VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Qian Yang

802.1X AUTHENTICATION AND AUTHORIZATION IN WIRED NETWORK

Technology and Communication
2010

FOREWORD

This thesis is aimed to design a port-based authentication and authorization in wired network system by IEEE 802.1X. Supplicant needs to communicate with RADIUS server (authentication and authorization server) via authenticator and gets result from RADIUS server.

After four months hard work, I finally finished this project. During the configuration and implementation progress, I really learned a lot, like did many researches, found mistakes and solved problems.

First of all I have to appreciate my parents. They are my solid support.

Then I would like to thank Mr Antti Virtanen and Mr Hannu Teulahti, they were my supervisor and technology support. They helped me to solve a lot of problems and gave me lots of useful comments.

Finally I would like to thanks all the teachers in VAMK and all my friends with me during these four years.

Vaasa, 1 June 2010

Qian Yang

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Degree Programme of Telecommunication Engineering

ABSTRACT

Author	Yang Qian
Title	802.1 X Authentications and Authorization in Wired Network
Year	2010
Language	English
Pages	47
Name of Supervisor	Antti Virtanen

This project is mainly to build a port-based authentication and authorization in wired network system. Here I took HP switch as the authenticator; VAMK's NPS as authentication server; and Window XP PC as a client.

The method is to install 802.1X supplicant software on client; use PUTTY to configure Authenticator; use IDM to do RADIUS server configuration. The essence is to make authenticator communicates with RADIUS server.

Now the whole authentication and authorization system is working fine, each user plugging to an authenticator is required to login, and then authentication server will give response, and the user will pass or fail. Authorized supplicant will get correct IP address according to its membership; unauthorized supplicant and guest will be forced to the GUEST VLAN.

This project is a good 'shot' in network authentication area. In the future, 802.1X will play a significant role in the rapid development high-tech era.

Keywords 802.1X, Authentication, port-based

ABBREVIATIONS

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
AD	Active Directory
CHAP	Challenge Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
EAP-MD5	EAP Message Digest 5
EAP-OTP	EAP One Time Password
IDM	Identity Driven Manager (ProCurve)
IEEE	Institute of Electrical and Electronics Engineers
LAN	IEEE 802 Local Area Network
MAC	Media Access Control
NPS	Network Policy Server
PACP	Port Access Control Protocol
PAE	Port Access Entity
PAP	Password Authentication Protocol
PPP	Point to Point Protocol
PUTTY	A free TELNET/SSH client
RADIUS	Remote Authentication Dial in User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
VLAN	Virtual LAN
WEP	Wired Equivalent Privacy

CONTENTS

1 Introduction

1.1 Introduction of port-based access protocol

IEEE 802.1X is very simple in concept. Its purpose is to implement access control at the point at which a user joins the network. IEEE802.1X protocols configuration is in order to provide a means of authenticated and authorized devices which are physically attached to the LAN infrastructure and preventing the access which are unauthenticated. It focuses on the ports open or close, for the authenticated users, ports open; otherwise, ports are closed.

After authorization, the client will be assigned to a specified VLAN according to the VLAN membership it belongs to no matter which port it physically connects to the network.

1.2 Purpose of this project

This project is to build a secure port-access wired network system.

To implement this project, three main tasks should be achieved:

Basic configuration for HP ProCurve switches needs to be done at first.

Integrate 802.1X authentication to Windows AD domain. With 802.1X authentication; devices need to send their domain accounts and passwords for authenticating when they have a port-to-port connection with LAN infrastructure.

Then the IDM and putty will be needed to do the VLANs dynamic assignment and allow the network access according to the username and group, by this way, 802.1X VLAN assignments can provide secure data separation. It is like the users from different groups can connect to any port on any edge of switch, and be assigned to the VLAN appropriate to their groups at once and they will always

have access to the same set of network resources. Here will have a GUEST VLAN for the unauthorized clients as well as some guest users without a domain account, but the resources are quite limited.

2 Why 802.1 X is needed

2.1 Background

Port-based Access Control is one of the most important elements of security. The current authentication system in wired network of VAMK focuses only on the domain users, which is not able to prevent any unauthenticated access by the device (laptop, printer, telephone) having a physical connection. Any user can access its wired network and has unlimited internet bandwidth if it connects to the switch with one network cable, network administrator even can not control those users at all [7].

Port-access control can fix this shortcoming. Configure IEEE 802.1X in school's system can provide security on the "edge" of a network; it can protect VAMK's network and switches from unauthorized access as well. The devices which are not in VAMK domain will be asked username and password to login the wired network, only the authenticated ones can access the network. So 802.1X authentication will be more secure than the current authentication system.

2.2 Objectives

The objectives of this project are to configure the 802.1X in the target switches and active 802.1X authentication/authorization in VAMK's network system.

Then VAMK's network will prevent all the unauthorized access upon I make this project work. And the authorized users will be assigned to the specified VLAN according to the groups they are belonging to. It means the network can control which VLAN user can go, restricting to access resources according user's profile [1].

3 The overview of 802.1X standard

3.1 What are 802.1 X?

In June 2001, IEEE adopted 802.1X as access management protocol standard. Figure 1 show a picture extracted directly from the IEEE 802.1X White Paper illustrating the relationships among the entities [1].

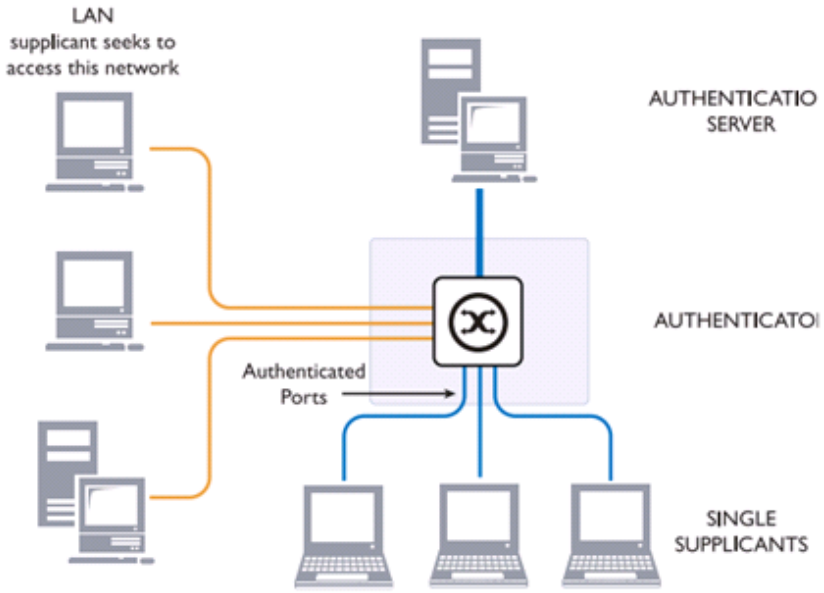

Figure 1: The 802.1X system [1].

802.1X is the IEEE standard for Port-based network access control; it authenticates and authorizes devices physically attached to a LAN and requests the login details, and prevents the access in case the authentication fails [7].

3.2 Why was 802.1X developed?

IEEE 802.1X originated in 802.11 protocols, and it designed to adapt the following requirements [1]:

Public Network Security;

Network Control Right at the Port Level;

Authentication, Authorization, Accounting;

Distribution of Dynamic Encryption Key (WEP)

3.3 The main elements of 802.1X

You can see the main elements of 802.1X and structure in Figure 1 above.

Client/Supplicant

The supplicant is a client that desires to access the network. Typically; a supplicant is a user workstation. Supplicant software is already implemented natively in some Microsoft Windows operating systems, like Windows XP, Vista and Windows 7, or can be downloaded and added to PC [1].

Port

A port is the point at which a client connects to the LAN infrastructure. The reason 802.1X called “port”-based authentication is the authenticator has two virtual ports, controlled port and the uncontrolled port, uses the same entity port attach to the LAN [8], as you can see in figure 2.

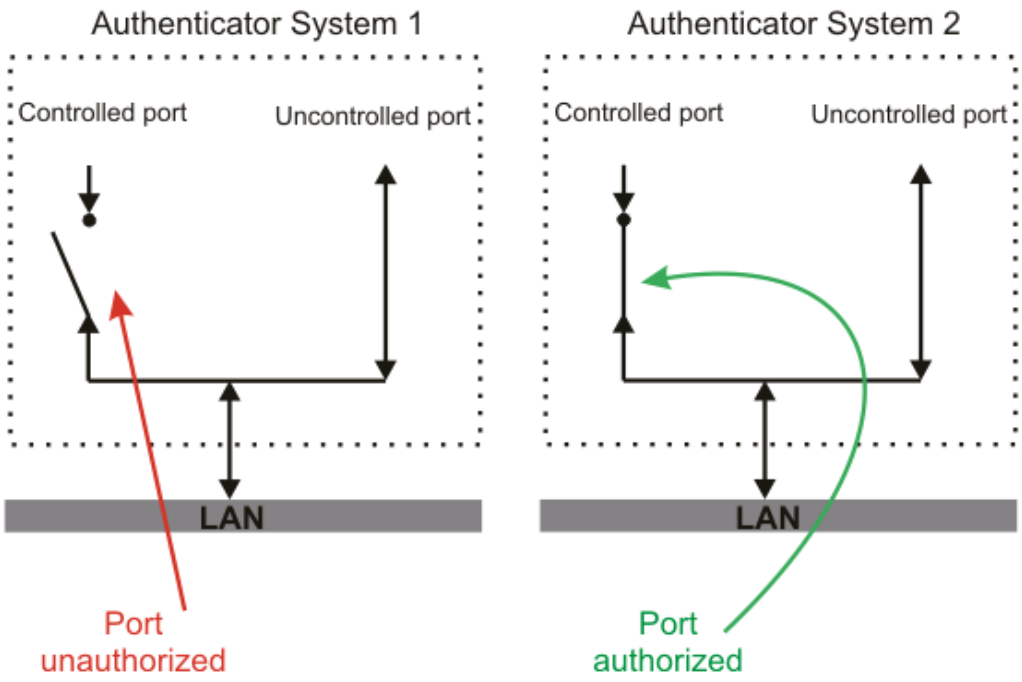

Figure 2: The authorization states of controlled port [8]

Please see the authentication system 1 in Figure 1, before authentication, only the uncontrolled port is open which only allows EAPOL packet to go through; after authentication, you can find in authentication system 2 in Figure 2, the controlled port is open and which allows to access the network resources.

