Implementation of IEEE 802.1X in wired networks

Best Practice Document

Produced by UNINETT led working group on security (UFS 133)

Authors: Øystein Gyland, Tom Myren, Rune Sydskjør, Gunnar Bøe

March 2013

Document No: GN3-NA3-T4-UFS133
Version / date: 18.03.2013
Original language: English
Original title: “Anbefalt sikkerhetsløsning for IEEE 802.1X i kablet nettverk”
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 campus networking as part of a joint-venture project within the HE sector in Norway.

The research leading to these results 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

1 Background

Ensuring the security of wired networks where physical access to outlets is unrestricted is resource-demanding and IEEE 802.1X is the most elegant solution in this respect. IEEE 802.1X is a layer 2 protocol that enforces user or machine authentication. Typically a port is closed to most types of traffic until the connected user or machine has been authenticated. The switch will forward EAPoL traffic between the supplicant (machine) and the RADIUS server.

2 Introduction

This document provides information about configuring IEEE 802.1X in wired networks. The recommendation is generic but includes instructions for vendor-specific configuration of some switches. General configuration of switches is described in [UFS 105] “Recommended Configuration of Switches in Campus Networks”.

This document describes the use of IEEE 802.1X in switched, wired networks. The reason for using 802.1X authentication is the desire to maintain control of which machines and users are able to access the network. This solution has been implemented for some time in wireless networks and detailed information about configuring a RADIUS server and about how IEEE 802.1X functions can be found in [UFS 112] “Recommended Security System for Wireless Networks”. IEEE 802.1X has not been used to the same extent in wired networks, but with increasing focus on security and new threats there is a need to exercise better control. Several universities/colleges in Norway have long experience with using IEEE 802.1X authentication in wired networks.

[UFS 122] “Recommended ICT Security Architecture in the Higher Education Sector”, which introduces security zones, provides recommendations for how IEEE 802.1X authentication should be used.

IEEE 802.1X is very flexible, facilitating dynamic VLAN allocation, client checks and simple use of quarantine vlans.

3 The elements of IEEE 802.1X

In IEEE 802.1X, three parties are involved in the authentication process; the supplicant (on the client machine), the authenticator (the switch) and the authentication server (RADIUS). In addition there is usually a user database in a directory server (LDAP/AD/SQL) to which RADIUS refers. If eduroam (802.1X in a wireless network) is already in use, the RADIUS and directory servers can be re-used.

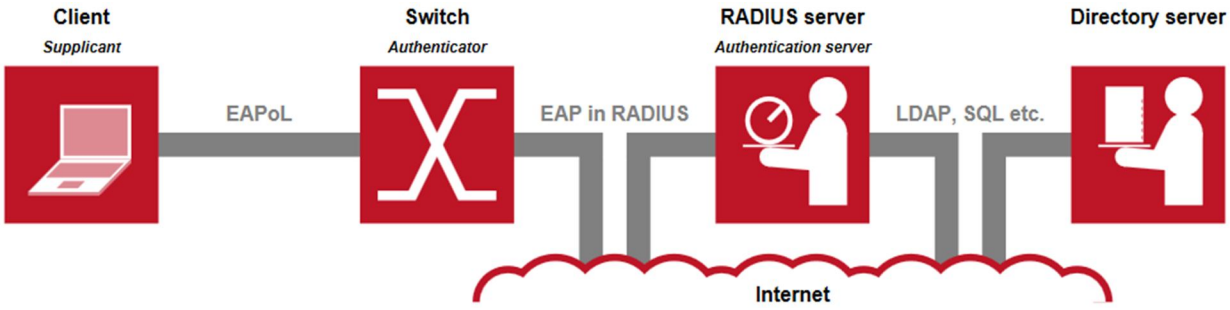


Figure 1: The elements of IEEE 802.1X

When connecting to an IEEE 802.1X activated switch, this will (if the client is configured for 802.1X) forward EAPoL traffic to the RADIUS server. If a client without 802.1X configuration or functionality is connected to the network, the switch configuration will determine what access the client will be granted. This may be no network connectivity at all; i.e. the switch port shuts down, or as we recommend, the switch port is assigned to a VLAN with restricted access. Such restriction can be achieved by means of access lists or a firewall, and may vary depending on what the current security policy is. For example, only Internet access may be granted or only access to certain parts of an internal network.

