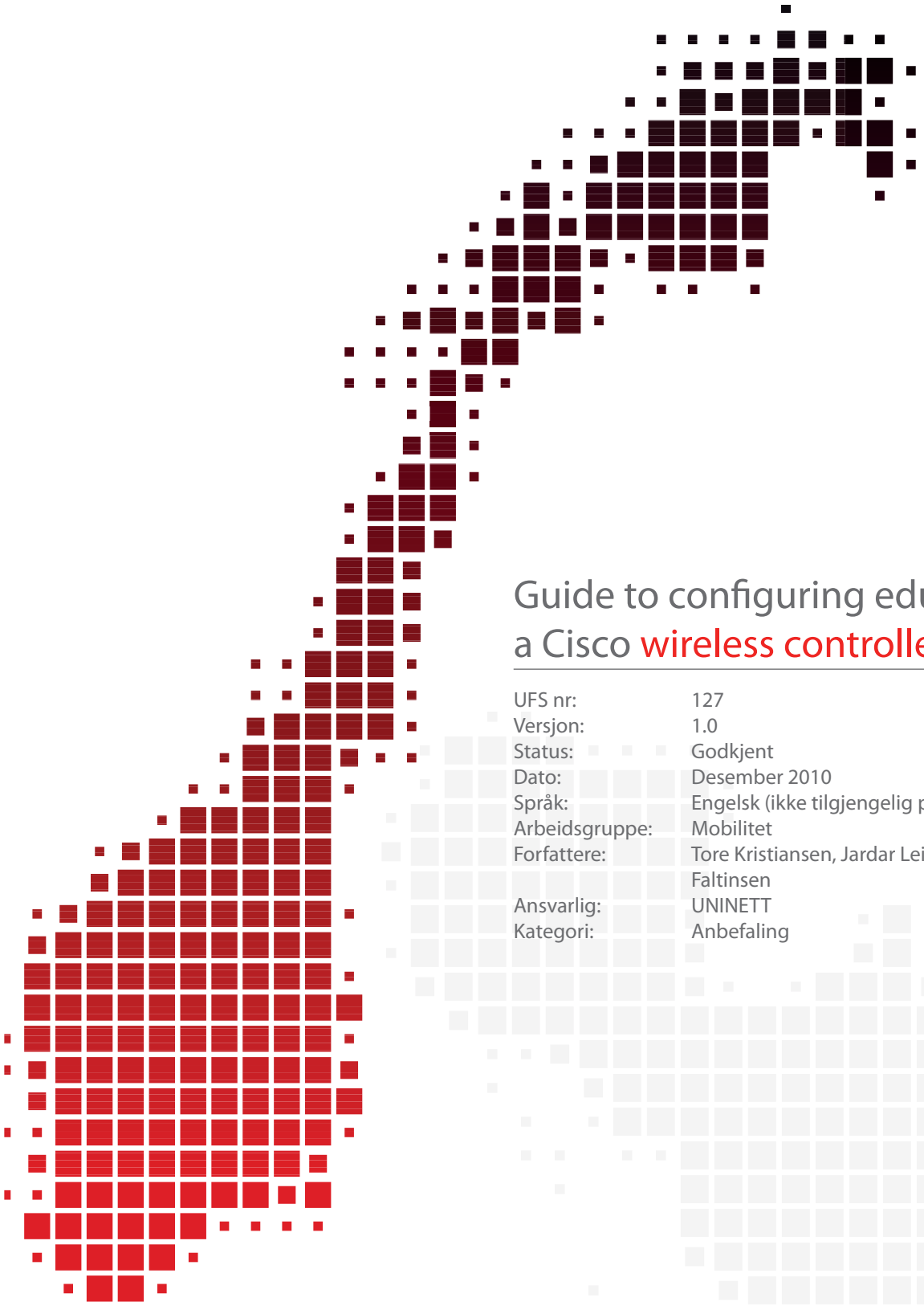
UNINETT Fagspesifikasjon



Guide to configuring eduroam using a Cisco wireless controller

UFS nr:	127
Versjon:	1.0
Status:	Godkjent
Dato:	Desember 2010
Språk:	Engelsk (ikke tilgjengelig på norsk)
Arbeidsgruppe:	Mobilitet
Forfattere:	Tore Kristiansen, Jardar Leira, Vidar Faltinsen
Ansvarlig:	UNINETT
Kategori:	Anbefaling

Document No: GN3-NA3-T4-UFS127
Version / date: December 2010
Original language: Norwegian
Original title: "Veiledning for eduroam oppsett med Cisco trådløs controller"
Original version / date: September 2010
Contact: campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT led working group on mobility as part of a joint-venture project within the HE sector in Norway. Stian Lysberg has contributed to appendix B.

The [third revision review and the] translation of this report has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

UFS127 is a UNINETT Technical Specification prepared by UNINETT in co-operation with the HE sector's work group for mobility, gc-mobilitet@uninett.no. The Technical Specification has received final approval after a four-week open consultation period with the HE sector.

UFS127 is a guide to configuring eduroam, including IEEE 802.1X, in a Cisco controller-based environment, i.e. a configuration based on one or more Cisco controllers which govern the traffic to and from Cisco lightweight access points (LAP). The guide applies both to Cisco 5500 Series and 4400 Series controllers (WLC). Any differences in configuration between the 5500 Series and the 4400 Series are specified. In principle the guide will also apply to wireless systems provided by suppliers other than Cisco.

The recommendation provides advice for network planning, the configuration of RADIUS, the configuration of a controller, radio planning and the physical installation of access points. The recommendation also includes a number of attachments, a "cookbook" for configuration based on autonomous access points, configuration of Microsoft RADIUS servers and configuration of FreeRADIUS.

Introduction

This document is a guide to configuring eduroam in a Cisco controller-based environment, i.e. a configuration based on one or more Cisco controllers which govern the traffic to and from Cisco lightweight access points (LAP). The guide applies both to Cisco 5500 Series and 4400 Series controllers (WLC). Any differences in configuration between the 5500 Series and the 4400 Series are specified.

In principle the guide will also apply to wireless systems provided by suppliers other than Cisco.

For information on the configuration and operation of IEEE 802.1X, see UFS112 [1]. The description in this case is based on the use of autonomous access points, but the principle will be the same. In a controller system it is the controller which acts on behalf of the access point, including issues regarding the RADIUS authentication of users.

When configuring a controller-based wireless network, there are many things which need to be planned and performed in the correct order. The main points are dealt with in the following chapters:

1. Network planning
2. Configuring RADIUS
3. Configuring a controller
4. Radio planning
5. Physical installation of access points.

As an alternative to a controller-based system, a configuration may be chosen which is based on autonomous access points. However, in the interests of security, this is *not* recommended. A configuration using autonomous access points requires the use of a dot1q trunk with all the necessary VLAN connections to an access point. Since access points can be located in open areas with round-the-clock access, with a little knowledge a user may be able to replace an access point with a PC which in turn would be able to access VLANs that it should not be able to access, or act as an intermediary in a man-in-the-middle attack. Guidelines for how to configure eduroam without the use of a controller are nevertheless provided in Attachment A.

1 Network planning

1.1 Necessary components

The number of access points and the type of controller(s) may be evaluated depending on the size and layout of the premises. Refer to Chapter 4 *Radio planning*, for guidelines for estimating the number of access points. Remember to allow for estimated growth in the coming years, bearing in mind the radio-related limitations in effect. The type of controller should be considered on the basis of the estimated total number of access points. For larger installations, the latest 5508 controller (with eight GE ports) is currently recommended. This is capable of handling up to 12, 25, 50, 100, 250 or 500 access points, depending on which licence one purchases. It is easy to expand the number of licences later. The 4400 Series includes two different products: 4402 (with two GE ports) and 4404 (with four GE ports). In addition there is the WiSM module for the Catalyst 6500. The WiSM consists of two 4404 controllers each with four rear-facing GE ports, each of which can handle up to 150 access points.

In larger installations one should consider using more controllers, for the sake of fault tolerance. Each access point may be configured to use a primary and a secondary controller (and a tertiary one if desired). Note also that UNINETT has a WiSM module in its spare parts storeroom which may be sent out in the event of serious operational problems.

If one only has a single controller, WCS (Wireless Control System) management software is strictly speaking *not* necessary. It is perfectly possible to manage with a web-based management interface directly to the controller. However, if several controllers are used, WCS is recommended.

For the mapping and monitoring of all the Wi-Fi units in a wireless network, to produce plan drawings and so on, a dedicated hardware product, MSE (Mobility Service Engine) should be obtained. MSE can handle up to 18,000 Wi-Fi units (clients and access points) and can be integrated with WCS. An option is an LA (Location Appliance), which can handle up to 2500 Wi-Fi units (and can also be integrated with WCS, up to version 6.0).

1.2 IP addresses and subnets

It is necessary to plan which IP addresses and VLANs are to be used for the various purposes:

- The Wireless LAN Controller (WLC) must have administrative IP addresses
- Any Wireless Control System (WCS), Mobility Service Engine (MSE) and/or Location Appliance (LA) must have IP addresses
- The access points must have management IP addresses which should be separated on a dedicated subnet.
- Users must have their own subnet or user class. The controller must also have one IP address per user subnet.

Figure 1 provides a summary. Each network cloud represents an IP subnet with the exception of the eduroam hierarchy which for the sake of simplicity is given its own network cloud. The arrows between the clouds indicate the necessary traffic pattern and form the basis for deciding which ports must be opened in package filters (if the units are located in different subnets). One must select a configuration in which, for example, the operating network and services are in the same subnet. In any event it is recommended that the access points be located in a dedicated subnet, since these network points are exposed in open premises and risk being tapped. The controller(s) (WLC(s)) should also be separated from the service or server network, but may for example be located in a general management network for switches.

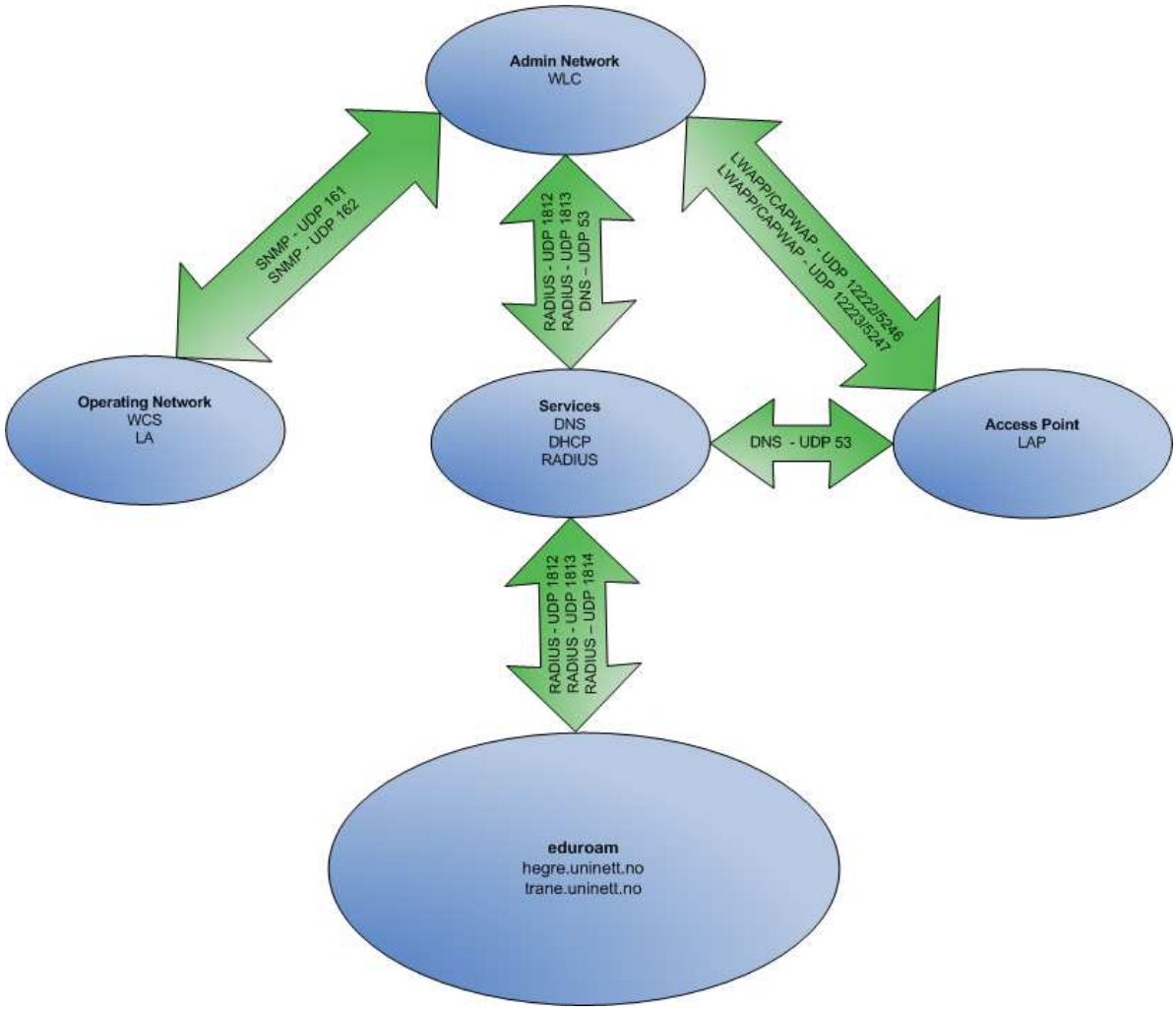


Figure 1: Proposed subnets and necessary traffic pattern

1.3 The wireless controller (WLC)

The 5500 controller has one administrative IP address (Management), while the 4400 controller requires two administrative IP addresses (Management and AP Manager). A WiSM module consists of two 4400 controllers and consequently requires four administrative IP addresses. The Management IP address is the one which is used for general administration of the controller and is the contact address to and from other systems such as WCS and RADIUS server. The Management address is also used for communication with the access points, but here the 4400 controller also has the AP Manager address which is used in communication with the access points after the initial contact has been

established by means of the Management address. The Management and AP Manager addresses should be located in the same subnet.

It does not matter which IP addresses in a subnet are used for this purpose, but the addresses should be located in a subnet which is protected against general access, designated “Admin Network” in Figure 1. Strict data filter rules must apply to Admin Network, with access only for specific purposes.

The controller must also be represented in all the VLANs it is to serve via the wireless network. Traditionally, the first network address in the subnet is used as the router address. It does not matter which address is used for the controller, but as a matter of form we recommend using an address located immediately after the router.

```
Management IP address: In a restricted administration network
AP Manager IP address : In the same restricted administration network
  NB: For 5500 series controllers, it is not necessary to configure an AP Manager
  address. The Management interface acts as an AP Manager interface by
  default and the APs will associate themselves with this interface.

WCS’s address in the service VLAN
- Near the beginning of the address space in the relevant VLAN
Filter:
 - If CAPWAP(*): UDP 5246 and UDP 5247 to/from access point VLAN
 - If LWAPP(*): UDP 12222 and UDP 12223 to/from access point VLAN
 In addition:
 - UDP 1812 to RADIUS
 - UDP 1813 to RADIUS
 - UDP 161 and 162 to/from WCS and any other management tools
 - TCP 443 or 80, 22 or 23 from units for administration

(*) Beginning with controller software version 5.2, CAPWAP is used instead
    of LWAPP for communication between access pointaccess points and controller.
```

1.4 The WCS, MSE and LA administration software

WCS runs under either Windows Server or Red Hat Linux. This can be on a virtual server. MSE and LA are separate hardware platforms which can be located on any subnet as long as they can communicate with WLC using SNMP, but access to these applications must, for security reasons, be restricted. Ideally they should be located on a subnet restricted to administrative use. This is represented by the “Operational Network” in Figure 1.

```
WCS address: In a restricted administration network
MSE/LA address: In a restricted administration network
Filter:
 - UDP 161 and 162 to/from WCS
```

1.5 Access points

The network cables connected to access points are often exposed in open areas and can represent a security risk. An unauthorised person tapping into such a cable can potentially gain access to subnets to which he or she should not have access and this may also enable man-in-the-middle attacks on users. The network should therefore be organised in such a way that network access in practice is unusable for anybody tapping into the cable. Here a controller-based system has a major advantage over autonomous access points. In a controller-based system it is *not* necessary to configure a dot1q trunk into the access point. By locating the access points in a separate, dedicated subnet and strictly restricting access to this subnet, any attempt to tap into the system will be rendered futile. All an access point needs to communicate with is DNS (to discover the controller) and subsequently communicate with the controller's management address(es) via the UDP ports. All other ports should be blocked.

It is recommended that DHCP be used to assign IP addresses to the access points. The assignment of names to the access points is done within the controller system, either in the controller itself or using WCS once the access point has been connected (See Section 1.5.1).

One may choose to limit the use of official IPv4 addresses by using RFC1918 addresses for all the access points, but the organisation must then route this network internally so that the access points can reach the controller and, if necessary, the DNS. Note that such a configuration will not be possible in cases where the traffic between controller and access point is routed by UNINETT, i.e. over the UNINETT backbone.

In the future there may be an option to use IPv6 addresses in the management of access points, but this is not currently supported.

1.5.1 The access point connection process

Communication between an access point and a controller is by means of a special protocol. Older controller software, i.e. v 5.1 and older, used the LWAPP protocol. Since the introduction of version 5.2, the standard-based CAPWAP protocol (RFC 5415) has been used. CAPWAP is based on Layer 3 (IP) communication between access point and controller. Layer 3 communication is also preferable for LWAPP, although Layer 2 is optional for 4400 Series controllers. Given our recommendation to separate access points and controllers in different subnets, we recommend Layer 3 mode in any case.

As mentioned previously, the 5500 Series controller has only one Management address, which is used for all communication with access points. In the case of the 4400 Series controller, the situation is more complex, since both the controller's Management address and its AP Manager address are used by the access points. In connection with the initial association the Management address will be used. Once the configuration has been downloaded to the access point (and any new firmware), it will begin to use the AP Manager address instead.

The methods supported by an access point for the initial *discovery* of a controller vary somewhat depending on what model of access point is in use. However, what they all have in common is that they support three alternatives, and in this case we recommend Method 3 – *DNS discovery*:

1) Saved IP address. The access point uses the IP address already saved in the access point. This means that the access point must previously have saved this information when it has been connected to the controller or that the information must have been entered manually (via a serial cable).

2) DHCP server discovery. By using DHCP option 43 for the subnet, the address of the controller can be provided simultaneously with other information via DHCP. Further information regarding how this is done on different DHCP servers can be found at:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml

3) DNS discovery. The access point uses the domain name (provided by DHCP) in conjunction with the unit name “CISCO-CAPWAP-CONTROLLER” or “CISCO-LWAPP-CONTROLLER” and then looks this up in the DNS. For example, the domain name “uninett.no”, in conjunction with “CISCO-CAPWAP-CONTROLLER” gives “CISCO-CAPWAP-CONTROLLER.uninett.no”. Of course, this requires the controller to be first registered in the DNS. It is recommended that *both* the “CISCO-CAPWAP-CONTROLLER” and “CISCO-LWAPP-CONTROLLER” names be entered in the DNS, since older access points will not recognise CAPWAP in connection with initial association (until they have been upgraded).

   For ISC DCHP, enter:

```
option domain-name "yourdomain.no";
```

   ...in the shared network specification for the subnet or globally. Cisco access points do not support an option containing several domain specifications, such as

```
option domain-name "uninett.no win.uninett.no home.uninett.no";
```

```
Configure a VLAN with an IPv4 subnet large enough for all access pointaccess
points with realistic growth potential. Configure DHCP support for this subnet.

Use Layer 3 communication between the access points and the controller.

All ingoing and outgoing traffic in the access point subnet shall be blocked
except:
 - If CAPWAP: UDP 5246 and UDP 5247 to/from access point VLAN
 - If LWAPP: UDP 12222 and UDP 12223 to/from access point VLAN
 - DNS – UDP 53 (may be restricted to relevant DNS servers)
```

1.6 Users

Using RADIUS and dynamic VLAN assignment (AAA override), it is possible to grant different groups access to different subnets or VLANs using the *same* SSID (for example “eduroam”). It is desirable to separate users into different subnets to be able to use filters to regulate the level of access of external and internal services.