Authenticator

Authenticator is the one who works between supplicant and authenticator server, and provides the entry point for client into the network, normally it is the switch port. The authenticator requires the supplicant to provide 802.1X credentials, which are forwarded to the authentication server [1].

HP ProCurve can serve as authenticators. VAMK has changed most of switches to HP ProCurve 2910a1-24G and HP ProCurve 2910a1-48aG (Figure 3 and Figure 4).

Figure 3: HP ProCurve 2910a1-24G [6]

Figure 4: HP ProCurve 2910a1-48G [6]

For both HP ProCurve 2910a1-24G and HP ProCurve 2910a1-48G, Layer 2 switching: VLAN supporting and tagging; dynamic assignments of VLANs, layer3 routing: Static IP routing; RIP, security: Multiple user authentication method, like 802.1X; authentication flexible.

Authenticator will send the supplicants' submitted information to a suitable authentication server (RADIUS); it allows verification of user credentials to determine the consequent port authorization status. The switch acts as an intermediary (proxy) between the client and authentication server [6].

Authentication server (RADIUS)

The Remote Authentication Dial in User Service server, it based on client/server model. There are three components of RADIUS server, The first database "users"

used for storing user's information (e.g., username, password, and use of the agreement, IP address and other configuration), the second database "clients" used to store information (e.g. RADIUS shared key), the third Shared database "dictionary" to interpret the information stored in the agreement of RADIUS attributes and value of meaning. (Figure 5)

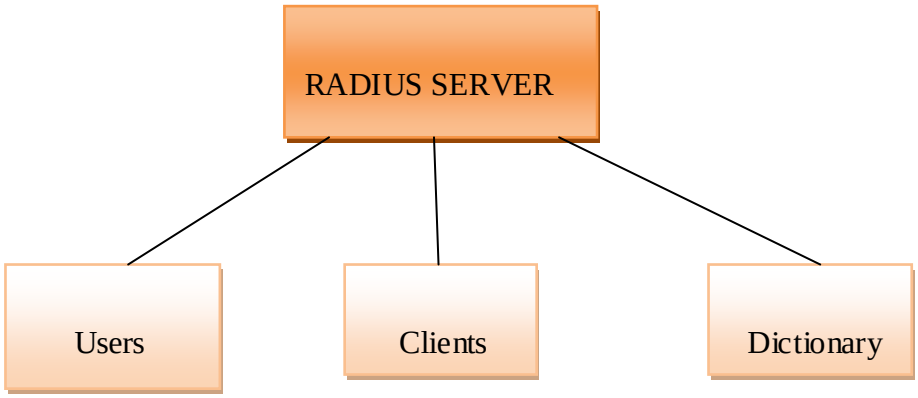

Figure 5: The components of RADIUS server

RADIUS server supports multiple authentication subscribers. When the subscriber's name and primitive password provided, RADIUS server can support point-to-point protocol (PPP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP) and other authentication mechanism. RADIUS server provides user identity verification, dynamic VLAN assignment, and central management and accounting information about how long was a user connected to the network [1].

EAP

EAP-Extensible Authentication Protocol is one of the most important elements in 802.1X authentication. It acts like an agent, to make the introductions and to close the deal [1].

There are five most widely used EAP types in Figure 6:

	Server Authentication	Supplication Authentication	Dynamic Key Delivery	Security Risks
EAP-MD5	None	Password Hash	No	Man-in-the-middle (MitM) attack, Session hijacking
LEAP	Password Hash	Password Hash	Yes	Identity exposed, Dictionary attack.
EAP-TLS	Public Key (Certificate)	Public Key (Certificate or SMART Card)	Yes	Identity exposed
EAP-TTLS	Public Key (Certificate)	CHAP, PAP, MS-CHAP (v2), EAP	Yes	MitM attack
PEAP	Public Key (Certificate)	Any EAP such as EAP-MS-CHAPv2 or Public Key	Yes	MitM attack; identity hidden in phase 2 but potential exposure in Phase 1

Figure 6: EAP types [1]

All EAP messages has a similar format (Figure 7)

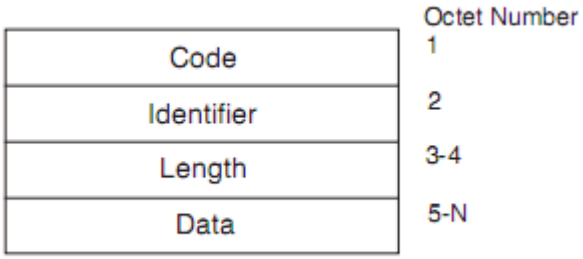

Figure 7: EAP messages format [7]

Code is one byte indicating the type of message:

- ✓ Request (01)

- ✓ Response (02)
- ✓ Success (03)
- ✓ Failure (04)

Identifier is in a range of 0-255; Length is a 16-bit value, which includes total number of bytes in EAP message (code and so on); Data is actual request or response data being sent [7].

There is an extra type field, which is used to identify the request and response (Figure 8).

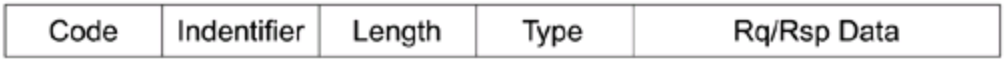

Figure 8: EAP request/response message format [9]

Here is an outline of Authentication sequence in figure 9

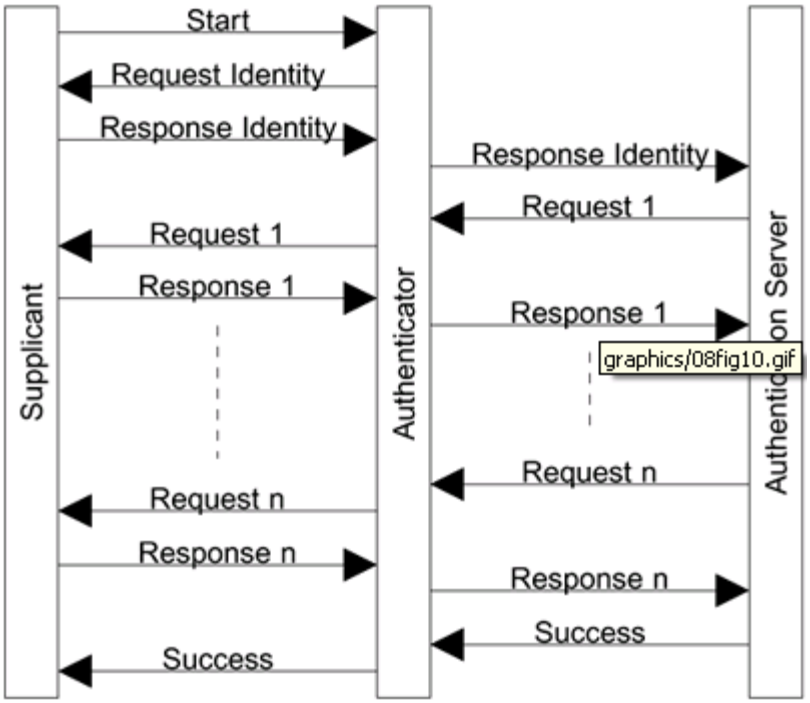

Figure 9: EAP Message Flow [9]

The supplicant first connect to the network port and desired to access, then authenticator first send request/response identity message to supplicant, after supplicant send a response message back, the authenticator need to contact with authentication server to find out whether the supplicant to be allowed in. The authentication server cannot make decision until it has verified the supplicant's identity correspond to the data stored in dictionary [9] .

EAPoL

Before the authentication, 802.1X only lets the EAPoL (Extensible Authentication Protocol over LAN) data to go through the switch port which the device connected to, after the authentication the normal data can be smoothly through the Ethernet port [1].

GUEST VLAN

Guest VLANs provide an attractive and feasible interim path to implementing a comprehensive 802.1X solution. Now anyone that is a visitor to our campus or other site that has active ports, can access GUEST VLAN to get special services which are specially set for them during their stay. And it also useful non-802.1X clients, the one without 802.1X supplicant software added on, or the one which does have 802.1X for its own home network, but which isn't registered on your RADIUS server. At the same time, private network kept secured.

If the 802.1X is enabled on a port and client fails to pass the 802.1X authentication or is not running the 802.1X supplicant software, the switch will do one of two things: block the client, or provide guest access. In Figure 10, the unauthorized clients went to the GUEST VLAN which only provides security services, like download 802.1X software and upgrade it from the GUEST VLAN server. The secured network is closed, only after the clients are authorized [5].

