window, select **Authentication Type**, and click **Add...**

This will open the **Authentication Method** window.

- Within this window, tick the check box beside **PAP**, as this is the Authentication method used in login authentication requests from all the Allied Telesis switches in use in this solution.

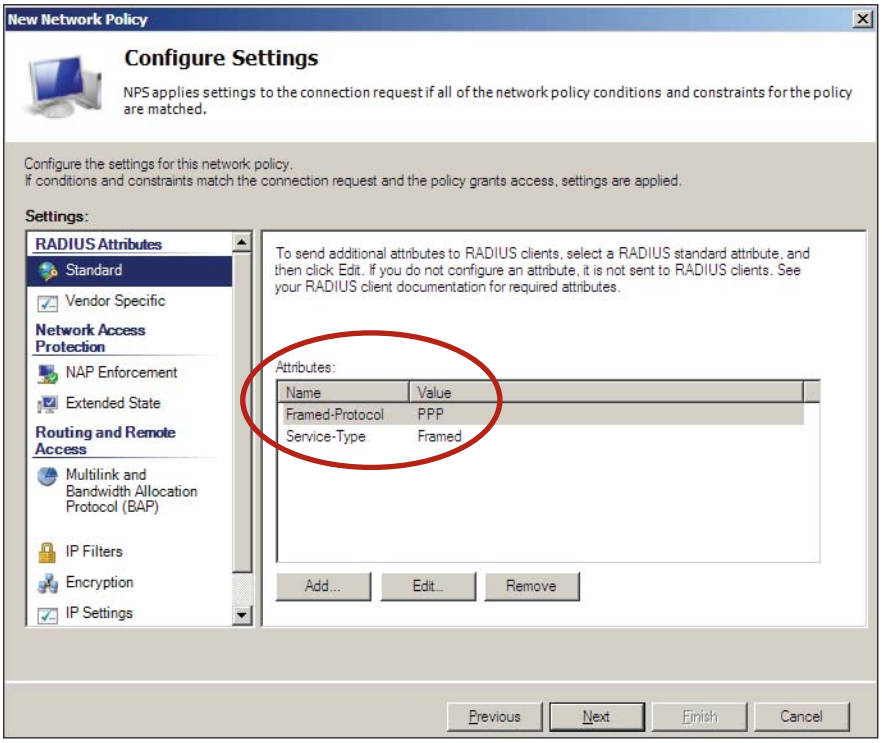


- Click **OK**, to drop back into the **Specify Conditions** window, and then click **Next** to move along to the **Configure Authentication Methods**.

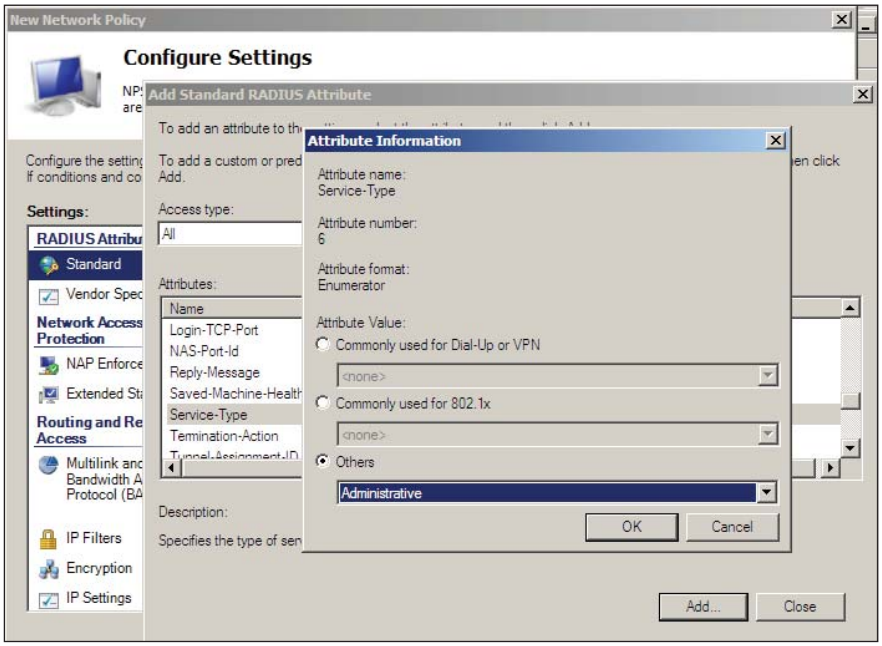


- In this window, choose only one authentication method **Unencrypted Authentication (PAP, SPAP).**
- You will receive a popup message warning that this is an insecure authentication method, and offering to take you to a help page that explains about authentication methods. Just click **No** on this message, and move on.
- Click **Next** twice to move along to the **Configure Settings** window.

