

LAN Client Authentication

Introduction

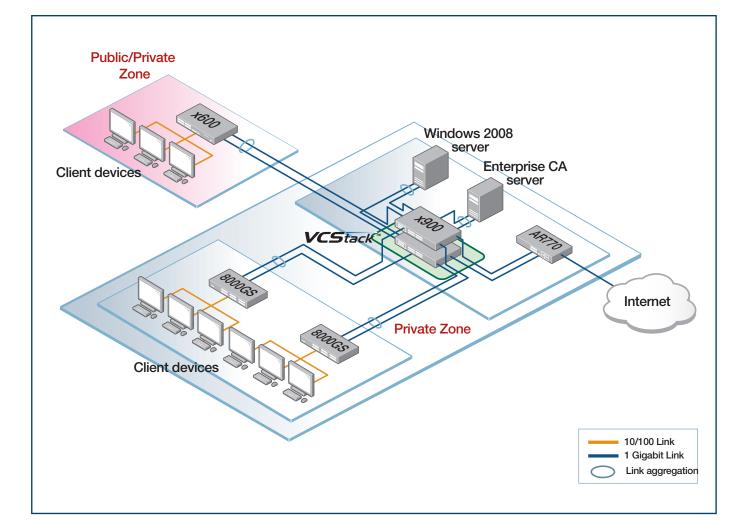
The key to strong LAN security, and seamless mobility within an Enterprise network, is to identity and authenticate the user at their point of connection to the network.

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:

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



| Introduction | 1 |
|---|-----|
| Network scenario | 3 |
| Switch Configurations | 4 |
| Setting up the Windows 2008 Server | 10 |
| Configuring IP interface(s) | 10 |
| Installing Active Directory | 11 |
| Adding users and groups to Active Directory | 15 |
| Installing Network Policy Server | 19 |
| Registering NPS with Active Directory | 20 |
| Obtaining a server certificate for the server that is running NPS | 21 |
| Adding RADIUS clients to the Network Policy Server | 22 |
| Setting up a Connection Request Policy | |
| Setting up Network Policies | 26 |
| Setting up Client PCs to perform 802.1x authentication | |
| Joining the PCs to the domain | |
| Configuring the PC as an 802.1x supplicant | |
| Performing 802.1x authentication | |
| 802.1x Authentication with Certificates | 41 |
| Configuring Policies on the Network Policy Server to use certificates | 41 |
| Setting up the client PC to perform Certificate Authentication | 43 |
| Obtain user certificates | 43 |
| Download the Certificate Authority server's Root certificate | 45 |
| Set up the NIC card to perform authentication by certificate | |
| Verifying the authentication from the switch command-line | |
| Multiple supplicants on the same x600 port, assigned to different VLANs | |
| Setting up MAC-based authentication | 54 |
| Configuring the Network Policy server to Proxy MAC-based RADIUS requests to the VCStack RADIUS server | 55 |
| Creating MAC address entries in the Active Directory User database | 60 |
| Appendix 1: | |
| Setting up the x900 VCStack as a DHCP server | 61 |
| Setting up the Windows 2008 Network Policy Server to authenticate Management access to the | 0.0 |
| switches | 66 |

Network scenario

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

- 1. A fully private zone in which only registered users (i.e., users registered in the Active Directory hosted on the Windows Server) may connect.
- 2. 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 MACbased 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

101100101010010000100000101C 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

| | hostname Triple-Auth |
|---|---|
| The Network Policy server in the windows 2008 server is used for validation of 802.1x authentication requests | 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 |
| 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 | 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 |
| The validation of Web-based authentication requests is performed within the switch's own RADIUS server | 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 |
| 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 group NPS local |

| | crypto pki trustpoint local crypto pki enroll local |
|--|--|
| | radius-server local |
| Set up the Local RADIUS server. | server enable nas 127.0.0.1 key awplus-local-radius-server |
| The only NAS configured for the server is 127.0.0.1, so it will only accept internally-generated requests. | group otheroffices |
| It is configured with username/password set up for visitors | vlan 40 |
| from other offices, who will be dynamically allocated VLAN | group externalvisitors vlan 50 |
| 40; and for external visitors, who will be dynamically allo- | user InternalVisitor password ikiG4JcsKEwFlhL |
| cated to VLAN50 | group otheroffices |
| | user ExternalVisitor password ikiG4JcsKEwFlhL |
| | group externalvisitors |
| | vlan database |
| | vlan 2 name uplink |
| The switch is configured with one static VLAN (VLAN 2) that | vlan 10 name Accounting |
| is used for communication with the rest of the network. The | vlan 20 name Engineering |
| other 5 VLANs are used for dynamic allocation to users | vlan 30 name Marketing vlan 40 name OtherOffices |
| | vlan 50 name ExternalGuests |
| | vlan 60 name GuestsVLAN |
| | interface port1 0 1 1 0 22 |
| The first 22 ports on the switch are available for users to | interface port1.0.1-1.0.22 auth-mac enable |
| connect to. They are all configured with triple authentication | auth-Web enable |
| with dynamic VLAN assignment and VLAN60 as the guest | dot1x port-control auto |
| VLAN. The ports are configured to support multiple sup- | auth host-mode multi-supplicant |
| plicants on a single port, in case a hub or EAP-forwarding | auth guest-vlan 60 |
| L2 switch is attached to one of the ports, to enable multiple | auth dynamic-vlan-creation type multi |
| users to share that port | spanning-tree portfast spanning-tree portfast bpdu-guard enable |
| | |
| Ports 23 and 24 are configured as a link aggregration group | interface port1.0.23-1.0.24 |
| to connect the switch to the virtual chassis stack in the core | switchport access vlan 2 static-channel-group 1 |
| | stato shamor group i |
| Set up a DHCP server on the switch that is used specifically | ip dhcp pool Temporary |
| for the Web-Auth users to have an IP address for a brief | network 192.168.160.0 255.255.255.0 |
| time whilst they authenticate via HTTP. The leasetime is set | range 192.168.160.20 192.168.160.40 default-router 192.168.160.10 |
| to 30 seconds, so the DHCP lease will be re-newed very | lease 0 0 0 30 |
| quickly after the authentication has been completed | subnet-mask 255.255.255.0 |
| | service dhcp-server |
| | 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 addresses are configured on all the VLANs. All the client | ip dhcp-relay server-address 192.168.2.254 |
| VLANs are configured to relay DHCP requests to the | interface vlan30 |
| DCHP server in the network core | 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 route 0.0.0.0/0 192.168.2.252 The default route is via the x900 VCStack log buffered level errors All log messages are sent to a syslog server. Higher-severity log log host 192.168.2.254 messages are also buffered on the switch itself log host 192.168.2.254 level debugging access-list 1 permit 192.168.2.253 Allow read-only SNMP monitoring from one management snmp-server enable trap auth nsm station snmp-server community public ro 1 snmp-server host 192.168.2.253 version 2c public Configure NTP (Network Time Protocol) with the IP ntp server 192.168.2.252 address of the NTP server 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 radius-server host 192.168.2.254 key MS-IAS at 192.168.2.254. The Network Policy Server will process aaa authentication dot1x default radius 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 Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server. aaa authentication login default radius local If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request The switch is configured with one static VLAN (VLAN 2) that is used for communication with the rest of the network. The vlan database other 4 VLANs are used for dynamic allocation to users vlan 2,10,20,30,50 interface vlan 50 vlan50 is designated as the guest VLAN for the switch dot1x guest-vlan exit interface range ethernet 1/e(1-24) dot1x re-authentication dot1x mac-authentication mac-and-802.1x The 24 10/100 ports are configured for MAC-based and dot1x guest-vlan enable 802.1x authentication. They accept dynamic VLAN allocadot1x radius-attributes vlan tion, and will put unathenticated users into the guest 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 |
| 900 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 | stack resiliencylink eth0 |

stack resiliencylink eth0

stack 1 priority 1

Use priority to pre-elect the VCStack master switch

stacking link fails, communication is maintained to allow

LAN Client Authentication |7

NETWORK SMARTER

graceful reconfiguration

Tested Solution | Networking Management sessions on the switch will be authenticated by radius-server host 192.168.2.254 key MS-IAS RADIUS, using the windows 2008 Network Policy server. If the server is unavailable, then the switch will fall back to usaaa authentication login default group Radius local ing the local user database to authenticate the request vlan database vlan 2 name core vlan 10 name Accounting The switch is configured with 8 VLANs 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 access-list 3001 permit udp any range 67 68 any range 67 All DHCP will be allowed through 68 External visitors' traffic (apart from DHCP) cannot go to any 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 internal addresses access-list 3004 deny ip 192.168.150.0/24 10.0.0/8 Visitors from other offices' traffic (apart from DHCP) cannot access-list 3005 deny ip 192.168.140.0/24 192.168.0.0/16 go to local internal addresses, but can go out onto the corporate WAN The final ACL allows through all the traffic that has not been access-list 3006 allow ip any any explicitly blocked by the previous ACLs Create link aggregation groups across the VCStack members for resiliency 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 The ports that connect to the x600 are untagged in VLAN 2 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

| | interface p switchpor switchpor static-cha |
|---|---|
| | ip access ip access ip access ip access ip access ip access ip access |
| The ports that connect to the 8000S switches are tagged in all VLANs except the InternalVisitors VLAN | interface p switchpor switchpor static-cha ip access |
| · | ip access ip access ip access ip access ip access ip access |
| | interface p switchpor switchpor |
| | static-cha ip access ip access ip access ip access |
| | ip access ip access interface p switchpor |
| | switchpor static-cha ip access- ip access- |