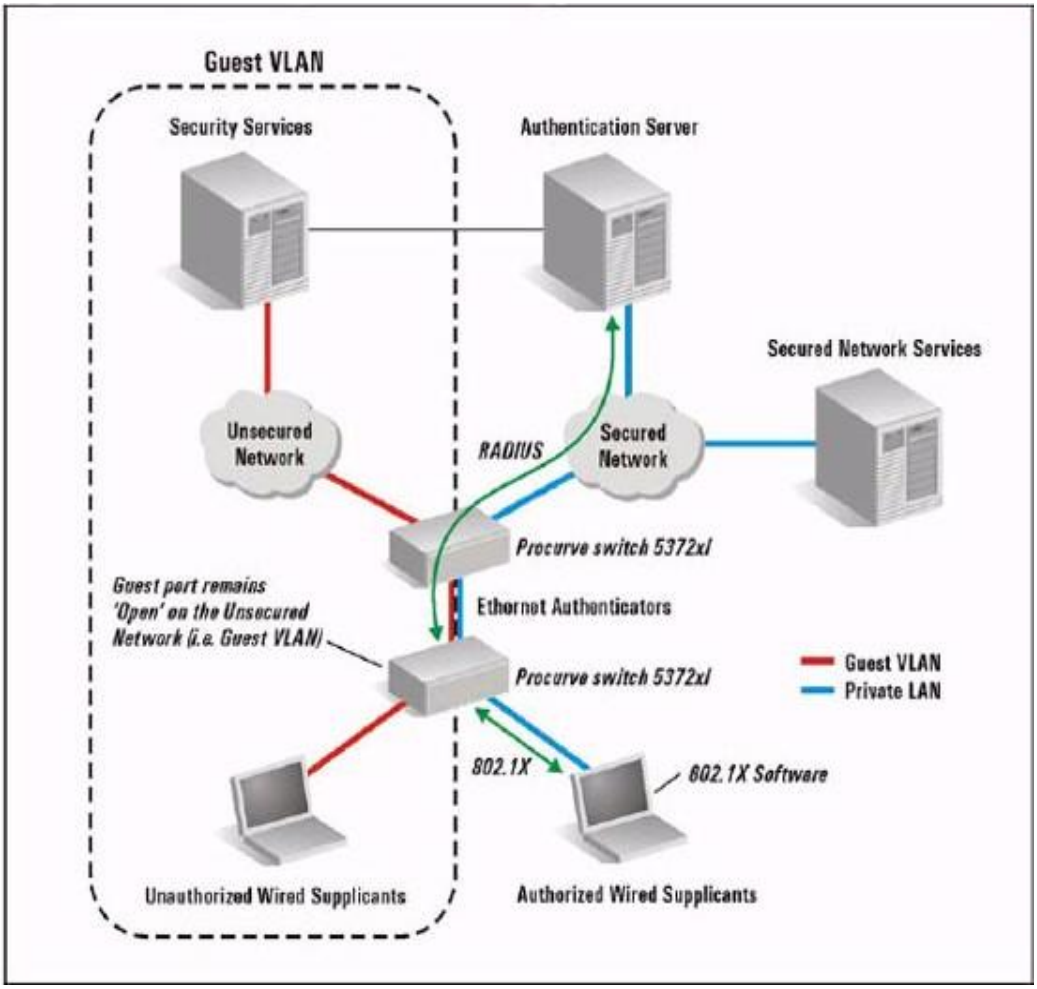

Figure 10: How GUEST VLAN works [5]

ProCurve IDM

ProCurve Identity Driven Manager (IDM) is an add-on module of ProCurve Manager Plus (PCM+) which extends the functionality of PCM+. It simplifies to configure the user's access by automatically discovering RADIUS server, user group and Realms. Using IDM you assign access rights and connection attributes at network switch; control RADIUS server, Web –Authentication, MAC-Authentication, 802.1X security protocols and VLAN dynamic assignment and monitor users on network. And you can see the RADIUS server for the IDM in Figure 11, host of the RADIUS server is 193.166.X.X. [4]

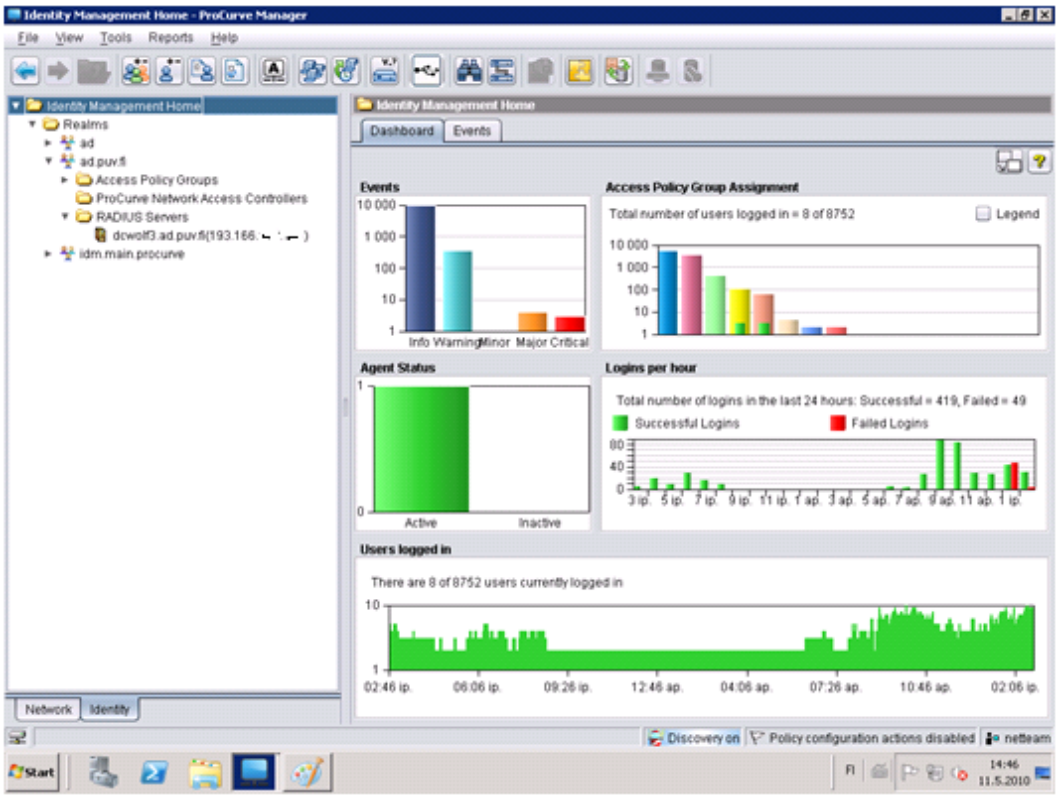

Figure 11: ProCurve Identity Driven Manager Home

3.4 Basic Process of 802.1X authentication

Read Figure 12, it illustrates on the general level of 802.1X authentication process and shows how the two virtual ports of authenticator work in the whole authentication process, which can combine with Figure 2. The uncontrolled port only used for forwarding the EAPOL packet to the RADIUS server. After authorized, the controlled port will get through the network; users can view the network resource (Figure 12)

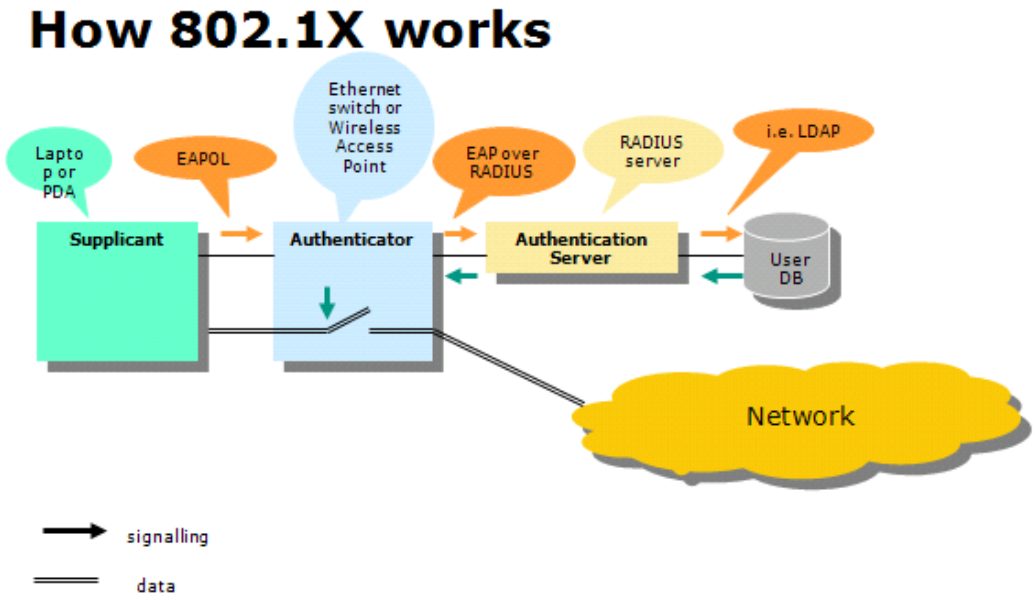

Figure 12: How 802.1X works [2]

The following steps outline the basic authentication and authorization process, refer to step numbers marked on the Figure 13:

1) The authenticator initiates the authentication message exchange by sending an EAP-Request/Identity packet

2) The supplicant sends an EAP-Response/Identity packet (includes supplicant's username) to the authentication server via authenticator; RADIUS server confirms its identity.

3) RADIUS server received the username forward up by authenticator, it checks the database with the user list to find the corresponding username, and then RADIUS server chooses an authentication algorithm to verify user's identity. It sends back a corresponding EAP-Request/MD5-Challenge to 802.1X client via authenticator.

4) The supplicant sends an EAP-Response/Identity packet (authentication credentials) to authentication server via authenticator.

5) The authentication server sends an EAP-Success packet to the supplicant via authenticator if it's a legitimate user; otherwise it sends an EAP-Fail packet.

   Upon the authorization by the authentication server, the supplicant can get IP address according to its VLAN membership and has access to network via the control port.

6) When supplicant sends EAP-Logoff packet, the port sets to unauthorised [1].

