



3Com[®] SuperStack[®] 3 Switch Family
3Com[®] Switch 5500 Family

Technical Notes:

Microsoft IAS, Funk Steel-Belted Radius Server,
FreeRADIUS and Cisco Secure ACS Setup

June 2005

William Roose

Product Engineer, 3Com Corporation

Contents

1	INTRODUCTION	4
1.1	APPLICABLE PRODUCTS	4
2	MICROSOFT IAS RADIUS SETUP.....	5
2.1	INSTALL WINDOWS 2000 SERVER (VANILLA INSTALL).....	5
2.2	INSTALLING THE CERTIFICATE SERVER.....	7
2.3	INSTALLING IAS.....	8
2.4	CONFIGURE A CERTIFICATE AUTHORITY.....	9
2.5	SETUP THE INTERNET AUTHENTICATION SERVICE (RADIUS).....	11
2.6	GENERATE A CERTIFICATE	13
2.7	CONFIGURE FOR SWITCH LOGIN.....	21
2.7.1	Switch login via PPP connection.....	21
2.7.2	Switch login via Telnet / SSH.....	23
2.8	CONFIGURE THE CLIENT	26
2.9	CONFIGURE AUTO VLAN AND QoS MEMBERSHIP.....	26
2.9.1	Summary of auto VLAN and QoS attributes	30
3	FUNK RADIUS SETUP.....	33
3.1	DOWNLOADING AND INSTALLING FUNK.....	33
3.2	CONFIGURING AUTO VLAN AND QoS	37
3.2.1	Summary of auto VLAN and QoS attributes	37
4	CONFIGURING FREERADIUS.....	38
4.1	ADDING A CLIENT.....	38
4.2	UPDATING THE DICTIONARY FOR SWITCH LOGIN.....	38
4.3	ADDING USERS.....	39
4.3.1	For Switch Login	39
4.3.2	For Network Login	39
4.4	AUTO VLAN AND QoS SETUP.....	39
4.4.1	Ensure you have the attributes defined in the dictionary files.....	39
4.4.2	Add the return list attributes to the user in the users file.....	40
5	CISCO SECURE ACS SETUP (TACACS+)	40
5.1	ADDING A 3COM SWITCH AS A CLIENT OF CISCO SECURE ACS.....	41
5.2	ADDING A USER FOR NETWORK LOGIN.....	43
5.3	ADDING A USER FOR SWITCH LOGIN	44
6	RADIUS CLIENTS	47
6.1	WINDOWS XP BUILT-IN CLIENT.....	47
6.2	AEGIS CLIENT INSTALLATION	47
6.2.1	Registering the Aegis Client	47
6.2.2	Configuring the Aegis Client	48
7	CONFIGURE THE SUPERSTACK 3 SWITCH	50
7.1	NETWORK LOGIN	50
7.2	SWITCH LOGIN	51
7.3	RADIUS AUTHENTICATED DEVICE ACCESS (RADA).....	52
7.3.1	General setup tips.....	52
7.3.2	Ensuring only company devices are connected to the corporate network.....	53
7.3.3	Guest VLAN.....	54
7.3.4	Easing the roll out of 802.1x network security	55

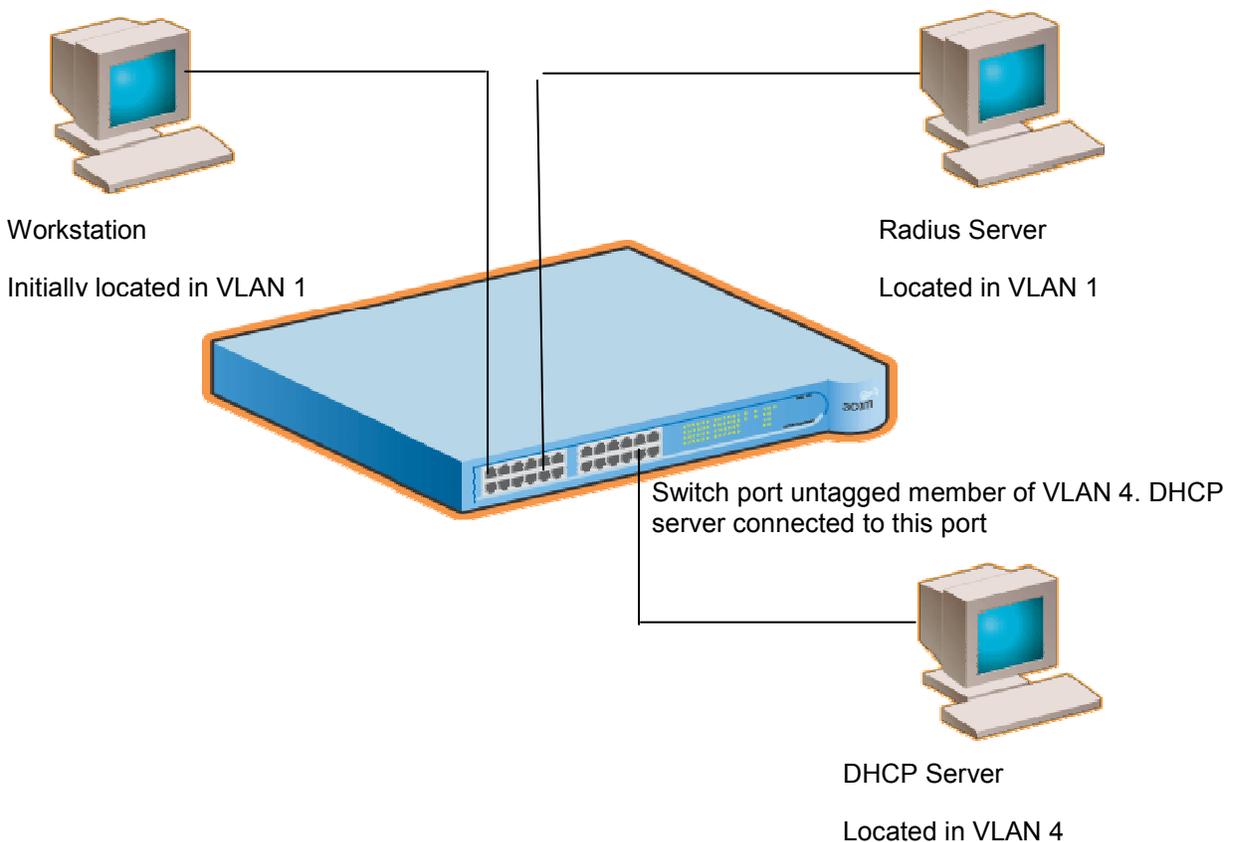
7.3.5	<i>Ensure devices have the latest virus definitions (Intermediate VLAN)</i>	55
7.4	CHECK LIST ATTRIBUTES SUPPORTED ON 4400	58
7.5	RETURN LIST ATTRIBUTES SUPPORTED ON 4400	58
7.6	PROBLEM DIAGNOSIS	59
8	CONFIGURING THE 5500 FAMILY SWITCH	59
8.1	GENERAL RADIUS SETUP.....	59
8.1.1	<i>Domain and RADIUS scheme creation</i>	60
8.2	NETWORK LOGIN	61
8.3	SWITCH LOGIN	63
8.4	RADIUS AUTHENTICATED DEVICE ACCESS (RADA).....	63
8.5	RETURN LIST ATTRIBUTES SUPPORTED ON 5500	64
8.6	PROBLEM DIAGNOSIS	65

1 Introduction

This document covers the installation of Windows 2K server on a PC and configuration to work with RADIUS based-authentication with a 3Com SuperStack 3 switch and a client PC running Windows XP.

It also covers the configuration of Auto VLAN and QoS parameters for SuperStack 3 Switch 4400 Version 4.0 software.

Below shows an example setup of a simple RADIUS network.



1.1 Applicable Products

This document applies to:

SuperStack 3 Switch 4400: Supports Network Login (validating users access to the network) and Switch Login (validating users access to the switch). The 4400 also supports dynamic VLAN and QoS port assignment based on user.

SuperStack 3 Switch 3870: Supports Network Login (validating users access to the network) and Switch Login (validating users access to the switch).

SuperStack 3 Switch 3200: Supports Network Login (validating users access to the network) and Switch Login (validating users access to the switch).

SuperStack 3 Switch 4900: Supports Switch Login only

3Com Switch 40x0: Supports Switch Login only

2 Microsoft IAS RADIUS Setup

2.1 Install Windows 2000 Server (Vanilla Install)

Patch from the Microsoft website (windowsupdate.microsoft.com)

Once complete, run “dcpromo” to turn it into a Domain Name server. Note: you need to do this first, before enabling it as a certificate server.

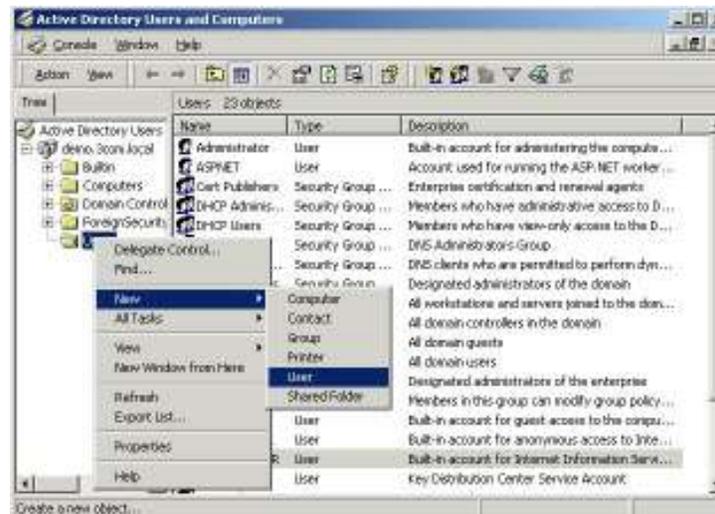
When I set it up I created the domain demo.3com.local and also enabled it as a DNS server for the network.

Note: EAP-TLS is not available in mixed mode, which supports Windows NT and 2000 clients. The server needs to be changed to run in Native mode. This is done under “Active Directory Users and Computers. Right Click on Domain and choose properties. Click on “Change Mode”



Next, you need to add a user that is allowed to use the network. This is done using the “Active Directory Users and Computers” window.

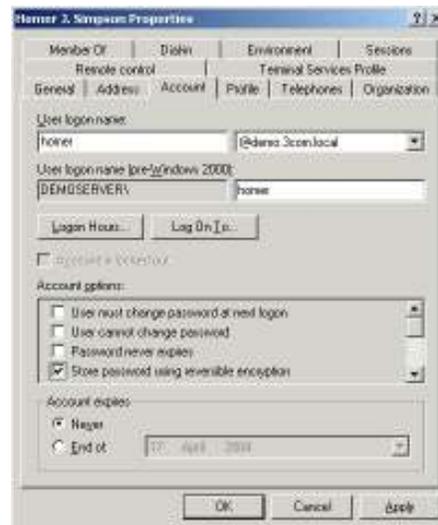
Add a new user by right-clicking on the “users” folder in the left hand window and then choose New->User, as shown below



Create a user by following the wizard and adding the appropriate information at each stage:



Once created, the password should be set to be stored in reversible encryption. To do this, right click on the user and click on Properties. Under the account tab, check the box that says "Store password using reversible encryption".

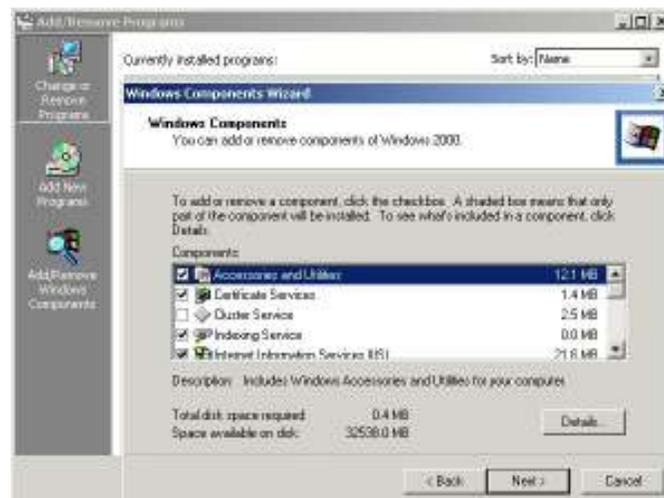


Note: Once you do this, you have to re-enter the password for the account. This is done by right-clicking on the user account and choosing “Reset Password...”

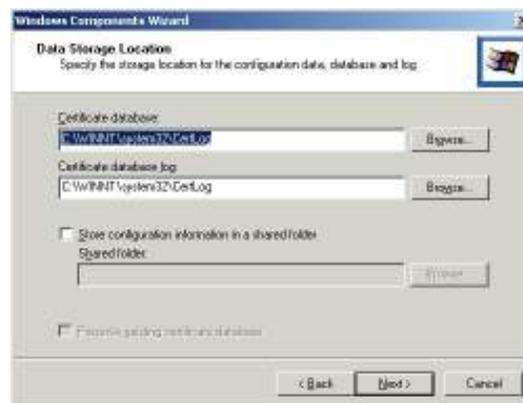
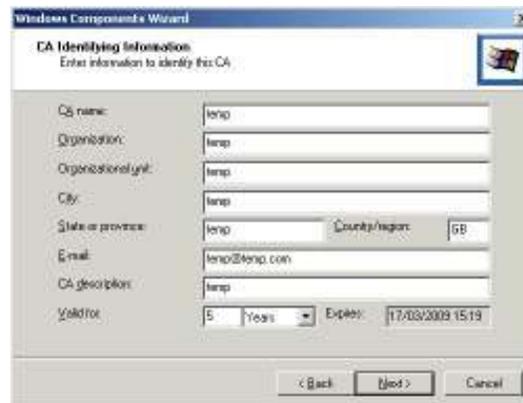
2.2 Installing the certificate server

If you want to use EAP-TLS certificate based authentication, you need to enable the Certificate services in windows. You need to do this after you have turned the machine into a domain server as it won't let you do it after certification has been enabled.

This is done under Control Panel->Add/Remove Programs-> Add/Remove Windows Components. The “Certificate Services” component should be checked.



In the wizard that comes up, the Certificate authority type should be Enterprise root CA, and the CA Identifying information can be up to yourself. Below I have just used the term “temp”.



Then allow the wizard to install and set up the certificates server. The install CD will be required for this.

2.3 Installing IAS

Also in "Add/Remove Windows Components", enable "Networking Services". Under the detail of "Networking Services", "Internet Authentication Service" should be checked.



And click OK at the end

2.4 Configure a Certificate Authority

Click on the Start Button -> Programs -> Administrative Tools -> Certification Authority

Right-click **Policy Settings** under your Certificate Authority server, select **New -> Certificate to Issue**



Select Authenticated Session and Select OK.



Click on the Start Button -> Programs -> Administrative Tools -> Active Directory Users and Computers

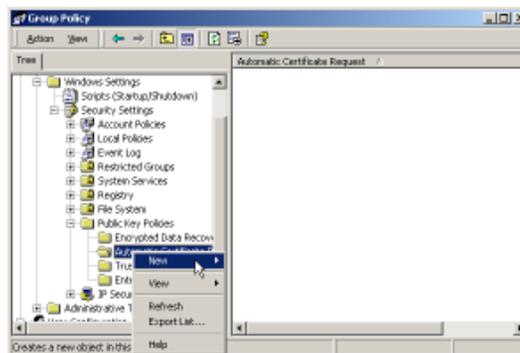
Right-click on your active directory domain, and select **Properties**



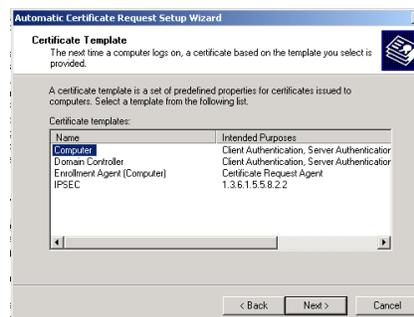
Select the **Group Policy** tab, ensure that the **Default Domain Policy** is highlighted, and click **Edit**. The Group Policy editor is launched.



