Configuration Examples

802.1x port-based and MAC-based Access Control

Technical Support Department

D-Link Corp.

Aug 2004

D-Link Solution for Secure Network

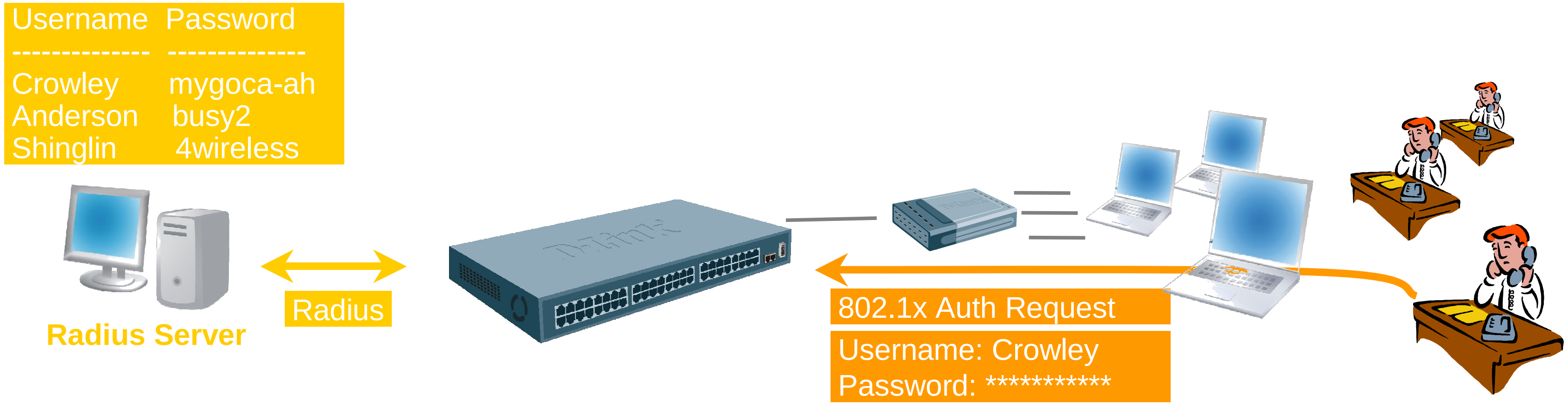
- **Authenticate User Identity**

802.1x

The 802.1X protocol is the next-generation LAN authentication protocol ratified by the IEEE. It enables user authentication in both wireless and wired. It is expected to become the de facto authentication standard in both wired and wireless LANs.
The 802.1X standard is included in the newest Microsoft Windows XP operating systems.