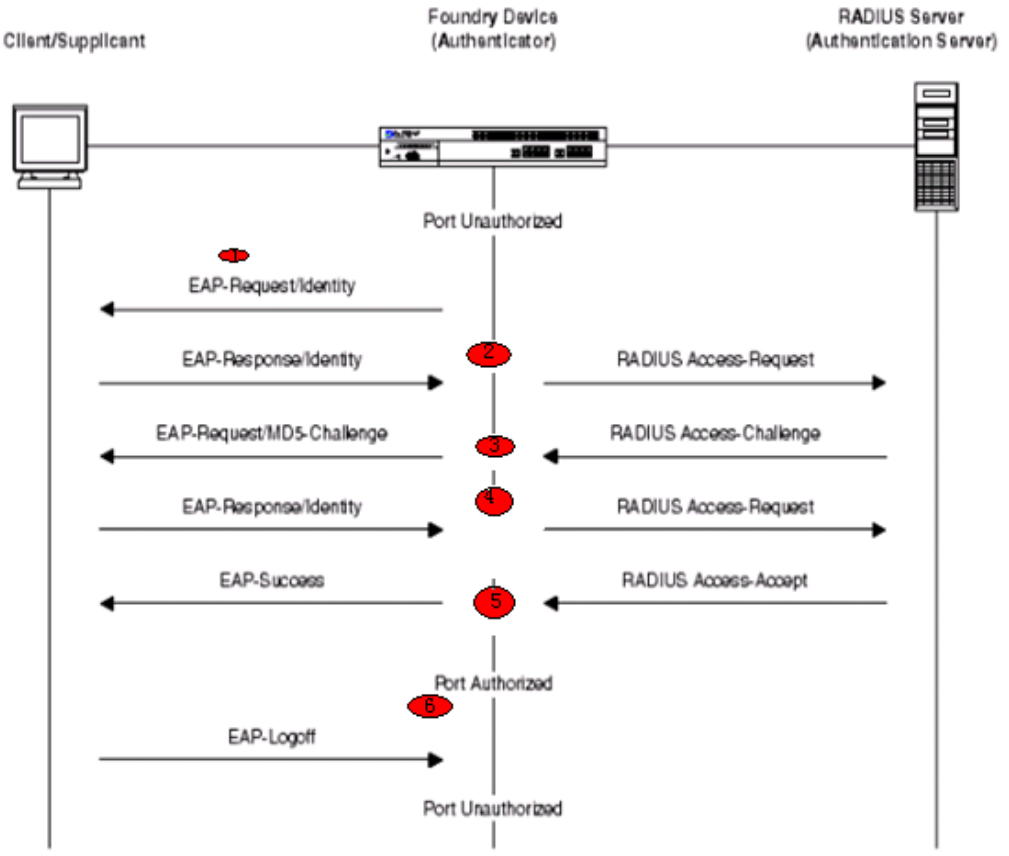

Figure 13: Port Authentication process [3]

4 Implementation of 802.1X

4.1 System overview

To implanting the authentication and authorization, there are three main tasks shall be achieved:

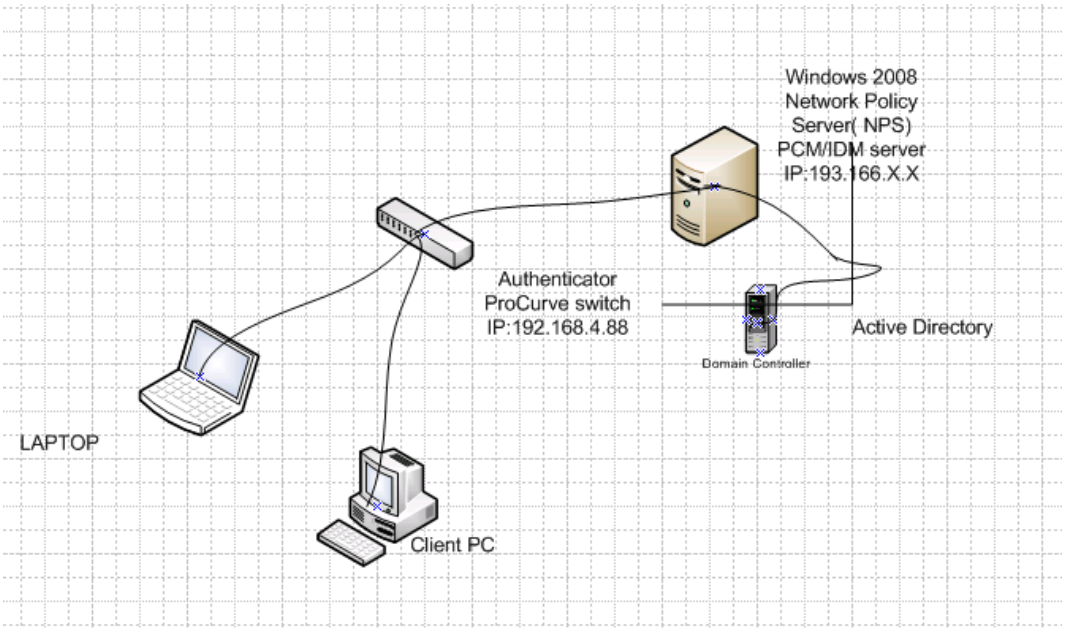

Figure 14: Implementation System overview

RADIUS server: Windows 2008 NPS Server (193.166.X.X) as RADIUS Server and PCM/IDM Server for this project.

Authenticator: HP ProCurve switch, IP Address is 192.168.4.88.

Supplicant: PC/Laptop/Printer

As it showed in Figure 14, supplicant PC communicates with RADIUS Server via authenticator.

4.2 Configure 802.1X client.

As I mentioned above in chapter 2, 802.1X supplicant software is implemented natively in some Microsoft Windows operating system, for instance: Windows XP, VISTA and Windows 7. For Linux, you can download an open source like open 1x and add it to the PC.

Window XP client was used here as an example.

- Download server certificate.

Download 'dcwolf' certificate from PUV webpage.

Choose "Install certificate", and place it in "Trusted Root certification authorities" store, then click "OK" (Figure 15).

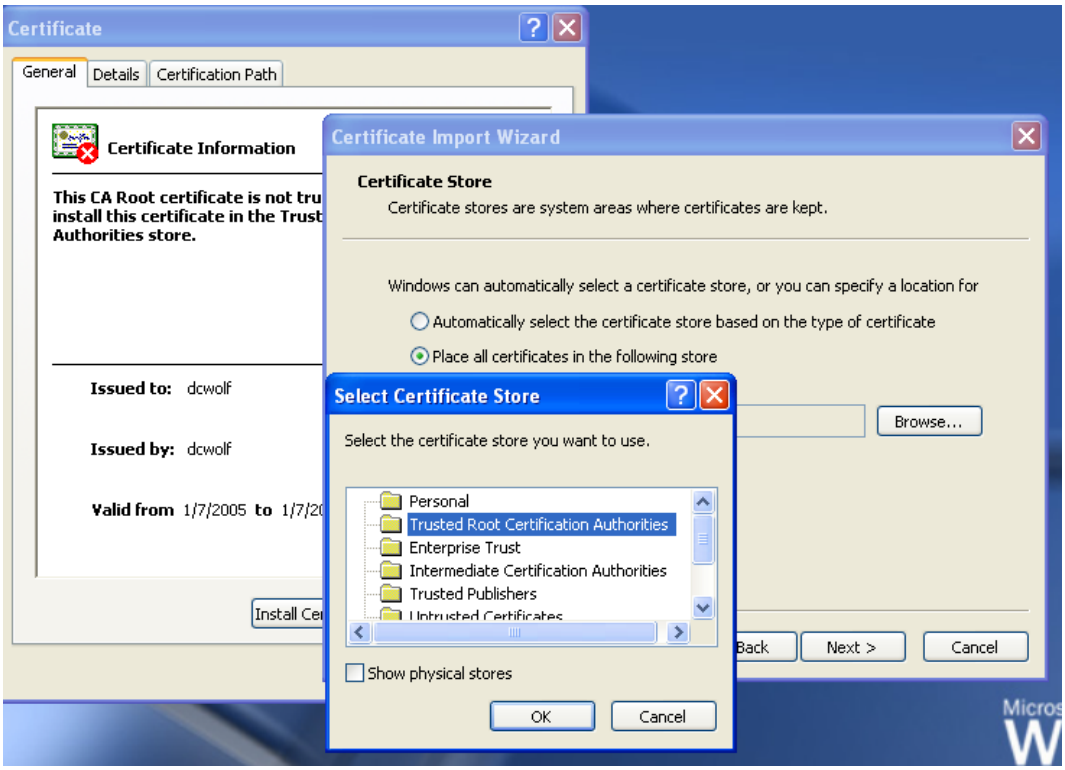

Figure 15: Certificate installation

- Local connection properties setting.

Click from the “Start Menu” go to All Connections. Then in All Connections click on Local Connection, right click on it and choose properties, then choose authentication. On the Authentication tab, enable IEEE 802.1X and choose protected EAP as the network authentication method: (Figure 16)

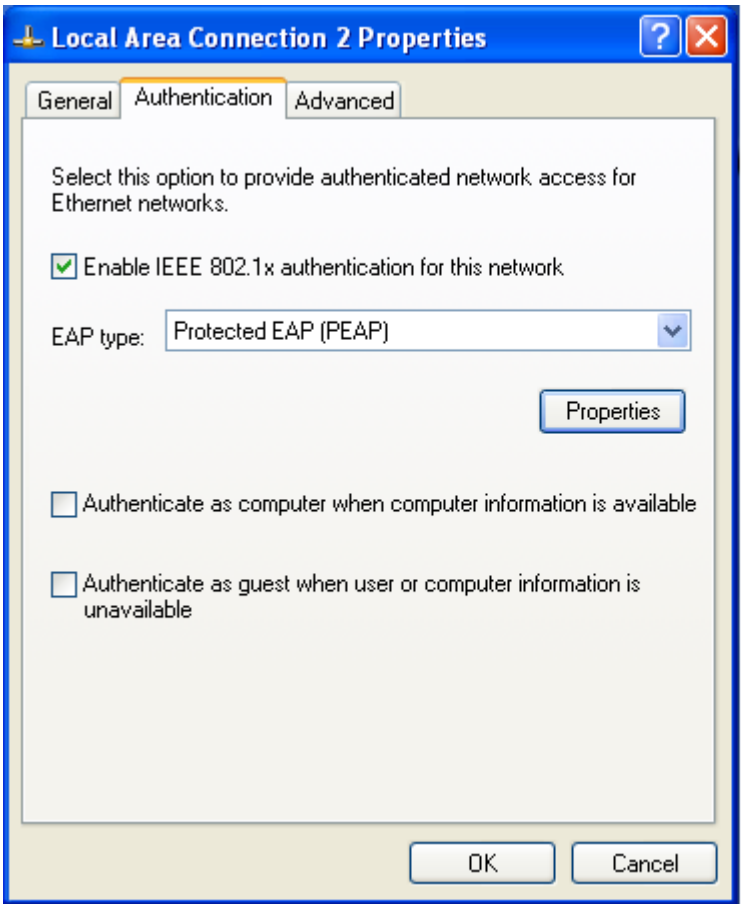

Figure 16: Enable 802.1X

Then click on the Properties to configure PEAP. Put a check mark in the Validate server certificate box. Choose school server certificate “dcwolf” from Certification Authorities, and select EAP-MSCHAP v2 as the authentication method.