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

p access-group 3001 p access-group 3002 p access-group 3003 p access-group 3004 p access-group 3005 p 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

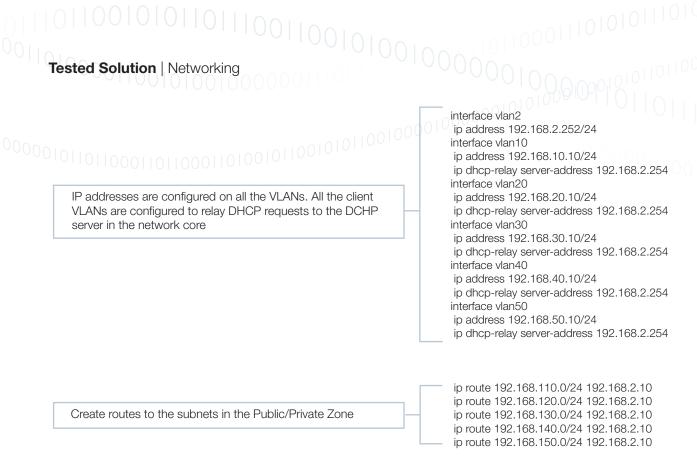
nterface port1.0.3 switchport mode trunk switchport trunk allowed vlan add 2,10,20,30,50 static-channel-group 3 p access-group 3001 p access-group 3002 p access-group 3003 p access-group 3004 p access-group 3005 p access-group 3006

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



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:

- 1. Active Directory Domain Controller
- 2. 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:

DI0000100000

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.

| Server Manager | | |
|---|---|--|
| File Action View Help | | |
| 💠 🧆 🖄 📅 🔯 | | |
| Server Manager (2K8TEST02) | Roles | |
| Server Manager (2K8TEST02) Roles File Services File Services File Services File Services File Configuration | Vev: the health of the roles installed on your server and add or remove roles and features. | |
| B Storage | ⑦ Roles Summary | Roles Summary Help |
| | Roles: 1 of 16 installed His Services | i <mark>ddi Roles</mark> Remove Roles |
| | ⑦ File Services | File Services Help |
| | Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and ena | ble access for UNDX client computers |
| | Role Status | Go to File Services |
| | Messages: None | |

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

| Add Roles Wizard | | × |
|--|--|--|
| Select Server Ro | les | |
| Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results | Select one or more roles to install on this server. Roles Active Directory Certificate Services Active Directory Pederation Services Active Directory Rights Management Services Active Directory Rights Management Services Application Server DHCP Server DNS Server Fist Services Print Services Old Services Use Server (IIS) Windows Deployment Services Deployment Services Print Services Mode Server (IIS) Veto Server roles | > Install Cancel Install |

4. 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.

| Add Roles Wizard | | X |
|---|--|---|
| Installation Resu | llts | |
| Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results | The following roles, role services, or features were installed successfully: Active Directory Domain Services Installation succeeded Active Directory Domain Controller We the Active Directory Domain Services Installation Wizard (depromo.exe) to make the server a fully functional domain controller. Close this wizard and launch the Active Directory Domain Services Installation Wizard (depromo.exe). Print, e-mail, or save the installation report | |

1. 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).

| Server Manager | | | |
|---------------------------|---|---|----------------------|
| F Active Directory Domain | Services Installation Wizard | × | |
| | Welcome to the Active Directory Domain Services Installation Wizard This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next. | , | and add or remov |
| | Use <u>advanced mode installation</u> Leam more about the additional options that are available in <u>advanced mode installation</u> . More about <u>Active Directory Domain Services</u> | | sers and domains |
| | < Back Next > Can | cel | |
| | Role Services: 1 installed Role Service Active Directory Domain Controller Identity Management for UNIX Server for Network Information Services Password Synchronization Administration Tools Description: | Status Installed Not insta Not insta Not insta Not insta | lled lled lled |

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.

| Active Directory Domain Services Installation Wizard | × |
|---|-------|
| Choose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest. | |
| C Existing forest | |
| C Add a domain controller to an existing domain | |
| Create a new domain in an existing forest This server will become the first domain controller in the new domain. | |
| Create a new domain tree root instead of a new child domain | |
| Create a new domain in a new forest | |
| More about possible deployment configurations | |
| | |
| | |
| | |
| < Back Next > Ca | incel |

Click Next.

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

| Active Directory Domain Services Installation Wizard | × |
|--|-------|
| Name the Forest Root Domain The first domain in the forest is the forest root domain. Its name is also the name of the forest. | |
| Type the fully qualified domain name (FQDN) of the new forest root domain. | |
| FQDN of the forest root domain: Solutions.net | _ |
| | |
| Example: corp.contoso.com | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| < Back Next > Ca | ancel |
| | |

► 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.

| Active Directory Domain Services Installation Wizard | × |
|---|--------|
| Additional Domain Controller Options | |
| Select additional options for this domain controller. | |
| DNS server | |
| 🔽 Global catalog | |
| Read-only domain controller (RODC) | |
| Additional information: | |
| cannot be an RODC. We recommend that you install the DNS Server service on the first do controller. | main |
| More about additional domain controller options | |
| < Back Next > | Cancel |

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.

| Active Directory Users and Computers | | | | |
|--|----------------------------------|-----|--|--|
| File Action View Help | | | | |
| 🗢 🔿 🔰 📊 🖌 📋 🛠 🛛 |] 🖸 😖 🛛 🖬 🗏 🐭 🗑 🔻 | 1 | | |
| Active Directory Users and Comput | Name Type | De | | |
| 🕀 🚞 Saved Queries | Accountant01 User | | | |
| NewForest.Com | & Accountants Security Group | 1 | | |
| 🕀 🚞 Builtin | Administrator User | Buj | | |
| E Computers | & Allowed ROD Security Group | Me | | |
| 🕀 📴 Domain Controllers | & Cert Publishers Security Group | Me | | |
| ForeignSecurityPrincipals | & Denied ROD Security Group | ME | | |
| Delegate Control | DnsAdmins Security Group | DN | | |
| Find | DnsUpdatePr Security Group | DN | | |
| | Domain AdminsSecurity Group | De | | |
| New | Computer Group | All | | |
| All Tasks | Contact Group | AIL | | |
| View | Group / Group | All | | |
| | InetOrgPerson Group | All | | |
| Refresh | MSMQ Queue Alias Group | Dei | | |
| Export List | Printer / Group | Me | | |
| Properties | User / Group | Me | | |
| | Shared Folder | Bu | | |
| Help | Marketer01 User | 1 | | |
| | Recurity Group | - | | |
| | 🧟 RAS and IAS Security Group | Se | | |
| and the second sec | Read-opty D "equilibric Crownson | We | | |

▶ Type in a Group Name.

| Yeate in: NewForest.Com/Users Group name: Engineering Group name (pre-Windows 2000): Engineering Group scope Group type O Domain local © Security © Global Distribution OK Cancel | ew Object - Group | X |
|---|--------------------------------|----------------|
| Engineering Group name (pre-Windows 2000): Engineering Group scope O Domain local O Global O Universal | Create in: NewFores | st.Com/Users |
| Group name (pre-Windows 2000): Engineering Group scope O Domain local O Global O Universal | Group name: | |
| Engineering Group scope O Domain local O Global Universal | Engineering | |
| Engineering Group scope O Domain local O Global Universal | Group name (pre-Windows 2000): | |
| C Domain local C Global C Universal | | |
| C Domain local C Global C Universal | - Croup areas | - Crown have |
| © Global © Universal | | |
| C Universal | | |
| | | S Distribution |
| OK Cancel | | |
| OK Cancel | | |
| | | OK Cancel |

• 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.

| 011011000110110001101001011001010 | | | | |
|-------------------------------------|----------------------|----------------|-----|--|
| Active Directory Users and Com | | | | |
| File Action View Help | | | | |
| 🗢 🔿 🖄 💼 🔏 🗈 🛠 🖬 | i 🖸 🔒 🔽 🖬 | 1 🙁 🐮 🏹 | | |
| 📔 Active Directory Users and Comput | Name | Туре | De | |
| 🕀 🚞 Saved Queries | 👗 Accountant01 | User | - 3 | |
| NewForest.Com | & Accountants | Security Group | - 3 | |
| 🕀 🔛 Builtin | \delta Administrator | User | Bu | |
| Computers | & Allowed ROD | Security Group | Mé, | |
| | & Cert Publishers | Security Group | Me | |
| | Benied ROD | Security Group | Me | |
| Delegate Control | & DnsAdmins | Security Group | DN | |
| Find | & DnsUpdatePr | | DN | |
| New | Computer | Formity Group | Des | |
| All Tasks | Contact | rity Group | All | |
| Airtaka | Group | rity Group | All | |
| View 🕨 | InetOraPerson | rity Group | All | |
| Refresh | MSMQ Queue Alia | rity Group | All | |
| Export List | Printer | irity Group | | |
| | User | irity Group | Des | |
| Properties | Shared Folder | irity Group | Mé | |
| Help | 1.0 | urity Group | Me. | |
| incip. | Guest | User | Bui | |
| - Automation - and - and - | Marketer01 | User | | |

► Type in the user details.

| w Object - User | | |
|----------------------|----------------------|--------|
| Create in: | NewForest.Com/Users | |
| First name: | Engineer01 Initials: | |
| Last name: | | |
| Full name: | Engineer01 | |
| User logon name: | | |
| Engineer01 | @NewForest.Com | • |
| User logon name (pre | -Windows 2000): | |
| NEWFOREST\ | Engineer01 | |
| | | |
| | < Back Next > | Cancel |

Click Next.