As a rule, a typical educational institution will have at least the following user groups:

- Employees
- Students
- Guests

One may also wish to create a distinction between different types of employees, students and guests.

The configuration of FreeRADIUS in connection with dynamic VLAN assignment is described in detail in Chapter 9 of UFS112 [1].

The same VLAN should *not* be used for wireless access as for wired network access, primarily for security reasons. It may be difficult to trace both faults and breaches of ICT rules and security if one is

unable to distinguish between IP addresses used by wired clients, which are often anonymous, and wireless clients. It is also desirable to reduce broadcast traffic to a minimum so that this does not affect the capacity of the wireless connections. Restricting the subnet to include only wireless connections is a good way to achieve this. In addition it is possible to control what forms of traffic are to be permitted, for example by not distributing multicast traffic.

A VLAN, which is defined in a virtual interface in the controller, can be used simultaneously in several SSIDs. In other words, a VLAN for guests may be used simultaneously both for eduroam guests and for a guest network with other types of authentication. The eduroam guests will still benefit from the encryption in the wireless network provided by WPA, but both will have to comply with the filtering rules for the network which are defined in the router.

```
- Several VLANs with subnet large enough to serve the relevant user group
- Address early in the address space for WLC for each VLAN which is to be
  served
- Filter according to security requirements.
```

2 Configuring RADIUS

Experience shows that it often takes a great deal of time to achieve the proper dialogue between a RADIUS server and the relevant user database. As regards RADIUS and user databases, there are a number of alternatives to choose from. If the RADIUS server is also to be used for other purposes (such as VPN), this in itself can present a challenge. We recommend a dedicated RADIUS server for wireless networks (remember that for some systems, it is easy to configure several RADIUS servers on the same server, communicating through different ports).

RADIUS servers frequently used in the HE sector are:

- FreeRADIUS 1.x
- FreeRADIUS 2.x
- Microsoft IAS (Windows 2003 server)
- Microsoft NPS (Windows 2008 server)

User databases frequently used in the HE sector are:

- Microsoft Active Directory (AD)
- OpenLDAP
- Novell eDirectory
- Cerebrum

The organisation of the user database itself can vary from institution to institution: there are, for example, many ways of organising an LDAP tree. In other words, it is difficult to provide a unique explanation of how one should make connections between RADIUS and a user database.
For details of configuring FreeRADIUS 1.x, see UFS112 [1]. The configuration of FreeRADIUS 2.x has changed somewhat, but UFS112 will still be of assistance. In addition, Attachment A2 [2] of the “eduroam cookbook” is recommended. A guide to the configuration of Microsoft IAS and NPS is provided in Attachment B.
A common requirement for all installations is a server certificate for the RADIUS server. The server certificate is used by the wireless client to verify the authenticity of the RADIUS server before 802.1X

authentication can be completed. Here one can choose between using self-generated or purchased certificates.

Self-generated certificates is the most secure option, but entail significant extra work, since it is necessary to perform a separate certificate installation in every single client which is to be granted access to the wireless network. The way in which you save your own root certificate and your own certificate hierarchy is described in Chapter 4 of UFS112 [1].

A simpler and "secure enough" way to achieve this is to make use of UNINETT's server certificate service, SCS (http://www.uninett.no/scs). UNINETT is actually a member of TERENA's TCS (*TERENA Certificate Service*) project and can supply user certificates to our members who belong to Comodo UserTrust. Most operating systems are accompanied by a client certificate with a public key from Comodo UserTrust. A detailed "cookbook" for ordering a UNINETT SCS certificate is available at http://forskningsnett.uninett.no/scs/hvordan.html. When you have received a certificate it must be installed in your RADIUS server. See Attachment C for installation of a certificate for FreeRADIUS 2.x.

Once IEEE 802.1X is functioning internally, the national connection to eduroam can be configured. In general terms this involves rerouting the requests from users with unrecognised realms and accepting requests from one's own users who are visiting other institutions. For more information about eduroam, see Chapter 10 of UFS112 [1] and the "eduroam cookbook" [2].

```
- Obtain server certificate for RADIUS
- Configure RADIUS server for the user database
- Connect RADIUS server to eduroam (top level in Norway is handled by
  hegre.uninett.no and trane.uninett.no)
- Filter:
    o RADIUS Authentication UDP 1812 to/from hegre.uninett.no and
      trane.uninett.no
    o RADIUS Accounting UDP 1813 to/from hegre.uninett.no and
      trane.uninett.no
    o RADIUS Proxy UDP 1814 to/from hegre.uninett.no and
      trane.uninett.no
```

3 Configuring a controller

Once one has completed network planning and has one's IP addresses ready (cf. Chapter 1), the controller can be configured. It is even simpler if one also first has the details of the RADIUS server at hand (Chapter 2).

This guide applies only to basic functionality and for systems with a *single* controller. If the system contains several controllers there is more to take into account (distribution of access points, zones/groups, and so on), but in principle this guide will also serve as a basis for such a configuration.

Strictly speaking, all configuration work can be performed via the command line (CLI) but the controllers do not use Cisco's IOS, and Cisco recommends the use of the web interface (if necessary via WCS) for most of the configuration.

The configuration is performed in the following steps:

A. Use of serial cable / console for the initial configuration using the Configuration Wizard in the CLI

B. Use of service port / management with a web browser (HTTP) for further configuration.
   1. Create virtual interfaces
   2. Define RADIUS servers
   3. Create a WLAN
   4. Connect access points.

Note: Some versions of the WLC/WCS web server works best with Internet Explorer. In other words one might find that certain options unfortunately "disappear" or are not correctly displayed in other web browsers.

3.1 Initial configuration on a console

Initially a number of questions are asked in the Configuration Wizard when you turn on the controller for the first time. When these have been answered, the configuration should resemble the following example:

```
Welcome to the Cisco Wizard Configuration Tool
 Use the '-' character to backup
 System Name [Cisco_34:21:11]: WLC
 Enter Administrative User Name (24 characters max): admin
 Enter Administrative Password (24 characters max): *****
 Service Interface IP Address Configuration [none][DHCP]: none
 Enable Link Aggregation (LAG) [yes][NO]: No
 Management Interface IP Address: 192.168.0.10
```

```
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.0.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 192.168.0.20
AP Transport Mode [layer2][LAYER3]: LAYER3
AP Manager Interface IP Address: 192.168.0.11
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.0.20):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Group
Network Name (SSID): TEMP
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Enter Country Code (enter 'help' for a list of countries) [US]: NO
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
Configuration saved!
Resetting system with new configuration...
```

Note**:** As mentioned above, the AP Manager Interface must not be configured in the 5500 controller. Here the Management Interface acts as an AP Manager Interface.

The following is an explanation of the individual configuration parameters:

System Name: Choose a suitable name using your own name convention, for example “uninett-4402-50-wlc”.

Enter Administrative User Name: e.g. “admin”

Enter Administrative Password: use something appropriate

Service Interface IP Address Configuration [none][DHCP**]: none**

The “service interface” is an “out-of-band” address which can be used to manage the control by way of IP. This is all it is used for and often it is not used at all. Since a gateway cannot be specified for this address, it cannot be routed out of the subnet (out-of-band address). It is a good backup address in case the Management address cannot be reached. It is also useful during the initial configuration after the CLI configuration has been completed. One can connect this port to the administration network or provide an RFC1918 address and connect directly to the port using a PC.
If “none” is selected, the address is set to 10.0.0.1/255.255.255.0. It may be changed later via the web interface.

Enable Link Aggregation (LAG) [yes][NO]: No

In the case of small installations, there is no need to use more than one SFP port. In that case, enter “no”. For larger installations you should bundle several SFP ports using link aggregation. In that case, enter “yes”.

Management Interface IP Address:

This is the address which will later be used to administer the controller via HTTP, HTTPS, Telnet, SSH and/or SNMP. WCS uses SNMP to communicate with the controller at this address. The address will also be used by the access points to discover their controller. The address should therefore be registered in the DNS as “CISCO-CAPWAP-CONTROLLER.yourdomain.no” and “CISCO-LWAPP-CONTROLLER.yourdomain.no”.

It should be possible to route this address internally and preferably also externally if, for example, one needs external support. Strict filters should be in place to prevent unwanted units from contacting it, cf. Chapter 1. The access points must obtain access only via UDP on ports 5246/5247 (CAPWAP) or 12222/12223 (LWAPP). In addition, the RADIUS server must have access to this address on UDP ports 1812 and 1813. If one has WCS, MSE and/or LA and they are located in another network, they must also be able to communicate with the WLC's address using SNMP.

Management Interface Netmask: Self-explanatory

Management Interface Default Router: Self-explanatory

Management Interface VLAN Identifier (0 = untagged): ID of the VLAN in which the Management address is located.

Management Interface Port Num [1 to 4]: For a stand-alone controller, an SFP port must be selected. This is normally Port 1.

Management Interface DHCP Server IP Address: The IP address of the DHCP server used by the system.

AP Transport Mode [layer2][LAYER3]: LAYER3

This determines which layer the LWAPP/CAPWAP traffic is to be located in. If this question is asked, you must choose LAYER3. This is compulsory for WiSM. It is also compulsory for software version 5.2 and newer in autonomous controllers.

AP Manager Interface IP Address: (not applicable to the WLC 5500 Series)

When using a 4400 Series controller, this is the address with which the access points communicate after they have established contact with the controller via the Management address. It should be located in the same subnet as the Management address. Since only the access points need to communicate with this address, the filter only needs to be opened for UDP ports 12222/12223 and 5246/5247 from the subnet in which the access points are located.

AP Manager Interface DHCP Server: As for the Management address.

Virtual Gateway IP Address: 1.1.1.1

This is used if Layer 3 security is being used (e.g. in a web portal) or if there are several controllers (mobility managers). It is a virtual address accessible from, for example, the clients which are to access a web page requiring login. The default setting is "1.1.1.1".

Mobility/RF Group Name:

Create a name which describes the wireless system in use. The name should be short. For example, the organisation's name, such as "uninett", "ntnu" or something similar, could be used.
Almost all the remaining options can be filled in at random, since they will be corrected anyway through the web interface.

One exception:

Enter Country Code: NO (to obtain the correct radio frequencies)

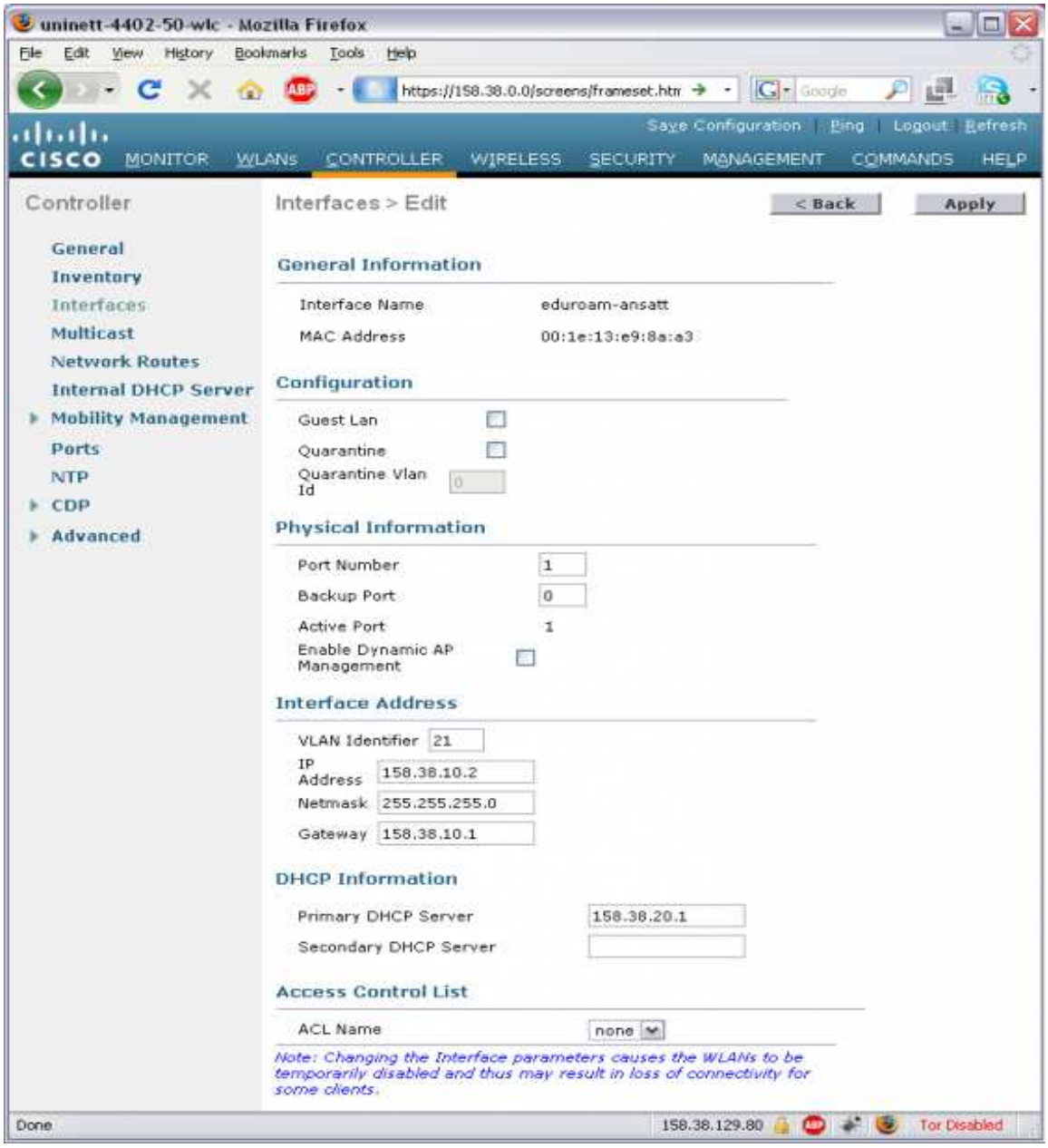
3.2 Further configuration via web browser

Once the controller has restarted, it will be ready for configuration via the web browser in communication with the Management address or service interface.

3.2.1 Creating a virtual interface

Path: Controller → Interfaces

A virtual interface must be created for every VLAN one wishes to make available to users. As a rule this means a minimum of one for employees, one for students and one for guests. These are VLANs which must naturally be located in the trunk of the controller (authorised VLANs in the trunk are regulated by the switch to which the SFP port(s) in the controller are connected).

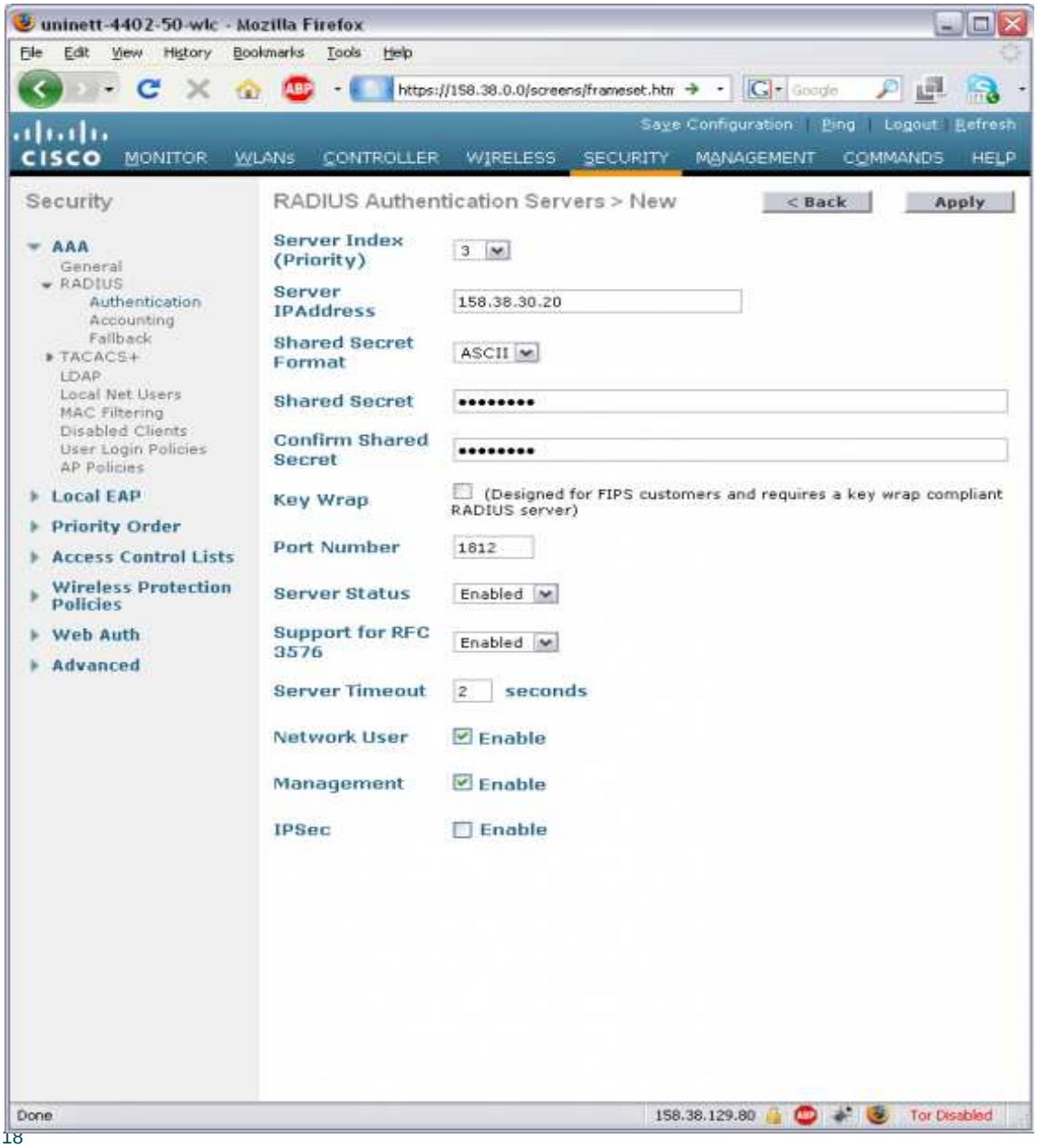


The controller must have its own IP address in each VLAN which it is to serve. Strictly speaking, it does not matter which IP address this is in the subnet as long as there is no conflict with another unit, but it is a good rule to use the first available after the router's address.
The screen shot shows a typical configuration for such a virtual interface.