Under Computer Configuration -> Windows Settings -> Security Settings -> Public Key Policies, right-click **Automatic Certificate Request Settings**, Select **New**, then **Automatic Certificate Request**.



When the Certificate Request Wizard comes up, select Next. Select the Computer certificate template, and click Next.



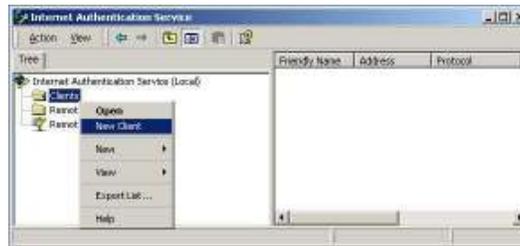
Ensure that your Certificate Authority is checked, then click **Next**. Review the policy change information and click **Finish**.

Open up a command prompt (Start -> Run, type **cmd** and press enter), and type **secedit /refreshpolicy machine_policy**. It may take a few minutes for it to take effect.

2.5 Setup the Internet Authentication Service (Radius)

Click on the Start Button -> Programs -> Administrative Tools -> Internet Authentication Service

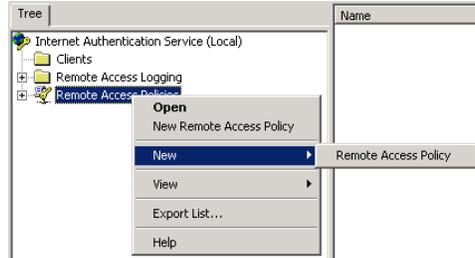
Right-click on **Clients**, and Select **New Client**.



Enter a name for your device that supports IEEE 802.1x, and click **Next**.

Enter the IP address of your device that supports IEEE 802.1x, and set a shared secret. Select **Finish**. Leave all other settings default.

Right-Click on **Remote Access Policies**, and Select **New Remote Access Policy**.



Give the policy a name, for example EAP-TLS, and select **Next**.

Click **Add...** In this screen you are setting conditions of using the policy to access the network.

Select

Day-And-Time-Restrictions, and click **Add...**



Click **Permitted**, then **OK**. Select **Next**.

Select **Grant remote access permission**, and click **Next**

Click on **Edit Profile...** and select the **Authentication** tab. Make sure **Extensible Authentication Protocol** is selected, and **Smart Card or other Certificate** is set. Deselect other authentication methods listed. Click **OK**.



Click the **Configure** button, next to the EAP type selector.

Select the appropriate certificate and click **OK**. There should be at least one certificate. This is the certificate that has been created during the installation of the Certification Authority Service.



It is possible that Windows asks you if you wish to view the Help topic for EAP. Select **No** if you want to continue with the installation. Click **Finish**.

Important: For EAP-TLS to work correctly, there should only be one policy configured in IAS.

Enable Remote Access Login for Users. Click on the Start Button -> Programs -> Administrative Tools, and select **Active Directory Users and Computers**.

Double click on the user for which you want to enable authentication to bring up its account properties.

Select the **Dial-in** tab, and select **Allow access**. Click **OK**.



Click OK to confirm.

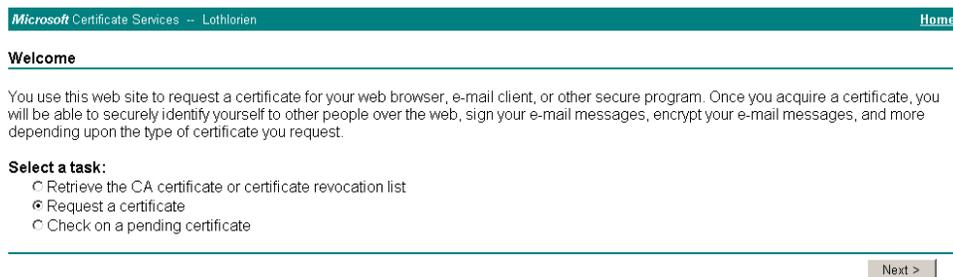
Next step is to configure the Switch for RADIUS access and client authentication.

2.6 Generate a certificate

We have to request a certificate from the Certification Authority. This certificate will be used to authorize the client against the RADIUS Server. There are two ways to request a certificate, the advanced request or standard request. We will perform an advanced request. The standard request differs in the way the certificate is stored on the local computer. Later on in the setup, the certificate needs to be mapped to the username in the Active Directory Services. This needs to be done for both the advanced and standard request.

On the server, open Internet Explorer and enter **http://localhost/certsrv** in the URI

When you are prompted for a login, enter the user account name and password that you will be using for the certificate.



Select **Request a certificate** and click **Next >**

There are two options to choose for requesting a certificate. In this scenario, we choose to create an Advanced Request

Select **Advanced request** and click **Next >**

Microsoft Certificate Services -- Lothlorien [Home](#)

Choose Request Type

Please select the type of request you would like to make:

User certificate request

Advanced request

Select the first option and click **Next >**

Microsoft Certificate Services -- Lothlorien [Home](#)

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Use the settings from the screenshot below. You can choose different key options. Click **Save** to save the PKCS #10 file. We are going to use this file to generate a certificate

Microsoft Certificate Services -- Lothlorien [Home](#)

Advanced Certificate Request

Certificate Template:
Authenticated Session

Key Options:
CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange Signature Both

Key Size: 512 (Min: 384, Max: 1024, common key sizes: 512, 1024)

Create new key set

- Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
- Use local machine store
You must be an administrator to generate a key in the local machine store.

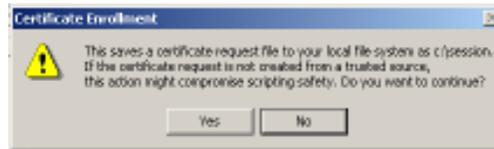
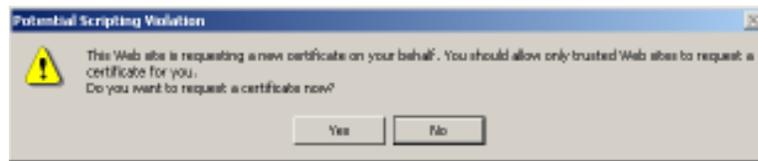
Additional Options:
Hash Algorithm: SHA-1
Only used to sign request.

Save request to a PKCS #10 file
File name: C:\session

This request will be saved and not submitted.

Attributes:

You will receive two warning messages. Dismiss both by clicking **OK**



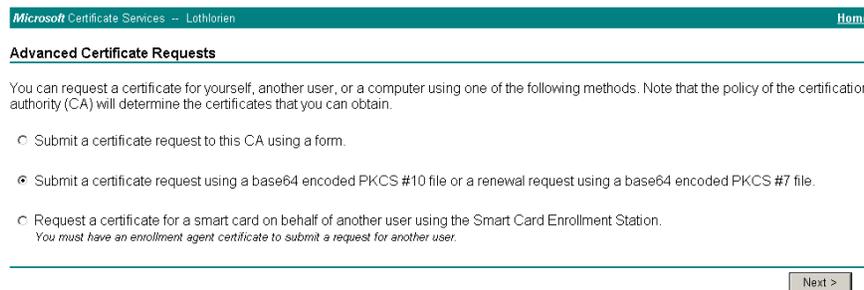
The PKCS #10 file is now saved to the local drive. We are now going to use this file to generate a portable certificate. Click the **Home** hyperlink at the right top of the CA Webpage.

Microsoft Certificate Services -- Lothlorien

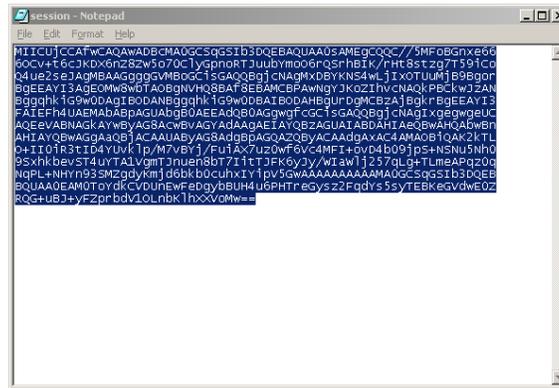
[Home](#)

Select **Request a certificate** → **Next** → **Advanced request** → **Next**

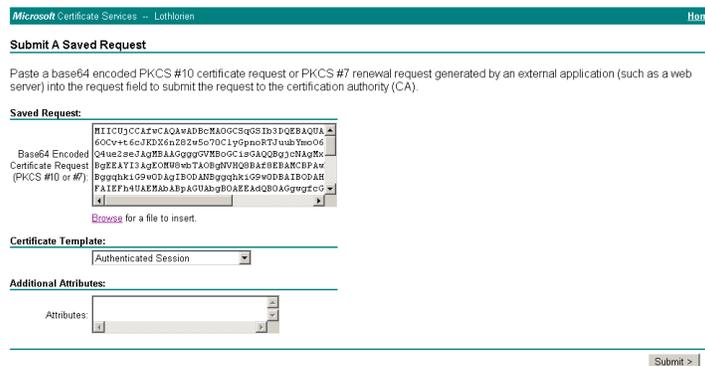
Now, select the second option as shown in the screenshot below, and click **Next >**



Open the previously saved PKCS #10 certificate file in Notepad, select all (Control + a) and copy (Control + c), as shown below



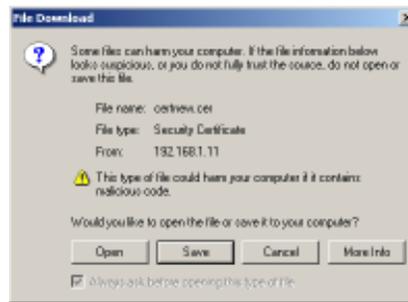
Paste the copied information into the **Saved Request** field as shown below. Select "Authenticated Session" from the **Certificate Template** selector and click **Submit >**



You can now download the certificate and certificate path. In addition, the certificate is installed on the Certification Authority. You can verify this in the CA Administration tool under **Issued Certificates**



Click on the **Download CA Certificate** hyperlink to save the certificate. Save the file as DER encoded.



Also, click on the **Download CA certification path** hyperlink to save the PKCS #7. This file is not really required for IEEE 802.1x functionality.



You can now install both files on the workstation that requires IEEE 802.1x Network Login

From the workstation, first double-click the certificate file (extension is .cer)



Click **Install Certificate**. This will launch the certificate import wizard



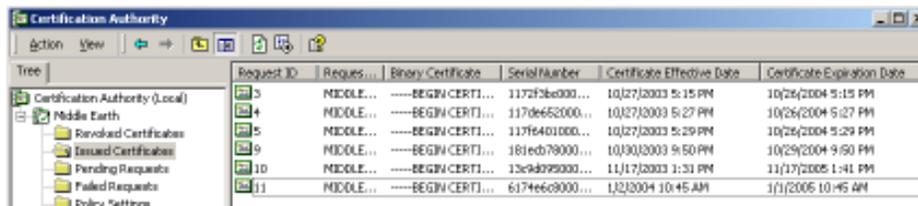
Leave the settings on the next screen as is, and click **Next >**



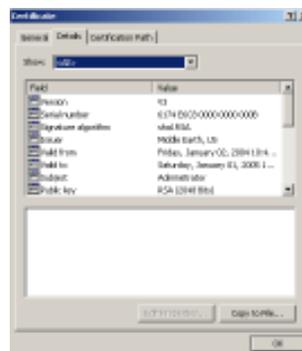
Click **Finish** to install the certificate, and dismiss the confirmation screen.



Now, launch the Certification Authority management tool on the server and expand the “Issued Certificates” folder. You should see the newly created certificate.



Double-click on the certificate that was generated by the client and click on the **Details** tab



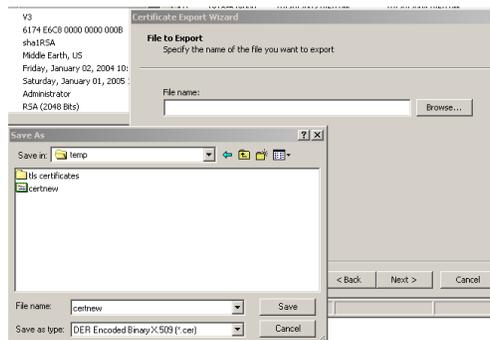
Click on **Copy to File** to save the certificate. This action is actually already performed with the advanced request, but this is an alternative way to save the certificate. We will be using this certificate to attach to the user in the Active Directory Services. Click **Next** when the wizard is launched.



Save the certificate in a path, using DER x.509 encoding.



Provide a name to the certificate and save it to a specified location.



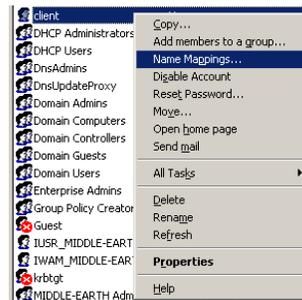
Click **Finish** and dismiss the confirmation box.



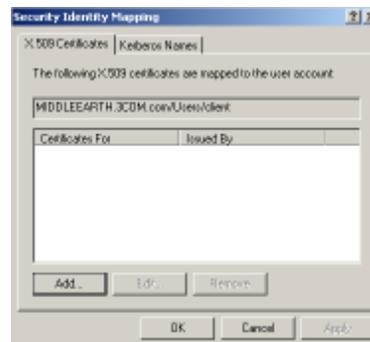
Exit the Certification Authority management tool and Launch Active Directory Users and Computers management tool. Make sure that in the **Action** menu you have enabled **Advanced Features** as shown below.



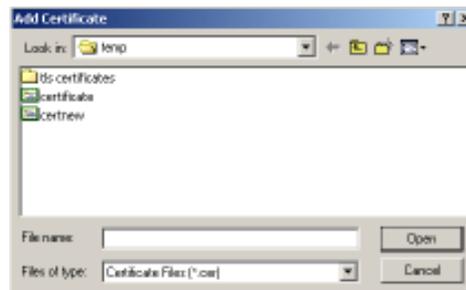
Select the user that becomes the IEEE 802.1x client, right click on that user and select **Name mappings**.



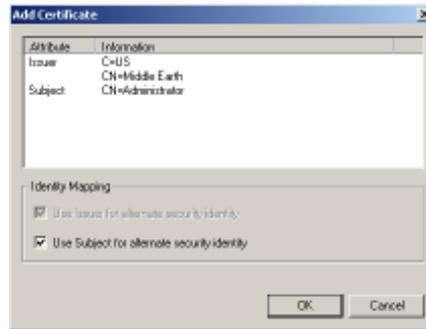
Click **Add**.



Select the certificate that you have just exported and click **Open**.



Click **OK**



In the Security Identity Mapping screen, click **OK** again to close it.

Close the Active Directory Users and Domains management tool. This concludes the configuration of the server side.

There is an easier way to request and install certificates and that is to choose a User Certificate instead of an Advanced Certificate request. This method allows you to install the certificate on your computer directly after it is generated. The standard request does not require you to go through the complex configuration. The intention of this document however is to show you what the possibilities are for generating certificates.

2.7 Configure for Switch Login

The following describes setting up of the Microsoft IAS server to allow switch login.