IEEE 802.1X is based on mutual authentication between client and RADIUS server. The client may authenticate using a username and password or a certificate. The RADIUS server *must* authenticate using a certificate. It is possible to use 802.1X without the client checking the validity of the server certificate or the name of the certificate; however this is *not* a recommended solution. See the descriptions of RADIUS server and client authentication below.

3.1 Certificate authentication of the RADIUS server

The purpose of this is to enable the client to verify that it is communicating with the correct RADIUS server. Authentication is initiated either by the supplicant or by the authenticator when the client connects to the network. The RADIUS server will send its certificate to the supplicant by way of an authenticator before authentication of the user or machine takes place. The client must have previously installed the public certificate of the certification authority (CA) that has issued and signed the RADIUS server's certificate. This may be distributed using e-mail, a web page or a management system such as AD. The client checks the validity of the RADIUS server's certificate using the CA certificate. Since CA certificates often are pre-installed on many clients, the client should also check the name of the certificate. Using a certificate from local CA, rather than certificates from a larger, commercial CA, also reduces the possibility of phishing.

3.2 User authentication

This can be achieved using one of the following options:

- Personal certificate (EAP-TLS)
- User name and password (EAP-TTLS or EAP-PEAP with MSCHAPv2 is recommended).

Authentication in this context is identical with the authentication which takes place when using eduroam (802.1X in wireless networks), see [UFS 112] "Recommended Security Solution for Wireless Networks".
In contrast to machine authentication, user authentication can be used for privately-owned machines and other machines that are not a natural part of the IT department's operational setup. User authentication can be done with the same RADIUS server as for machine authentication. Configuration of the machine may be challenging, particularly if the user himself has to setup 802.1X on his own machine. This document includes configuration examples of the most common clients for user authentication.

3.3 Machine authentication

Machine authentication is most often used for Windows machines enrolled in AD, but can also be used for Mac and Linux clients. As with user authentication either EAP-TLS (machine certificate) or EAP-PEAP (the machines AD name and password) is used for machine authentication. If one chooses to use EAP-TLS a certificate can be issued to the machine on enrolling in a domain (auto-enrolment). Configuration can be arranged at initial install so that the machine is prepared for IEEE 802.1X without the user needing to do any configuration later. Machines enrolled in AD can receive updates and be remotely administered, even if the user is not logged in. A user can login locally on his machine, in the same way as when 802.1X is not in use. In Windows it is possible to utilise machine authentication and/or user authentication. This would provide a possibility to assign different VLAN's depending on what type of authentication that was performed. We have seen some reported problems getting renewed IP address and/or gateway when a client is machine authenticated, and then moves to another VLAN due to user authentication. This functionality has so far not been tested at UNINETT.

Machine authentication simplifies operational administration and is the recommended solution in combination with user authentication.

More information about the setup of policy using Windows NPS for machine authentication is available from Microsoft Technet [TECHNET].

4 RADIUS

All modern RADIUS servers support IEEE 802.1X. This includes FreeRADIUS and the different Windows variants that are most commonly used in the HE sector in Norway. If eduroam is already in operation, the same infrastructure can be used.

Using RADIUS, the following can be achieved:

- Dynamic VLAN allocation
- Connection to AD/LDAP/local user database, etc.
- RADIUS proxy with hierarchical solutions such as eduroam.

If eduroam has already been set up, it is recommended to use the same RADIUS server with an additional configuration that assigns user groups to separate VLANs (student, researcher, administration, etc.). The RADIUS server can distinguish wired clients from eduroam clients based on the origin of the RADIUS enquiry (using NAS-Identifier or NAS-IP-Address attribute). For best possible uptime it is recommended to have a redundant RADIUS and user database solution, and when possible also provide site redundancy.

4.1 Troubleshooting

- In FreeRADIUS: `radiusd -X` provides large amounts of information and is therefore not suitable in a production environment. The accounting logs may contain useful information.
- Use a Linux machine as an authenticator (cf. figure 1): `eapol_test` is a program which accompanies `wpa_supplicant` and communicates directly with the RADIUS server. `eapol_test` provides a lot of information and is a useful tool for testing and troubleshooting
- On a Linux client: `wpa_supplicant -dd` provides a lot of useful debug information.