D-Link’s Implementation

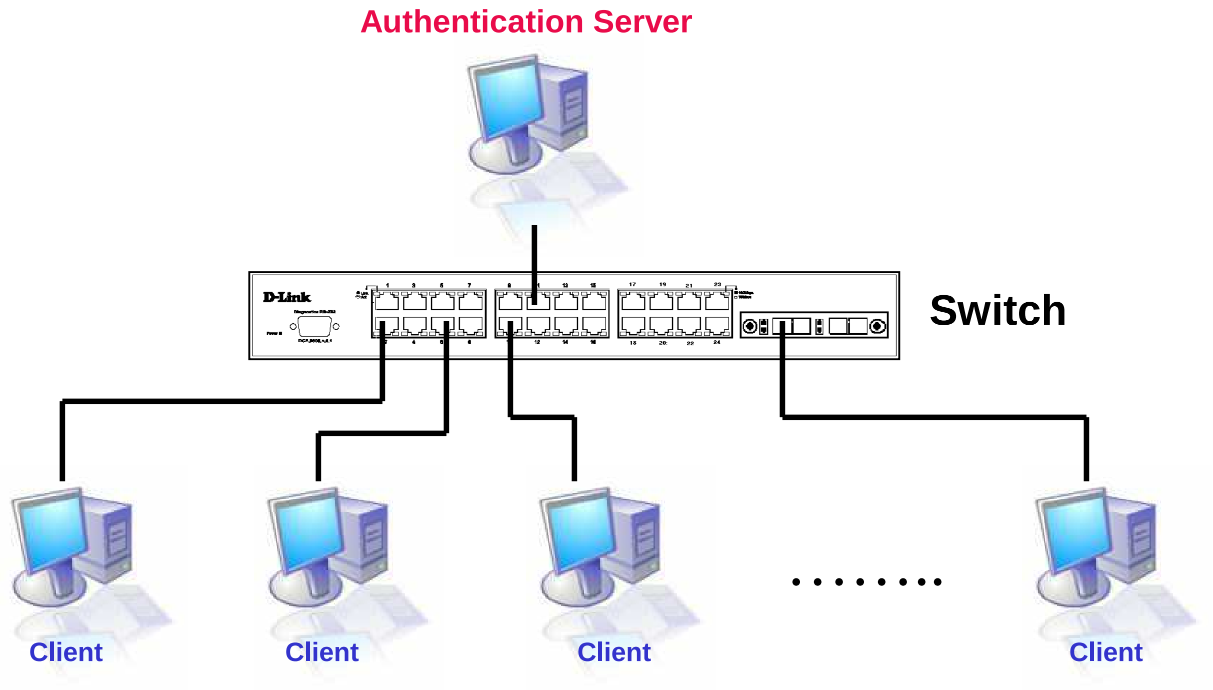
- **Port-based 802.1x:** users have to be authenticated before able to access the network, and switches will unlock the the port only after users pass authentication
- **MAC-based 802.1x:** D-Link switch can perform authentication per MAC address based which means each switch port can authenticate multiple PCs’ access



Username	Password
-------------	-------------
Crowley	mygoca-ah
Anderson	busy2
Shinglin	4wireless

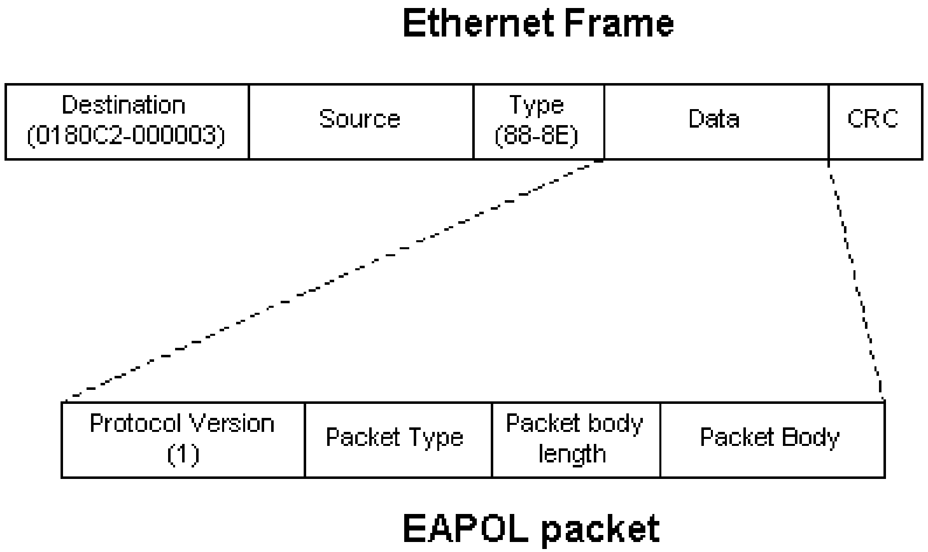
IEEE 802.1x Definition

Defines a Client/Server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. The Authentication Server authenticates each Client connected to a switch port before making available any services offered by the switch or the LAN. .



IEEE 802.1x Definition

- Defines a special multicast address for *Extensible Authentication Protocol over LAN* **(EAPOL)** packets, which is called *Port Access Entity* **(PAE)** group address. This enable 802.1X aware network access servers to listen for and steal packets containing this multicast address.