2.7.1 Switch login via PPP connection

Firstly, create a Windows Group to contain users that are allowed access to the switch. Also add a user and make it a member of this windows group:

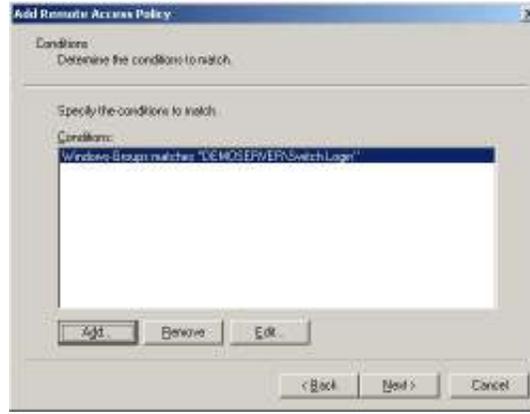
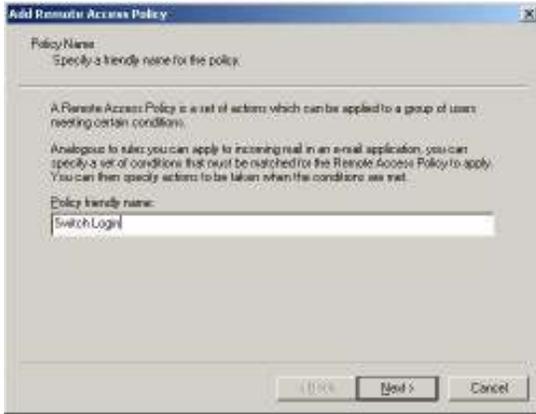


Next, create a new remote access policy under IAS. Call it Switch Login.

Specify it to match users in the switch access group

Next, create a new remote access policy under IAS. Call it Switch Login.

Specify it to match users in the switch access group

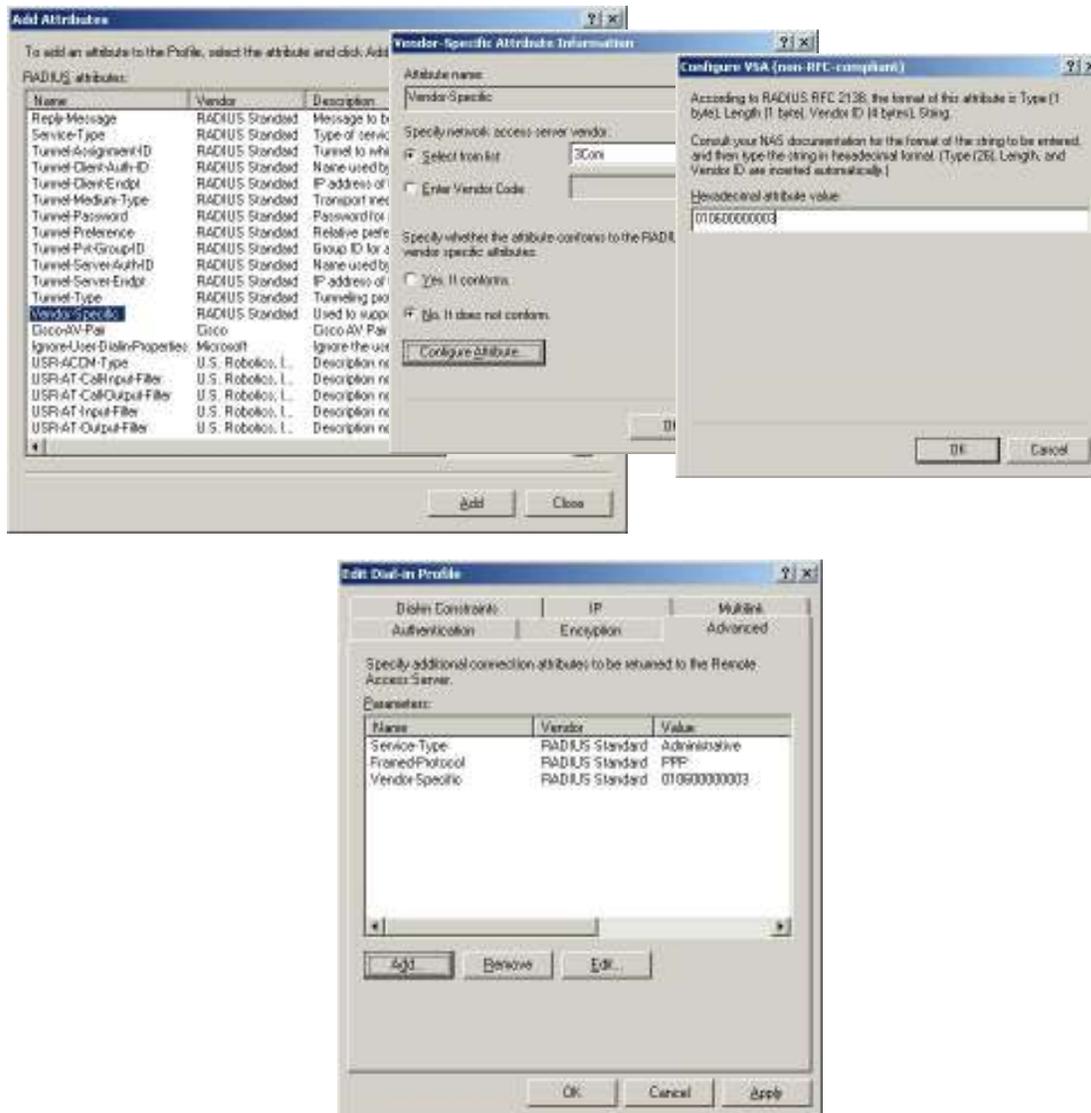


And allow it to grant access to these users

Change the Service-Type to be "Administrative"



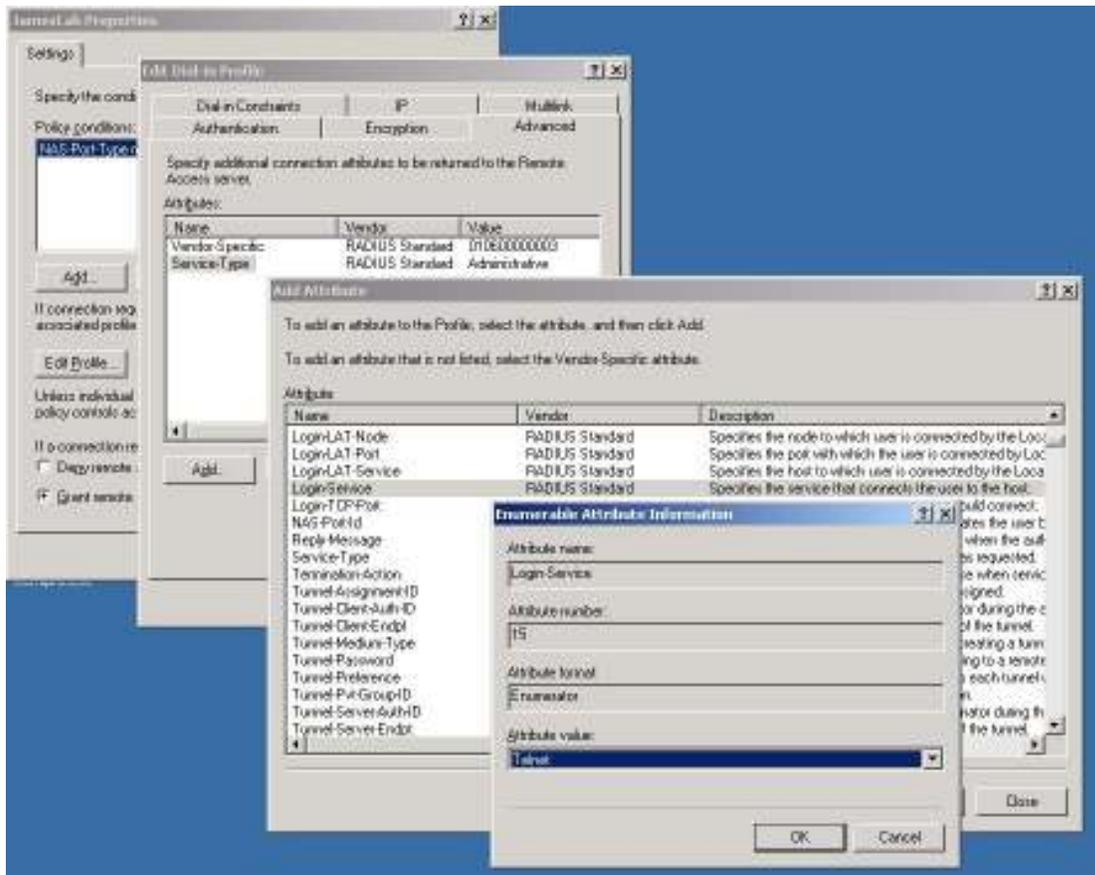
Also, add a Vendor specific attribute to indicate the access level that should be provided:



Note: The Value 010600000003 indicates admin privileges for the switch. 01 at the end indicates monitor and 02 indicates manager access. On the 5500, 00 indicates visitor level.

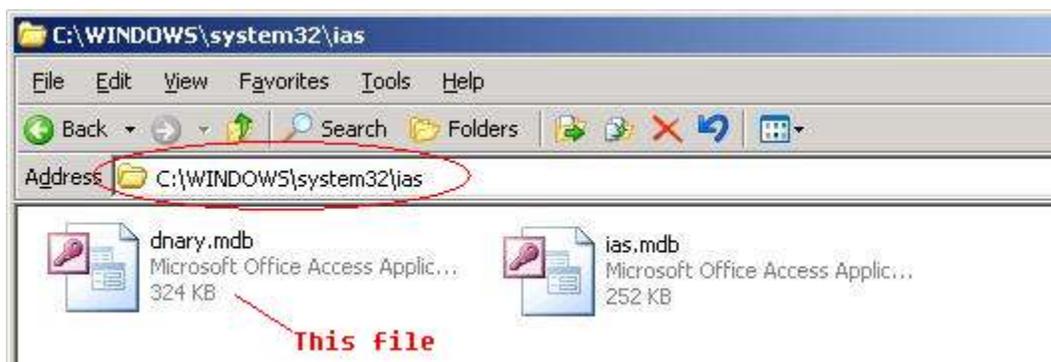
2.7.2 Switch login via Telnet / SSH

To allow switch login via Telnet, another attribute "Login-Service" need to be added. As shown in the photo below, right-click on the profile needs to be edited, then "properties" → "Edit Profile" → "Add" → "Login-Service" → "Telnet" → "OK" → "Close" → "OK" → "OK". Now, switch login via telnet is allowed.



To allow switch login via SSH, need to modify the IAS system file as shown in the photo below.

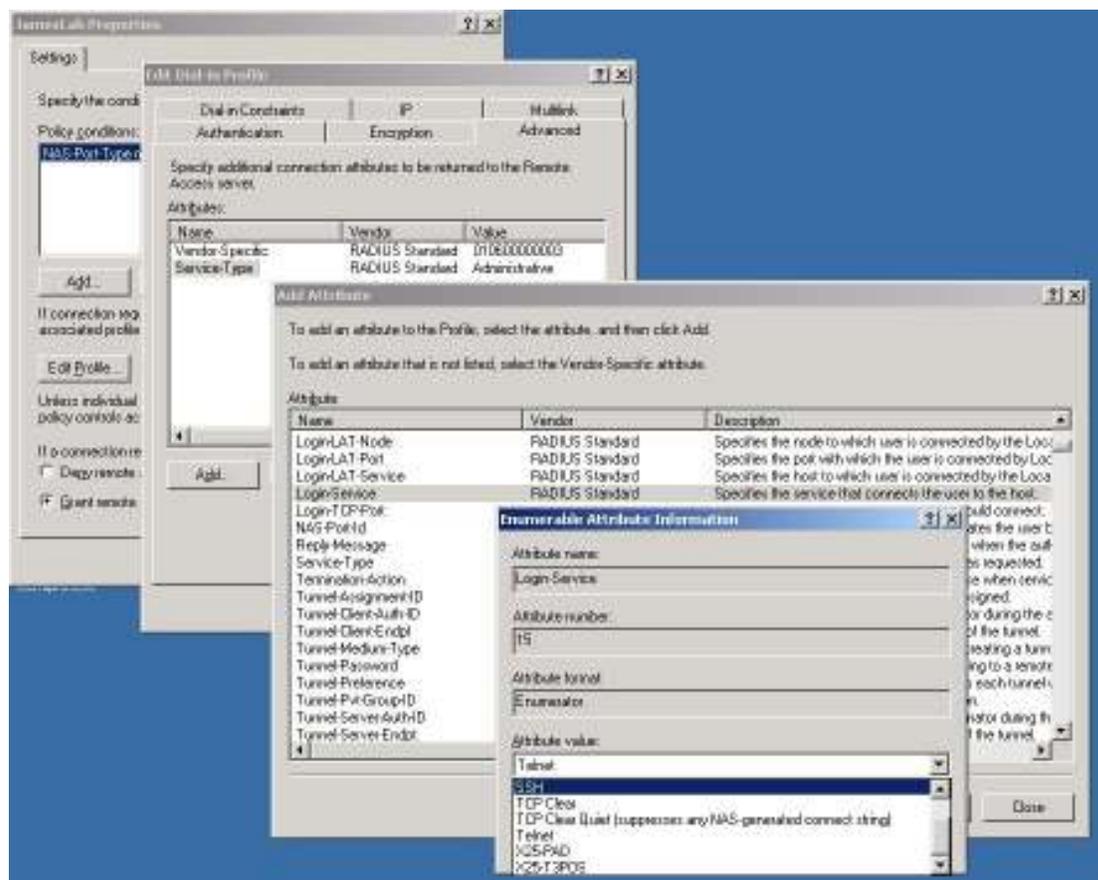
Note: 3Com will not take any responsibility to the influence or damage caused by the following operations.



Open `C:\WINDOWS\system32\ias\dnary.mdb` with MS Access, then find and open table "Enumerators", add a new record into this table as shown in the photo below:

Name	Enumerates	Value
Send-Listen	Framed-Routing	3
Telnet	Login-Service	0
Rlogin	Login-Service	1
TCP Clear	Login-Service	2
Portmaster (proprietary)	Login-Service	3
LAT	Login-Service	4
X25-PAD	Login-Service	5
X25-T3POS	Login-Service	6
TCP Clear Quiet (suppr	Login-Service	8
SSH	Login-Service	50
User-Name	Manipulation-Target	1

Then save the database file, restart the IAS service, now SSH appears in the list as shown in the photo below:



Choose "SSH", and then save the configuration. Now switch login via SSH is allowed.

2.8 Configure the client

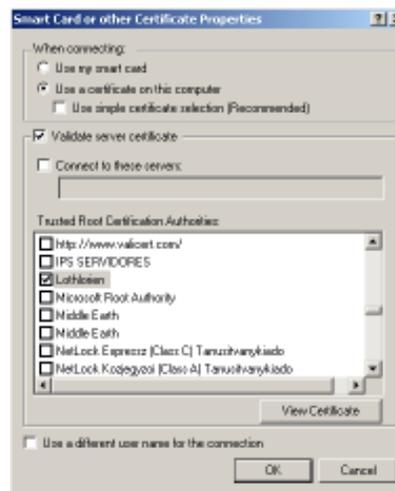
Windows XP has already a built in IEEE 802.1x client. For Windows 2000, Service Pack 3 is required, plus the IEEE 802.1x client patch for Windows 2000 (if required). Downloaded from: <http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=6B78EDBE-D3CA-4880-929F-453C695B9637>

After the updates are installed, you need to start the Wireless Authentication Service in Component Services on the Windows 2000 workstation.