3.2.2 Defining a RADIUS server

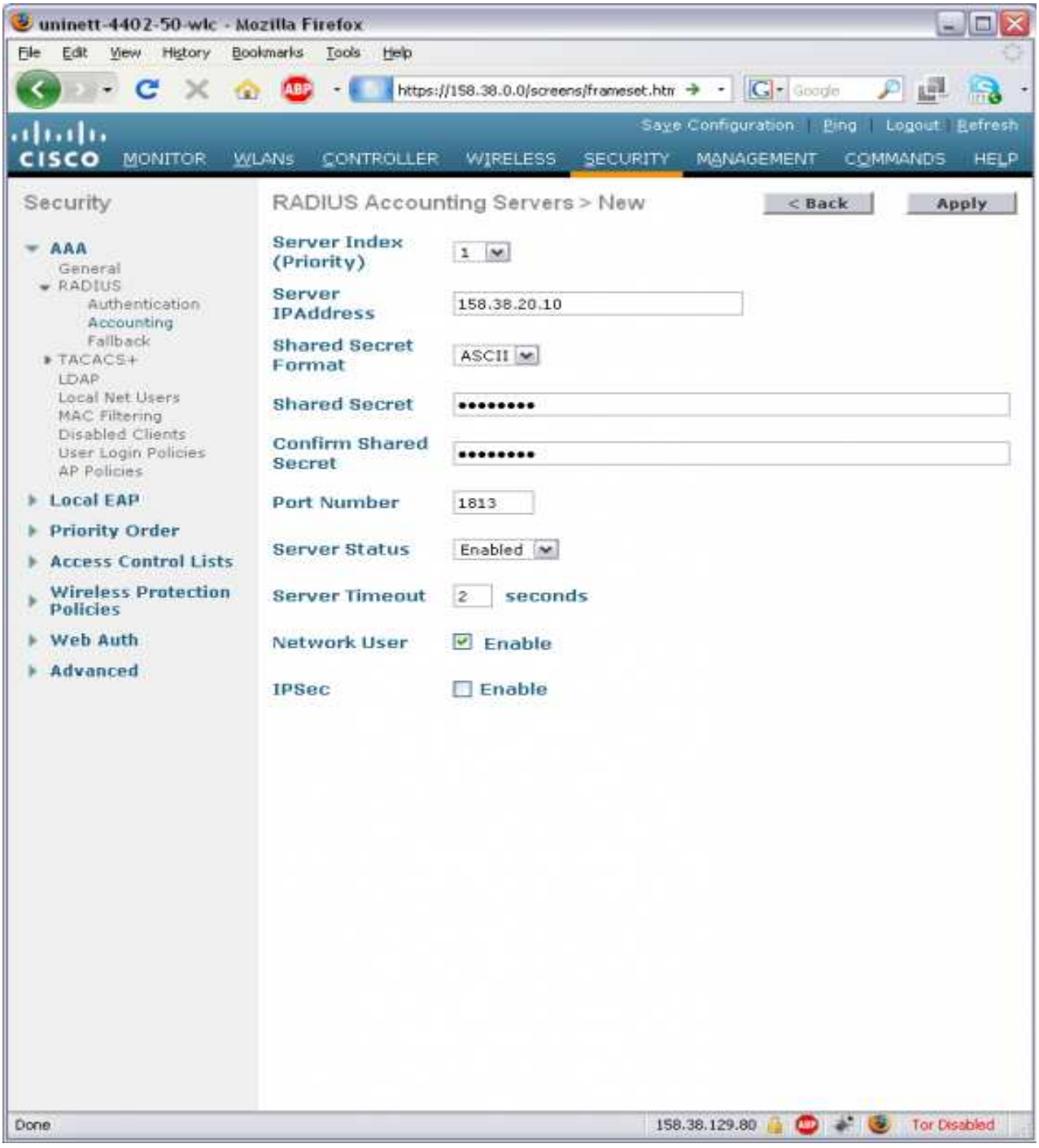
Path: Security → RADIUS → Authentication

It is advisable to ensure that the RADIUS servers are in place before beginning to define a WLAN. Several RADIUS servers may be included, which are of course the organisation's own servers. A shared secret should be established which differs from that for eduroam's national servers. The port number for authentication is usually UDP 1812.



Path: Security → RADIUS → Accounting

Accounting should also be configured and is required by eduroam. This is done in exactly the same way as for Authentication, but normally uses UDP port 1813.

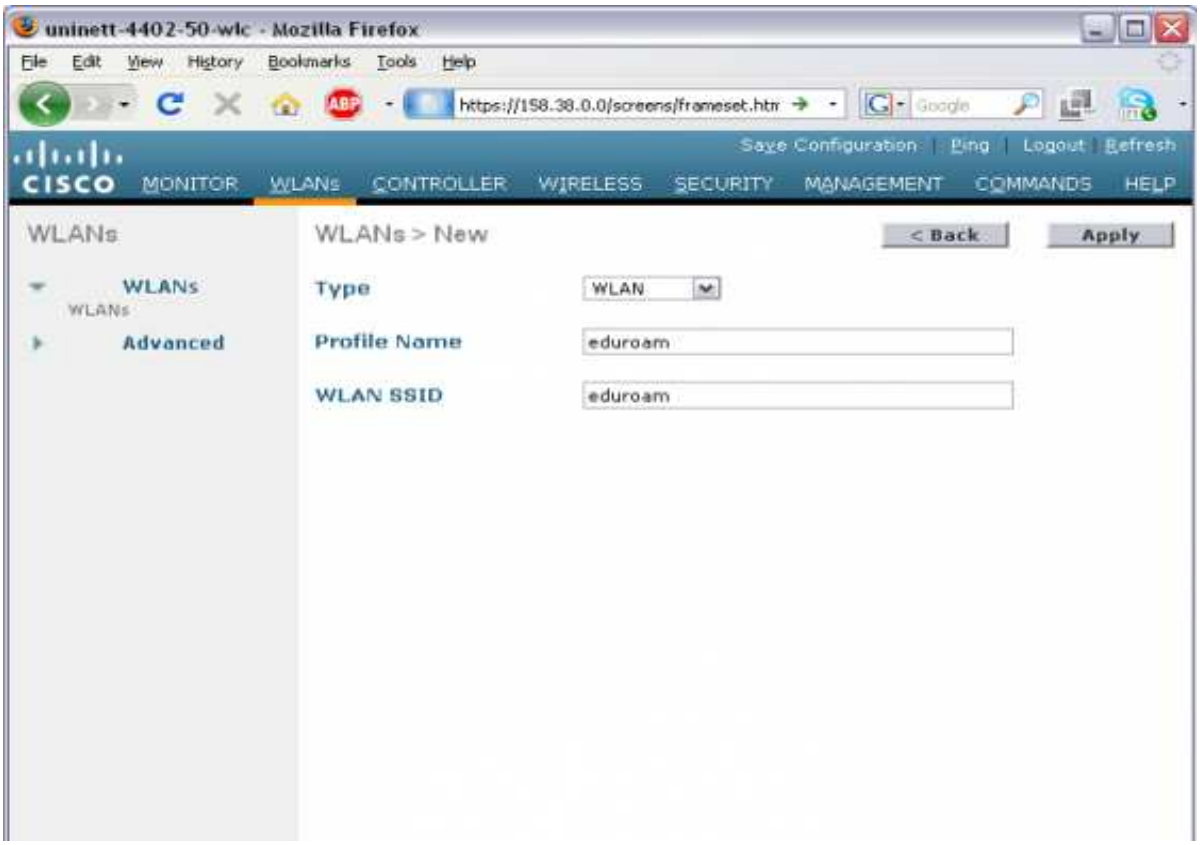


3.2.3 Creating a WLAN (SSID)

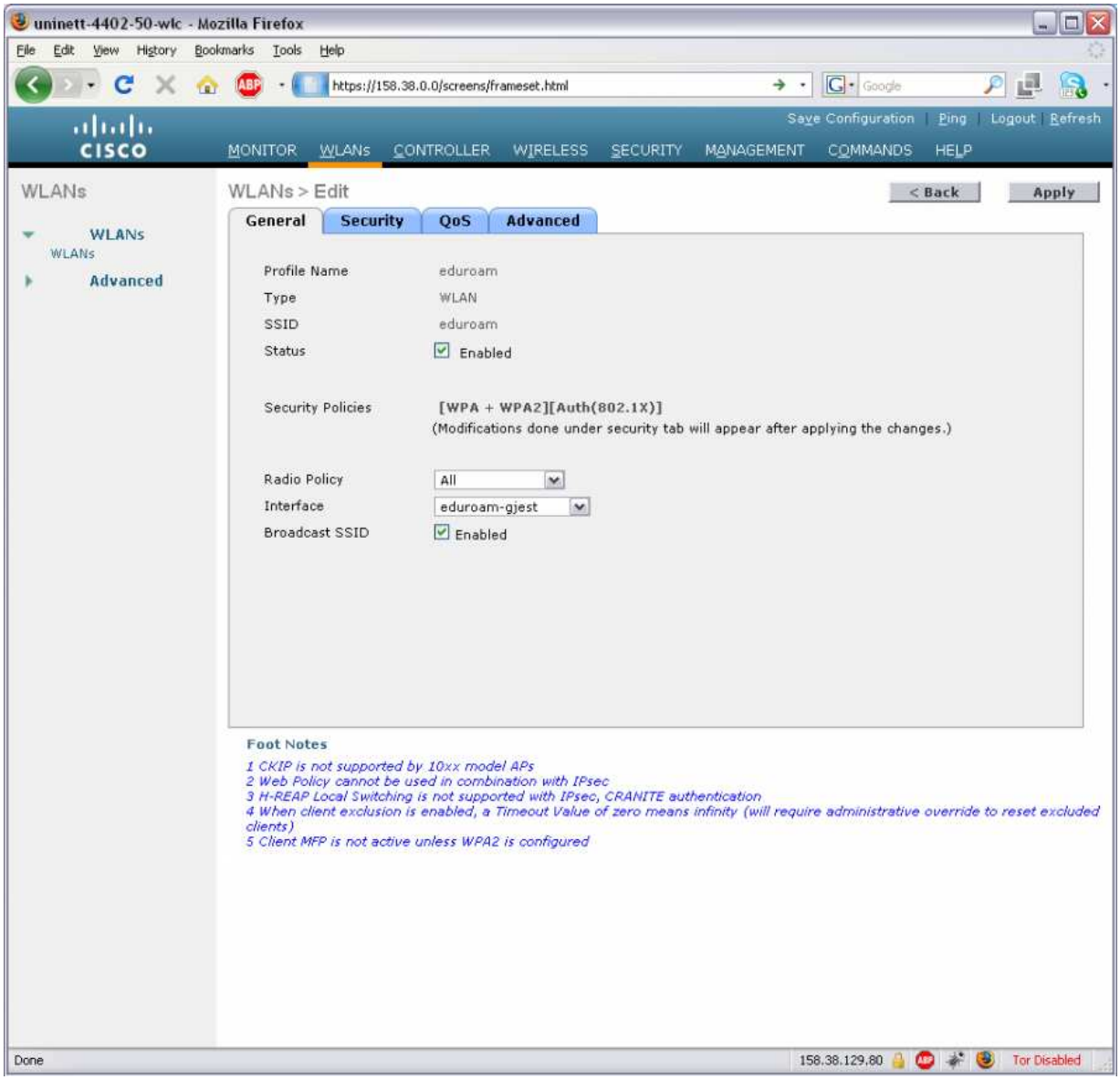
Path: WLANs → WLANs

Initially all that is needed is the SSID “eduroam”, but usually it is desirable to have an SSID for guests who cannot use “eduroam” or if an SSID is required for testing. An SSID can serve one or more of the virtual interfaces which have previously been defined and can easily be switched on or off as required.

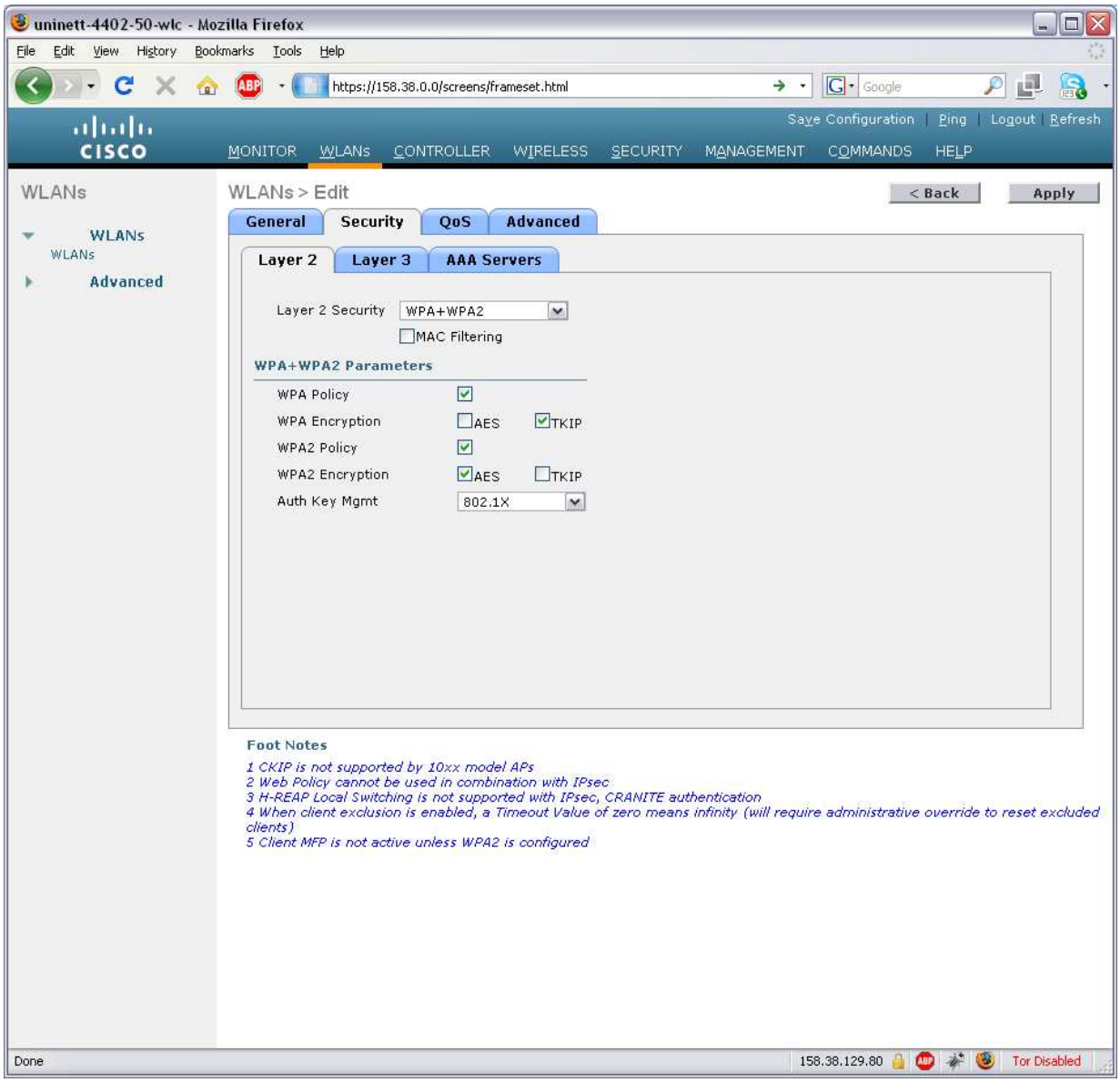
The first thing that must be done is to define a profile name and specify an SSID. This information cannot be changed later.



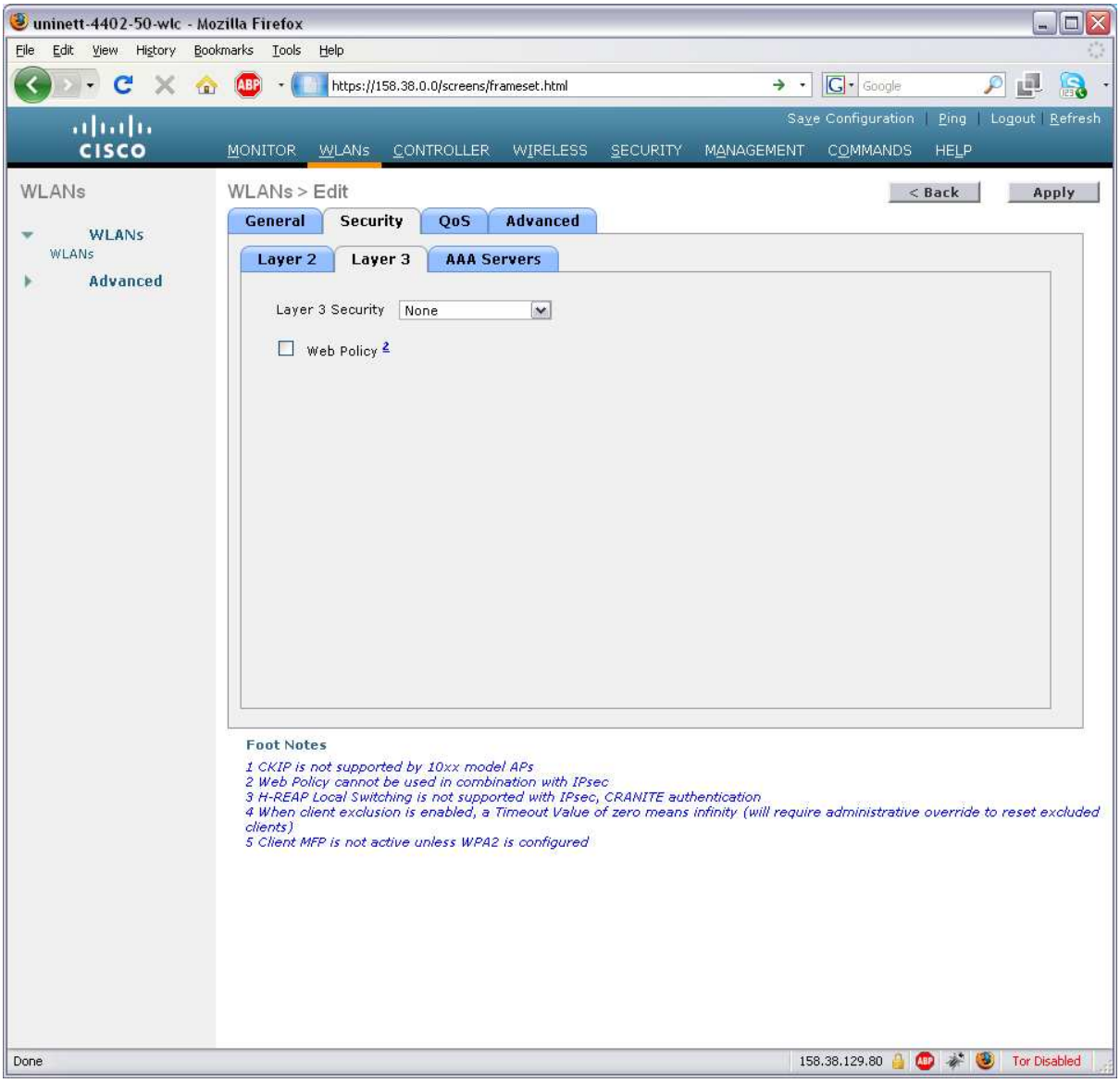
Under **General**, the WLAN can be enabled or disabled at any time. Usually the SSID is set to broadcast and for eduroam this is mandatory. Here we have configured “Interface” as a virtual interface intended for the use of guests. This VLAN has the lowest level of security and functions as a fall-back network. Users of other categories will be referred to other VLANs. Further information on this will be found below.