▶ Type in the user Password.

| New Object - User | × |
|--|------|
| Create in: NewForest.Com/Users | |
| Password: Confirm password: | |
| User must change password at next logon User cannot change password | |
| Password never expires Account is disabled | |
| | |
| < Back Next > Ca | ncel |

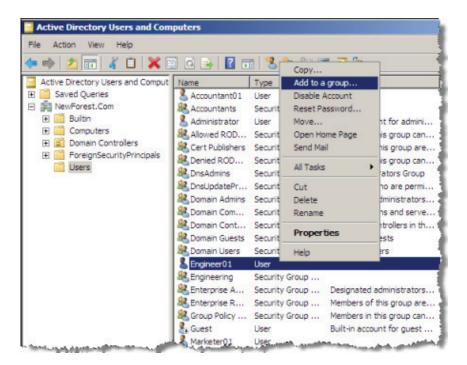
► Click Next.

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...



00010000001100114

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

| Select Groups | ? × |
|--|--------------|
| Select this object type: | |
| Groups or Built-in security principals | Object Types |
| From this location: | |
| NewForest.Com | Locations |
| Inew dest.com | Locations |
| Common Queries | |
| Name: State with | Columns |
| Name: Starts with 💌 | |
| Description: Starts with 🔽 | Find Now |
| Disabled accounts | Stop |
| Non expiring password | |
| | |
| Days since last logon: | |
| | |
| | |
| | DK. Cancel |
| Search results: | |
| Name (RDN) Description In Folder | |
| | |

- 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.

| elect Groups | | | | ? |
|--|--|---|---------------|------------------|
| Select this object ty | | | | |
| Groups or Built-in s | security principals | | <u>O</u> bjec | t Types |
| rom this location: | | | | |
| NewForest.Com | | | Loc | ations |
| Common Queries | | | | |
| N <u>a</u> me: | Starts with 💌 | | - | <u>C</u> olumns |
| Description: | Starts with 💌 | | - | Find <u>N</u> ow |
| □ □ Disabled ac | counts | | | Stop |
| Non expiring | | | | |
| | n naxwinin | | | |
| Hollogphili | g password | | | ~ |
| Days since last | | | | - 77/ |
| | | | | 9 7 |
| | | | | 9 7 |
| Days since last | | | ок | 970 Cancel |
| Days since last earch res <u>ults:</u> | logon: | In Folder | ОК | Solution Cancel |
| Days since last earch res <u>u</u> lts: ame (RDN) | logon: | In Folder NewForest.Com | ок | Cancel |
| Days since last earch res <u>ults:</u> ame (RDN) | Description All workstations | | ОК | Cancel |
| Days since last earch res <u>ults:</u> ame (RDN) Domain Comp Domain Contr | Description All workstations All domain contr | NewForest.Com | ок | Cancel |
| Days since last earch res <u>ults:</u> ame (RDN) Domain Comp Domain Contr | Description All workstations All domain contr | NewForest.Com NewForest.Com | ок | Cancel |
| Days since last learch results: ame (RDN) Domain Comp Domain Contr Domain Guests | Description All workstations All domain contr All domain guests | NewForest.Com NewForest.Com NewForest.Com | ок | Cancel |
| Days since last earch results: ame (RDN) Domain Comp Domain Contr Domain Guests Domain Users | Description All workstations All domain contr All domain guests | NewForest.Com NewForest.Com NewForest.Com NewForest.Com NewForest.Com | ок | Cancel |

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.

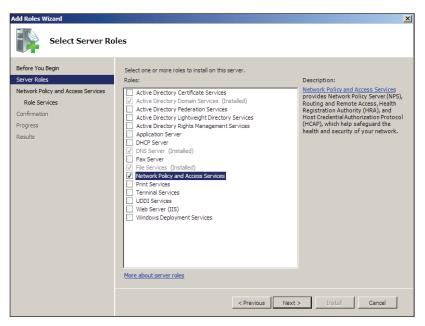
Installing Network Policy Server

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.

| Add Roles Wizard | | X |
|---|--|---|
| Select Role Serv | ices | |
| Before You Begin Server Roles Network Policy and Access Services Confirmation Progress Results | Select the role services: Description: Routing provides support for NAT Routing provides support for NAT Routing in a diamote Access Services Routing in a diamote Access Services Routing in a diamote Access Service Routing in a diamote Access Service Head the Registration Authority Host Credential Authorization Protocol More about role services More about role services Korting Kentrest contact conta | |

- 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.

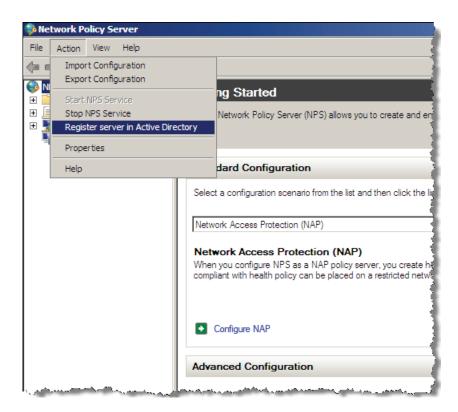
| Add Roles Wizard | | x |
|--|--|---|
| Installation Resu | ilts | |
| Before You Begin Server Roles Network Policy and Access Services Role Services Confirmation Progress Results | Installation successfully: • Network Policy and Access Services • Installation succeeded Installation succeeded The following role services were installed: Network Policy Server Routing and Remote Access Services Reviewere Access Service Image: A ccess Service | |
| | Print, e-mail, or save the installation report | |
| | <previous next=""> Close Cancel</previous> | |

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.

| 📕 Server Manager | | |
|---|--|---|
| File Action View He | elp | |
| 🗢 🔿 🔰 🔂 | | |
| Server Manager (NPS1) | NPS (Local) | 2 |
| Roles Active Director Active Director Active Director Active Director Active Director NS Server NNS Server Network Policy | y Domain Se and Access | ted blicy Server (NPS) allows you to create and a n-wide network access policies for client heat request authentication, and connection requ |
| ⊟ ♦ NPS (Local) | Import Configuration | tion |
| ⊕ | Stop NPS Service | nario from the list and then click the |
| | Register server in Active Direct Properties | n (NAP) |
| | View | |
| | Help | ble client computers before they con ampoint can be placed on a restricted netv |
| | into compliance. | _ |
| | Advanced Co | nfiguration |

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...

| 🚡 File Action View Favorites Window | Help | | |
|---------------------------------------|----------|-------------------------|------|
| 🔶 🔿 🞽 📅 📋 🗳 👘 | | | 1 |
| Console Root | Issued 1 | To 🔺 | Issu |
| 🖃 🚋 Certification Authority (Local) | New | Forest-NPS1-CA | New |
| 🖃 🝶 NewForest-NPS1-CA | | 1.NewForest.Com | New |
| Revoked Certificates | | 1.NewForest.Com | New |
| Issued Certificates | | 1.NewForest.Com | New |
| Pending Requests | | | - 1 |
| Failed Requests | | | - 3 |
| Certificate Templates | | |) |
| Certificates (Local Computer) | | | - 2 |
| Personal Certificates | | | - 1 |
| Certificates All Tasks | • | Request New Certificate | - 1 |
| Enterprise Trust | | Import | - 3 |
| Intermediate Ce View | • | | - 1 |
| Trusted Publishe New Window fro | m Here | Advanced Operations | 1 |
| 🕀 🧮 Untrusted Certi 🛛 New Taskpad Vie | w | | - 1 |
| 🕀 📔 Third-Party Roo ———— | | - | 1 |
| | | | - 2 |
| 🕀 🚞 Certificate Enro 🛛 Export List | | | - 7 |
| E Smart Card Trus Help | | - - | |
| 160 | 1 | | - 1 |
| | ن الله | | ~.d |

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.

| 🙀 Certificate Enrollment | | |
|--|---|------------------------------|
| 🔄 Certificate Enrollment | | |
| Request Certificates You can request the following types of certificates | stes. Select the certificates you want to req | uest, and then click Enroll. |
| Directory Email Replication | i) STATUS: Available | Details(y) |
| Domain Controller | 🔅 STATUS: Available | Details |
| Domain Controller Authentication | i) STATUS: Available | Details |
| RAS and IAS Server | 🔅 STATUS: Available | Details() |
| | | |
| | | |
| Show all templates | | |
| Learn more about <u>certificate types</u> | | |
| | | Enroll Cancel |

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.

| 🞭 Network Policy Server | |
|--|-------------------------|
| File Action View Help | 1 |
| 🗢 🔿 🙍 🖬 🛛 🖬 | |
| E RADIUS Clients and Servers | JS clients allow you to |
| RADIUS Clients Remote RADIU | |
| Export List | IP Address D |
| Connection Rec View | 192.168.0.3 F |
| Network Policies Refresh | 192.168.0.56 |
| | 192.168.2.10 R |
| Network Access Pro Help Accounting | |
| | 1 |
| | |
| | |

The New RADIUS client window opens.