After starting the service (set it to startup type: Automatic), open the Network and Dial up connections folder, right click on the desired Network Interface and select "Properties".

Select the **Authentication** tab and check the **Enable Network Access Control using IEEE 802.1x**

Set **Smart Card or Certificate** as EAP type and select the previously imported certificate as shown below.



You should now be able to establish an IEEE 802.1x session, using Microsoft's Internet Authentication Service. When you are prompted to select a certificate (it could be that there are additional active certificates on your client computer), select the certificate that you have installed for this specific Certification Authority server.

If you encounter problems, the event viewer on the server show detailed information as to what is happening, better what is going wrong. You should check the System log.

This concludes the standard configuration of IEEE 802.1x, using certificates with Windows 2000 Internet Authentication Services and Certification Authority. The next paragraph demonstrates how to configure VLAN membership using Vendor Specific Attributes.

2.9 Configure auto VLAN and QoS membership

The first step is to define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group. The VLAN Groups are used by IAS to assign the proper VLAN ID to each user account.

Click on the Start Button -> Programs -> Administrative Tools -> Active Directory Users and Computers

Using the **Active Directory Users and Computers** administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the switch. The VLAN Groups must be created as Global/Security groups. In this example we will create one group that will represent VLAN 4.

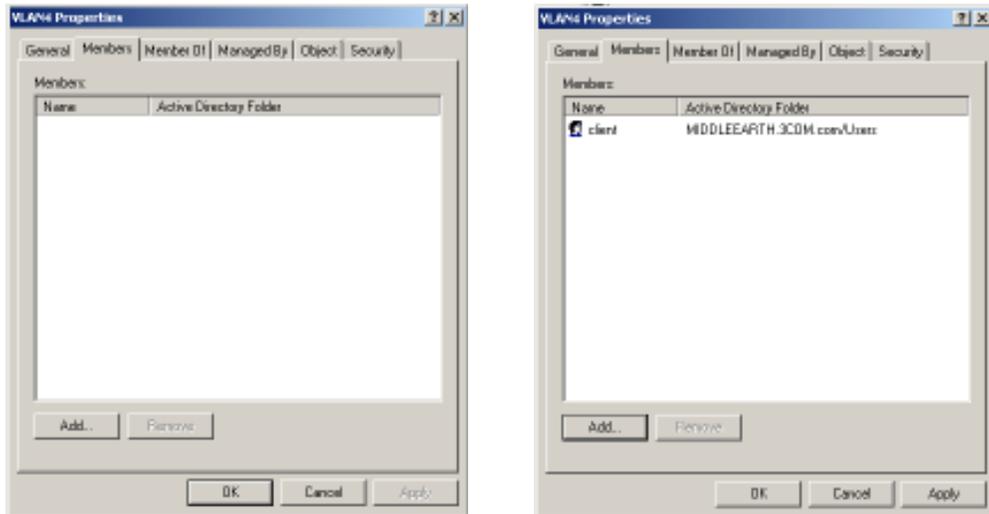
Select the “Users” folder from the domain (see below), and click on 



- Name the VLAN Group with a descriptive name that describes the VLAN Group's function, for example “VLAN4”



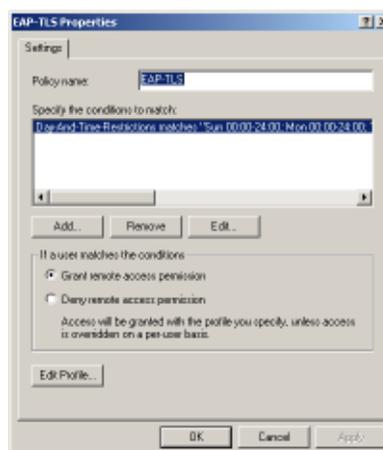
- Check the **Global** Group Scope parameter.
- Check the **Security** Group Type parameter.
- Click “OK” and then select the group, right click and select “Properties”.
- Click on the “Members” tab and add the users that have received the certificate and will use the VLAN functionality.



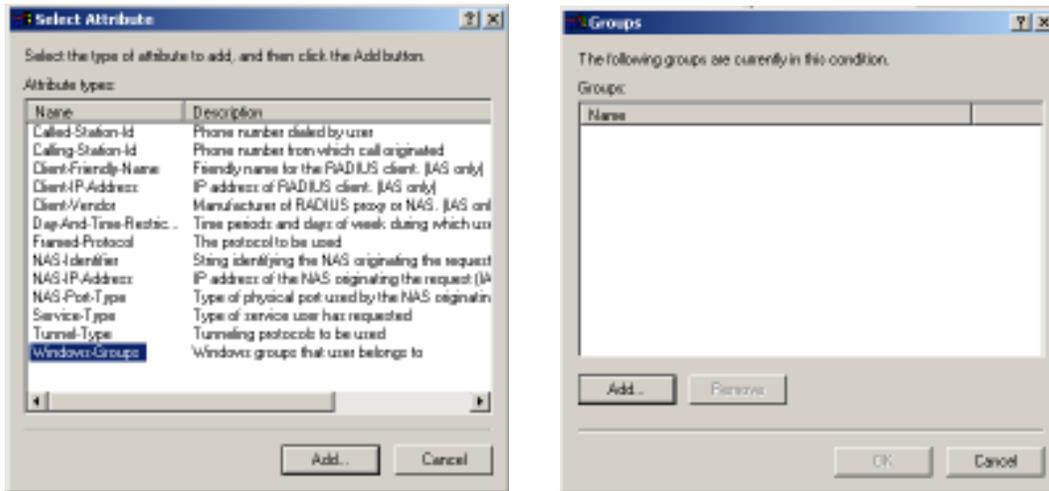
- Click on the Start Button -> Programs -> Administrative Tools -> Internet Authentication Service.
- Click on "Remote Access Policies", select the policy that you have configured earlier, right click and select "Properties".



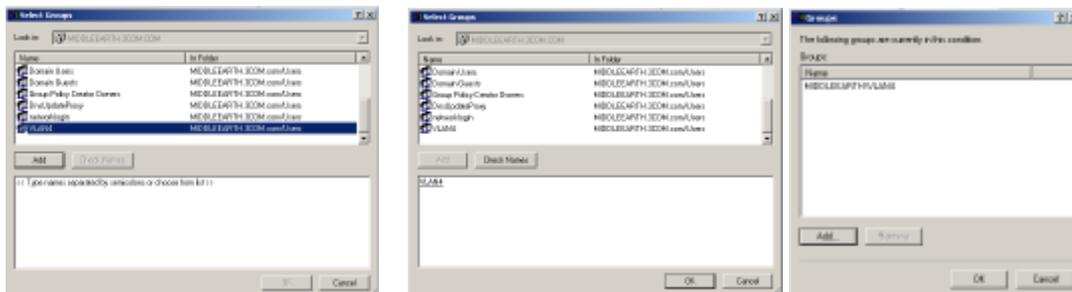
- Click "Add". We will be adding policy membership.



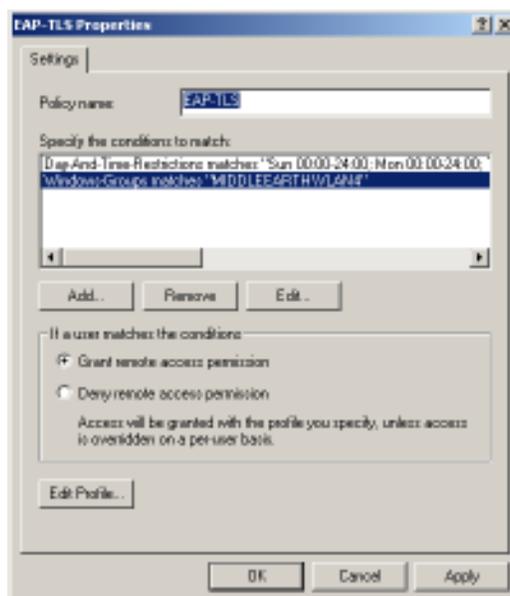
- Select the "Windows-Groups" attribute type and click on the "Add" button.



- Click "Add" again.
- Select the VLAN group that you have just created and click "Add". Click "OK" to confirm.



- Click "OK" again and you are back in the Security Policy properties.

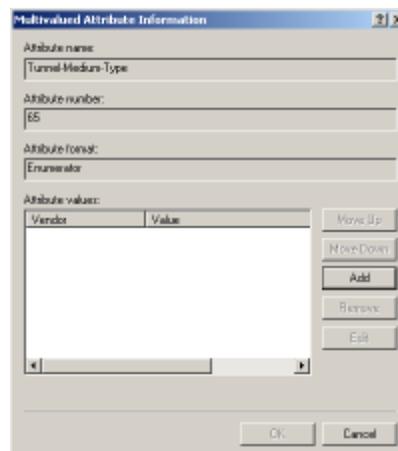


- Click “Edit Profile”
- Select the “Advanced” tab.
- Click “Add”. From the list we need to add three Radius attributes for VLAN
 - o Tunnel-Medium-Type
 - o Tunnel-Pvt-Group-ID
 - o Tunnel-Type
- And for QoS, we need to add one Radius attribute as a string:
 - o Filter-id

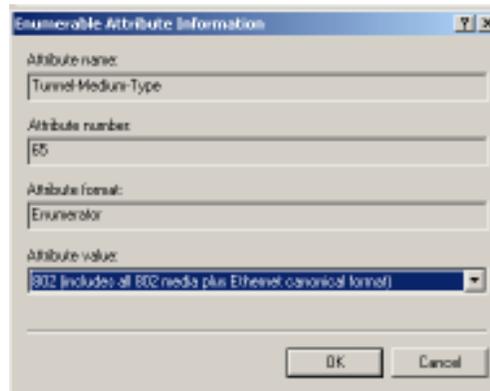
2.9.1 Summary of auto VLAN and QoS attributes

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name
For Auto VLAN		
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	← VLAN value
Tunnel-Type	VLAN	

- Select “Tunnel-Medium-Type” and click “Add”.



- Ensure that the Attribute value is set to 802 and click “OK”.

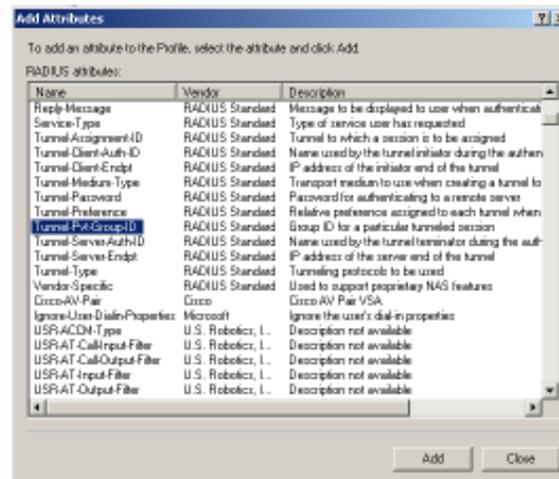


The dialog box titled "Enumerable Attribute Information" contains the following fields:

- Attribute name: Tunnel-Medium-Type
- Attribute number: 65
- Attribute format: Enumerated
- Attribute value: 802 (includes all 802 media plus Ethernet canonical format)

Buttons: OK, Cancel

- Click “OK” again on the Multivalued Attribute Information screen and you are back in the “Add Attributes” screen.
- Now, select the “Tunnel-Pvt-Group-ID” entry and click “Add”.

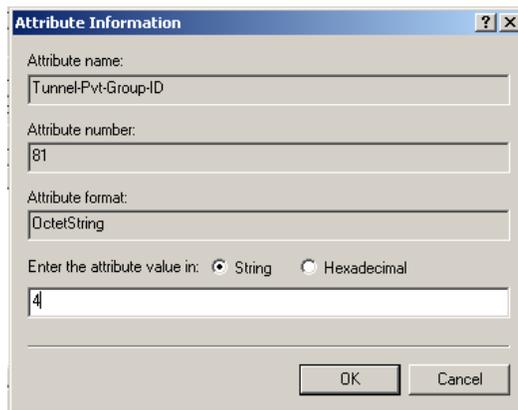


The dialog box titled "Add Attributes" contains a table of RADIUS attributes:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Message to be displayed to user when authentication fails
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authentication
Tunnel-Client-Endpoint	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel to a remote server
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when multiple tunnels are available
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the authentication
Tunnel-Server-Endpoint	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-NA-Pair	Cisco	Cisco AN Pair VSA
Ignore-User-Dial-Properties	Microsoft	Ignore the user's dial-in properties
USRACM-Type	U.S. Robotics, L.	Description not available
USRAT-Call-Input-Filter	U.S. Robotics, L.	Description not available
USRAT-Call-Output-Filter	U.S. Robotics, L.	Description not available
USRAT-Input-Filter	U.S. Robotics, L.	Description not available
USRAT-Output-Filter	U.S. Robotics, L.	Description not available

Buttons: Add, Close

- Click “Add”, ensure that the Attribute value is set to 4 (Attribute value in string format), and click “OK”. This value represents the VLAN ID.



Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

Enter the attribute value in: String Hexadecimal

4

OK Cancel



Multivalued Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

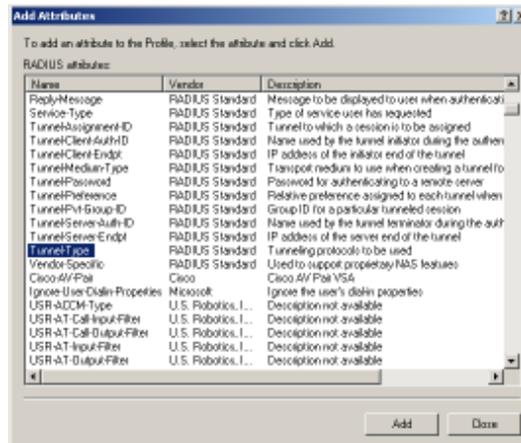
Attribute values:

Vendor	Value
RADIUS Standard	4

Move Up
Move Down
Add
Remove
Edit

OK Cancel

- Click “OK” again on the Multivalued Attribute Information screen and you are back in the “Add” Attributes” screen.
- Now, select the “Tunnel-Type” entry and click “Add”.



Add Attributes

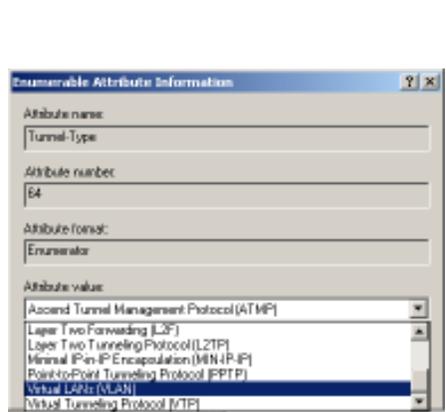
To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor	Description
ReplyMessage	RADIUS Standard	Message to be displayed to user when authenticating.
Service-Type	RADIUS Standard	Type of service user has requested.
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authentication.
Tunnel-Client-Endpoint	RADIUS Standard	IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel to a remote server.
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server.
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when Group ID for a particular tunneled session.
Tunnel-Pvt-Group-ID	RADIUS Standard	Name used by the tunnel terminator during the authentication.
Tunnel-Server-Endpoint	RADIUS Standard	IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used.
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features.
Cisco-AAA-Post-Auth	Cisco	Cisco AAA Post-Auth.
Ignore-User-Claim-Properties	Microsoft	Ignore the user's claim properties.
USR-ACM-Type	U.S. Robotics, I...	Description not available.
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available.
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available.
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available.
USR-AT-Output-Filter	U.S. Robotics, I...	Description not available.