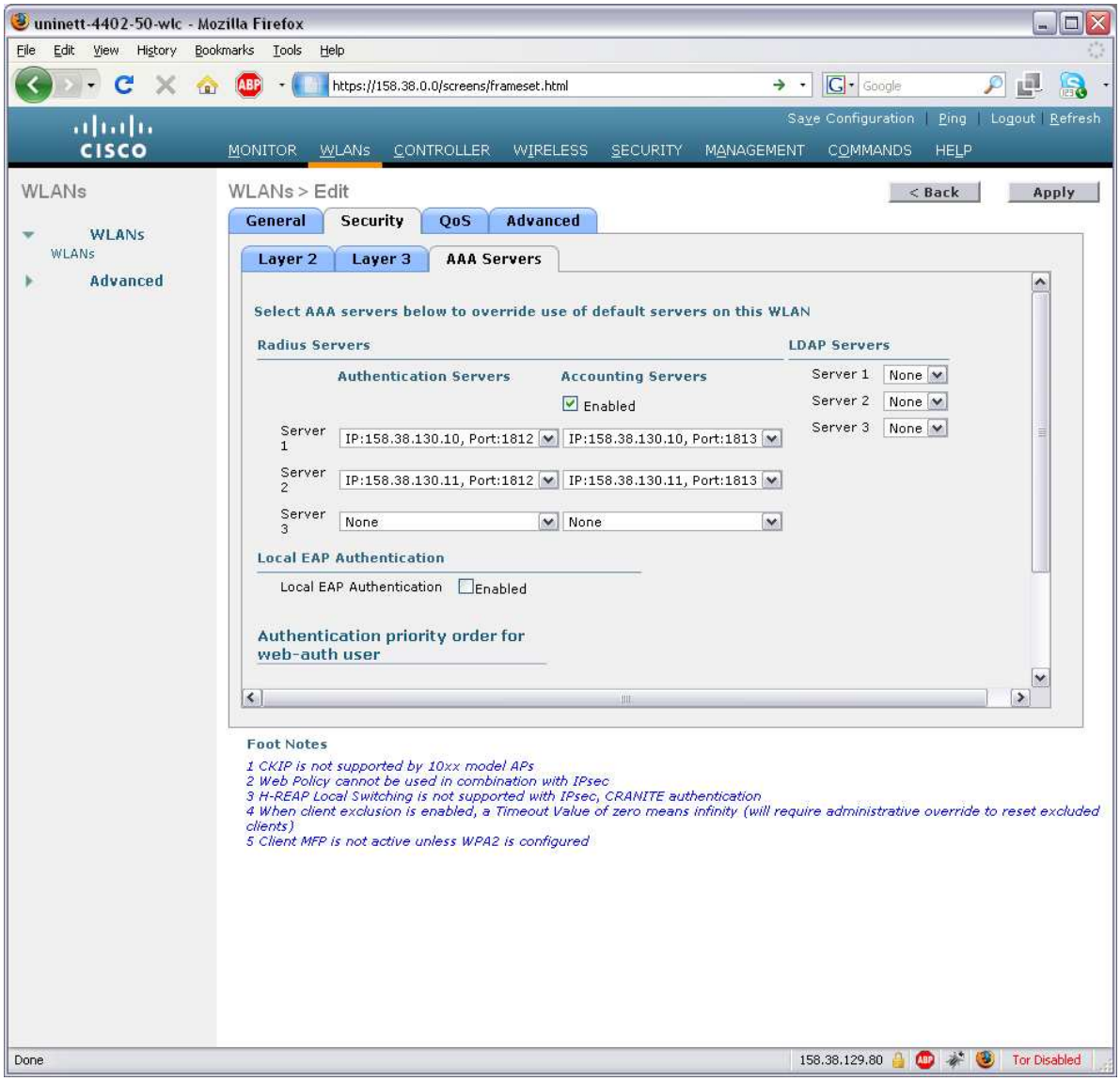
WPA+WPA2 are configured under **Security and Layer 2**. It is actually in conflict with 802.11i to have more than one method in a single network, but it is very common and is supported by most clients. However, since not all clients support other “variants”, it is recommended to keep to WPA-TKIP and WPA2-AES.



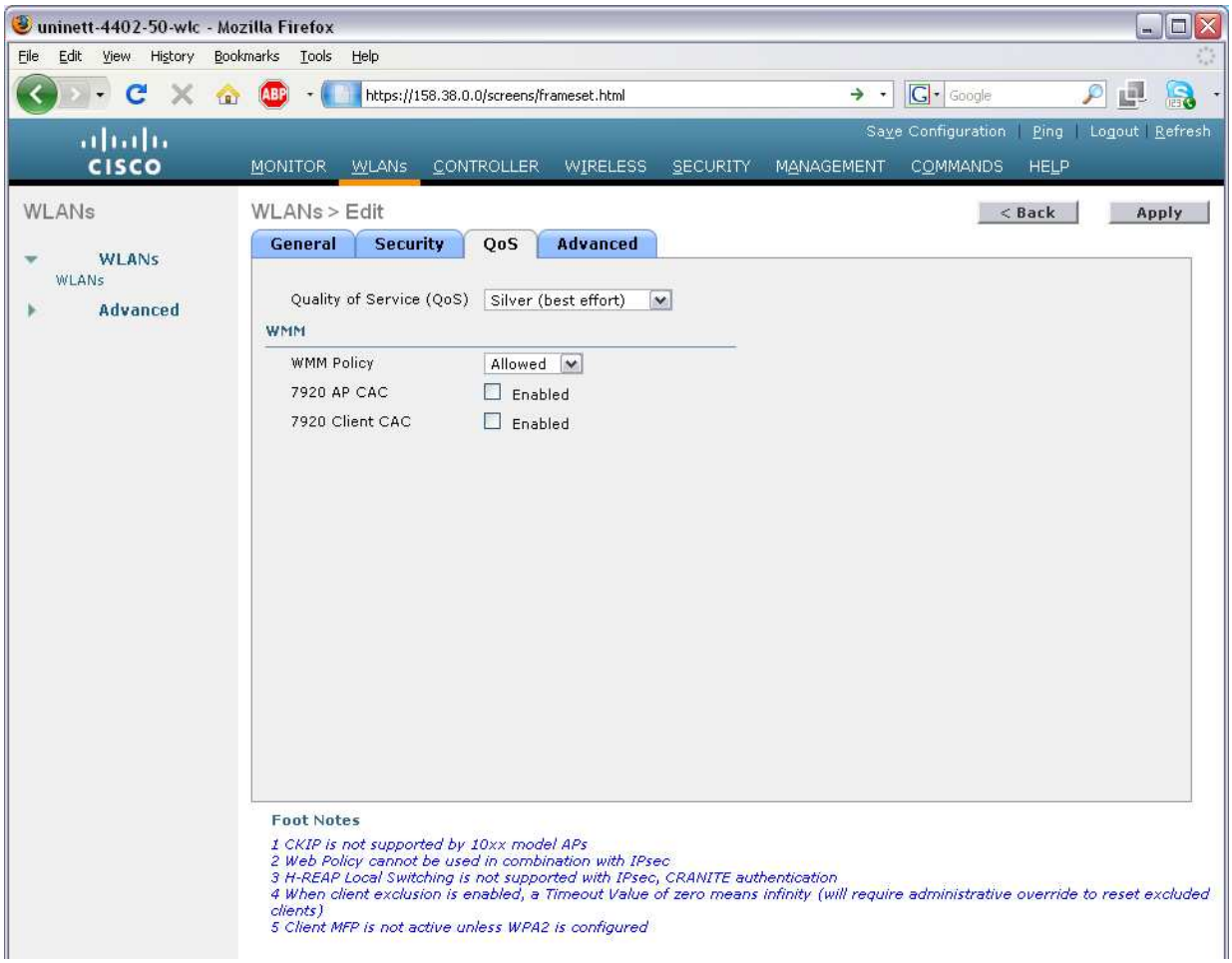
Security Layer 3 shall be “None”.



Under **Security AAA Servers we select the previously defined** RADIUS servers for Authentication and Accounting.



What one selects under QoS depends to some extent on how the organisation otherwise supports QoS in its network. The first QoS options are TOS (Type Of Service) values for IP tagging. Unfortunately this tagging will apply to *all* clients in this WLAN and therefore in practice is not applicable to eduroam. On the other hand, WMM depends on the relationship between the controller (access point) and clients, and may provide measurable benefits for real-time applications, so "WMM Policy Allowed" is recommended.



Under **Advanced** there are certain options to which one must give some thought, but as a rule these are:

Allow AAA Override: Enabled – This makes it possible to let RADIUS **override the VLAN which has been assigned to the WLAN.** In other words, a user of a different category is assigned to another VLAN. Failure to override will result in the user being assigned to the VLAN which is defined for the WLAN. In this way, it is possible to assign users to separate VLANs depending on their class, such as employee, student or guest, without using different wireless profiles.

Aironet IE: Enabled – Useful for those clients with this type of support.

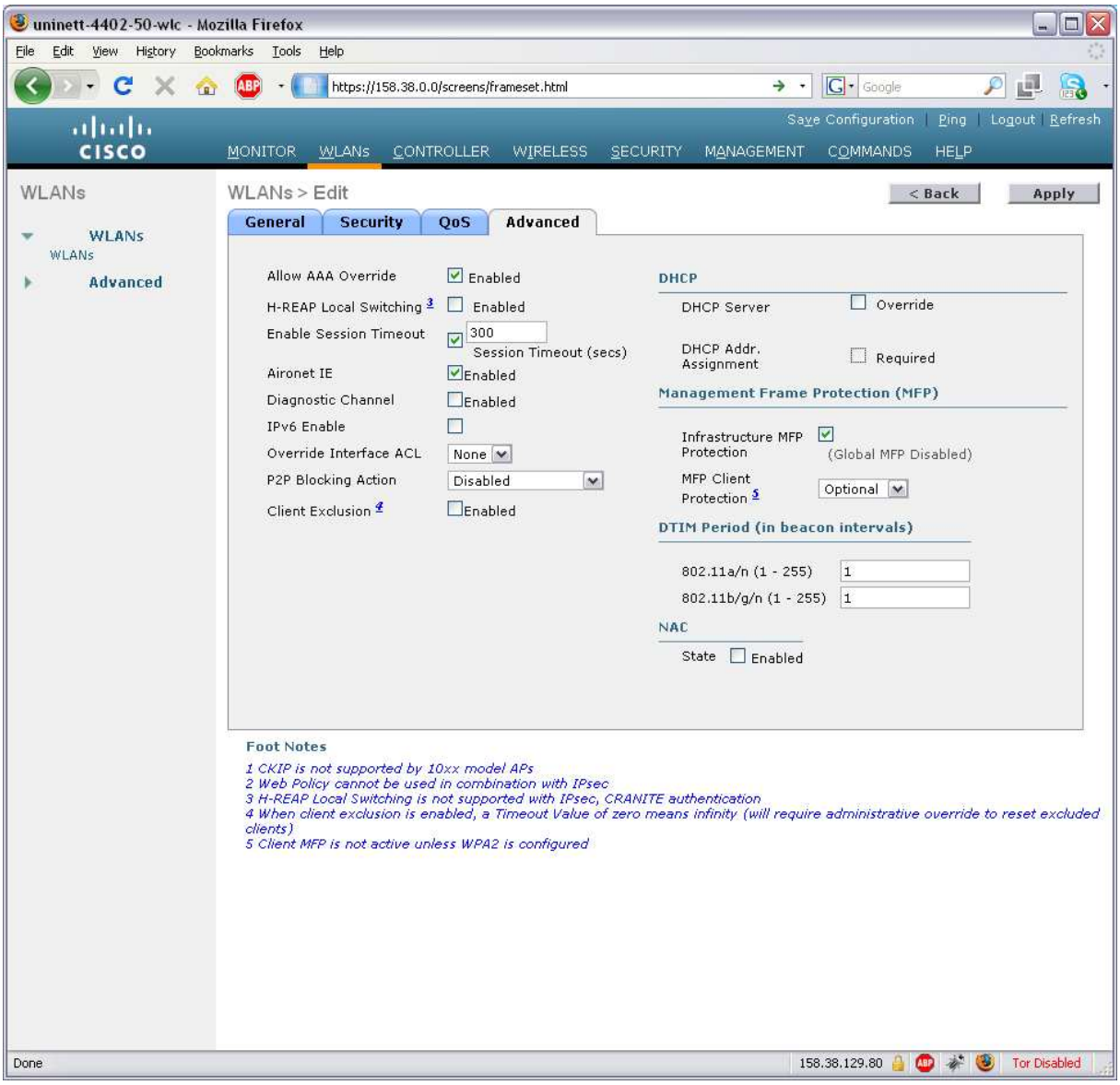
P2P Blocking Action: Disabled – This determines whether wireless clients are able to communicate directly with each other (via WLC) or not. For security reasons it is not advisable to allow clients to do this, so we recommend "Disabled", but it is up to each organisation to consider this.

Client Exclusion: Disabled – This is also a security feature. If, for example, a client fails to authenticate itself a certain number of times, there will be a compulsory ban before the client can try again. This can be more irritating than useful, so we recommend “Disabled”.

DHCP Server: No Override – Here it is possible to override the DHCP server which has been configured for the virtual interface.

DHCP Addr. Assignment: Required – One can set a condition that clients **must** obtain an IP address from a DHCP server: that is, a client is not permitted to define its own IP address statically. Ideally this should be set to required, but experience has shown that this setting can cause problems for some clients. In case of a temporary loss of connectivity, the controller will require a renewal of DHCP address and some clients has problems with handling this situation.

Management Frame Protection (MFP) – Attempts to protect against DoS, man-in-the-middle and dictionary attacks on the wireless network. To enable Client Protection, the clients must support CCX (Cisco Compatible eXtension program).

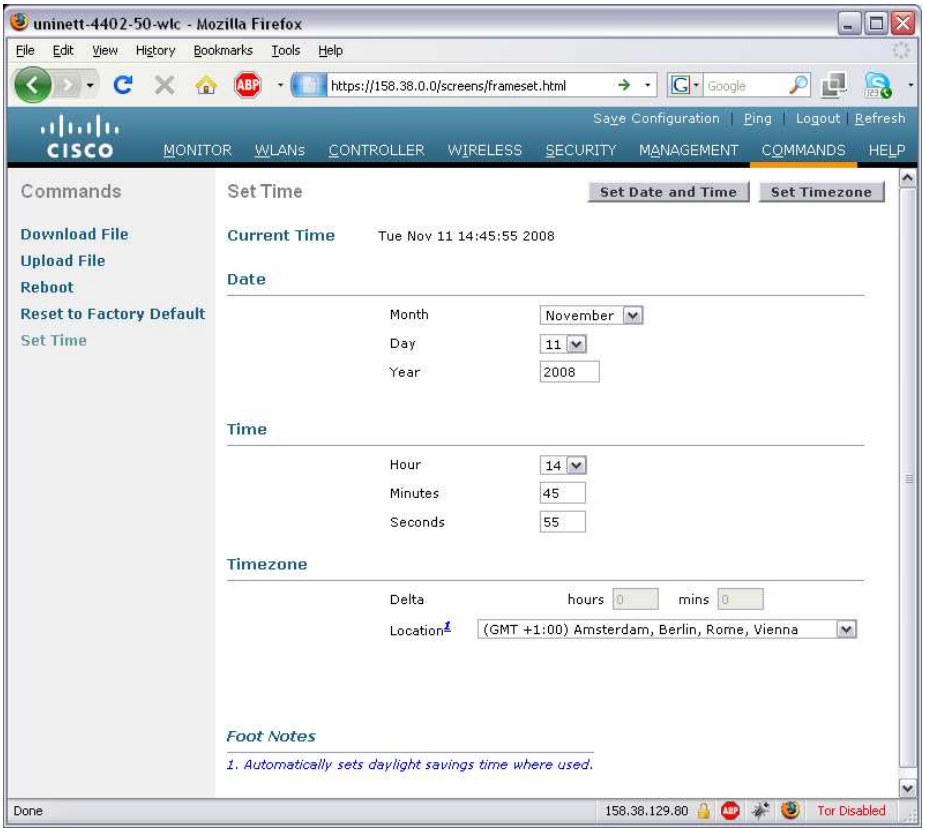


After pressing “Apply”, this WLAN will be activated.

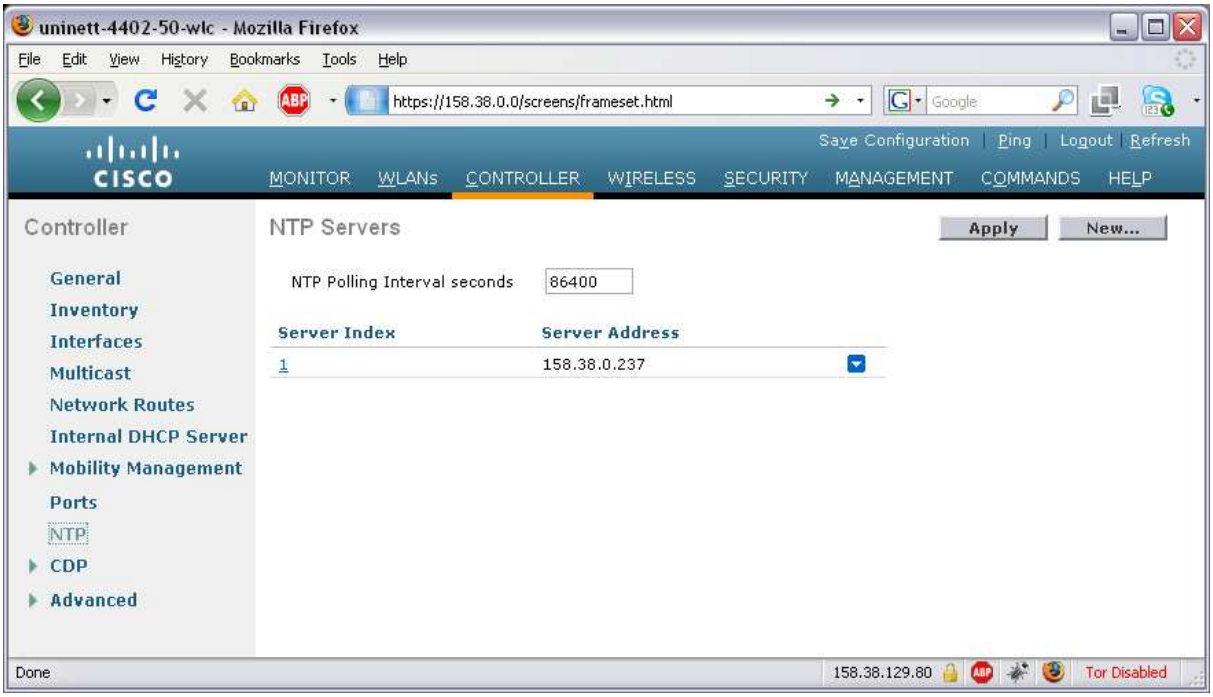
3.2.4 Connecting access points

After going through all the steps so far it is time to connect some access points to the network. Section 1.5.1 explains the access point connection process.

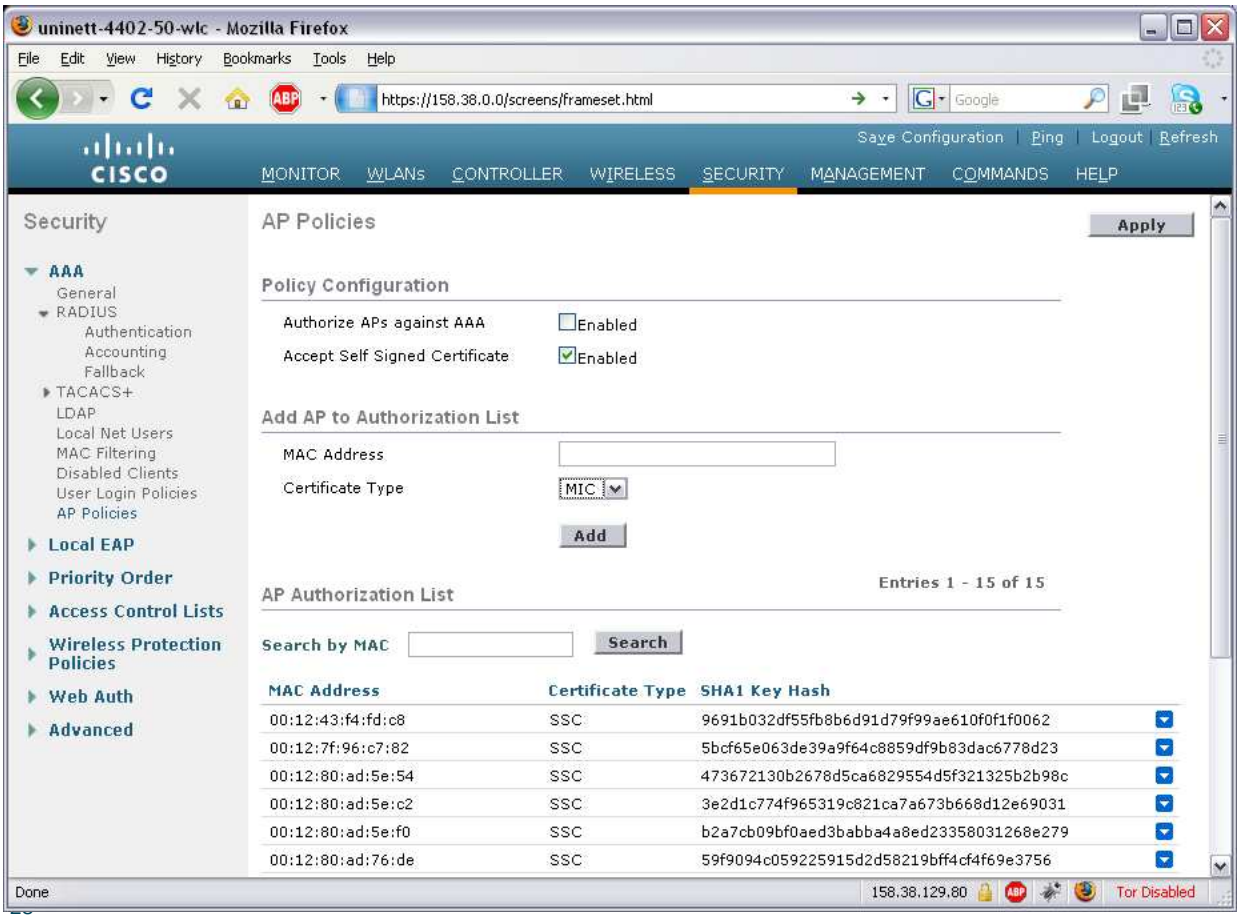
All access points have their own X509 certificates. For this to function and for the access point to connect, it is important that the WLC's time is correctly set so that the certificate is valid.