5 Network Configuration

“All” modern switches support IEEE 802.1X, but their functionality varies. Several clients behind the same switch port (a small non-802.1X switch or PC connected to SIP phone) can be a challenge in combination with 802.1X. Solutions for such setups are not part of this recommendation.

5.1 Cisco switches

Cisco IOS modified the syntax for configuration of IEEE 802.1X in version 12.2.50. For information about earlier versions, see Cisco’s documentation. The following is a good example of a minimum configuration (assuming IOS ≥ 12.2.50)

Global configuration:

```
aaa new-model
aaa group server radius radius-dot1x-group
server-private <host> auth-port 1812 acct-port 1813 key <key>
!
aaa authentication dot1x default group radius-dot1x-group
dot1x system-auth-control
! For dynamic Vlan assignment:
aaa authorization network default group radius-dot1x-group
```

Per interface configuration:

```
switchport mode access
switchport access vlan XX        ! if not using dynamic VLAN assignment
authentication port-control auto
dot1x pae authenticator
```

Additional configuration to provide a guest network for machines without dot1x and in the event of errors:

Global configuration:

```
dot1x guest-vlan supplicant
```

Per interface configuration:

```
authentication event fail action authorize vlan <vlan-nr>
authentication event server dead action authorize vlan <vlan-nr>
authentication event no-response action authorize vlan <vlan-nr>
authentication event server alive action reinitialize
```

If it is not necessary to authenticate or if authentication fails it may take a long time before the switch grants access to the network. This may be due to high default values. We recommend adjusting default timers to speed up the process.

The following are some examples of timeout parameters which may be altered:

```
dot1x timeout quiet-period <sec>   ! default value 60
dot1x timeout tx-period <sec>      ! default value 60
dot1x timeout supp-timeout <sec>   ! default value 60
```

Detailed documentation of these parameters can be found on Cisco's website.

5.1.1 Troubleshooting Cisco switches

- `debug dot1x (events,all,packets)` is generally unsuitable in an environment where many users are connected, because of the large amount of information which is output on the terminal and the lack of filtering possibilities. If used, the output should be read on a log server, not in CLI.
- `sh dot1x interface XX/YY detail` provides an overview of whether IEEE 802.1X authentication is switched on and the status of the authentication (fault, in progress, etc.).

5.2 HP switches

The following is an example of a minimum configuration:

```
aaa authentication port-access eap-radius
aaa accounting network start-stop radius
radius-server host <ip-addr> key <key>
```

Provides support for dynamically allocated VLAN:

```
aaa port-access gvrp-vlans
```

Specifies which ports shall have dot1x authentication:

```
aaa port-access authenticator <port-range>
aaa port-access authenticator <port-range> auth-vid <vlan-nr>
aaa port-access authenticator <port-range> unauth-vid <vlan-nr>
aaa port-access authenticator <port-range> logoff-period 60
aaa port-access authenticator active
```

5.2.1 Troubleshooting HP switches

- `show port-access authenticator clients` returns the status of authentication of the ports.
- `debug security port-access authenticator` is also useful.

6 Client-specific elements

Modern operating systems provide built-in IEEE 802.1X client support.

The recommended configuration for all types of clients is the distribution of client profiles by a central management system, where AD is one of several options. The text below explains how an 802.1X profile can be configured on the most common clients.