Add Close

- Click “Add” again.
- In the pull down menu, select “Virtual LANs” and click “OK”.



Enumerable Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
84

Attribute format:
Enumerated

Attribute value:
Ascend Tunnel Management Protocol (ATMP)

Layer Two Forwarding (L2F)
Layer Two Tunneling Protocol (L2TP)
Minimal IP-in-IP Encapsulation (MIN-IP-IP)
Point-to-Point Tunneling Protocol (PPTP)
Virtual LANs (VLAN)
Virtual Tunneling Protocol (VTP)



Multivalued Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
84

Attribute format:
Enumerated

Attribute values:

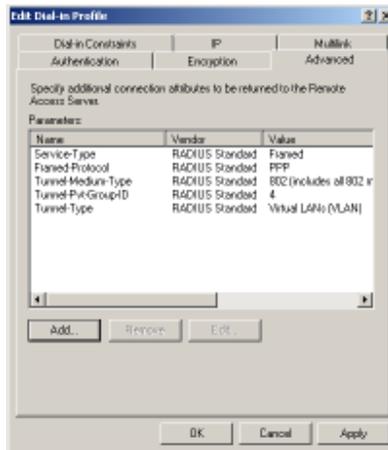
Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

Move Up
Move Down
Add
Remove
Edit

OK Cancel

- Click “OK” again and you are back in the “Add” Attributes” screen.

- Click “Close” on the “Add Attributes” screen. You will now see the added attributes



- Click “OK” to close the Profile screen and “OK” again to close the Policy screen. This concludes the configuration of the Internet Authentication Service.

In order to test this, the workstation is connected to a port that does not have to be a member of VLAN 4. Ensure that there is a DHCP server, connected to the switch that resided on a switch port that is an untagged member of VLAN 4. The Radius server resides in the same VLAN as the workstation.

Once authenticated the switch will receive VLAN information from the Radius server and will place the switch port in the associated VLAN.

For troubleshooting, you can use the Event Viewer on both the workstation and the Radius server.

3 Funk Radius Setup

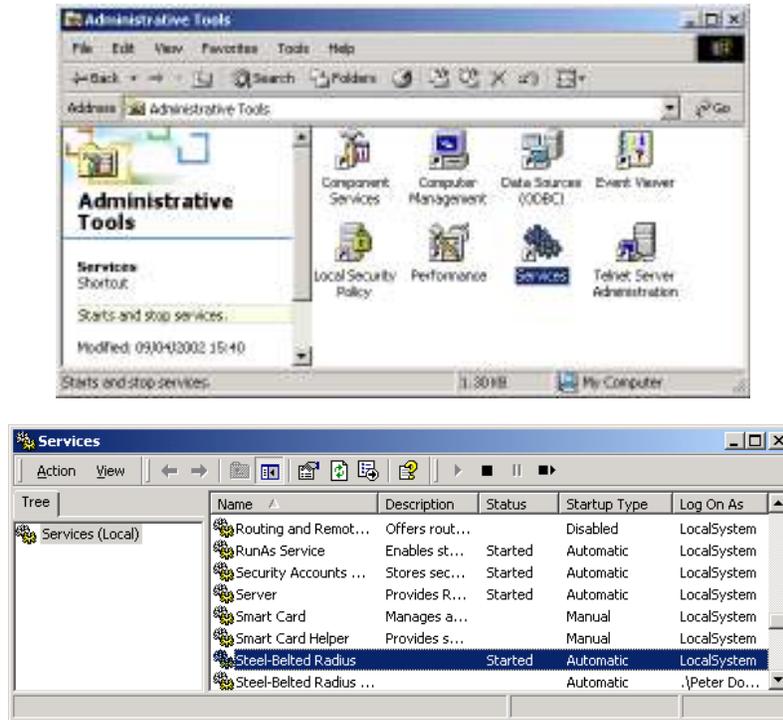
3.1 Downloading and installing Funk

Funk Radius is not a 3Com product and will not be supported by 3Com. Funk Radius is simple to setup and operate, this document will guide you through the very basics for operation with the 3Com Switch for the purposes of a product demonstration

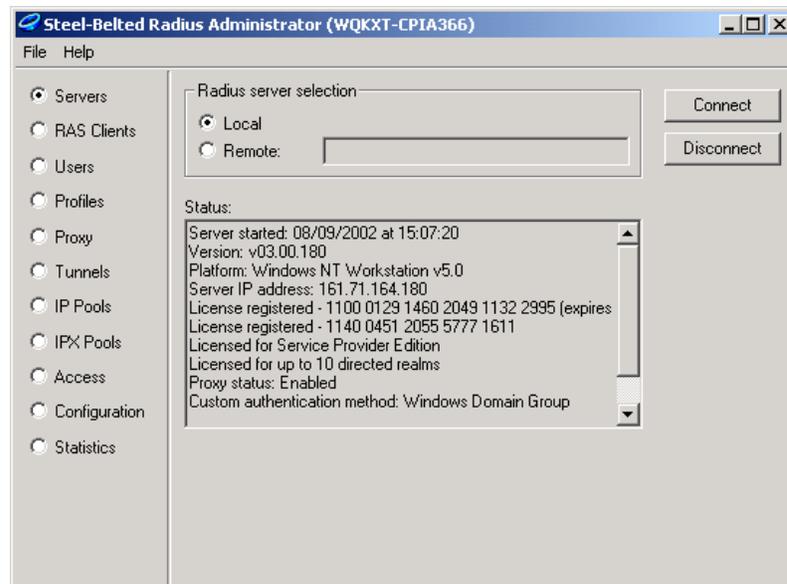
Funk Steal Belt Radius Server can be downloaded from www.funk.com. Once installed you have a 30 days license to use it.

Once installed you will need to edit a couple of files to make it work. First of all open eap.ini (\radius\service\EAP.ini) and remove the “;” before MD5-Challenge Line. This enables the MD5-challenge

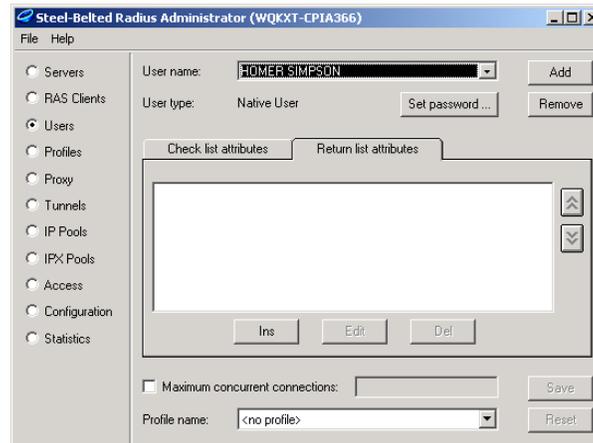
Eap.ini ← or copy this file to \radius\service (already edited)



Funk Radius is now ready to run. Start the program from the start menu and click connect to start listening for clients.

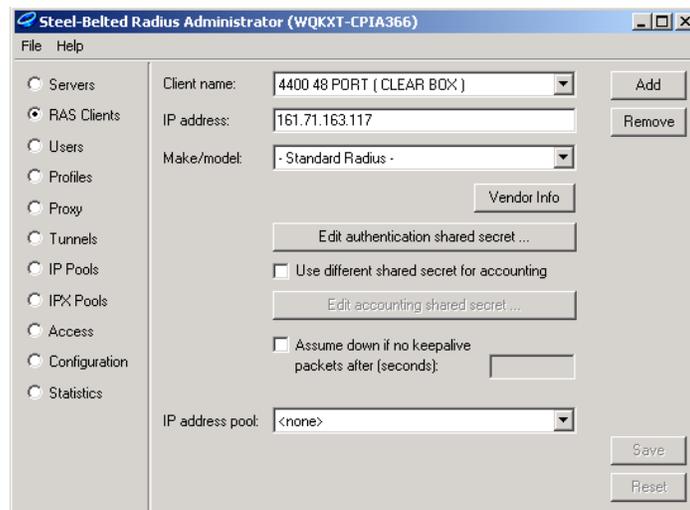


Add a user for your demonstration, and their password, passwords are case sensitive.



Now the shared secret must be entered this is used to encrypt the authentication data and must be identical on the switch and the Radius Server

You must enter the details for the RAS clients, the name is arbitrary, enter the IP address and the shared secret.



3.2 Configuring auto VLAN and QoS

Return attributes from the Funk RADIUS server can be configured to be returned to the switch. At the time of writing the correct tunnel attributes do not exist in the default configuration of Funk Radius, therefore some Dictionary files need to be edited before the steel belted service is started.



Radius.dct ←Pre-edited dictionary file. Copy this file into your Radius\service directory.

By placing a R after the correct attributes in the file, they will now appear as potential Return list attributes for every user

```

radius.dct Notepad
File Edit Format View Help
#####
#----- Tunnel Attributes -----
#####
ATTRIBUTE Tunnel-Type          64 [tag=0 data=integer] tR
VALUE Tunnel-Type              PPTP 1
VALUE Tunnel-Type              L2F  2
VALUE Tunnel-Type              L2TP 3
VALUE Tunnel-Type              ATMP  4
VALUE Tunnel-Type              VTP   5
VALUE Tunnel-Type              AH    6
VALUE Tunnel-Type              IP-IP 7
VALUE Tunnel-Type              MIN-IP-IP 8
VALUE Tunnel-Type              ESP   9
VALUE Tunnel-Type              GRE   10
VALUE Tunnel-Type              DVS   11
VALUE Tunnel-Type              IP-IP-Tunneling 12
VALUE Tunnel-Type              VLAN  13
ATTRIBUTE Tunnel-Medium-Type   65 [tag=0 data=integer] tR
VALUE Tunnel-Medium-Type       IP    1
VALUE Tunnel-Medium-Type       X.25  2
VALUE Tunnel-Medium-Type       ATM   3
VALUE Tunnel-Medium-Type       Frame-Relay 4
    
```

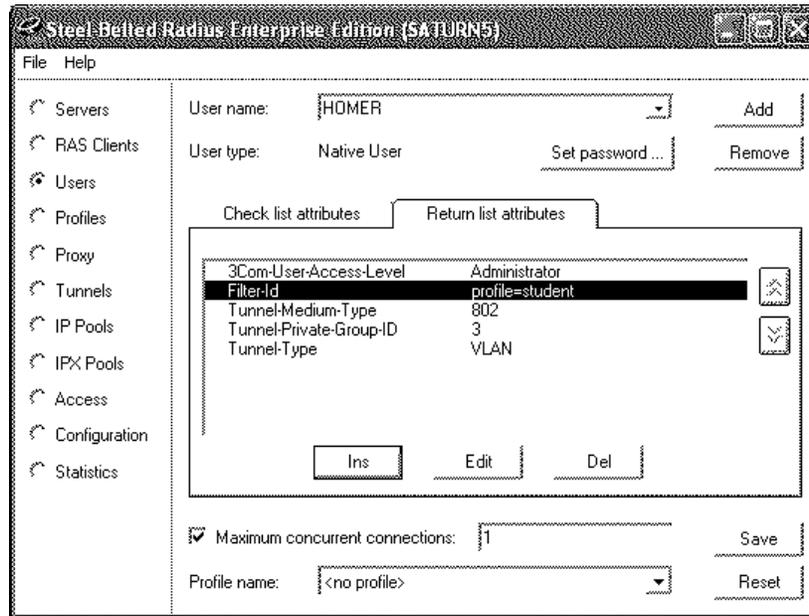
Once this file has been replaced, you will need to stop and restart the Steel-Belted RADIUS service.

To use these return list attributes, they need to be assigned to a user or group. Create a new user and add the following return list attributes:

3.2.1 Summary of auto VLAN and QoS attributes

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name
For Auto VLAN		
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	← VLAN value
Tunnel-Type	VLAN	

Note: The VLANs and QoS profiles must be created on the 3Com switch unit.



4 Configuring FreeRadius

FreeRADIUS comes as source from <http://www.freeradius.org>. Download and install it following the instructions from the website. I have used it under Solaris 2.6 and seen it working under RedHat Linux

This guide covers setting up the server with a 3Com switch as the client and adding users. This is covered below to allow you to set up a demo. It assumes that you have a standard version of FreeRADIUS installed.

4.1 Adding a client

The client to add is the details of the 3Com switch. This should be added to the existing file "clients.conf" in /usr/local/etc/raddb, add an entry for the switch you wish to administer:

```
client aaa.aaa.aaa.aaa {
    secret      = a-shared-secret
    shortname  = a-short-name
}
```

Where aaa.aaa.aaa.aaa is the IP address of the 3Com switch.

4.2 Updating the dictionary for Switch login

Create a new file called "dictionary.3Com" in /usr/local/etc/raddb containing the following information:

```
VENDOR      3Com      43
```

ATTRIBUTE	3Com-User-Access-Level	1	Integer	3Com
VALUE	3Com-User-Access-Level	Monitor	1	
VALUE	3Com-User-Access-Level	Manager	2	
VALUE	3Com-User-Access-Level	Administrator	3	

So that the new file will be used in configuring the server, edit the existing file “dictionary” in /usr/local/etc/raddb to add the following line:

```
$INCLUDE dictionary.3Com
```

Here is a pre-edited file:



dictionary.3Com

Remember to still add the “Include” line to the dictionary file.

4.3 Adding Users

4.3.1 For Switch Login

In the existing file “users” in /usr/local/etc/raddb, add an entry for each user who is authorized to administer the switch, indicating that the server should return the 3Com vendor specific attribute “3Com-User-Access-Level” in the Access-Accept message for that user.

```
user-name Auth-Type = System, 3Com-User-Access-Level = Administrator
```

4.3.2 For Network Login

As above, but the Auth-Type should be local:

```
user-name Auth-Type := Local, User-Password == "password"
```

When running up the RADIUS server with “radiusd”, turn on debugging so you can see any problems that may occur with the authentication:

```
cd /usr/local/sbin
./radiusd -sfxyz -l stdout
```

4.4 Auto VLAN and QOS setup

It is slightly more complex to set up auto VLAN and QoS using FreeRADIUS, as the dictionary file needs to be specially updated.

4.4.1 Ensure you have the attributes defined in the dictionary files

For auto VLAN, you need to make sure that you update the dictionary.tunnel file. Ensure that you have the following lines:

ATTRIBUTE	Tunnel-Type		64	integer has_tag
ATTRIBUTE	Tunnel-Medium-Type		65	integer has_tag
ATTRIBUTE	Tunnel-Private-Group-Id		81	string has_tag
VALUE	Tunnel-Type	VLAN	13	
VALUE	Tunnel-Medium-Type	TMT802		6



Or here is the pre-edited dictionary file: `dictionary.tunnel`

4.4.2 Add the return list attributes to the user in the users file

Once this is done, it's merely a matter of adding the return list attributes to the user:

```
bob    Auth-Type := Local, User-Password == "bob"
      Tunnel-Medium-Type = TMT802,
      Tunnel-Private-Group-Id = 2,
      Tunnel-Type = VLAN,
      Filter-Id = "profile=student"
```

For details of the meanings of each of these return list attributes see section Return List Attributes Supported on 4400.

Note: If you make the "Tunnel-Medium-Type" 802 in the users file, assuming it is going to be looked up in the dictionary and return the integer 6, then it does not. FreeRADIUS sees "802" as a number, rather than a string in the "users" file, therefore does not bother looking in the dictionary and returns Tunnel-Medium-Type as integer 802 rather than integer 6.

