

Tested Solution: LAN Client Authentication



Introduction

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

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

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

This solution will explain how to:

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

Contents

- Introduction see page 3
- Network scenario see page 3
- **Switch Configurations** see page 4
- Setting up the Windows 2008 Server see page 10

Configuring IP interface(s) see page 10

- Installing Active Directory see page ||
- Adding users and groups to Active Directory see page 15
- Installing Network Policy Server see page 19
- Registering NPS with Active Directory see page 20
- Obtaining a server certificate for the server that is running NPS see page 21
- Setting up a Connection Request Policy see page 24
- Setting up Network Policies see page 26
- Setting up Client PCs to perform 802.1x authentication see page 36

Joining the PCs to the domain see page 36

Configuring the PC as an 802.1x supplicant see page 38

Performing 802.1x authentication see page 39

■ 802.1x Authentications with Certificates see page 41

Configuring Policies on the Network Policy Server to use certificates see page 41

- Setting up the client PC to perform Certificate Authentication see page 43
 - **Obtain user certificates** see page 43
 - Download the Certificate Authority server's Root certificate see page 45
 - Set up the NIC card to perform authentication by certificate see page 49
- Verifying the authentication from the Switch command-line see page 52

Multiple supplicants on the same x600 port, assigned to different VLANs see page 52

- **Setting up MAC-based authentication** see page 54
- Configuring the Network Policy server to Proxy MAC-based RADIUS requests to the VCStack RADIUS server see page 55

Creating MAC address entries in the Active Directory User database see page 60

■ Appendix I – Setting up a DHCP server see page 61

Setting up the x900 VCStack as a DHCP server see page 61

Setting up the Windows 2008 server as the DHCP server see page 63

Appendix 2 – Setting up the Windows 2008 Network Policy Server to authenticate Management access to the switches see page 67

Network scenario

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

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

Solution description

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

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

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

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

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

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

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

Switch Configurations

x600

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

The switch uses three different RADIUS servers.

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

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

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

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

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

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

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

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

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

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

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

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

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

aaa authentication login default group NPS local

crypto pki trustpoint local

crypto pki enroll local radius-server local server enable Set up the Local RADIUS server. 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 group otheroffices accept internally-generated requests. vlan 40 It is configured with username/password set up for visitors from group externalvisitors other offices, who will be dynamically allocated VLAN 40; and for vlan 50 external visitors, who will be dynamically allocated to VLAN50 user InternalVisitor password ikiG4JcsKEwFlhL group otheroffices user ExternalVisitor password ikiG4JcsKEwFlhL group externalvisitors vlan database vlan 2 name uplink vlan 10 name Accounting The switch is configured with one static VLAN (VLAN 2) that is vlan 20 name Engineering used for communication with the rest of the network. The other vlan 30 name Marketing 5 VLANs are used for dynamic allocation to users vlan 40 name OtherOffices vlan 50 name ExternalGuests vlan 60 name GuestsVI AN interface port I.O.I-I.O.22 auth-mac enable The first 22 ports on the switch are available for users to connect auth-Web enable to. They are all configured with triple authentication with dynamic dot1x port-control auto VLAN assignment and VLAN60 as the guest VLAN. The ports auth host-mode multi-supplicant are configured to support multiple supplicants on a single port, in auth guest-vlan 60 case a hub or EAP-forwarding L2 switch is attached to one of the auth dynamic-vlan-creation type multi ports, to enable multiple users to share that port spanning-tree portfast spanning-tree portfast bpdu-guard enable interface port1.0.23-1.0.24 Ports 23 and 24 are configured as a link aggregration group to switchport access vlan 2 connect the switch to the virtual chassis stack in the core static-channel-group | ip dhcp pool Temporary Set up a DHCP server on the switch that is used specifically for network 192.168.160.0 255.255.255.0 the Web-Auth users to have an IP address for a brief time whilst range 192.168.160.20 192.168.160.40 they authenticate via HTTP. The leasetime is set to 30 seconds, default-router 192.168.160.10 so the DHCP lease will be re-newed very guickly after the lease 0 0 0 30 subnet-mask 255.255.255.0 authentication has been completed service dhcp-server interface vlan2 ip address 192.168.2.10/24 interface vlan I 0 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 address 192.168.160.10/24

The default route is via the x900 VCStack	ip route 0.0.0.0/0 192.168.2.252
All log messages are sent to a syslog server. Higher-severity log messages are also buffered on the switch itself	log buffered level errors log host 192.168.2.254 log host 192.168.2.254 level debugging
Allow read-only SNMP monitoring from one management station	access-list 1 permit 192.168.2.253 snmp-server enable trap auth nsm snmp-server community public ro 1 snmp-server host 192.168.2.253 version 2c public
Configure NTP (Network Time Protocol) with the IP address of the NTP server	ntp server 192.168.2.252
8000S	
Enable 802.1× globally	dot I × system-auth-control
The switch cannot configure separate RADIUS servers for 802.1x authentication and MAC-based authentication. So, it will forward all authentication requests to the Network Policy Server running on the Windows 2008 server at 192.168.2.254. The Network Policy Server will process 802.1x requests itself. For the MAC-based authentication requests, it acts as a RADIUS proxy, and forwards the requests to the RADIUS server running within the core VCStack	radius-server host 192.168.2.254 key MS-IAS aaa authentication dot1x default radius
Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server. If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request	aaa authentication login default radius local
The switch is configured with one static VLAN (VLAN 2) that is used for communication with the rest of the network. The other 4 VLANs are used for dynamic allocation to users	vlan database vlan 2,10,20,30,50
vlan50 is designated as the guest VLAN for the switch	interface vlan 50 dot l x guest-vlan exit
The 24 10/100 ports are configured for MAC-based and 802.1x authentication.They accept dynamic VLAN allocation, and will put unathenticated users into the guest VLAN	interface range ethernet 1/e(1-24) dot1× re-authentication dot1× mac-authentication mac-and-802.1× dot1× guest-vlan enable dot1× radius-attributes vlan dot1× port-control auto spanning-tree portfast spanning-tree guard root exit