Fill in the details of the RADIUS client:

| New RADIUS Client |
|--|
| Enable this RADIUS client |
| Name and Address |
| Friendly name: |
| 8000S |
| Address (IP or DNS): |
| 192.168.2.11 Verify |
| Vendor |
| Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list. |
| Vendor name: |
| RADIUS Standard |
| Shared Secret |
| To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. |
| Manual O Generate |
| Shared secret: |
| ••••• |
| Confirm shared secret: |
| ••••• |
| Additional Options Additional Options Access-Request messages must contain the Message-Authenticator attribute RADIUS client is NAP-capable |
| OK Cancel |

- ► 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.

| Network Policy Server | | |
|--|--|---|
| File Action View Help | | |
| 🗢 🔿 🙍 🖬 👔 🖬 | | |
| NPS (Local) ADIUS Clients and Servers Policies Connection Request Policies | Connection request policies allow you to design locally or forwarded to remote RADIUS servers PEAP authentication in connection request po | |
| Network New | Policy Name Status | |
| Health P Export List | | ed 2 Unspecified |
| Network Acc View | | ed 3 Unspecified |
| Accounting | Disabl | |
| Refresh | Use Windows authentication for all users Disabl | ed 999999 Unspecified |
| Help | | |
| | E Locally Processed | |
| | | |
| | Conditions - If the following conditions are met: | |
| | Condition Value | |
| | Day and time restrictions Sunday 00:00-24:00 Mon | day 00:00-24:00 Tuesday 00:00-24:00 Wednesday |
| | | |
| | | |
| | | |
| | | |
| | Settings - Then the following settings are applied: | |
| | Contra 1 | alue |
| | | aue ocal Computer |
| | Extensible Authentication Protocol Configuration C | |
| | I I | • |
| New | | |
| 1 | |) |

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

| New Connectio | n Request Policy | X |
|----------------|---|---|
| | Specify Connection Request Policy Name and Connection Type | |
| | You can specify a name for your connection request policy and the type of connections to which the policy is applied. | |
| Policy name | : | |
| Locally Proces | ssed | |
| type or Vendor | ed | |
| | | |
| | Previous Next Finish Cancel | 1 |

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.

| New Connection | Request Policy | × |
|----------------|---|---------------------------------|
| | Specify Conditions | |
| | Specify the conditions that Day and time restrictions | × |
| Carathiana | Select condition 12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12 | ОК |
| Conditions: | Select a condition, and th | Cancel |
| | Tunnel Type The Tunnel Type Monday | _ |
| | Day and time Tuesday | Permitted |
| | Day and Time R Day and Time R Expressions are constructed as a construction are constructed as a constructed as constructed as constructed as a constructed as a constructed as | C Denied |
| | Identity Thursday | |
| | Identity Type The Identity Typ Saturday | |
| | RADIUS Client Sunday through Saturday from 12:00 AM to 12:00 AM | |
| | Calling Station The Calling Station to condition specifies the network access server telephone norm | per graned by the access chemi. |
| Condition des | | |
| | | Add Cano |

- 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:

| | n Request Policy |
|-------------|--|
| | Specify Authentication Methods |
| | Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP. |
| Override | network policy authentication settings |
| | ntication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X, with NAP, you must configure PEAP authentication here. |
| EAP types a | re negotiated between NPS and the client in the order in which they are listed. |
| EAP Types | |
| | Move Up Move Down |
| Add | Edit Remove |
| | re authentication methods: |
| | t Encrypted Authentication version 2 (MS-CHAP-v2) can change password after it has expired |
| | t Encrypted Authentication (MS-CHAP) |
| | can change password after it has expired id authentication (CHAP) |
| | pted authentication (PAP, SPAP) |
| | ents to connect without negotiating an authentication method. |

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

<u>201</u>00000010

| w Connection Reques | Policy | x |
|---|--|---|
| Comp | leting Connection Request Policy Wizard | |
| You have successfully cre Locally Processe | ated the following connection request policy: | |
| Policy conditions: | | |
| Condition | Value | |
| | Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00: | |
| Policy settings: Condition | Value | |
| Authentication Provider | | |
| To close this wizard, click | Finish. | |
| | Previous Next Finish Cancel | 1 |

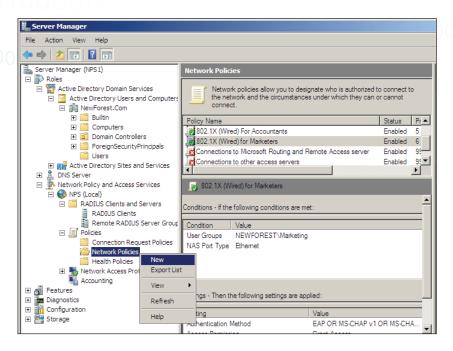
Setting up Network Policies

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.

| Specify Network Policy Name and Connection Type To can specify a name for your network policy and the type of connections to which the policy is applied Policy name Specify Connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server Inspecified Unspecified Image: Specified | New Network P | Policy | X |
|--|---|---|---|
| 802.1x (Wired) For Engineers Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific Unspecified 10 | | | |
| Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or feative access server: Unspecified Vendor specific: 10 4 | Policy name | x. | |
| Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific. | 802.1x (Wired | i) For Engineers | |
| | Select the type type or Vendor Type of ne Unspecifie O Vendor spe | e of network access server that sends the connection request to NPS. You can select either the network access server repectic. etwork access server: ed | |
| Previous Next Finish Cancel | | Previous Next Sixth Count | 1 |

Click Next.

Tested Solution | Networking

In the Specify Conditions window:

Click Add...

Mathematical Conductions

Mathematical Conductions

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum

| Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required. | | | | | |
|--|-------|----------|------|--------|--------|
| Conditions: | | | | | |
| Condition | Value | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Condition description: | | | | | |
| Condition accomption. | | | | | |
| | | | | | |
| | | | | | |
| | | | Add | Edit | Remove |
| | | | | | |
| | | | | | |
| | | Previous | Next | Finish | Cancel |
| | | Frevious | INEX | FINISH | Cancel |

▶ Select User Groups, and click Add...

| New Netw | vork Policy |
|------------|--|
| | Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required. |
| Select cor | ndition |
| Select a d | condition, and then click Add. |
| Groups | |
| | Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected |
| | Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups. |
| | User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups. |
| HCAP | |
| 1 | Location Groups The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition. |
| 60 | HCAP User Groups |
| | A <u>d</u> d Cancel |

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

▶ In this window, click Add Groups...

| New Network Policy | | |
|---|-----------------------------------|--|
| Specify Conditions Specify the conditions that determine whether this network policy is evaluated for of one condition is required. | r a connection request. A minimum | |
| Select condition | X | |
| Select a condition, and the User Groups | × | |
| Groups Windows Group The Windows Group Groups Groups Groups | f the selected | |
| Machine Group: The Machine Gro | ected groups. | |
| User Groups The User Groups HCAP | ups. | |
| Location Group The HCAP Locati required to match network access s Add Groups Remove | ocation groups e third party | |
| Add Groups | al Add Cancel | |

This will open the Select Group window.

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

| Select Group | ? × |
|--------------------------------------|--------------|
| Select this object type: | |
| Group | Object Types |
| From this location: NewForest.Com | |
| J, | Locations |
| Common Queries | |
| Name: Starts with | Columns |
| Description: Starts with | Find Now |
| Disabled accounts | Stop |
| Non expiring password | |
| Days since last logon: | |
| | |
| | OK. Cancel |
| Search results: | |
| Name (RDN) Description In Folder | |
| | |
| | |
| | |
| | |
| | |
| | |
| l | |

Click Find Now.

| lect Group | |
|--|--------------|
| beleur this object type. | |
| Group | Object Types |
| From this location: | |
| NewForest.Com | Locations |
| Common Queries | |
| | |
| Name: Starts with 💌 | Columns |
| Description: Starts with | Find Now |
| | |
| Disabled accounts | Stop |
| Non expiring password | |
| Days since last logon: | |
| <u> </u> | |
| | |
| | |
| | |
| Search results: | OK Cancel |
| lame (RDN) Description In Folder | OK Cancel |
| Search results: lame (RDN) Description In Folder Denied ROD Members in this NewForest.Com DnsAdmins DNS Administrat NewForest.Com | OK Cancel |

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.

| New Network P | olicy | | | | | | × |
|----------------------------------|-------|---|------------------|------------------|-------------------|--------------------|------------------|
| | | onditions ditions that determine n is required. | e whether this | network polic | / is evaluated fo | or a connection re | quest. A minimum |
| Conditions: | | | | | | | |
| Condition | n | Value | | | | | |
| 🚨 User Gro | ups | NEWFOREST\Engine | eering | | | | |
| Condition desc The User Group | | ifies that the connecting | g user must bela | ong to one of th | e selected group | NS. | |
| | | | | | A <u>d</u> d | <u>E</u> dit | <u>R</u> emove |
| | | | [| <u>P</u> revious | <u>N</u> ext | Einish | Cancel |

NewForest.Com..