WLC supports NTP, which is set at another location. NTP server is usually the nearest router. If not another NTP server can be used, as in this example



If a previously autonomous access point has been converted to a lightweight access point and the application has not specified an SSC for the access point, the SSC or the MIC (the MAC address for the access point's Ethernet address) must be entered before the access point is permitted to connect. This will be found under **Security → AAA → AP Policies.**



3.2.5 Further details

Once a access point has been connected it will be possible to see the SSID which has been created.

Under **Management one may wish to configure a number of things, such as** SNMP parameters (which shall be used in communication with, among other things, the WCS), HTTP, Telnet, administration users, logging, and so on.

Regarding timeout values for EAP authentication, the section “Manipulating EAP Timers” in the Cisco document
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080665d18.shtml
gives some valuable recommendations that should be considered.

4 Radio planning

Carrying out effective radio planning involves a lot of work and can be very time-consuming. The controller assists to the best of its ability by adjusting the channel and power according to the prevailing conditions, but for a good result manual radio planning is essential.

Radio planning consists of surveying the radio frequency signal from given positions in order to determine the optimal location of the access points. Radio planning can be based on one of two criteria:

- Optimal capacity and coverage of the wireless network, i.e. as many access points as possible.
- Covering the required area using the smallest possible number of access points.

A third option may be to build the infrastructure to optimally detect the location of clients, but this is considered of secondary importance in this document.

Radio planning should be carried out for both 2.4 GHz and 5 GHz. Since 5 GHz usually has a shorter range than 2.4 GHz at the same effective re-adiated power, this should be taken into account if one is planning to use as few access points as possible. If one is to use as many access points as possible, one will in practice reduce the power output at 2.4 GHz so that 5 GHz will have at least as large a range. This therefore ceases to be a problem and one may not need to make measurements for both wavebands.

To carry out effective radio planning it is important to have the best possible knowledge of the structure of the building. One must also have access to most of the building in order to carry out the measurements. This means that measurements in some locations must take place outside of normal working hours, when rooms and auditoriums are vacant. If the properties of the building are broadly the same in several locations, it may be possible to get by with fewer measurements by copying the results from those locations. Otherwise one should preferably make measurements at all potential locations.

Simple measuring tools are:

- A wireless client with representative radio quality, i.e. not the client with the best radio, since this could result in problems for clients with radios of lower quality.
- An application such as NetStumbler, which can provide continuous feedback regarding signal strength and noise level.
- Plan drawings of the building, preferably several copies printed on paper.
- Felt tip markers in three colours.
- A access point of the type to be used, in an autonomous version, since the controller is not yet

operating and/or the cabling is not yet installed. Configure a unique SSID and preferably use a long Cat 5 cable and PoE for power supply. Network connection is not needed, although it is preferable, since one will want to change the power level as one determines what may work best under the current circumstances..

- A telescopic pole or other equipment to locate the access point temporarily as close as possible to the desired position.
- Preferably an assistant.

The method is as follows:

1. Locate the access point as near to the desired location as possible.
2. Use the client. Walk around, finding the extent of the desired signal strength, e.g. -70/75 dB is defined as the minimum acceptable quality.
3. Mark the boundary on the plan drawing.
4. Move the access point to the next potential location.
5. Repeat the measurements but mark the plan drawing with a different colour. Etc.

The different marker colours are used to represent different 2.4 GHz channels. There is only room for three channels in the same area. What one is trying to do is therefore to cover the entire area with colour but without fields of the same colour touching each other. If two fields of the same colour meet, there is a potential problem area which should be remedied by adjusting location and/or power output.

Remember that radio signals can also penetrate floors and ceilings, so the location of access points above and below the floor in question must also be taken into account.

AirMagnet Survey [3] and Airmagnet Planner [3] may be borrowed from UNINETT for use in radio planning. This software is associated with a specific wireless card which is provided. It can import plan drawings in the form of AutoCAD files, for example, and the Planner module can be used for virtual planning while the Survey module displays actual measurements. In short, this is an automatic and far more precise method of carrying out radio planning than using markers on paper. It also provides possibilities for making slight virtual adjustments to the access points to see what effect this has. Contact UNINETT in order to borrow this tool.

UNINETT also offers AirMagnet Spectrum Analyzer [3] (this product is now owned by Cisco), which displays everything happening in the frequency range, not just 802.11 traffic. This is very helpful in cases where there are connectivity problems which are impossible to understand on the basis of the 802.11 traffic alone.

5 Physical installation of access points

Where the access points are to be located has been determined by radio planning. The physical installation of the access points involves first the establishment of new network points at the locations of the access points. These points must then be patched to a switch and the access point must be installed.

Most access points support PoE, i.e. 802.3af. Some newer access points which support 802.11n require more power and consequently one must have 802.3at. PoE is far more practical and usually cheaper than installing a separate power outlet close to the access point and connecting a permanent power supply. That solution also results in the loss of the possibility of remotely controlling the power supply in order to switch the access point on or off. Naturally, one must not use Cat 5 cable splitting with PoE (i.e. divide the four pairs into two connections each with two pairs). A disadvantage with using PoE is the extra heat it generates. The PoE switches often cause a rise in temperature, especially in smaller rooms and cabinets where they are often placed.

To provide PoE to the access point one will need either a PoE-compatible switch or a PoE injector.

Most access points are supplied with some form of installation kit. Follow the installation instructions for the access point. Note that the correct way to install a Cisco AP1130/AP1140/3500i is with the flat, plastic surface *down*. In other words, it is not optimally located when attached to a wall, although this is possible and probably preferred in some cases. This issue should have been determined during the radio planning. The radio should be located at least 20 centimetres from any metal objects.

```
-  Install wiring between switch and access point
-  Install access point/access points
-  Use power preferably by way of PoE from the switch, or through injector
```

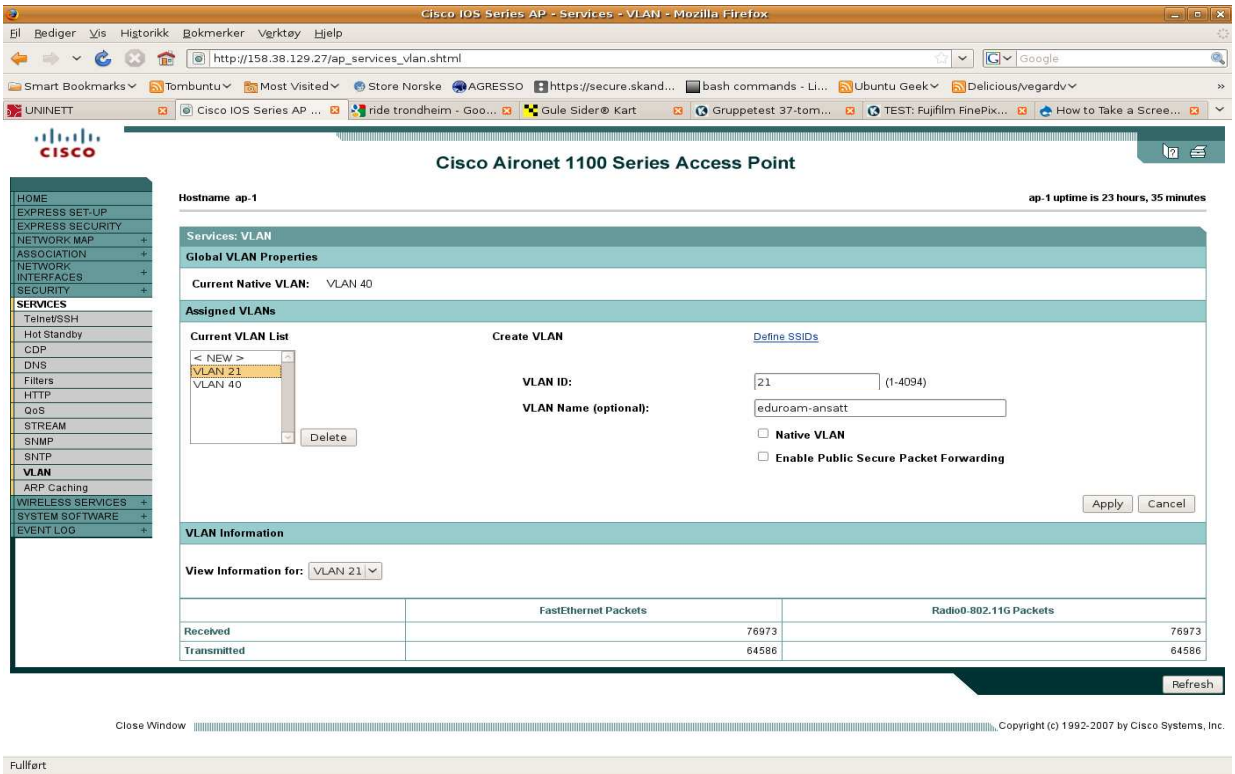
A. Configuration using autonomous access points

The following is a description of how configuration may be carried out using autonomous access points. As mentioned earlier, this type of configuration is not recommended from the point of view of security.

A.1 VLAN setup

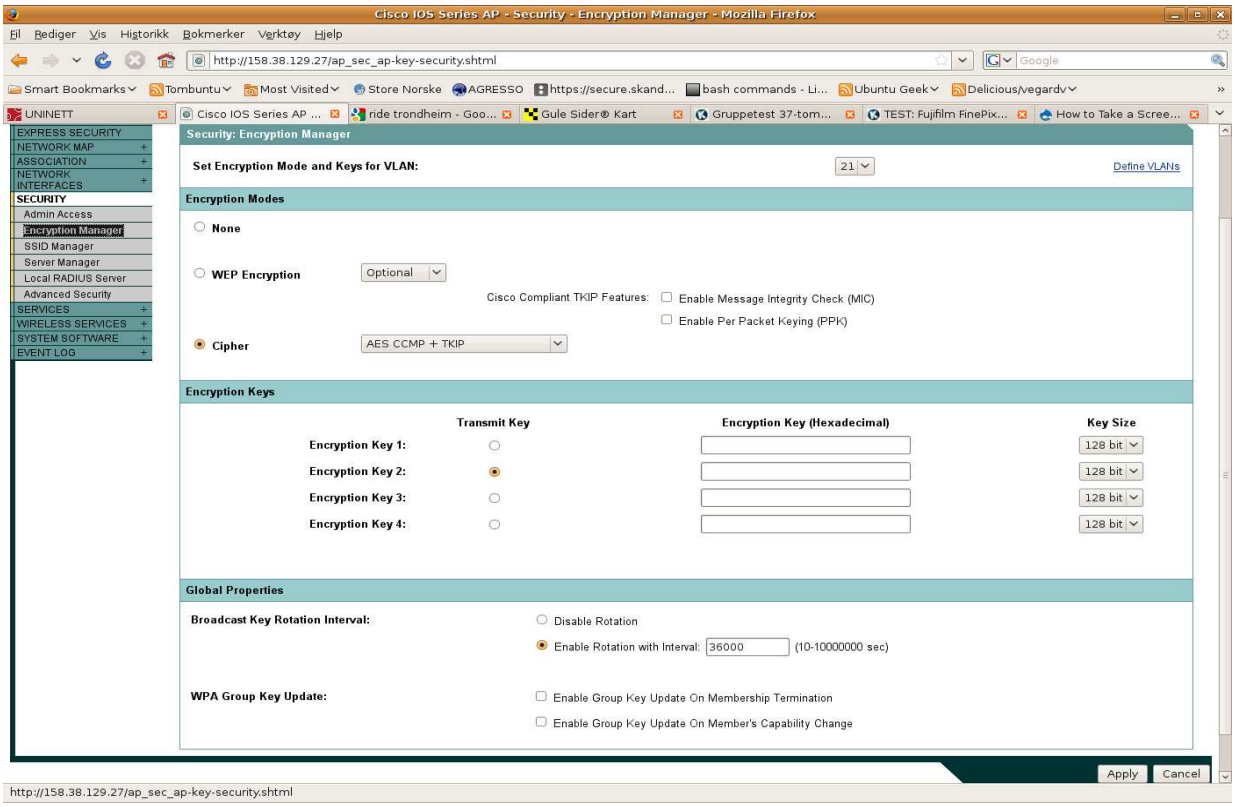
First we set up the VLAN, assuming that the access point is already configured with the necessary Management IP address, etc.

1. Log on to the access point using a web browser.
2. Go to SERVICES→VLAN to create the necessary VLANs. In our example, VLAN 21 has been created for eduroam employees and VLAN 40 for management. Remember to tick “Native VLAN” for VLAN 40.



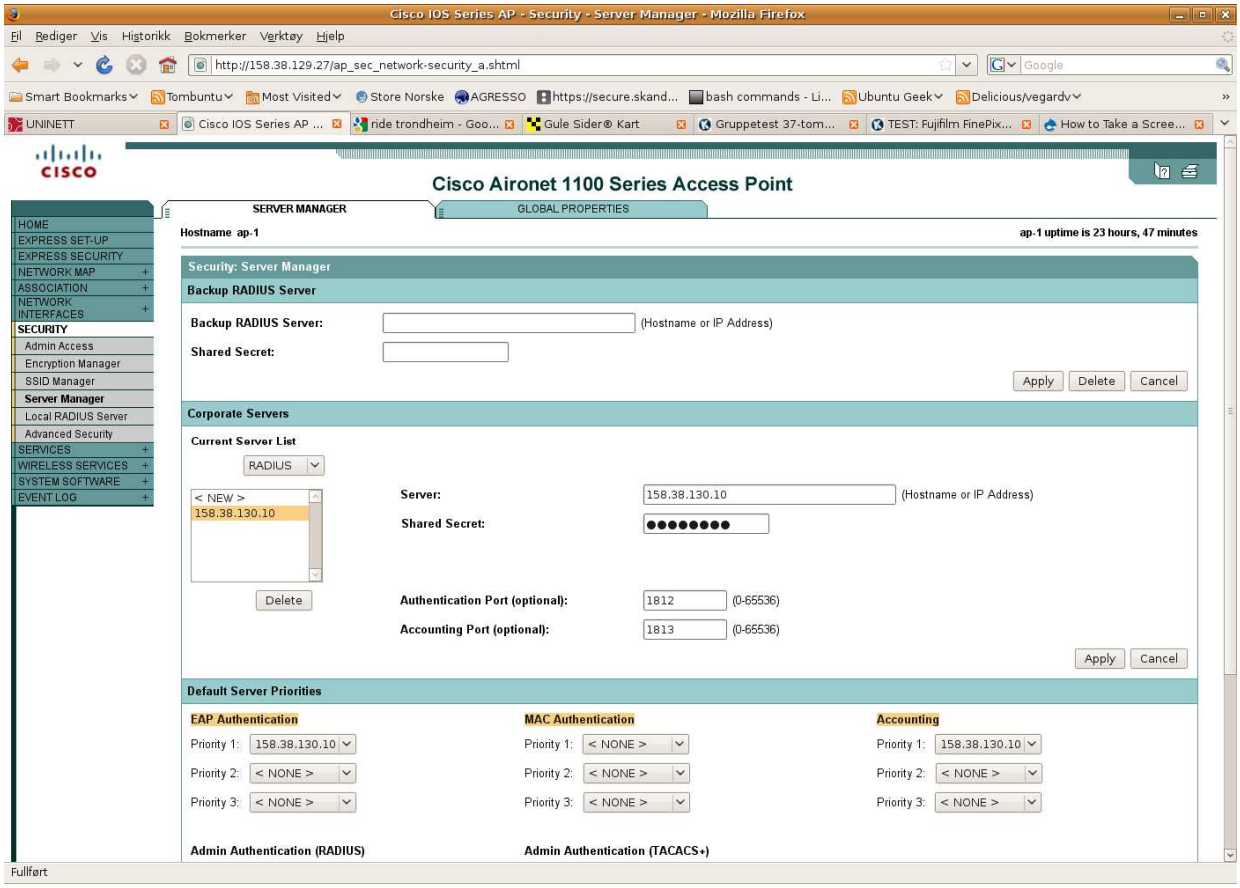
A.2 Encryption configuration

Now go to SECURITY → Encryption Manager and specify the necessary encryptions for VLAN 21. The minimum requirement here is TKIP, since not all types support AES. Select “Enable rotation” of the key and specify a value of, for example, 36,000 seconds.



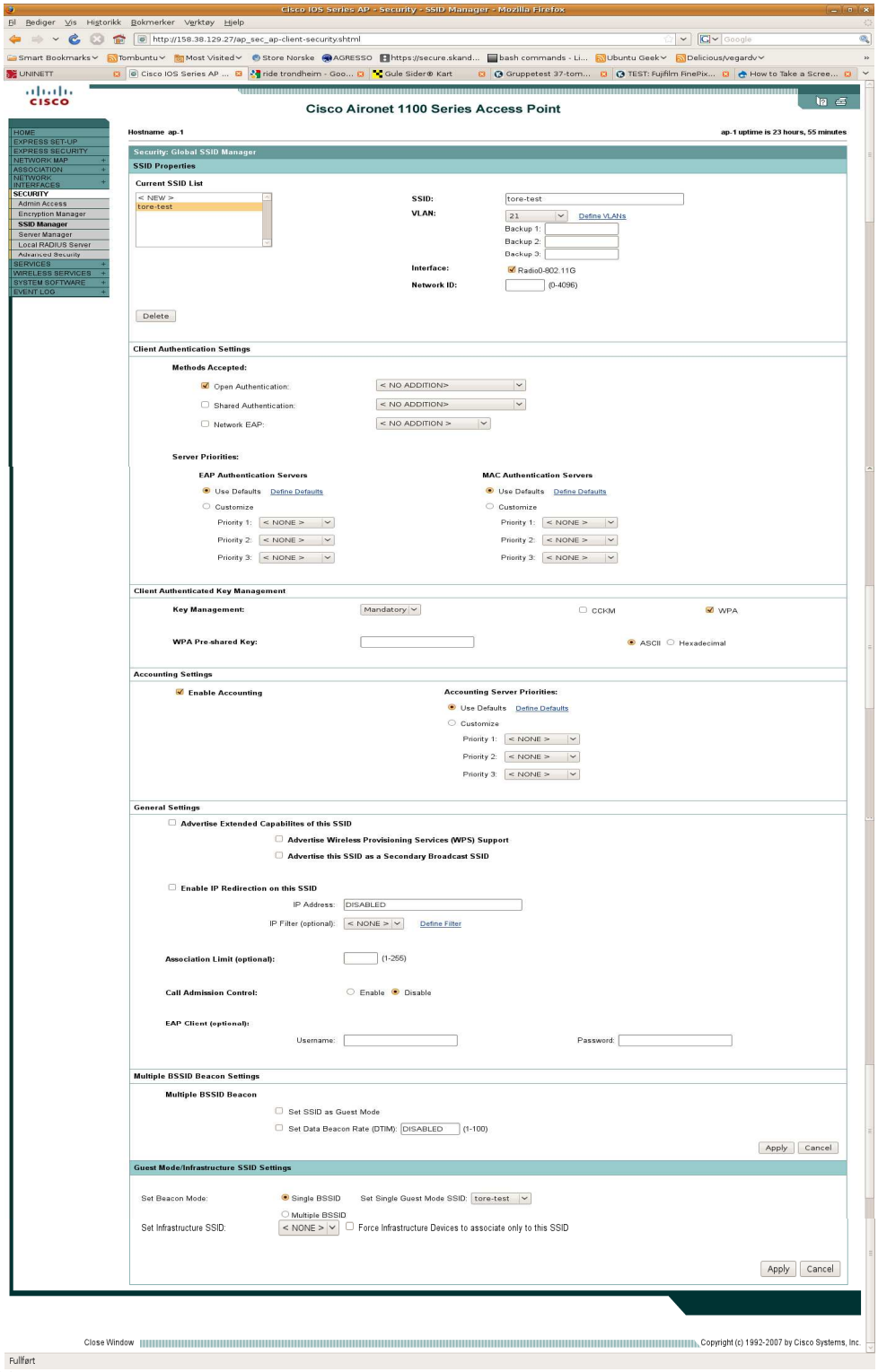
A.3 RADIUS configuration

Go to SECURITY → Server Manager and add the external RADIUS server using the shared secret. Specify the port number of the Authentication Port and Accounting Port, as well as the IP address for EAP Authentication and Accounting (in this case the same RADIUS server).