This is why I have added the Tunnel-Medium-Type as "TMT802" rather than "802" in the dictionary file, so there are characters in it to force the "users" file to lookup the value in the dictionary.

5 Cisco Secure ACS Setup (TACACS+)

Cisco Secure ACS and TACACS+ are proprietary protocols and software created by Cisco which provide similar functionality as a RADIUS server. Some enterprises today may already contain a Cisco Secure ACS server with TACACS+ that they wish to continue to use to provide centralised control over network and management access.

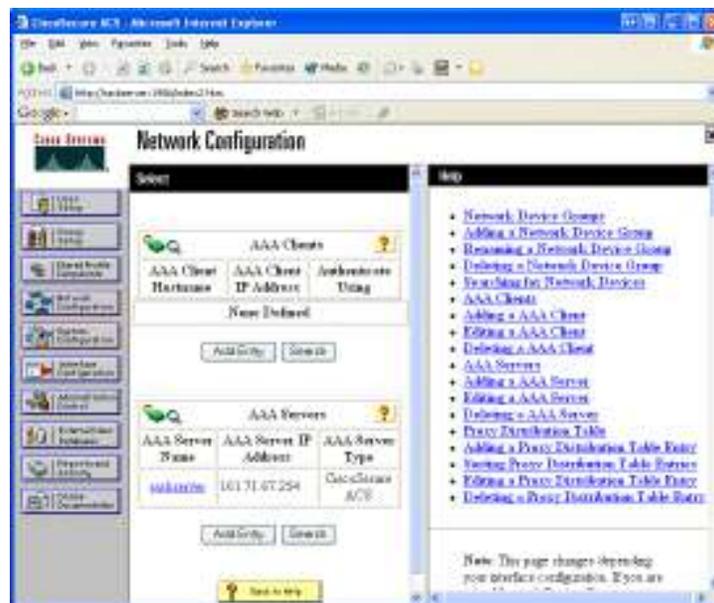
As 3Com does not directly does not support the proprietary TACACS+ protocol, it can lead to the incorrect assumption that a 3Com switch cannot be authenticated in an environment based on TACACS+ and Cisco Secure ACS.

Cisco's windows based Cisco Secure ACS server also contains a built in RADIUS server. This RADIUS server integrates seamlessly with the TACACS database allowing 3Com switches to authenticate correctly using RADIUS protocol. Users that already exist on the TACACS+ server can be authorised using the TACACS+ or RADIUS server, an optional VLAN and QoS profile can be applied to the user. Network administration users can also be authorised using the built in RADIUS server, providing centralised access to 3Com switches.

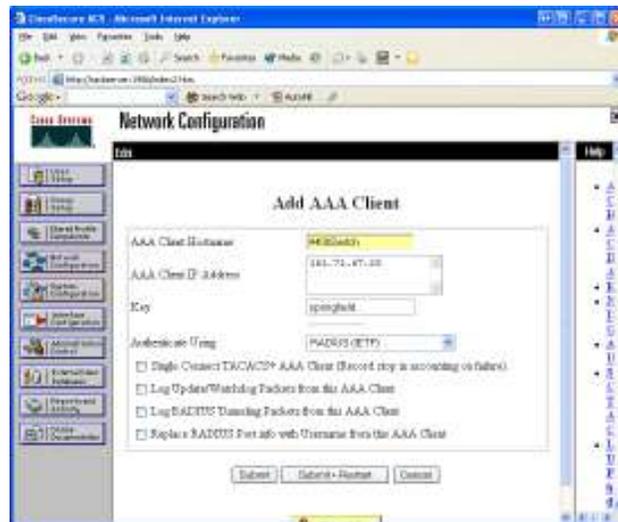
This section covers the setup of Cisco Secure ACS (v3.3) to operate using RADIUS with a 3Com switch. The configuration of Cisco Secure ACS all takes place through a web interface. You can log into the web interface from any PC or the localhost of the server, using port 2002 - eg <http://TACACS-server:2002>.

5.1 Adding a 3Com switch as a client of Cisco Secure ACS

Once logged into the Cisco secure ACS interface, click on "Network Configuration" on the left hand side and then "Add entry", under AAA clients.

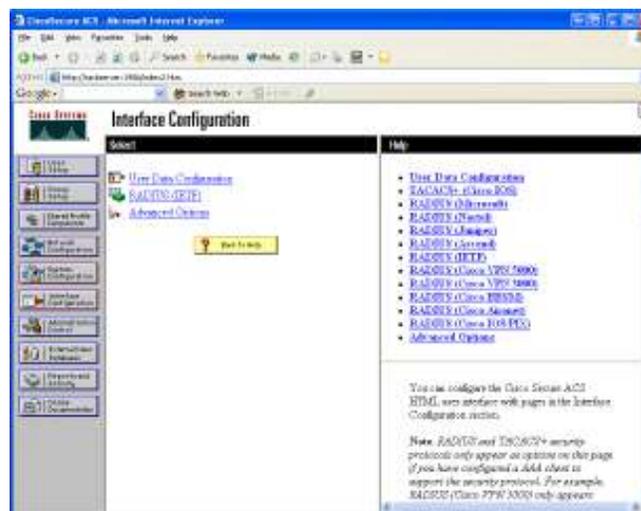


Add the details of the 3Com switch. An example is below:



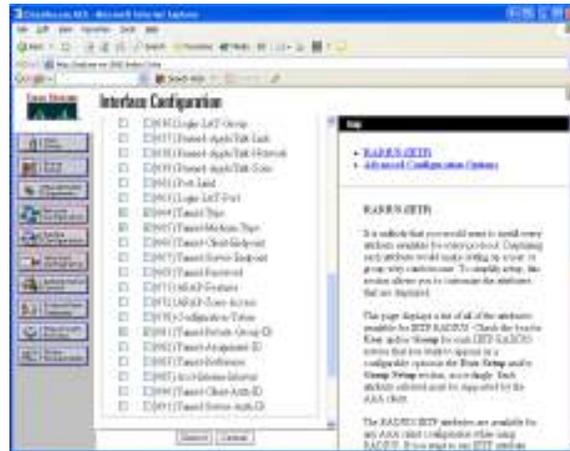
Note: you cannot have spaces in the AAA Client Host name.

Once a client with RADIUS has been defined, the options for RADIUS configuration will appear under the "Interface Configuration" option.



Selecting RADIUS (IETF) allows you to edit which RADIUS attributes are available. If you want to use auto VLAN and QoS, ensure that you have the following options selected for user and group:

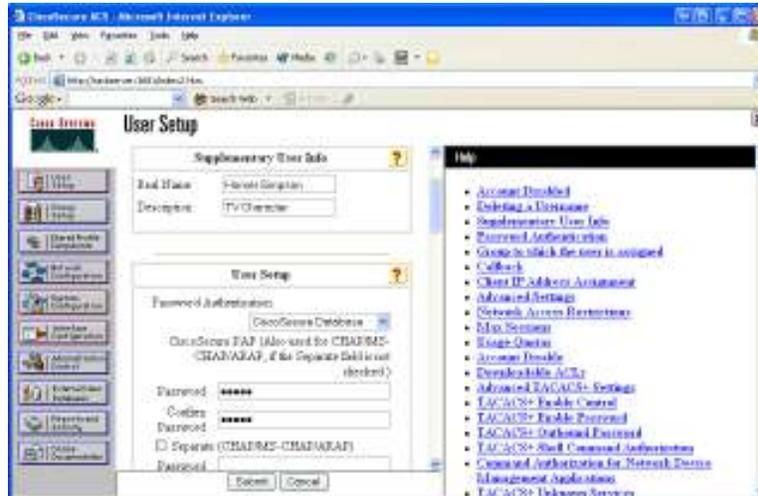
Filter-ID
 Tunnel-Type
 Tunnel-Medium-Type
 Tunnel-Private-Group-ID



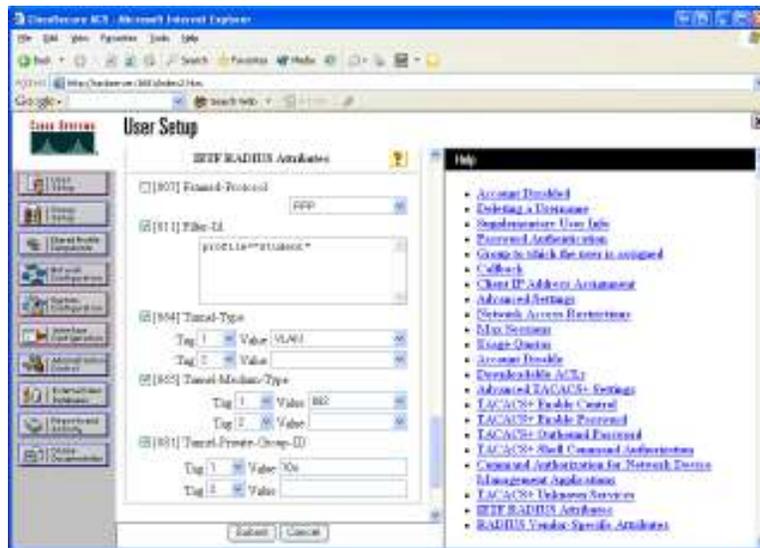
5.2 Adding a user for Network Login

From the left hand side menu, select “User setup”. Enter the username, and click “Add/edit”

Enter the user information as requested:



If you want to return specific RADIUS attributes, they can be set further down the user profile. Below, we have set the user up to use the student profile and be assigned to VLAN 10 untagged.



Note: the RADIUS attributes need to be set up as described in the previous section.

5.3 Adding a user for Switch Login

Adding a user for switch login is slightly more complex, as 3Com specific RADIUS attributes are required to be returned to the 3Com switch. These RADIUS attributes are used to define the access level of the the user to the management interface.

The required RADIUS attributes can be added to the ACS server, by editing an ini file and compiling it into the Secure ACS RADIUS server. This has already been created and is attached below:

```
[User Defined Vendor]

Name=3Com
IETF Code=43
VSA 1=3Com-User-Access-Level

[3Com-User-Access-Level]

Type=INTEGER
Profile=OUT
Enums=3Com-User-Access-Level-Values

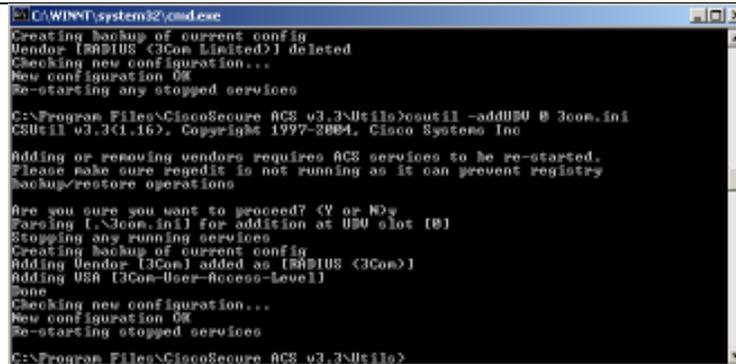
[3Com-User-Access-Level-Values]
1=Monitor
2=Manager
3=Administrator
```

Or here is a version in a text file: 3com.ini

The details of this file can be added to Cisco's secure ACS using an application called csutil.exe. This can be found in the "utils" directory of the install path (eg. C:\program files\Cisco Secure ACS\utils\).

Copy the 3Com.ini file into the utils directory and then, using a command prompt, execute csutil.exe with the following arguments:

```
csutil -addUDV 0 3Com.ini
```



```
C:\WINNT\system32\cmd.exe
Creating backup of current config
Vendor [RADIUS (3Com Limited)] deleted
Checking new configuration...
New configuration OK
Re-starting any stopped services

C:\Program Files\CiscoSecure ACS u3.3\utils>csutil -addUDV 0 3com.ini
CSUtil v3.3(1.16). Copyright 1997-2004. Cisco Systems Inc

Adding or removing vendors requires ACS services to be re-started.
Please make sure regedit is not running as it can prevent registry
backup/restore operations

Are you sure you want to proceed? (Y or N)y
Parsing [.\3com.ini] for addition at UDV slot [0]
Stopping any running services
Creating backup of current config
Adding Vendor [3Com] added as [RADIUS (3Com)]
Adding User [3Com-User-Access-Level]
Done
Checking new configuration...
New configuration OK
Re-starting stopped services

C:\Program Files\CiscoSecure ACS u3.3\utils>
```

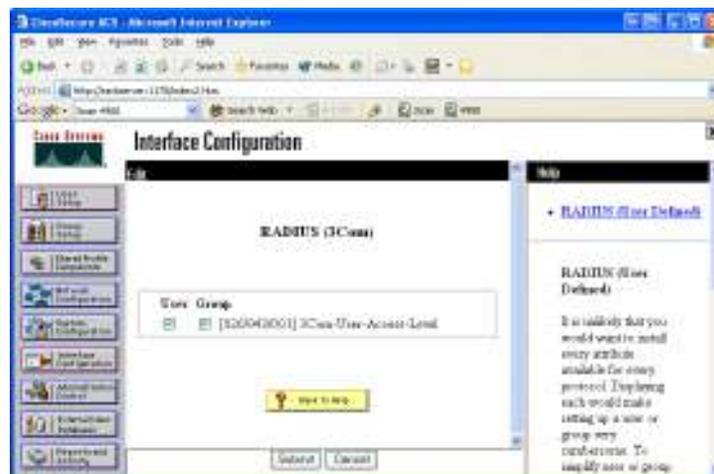
This will add 3Com.ini information into UDV (User Defined Vendor) slot 0. A list of information held in each slot can be seen by executing the command:

```
csutil -listUDV
```

This will stop the ACS server, add the RADIUS information, then restart the server. Once complete, log into the Secure ACS server again. To use the new RADIUS attributes, a client needs to be a user of the "RADIUS (3Com)" attributes. Add, or modify a device to use RADIUS (3Com). Note that the IETF attributes will still all be available and the 3Com attributes are appended to them.



Under the Interface Configuration, click on RADIUS (3Com) and ensure that the 3Com-User-Access-Level appears for both user and group setups:

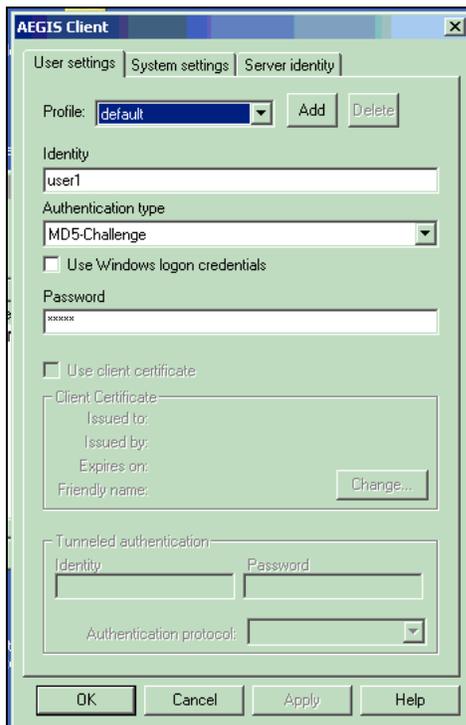
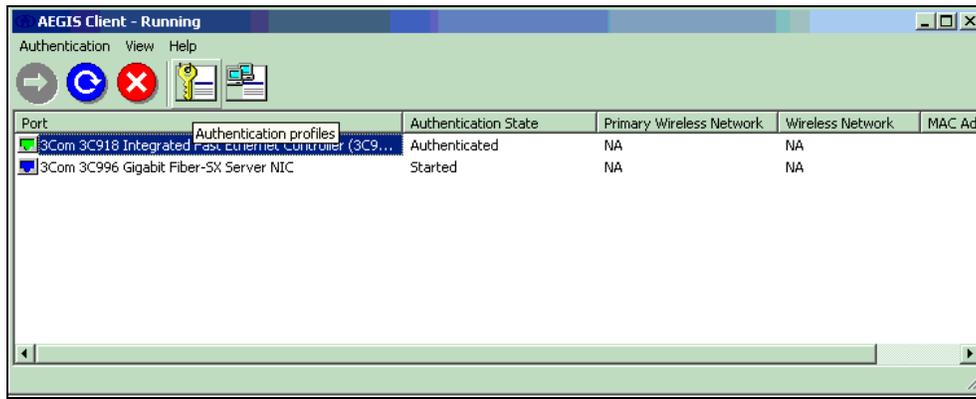


Next, we need to add a user and set their access level to a 3Com switch. Create a user as previously for network login. At the bottom of the configuration, there should also be the option for configuring the access level as shown below:

- Select Help on the top of Aegis Client → Register.
- Copy the License ID indicated at the bottom of the dialog into the License ID field.
- Copy the License Key provided in this email into the License Key field.
- Press OK button

6.2.2 Configuring the Aegis Client

After registration is finished, the Aegis Client need be configured. Click the Key icon, and a dialog will appear:



(**Note:** Leave the Profile as default, the Identity is an account which has been created on RADIUS Server with the Password.)