Ethernet Frame

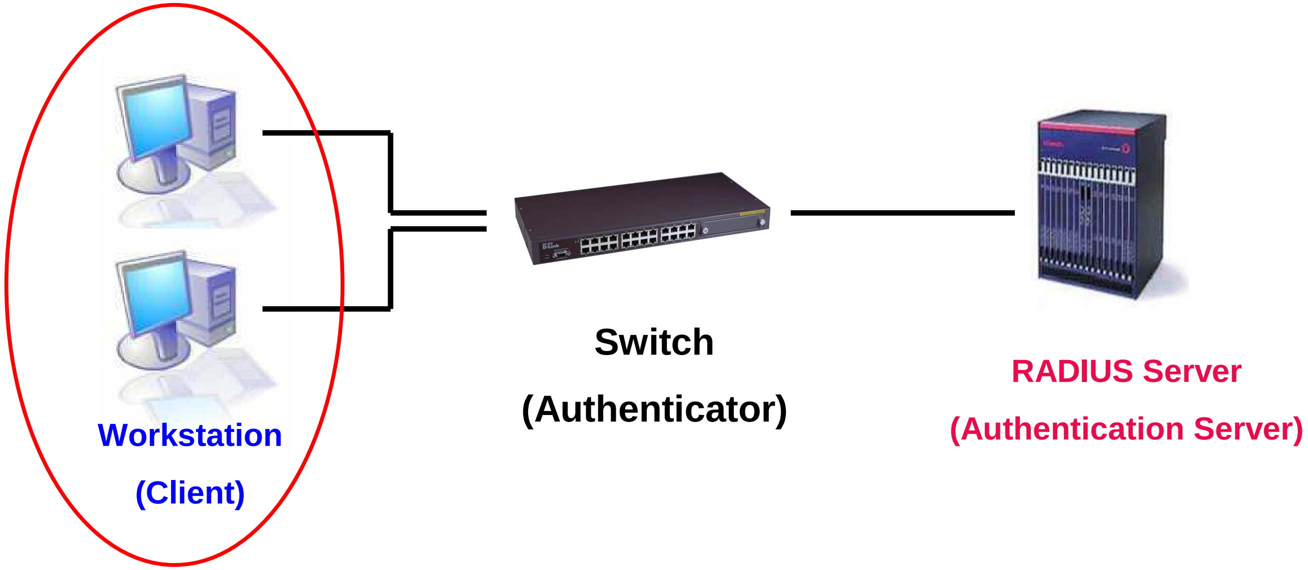
Destination (0180C2-000003)	Source	Type (88-8E)	Data	CRC