Then click on Configure (Figure 17).

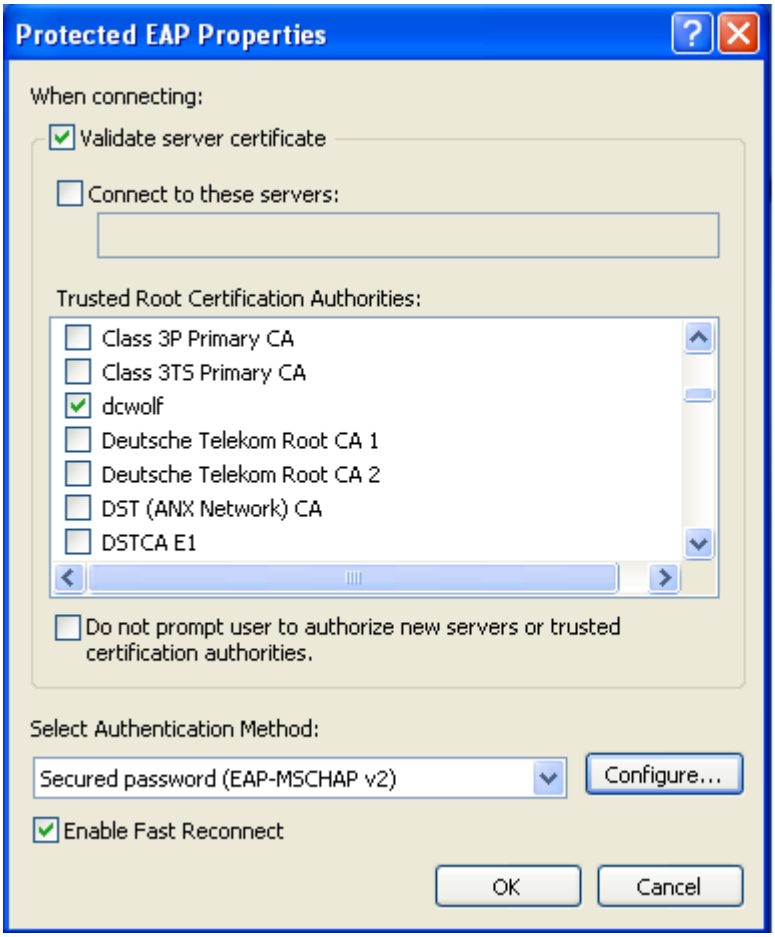

Figure 17: EAP properties

In the EAP-MSCHAP v2 properties box, select automatically use my Windows logon name and password, and click OK (Figure 18)

Figure 18: EAP MSCHAPv2 Properties

In the EAP Properties window, select Enable Fast Reconnect. Click OK twice.

4.3 Authenticator configuration

PUTTY is to be used for switch configuration, which is free for Telnet /SSH client.

Basic settings of ProCurve switch in Figure 19:

/include-credentials/ should to be given once by hand before copy/paste the others settings.

The last port is required to set as an uplink port (24 or 48)

IP addresses *192.168.1.1* and *192.168.1.2* work as IP helper. The IP helper allows the user to forward specific UDP broadcast from one interface to another.

Command *IP route 0.0.0.0.0.0.0* is to configure a default route; traffic is load-balanced over the multiple routes. IP address *192.168.4.1* is the default-gateway. Use the IP default-network and *IP route 0.0.0.0 0.0.0.0* commands to set the gateway of last resort on routers that have IP routing enabled

IP address *193.166.X.A* and *193.166.X.B* are VAMK's two servers.

```
include-credentials
password operator sha1 "446410a140d4e16355e0a38e4f924fa1a4c7790f"
password manager sha1 "446410a140d4e16355e0a38e4f924fa1a4c7790f"
sntp unicast
sntp server priority 1 192.168.1.1
sntp server priority 2 192.168.1.2
timesync sntp
ip authorized-managers 193.166.X.A     255.255.255.255 access Manager
ip authorized-managers 193.166.X.B      255.255.255.255 access Manager
ip ssh filetransfer
ip route 0.0.0.0 0.0.0.0 192.168.4.1
router rip
   no auto-summary
   exit
snmp-server community "public" Unrestricted
snmp-server host 193.166.X.A      "public"
snmp-server host 193.166.X.B     "public"
```

Figure 19: Basic configuration of ProCurve switch

Some commands are needed to be explained, see table 1 below:

Table1: Basic commands for configuring VLAN

Commands	Meaning
Tagged	A port that "carries" multiple VLANs using the 802.1q, for instance an uplink, like "trunk" in Cisco commands.
Untagged	A port that belongs to a unique VLAN and is untagged.

All the needed VLANs should be added in target switch, this step is the base of VLAN dynamic assignment. Here VLAN316 manages HP ProCurve switch; VLAN320 is printer's VLAN and untagged port 23 to it; VLAN365 works for PUV-STUDENT; VLAN332 works for PUV-STAFF; VLAN380 is for guests (Figure 20).

Give the IP address: 192.168.4.88 to the switch.

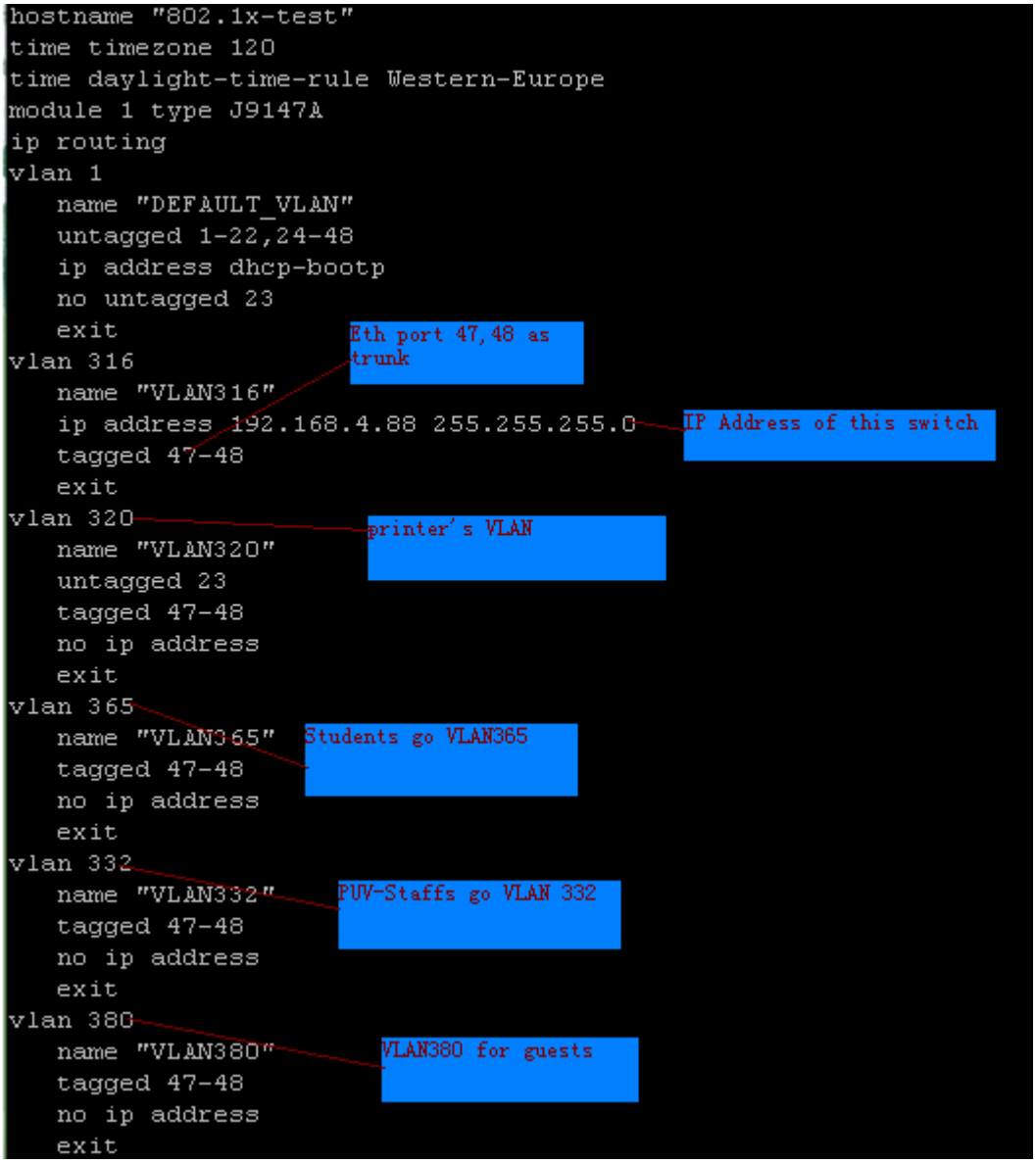

Figure 20: Basic configuration on the switch

Then to configure 802.1X Authentication the switch, first I defined the RADIUS server on the switch, and then specified the authentication protocol “EAP”, next defined the port-authenticator ports and final I activated those port.

```
802.1x-test(config)# aaa authentication port-access eap-radius
802.1x-test(config)# radius-server host 193.166.140.181 key procurve
802.1x-test(config)# aaa accounting network start-stop radius
802.1x-test(config)# aaa port-access authenticator 1-20 unaut
 unauth-period
 unauth-vid
802.1x-test(config)# aaa port-access authenticator 1-20 unauth-vid 380
802.1x-test(config)# aaa port-access authenticator active
802.1x-test(config)#
```

Figure 21: 802.1X configuration on ProCurve switch

In Figure 21, the first line command is to tell the switch to access a RADIUS server, which host is 193.166.140.181, and use "procurve" as an encryption key during authentication sessions with specified server. This key must match the key used on RADIUS server, and then the RADIUS server can communicate with authenticator.