NewForest.Com..

NewForest.Com.

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

👫 Domain Users 🛛 All domain users

Enterprise Ad... Designated admi...

Engineering

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

| New Network P | Policy X |
|---------------------------|--|
| | Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy. |
| C Access de Deny acces | ss if client connection attempts match the conditions of this policy. |
| | Brevious Next Einish Cancel |

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

| New Network P | olicy | × | | |
|---|--|--|--|--|
| | authentication, you must configure an EAP type | thods required for the connection request to match this policy. For EAP . If you deploy NAP with 802.1X or VPN, you must configure ch overrides network policy authentication settings. | | |
| EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up | | | | |
| | | Add EAP X Authentication methods: Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) | | |
| Microsoft E | Edit Remove authentication methods: norypted Authentication version 2 (MS-CHAP-v2) in change password after it has expired norypted Authentication (MS-CHAP) | Microsoft: Secured password (EAP-MSCHAP v2) | | |
| Encrypted Unencrypte Allow client | n change password after it has expired authentication (CHAP) id authentication (PAP, SPAP) is to connect without negotiating an authentication m chine health check only | OK Cancel | | |
| | | Previous Next Einish Cancel | | |

- ► 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.

| New Network | Policy | | × |
|---|--|--|---|
| | Configure NPS applies set are matched. | Settings gs to the connection request if all of the network policy | conditions and constraints for the policy |
| | settings for this netw nd constraints matc | rk policy. he connection request and the policy grants access, settin | gs are applied. |
| RADIUS AI Standa Control Vendor Network Ai Protection NAP Er Extend Routing an Access | rd Specific cocess nforcement ed State | To send additional attributes to RADIUS clients, selective noick Edit, if you do not configure an attribute, it your RADIUS client documentation for required attributes: Attributes: Name Value Framed-Protocol PPP Service-Type Framed | is not sent to RADIUS clients. See |
| | dth Allocation ol (BAP) rs tion | Add Edit Remove | |
| | | Previous N | ext <u>Finish</u> Cancel |

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

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

| Add Standard RADIUS Attribute | × |
|---|-----|
| To add an attribute to the settings, select the attribute, and then click Add. | |
| To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add. | |
| Access type: | |
| Attributes: | |
| Name | 1 |
| Tunnel-Password | |
| Tunnel-Preference | |
| Tunnel-Pvt-Group-ID | |
| Tunnel-Server-Auth-ID | |
| Tunnel-Server-Endpt | Į . |
| Tunnel-Type | 1 |
| | 1 |
| Description: | |
| Specifies the tunneling protocols used. | |
| Add Close | |

► 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).

| Attribute Information | × |
|------------------------------------|-----------|
| Attribute name: Tunnel-Type | |
| Attribute number: 64 | |
| Attribute format: Enumerator | |
| Attribute Value: | |
| C Commonly used for Dial-Up or VPN | |
| <none></none> | v |
| Commonly used for 802.1x | |
| Virtual LANs (VLAN) | • |
| O Others | |
| <none></none> | v |
| | OK Cancel |
| | |

- 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

| Add Standard RADIUS Attribute |
|--|
| To add an attribute to the settings, select the attribute, and then click Add. |
| To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add. |
| Access type: All |
| Attributes: |
| Name |
| Tunnel-Client-Endpt |
| Tunnel-Medium-Type |
| Tunnel-Password |
| Tunnel-Preference |
| Tunnel-Pvt-Group-ID |
| Tunnel-Server-Auth-ID |
| Tynnal Server Endot |
| |
| |
| Description: |
| Specifies the transport medium used when creating a tunnel for protocols (for example, L2TP) that can operate over multiple transports. |
| Add Close |

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

| 001100 | |
|--|----------|
| Attribute Information | × |
| Attribute name: Tunnel-Medium-Type | |
| Attribute number: 65 | |
| Attribute format: Enumerator | |
| Attribute Value: Commonly used for 802.1x | |
| 802 (includes all 802 media plus Ethemet canonical format) | • |
| C Others | |
| <none></none> | v |
| ОК | Cancel |

- ▶ 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:

| Add Standard RADIUS Attribute | x |
|--|---|
| To add an attribute to the settings, select the attribute, and then click Add. | |
| To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add. | |
| Access type: All | |
| Attributes: | |
| Name | - |
| Tunnel-Client-Endpt | |
| Tunnel-Medium-Type | |
| Tunnel-Password | |
| Tunnel-Preference | |
| Tunnel-Pvt-Group-ID | |
| Tunnel-Server-Auth-ID | - |
| Typnel-Server-Endat | - |
| Description: Specifies the Group ID for a tunneled session. | |
| Add Close | |

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

| Attribute Information | <u>×</u> |
|---|-----------|
| Attribute name: Tunnel-Pvt-Group-ID | |
| Attribute number: 81 | |
| Attribute format: OctetString | |
| Enter the attribute value in: • String | |
| C Hexadecimal | |
| 20 | |
| | OK Cancel |

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

| New Network Policy | | | | | | |
|--|--|-----------------|----------------|--|--|--|
| | Configure Se NPS applies settings are matched. | | n request if a | all of the network policy conditions and constraints for the | | |
| | Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied. Settings: | | | | | |
| RADIUS At Standar Vendor Network Ac Protection | d Specific | then click Edit | If you do no | s to RADIUS clients, select a RADIUS standard attribute, and t configure an attribute, it is not sent to RADIUS clients. See entation for required attributes. | | |
| NAP En | forcement | Attributes: | | Value | | |
| N Extende | ed State | Tunnel-Type | | Virtual LANs (VLAN) | | |
| Routing an Access | d Remote | Tunnel-Media | | 802 (includes all 802 media plus Ethemet canonical for 20 | | |
| Multilini Bandwie Protoco | dth Allocation | | 1000-12 | 20 | | |
| IP Filter | rs | | | | | |
| Recrypt | tion | A <u>d</u> d | <u>E</u> dit. | <u>R</u> emove | | |
| IP Settir | ngs 💌 | | | | | |
| | | | | | | |

► 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

 $^{\circ}$ There are two steps to setting up the Client PCs: $^{\circ}$

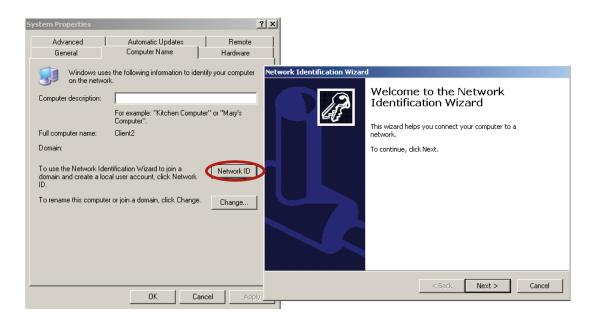
- ► Join the PCs to the Domain
- ► Configure the PCs as 802.1x supplicants

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, ...

| Network Identification Wizard | |
|---|------|
| Connecting to the Network How do you use this computer? | B |
| Select the option that best describes your computer: | |
| This computer is part of a business network, and I use it to connect to other computers at work | |
| This computer is for home use and is not part of a business network. | |
| < Back Next > Car | ncel |

Click Next.

▶ In the next window, choose My company uses a network with a domain.

| Network Identification Wizard | | |
|---|--|--|
| Connecting to the Network What kind of network do you use? | | |
| Select the option that best describes your company network: | | |
| • My company uses a network with a domain | | |
| C My company uses a network without a domain | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| < Back Next > Cancel | | |

► 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.

| Network Identification | n Wizard | | | | | | |
|------------------------|--|--|--|--|--|--|--|
| | User Account and Domain Information A user account gives you access to files and resources on a network. | | | | | | |
| | Type your Windows user account and domain information. If you do not have this information, ask your network administrator. | | | | | | |
| User name: | Engineer01 | | | | | | |
| Password: | ••••• | | | | | | |
| <u>D</u> omain: | NEWFOREST | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | < Back Next > Cancel | | | | | | |

► 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.

| 上 Test LAN Properties | ? × |
|--|--------|
| General Authentication Advanced | |
| General Authentication Advanced Select this option to provide authenticated network acces this Ethernet adapter ✓ Enable IEEE 802.1× authentication Choose a network authentication method: Protected EAP (PEAP) ✓ Settings Cache user information for subsequent connections to this network | ss for |
| | |
| OK | Cancel |

- 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.

| EAP MSCHAPy2 Properties | | | |
|---|--|--|--|
| | | | |
| When connecting: | | | |
| Automatically use my Windows logon name and password (and domain if any). | | | |
| OK Cancel | | | |

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.

00000|Triple-Auth#show vlan 20 00000|Triple-Auth#show vlan 20

| VLAN ID | Name | Туре | 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 vian

console# show dot1x ethernet 1/e1

802.1x is enabled

| Dowt | Admin | Oper | Reauth Control | Reauth | Username |
|----------|-------|------------|-------------------|--------|----------------------|
| Port | Mode | Mode | | | |
| 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 Mach | |
| State: | AUTHENTICATED |
| | |
| Backend State Machine | TDIE |
| State: | IDLE |

| State: | | ΤL |
|----------------|----------|----|
| Authentication | success: | 11 |
| Authentication | fails: | 7 |

console# sh vlan

| Vlan | Name | Ports | Туре | Authorization |
|------|------|---|-----------|---------------|
| | | | | |
| 1 | 1 | <pre>1/e(2-5,7-48),1/g(1-4), 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)</pre> | other | Required |
| 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.