	interface range ethernet 1/g1,2/g1
	switchport trunk allowed vlan add 2
Two gigabit ports one from each stack member are	switchport trunk allowed vlan add 10
aggregated together to create a resilient link to the network	switchport trunk allowed vlan add 20
aggregated together to create a resilient link to the network	switchport trunk allowed vlan add 30
core. These ports are tagged in all the vLAINS on the switch	switchport trunk allowed vlan add 50
	chappel-group. I mode on
	ovit
	exit
	Interface vian 2
	ip address 192.168.2.11 255.255.255.0
	exit
	ip dhcp snooping
	ip dhcp snooping vlan 10
	ip dhcp snooping vlan 20
DHCP snooping guards against rogue server and server	ip dhcp snooping vlan 30
exhaustion attacks	ip dhcp snooping vlan 50
	interface port-channel I
	ip dhep shooping trust
	exit
Allow read-only SNMP monitoring from one management	snmp-server community public ro 192,168,2,253 view Default
station. Send traps to that same management station	spmp-server host 192.168.2.253 public traps 2
,	
	sntp client enable vlan 2
	clock source sntp
System time is provided from an SNTP server	sptp unicast client enable
	shtp server 192 168 2 252
	Ship Server 172.100.2.232
All log messages are sent to a syslog server. Higher-severity log	logging 192,168,10,11
messages are also buffered on the switch itself	logging buffered errors
x900 Stack	
	log buffered level errors
All log messages are sent to a syslog server. Higher-severity	log bast 192 168 2 254
log messages are also buffered on the switch itself	log host 192.168.10.11 level debugging
	log host 172.100.10.11 level debugging
	access list permit 192 168 10 13
Allow read-only SNMP monitoring from one management	comp convor anable trap such nem
station	shimp-server enable trap autilitism
Station	snmp-server community public rol
	snmp-server host 192.168.10.13 version 2c public
A resiliency link backs up the dedicated stacking link. If the	
stacking link fails, communication is maintained to allow graceful	stack resiliencylink eth0
reconfiguration	J
Use priority to pre-elect the VCStack master switch) stack priority

Management sessions on the switch will be authenticated by RADIUS, using the windows 2008 Network Policy server: If the server is unavailable, then the switch will fall back to using the local user database to authenticate the request	radius-server host 192.168.2.254 key MS-IAS aaa authentication login default group Radius local
The switch is configured with 8 VLANs	vlan database vlan 2 name core vlan 10 name Accounting vlan 20 name Engineering vlan 30 name Marketing vlan 40 name OtherOffices vlan 50 name ExternalGuests
Create ACLs that will control where the various categories of users will be able to access	
All DHCP will be allowed through	access-list 3001 permit udp any range 67 68 any range 67 68
External visitors' traffic (apart from DHCP) cannot go to any internal addresses	access-list 3002 deny ip 192.168.150.0/24 192.168.0.0/16 access-list 3003 deny ip 192.168.150.0/24 172.16.0.0/12 access-list 3004 deny ip 192.168.150.0/24 10.0.0.0/8
Visitors from other offices' traffic (apart from DHCP) cannot go to local internal addresses, but can go out onto the corporate WAN	access-list 3005 deny ip 192.168.140.0/24 192.168.0.0/16
The final ACL allows through all the traffic that has not been explicitly blocked by the previous ACLs	access-list 3006 allow ip any any
Create link aggregation groups across the VCStack members for resiliency	
The ports that connect to the x600 are untagged in VLAN 2	interface port1.0.1 switchport access vlan 2 static-channel-group 1 ip access-group 3001 ip access-group 3002 ip access-group 3004 ip access-group 3005 ip access-group 3006 interface port2.0.1 switchport access vlan 2 static-channel-group 1 ip access-group 3001 ip access-group 3002 ip access-group 3003 ip access-group 3004 ip access-group 3005 ip access-group 3005

ip access-group 3001 ip access-group 3002 ip access-group 3003 ip access-group 3004 ip access-group 3005 ip access-group 3006 interface port2.0.2 switchport mode trunk switchport trunk allowed vlan add 2,10,20,30,50 The ports that connect to the 8000S switches are tagged in all static-channel-group 2 VLANs except the InternalVisitors VLAN 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 port I.0.3 switchport mode trunk switchport trunk allowed vlan add 2,10,20,30,50 static-channel-group 3 ip access-group 3001 ip access-group 3002 ip access-group 3003 ip access-group 3004 ip access-group 3005 ip access-group 3006 interface port2.0.3 switchport mode trunk switchport trunk allowed vlan add 2,10,20,30,50 static-channel-group 3 ip access-group 3001 ip access-group 3002 ip access-group 3003 ip access-group 3004 ip access-group 3005 ip access-group 3006

interface port1.0.2 switchport mode trunk

static-channel-group 2

switchport trunk allowed vlan add 2,10,20,30,50

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

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

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

ip address 192.168.2.252/24 interface vlan I 0 ip address 192.168.10.10/24 ip dhcp-relay server-address 192.168.2.254 interface vlan20 ip address 192.168.20.10/24 IP addresses are configured on all the VLANs. All the client VLANs ip dhcp-relay server-address 192.168.2.254 are configured to relay DHCP requests to the DCHP server in interface vlan30 the network core ip address 192.168.30.10/24 ip dhcp-relay server-address 192.168.2.254 interface vlan40 ip address 192.168.40.10/24 ip dhcp-relay server-address 192.168.2.254 interface vlan50 ip address 192.168.50.10/24 ip dhcp-relay server-address 192.168.2.254 ip route 192.168.110.0/24 192.168.2.10 ip route 192.168.120.0/24 192.168.2.10 Create routes to the subnets in the Public/Private Zone ip route 192.168.130.0/24 192.168.2.10 ip route 192.168.140.0/24 192.168.2.10 ip route 192.168.150.0/24 192.168.2.10

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

interface vlan2

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

Setting up the Windows 2008 Server

This solution uses two roles of the windows 2008 server:

- Active Directory Domain Controller
- Network Policy Server

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

Configuring IP interface(s)

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

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

Installing Active Directory

To install Active Directory:

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

Server Manager		
File Action View Help		
🗢 🔿 🖄 📅 🛛 🖬		
Server Manager (2K8TEST02)	Roles	
(F) File Services (F) Features (F) Features (F) Features (F) Features	View the health of the roles installed on your server and add or remove roles and features.	
E Storage	Roles Summary	🔀 Roles Summary Help
	Roles: 1 of 16 installed File Services	iiiin Add Roles iiii Remove Roles
	File Services	File Services Help
	Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching	rching, and enable access for UNIX client computers
	Role Status	Go to File Services
	Messages: None	

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 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 Federation Services Active Directory Fights Wanagement Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Constalled Network Policy and Access Services Print Services UDDI Services	Electription: Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
	Web Server (IIS) Windows Deployment Services More about server roles	ext > Install Cancel

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		×
Installation Res	ults	
Before You Begin Server Roles Active Directory Domain Services	The following roles, role services, or features were installed successfully:	_
Confirmation		
Results	 Active Directory Domain Services Installation succeeded 	
	Active Directory Domain Controller Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller. Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).	
	Print, e-mail, or save the installation report	
	< Previous Next > Close Cancel	

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).