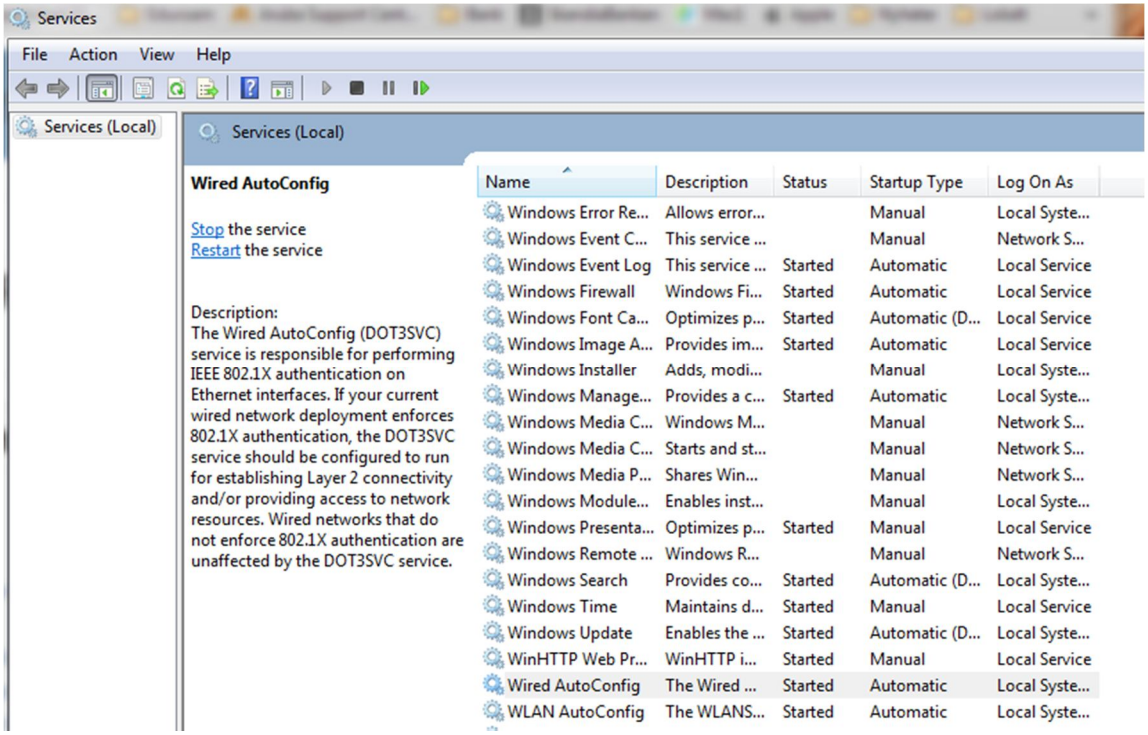
Some potential challenges should be mentioned:

- Several operating systems have varying configurations for different software versions:
    - Apple: 10.5 (Leopard), 10.6 (SL), 10.7 (Lion), 10.8 (ML) all have different configurations.
    - Windows: XP, Vista, Windows 7, Windows 8 also have different configurations. We do *not* recommend using 802.1X on earlier versions then Windows 7.
    - Linux and FreeBSD have several different supplicants.
- The introduction of IEEE 802.1X requires user support personnel to have detailed knowledge of several operating systems.