Here are the explanations for the other commands in Figure 23:

/aaa authentication port-access eap-radius/ configures EAP as primary password authentication method for the port-access.

/aaa port-access authenticator 1-20 unauth-vid 380/ enable Port 1-20 to act as 802.1X authenticator ports. Unauthorized users will be forced to VLAN 380 which is GUEST VLAN

/aaa network accounting network start-stop radius/ RADIUS server will account the time from user login until logout.

/aaa port-access authenticator active/ Actives 802.1X port-access on the ports that I have configured as authenticators.

And if you want view the RADIUS information, type commands/show RADIUS/ , here you can get general RADIUS information (Figure22).

```
802.1x-test(config)# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- --------------------------------
  193.166.140.181 1812  1813  procurve
```

Figure 22: show RADIUS information

Use the command /show authentication/ to verify that Port-access is enable with EapRADIUS (Figure23)

```
802.1x-test# show authentication

 Status and Counters - Authentication Information

  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Local      None       Local      None
  Port-Access | EapRadius  None
  Webui       | Local      None       Local      None
  SSH         | Local      None       Local      None
  Web-Auth    | ChapRadius None
  MAC-Auth    | ChapRadius None
```

Figure 23: Verified port-access method

4.4 Configuration of RADIUS server by IDM

IDM is a plug-in module of ProCurve Manager Plus, it works based on an IDM RADIUS Agent that is installed and resists on the RADIUS server.

Using IDM, administrator can control the access policies such as time, location and resources, the management interface gives administrator a bird's eye view to monitor users' when and from where to login and logout the network.

Step 1: IDM Active Directory Synchronization

IDM will automatically discover the domain users and groups for Active Directory.

Navigate to Tools -> preferences ->Identity Management ->User Directory Settings

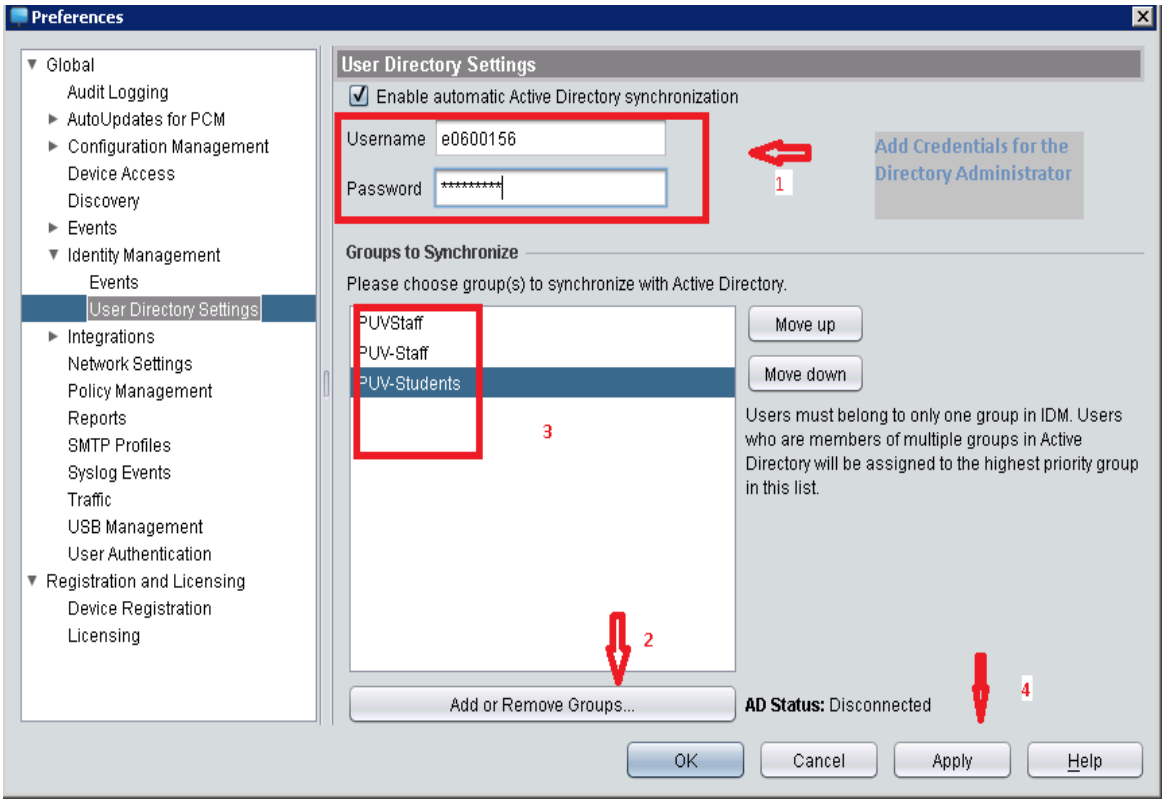

Figure 24: Active Directory synchronization.

In Figure 24: please see the procedure follow the mark, and I add three groups which are needed to be configured from Active Directory.

Step2: Access Policy Grouping

Once the groups have been discovered by Active Directory synchronization, access policy groups will be shown in the IDM interfaces.

Look at Figure 25, three groups which were selected in step 1 automatically appeared in Access Policy Groups.

Realm here is similar to an Active Directory Domain, but it works across non-windows, like Linux. Generally specified in user-name as username@realm for instance, my user-name is e0600156@ad.puv.fi.

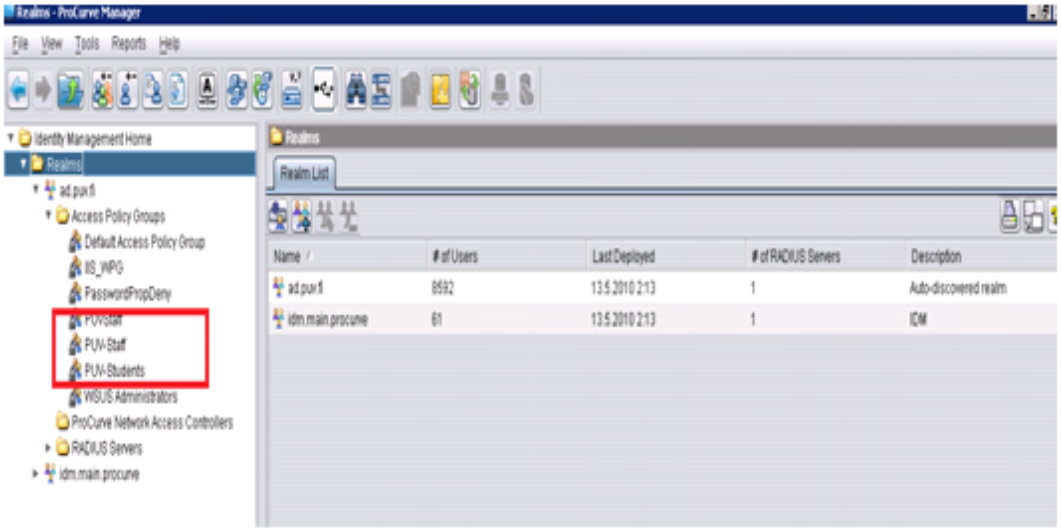

Figure 25: IDM Access Policy Group interface.

Step 3: Configure identity management.

In IDM, go to the Realm Properties click on the icon  to open Identity Management Configuration, you will see the navigation tree on the left: Access Profiles, Location, Times, Network Resources.

Access Profiles Define the settings that will be assigned to a group users after successful authentication. It contains:

A VLAN;

A QoS parameter;

A bandwidth;

Figure Network access rules.

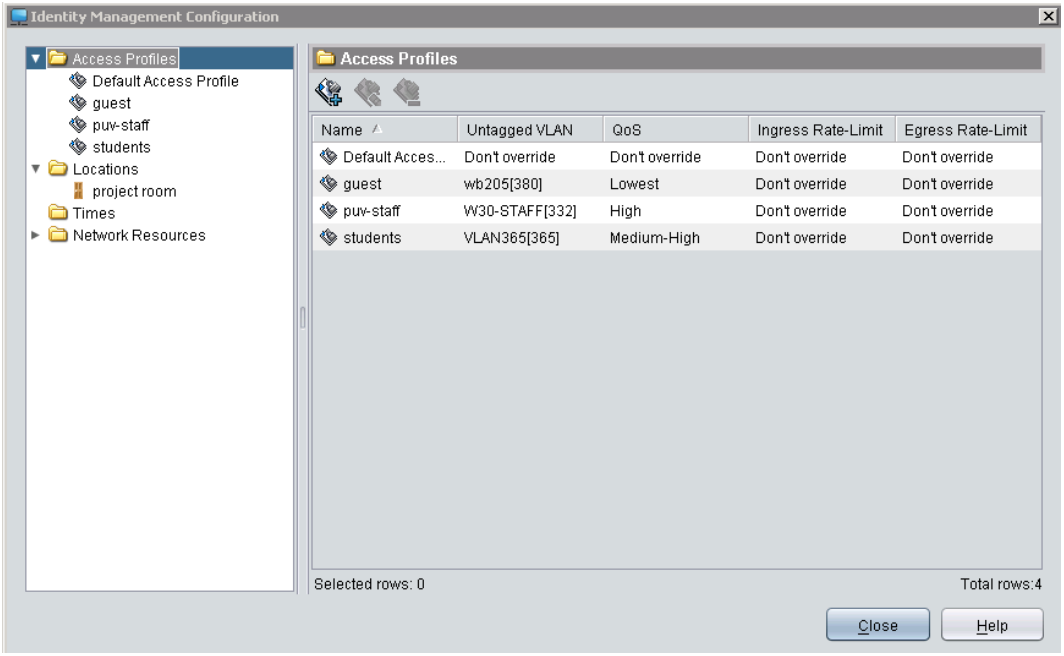

Figure 26: In the Access Profiles shown guest is configured to use VLAN380, puv-staff uses VLAN332, student with VLAN365.