Oomain 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. Image: Use advanced mode installation Learn more about the additional options that are available in <u>advanced mode installation</u> . More about Active Directory Domain Services	and add or r
	isers and dom
< <u>Back</u> <u>N</u> ext > Canc	cel
	Cel
< <u>Back</u> <u>Next</u> > Cance • Role Service: Active Directory Domain Controller Active Directory Domain Controller Active Directory Domain Controller 	cel
< <u>Back</u> <u>Next</u> > Cance 	cel Status Installed Not installed Not installed
< Back Next > Cance 	cel Status Installed Not installed Not installed Not installed
< Back Next > Cancel 	Cel Status Installed Not installed Not installed Not installed Not installed

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**.

ctive Directory Domain Services Inst	allation Wizard	
hoose a Deployment Configuration You can create a domain controller for an	n existing forest or for a new forest.	
C Existing forest		
C Add a domain controller to an e	xisting domain	
C Create a new domain in an exist This server will become the first	ting forest domain controller in the new domai	in
Г Create a new domain tree ro	oot instead of a new child domain	
• Create a new domain in a new forest	>	
More about possible deployment configur	rations	
	< Back Next >	Cancel
	< Back Next >	Cance

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.	Ţ
Type the fully qualified domain name (FQDN) of the new forest root domain.	
FQDN of the forest root domain:	
newforest.com	
Example: corp.contoso.com	
	- 1
< Back Next >	Cancel

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.

Additional Domain Controller Options		
Select additional options for this domain cont	roller.	
DNS server		
🔽 Global catalog		
Read-only domain controller (RODC)		
Additional information:		
cannot be an RODC. We recommend that you install the DNS Se controller.	erver service on the first domain	¥
More about <u>additional domain controller opti</u>	<u>ions</u>	

Click Next.

The remaining windows in the wizard are straight-forward.

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

Adding users and groups to Active Directory

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

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

To add users and groups to Active Directory:

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



Type in a Group Name.

Group name:	
Lengineering	
Group name (pre-Windows 2)	000):
Engineering	
Group scope	Group type
C Domain local	Security
Global	C Distribution
C Universal	
O Universal	

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**.

Active Directory Users and Con	nputers	
File Action View Help		
🗢 🔿 🖄 🛅 🔏 🗎 🗱	7 🖆 🈹 🚺 🖬 🖬 😼 🛍	7 🤇
Active Directory Users and Comput	Name Type	De
Aved Queries	Accountants Security Group	
	Administrator User	But
Domain Controllers	Cert Publishers Security Group	Mel
	Denied ROD Security Group	Me
Find	DnsUpdatePr Security Group	DN
New 🕨	Computer Com	Des
All Tasks 🕨	Contact rity Group	All
View 🕨	InetOrgPerson urity Group	All
Refresh	MSMQ Queue Alias rity Group	
Export List	User urity Group	Des
	Shared Folder rity Group	Me
нер	Guest User	Bui

Type in the user details.

•				
First name:	Engineer01	1	Initials:	
Last name:				
Full name:	Engineer01	1		_
User logon name:	i.			
Engineer01		@NewFores	t.Com	•
User logon name	(pre-Windows 20	000):		
NEWFOREST		Engineer01		

Click **Next**.

Type in the user **Password**.

Password:	•••••	
Confirm password:	•••••	
User must change	password at next logon	
User cannot chan	ge password	
Password never e	xpires	
Account is disable	d	

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...**

Active Directory Users and Com	puters			
File Action View Help				
 	i 🖸 🔒 🔽 🖬	1 🕹 j	▲. Orm r== ►. Copy	1
Active Directory Users and Comput	Name	Туре	Add to a group	
🗄 🚞 Saved Queries	& Accountant01	User	Disable Account	
Ima NewForest.Com	Accountants	Securit	Reset Password	1 1
🖲 🛄 Builtin	👗 Administrator	User	Move	ht for admini
Computers	& Allowed ROD	Securit	Open Home Page	is group can
E Domain Controllers	& Cert Publishers	Securit	Send Mail	his group are }
	& Denied ROD	Securit	All Tacks	is group can
Users	Section 2018	Securit.	All I dana 🗸	ators Group
	& DnsUpdatePr	Securit	Cut	ho are permi
	Somain Admins	Securit	Delete	dministrators
	Somain Com	Securit	Rename	hs and serve 1
	Bomain Cont	Securit	Properties	htrollers in th 🕻
	Somain Guests	Securit	Proper des	ests
	Somain Users	Securit	Help	ers 1
	Engineer01	User		
	Sector Engineering	Security	/ Group	
	Enterprise A	Security	Group Designated	administrators]
	Enterprise R	Security	/ Group Members of	this group are
	Group Policy	Security	Group Members in	this group can
	💑 Guest	User	Built-in acco	unt for guest
- Sunday and A state of the sunday and the	Marketer 01	User	م المحمد المحاصيين الم	الخاصيب مح

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

elect Groups				? ×
Select this object Groups or Built - From this locatio	t type: n security principals n:			Object Types
NewForest.Com	es l			Locations
Name:	Starts with 💌			Columns
Description:	Starts with 💌			Find Now
Disabled	accounts ring password			Stop
Days since la	ast logon:	I		9 7
Search results:	Description	In Folder	0	K. Cancel
	Description			

- 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.

Select Groups				<u>? ×</u>
Select this object ty Groups or Built-in s	pe: ecurity principals			<u>O</u> bject Types
NewForest.Com				Locations
, Common Queries	1			
Name:	tarts with tarts			<u>C</u> olumns Find <u>N</u> ow Stop
Search res <u>u</u> lts:			0	K Cancel
Name (RDN)	Description	In Folder		▲
Domain Comp Domain Contr Domain Guests	All workstations All domain contr All domain guests All domain users	NewForest.Com NewForest.Com NewForest.Com NewForest.Com		
Engineering Enterprise Ad Enterprise Re	Designated admi Members of this	NewForest.Com NewForest.Com NewForest.Com	l	

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

Installing Network Policy Server

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

To install the Network Policy Server:

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

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



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



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

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

Add Roles Wizard Installation Resu	llts
Before You Begin Server Roles Network Policy and Access Services	The following roles, role services, or features were installed successfully:
Role Services Confirmation Progress Results	Network Policy and Access Services Installation succeeded The following role services were installed: Network Policy Server Routing and Remote Access Services Remote Access Service I You can use a wizard in the NPS console to configure Network Access Protection (NAP). To open the NPS console after installation, go to Server Manager or click Start, Administrative Tools, Network Policy Server.
	Print, e-mail, or save the installation report <previous< td=""> 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.