After the configuration has finished, restart the client either by rebooting or stopping and re-starting the service.

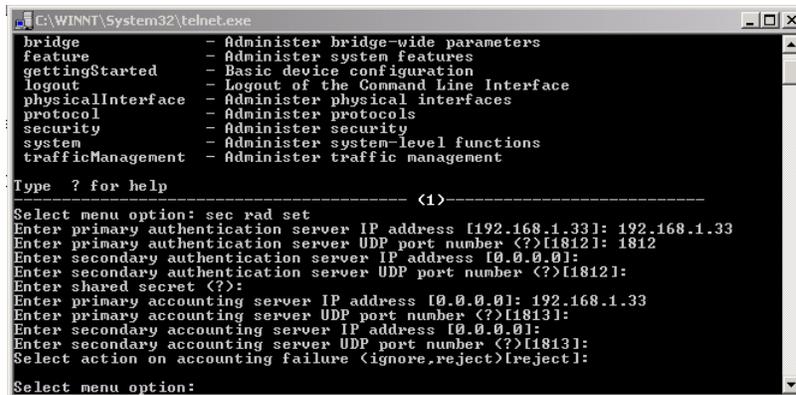


Click the OK button, then return to Aegis Client main interface. To restart the client, press the button with the red-cross. If authentication is successful, the icon becomes green.

7 Configure the SuperStack 3 Switch

7.1 Network Login

- Establish a Telnet or console session to the Switch.
- On the console, enter: **sec rad set**



```

C:\WINNT\System32\telnet.exe
bridge          - Administer bridge-wide parameters
feature         - Administer system features
gettingStarted  - Basic device configuration
logout         - Logout of the Command Line Interface
physicalInterface - Administer physical interfaces
protocol        - Administer protocols
security        - Administer security
system          - Administer system-level functions
trafficManagement - Administer traffic management

Type ? for help
----- (1)-----
Select menu option: sec rad set
Enter primary authentication server IP address [192.168.1.33]: 192.168.1.33
Enter primary authentication server UDP port number (?)[1812]: 1812
Enter secondary authentication server IP address [0.0.0.0]:
Enter secondary authentication server UDP port number (?)[1812]:
Enter shared secret (?):
Enter primary accounting server IP address [0.0.0.0]: 192.168.1.33
Enter primary accounting server UDP port number (?)[1813]:
Enter secondary accounting server IP address [0.0.0.0]:
Enter secondary accounting server UDP port number (?)[1813]:
Select action on accounting failure <ignore,reject>[reject]:
Select menu option:

```

- Provide the IP address of the Internet Authentication Server and ports that are used
- Enable the ports on the Switch that you would like to use for Authentication.
- On the console, enter: **sec net acc po**



```

C:\WINNT\System32\telnet.exe
Type ? for help
----- (1)-----
Select menu option:
Menu options: -----3Com SuperStack 3 Switch 4400-----
bridge          - Administer bridge-wide parameters
feature         - Administer system features
gettingStarted  - Basic device configuration
logout         - Logout of the Command Line Interface
physicalInterface - Administer physical interfaces
protocol        - Administer protocols
security        - Administer security
system          - Administer system-level functions
trafficManagement - Administer traffic management

Type ? for help
----- (1)-----
Select menu option: sec net acc port
Select user ports <unit:port...?>:

```

- Enter the port number and set the security level. In this setup we are going to use standardSecurity

```

E:\WINNT\System32\telnet.exe
system - Administer system-level functions
trafficManagement - Administer traffic management

Type ? for help
----- (1) -----
Select menu option:

Menu options: -----3Com SuperStack 3 Switch 4400-----
bridge - Administer bridge-wide parameters
feature - Administer system features
gettingStarted - Basic device configuration
logout - Logout of the Command Line Interface
physicalInterface - Administer physical interfaces
protocol - Administer protocols
security - Administer security
system - Administer system-level functions
trafficManagement - Administer traffic management

Type ? for help
----- (1) -----
Select menu option: sec net acc po
Select user ports (unit:port...?): 1:1
Enter mode of operation (?)[noSecurity]: standard
Select menu option:

```

- To view statistics on successful or failed logon attempts, enter: **sec rad auth di**
- To view statistics on the secured port, enter: **sec net acc det unit:port**

7.2 Switch Login

- Establish a Telnet or console session to the Switch.
- On the console, enter: **sec dev auth**

```

Telnet 141.71.67.27

Type "quit" to return to the previous menu or ? for help
----- (1) -----
Select menu option (security)! dev

Menu options: -----3Com SuperStack 3 Switch 4400 PWR-----
access - Administer access rights
authentication - Administer authentication mode
ssh - Administer SecureShell
trustedIpHost - Administer Trusted IP Host
user - Administer users

Type "quit" to return to the previous menu or ? for help
----- (1) -----
Select menu option (security/device)! auth

Menu options: -----3Com SuperStack 3 Switch 4400 PWR-----
loginz - Display authentication attempts
statisticz - Display authentication statisticz
summary - Display summary information
systemMode - Modify authentication mode

Type "quit" to return to the previous menu or ? for help
----- (1) -----
Select menu option (security/device/authentication)!

```

- Change the login mode using the systemMode command to enable RADIUS switch login
- Note – if the RADIUS server isn't defined (as outlined above) a warning will be shown.

```

Telnet 161.71.67.27
authentication - Administer authentication mode
ssh - Administer SecureShell
trustedIpHost - Administer Trusted IP Host
user - Administer users

Type "quit" to return to the previous menu or ? for help
-----
Select menu option <security/device>: auth
-----
Menu options: -----3Com SuperStack 3 Switch 4400 PWR-----
logins - Display authentication attempts
statistics - Display authentication statistics
summary - Display summary information
systemMode - Modify authentication mode

Type "quit" to return to the previous menu or ? for help
-----
Select menu option <security/device/authentication>: sys
Select authentication mode <local,RADIUS>[local]: RADIUS

WARNING: RADIUS is not configured. RADIUS authentication will fail.
Do you wish to continue <yes,no>[no]: yes

Select menu option <security/device/authentication>:

```

- Before RADIUS login will work, the server needs to be configured with the correct return list attributes. See the 3com-user-access-level return list attribute below
- **If the switch cannot access the RADIUS server it will revert to its local database for authentication on the console port. The Web and Telnet interfaces do not revert and will not authenticate if the switch cannot access the RADIUS server.**

7.3 Radius Authenticated Device Access (RADA)

Radius Authenticated Device Access (RADA) extends the functionality of 802.1x login. RADA has been developed internally by 3Com as a feature to ensure only allowed devices have access to network resources. It is similar to Disconnect Unknown Device (DUD), however allows centralized management of the device database and works alongside 802.1x Network Login to ensure both the device AND the user are authorized.

The feature is very flexible, allowing the network administrator many different ways of securing their network, while not being overly complex to reduce the productivity of users of the network.

There are a number of advantages that the RADA feature provides in v5.0 software. This section covers the different RADA setups and the advantages they provide. It assumes understanding of RADIUS server setups for 802.1x and return list attributes for auto VLAN and QoS.

Currently RADA is only available on the 3Com SuperStack 3 Switch 4400 v5.X and above.

7.3.1 General setup tips

The below examples use Microsoft IAS as the RADIUS server, but configuration should be similar on any other RADIUS server.

The RADA feature is very flexible and there can be more than one solution to a problem using RADA and 802.1x. We have tried to suggest the best method here, however users may want to do it differently and will achieve a similar solution.

By default, the 3Com Switch will send the username and password to the switch as the MAC address of the end client. This means for each device, a new user has been created on the RADIUS server. This can be inconvenient, therefore RADA has the ability to change the username and password to fixed strings. This means only one user is required on the RADIUS server to support RADA. The devices are still identified using its MAC address, but it is sent as the check-list

attribute “Calling-Station-Id”. The fixing of the username and password strings is done by writing to the MIB items secureRadaAuthUsername and secureRadaAuthPassword.

The Radius server should be setup to create a new windows group for MAC addresses and contain a username and password that matches the details entered into the MIB:



The remote access policy should check to see if the username is a member of the MAC address group and that the calling-station-ids match:



7.3.2 Ensuring only company devices are connected to the corporate network

Scenario

As an increasing number of breaches of security happen from within the network, the case for ensuring only known devices can be connected to the network becomes stronger. As a result, only recognised devices should be allowed access to the network, while blocking unknown foreign devices.

Setup

RADA allows centralised control of devices based on MAC address. If the device is recognised as a company device, then network access can be granted, else the device will be blocked.

```
Select menu option (security/network/access): port
Select user ports (unit:port...,?): 1:1-1:24
Enter mode of operation (?) [rada]: rada
Enter the number of authorized addresses (1-233) [1]: 1
Enter Unauthorized Device action (?) [allowDefaultAccess]: block
Source of port VLAN membership and QoS profile
switch,RADIUS,?) [RADIUS]: RADIUS
```

7.3.3 Guest VLAN

Customers, while wanting to secure their network, would like the flexibility of allowing foreign devices limited network access. This is useful if they have a third party on site, requiring internet access.

Scenario

Customer wants to ensure that all devices are known, but does not want to have to install a client to use 802.1x user authentication. Customer also wants to allow internet access only, to unknown devices.

Setup

As a simple example, let's assume that the known devices will be placed on VLANs 2-9. VLAN 10 is a guest VLAN that only allows internet access. For this setup, the default or guest VLAN 10 should be applied to all end station ports, as the static VLAN (untagged if no tagging is done on the end clients).

Each end client port should be put into RADA mode. Ideally only one end client should be on each port, therefore only one authorized address should be allowed. The "Unauthorized Device action" should be to allow default access. This means that if the device is not known by the RADIUS server, the port is still opened to traffic.

The source of the VLAN membership and QoS profile should come from the RADIUS server. This means that when a known device is seen, VLANs 2-9 can be returned dynamically from the RADIUS server allowing the devices full network access.

```
Select menu option (security/network/access): port
Select user ports (unit:port...,?): 1:1-1:24
Enter mode of operation (?) [noSecurity]: rada
Enter the number of authorized addresses (1-233) [1]: 1
Enter Unauthorized Device action (?) [allowDefaultAccess]: allow
```

```
Source of port VLAN membership and QoS profile
(switch,RADIUS,?) [RADIUS]: RADIUS
```

If a device is recognized by the RADIUS server, the VLAN will be dynamically assigned to the port to allow correct network access. If the device is rejected by the RADIUS server, then the port will still allow network traffic from the device, but using the statically assigned VLAN, the guest VLAN, allowing access to limited network resources eg internet only.

7.3.4 Easing the roll out of 802.1x network security

Scenario

With 802.1x Network Login, each end-station client must have an 802.1x client installed. This can complicate the roll out as clients will not be able to connect until an 802.1x client has been installed. Also, switch ports would have to be configured to either operate in 802.1x or RADA, dependent on the edge device attached.

Solution

With RADA enabled on the 3Com Switch 4400, no client needs to be installed on the end station as it is based on the MAC address of the device. This means that RADA can allow centralized security management immediately, even for devices that do not support 802.1x. This will give network administrators immediate control over the devices on the network, while the addition of 802.1x security will further secure the devices and users on the network.

Setup

Ports can be set to operate with 802.1x or RADA simultaneously. The switch will try and authenticate the port using RADA and the devices MAC address, or using 802.1x. If either method results in authentication from the RADIUS server, the port will be authorized, and will allow network traffic.

```
Select menu option (security/network/access): port
Select user ports (unit:port...,?): 1:1-1:24
Enter mode of operation (?) [rada]: RadaOrSecureLogin
Enter the number of authorized addresses (1-233) [1]: 1
Enter Unauthorized Device action (?) [allowDefaultAccess]: block
Source of port VLAN membership and QoS profile
(switch,RADIUS,?) [RADIUS]: RADIUS
```

If both 802.1x and RADA result in authentication from the RADIUS server, then the 802.1x details will be used above the RADA details. If VLAN and QoS details are returned from the RADIUS server, then the 802.1x details will be used over the RADA details.

7.3.5 Ensure devices have the latest virus definitions (Intermediate VLAN)

Scenario

One of the biggest threats to a corporate network comes from the inside with worms and viruses. Companies want to ensure that the devices connected to their network have the latest virus definition to prevent the spread and infection of computer worms. The network administrator would like to isolate devices onto an intermediate VLAN for virus checking and windows updates before allowing the device onto the main network, regardless of who the user is

Setup

RADA can operate with 802.1x to provide this behavior. Each end station port should be put into RadaElseSecureLogin mode. This ensures initially that the device is authorized access to the network, and then that the user is allowed. If the device authorization fails, then the user authentication will also fail, as the device is not known to be safe.

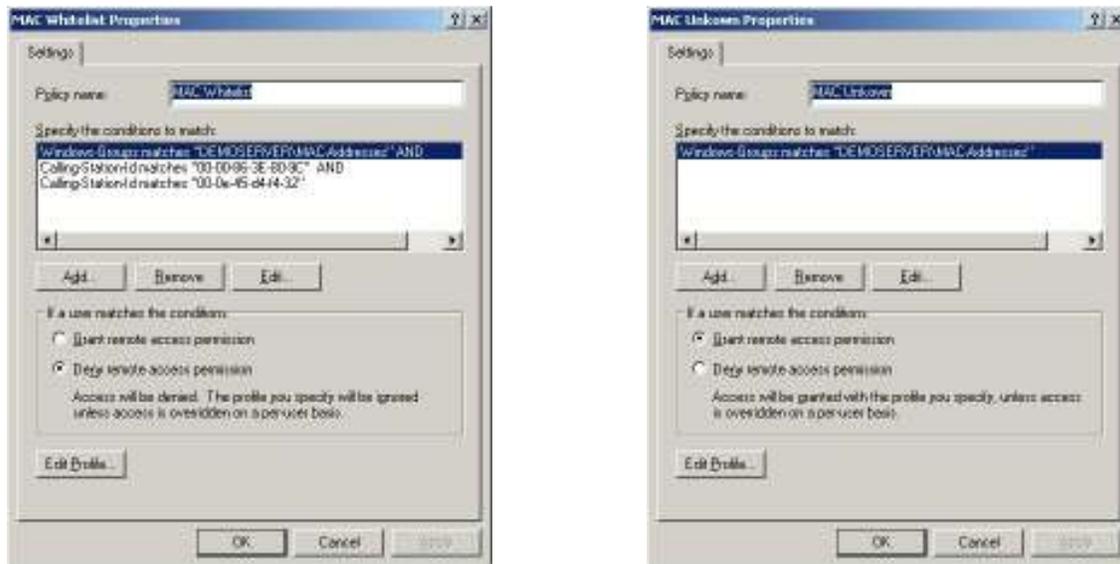
```
Select menu option (security/network/access): port
Select user ports (unit:port...,?): 1:1-1:24
Enter mode of operation (?) [rada]: RadaElseSecureLogin
Enter the number of authorized addresses (1-233) [1]: 1
Enter Unauthorized Device action (?) [allowDefaultAccess]: allow
Source of port VLAN membership and QoS profile
(switch,RADIUS,?) [RADIUS]: RADIUS
```

Note: 802.1x authentication will only be carried out if the MAC address is REJECTED/UNAUTHORIZED by the RADIUS server. Therefore if the "Unauthorized Device action" is "block", although the device is allowed on the network, all traffic to the device will be blocked until 802.1x authentication has taken place.