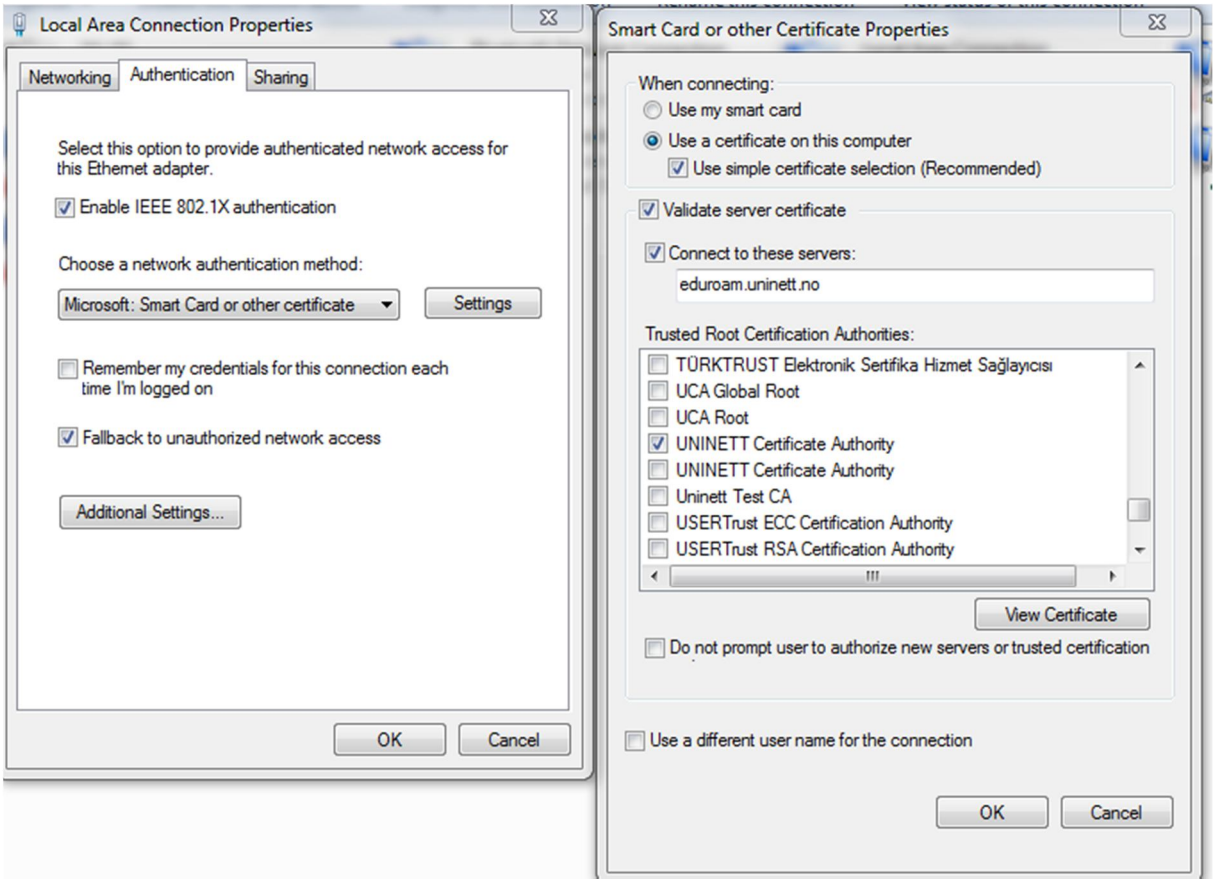
6.1 Windows

We recommend IEEE 802.1X authentication only on Windows 7 or later versions. The following is an example of manual client configuration in Windows 7. Note that this is best performed by means of auto-enrolment from AD, without user involvement.

Start “Services” and under the properties for “Wired AutoConfig”, set the “Startup Type” to “Automatic”. Then start the service. See the figure below:



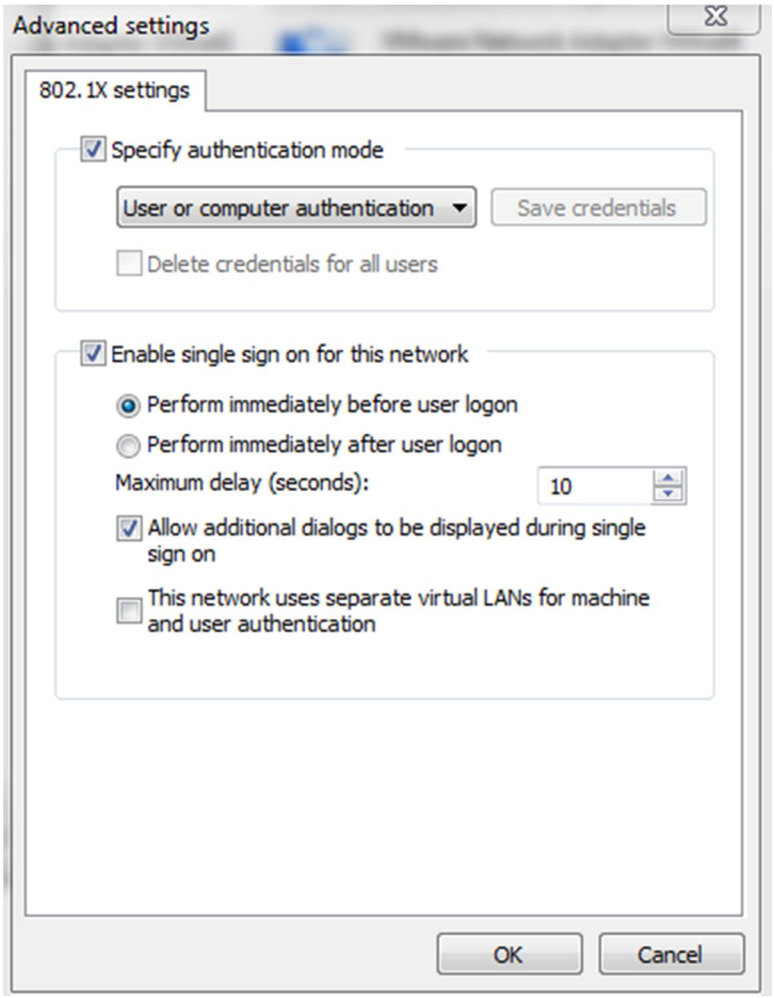
- Now go to Control Panel → Network and sharing center → Change adapter settings.
- Right-click on the appropriate “Local Area Connection” and then select “Properties”.
- Now go to the “Authentication” tab which appeared after Wired AutoConfig was started.