Obtaining a server certificate for the server that is running NPS

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

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

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

To obtain a server certificate:

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



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

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

Certificate Enrollment		
Certificate Enrollment		
Request Certificates		
Vou con request the following types of certifica	the Colort the certificates you want to recu	aat, and then did. Earoll
rou can request the following types of certifica	ates. Select the certificates you want to requ	est, and then click Enroll.
Directory Email Replication	🔅 STATUS: Available	Details 🛞
Domain Controller	💓 STATUS: Available	Details 🛞
Domain Controller Authentication	💓 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 Hel	b		1
🗢 🔿 🖄 🖬 🛛			
NPS (Local)	Servers	RADI	JS clients allow you to
RADIUS Clients	New RADIUS Clier	nt	3
	Export List		IP Address D
Connection Red	View	•	192.168.0.3 A
Health Policies	Refresh		192.168.0.56 F
Network Access Pro Accounting	Help		2

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:	
80005	
Address (IP or DNS):	
192.168.2.11	Verify
Vendor	
Specify RADIUS Standard for most RADIUS clients, or select the RAD vendor from the list.	IUS client
Vendor name:	
RADIUS Standard	•
Shared Secret	
To manually type a shared secret, click Manual. To automatically gener secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive.	rate a shared same shared
Manual O Generate	
Shared secret:	
•••••	
Confirm shared secret:	
•••••	
Additional Options Access-Request messages must contain the Message-Authenticato	or attribute
RADIUS client is NAP-capable	
ОК	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.

server		_ 🗆 🗵
File Action View Help		
< 🔿 🗾 🖬 🛛 🖬		
Image: Second	Connection request policies allow you to designate whether connection requests an locally or forwarded to renote RADIUS servers. For NAP VPN or 802.1X, you must PEAP authentication in connection request policy. Policy Name MAC-Auth RADIUS Enabled 2 Unspecified MAC-Auth RADIUS Enabled 2 Unspecified NAP 802.1X (Wired) Disabled 4 Unspecified Use Windows authentication for all users Usabled 939393 Unspecified Conditions - If the following conditions are met: Conditions - If the following conditions are met: Conditions Conditions Value Day and time restrictions Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Settings - Then the following settings are applied: Setting Value	re processed configure d d d d d 00 Wednesday
	Authentication Provider Local Computer	-
	Extensible Authentication Protocol Conliguration Configured	
New	,	

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

w Connectio	n Request Policy	×
-	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		200
Locally Proces	sed	
type or Vendor Type of ne Unspecifie Vendor spe 10	specific. twork access server: ed cfin:	
	Draw starter March Citatistic Connect	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.

A minimum of one conditio	Day and time restrictions	
Conditions: Condition Select a condition, and th Select a condition The Turnel Type The Turnel Type Day and Time Pay and Time Pay and Time Condition Day and Time Day and Time Condition Day and Conditi	12.2.4.6.8.10.12.2.4.6.8.10.12 All Sunday Monday Tuesday Wednesday Thursday Friday Saturday	OK Cancel

- 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:

v Connectio	on Request Policy
	Specify Authentication Methods
Z	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
These authe	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
FAD been	vinniner gybernies de ingele nien de niende entre de niende de reste fan de fan de fan de fan de fan de fan de
EAP types a	re negotiared between NHS and the client in the order in which they are listed.
ЕАР Туре	s:
	Move Up
	Move Down
Add	Edit Remove
Less secu	re authentication methods:
Microso	It Encrypted Authentication version 2 (MS-CHAP-v2)
Microso	can change password after it has expired If Encryoted Authentication (MS-CHAP)
🗖 User	can change password after it has expired
Encrypte	ed authentication (CHAP)
Unencity	ypted authentication (PAP, SPAP)
-	ants to connect without negotiating an authentication method

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

C	w Connection Request Policy				
	leting Connection Request Policy Wizard				
You have successfully or Locally Processe	eated the following connection request policy:				
Condition	VALue	1			
Policy settings:	Value				
Policy settings: Condition Authentication Provider	Value Local Computer				

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.

w Network I	Policy			
	Specify Network Policy I You can specify a name for your networ	Name and Connect rkpolicy and the type of co	ction Type	licy is applied.
olicy name				
802.1x (Wired	d) For Engineers			
Vetwork conn	nection method			
elect the type	e of network access server that sends the co	onnection request to NPS. Yo	ou can select either the net	work access server
pe or Vendo	ir specific.			
Type of ne	etwork access server:			
Unspecifi	ied			
Vendor sp	ecífic:			
10	ㅋ			
1				
		Previous	Next Finis	n Cancel

Click Next.

In the Specify Conditions window:

Click Add...

ew Network Po	olicy						2
	Specify C Specify the cor of one condition	onditions nditions that det on is required.	ermine whether th	iis network polio	cy is evaluated for a	connection re	quest. A minimun
Conditions:							
Condition		Value					
J							
Condition descri	iption:						
					Add	E dit	Remove
				Previous	Next	Finish	Cancel

Select User Groups, and click Add...

New Network F	Policy	×
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A of one condition is required.	minimum
Select conditio	on	×
Select a condit	ion, and then click Add.	
Groups		
Wind The W Mach The M The M	ows croups /indows Groups condition specifies that the connecting user or computer must belong to one of the selected ine Groups lachine Groups condition specifies that the connecting computer must belong to one of the selected groups. Groups Ser Groups condition specifies that the connecting user must belong to one of the selected groups.	
HCAP		
Locat	tion Groups ICAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups et to match this policy. The HCAP protocol is used for communication between NPS and some third party	
required in the formation of the formati	rk access servers (NASs). See your NAS documentation before using this condition.	

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

In this window, click Add Groups...

New Network Poli	сү			×
s:	Specify Conditions t pecify the conditions t f one condition is requ	ions hat determine whether this net ired.	vork policy is evaluated for a	o connection request. A minimum
elect condition				2
Select a condition,	and the User Groups			×
Groups Window: The Wind	s Group lows Groups	group membership required to m	tch this policy.	f the selected
Machine The Mach	e Groupe hine Gro			ected groups.
User Gro The User	oups Groups			ups.
Location The HCA required t	P Locati to match		1	ocation groups
network a	access s	Add Groups	Remove	
HCAP U			OK Cancel	Agd 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	<u>? ×</u>
Select 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:	A
Search results:	DK Cancel
Name (RDN) Description In Folder	

Click Find Now.