The Access Profile is defined as follow in Table 2:

Table 2: Access Attributes:

Groups	Staff	Student	Guest
VLAN membership	Go to VLAN 332	Go to VLAN 365	Go to VLAN 380
QoS attributes	High	Medium-high	Lowest
Bandwidth	No specified	No specified	No specified

So when a user assigned to an access policy group is authenticated on the RADIUS server, the IDM agent will apply appropriate rule to accept or reject the user. The IDM agent modifies the RADIUS reply to provide desirable access network (Figure 27).

For example, users from PUV-Students are allowed to connect from project room at any time, from any system, using access profile students.

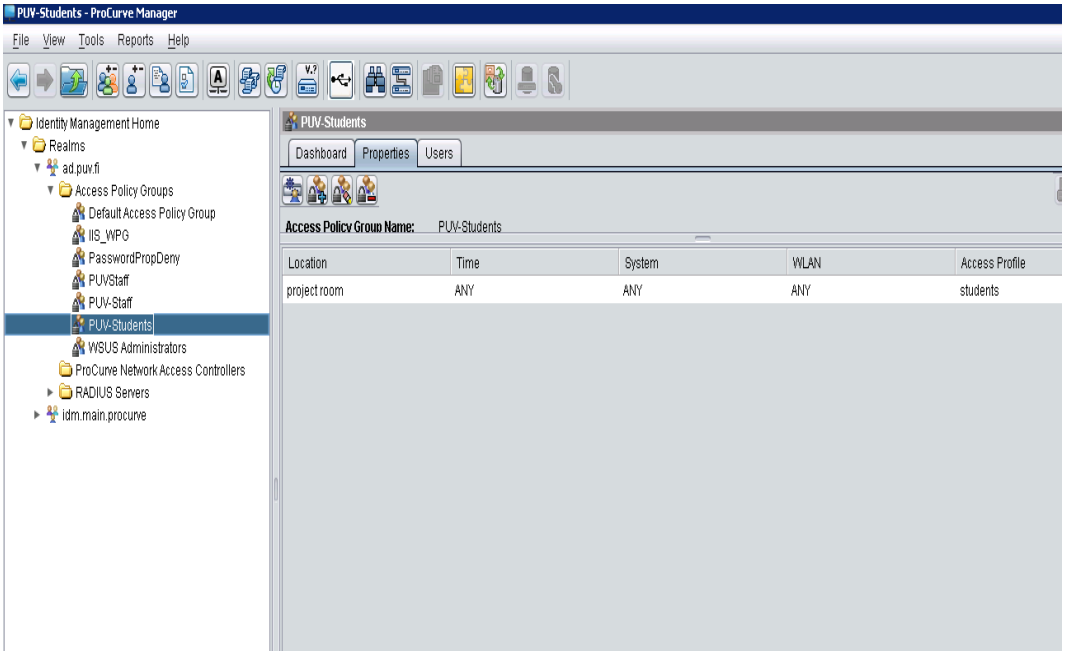

Figure 27: PUV-Students' properties.

When the user is authenticated, IDM will check the Access Policies in the order listed.

As well, users form PUV-Staff access policy group connect to the same physical ports will be authenticated using access profile staff, with the appropriate VLAN and network resources.

5 Test of the authentication/authorization.

5.1 Initialization

After introduction structure of the whole setting process, in this chapter we will through the screenshot to understand how the authentication worked step by step.

Plug a Windows XP client PC to a port authenticator. I obtained the follow message in Figure 28.

Figure: 28: Login message

Click on the message, a login window came out (Figure 29), types user-name and password, then click on OK.

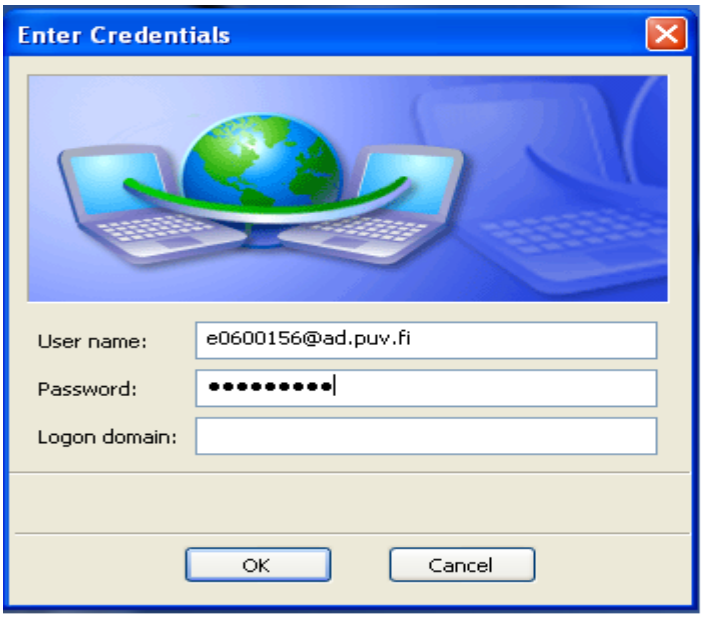

Figure 29: Login window

5.2 Results

Before be authenticated, client PC went to GUEST VLAN (VLAN 380) at first, refer to Figure 30, the IP address is from VLAN 380's IP pool.

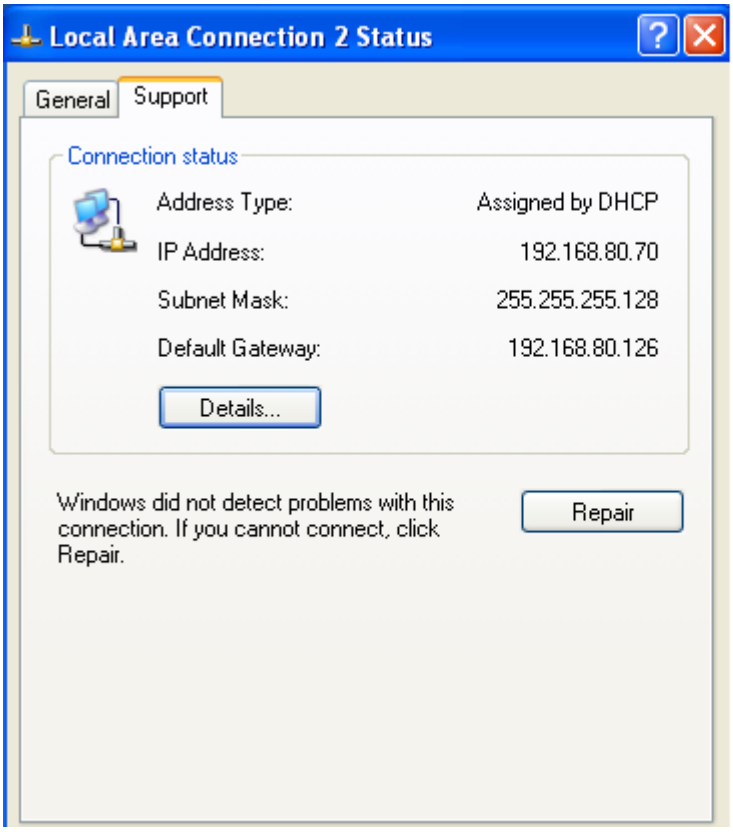

Figure 30: Before authentication the connection status.

Then client PC waited for the RADIUS server's reply, after 802.1X authenticated, the client connected port would be assigned to a new VLAN membership and access the student network resource.

If the supplicant passed authentication, the status changed to acquire an IP address from student's VLAN pool (Figure31).

In Figure 32, you can see the client PC already accessed to the network service in target VLAN 365.

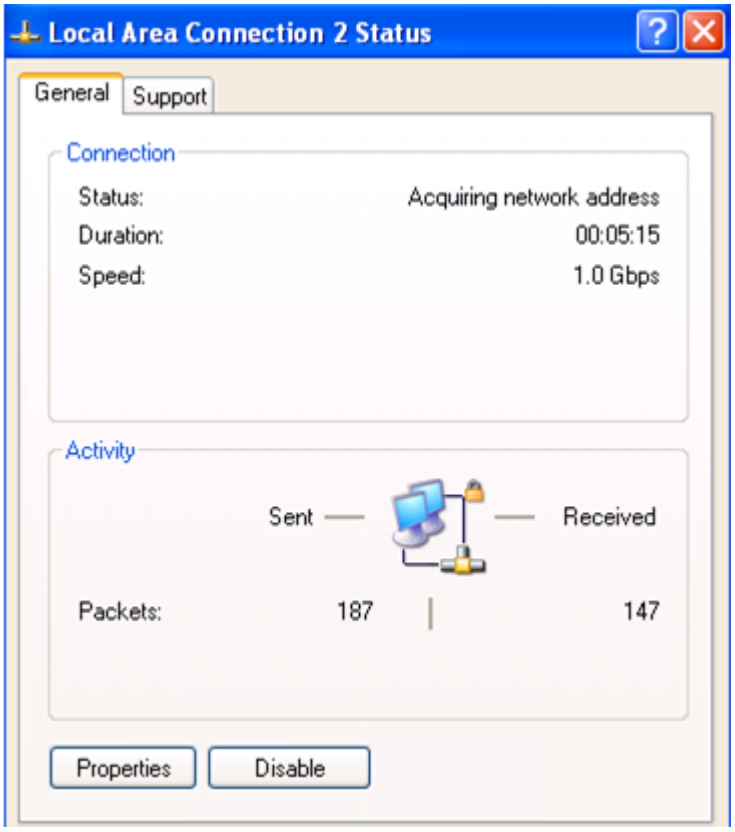

Figure31: After authentication, jumped out of GUEST VLAN, acquired for appropriate IP address.