A.4 Default VLAN

Now go to SECURITY → SSID Manager and specify the default VLAN.



B. Configuring Microsoft RADIUS servers

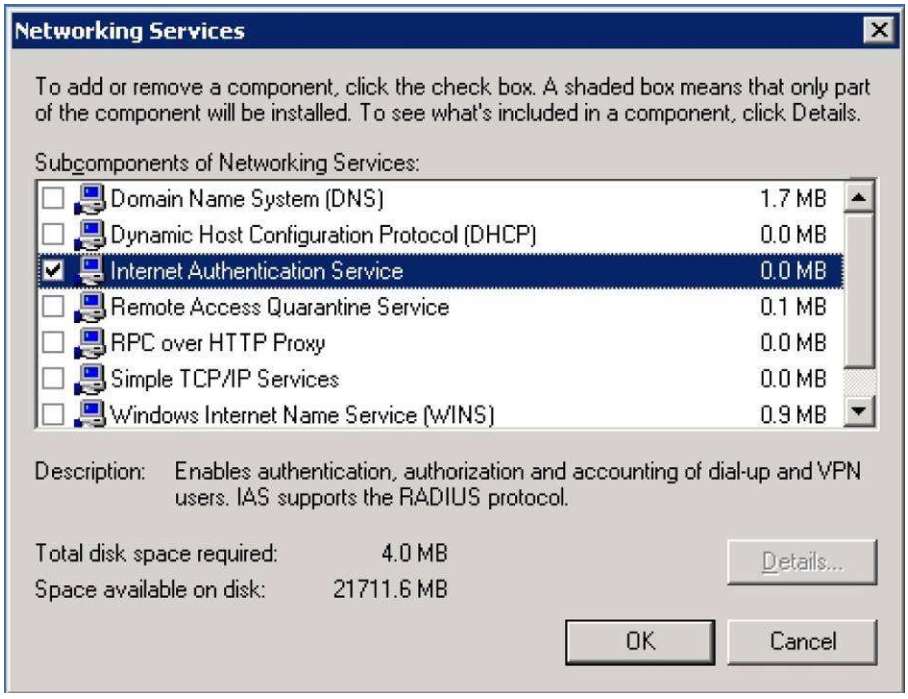
B.1 Configuring IAS (Windows 2003)

NB: This explanation assumes that the Windows 2003 server is registered in the domain.

Step 1: Installation of IAS

Go to Control Panel → Add or Remove Programs → Add/Remove Windows Components

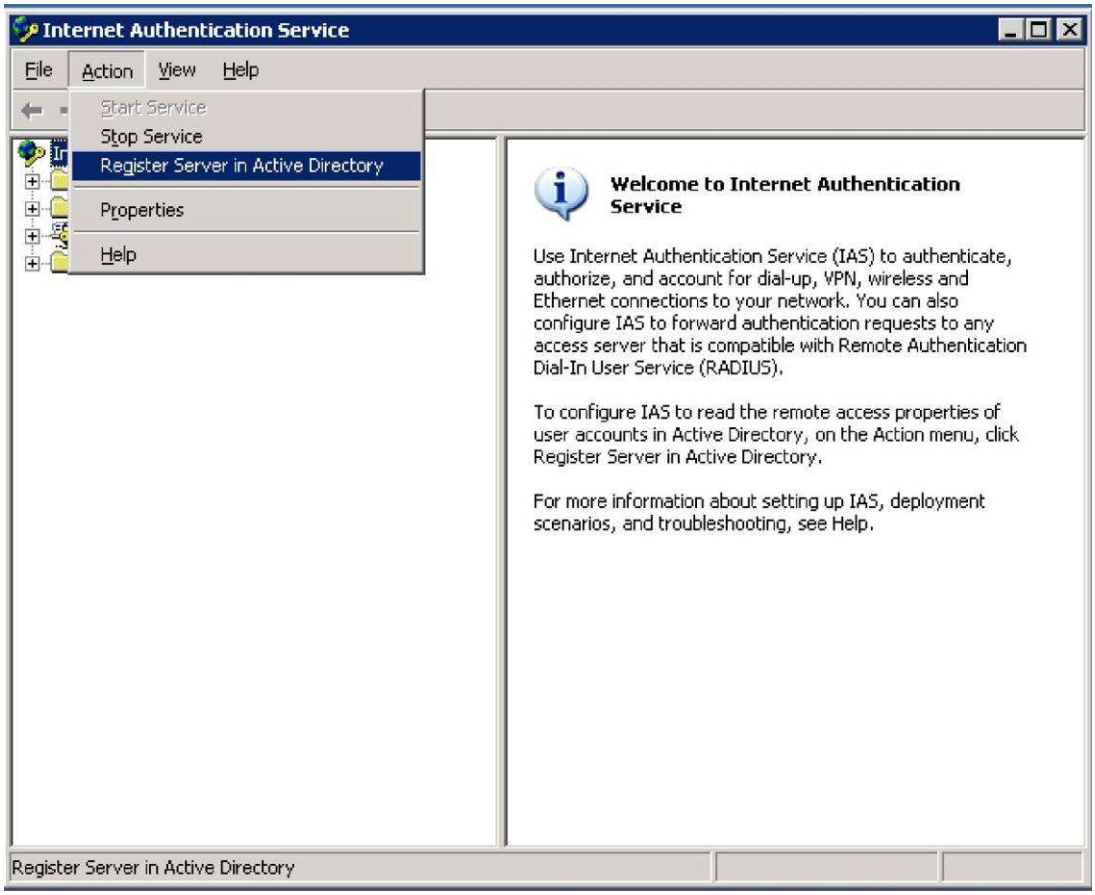
Select “Networking Services” and click on “Details”



Tick ”Internet Authentication Service”. Now click on “OK”, “Next” and “Apply” to install IAS.

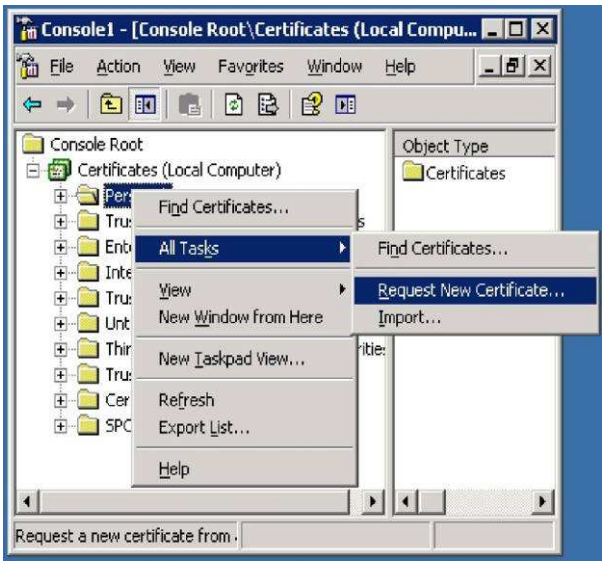
Step 2: Connecting to domain and certificates

Go to “Administrative Tools” on the Control Panel. Start “Internet Authentication Service”: Click on “Action” in the file menu. Click on “Register Server in Active Directory”



A certificate is required to activate PEAP. To add a certificate:

- Start → Run
- Type “mmc” and click on “OK”.
- In the window which opens, click on “File” and then ”Add/Remove Snap-in”.
- Click on “Add…” on the “Standalone” tab.
- Select “Certificates” and click on “Add”
- Select “Computer account” and click on “Next”
- Select “Local computer” and click on “Apply”
- Click on “Close” followed by “OK” in the windows which are open.



Click on the plus sign in front of “Certificates”. Right-click on “Personal”, select “All tasks” and then “Request New Certificate”

Follow the instructions on the screen until a new certificate has been created.
Close the console window.

Step 3: Adding clients in IAS

The clients are permitted to submit authentication requests to the RADIUS server, which the server then grants locally or forwards. For more information about the structure of eduroam, see the documentation of its infrastructure on the eduroam web page. The clients which can be added here may be access points, a control unit for wireless equipment (such as a Security Switch) or other RADIUS servers forwarding authentication requests here.

NB: When a control unit, such as a Security Switch or similar, is used for a wireless network one usually only needs to add it as a client and not all the access points.

Go to “Administrative Tools” on the Control Panel. Start “Internet Authentication Service”

Check if IAS is running; if not, click on “Action” in the file menu and click on “Start Service” (this will be grey if the service is already running).

- Right-click on “RADIUS Clients”, select “New RADIUS Client”, type a “Friendly Name” and IP address and click on “Next”.
    - (Examples of Friendly Names are Accesspoint1, AP-E314, SecuritySwitch, SchoolRADIUS: select one which is descriptive!)
- As the “Client-Vendor” one can select “RADIUS Standard”
- The Shared Secret must be the same in both the client and in the IAS setup.
    - A different Shared Secret must be used for each client

Repeat this process until all the clients have been added, remembering that other RADIUS servers which the forward authentication request shall also be added as clients.

If this is the central RADIUS server which is to be connected to eduroam, the core must also be added. To add the eduroam core, follow the same procedure as when adding clients but with the following settings:

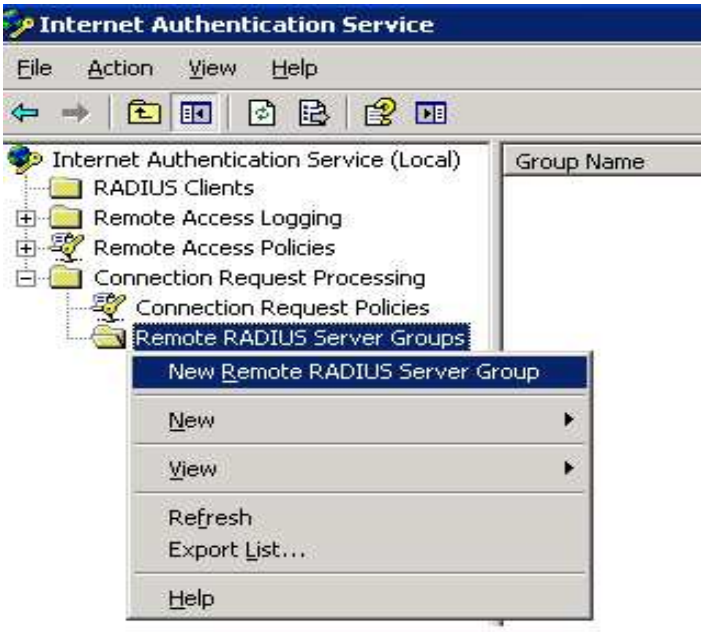
IP address: 128.39.2.22 (hegre.uninett.no) 158.38.0.184 (trane.uninett.no)
Friendly Name: eduroam
Shared Secret: If you have not received this, contact eduroam@uninett.no.

Step 4: Adding server groups to IAS

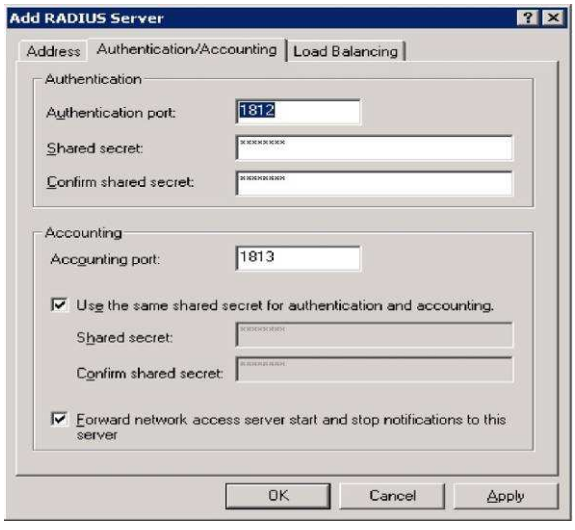
To enable IAS to forward authentication, a server group must be created.

If this RADIUS server is the last in a series of several and is not to forward authentication, it is not necessary to define any server groups. But as in Step 3, if the server is to be in communication with eduroam, eduroam must be added as a server group.

Right-click on “Remote RADIUS Server Groups” and select “New Remote RADIUS Server Group”



- Click on “Next”
- Select “Custom” and type in a name for the server group
  - If this is the server group used for connection to eduroam, the server group should be called “eduroam”
- Click on “Add” to add RADIUS servers to the server group.
- On the “Address” tab, enter the IP address or DNS name of the server.
- On the Authentication/Accounting tab, fill in the Authentication port and the shared secret
- On the “Load Balancing” tab, no changes are necessary in systems with redundancy.
- Click on “OK” followed by “Next”
- Remove the tick from “Start the New Connection Request Policy Wizard when this Wizard closes”
- Click on “Apply”



Repeat this procedure until all the server groups, for example a group for eduroam and a group for School, have been added.

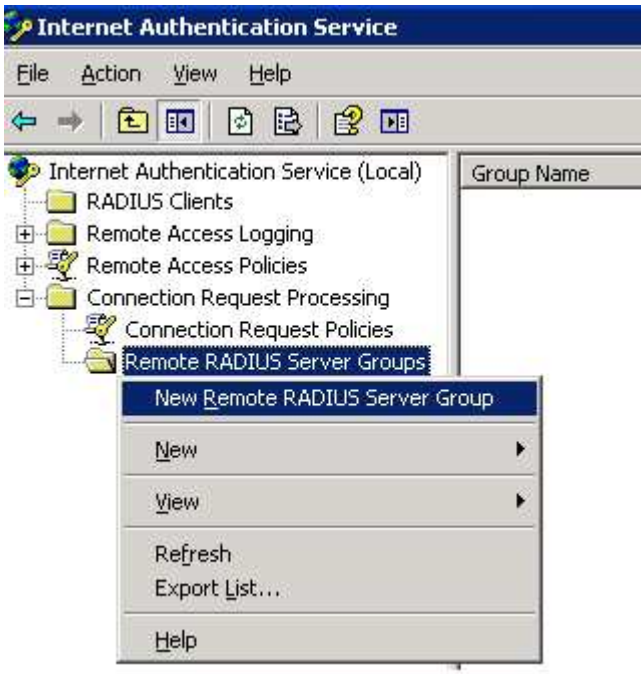
See www.eduroam.no for more information about eduroam.

Step 5: Connection Request Policies

Connection Request Policies determine where authorisation shall take place according to certain criteria. One policy may authenticate employees locally and forward all students to the RADIUS server associated with the school domain, while another policy directs all other users to the eduroam core. Since the policies are handled in a specific order, it is important that this is done correctly.

1. Users who are to be authenticated locally
2. Users who are to be forwarded to another RADIUS server (several of which can be configured)
3. All other users to be directed to eduroam

1. Right-click on “Connection Request Policy” and select “New Connection Request Policy”.



2. Click on “Next”
3. Select “A custom policy”, fill in the Policy name (for example, “Local”, “School” or “eduroam”) and click on “Next”.
4. Click on “Add” to add criteria for the connection.

Eduroam determines where a user belongs by using the realm which is indicated when the user types **username@organisation**. In spite of the apparent similarity, there is no connection between realm and e-mail address. However, in most cases it is possible to use a realm corresponding to an e-mail address. The realms used are often agreed in advance. If you have any queries, contact eduroam@uninett.no.

An example of a realm:

student.school.no is the connection to eduroam and forwards authentication to the employee.school.no RADIUS server. The “Employee” RADIUS server is the last in the series and receives authentications it is to use and forwards them.

Criteria for “Connection Policies” on the student.school.no RADIUS server:

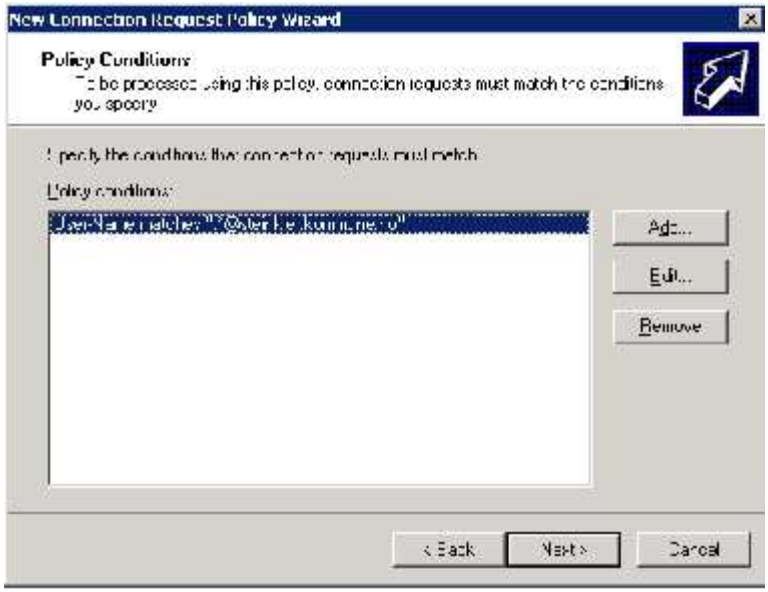
.*@student.school.no – All students, authenticated locally
.*@employee.school.no – All employees, sent to the “Employee” RADIUS server
.*@.* – All other users, sent to the “Employee” RADIUS server

Criteria for Connection Policies on the “Employee” RADIUS server:

.*@employee.school.no – All employees, authenticated locally

.*@.* – All other users, sent to the eduroam server

Select “User-Name” and click on “Add”. Fill in the criteria: for example “.*@student.school.no” specifies that all users who type in username@stuent.school.no shall be authenticated using this policy.



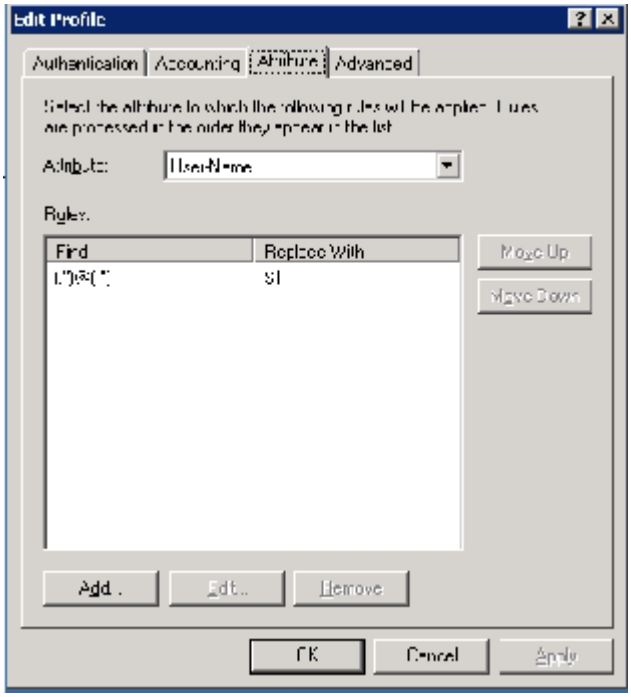
Click on “Next” and then “Edit Profile”.

On the “Authentication” tab, specify where the authentication request shall be directed:

- If one selects “Authenticate request on this server” the user is authenticated on this RADIUS server and the domain of which the user is a member. In that case:
  - Click on the “Attributes” tab
  - Select “Attribute: User-Name” and click on “Add”
  - Under “Find”, type: `(.*)@(.*)` and under “Replace with”, type: $1
- One may also select “Forward requests to the following remote RADIUS server group for authentication”: the authentication request is then forwarded to one of the server groups created in Step 4.