Select Engineers from the Search results:

Select Group				? ×
Select this object ty	ype:			
Group				Object Types
From this location:				
NewForest.Com				Locations
Common Queries	1			
Name:	Starts with 💌			Columns
				Fied New
Description:	itarts with 💌			Find Now
Disabled ac	counts			Stop
Non expiring	a password			
Days since last	logon: 📃 🔽			×1
\frown			0	K Cancel
Search results:				
Name (RDN)	Description	In Folder		<u> </u>
Denied ROD	Members in this	NewForest.Com		
Admins DnsAdmins	DNS Administrat	NewForest.Com		
DnsUpdatePr	DNS clients who	NewForest.Com		
Domain Admins	Designated admi	NewForest.Com		
Domain Comp	All workstations	NewForest.Com		
Bomain Contr	All domain contr	NewForest.Com		
Real Domain Guests	All domain guests	NewForest.Com		
🕂 Domain Users	All domain users	NewForest.Com		
		NewForest.Com		
Enterprise Ad	Designated admi	NewForest.Com	-	
De Entomrino Po	Momborn of this	New Forget Com		•

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.

ew Network Po	licy
	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A minim of one condition is required.
Conditions:	
Condition	Value
Condition descrip	ation: s condition specifies that the connecting user must belong to one of the selected groups. Add Edit
	Previous Next Einish Cancel

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

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



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

New Network I	Policy				×
	Configure Authentication M	ethods			
2	Configure one or more authentication metho authentication, you must configure an EAP ty Protected EAP in connection request policy, v	ds required for the co /pe. If you deploy NAI vhich overrides netwo	nnection reques P with 802.1X or rk policy authen	st to match this p r VPN, you must c tication settings.	olicy. For EAP configure
EAP types are	negotiated between NPS and the client in the orde	er in which they are liste	d.		
EAF Types.		Move L	qL		
		Add EAP	5991		×
		Authentication m	ethods:		
Add	Edit Roman	Microsoft: Sma Microsoft: Prote	rt Card or other o ected EAP (PEA)	ertificate P)	
700	nellow	Microsoft: Secu	ured password (E	EAP-MSCHAP v2)	
Microsoft F	Encrypted Authentication version 2 (MS-CHAP-v2)				
User ca	an change password after it has expired				IN
User ca	an change password after it has expired	1.1	Г		
Encrypted	authentication (CHAP)		5	OK	Cancel
Allow clien	ed authentication (PAP, SPAP) Its to connect without negotiating an authentication	n method.			
Perform ma	achine health check only				
		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.



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 Add.	fic, and then click
Access type:	
Al	
Attributes:	
Name	
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
Tunnel-Server-Endpt	
Tunnel-Type	
•	
Description	
Specifies the tunneling protocols used.	
	1 ~ 1
Add	

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:	
Commonly used for Dial-Up or VPN	
<none></none>	v
Commonly used for 802.1x	
Virtual LANs (VLAN)	•
C 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**.

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

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

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>	-
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-Pvt-Group-ID**:

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 Spe Add.	ecific, and then click
Access type:	
Al	
Attributes:	
Name	A
Tunnel-Client-Endpt	
Tunnel-Medium-Type	
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
Tunnel-Server-Endot	>
Description:	
Specifies the Group ID for a tunneled session.	
	1
Add	Close

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

Attribute Information	x
Attribute name: Tunnel-Pvt-Group-ID	
Attribute number: 81	
Attribute format: OctetString	
Enter the attribute value in: String	
O Hexadecimal	
20	
	OK Cancel

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

New Network P	olicy		
	Configure Set NPS applies settings t are matched.	tings o the connection request if	all of the network policy conditions and constraints for the
Configure the s If conditions ar <u>Settings</u> :	ettings for this network po nd constraints match the c	olicy. connection request and the p	olicy grants access, settings are applied.
RADIUS At Standar Vendor Network Ac Protection	tributes d Specific cxcess forcement	To send additional attribute then click Edit. If you do no your RADIUS client docum Attributes:	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.
	Lou .	Name	Value
Extende	ed State	Tunnel-Type	Virtual LANs (VLAN)
Routing an Access	d Remote	Tunnel-Medium-Type	802 (includes all 802 media plus Ethemet canonical for
Multilin Bandwie Protoco	k and dth Allocation d (BAP) rs	Tunnel-Pvt-Group-ID	20
- Encrypt	tion		Ramon
		A <u>a</u> a <u>E</u> arc	<u>H</u> emove
P Setti	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 802.1 x supplicants on the LAN.

Setting up Client PCs to perform 802.1x authentication

There are two steps to setting up the Client PCs:

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

Joining the PCs to the domain

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

To register a PC on the domain:

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



Click Next to open the Connecting to the Network window.

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



Click Next.

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

Network Identification Wizard	
Connecting to the Network What kind of network do you use?	(d)
Select the option that best describes your co	mpany network:
My company uses a network with a doma	in
O My company uses a network without a do	omain
]	< 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 Identificati	ion Wizard
User Account an A user account	d Domain Information : gives you access to files and resources on a network.
Type your Win information, as	dows user account and domain information. If you do not have this ik your network administrator.
<u>U</u> ser name:	Engineer01
Password:	•••••
Domain:	NEWFOREST
	< <u>Back</u> <u>Next</u> 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.

🚣 Test LAN Properties	? ×
General Authentication Advanced	
Select this option to provide authenticated network as this Ethernet adapter Enable IEEE 802.1X authentication Choose a network authentication method:	ccess for
Protected EAP (PEAP) Setting	JS
Cache user information for subsequent connection to this network	15
ОК	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 802.1 x authentication. If the check box is not ticked, the PC will open a window asking for a username/password every time it needs to perform 802.1 x authentications. This is a particular problem at the time when the PC is logging into the network. It cannot log into the network until the network connection has been authenticated, but if it needs user input to authenticate the connection, it cannot proceed at login time, as the request for user input cannot be popped up at login time.