- 802.1X is activated here. Specify the authentication method “Smart Card or other certificate” (TLS), or PEAP.

- Under “Settings”, select a certificate (machine authentication) as well as validation of server certificate. Note that a client machine certificate is required if this is to work as described for machine authentication. The example above shows how authentication is performed against the same RADIUS-server as for eduroam clients (eduroam.uninett.no).

- Under “Additional Settings”, the 802.1X authentication can be specified in more detail:



This menu provides a possibility for combining machine and user authentication.

If the authentication takes so long that the DHCP request times out, the machine will be left with a 169.254.0.0/16 non-routable, link local address, even if the authentication was successful. The machine will after a while send a new DHCP request and then get a correct IP address.
The simplest way to restart authentication is to disconnect and reconnect the network cable.

If one would like to configure 802.1X authentication on older Windows clients, detailed information can be found on Microsoft’s website [MS-VISTA].

6.2 Mac

As of Mac OS X 10.7 Lion, Apple limited the possibilities for configuring 802.1X authentication locally on the machine. The 802.1X tab is still displayed under Network Configuration but only provides a possibility of viewing 802.1X profiles or selecting one if several are available. It is still possible to connect to the 802.1X network manually.

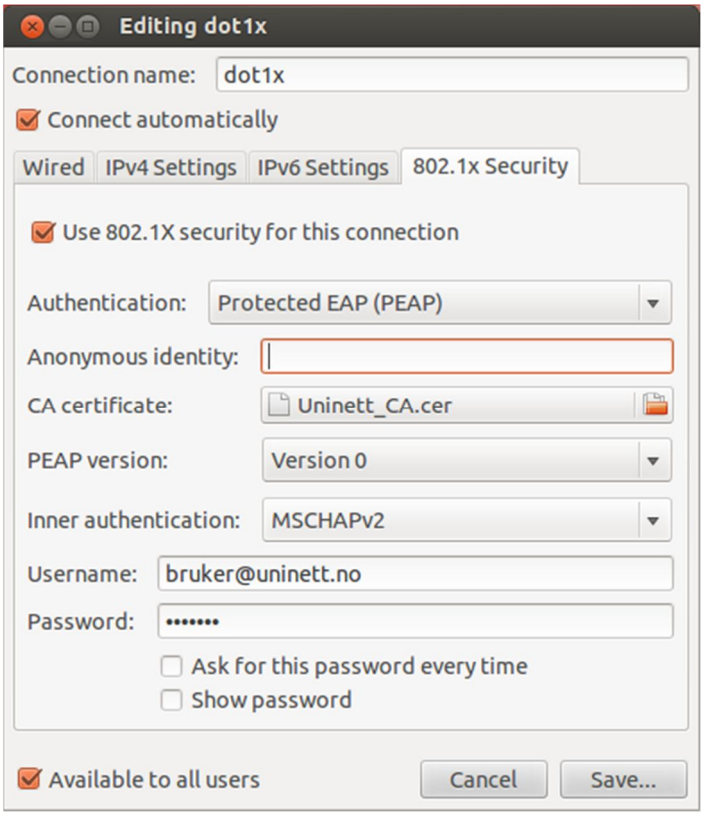
- When connecting to an 802.1X-activated port for the first time, the user will be prompted to accept the RADIUS-server's certificate and thereby save it. An obvious weakness is that the user can far too easily accept an invalid server. The user is then asked for a user name and password, and the profile is created on the machine. This is not a recommended method.