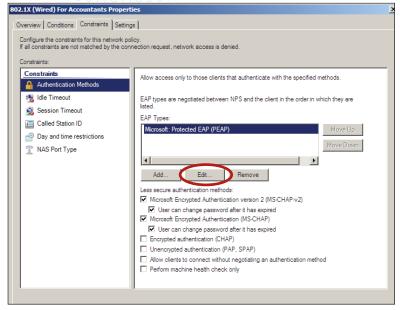
In the example below, we will edit the Accountants Network Policy.

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

| Network Policies | | | | |
|---|-------|--|--|--|
| Network policies allow you to designate who is authorized to connect to the network and the circan or cannot connect. Move Up Policy Name Move Down S02.1X (Wired) For Accountants Delete 802.1X (Wired) For Encineers Rename Duplicate Policy Properties 802.1X (Wired) For Accountants Help Conditions - If the following conditions are met: Accountants | | | | |
| Condition Value User Groups NEWFOREST\Accountants | | | | |
| Settings - Then the following settings are a Setting Extensible Authentication Protocol Config Ignore User Dial-In Properties Access Permission | Value | | | |

Tested Solution | Networking In the Properties window, open the Constraints tab.

- 00000



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.

| E | dit Protected EAP Prope | erties | × | | |
|--|---|---------------------|---|--|--|
| | Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate. | | | | |
| | Certificate issued | NPS1.NewForest.Com | | | |
| | Friendly name: | | | | |
| | Issuer: | NewForest2003 | | | |
| | Expiration date: | 4/8/2010 9:07:50 PM | | | |
| Enable Fast Reconnect Disconnect Clients without Cryptobinding Eap Types | | | | | |
| | Smart Card or other certif Secured password (EAP-M | | | | |
| | Add Edit | Remove OK Cance | : | | |

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

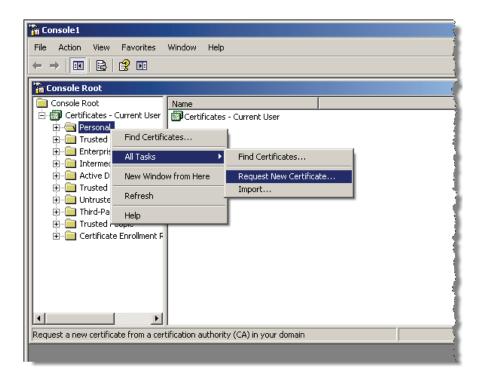
- Obtain user certificates
- Download the Certificate Authority server's Root certificate
- Set up the NIC card to perform authentication by certificate

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...



011001010110111001100101000000

This will open the Certificate Request Wizard:



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

| Certificate Request Wizard | × | | | |
|--|-----------|--|--|--|
| Certificate Types A certificate type contains preset properties for certificates. | | | | |
| Select a certificate type for your request. You can access only certificate ty you have permissions for and that are available from a trusted CA. | /pes that | | | |
| Certificate types: | | | | |
| Bacic EES User | | | | |
| To select a cryptographic service provider and a CA, select Advanced. | | | | |
| < Back Next > | Cancel | | | |

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

| ertificate Friendly Name and Descri You can provide a name and description | n that help you quickly identify a specif | ic |
|---|---|--------|
| certificate. | | |
| | | |
| Type a friendly name and description f Friendly name: | or the new certificate. | |
| Engineer Cert | _ | |
| | | |
| Description: | | |
| Certiuficate for authentication | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < <u>B</u> ack <u>N</u> ext > | Cancel |
| | | |

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).

| 🏉 Internet B | Explorer | cannot display the webpage - Windows Internet Explorer |
|--------------|----------|--|
| OO - | 🦲 http | ://192.168.2.253/certsrv 💽 🐓 🗙 Live Search |
| 🖌 🏟 (| Connec | ting 🏠 🔹 🗟 👻 🖶 🕈 🖻 Pa |
| i | Inte | Connect to 192.168.2.253 |
| | Most | Connecting to 192.168.2.253. |
| | • | |
| | • | User name: I NewForest\Engineer01 v |
| | What | Password: |
| | • D | |
| | 🕞 M | OK Cancel |
| | h statio | |

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.

| Alicrosoft Certificate Services - Windows Internet Explorer | |
|---|--|
| C C + I Ttp://192.168.2.253/certsrv/ | 💽 🛃 🗙 Live Search 🖉 🗸 |
| 😪 🎄 🍘 Microsoft Certificate Services | 🏠 🔹 🔝 👻 🖶 🔹 🕑 Page 🔹 🎯 Tools 🔹 🍟 |
| Microsoft Certificate Services NewForest2003 | Home |
| Welcome | |
| Use this Web site to request a certificate for your We certificate, you can verify your identity to people you c messages, and, depending upon the type of certificat | ommunicate with over the Web, sign and encrypt |
| You can also use this Web site to download a certificat certificate revocation list (CRL), or to view the status of | |
| For more information about Certificate Services, see | Certificate Services Documentation. |
| Select a task: Request a certificate View the statue of a pending certificate request | |
| Download a CA certificate, certificate chain, or CF | |
| | |
| | |
| | |
| http://192.168.2.253/certsrv/certrqus.asp | Internet €, 100% |

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

Click the link Download CA certificate

| All Crosoft Certificate Services - Windows Internet Explorer | |
|--|-----------------|
| Coo v 🖉 http://192.168.2.253/certsrv/certcarc.asp | P - |
| 😪 🎄 🏉 Microsoft Certificate Services 🐴 🔹 🔂 🗸 🎰 Page 🔹 🎯 | Tools 🗸 » |
| | |
| Microsoft Certificate Services NewForest2003 | lome |
| Download a CA Certificate, Certificate Chain, or CRL | |
| To trust certificates issued from this certification authority, install this CA certificate chain. | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | |
| CA certificate: | |
| Current [NewForest2003] | |
| Encoding method: | |
| @ DER | |
| © Base 64 | |
| Download CA certificate | |
| Download latest base CRL | |
| Download latest delta CRL | |
| | — |
| | V |
| Done |)0% • // |

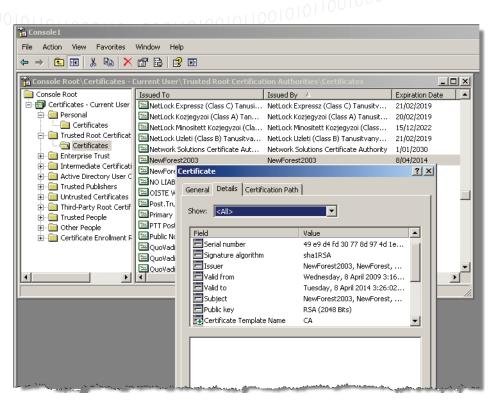
> You will then be offered the opportunity to open or save the certificate. Choose to Save it.

| Alicrosoft Certificate Services - Windows Internet Explorer | ۲ |
|--|---|
| 🚱 🕤 👻 🕅 http://192.168.2.253/certsrv/certcarc.asp | |
| 🙀 🎄 🌈 Microsoft Certificate Services 🏠 🔹 🔂 Page 🔹 🎯 Tools 🔹 | » |
| |] |
| Microsoft Certificate Services NewForest2003 Home | |
| Download a CA Certificate, Certificate Chain, or CRL | |
| To trust certificates issued from this certification authority, install this CA certificate chain. | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | |
| CA certificate: File Download - Security Warning | |
| Current [NewForest2003] Do you want to open or save this file? Name: certnew.cer Type: Security Certificate, 1.16KB From: 12,168,2,253 | |
| C DER Cappel Cappel | |
| © DER © Base 64 | |
| Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL | |
| Done Internet 🔍 100% 🗸 | |

• Click Yes on the next question.

| Potential | Scripting Violation | X |
|-----------|---|---|
| 1 | This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on computer and gain access to your data. | |
| | Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No. | |
| | Yes No | |

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:

| 🚣 Test LAN Properties | <u>?</u> × | | | | |
|--|------------|--|--|--|--|
| General Authentication | Advanced | | | | |
| Select this option to pro this Ethernet adapter. I Enable IEEE 802.1> Choose a network auth | | | | | |
| Protected EAP (PEAP) | 2 Settings | | | | |
| Protected EAP (PEAP) Settings Cache user information for subsequent connections to this network | | | | | |
| | OK Cancel | | | | |

▶ 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

Protected EAP Properties ? × When connecting: Validate server certificate Connect to these servers: Trusted Root Certification Authorities: 🔲 NetLock Uzleti (Class B) Tanusitvanykiado Network Solutions Certificate Authority NewForest2003 NewForeschiPS1-CA 🔲 OISTE WISeKey Global Root GA CA Post. Trust Root CA Primary Utility Root CA • • Þ $\hfill\square$ Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method: Configure... Smart Card or other Certificate • Enable Fast Reconnect П Enable Quarantine checks 🔲 Disconnect if server does not present cryptobinding TLV

▶ Click Configure...