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

Performing 802.1x authentication

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

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

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

```
Triple-Auth#show dot1x supplicant int port1.0.13
Interface port1.0.13
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    WebBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0
  Supplicant name: Engineer01
  Supplicant address: 0002.b363.319f
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 9
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 8
    CD: adminControlledDirections: both - operControlledDirections: both
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 20
```

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

Triple-Auth#show vlan 20

VLAN ID	Name	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 vlan**

console# show dot1x ethernet 1/e1

802.1 x is enabled

Port	Admin Mode		Oper Mode	Reauth Control	Reauth Period	Username
1/e1	Auto		Authorized	Disabled	3600	NEWFOREST\Engineer01
Quiet per Tx period Max req: Supplican Server ti Session T MAC Addre Authentic	riod: d: nt timeout: meout: Time (HH:MM:SS): ess: eation Method:	60 30 2 30 30 00: Ren	Seconds Seconds Seconds :00:27 :02:b3:63:31:91 mote	E		
Authentic State: Backend S State: Authentic Authentic	on Cause: ator State Machi State Machine ation success: ation fails:	Not ne AU IDI 11 7	L TERMINATED	et		

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.



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

view Conditions Constraints Set	tings
figure the constraints for this network I constraints are not matched by the c Instraints:	policy. connection request, network access is denied.
onstraints	Allow access only to those clients that authenticate with the specified methods.
	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Microsoft: Protected EAP (PEAP) Move Up
NAS Port Type	Add Edt Remove
	Less secure autonentication methods: ✓ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) ✓ User can change password aftert it has expired
	Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Enconcented authentication (CHAP)
	Logspecial memoral (197) Loncoyted automication (PA, SPAP) Allow clients to connect without negotiating an authentication method
	Perform machine health check only

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**.

A certificate that is co Policy will override this	infigured for Protected EAP in Connection Request s certificate.	
Certificate issued	NPS1.NewForest.Com	-
Friendly name:		
Issuer:	NewForest2003	
Expiration date:	4/8/2010 9:07:50 PM	
Enable Fast Recon Disconnect Clients ap Types Smart Card or other c Secured password (E/	nect without Cryptobinding ertificate AP-MSCHAP v2)	

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

Setting up the client PC to perform Certificate Authentication

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

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

Obtain user certificates

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

To obtain a user certificate from the Certificate Authority:

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



This will open the Certificate Request Wizard:



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

tifi	cate Request Wizard	
Ce	rtificate Types	
	A certificate type contains preset properties for certificates.	
	Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.	
	Certificate types:	
	Bacic EES	
C	User	
C	User	
C	User	
C		
C	To select a cryptographic service provider and a CA, select Advanced.	
C	To select a cryptographic service provider and a CA, select Advanced.	
C	To select a cryptographic service provider and a CA, select Advanced.	
C	To select a cryptographic service provider and a CA, select Advanced.	

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

You can provide a name and o certificate.	description that help you qu	uickly identify a specific	
Type a friendly name and des	cription for the new certific	ate	
Friendly name:			
Engineer Cert			
Description:			
Certiuficate for authentication	n		

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).

🖈 🏟 🄇	Connecti	ng	🗿 • 🔊 - 🖶 • 🖻 •
1	Inter	Connect to 192.168	2.253 ? X page
	Most I	Connecting to 192.16	8.2.253.
	•	User name: Password:	NewForest\Engineer01
	What		Remember my password
	● Di Mo		OK Cancel

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.

Aicrosoft Certificate Services - Windows Internet Explorer		
	🔽 🐓 🗙 Live Search	<mark>- م</mark>
😪 🏟 🏉 Microsoft Certificate Services	🐴 🔹 🗟 🔹 🖶 Page 🔹 🎯 Tools	; • »
Microsoft Cartificate Casicas Nov/Ecrost2002	 Uom	
WICTOSON CERTIFICATE Services NewForest2005	nom	2
Welcome		_
Use this Web site to request a certificate for your We certificate, you can verify your identity to people you messages, and, depending upon the type of certifica	Web browser, e-mail client, or other program. By using a ou communicate with over the Web, sign and encrypt icate you request, perform other security tasks.	
You can also use this Web site to download a certific certificate revocation list (CRL), or to view the status	ificate authority (CA) certificate, certificate chain, or tus of a pending request.	
For more information about Certificate Services, see	see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request	t	
Download a CA certificate, certificate chain, or C		
		-
		-
http://192.168.2.253/certsrv/certrqus.asp	💽 🚺 💽 Internet	• //.

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	_ 🗆 🗙
🚱 🕤 🔻 🔊 http://192.168.2.253/certsrv/certcarc.asp	₽ -
😭 🎶 🎉 Microsoft Certificate Services 👔 🔹 🔂 🗸 🎰 Page	• 🕥 Tools • »
Microsoft Certificate Services NewForest2003	<u>Home</u>
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	
O Base 64	
Download CA certificate	
Download latest base CRI	
Download latest delta CRL	
	~
Done Internet	💐 100% 🔻 //

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

Microsoft Certificate Services - Windows Internet Explorer	×
	🔹 🍫 🗙 Live Search 🖉 🔹
🙀 🎄 🌈 Microsoft Certificate Services	🏠 🔹 🔂 🔹 🧓 🖌 🙀 Page 🔹 🎯 Tools 🔹 🎽
Microsoft Certificate Services NewForest2003 Download a CA Certificate, Certificate Chain, or C To trust certificates issued from this certification autho	RL
To download a CA certificate, certificate chain, or CRI	, select the certificate and encoding method.
CA certificate:	wnload - Security Warning X ou want to open or save this file? Name: certnew.cer Type: Security Certificate, 1.16KB Form: 192,159,252
Encoding method: © DER © Base 64 Development of the table of	Open Save Cancel
Download CA certificate chain Download latest base CRL Download latest delta CRL	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the tick?</u>
Done	👻

Click **Yes** on the next question.