The more complex setup comes with the RADIUS server. The RADIUS server can be configured to operate using either **MAC Whitelist** or **MAC blacklist**.

MAC Whitelist

This is the more secure way to run a network. It assumes that devices are not allowed on the network until their MAC address has been added to the RADIUS server. Two Remote Access Policies (RAP) should be created to obtain this behaviour. The first, called "MAC whitelist" should recognise the allowed devices and DENY access to them. The second RAP should capture any unknown MAC addresses and GRANT network access to them. A dynamic VLAN can be returned to the ports of these devices to place them into their own subnet away from the rest of the network.

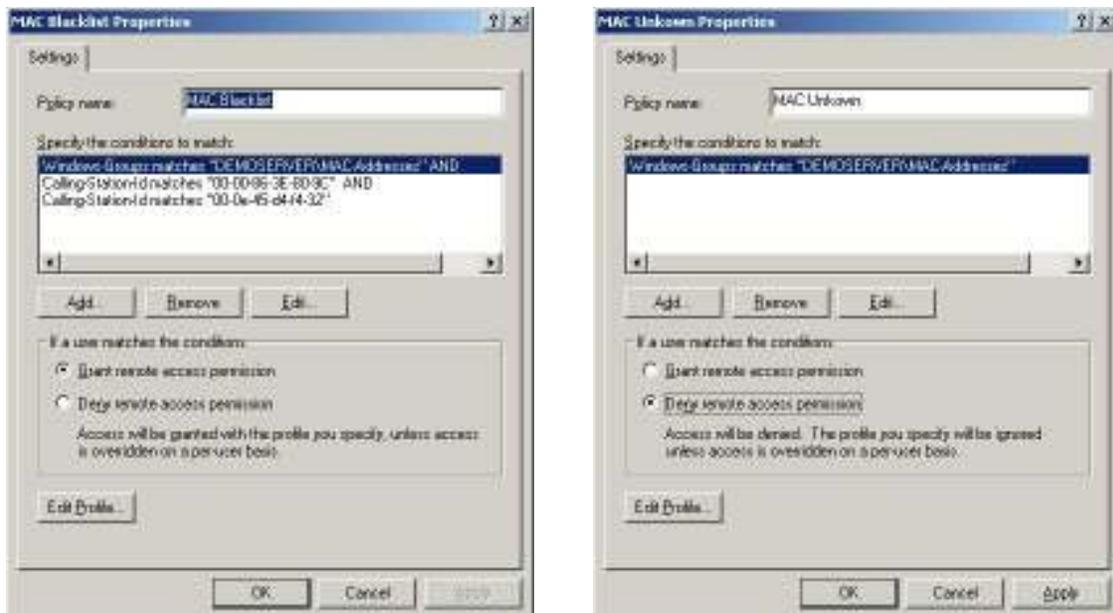


Note: The MAC Whitelist RAP should be tested before the MAC Unknown RAP.

MAC Blacklist

This is a more open method to use RADA and 802.1x but still providing centralised security to isolate rogue devices from the network. The idea of having a MAC Blacklist is to allow access to the network for all devices using RADA and 802.1x. However if a device is seen to be creating suspicious network traffic or is suspected to be infected with a virus, the device's MAC address can be added to a black list. This will either prevent access to the network completely or force the device onto a VLAN for cleaning.

The setup of the RADIUS server to achieve this behaviour is similar to the MAC whitelist, with 2 remote access policies required to do the RADA authentication:



Using either MAC whitelist, or MAC blacklist, once the device has been authorised using RADA, the port needs to be authorised using 802.1x to ensure that the user also has network access.

7.4 Check List Attributes Supported on 4400

The 4400 will send certain attributes to the Radius server to be checked. These are listed below:

Calling-Station ID

This is the MAC address of the device logging on. This allows the administrator to effectively lock a user to network device. This would mean that the user could not log onto the network from any other machine.

NAS-IP-Address

This is the IP address of the NAS (in our case the switch 4400). This is supported for logging purposes.

NAS-Port

This is the Physical Port of the device logging on. It returns the unit and port as an IfIndex. For Example Unit 2 port 1 would be returned from the 4400 as "201". This is supported for logging purposes.

NAS-Port-Type

This determines the type of media being used to join the network. It could be use to allow login through the Ethernet and stop them using the Wireless network.

Service-Type

Framed = network login and Administrative = Switch Login. This adds the capability to restrict a user to Just Switch Login.

7.5 Return List Attributes Supported on 4400

3Com-User-Access-Level (also supported on 4900/40x0)

This determines the Access level a user will have with Switch Login. This can be administrator, manager or monitor.

You may need to add the return list attributes to a dictionary file. Below is the info you need:

VENDOR	3Com	43		
ATTRIBUTE	3Com-User-Access-Level	1	Integer	3Com
VALUE	3Com-User-Access-Level	Monitor	1	
VALUE	3Com-User-Access-Level	Manager	2	
VALUE	3Com-User-Access-Level	Administrator	3	

Acct-interim-interval

This defines how often the switch will send Accounting Details back the Radius server. The accounting details include session information such as pack counts, error counts. These are Logged and can be used for charging mechanisms. The value is in seconds, minimum value is 60 seconds.

Session-Timeout

Forces the Termination action after a period of time defined in seconds. This is useful for security purposes, as it prevents machines being permanently logged in.

Termination Action

When Session-Timeout is reached this attribute defines the action that must be taken.

- Default the user will be forcibly logged out.
- RADIUS-Request, will require the user to re-authenticate, if authentication is successful all session data (such as packet counts) continues.

Auto VLAN

Uses three return list attributes to dynamically assign VLAN(s) to a port as the user logs in.

Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	← VLAN value
Tunnel-Type	VLAN	

Auto QoS

Uses the Filter-Id standard RADIUS attribute

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name

7.6 Problem Diagnosis

There are ways to check that auto VLAN and QoS are working correctly. To see what VLAN and QoS profile have been dynamically assigned to the port, use the **bridge port detail** from the cli. Looking under bridge VLAN detail or trafficmanagement QoS profile detail will **NOT** show the dynamically assigned VLAN and profile. These show the manually assigned VLAN and profile.

8 Configuring the 5500 Family switch

8.1 General RADIUS setup

The 5500family supports multiple RADIUS server profiles, which can then be assigned to a domain. This extra power and functionality makes it slightly more complex to set up and configure compared with the SuperStack 3 products.

This guide covers the recommended stages to go through to setup the 5500 for switch login.

8.1.1 Domain and RADIUS scheme creation

The 5500 family can have 1 or more domains created on it. A domain on the 5500 family is similar to a windows domain. By default, there is one domain created called "system". This uses the system radius server to validate users. The information about the local domain can be seen by typing "display domain"Eg:

```
<5500-EI>display domain
0 Domain = system
  State = Active
  Scheme = LOCAL
  Access-limit = Disable
  Domain User Template:
  Idle-cut = Disable
  Self-service = Disable
  Messenger Time = Disable
```

This system domain uses the system RADIUS server. The details of the system RADIUS server can be seen displaying radius settings:

```
[5500-EI]dis radius
-----
SchemeName =system                               Index=0
Type=extendedtype
Primary Auth IP =127.0.0.1      Port=1645   State=active
Primary Acct IP =127.0.0.1      Port=1646   State=active
Second Auth IP =0.0.0.0         Port=1812   State=block
Second Acct IP =0.0.0.0         Port=1813   State=block
Auth Server Encryption Key= 3com
Acct Server Encryption Key= 3com
Accounting method = required
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts =5
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min) =5
Username format =without-domain
Data flow unit =Byte
Packet unit =1
```

As you can see, the system RADIUS server currently uses itself to validate users.

It is not recommended that you change the system domain, as it could result in locking all users out of the switch. This could happen if you change the default RADIUS server to use an external RADIUS server, which is unavailable.

A new RADIUS scheme should be created as follows:

```
[5500-EI]radius scheme NewSchemeName
New Radius scheme
[5500-EI-radius-NewSchemeName]
```

Next, we need to add the attributes of the RADIUS server. This involves configuring the RADIUS server IP address and shared secret.

```
[5500-EI-radius-NewSchemeName]key authentication mysharedsecret
[5500-EI-radius-NewSchemeName]primary authentication 161.71.67.250
[5500-EI-radius-NewSchemeName]
```

The RADIUS profile will not become active unless an accounting server is also defined. If you don't have an accounting server, then the RADIUS scheme needs to have accounting set to "optional"

```
[5500-EI-radius-NewSchemeName]accounting optional
[5500-EI-radius-NewSchemeName]
```

Next, create a new domain as follows:

```
[5500-EI]domain Demo
New Domain added.
[5500-EI-isp-Demo]
```

Change the domain to use the new RADIUS server that you have configured:

```
[5500-EI-isp-demo]radius-scheme NewSchemeName
```

And that completes the configuration of the new radius server and associating it with a domain.

8.2 Network Login

To enable network login, it first has to be enabled globally, by issuing the command dot1x:

```
[5500-EI]dot1x
802.1x is enabled globally
```

Once enabled globally, it needs to be enabled on a per port basis. This can be done in one of 2 ways. If you just want to enable dot1x on one port, go into the interface of the port, and enabling dot1x on the port. Eg:

```
[5500-EI]interface ethernet 1/0/7
[5500-EI-Ethernet1/0/7]dot1x
 802.1x is enabled on port Ethernet1/0/7
[5500-EI-Ethernet1/0/7]
```

Alternatively, if you want to enable dot1x on more than 1 port, use the global dot1x command as follows:

```
[5500-EI]dot1x interface Ethernet 1/0/7 to Ethernet 1/0/12 Ethernet
1/0/14 to Ethernet 1/0/20
 802.1x is enabled on port Ethernet1/0/7 already
 802.1x is enabled on port Ethernet1/0/8
 802.1x is enabled on port Ethernet1/0/9
 802.1x is enabled on port Ethernet1/0/10
 802.1x is enabled on port Ethernet1/0/11
 802.1x is enabled on port Ethernet1/0/12
 802.1x is enabled on port Ethernet1/0/14
 802.1x is enabled on port Ethernet1/0/15
 802.1x is enabled on port Ethernet1/0/16
 802.1x is enabled on port Ethernet1/0/17
 802.1x is enabled on port Ethernet1/0/18
 802.1x is enabled on port Ethernet1/0/19
 802.1x is enabled on port Ethernet1/0/20
[5500-EI]
```

802.1x login is now enabled on the port. When a device with an 802.1x client connects to the port, the user will be challenged for a username and password. The username should be in the form "user@domain" where "domain" is the name of the domain that was created on the 5500. This will tell the 5500 which domain, and subsequently which RADIUS server the user is associated with.

By default, the username sent to the RADIUS server for verification will be in the form user@domain. To just send the username without the domain extension to the RADIUS server (ie. In the same form as the 4400). This is changed under the RADIUS scheme as follows:

```
[5500-EI-radius-NewSchemeName]user-name-format without-domain
```

8.3 Switch Login

The 5500 family supports Switch login, to allow multiple users access to the management interface of the 5500. The architecture of the 5500 is based on the same RADIUS attributes that are used on the SuperStack 3 family. This allows the same user database on the RADIUS server to be used between product families to manage the whole network.

Once the RADIUS server and domain have been set up, as covered in section 8.1, then switch login is enabled.

By default, when you use the username admin to login, you are actually logging in as "admin@local". If no domain is given, the "@local" is automatically added at the end of the username. This states the user is a member of the local domain, and as a result uses the local RADIUS server.

Based on the set up in section 8.1 to login using the external RADIUS server defined, you need to login as user@domain, eg joe@demo. This will try to log you into the demo domain, which uses the external, rather than the internal RADIUS server.

By default, the username sent to the RADIUS server for verification will be in the form user@domain. To just send the username without the domain extension to the RADIUS server (ie. In the same form as the 4400). This is changed under the RADIUS scheme as follows:

```
[5500-EI-radius-NewSchemeName]user-name-format without-domain
```

8.4 Radius Authenticated Device Access (RADA)

RADA is enabled on the 5500 in a similar way to user authentication. Follow section 8.1 to set up the domain and RADIUS server you want to use for RADA.

Next, enable RADA globally. This is done with the command "mac-authentication". Also, set mac-authentication to be a member of the domain that contains the RADIUS server that you wish to use:

```
[5500-EI]mac-authentication
MAC Authentication is enabled globally
[5500-EI]mac-authentication domain testnet
[5500-EI]
```

Next, as with dot1x, RADA needs to be enabled on each port using the "mac-authentication" command under the interface view. Eg:

```
[5500-EI]interface Ethernet 1/0/8
[5500-EI-Ethernet1/0/8]mac
[5500-EI-Ethernet1/0/8]mac-authentication
mac-auth is enabled on port Ethernet1/0/8
[5500-EI-Ethernet1/0/8]
```

Note that dot1x and mac-authentication cannot both be enabled on a port at the same time.

When a device connects to the port, the MAC address is sent to the RADIUS server. The MAC address is sent in the form XXXXXXXXXXXX. No domain information is sent with the MAC

address to the RADIUS server. The MAC address format is different to the 4400, which is XX-XX-XX-XX-XX-XX.

8.5 Return List Attributes Supported on 5500

3Com-User-Access-Level

This determines the Access level a user will have with Switch Login. This can be administrator, manager, monitor or visitor. This is the same as for SuperStack 3, with the visitor level added.

You may need to add the return list attributes to a dictionary file. Below is the info you need:

VENDOR	3Com	43		
ATTRIBUTE	3Com-User-Access-Level	1	Integer	3Com
VALUE	3Com-User-Access-Level	Visit	0	
VALUE	3Com-User-Access-Level	Monitor	1	
VALUE	3Com-User-Access-Level	Manager	2	
VALUE	3Com-User-Access-Level	Administrator	3	

Auto VLAN

Uses three return list attributes to dynamically assign VLAN(s) to a port as the user logs in.

Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	← VLAN value
Tunnel-Type	VLAN	

Note: Before the VLAN is correctly received by the 5500, you need to execute the following command on the 5500 to use standard private-group-ID:

```
[5500-EI] private-group-id mode standard
```

Auto QoS

Uses the Filter-Id standard RADIUS attribute

For Auto QoS	Return String	Comment
Filter-id	student	QoS Profile name

8.6 Problem Diagnosis

The 5500 5500 family provides good debug of radius. Terminal debugging can be enabled with the command:

```
<5500-EI> Terminal debugging
```

Once enabled, different debug traces can be enabled to the terminal. Eg to turn on radius debugging, execute the command:

```
<5500-EI> debugging radius packet
```