Click on “OK” followed by “Next” and “Apply”.

Create a Connection Request Policy for every connection this RADIUS server is to serve.



Step 6: Remote Access Policies

Remote Access Policies handle the local authentication and can for example grant different users access to different networks: some to the guest network, some to VLAN 10, VLAN 12, etc.

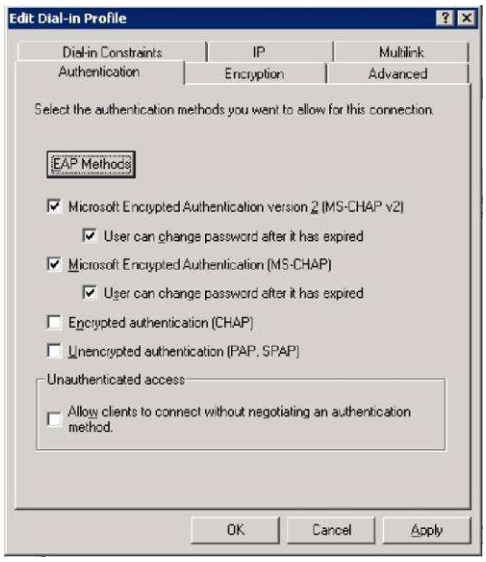
- Right-click on “Remote Access Policies” and select “New Remote Access Policy”
- Click on “Next”, select “Set up a custom policy” and type in a name for the policy
- Choose descriptive names for policies, such as “Employees with guest network”, “Students in VLAN10”, etc.
- Click on “Next”
- “Policy conditions” are the criteria which determine whether a user shall use this policy or try the next.
- Click on “Add”
    - The criteria which should be checked for each Remote Access Policy are up to the system operators and depend to a large extent on how allocation is to take place.

Some standard options may be:

“NAS-Port-Type” adding “Ethernet”, “Wireless – IEEE802.11” and “Wireless – Other” “Windows-Groups” adding “Domain Users” and, for example, “Quarantine” or “WiFi VLAN10” or other groups from AD. **NB: The AD groups must be created first!**

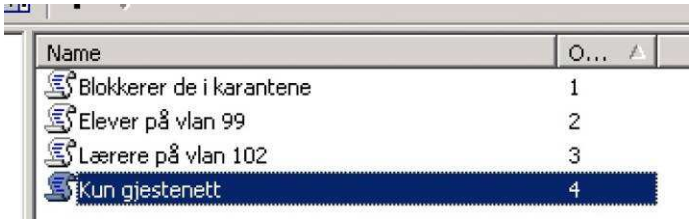
- When the criteria have been determined, click on “Next”, select “Grant remote access permission” and click on “Next”.
    - Remote Access Policies may also be created which deny access to users. For example, all users belonging to the security group “Wireless Access Denied” will be assigned the criterion “Deny remote access permission”. But remember: the policies are handled in a predetermined order and users will obtain access to the first alternative which is appropriate. Hence it may be wise to specify all policies which use “Deny remote access permission” first.
- Click on “Edit Profile…”
    - The properties which should be specified in the profile depend somewhat on the application but the following must be included:

- Click on the “Authentication” tab
- Click on “EAP Methods”, click on “Add”, select “Protected EAP (PEAP)”, click on “OK”.
- To check that a PEAP has been created with a single certificate, click on “Edit …” Click on “OK” and tick:
- “Microsoft Encrypted Authentication version 2 (MS-CHAP v2)”
- The use of “User can change password after it has expired” is optional



- Click on “OK”, then “Next” and “Apply”

Do this for each Remote Access Policy that is needed.



Step 7: RADIUS attributes

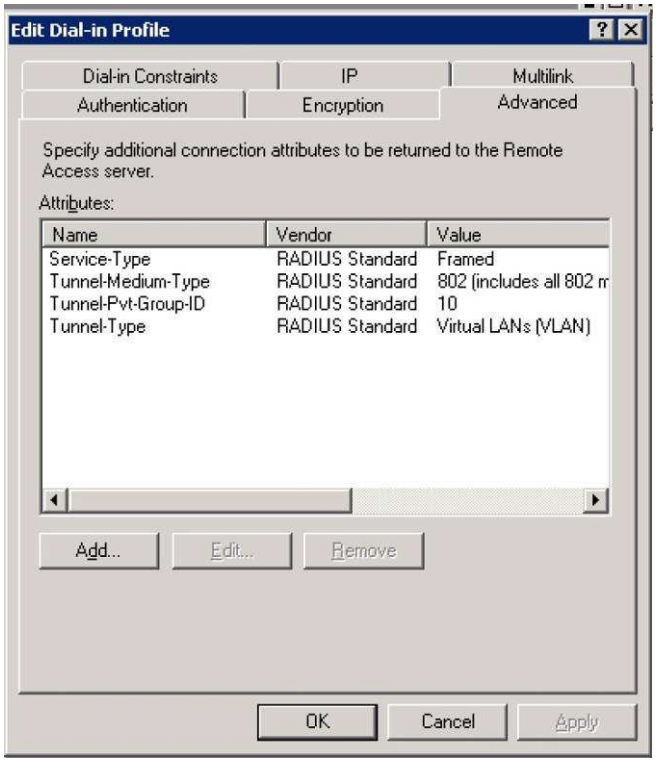
Remote Access Policies may be expanded using RADIUS attributes. The RADIUS attributes can, among other things, provide the user with access to different VLANs.

Right-click on a Remote Access Policy: for example “Students in VLAN 10”, and select “Properties”

Click on “Edit Profile” and select the “Advanced” tab

There are many ways of configuring different RADIUS attributes. The following is a description of what is needed to assign a user to a different VLAN from that supplied as standard by the access points or controller unit:

- Click on “Add”, select “Tunnel-Medium-Type” and click on “Add”
- Click on “Add” again and select “802 (Includes all 802 media plus Ethernet canonical format)”
- Click on “OK” twice to return and select additional attributes.
- Select “Tunnel-Pvt-Group-ID” and click on “Add”
- Click on “Add” again and type the name of the VLAN which is to be used, for example “10”
- Click on “OK” twice to return and select additional attributes.
- Select “Tunnel-Type” and click on “Add”
- Click on “Add” again and select “Virtual LANs (VLAN)”
- Click on “OK” twice, then click on “Close” in the “Add attribute” window
    - The list will now look something like the illustration below.



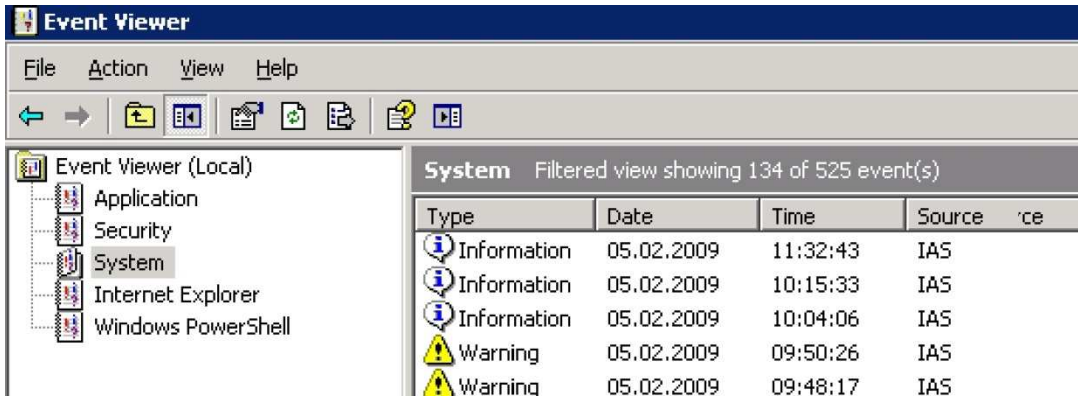
Click on “OK” twice and repeat this step for all the Remote Access Policies which are to be modified.

Step 8: Logging

IAS adds log entries to the Event Log and writes them to a file.

Open “Event Viewer” and select “System”. All events under Source “IAS” are logs generated by IAS.

IAS creates the log entries “Error”, “Warning” and “Information”



The logs contain a great deal of useful information such as:

User ola.nordmann was granted access.
“Granted access” or “denied access”

Fully-Qualified-User-Name = school.no/Users/Ola Nordmann
Full path of the user in the AD

Client-Friendly-Name = SecuritySwitch
The client which has sent the authorisation request to this RADIUS server

Client-IP-Address = 10.10.10.91
The Client’s IP address

Calling-Station-Identifier = 00-1A-73-F5-34-7D
The MAC address of the user who is attempting to gain access

NAS-Port-Type = Wireless - IEEE 802.11
The type of network being used

Proxy-Policy-Name = School
The Connection Request Policy being used

Authentication-Provider = Windows
The program used by the user to connect to the wireless network

Policy-Name = students in VLAN 10
The Remote Access Policy being used

B.2 Configuring NPS (Windows 2008)

Step 1: Add a role

Add the role “Network Policy and Access Services”, the only role service required by the Network Policy Server.

Open the Network Policy Server by clicking on “Start Menu” → “Administrative Tools”→
“Network Policy Server”

Under “Network Policy Server”, click on “Action” in the file menu and click “Register server in Active Directory”. Make sure that the service has also been started (“Start NPS” is grey).

A certificate is required to activate PEAP. To add a certificate: Start → Run

Type “mmc” and click on “OK”.

In the window which opens, click on “File” and then “Add/Remove Snap-in”. Click on “Add…” on the “Standalone” tab.

Select “Certificates” and click on “Add”

Select “Computer account” and click on “Next”
Select “Local computer” and click on “Apply”
Click on “Close” followed by “OK” in all the windows that are open.

Click on the plus sign in front of “Certificates”. Right-click on “Personal”, select “All tasks” and “Request New Certificate”

Follow the instructions on the screen until a new certificate has been created. Close the console window.

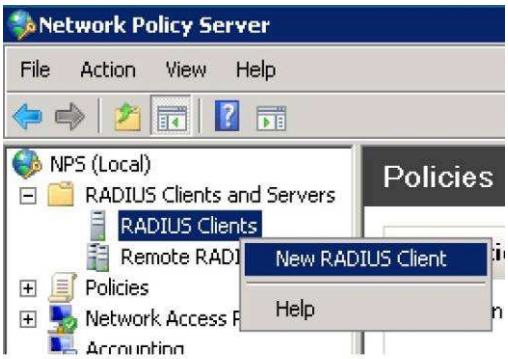
Step 2: Radius

The clients are permitted to submit authentication requests to the RADIUS server, which the server then grants locally or forwards. For more information about eduroam, visit www.eduroam.no. The clients which can be added here may be access points, a control unit for wireless equipment (such as a Security Switch) or other RADIUS servers forwarding authentication.

NB: When a control unit, such as a Security Switch or similar, is used for a wireless network one usually only needs to add it as a client and not all the access points.

Open the Network Policy Server by Clicking on “Start Menu” → “Administrative Tools”→
“Network Policy Server”

Expand “RADIUS Clients and Servers”, right-click on “RADIUS Clients” and select “New RADIUS Client



- Type in a “Friendly Name”
    - (Examples of Friendly Names are Accesspoint1, AP-E314, SecuritySwitch, SchoolRADIUS: select one which is descriptive!)
- Type in an IP address or full DNS name
- Under “Vendor name”, “RADIUS Standard” may be selected
- The Shared Secret must be the same in both the client and in the NPS setup.
    - A different Shared Secret may be used for each client
- Click on “OK”

Repeat this procedure until all the clients have been added. Remember that other RADIUS servers which forward authentication requests shall also be added as clients.

NB: If this is the central RADIUS server which is to be connected to eduroam, the core must also be added.

To add the eduroam core, follow the same procedure as when adding clients but with the following settings:

IP address: 128.39.2.22 (hegre) 158.38.0.184 (trane)

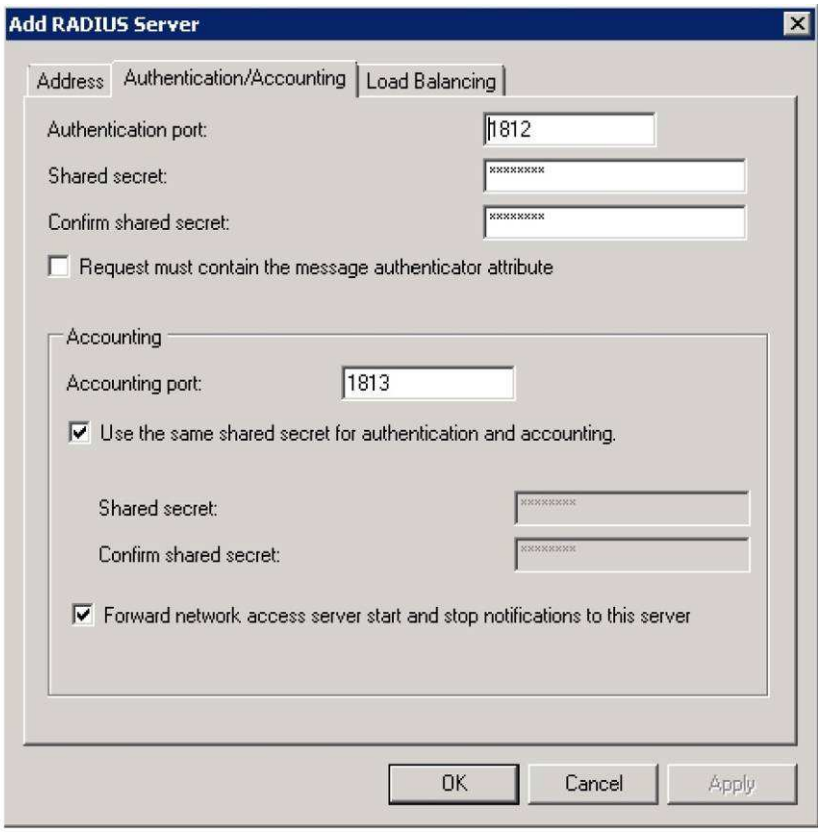
Friendly Name: eduroam

Shared Secret: If you have not received this, contact eduroam@uninett.no.

Step 3: Adding Remote RADIUS Server Groups

To enable NPS to forward authentications, a server group must be created. If this RADIUS server is the last in a series of several and is not intended to forward authentication, it is not necessary to define any server groups. If the server is to be in communication with eduroam, eduroam must be added as a server group.

- Right-click on “Remote RADIUS Server Groups” and select “New”
- Type in a “Group name” and click on “Add”
  - If this is the server group used for connection to eduroam, the server group should be called “eduroam”
- On the “Address” tab, enter the IP address or DNS name of the server.
- In the “Authentication/Accounting” tab, type in the Authentication Port and Shared Secret



- On the “Load Balancing” tab, no changes are necessary in systems with redundancy.
- Click on “OK” in both windows.

Repeat this procedure until all the server groups, for example a group for eduroam and a group for School, have been added.

See www.eduroam.no for more information about eduroam.

Step 4: Connection Request Policies

Connection Request Policies determine where authorisation shall take place according to certain criteria. One policy may authenticate employees locally and forward all students to the RADIUS server associated with the school domain, while another policy directs all other users to the eduroam core. Since the policies are handled in a specified order, it is important that this is done correctly.

1. Users who are to be authenticated locally
2. Users who are to be forwarded to another RADIUS server (several of which can be configured)
3. All other users to be directed to eduroam

- Expand “Policies”, right-click on “Connection Request Policy” and select “New”
- Type in the Policy name (for example, “Local”, “School” or “eduroam”) and click on “Next”
- Click on “Add” to add criteria for the connection.

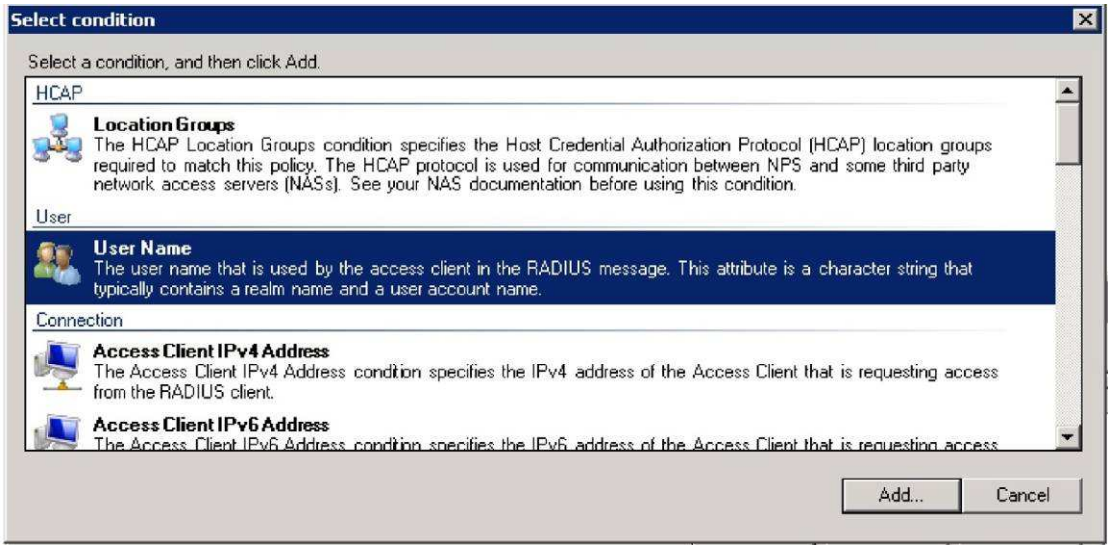
eduroam determines where a user belongs by using the realm which is indicated when the user types username@organisation. In spite of the apparent similarity, there is no connection between realm and e-mail address. However, in most cases it is possible to use a realm corresponding to an e-mail address. The realms used are often agreed in advance. If you have any queries, contact *eduroam@uninett.no*

An example of a realm:
student.school.no is the connection to eduroam and forwards authentication to the employee.school.no RADIUS server. The “Employee” RADIUS server is the last in the series and receives authentication requests it shall use and forwards them.

Criteria for Connection Policies on the student.school.no RADIUS server:
.*@student.school.no – All students, authenticated locally
.*@employee.school.no – All employees, sent to the “Employee” RADIUS server
.*@.* – All other users, sent to the “Employee” RADIUS server

Criteria for Connection Policies on the “Employee” RADIUS server:
.*@employee.school.no – All employees, authenticated locally
.*@.* – All other users, sent to the eduroam server

- Select “User-Name” and click on “Add”. Fill in the criteria, for example “.*@student.school.no” specifies that all users who type in username@student.school.no shall be authenticated using this policy.
- Click on “OK” followed by “Next”



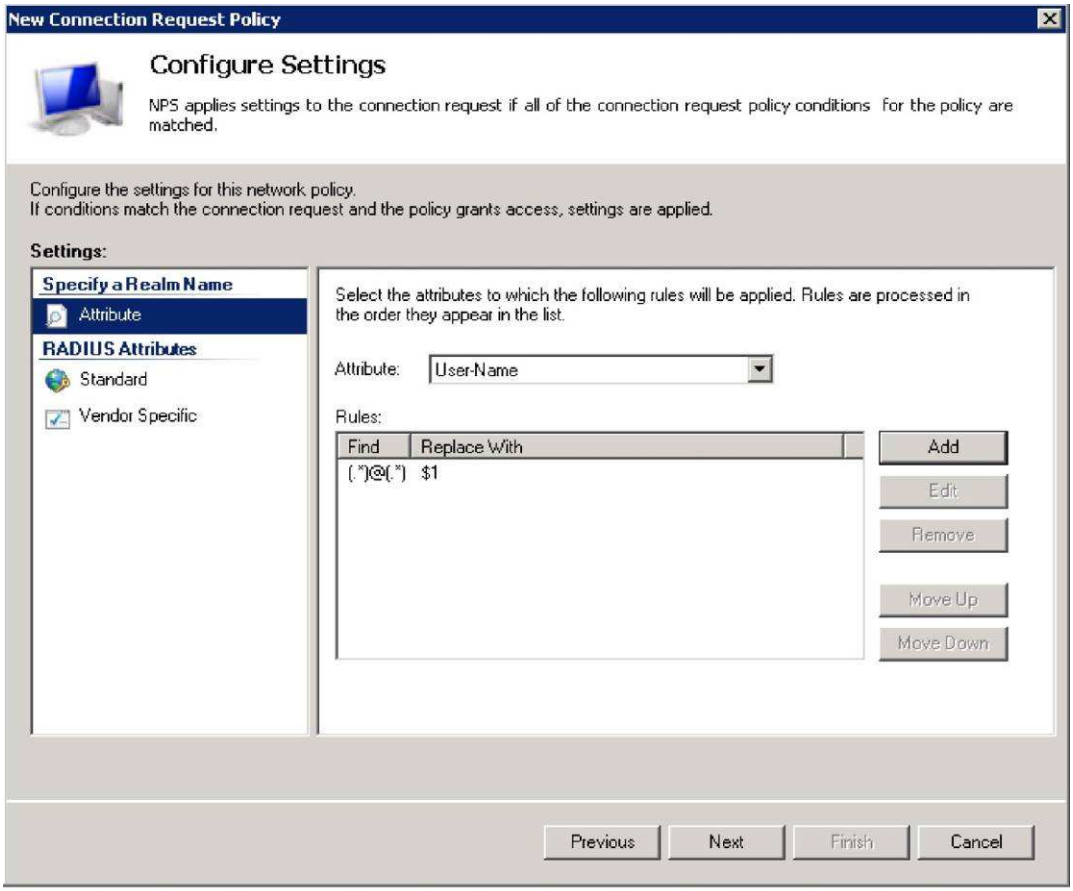
The “Authentication” option controls where the authentication is to be directed to.