Potentia	l Scripting Violation
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 this 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			? ×
General Authentication Adv	anced		
General Authentication Adv. Select this option to provide this Ethernet adapter. Image: Choose a network authentice Image: Choose a network authentice Protected EAP (PEAP) Image: Cache user information Into this network	anced	ed network id: Settii ent connecti	access for ngs
		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
NewForest-NP51-CA
OISTE WISEKey Global Root GA CA
Post. Trust Root CA
Primary Utility Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Smart Card or other Certificate
Enable Fast Reconnect
Enable Quarantine checks
Disconnect if server does not present cryptobinding TLV
OK Cancel

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				
NewForest2003				
View Certificate				
Use a different user name for the connection				
UK 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		? ×
User name on certificate:		
Engineer01@NewForest.	Com	-
Accountant01@NewFore	ist.Com	
Administrator@NewForest	Lom t.Com	
Tssuer:	NewForest2003	
Expiration date:	9/04/2010 9:06:37 a.m.	
	OK Cancel View Cer	tificate

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

Verifying the authentication from the switch command-line

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

```
Interface port1.0.13
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    WebBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0
  Supplicant name: Engineer01@NewForest.Com
  Supplicant address: 0002.b363.319f
    authenticationMethod: 802.1X
    portStatus: Authorized - currentId: 22
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 21
    CD: adminControlledDirections: both - operControlledDirections: both
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    dynamicVlanId: 20
```

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

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

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

If the x600 port is also configured with the command

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

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

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

```
show 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
...
```

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

...

dynamicVlanId: 20

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

show vlan 10

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

show vlan 20

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

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

show platform table vlan

[Instance 1.0] VLAN table

••••

...

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

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

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

Setting up MAC-based authentication

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

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

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

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

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

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

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

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

8000S : username = 00024e2a80b4 password = 00024e2a80b4

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

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

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

The solution to difference (ii) above is a little more involved. Given that the 8000S must use the Windows 2008 server for its 802. Ix 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:

Enable the local RADIUS server	radius-server local server enable
Configure the x600 as a client	nas 192.168.2.10 key MAC-AUTH
The Windows 2008 will proxy requests to this server, so needs to be configured as a client of this server	nas 192.168.2.254 key MAC-AUTH
Create groups that define the VLAN-IDs that will be alloc devices that belong to different departments	ated to vlan 10 group engineeringPeripherals vlan 20 group marketingPeripherals vlan 30

Create 2 entries for each device that needs to be authenticated

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

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

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

To create a new Connection Request policy:

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

lew Connectio	n Request Policy	×
	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	a	
MAC-Auth RA	DIUS	
Select the type type or Vendo Type of ne Unspecifi O Vendor sp 10	e of network access server that sends the connection request to NPS. You can select either the network access server specific. ed	
	Previous Next Finish Cancel	

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...

lew Connectio	n Request Policy	x
	Specify Conditions	
	Specify the conditions that determine whether this connection request policy is evaluated for a connection re A minimum of one condition is required.	equest.
elect conditio	n	×
Select a condit	ion, and then click Add.	
HCAP		
User	CAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups ed to match this policy. The HCAP protocol is used for communication between NPS and some third party rk access servers (NASs). See your NAS documentation before using this condition.	
User The us typica	Name ser name that is used by the access client in the RADIUS message. This attribute is a character string that Illy contains a realm name and a user account name.	
Connection		
The A from t	ss Client IPv4 Address ccess Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access he RADIUS client.	
The A	ss Client IPv6 Address ccess Client IPv6 Address condition specifies the IPv6 address of the Access Client that is requesting access	-
	Add Can	cel

■ 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 pattem matching syntax.	
[0-9afAf]{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	on Request Policy	A REAL PROPERTY AND A REAL	×
	Specify Col The connection re remote RADIUS s	nnection Request Forwarding quest can be authenticated by the local server or it can be forwarded to RADIUS servers in a erver group.	
If the policy co	onditions match the c	onnection request, these settings are applied.	
Forwardin Request → Authen	g Connection tication nting	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: Inot configured> New C Accept users without validating credentials	
		Previous <u>N</u> ext Einish 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.

IAC-Auth Server			
ADIUS Servers:			
RADIUS Server	Priority	Weight	A <u>d</u> d
			Edit
			Hemove

■ 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	
Type the name or IP address of the RADIUS server you want to add.	
Server:	
192.168.2.252	Verify
OK Cancel	Apply

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

Add RADIUS Server	X
Address Authentication/Accounting Load Balar	icing
Authentication port:	1812
Shared secret:	[
Confirm shared secret:	
🔲 Request must contain the message authentica	ator attribute
Accounting	
Use the same shared secret for authenticat	on and accounting.
Shared secret:	
Confirm shared secret:	
Forward network access server start and st	op notifications to this server
0	K 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 Conn The connection requiremote RADIUS serv	ection Request Forwarding est can be authenticated by the local server or it can be forwarded to RADIUS servers in a er group.	
If the policy co	nditions match the conn	ection request, these settings are applied.	
Forwarding Request) Connection ication ting	Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication. Authenticate requests antification Forward requests to the following remote RADIUS server group for authentication: MAC-Auth Server New Accept users without validating credentials	
		Previous Next Einish Cancel	1

- 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 802.1× 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 RADIUS Clients Remote RADIUS Server G Policies Connection Request Policie Network Policies Health Policies Health Policies Accounting	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 Cource MAC-Adh RADIUS Enable 2 U specified 3 Status Sta	
	MAC-Auth RADIUS	
	Conditions - If the following conditions are met: Condition Value User Name [0-9s fA-F](12)	•
	Settings - Then the following settings are applied:	
	Setting Value Authentication Provider Forwarding Request Authentication Provider Name MAC-Auth Server	•
•	▶ 	

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 I – 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 I I 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 I I subnet-mask 255.255.255.0

ip dhcp pool Engineeering-private network 192.168.20.0 255.255.05 range 192.168.20.20 192.168.20.210 dns-server 192.168.2.254 default-router 192.168.20.10 lease 30 | 1 subnet-mask 255.255.255.0

ip dhcp pool Engineeering-publicPrivate network 192.168.120.0 255.255.0 range 192.168.120.20 192.168.120.210 dns-server 192.168.2.254 default-router 192.168.120.10 lease 30 | | 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 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 | | 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 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 | | 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.

du Roles Wizaru		
Select Server R	oles	
Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings DHCP Scopes DHCP 6 Scopes DHCPv6 Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services (Installed) Active Directory Domain Services (Installed) Active Directory Federation Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory (Installed) DNS Server (Installed) Fax Server File Services Verbrok Policy and Access Services (Installed) Print Services UDDI Services UDDI Services Web Server (IIS) (Installed) Windows Deployment Services More about server roles	Description: <u>Dynamic Host Configuration Protocol</u> (<u>OHEP) Server</u> enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

- 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	k Connection Bindings	
Before You Begin Server Roles DHCP Server Network Connection Bindings	One or more network connectio be used to service DHCP clients Select the network connections Network Connections:	ns having a static IP address were detected. Each network connection can on a separate subnet. that this DHCP server will use for servicing clients.
IPV4 DNS Settings	IP Address	Туре
DHCPv6 Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Results		
	Details	
	Name:	Local Area Connection 2
	Network Adapter: Physical Address:	Intel(R) PRO/100 VE Network Connection 00-08-6A-F0-35-F4
		< Previous Next > Install Cancel

Click Next.