| Smart Card or other Certificate Properties | | | | | | |
|---|--|--|--|--|--|--|
| | | | | | | |
| O Use my smart card | | | | | | |
| Use a certificate on this computer | | | | | | |
| ✓ Use simple certificate selection (Recommended) | | | | | | |
| | | | | | | |
| Validate server certificate | | | | | | |
| Connect to these servers: | | | | | | |
| | | | | | | |
| , | | | | | | |
| Trusted Root Certification Authorities: | | | | | | |
| Microsoft Root Certificate Authority | | | | | | |
| MPHPT Certification Authority | | | | | | |
| NetLock Expressz (Class C) Tanusitvanykiado | | | | | | |
| 🔲 NetLock Kozjegyzoi (Class A) Tanusitvanykiado | | | | | | |
| 🔲 🗖 NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado 💻 | | | | | | |
| NetLock Uzleti (Class B) Tanusitvanykiado | | | | | | |
| Network Solutions Certificate Authority | | | | | | |
| VewForest2003 | | | | | | |
| | | | | | | |
| View Certificate | | | | | | |
| Use a different user name for the connection | | | | | | |
| OK Cancel | | | | | | |

ОK

Cancel

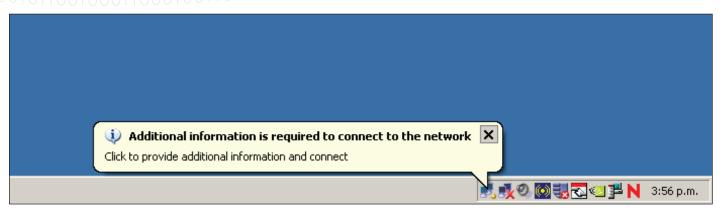
- ▶ In the Smart Card or other Certificate Properties window select:
 - Use a certificate on this computer
 - Use simple certificate selection
 - Validate server certificate

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.

| Select Certificate | | <u>?</u> × |
|---|------------------------|---------------|
| User name on certifica | ate: | |
| Engineer01@NewFo | rest.Com | - |
| Accountant01@New | | |
| Engineer01@NewFor Administrator@NewFor | prest.Com | |
| issuer: | INEWFOREST2003 | |
| Expiration date: | 9/04/2010 9:06:37 a.m. | |
| | | |
| | | |
| | OK Cancel View | v Certificate |

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.

Interface port1.0.13

Verifying the authentication from the switch command-line

```
10010
```

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>

```
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
```

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 downstraem of the same port. If an EAPforwarding L2 switch or hub is connected to an authenticating port of the x600 switch, 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