- If one selects “Authenticate request on this server” the user is authenticated on this RADIUS server and the domain of which the user is a member. Proceed as follows:
  - Click on the “Attributes” tab
  - Select “Attribute: User-Name” and click on “Add”
  - Under “Find”, type: (.*)@(.*)
  - Under “Replace with”, type: $1
- One may also select “Forward requests to the following remote RADIUS server group for authentication”. The authentication request is then forwarded to one of the server groups created in Step 3.

Click on “Next”

- “Override network policy authentication settings” must **not** be used in this connection.

Click on “Next”



Click on “OK” followed by “Finish”

Create a Connection Request Policy for each connection this RADIUS server is to serve.

Step 5: Network Policies

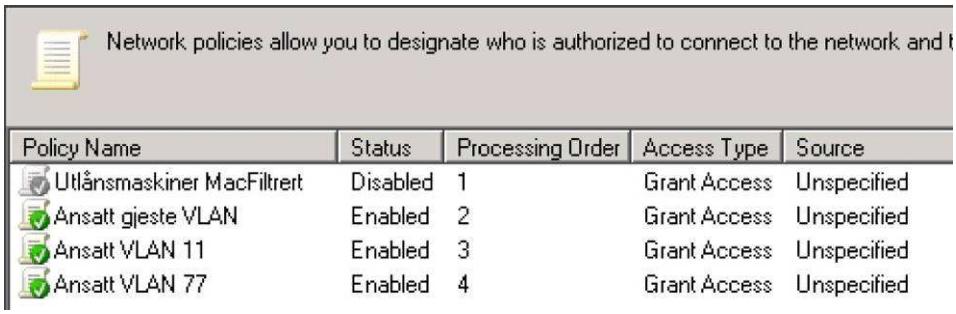
Remote Access Policies handle the local authentication and can for example grant different users access to different networks: some to the guest network, some to VLAN 10, VLAN 12, etc.

- Right-click on “Network Policies” and click on “New”
- Choose descriptive names for policies, such as “Employees with Guest network”, “Students in VLAN10”, etc.
- Click on “Next”
  - “Conditions” are the criteria which determine whether a user shall use this policy or try the next.
- Click on “Add”
  - The criteria which should be checked for each Network Policy are up to the system operators and depend to a large extent on how allocation is to take place.

Some standard options may be:
“User Groups”, adding “Domain Users” and for example “Quarantine” or “WiFi VLAN 10” or other groups from AD. **NB: The AD groups must be created first!**

- When the criteria have been specified, click on “Next”, select “Access granted” and click on “Next”
  - Network Policies may also be created which deny access to users. For example, all users belonging to the security group “Wireless Access Denied” will be assigned the criterion “Access denied”. But remember: the policies are handled in a predetermined order and users will obtain access to the first alternative which is appropriate. Hence it may be advisable to specify all policies which use “Access denied” first.
- Click on “Add”, add “Microsoft: Protected EAP (PEAP)” and click on “OK”
- Ensure that “Microsoft Encrypted Authentication version 2 (MS-CHAP v2)” is ticked.
  - The remainder of the selections are optional.
- Click on “Next”
- Note the NAS Port Type
- Select “Ethernet”, “Wireless – IEEE 802.11” and “Wireless – Other”
- Click on “Next”, then “Next” again, followed by “Finish”

Do this for each Network Policy that is needed.



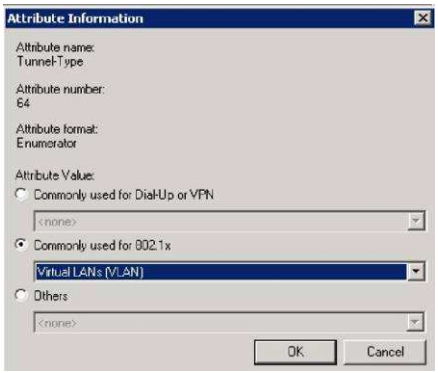
Step 6: RADIUS attributes

Network Policies may be expanded using RADIUS attributes. The RADIUS attributes can, among other things, provide the user with access to different VLANs.

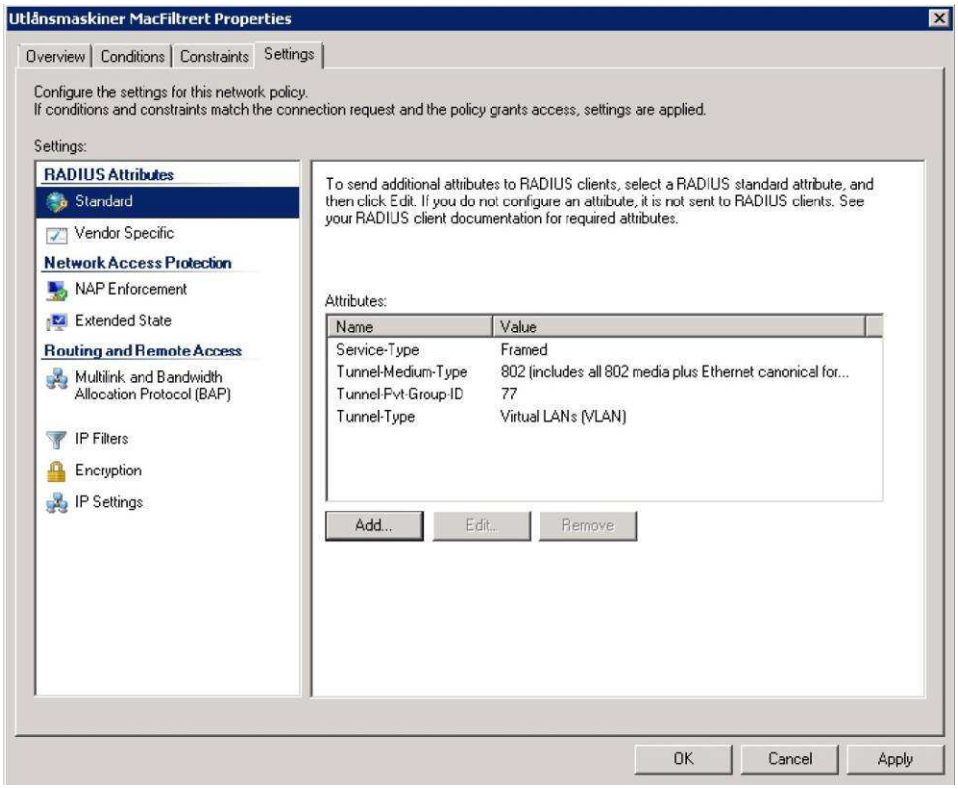
- Right-click on a “Network Policy” and select “Properties”
- Go to the “Settings” tab

There are many ways of configuring different RADIUS attributes. The following is a description of what is needed to assign a user to a different VLAN from that supplied as standard by the access points or controller unit:

- Click on “Standard” in the left-hand frame and click on “Add” in the right-hand frame.
- Find “Tunnel-Medium-Type” in the list and click on “Add”
- Click on “Add” again and select “802 (Includes all 802 media plus Ethernet canonical format)”
- Click on “OK” twice to return and select additional attributes
- Find “Tunnel-Pvt-Group-ID” in the list and click on “Add”
- Click on “Add” and type in the VLAN which is to be used. For example: “77”
- Click on “OK” twice to return and select additional attributes
- Find “Tunnel-Type” in the list and click on “Add”
- Click on “Add” and select “Virtual LANs (VLAN)”
- Click on “OK” twice and then on “Close”
- Click on “OK”



Repeat for all the Network Policies which need to be modified, for example in the VLAN.



Step 7: Logging

NPS adds log entries in the Event Log and writes them to a file.

Open the Event Viewer and go to “Custom Views”, “Server Roles” and “Network Policy and Access Services”. NPS creates the log entries “Warning” and “Information”, while “Error” entries are only logged in a file (in C:\Windows\System32\LogFiles)

also

Network Policy Server granted access to a user.
“Granted access” or “denied access”

Account Name: Ola.Nordmann
The user name in the user’s domain

Account Domain: School
The domain of which authentication is requested

Fully Qualified Account Name: school.no/Users/Nordmann, Ola
Full path of the account in the domain

Calling Station Identifier: 00-1A-73-F5-34-7D
The MAC address of the user who is attempting to gain access

Client Friendly Name: SecuritySwitch
The client which has sent the authorisation request to this RADIUS server

Client IP Address: 10.10.10.91
The client’s IP address

Proxy Policy Name: Local
The Connection Request Policy being used

Network Policy Name: Employee VLAN 77
The Network Policy being used

Authentication Server: RADIUS.employee.school.no
The name of this RADIUS server

Authentication Type: PEAP
The type of authentication being used

EAP Type: Microsoft: Secured password (EAP-MSCHAP v2)
The type of EAP being used

C. Installing a certificate for FreeRADIUS

To order and obtain a certificate with the help of UNINETT's SCS service, see http://forskningsnett.uninett.no/scs/hvordan.html. This also describes how to generate the RADIUS server's private key (CSR), using openssl. The private key must be submitted via UNINETT's SCS service and forms the basis for issuing a certificate. When this has been completed, the certificate must be installed on the RADIUS server.

FreeRADIUS requires the entire certificate chain to be included in the final certificate. In effect the certificate will consist of three parts: first the private key you have generated, then the certificate issued by TERENA and finally the certificate issued by Comodo UserTrust. The combined certificate is saved as "somethingorother.pem" It is then placed in the location specified in the RADIUS configuration, often in /etc/FreeRADIUS/cert/.

Below is an example of how such a certificate may appear (this is not a real certificate, as this could naturally not be published)

----BEGIN RSA PRIVATE KEY----- U1NMIENBMB4XDTEwMDUxMjAwMDAwMFoXDTEzMDUxMTIzNTk1OVowQzELMAkGA1UE BhMCTk8xEzARBgNVBAoTClVOSU5FVFQgQVMxHzAdBgNVBAMTFnJhZGl1cy10ZXN0 LnVuaW5ldHQubm8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4tn70 ..... LINUb9IahTiM2wccb1QbVLvBwk9f4wDOGQUO9H/euWi9PBqwyK+0gjdn28GR/dSR WvuSpfnLnR6e3wEDAgMBAAGjggFpMIIBZTAfBgNVHSMEGDAWgBQMvZNoDPPeq6NJ ays3V0fqkOO57TAdBgNVHQ4EFgQUJ0EwdzpCfPlnZlCh6dEq/Lsd73MwDgYDVR0P -----END RSA PRIVATE KEY----- -----BEGIN CERTIFICATE----- AQUFBwMCMBgGA1UdIAQRMA8wDQYLKwYBBAGyMQECAh0wOgYDVR0fBDMwMTAvoC2g K4YpaHR0cDovL2NybC50Y3MudGVyZW5hLm9yZy9URVJFTkFTU0xDQS5jcmwwbQYI ..... U1NMIENBMB4XDTEwMDUxMjAwMDAwMFoXDTEzMDUxMTIzNTk1OVowQzELMAkGA1UE BhMCTk8xEzARBgNVBAoTClVOSU5FVFQgQVMxHzAdBgNVBAMTFnJhZGl1cy10ZXN0 LnVuaW5ldHQubm8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4tn70 -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw+NIxC9cwcupmf0booNd ij2tOtDipEMfTQ7+NSUwpWkbxOjlwY9UfuFqoppcXN49/ALOlrhfj4NbzGBAkPjk tjolnF8UUeyx56+eUKExVccCvaxSin81joL6hK0V/qJ/gxA6VVOULAEWdJRUYyij ..... ays3V0fqkOO57TAdBgNVHQ4EFgQUJ0EwdzpCfPlnZlCh6dEq/Lsd73MwDgYDVR0P AQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG AQUFBwMCMBgGA1UdIAQRMA8wDQYLKwYBBAGyMQECAh0wOgYDVR0fBDMwMTAvoC2g -----END CERTIFICATE-----	Private key Certificate issued by TERENA Certificate issued by Comodo UserTrust

If you wish to verify the authenticity of the partial certificates from TERENA or Comodo, you must divide these into separate files (for example "partcertificate.pem") and then run the command:

```
openssl x509 -noout -text -in partcertificate.pem
```

The following is an example of the output obtained when this command was run for a TERENA partial certificate valid for the server called "radius-test.uninett.no":

root@sirius:~/tmp$ openssl x509 -noout -text -in test.pem Certificate: Data: Version: 3 (0x2) Serial Number: 52:75:c4:ea:b2:96:a3:04:96:23:6e:60:b0:52:f1:67 Signature Algorithm: sha1WithRSAEncryption Issuer: C=NL, O=TERENA, CN=TERENA SSL CA Validity Not Before: May 12 00:00:00 2010 GMT Not After : May 11 23:59:59 2013 GMT Subject: C=NO, O=UNINETT AS, CN=radius-test.uninett.no Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:b8:b6:7e:f4:83:54:34:bc:c5:38:ec:f8:2d:cf: ee:b1:1d:1b:f0:41:7a:fc:0a:71:c2:e0:fc:85:de: e9:cb:ed:8d:fa:06:b6:70:44:3e:8a:7f:fc:f3:b1: 20:f4:65:cf:f5:86:cd:12:0f:55:76:df:83:10:7a: f7:66:9a:17:f0:5a:15:02:81:21:5c:8f:13:d6:f5: 48:d6:15:84:bb:41:1c:06:9a:e9:1c:bf:da:2d:7a: 50:e9:12:4d:84:20:71:4e:a9:9c:66:63:db:70:ec: 32:36:60:c1:a0:10:53:2d:73:90:b7:bd:79:a5:08: 58:78:6b:00:26:66:c1:5d:c7:d9:71:c6:c3:a3:5e: 50:df:69:d3:0a:5f:7c:9e:4a:3a:53:74:7a:2c:d7: c1:83:b9:05:53:f5:38:ed:2a:70:2d:dc:2d:34:a2: ce:09:4d:1c:11:6b:04:44:25:ba:a2:46:09:23:e4: 86:4e:2c:83:54:6f:d2:1a:85:38:8c:db:07:1c:6f: 54:1b:54:bb:c1:c2:4f:5f:e3:00:ce:19:05:0e:f4: 7f:de:b9:68:bd:3c:1a:b0:c8:af:b4:82:37:67:db: c1:91:fd:d4:91:5a:fb:92:a5:f9:cb:9d:1e:9e:df: 01:03 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Authority Key Identifier: keyid:0C:BD:93:68:0C:F3:DE:AB:A3:49:6B:2B:37:57:47:EA:90:E3:B9:ED X509v3 Subject Key Identifier: 27:41:30:77:3A:42:7C:F9:67:66:50:A1:E9:D1:2A:FC:BB:1D:EF:73 X509v3 Key Usage: critical Digital Signature, Key Encipherment X509v3 Basic Constraints: critical CA:FALSE X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.6449.1.2.2.29 X509v3 CRL Distribution Points: URI:http://crl.tcs.terena.org/TERENASSLCA.crl Authority Information Access: CA Issuers - URI:http://crt.tcs.terena.org/TERENASSLCA.crt OCSP - URI:http://ocsp.tcs.terena.org X509v3 Subject Alternative Name: DNS:radius-test.uninett.no Signature Algorithm: sha1WithRSAEncryption 52:80:07:f2:9b:a5:50:f2:e3:43:4c:cd:5c:41:0c:96:cd:56: 21:10:c9:e6:a9:2a:fe:44:ae:a9:bc:77:5c:c8:d3:f4:59:30: 2e:a6:56:09:a3:2e:3f:3e:e7:09:cd:a1:c1:2e:d0:56:7d:b2: a7:eb:f0:e7:92:df:10:3b:26:89:36:34:b5:b3:e2:b0:52:db: 9e:22:1e:a8:fe:36:b2:24:cd:a4:33:e2:63:24:2d:aa:4d:de: 9c:fa:8a:fe:34:b3:42:2b:26:fa:2b:c9:f4:9f:87:1e:ad:54: db:bc:0f:a6:b3:de:57:02:19:cf:1d:7c:bd:58:e0:41:2e:65: 44:81:2b:66:53:49:2f:f0:18:1e:54:d6:3a:9a:2e:87:08:b6: 9c:a7:78:04:85:19:ba:4d:ac:ed:b3:d2:9d:d7:00:21:53:44: 5c:2f:29:8b:ab:d5:28:c6:bb:4a:34:c4:f2:45:fb:5b:14:e7: 75:b4:d8:79:28:f0:1b:9b:60:38:2f:c2:99:00:f8:9f:d7:34: 1c:0c:59:e9:58:35:36:a3:f0:36:e9:c3:be:6a:1b:c5:9b:6c: a1:46:20:ff:9b:64:68:a3:65:7f:ac:05:4a:05:9a:7e:5f:11: 44:a1:25:fe:0c:ce:6f:da:52:12:c5:5g:d9:e0:23:fa:60:f8: c2:f1:18:72	TERENA is the issuer Duration The server certificate has been issued to the server “radius-test” Public key Signature

References

[1] UFS112: Recommended Security System for Wireless Networks. Implementation of IEEE 802.1X. Jardar Leira, UNINETT. 20/12/2007.

[2] “eduroam cookbook”: GEANT2 Deliverable DJ5.1.5,3: Inter-NREN Roaming Infrastructure and Service Support Cookbook - Third Edition. 29/10/2008. Found at www.eduroam.org.

[3] Airmagnet Survey: http://www.airmagnet.com/products/survey/
Airmagnet Planner: http://www.airmagnet.com/products/planner/
Airmagnet Spectrum Analyzer: http://www.airmagnet.com/products/spectrum_analyzer/

Glossary

CAPWAP	Control And Provisioning of Wireless Access Points protocol, defined in RFC5415
CLI	Command Line Interface
LA	Cisco Location Appliance. Optional software application which provides location services.
LAP	Lightweight Access Point
LWAPP	Lightweight Access Point Protocol
MSE	Mobility Service Engine
SFP	Small form-factor pluggable transceiver or “mini-GBIC” (for Gbit Ethernet)
SSID	Service Set Identifier
WCS	Cisco Wireless Control System. Software for the administration of WLCs
WiSM	Cisco Wireless Services Module. Plug-in card for Cisco Catalyst 6500 containing two Cisco 4404 wireless controllers
WLC	Cisco Wireless LAN Controller
WMM	The Wi-Fi Alliance’s Wi-Fi Multimedia™ certification programme for multimedia properties.

Ved spørsmål omkring denne eller andre UFSer – kontakt campus@uninett.no
Andre UFSer er tilgjengelige på www.uninett.no/ufs