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

Add Roles Wizard	×
Specify IPv4 DI	NS Server Settings
Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings DHCP Scopes DHCPv6 Stateless Mode IPv6 DNS Settings DHCP Server Authorization Confirmation Progress Begits	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
	Alternate DNS Server IPv4 Address: Validate More about DNS server settings Yerevious 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.

Add or Edit I	OHCP Scopes		
Before You Begin	A scope is the range of pos addresses to clients until a	sible IP addresses for a network. The DHCP server cannot scope is created.	distribute IP
Server Koles	Add Scope	X	
Network Connection Binding A scope is a range of possible IP addresses for a network. The DHCP server cannot		<u>A</u> dd	
IPv4 DNS Settings IPv4 WINS Settings	distribute IP addresses to clients	until a scope is created.	Delete
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	Subnet Mask:	255.255.255.0	
Progress	Default Gateway (optional):	192, 168, 2, 10	
Results	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	<u>A</u> dd
Network Connection Bindings	Accounting Private	192.168.10.20 - 192.168.10.210	Edit
IPv4 DNS Settings	Marketing Private	192, 168, 20, 20 - 192, 168, 20, 210	
IPv4 WINS Settings	Accounting Public/Private	192, 168, 110, 20 - 192, 168, 110, 210	Delete
DHCP Scopes	Engineers Public/Private	192, 168, 120, 20 - 192, 168, 120, 210	
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, 210 192, 168, 150, 20 - 192, 168, 150, 210	
DHCP Server Authorization	External visitors	192.100.100.20 - 192.100.150.210	
Confirmation			
Progress			
Parulte			
	Properties		
	Add or select a scope to view its	properties	
	Add of select a scope to view its	proper des.	

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

Add Roles Wizard	×
Authorize DHCF	9 Server
Before You Begin Server Roles DHCP Server Network Connection Bindings IPv4 DNS Settings IPv4 WINS Settings DHCP Scopes DHCP Scopes DHCPv6 Stateless Mode	Active Directory Domain Services (AD DS) stores a list of DHCP servers that are authorized to service dients 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. C Use current credentials The credentials of the current user will be used to authorize this DHCP server in AD DS. User Name: wEWFOREST\administrator
DHCP Server Authorization Confirmation Progress Results	Use alternate credentials Specify domain administrator credentials for authorizing this DHCP server in AD DS. User Name: Specify Specify Specify Specify Specify This DHCP server must be authorized in AD DS before it can service clents. More about authorizing DHCP servers in AD DS
	< 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 Policy	×
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	
Policy name:	2010
Command Line Access	
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access set type or Vendor specific Imspecified Vendor specific: 10	rver
Previous Next Finish Car	ncel

- 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.

w Network P	olicy	×	-15
	Specify Conditions Authentication Method Specify the conditions that determ of one condition is required. Specify the authentication methods required to match this policy.	X	es
Conditions : Condition	Select condition Select a condition, and then clicky Image: Select a condition, and then clicky <th>Cancel</th> <th>acce</th>	Cancel	acce
Condition desc	packets, such as PPP or Service Type Service Type The Service Type condition restricts the policy to only clients specifying a certain type of ser Point to Point Protocol connections. Turned Turn Add Edit	vice, such as Tr	

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

New Network F	Policy	2
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For E4 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.	P
EAP types are r	negotiated between NPS and the client in the order in which they are listed. Move Up Move Down	
Add Less secure	Edit Remove	
Microsoft E Microsoft E User ca User ca Encrypted	an change password after it has expired Encrypted Authentication (MS-CHAP) an change password after it has expired Interpretation (CHAP)	
Allow cirem	is to connect without negotiating an authentication method.	
	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 Policy	×
Configure S NPS applies setting are matched.	ettings as to the connection request if all of the network policy conditions and constraints for the policy
Configure the settings for this networ If conditions and constraints match th Settings:	c policy. te connection request and the policy grants access, settings are applied.
RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Access	To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and 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. Attributes: Name Value Framed-Protocol PPP Service-Type Framed
Multilink and Bandwidth Allocation Protocol (BAP)	Add Edit Remove
IP Settings	
	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.

w Network Policy			×.
Co	nfigure Settings	s	
NP:	Add Standard RADIUS	Attribute	×
are	To add an attribute to the	Attribute Information	1
Configure the setting If conditions and co	To add a custom or pred Add.	Attribute name: Senzice-Tune	ien click
Settings:	Access type:	And the second	
RADIUS Attribu	All	6	
standard	Attributes:	Attribute format: Enumerator	
Vendor Spec	Name		_
Protection	Login-TCP-Port	Attribute Value:	
NAP Enforce	NAS-Port-Id Reply-Message		
Extended Sta	Saved-Machine-Health	C Commonly used for 902 1y	
Routing and Re Access	Service-Type Termination-Action		
Multilink and	Tunnel.Accimment.ID	 Others 	
Protocol (BA		Administrative	
IP Filters	Specifies the type of sen	OK Cancel	
Recryption	_		
IP Settings		Add	Close

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.

server				_		
File Action View Help						
🗢 🔿 🖄 🖬 🚺 🖬						
NPS (Local) RADIUS Clients and Servers Policies Connection Request Polici	Network policies allow you to designate under which they can or cannot conne	e who is authorized to connect .ct.	to the network and th	he circumstance	is	
i Network Policies	Policy Name	Status	Processing Order	Access Type	S 🔺	
📔 Health Policies	802.1X (Wired) For Accountants	Enabled	3	Grant Access	U	
🕀 🌆 Network Access Protection	802.1X (Wired) for Marketers	Enabled	4	Grant Access	U.,	
Recounting	802.1x (Wired) For Engineers	Enabled	5	Grant Access	U —	
	Command Line Access	Enabled	6	Grant Access	U 👻	
					►	
	Connections to Microsoft Routing and Ren	note Access server				
			_	_	•	
	Conditions - If the following conditions are met:					
	Condition Value					
	MIS-RAS Vendor ID 311\$					
	Settings - Then the following settings are appl	lied:				
	Setting	Value				
	Access Permission	Deny Access				
	Extensible Authentication Protocol Method	Microsoft: Smart Card or other	certificate		-	
	I					
	,					
J				J		

About Allied Telesis Inc.

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

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

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

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

Visit us online at www.alliedtelesis.com

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

www.alliedtelesis.com

© 2010 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 Rev. B