- In this window, start by removing the existing **Framed-Protocol** and **Service-Type** attributes.

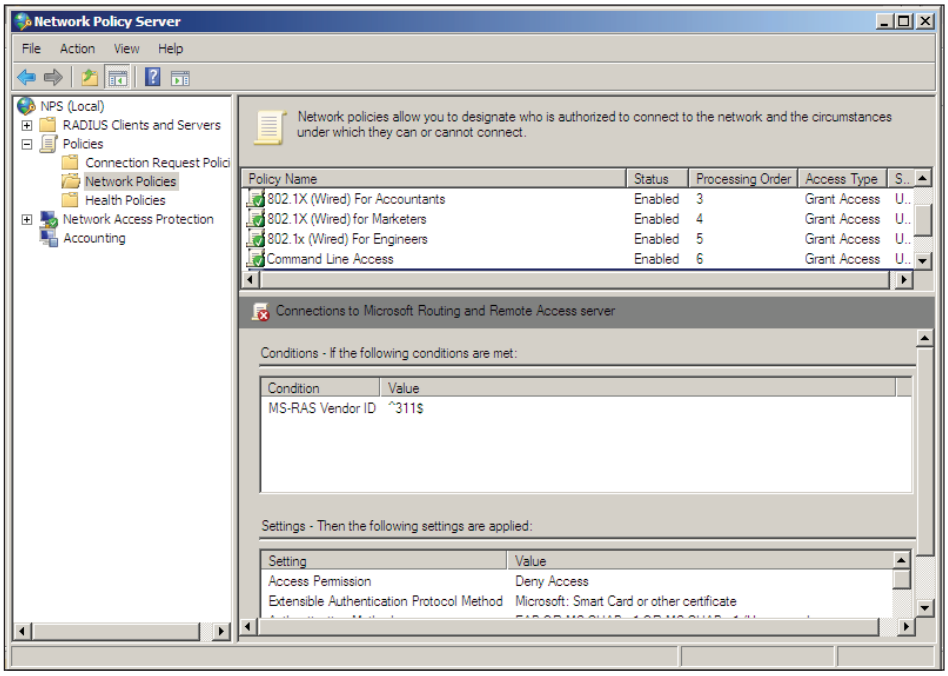


- Ensure that **Standard** is highlighted under settings: **RADIUS Attributes** in the left-hand pane of the window. Then click **Add...** to open the **Add Standard RADIUS Attribute** window.
- Highlight **Service-Type** in the list of Attributes, then click **Add...** to open the **Attribute Information** window.
- In this window, select **Others**, and then choose **Administrative** in the associated combo box.



- Click through the rest of the windows in the wizard, and then the Network Policy is complete.

Ensure that this new Network Policy appears beneath the 802.1x policies in the list of Network Policies.



About Allied Telesis Inc.

Allied Telesis is a world class leader in delivering IP/Ethernet network solutions to the global market place. We create innovative, standards-based IP networks that seamlessly connect you with voice, video and data services.

Enterprise customers can build complete end-to-end networking solutions through a single vendor, with core to edge technologies ranging from powerful 10 Gigabit Layer 3 switches right through to media converters.

Allied Telesis also offer a wide range of access, aggregation and backbone solutions for Service Providers. Our products range from industry leading media gateways which allow voice, video and data services to be delivered to the home and business, right through to high-end chassis-based platforms providing significant network infrastructure.

Allied Telesis' flexible service and support programs are tailored to meet a wide range of needs, and are designed to protect your Allied Telesis investment well into the future.

Visit us online at www.alliedtelesis.com

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

www.alliedtelesis.com

 C618-31019-00 Rev. B

Connecting The IP World

Allied Telesis