dynamicVlanId: 20

```
(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 dotlx 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
```

```
Tested Solution | Networking
...
....
dynamicVlanId: 10
 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
_____ ____
  Accounting STATIC ACTIVE port1.0.11(u) port1.0.13(u)
10
show vlan 20
VLAN ID Name
                           State Member ports
                    Туре
                              (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 Ba | ased Vlan Informa | tion: | Prio |
|--------|-------------------|-------|------|
| Index | Mac | Vid | |
| 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 ar | р | | | | | |
|----------|---------|----------------|-----------|-----------|---------|---------|
| IP . | Address | MAC Address | Interface | Port | Туре | |
| 192.168. | 2.253 0 |)0e0.1867.c69a | vlan2 | port1.0.4 | dynamic | |
| 192.168. | 2.254 | 000b.6af0.35f4 | vlan2 | port1. | 0.23 d | dynamic |
| 192.168. | 10.20 | 000e.2e5f.a7fc | vlan10 | port1. | 0.13 d | dynamic |
| 192.168. | 20.20 | 0002.b363.319f | vlan20 | port1. | 0.13 c | 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. By default, 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 (by default) : username = 00-02-4e-2a-80-b4 password = 00-02-4e-2a-80-b4

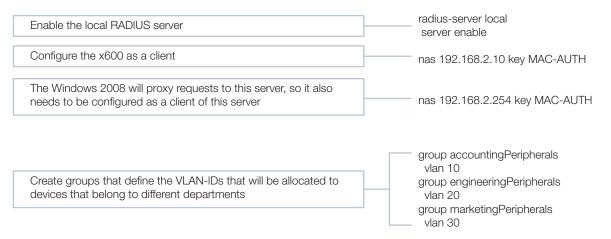
(ii) The x600 can be configured with different RADIUS servers for 802.1x and MAC-based authentication, whereas the 8000S must use the same RADIUS server for both types of authentication.

The solution to difference (i) above, is simple because fortunately, AlliedWare Plus can be configured to use different formats for the way that the MAC address is sent as a Username/Password. So, AlliedWare Plus can be configured to send the Username/Password in the same format as the 8000S uses. The command to configure this is:

auth-mac username unformatted

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 0002b363319f password 0002b363319f group engineeringPeripherals user 000065a383e4 password 000065a383e4 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:

| New Connectio | n Request Policy | x |
|----------------------------|--|---|
| | Specify Connection Request Policy Name and Connection Type You can specify a name for your connection request policy and the type of connections to which the policy is applied. | |
| Policy name MAC-Auth RA | DIUS | |
| type or Vendor | e of network access server that sends the connection request to NPS. You can select either the network access server | |
| Unspecifie | ed 💌 | |
| C Vendor spe | | |
| | | |
| | | |
| | | |
| | Previous Next Finish Cancel | 1 |

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....

| ew Connectio | n Request Policy | |
|--|--|----------|
| | Specify Conditions | |
| | Specify the conditions that determine whether this connection request policy is evaluated for a connection req A minimum of one condition is required. | uest |
| lect conditio | n | |
| Select a conditi | on, and then click Add. | |
| HCAP | | |
| require networ User User User I The us | er name that is used by the access client in the RADIUS message. This attribute is a character string that | |
| Connection | ly contains a realm name and a user account name. | |
| Acces | as Client IPv4 Address ccess Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access le RADIUS client. | |
| | as Client IPv6 Address cress Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access | • |
| | Add Cance | <u>+</u> |

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:

| User Name | × |
|---|---|
| Specify the user name of the access request message. You can use pattern matching syntax. | |
| [0-9a-fA-f]{12} | |
| OK Cancel | |

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:

| New Connectio | n Request Policy | | × |
|---|-------------------------|---|---|
| Specify Connection Request Forwarding The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group. | | | |
| | nditions match the conn | ection request, these settings are applied. | |
| Settings: Forwarding Connection Request Authentication Connection Accounting | | Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication. Authenticate requests on this server Forward requests to the following remote RADIUS server group for authentication: <u>snot configured></u> <u>New</u> Accept users without validating credentials | |
| | | Previous <u>N</u> ext Eiriish Cancel | 1 |

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.

| New Remote RADIUS Server Gro | oup | | × |
|------------------------------|----------|--------|----------------|
| <u>G</u> roup name: | | | |
| MAC-Auth Server | | | |
| RADIUS Servers: | | | |
| RADIUS Server | Priority | Weight | A <u>d</u> d |
| | | | <u>E</u> dit |
| | | | |
| | | | <u>R</u> emove |
| | | | |
| | | | |
| | | | |
| | | | |
| | | ОК | Cancel |
| | | | |

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

| Add RADIUS Server | × |
|--|---------|
| Address Authentication/Accounting Load Balancing | 1 |
| Type the name or IP address of the RADIUS server you want to add. Server: | |
| 192.168.2.252 | Verify |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | L Analy |
| OK Cance | Apply |

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

| Add RADI | IUS Server | × |
|----------|---|---|
| Address | Authentication/Accounting Load Balancing | |
| Authen | ntication port: | |
| Shared | d secret: | |
| Confirm | n shared secret: | |
| E Rec | equest must contain the message authenticator attribute | |
| Acco | ounting | |
| Acco | ounting port: 1813 | |
| ا 🗹 | Use the same shared secret for authentication and accounting. | |
| s | Shared secret: | |
| C | Confirm shared secret: | |
| | Forward network access server start and stop notifications to this server | |
| | | |
| | | |
| | OK Cancel Apply | |
| | | |

- ▶ 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):

| New Connectio | n Request Policy | | | × |
|-----------------------------------|---|--|--|-----------------|
| | Specify Connection Rec The connection request can be auther remote RADIUS server group. | | | US servers in a |
| | nditions match the connection request, th | ese settings are applied. | | |
| Settings: Forwardin Request | RADIÚS serve | rs for authentication, or are ac ta requests on this corror quests to the following remote | acessed locally, are forwarded to coepted without authentication. RADIUS server group for auther | |
| | | Previous | <u>N</u> ext Einish | Cancel |

- ▶ 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.

| Server | |
|--|---|
| File Action View Help | |
| 🗢 🔿 🖄 📷 🛛 🖬 | |
| NPS (Local) ADJUS Clients and Servers ADJUS Clients RADIUS Clients Remote RADIUS Server G Policies Connection Request Policie Network Policies Health Policies Health Policies | Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy. Policy Name Status Processing Order Unce MAC-Auth RADIUS Enable 3 Uspecified |
| n Accounting | Conditions - If the following conditions are met: Conditions - If the following conditions are met: Condition Value User Name [0-9a fA-F](12): |
| ۲ | Settings - Then the following settings are applied: Setting Value Authentication Provider Forwarding Request Authentication Provider Name MAC-Auth Server Image: |

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

 Tested Solution
 Networking

 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
 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.

| Add Roles Wizard | | × |
|---|---|---|
| Select Server Ro | bles | |
| Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings DHCP Scopes DHCP Scopes DHCP vof Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Results | Select one or more roles to install on this server. Roles: Description: | |

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

| Add Roles Wizard | | | × |
|--|---|---|---|
| Select Network (| Connection Bindings | | |
| Before You Begin Server Roles DHCP Server IPv4 DNS Settings IPv4 UNS Settings DHCP Scopes DHCPv6 Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Results | be used to service DHCP clients | ns having a static IP address were detected. Each network connection ca on a separate subnet. that this DHCP server will use for servicing clients. Type IPv4 | |
| | Details Name: Network Adapter: Physical Address: | Local Area Connection 2 Intel(R) PRO/100 VE Network Connection 00-08-6A-F0-35-F4 < <u>Previous</u> <u>Next > Install</u> Cancel | |

Click Next.

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

010010

| Add Roles Wizard | <u>×</u> |
|--|--|
| Specify IPv4 DN | S Server Settings |
| Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings IPv4 WINS Settings DHCP Scopes DHCP Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Results | When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4. Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server. Parent Domain: NewForest.Com Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server. Preferred DNS Server IPv4 Address: 192.168.2.254 Validate |
| | More about DNS server settings Next > Install Cancel |

- 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.

| dd Roles Wizard | | | 2 |
|--|---|---|------|
| Add or Edit D | OHCP Scopes | | |
| Before You Begin Server Roles | addresses to clients until a | | |
| DHCP Server | Add Scope | × | id |
| Network Connection Binding IPv4 DNS Settings | A scope is a range of possible IP distribute IP addresses to clients | addresses for a network. The DHCP server cannot until a scope is created. | it |
| IPv4 WINS Settings | | | lete |
| DHCP Scopes | Scope Name: | Accounting Private | |
| DHCPv6 Stateless Mode | Starting IP Address: | 192.168.10.20 | |
| IPv6 DNS Settings | Ending IP Address: | 192.168.10.210 | |
| DHCP Server Authorization Confirmation Progress Results | Subnet Mask: | 255.255.255.0 | |
| | Default Gateway (optional): | 192, 168.2, 10 | |
| | Subnet Type: | Wired (lease duration will be 6 days) | |
| | ☑ Activate this scope | OK Cancel | |

Click OK.

• Continue on to create all eight pools.

| Before You Begin Server Roles | A scope is the range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created. Scopes: | | |
|----------------------------------|--|--|--------|
| DHCP Server | Name | IP Address Range | Add |
| Network Connection Bindings | Accounting Private | 192, 168, 10, 20 - 192, 168, 10, 210 | - 10 |
| IPv4 DNS Settings | Engineering Private | 192.168.20.20 - 192.168.20.210 | Edit |
| IPv4 WINS Settings | Marketing Private Accounting Public/Private | 192.168.30.20 - 192.168.30.210 192.168.110.20 - 192.168.110.210 | Delete |
| DHCP Scopes | Engineers Public/Private | 192, 168, 120, 20 - 192, 168, 120, 210 | 1 |
| DHCPv6 Stateless Mode | Marketing Public/Private | 192.168.130.20 - 192.168.130.210 | |
| IPv6 DNS Settings | Visitors from other offices | 192.168.140.20 - 192.168.140.210 | |
| DHCP Server Authorization | External Visitors | 192.168.150.20 - 192.168.150.210 | |
| | | | |
| Confirmation | | | |
| Progress | | | |
| Results | | | |
| | Properties | | |
| | Add or select a scope to view its | properties. | |
| | More about adding scopes | | |

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

| Add Roles Wizard | | × |
|---|---|---|
| Authorize DHCF | Server | |
| Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings IPv4 WINS Settings DHCP Scopes DHCPv6 Stateless Mode | Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service clients on the network. Authorizing DHCP servers helps avoid accidental damage caused by running DHCP servers with incorrect configurations or DHCP servers with correct configurations on the wrong network. Specify credentials to use for authorizing this DHCP server in AD DS. Use current credentials The credentials of the current user will be used to authorize this DHCP server in AD DS. User Name: NEWFOREST\administrator | |
| DHCP Server Authorization Confirmation Progress Results | Use alternate credentials Specify domain administrator credentials for authorizing this DHCP server in AD DS. User Name: | |
| | < Previous Next > Install Cancel | |

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:

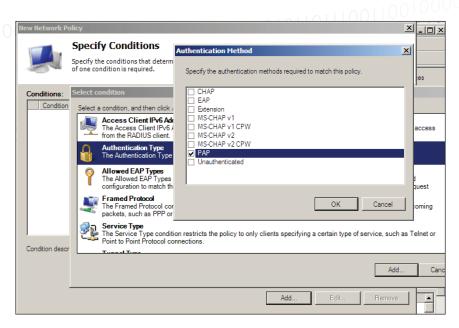
- Within the Network Policy Server manager, left-click on Network Policy in the left-hand pane, and choose New from the resulting pop-up menu. This will open the New Network Policy wizard.
- ▶ In the first window of the wizard, type in a Policy name.

| New Network P | olicy | × |
|---|--|---|
| | Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied. | |
| type or Vendor Type of ne Unspecifie C Vendor specifie | e Access ection method of network access server that sends the connection request to NPS. You can select either the network access server specific. twork access server: ed | |
| | Previous Next Finish Cancel | |

- 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.

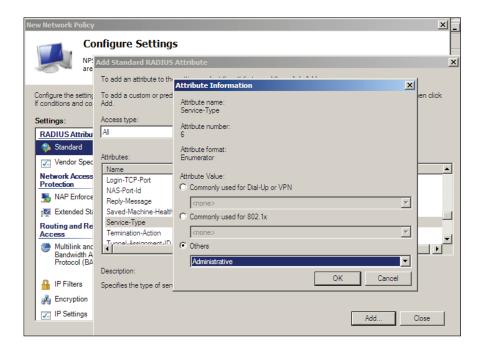
| New Network P | olicy | × | | |
|---|--|---|--|--|
| | Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings. | | | |
| EAP types are n | egotiated between NPS and the client in the order in which they are listed. Move Up Move Down | | | |
| Microsoft E | Edit Remove authentication methods: Image for the second seco | | | |
| Microsoft E User ca E Encrypted a Allow client | In change password after it has expired n change password after it has expired authentication (CHAP) authentication (CHAP) s to connect without negotiating an authentication method. chine health check only | | | |
| | Previous Next Finish Cancel | | | |

- ▶ 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.

| New Network Pol | icy | | |
|--|---|--------|---|
| | Configure | Sett | tings |
| | NPS applies setti are matched. | ngs to | o the connection request if all of the network policy conditions and constraints for the policy |
| | tings for this netwo constraints match | | blicy. connection request and the policy grants access, settings are applied. |
| Settings: | | | |
| RADIUS Attri | butes | | To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and |
| \Rightarrow Standard | | | then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes. |
| Vendor Sp | pecific | | |
| Network Acce Protection | 3 5 | | |
| NAP Enfo | rcement | | Attributes: |
| Extended | State | | Name Value Framed-Protocol PPP |
| Routing and Access | Remote | | Service-Type Frankd |
| Multilink a Bandwidth Protocol (| h Allocation | | |
| IP Filters | | | |
| 💑 Encryptio | n | | Add Edit Remove |
| IP Setting | s | - | |
| | | | |
| | | | Previous Next Einish Cancel |

- 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.

| 🞭 Network Policy Server | | |
|--|--|---|
| File Action View Help | | |
| 🗢 🔿 🔰 🖬 🚺 🖬 | | |
| NPS (Local) RADIUS Clients and Servers Policies Connection Request Polici | Network policies allow you to designate who is au under which they can or cannot connect. | uthorized to connect to the network and the circumstances |
| Network Policies | Policy Name | Status Processing Order Access Type S 🔺 |
| 📔 Health Policies | 802.1X (Wired) For Accountants | Enabled 3 Grant Access U |
| 🕀 퉔 Network Access Protection | 802.1X (Wired) for Marketers | Enabled 4 Grant Access U |
| National Accounting | 802.1x (Wired) For Engineers | Enabled 5 Grant Access U |
| | Command Line Access | Enabled 6 Grant Access U 🗸 |
| | | |
| | Remote Acces | ss server |
| | | |
| | Conditions - If the following conditions are met: | Ê |
| | Condition Value | |
| | MS-BAS Vendor ID ^311s | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Settings - Then the following settings are applied: | |
| | Setting Value | |
| | Access Permission Deny Acc | - |
| | Extensible Authentication Protocol Method Microsoft: | |
| | | |
| | | |
| | | |
| 2 | | , |

About Allied Telesis

For nearly 30 years, Allied Telesis has been delivering reliable, intelligent connectivity for everything from enterprise organizations to complex, critical infrastructure projects around the globe.

In a world moving toward Smart Cities and the Internet of Things, networks must evolve rapidly to meet new challenges. Allied Telesis smart technologies, such as Allied Telesis Management Framework[™] (AMF) and Enterprise SDN, ensure that network evolution can keep pace, and deliver efficient and secure solutions for people, organizations, and "things"—both now and into the future.

Allied Telesis is recognized for innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at alliedtelesis.com

Allied Telesis

NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895 Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830 EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

© 2015 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners. C618-31019-00 RevC