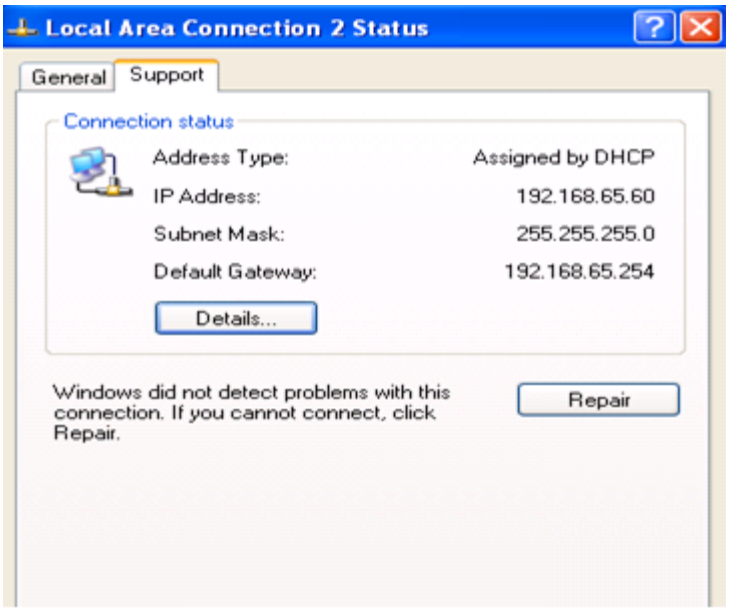

Figure 32: Final status for the authorized client.

So the client successful be authenticated and accessed to the student network resources.

You can check the login information form PUTTY in Figure 33 as well. Client connected from port 29, auth clients: 1, untagged VLAN: 365, RADIUS ACL

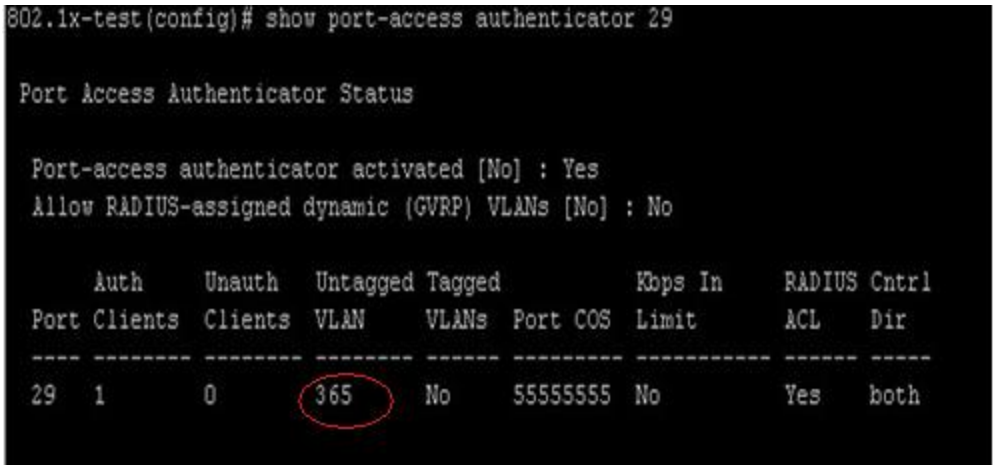

Figure 33: Result of the authenticated student from PUTTY

IDM is an efficient monitor tool and administrate interface.

And from the IDM event (Figure 34), the login details are in list. It shows user e0600156@ad.puv.fi from which 'ad.puv.fi' realm, belongs to group PUV-Students, access profile used student, client's device MAC address, location and etc.

Figure 34: Event detail form IDM

VAMK staff was authenticated, read Figure 35

```
802.1x-test(config)# show port-access authenticator 29

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

      Auth     Unauth   Untagged Tagged          Kbps In     RADIUS Cntrl
  Port Clients  Clients  VLAN     VLANs  Port COS  Limit       ACL    Dir
  ---- -------- -------- -------- ------ --------- ----------- ------ -----
  29   1        0        332      Yes    66666666  No          Yes    both
```

Figure 35: Result of authenticated staff from PUTTY

The physical port is the same, but untagged VLAN changed to 332 which are the VLAN for staffs.

In figure 36, it shows unauthenticated clients/ guests went to VLAN 380

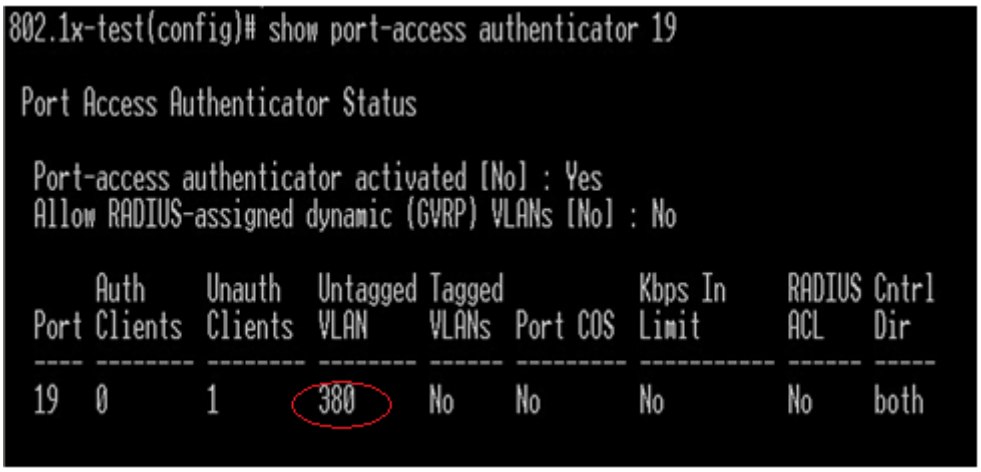

Figure 36: Result of unauthorized user or guest.

In those situations, you will go to the GUEST VLAN:

Domain users who type wrong user-name or password;

Non-802.1X supplicant;

Visitors,

For domain users, you need retry to login until authenticated then access to the appropriate network. Otherwise only get quite limited guest resources. And local LAN sign shows limited connection  .

6 Results and conclusions

Related to the chapter 5, the aim of this project is achieved.

The whole 802.1X wired network authentication and authorization system is built in switched environment. Authenticator communicates with RADIUS server and RADIUS server gives the authorization to supplicants. In the dynamic VLAN assignment section: enter the correct username and the password will be authorized and get the correct IP address according to the VLAN membership. The student's account went to the VLAN 365; Staff's account went to the VLAN 332, it is workable to separate the network service. Enter the incorrect username and password will be forced to the VLAN 380 to access limited network service. Visitors can only access to the VLAN 380. Now the wired network system is powerful to monitor and manage the login users, IDM interfaces can simplify this task.

The research project is just an attempt in a small range network. To be an authentication and authorization method, 802.1X can be used for the big range network, for example, an international company which has hundreds of departments with the need of separate services. In addition it also works for wireless network.

7 Summary

This is a long-term project which took four months in all to complete:

For the first two months, the main task was migration Cisco to HP switches and basic configuration of switch; the others were 802.1X authentication's configuration.

At the beginning of this project, problems came out one by one. First the RADIUS server could not communicate with authenticator by the share key; then client didn't get the right IP address because of the missing VLAN in the tested switch.

Finally, I achieved the objectives, now the wired network system is more secured, each client physically connected to the network port, needs to be authenticated by RADIUS server via authenticator: The one who be authorized by the RADIUS server can access the appropriate network by its VLAN membership; unauthenticated users or visitors are able to access GUEST VLAN; they can get limited network resources, and be kept apart from private network services.

So far, the leak of the security is that 802.1X controls one-way authentication, the attacker can intercept 802.1X messages between legitimate user and authentication server, then attacker will disguise as a legitimate user.

However, there are something needed to be upgraded in the future, like web-authentication and MAC authentication for non-802.1X supplicant. I believe that network security plays a significant role in the rapid development high-tech era.

REFERENCES

Electronic publication

[1] Allied Telesis 2006, 802.1X White Paper by Allied Telesis [online]. Available in www-form: < URL:http://www.alliedtelesis.com/media/pdf/8021x_wp.pdf>

[2]Dobbelsteijn, Erik, 29.10.2002, Amsterdam. What about 802.1X [online].Available in www-form: <URL: http://security.fi.infn.it/TRIP/8021x-dobbelsteijn.pdf>

[3]Free RADIUS server 2009 [online]. Available in www-form< URL:http://freeRADIUS.org/>

Referencing: (RFC 5080)

[4] Hewlett-Packard development company, L.P. 2009. HP ProCurve Identity Manager Driven 3.0 User's Guide [online].Available in www-form: <URL: http://cdn.procurve.com/training/Manuals/IDM-UG-May2009-5990-8851.pdf>

[5] Hewlett-Packard development company, L.P.2003. HP ProCurve Networking Security Solution, 802.1x and GUEST VLANs [online]. Available in www-form: <URL: http://www.hp.com/rnd/pdfs/guest_vlan_paper.pdf>

[6] Hewlett-Packard development company, HP ProCurve 2910al Switch Series overview [online]. Available in www-form: <URL: http://www.procurve.com/products/switches/HP_ProCurve_2910al_Switch_Series/overview.htm#J9145A>

[7] IEEE STD 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control [online]. Available in www-form: <URL: http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>

[8] LSK.802.1X Port-Based Authentication HOWTO [online], [revise in 18.10.2004]. Available in www-form:
<URL: http://tldp.org/HOWTO/html_single/8021X-HOWTO/>

[9] Viega John, chief scientist, Secure Software, Inc., co-author of Building Secure Software. 802.11 security [online]. Available in www-form:
<URL:http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/>

APPENDICES

List of configured HP ProCurve switch and Access Point:

Switches:

HP2910-wb004	192.168.4.40
HP 2910-wa334-1	192.168.4.46
HP2901-wa213	192.168.4.48
HP2910-wa225	192.168.4.55
HP2910-wa305-1	192.168.4.56

Access Point:

Puv-wa333	192.168.29.26
Puv-wa301	192.168.29.27
Puv-wa337	192.168.29.28
Puv-wa242	192.168.29.29
Puv-wa234	192.168.29.30
Puv-wa202	192.168.29.32
Puv-wa247	192.168.29.36
Puv-wa022	192.168.29.38