- It is also possible to use iPCU (iPhone Config Utility) to create a profile that is distributed to users. A profile may be defined for a single user or for a user group. It is important to specify the CA certificate of the RADIUS server (it accompanies the profile) and the name of the Trusted Server Certificate and *not* check "Allow Trust Exception". The profile is created in a `.mobilconfig` file (XML format) which is run on the client.

iPCU is available from Apple for both Windows and Mac, cf. [APPLE].

6.3 Linux

The following is an example of configuration of a Linux client using Network Manager:



6.4 Machines without support for IEEE 802.1X

A guest VLAN can be offered to devices that do not support IEEE 802.1X. In other words, fall-back to a VLAN with limited connectivity. This is recommended as a standard configuration. Refer to the configuration examples given for switches.

7 Alternatives to IEEE 802.1X

There are alternatives to using 802.1X in wired networks, but these have a several weaknesses. The most likely alternatives are:

- **MAC address lists** – Only clients with an approved, registered MAC address can connect to the network. This involves a very demanding maintenance regime and provides no real security improvement since MAC addresses are easy to forge.

- **Port security** – With port-security you can limit the number of MAC addresses for each port. The MAC addresses can be learnt dynamically or set statically. This gives no verification of each machine, but normally only corporate machines will be allowed as long as the number of MAC addresses are limited. However as with MAC address lists MAC addresses can be spoofed. And there will be some operational administration, for example when a port is shut down or if you want to block a port.

- **Web portals** – This method is commonly used in publicly accessible networks. Initially all services are blocked and the user is redirected to a web page to log on. Authentication can be protected by means of communication via TLS. This provides mutual authentication of the system and client via TLS, but in reality it is too easy for a user to ignore warnings of errors in certificates or whether TLS is being used at all. This makes it easy for an attacker to set up a false web portal. This solution may work as a public guest access to the network, but when used daily, it is not very user-friendly.

- **VLAN** – A VLAN in itself provides no client authentication but at least ensures the separation of different subnets/zones.

- No security.

Conclusion: Only IEEE 802.1X authentication provides adequate security when one wants to control which clients and users have access to the network.

References

[APPLE] http://www.apple.com/support/iphone/enterprise/

[MS-VISTA] http://windows.microsoft.com/en-GB/windows-vista/Enable-802-1X-authentication

[RAD-DB] Best Practice Document on “FreeRADIUS Database Connection”
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-freeradius-db.pdf

[RAD-AD] FreeRADIUS integration with AD
http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO

[TECHNET] http://technet.microsoft.com/en-us/library/hh831813.aspx#BKMK_ETLS

[UFS105] Recommended configuration of switches in campus networks
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs105.pdf

[UFS109] Cookbook for configuring Cisco IOS switches in campus networks (in Norwegian)
https://openwiki.uninett.no/gigacampus:ufs109

[UFS112] Recommended Security Systems for Wireless Networks
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs112.pdf

[UFS122] Recommended ICT Security Architecture in the Higher Education Sector
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs122.pdf

[UFS127] Guide to configuring eduroam using a Cisco wireless controller
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs127.pdf

Glossary

AD	Active Directory
CA	Certificate Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EAP-PEAP	EAP - Protected Extensible Authentication Protocol
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunnelled Transport Layer Security
HE	Higher Education
IEEE 802.1X	Authentication mechanism for wired and wireless networks.
iPCU	iPhone Config Utility
LDAP	Lightweight Directory Access Protocol
MAC	Media access control
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
NAS ID	Network Access Server IDentifier
NPS	Network Policy Server
PAE	Port Access Entity
RADIUS	Remote Authentication Dial In User Service; protocol for authentication, authorisation and accounting. Used between switch and RADIUS server.
SQL	Structured Query Language
XML	Extensible Markup Language

Complete BPDs available at www.terena.org/campus-bp/

campus-bp-announcements@terena.org