Protocol Version (1)	Packet Type	Packet body length	Packet Body

EAPOL packet

802.1x Device Role

- ***Device Roles: Client***

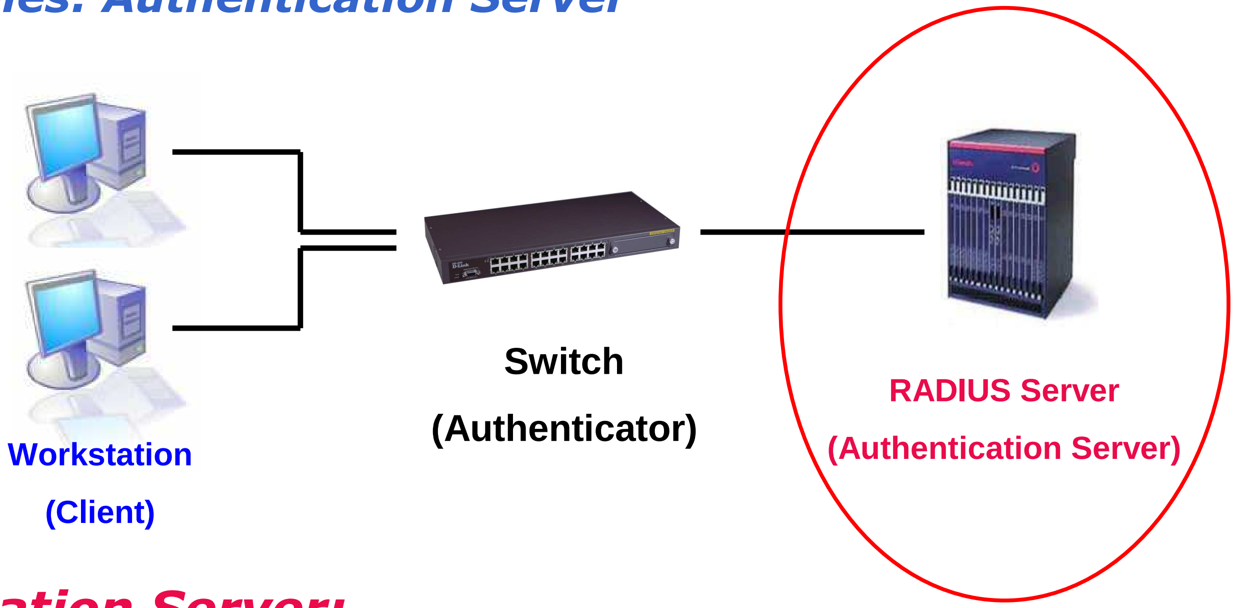


Client:

The device (Workstation) that requests access to the LAN and switch services and responds to the requests from the switch. The Workstation must be running *802.1x-Compliant client software* such as that offered in the Microsoft Windows XP operating system.

802.1x Device Role

- *Device Roles: Authentication Server*



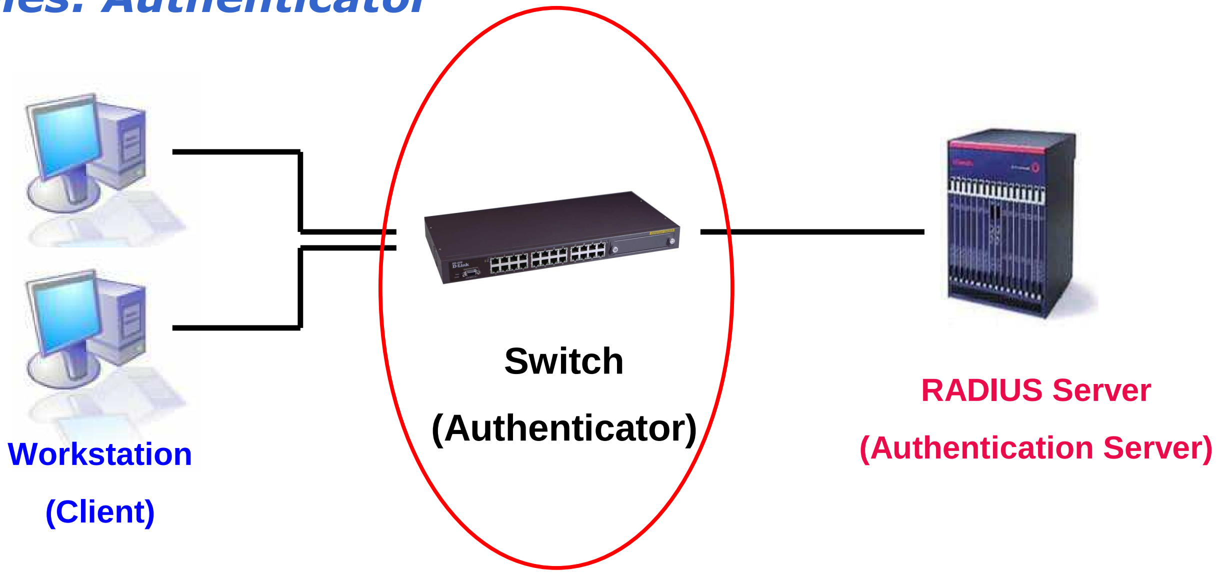
Authentication Server:

The Authentication Server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. *RADIUS* operates in a client/server model in which secure authentication information is exchanged between the *RADIUS* server and one or more *RADIUS* clients.

** Remote Authentication Dial-In User Service* **(RADIUS)**

802.1x Device Role

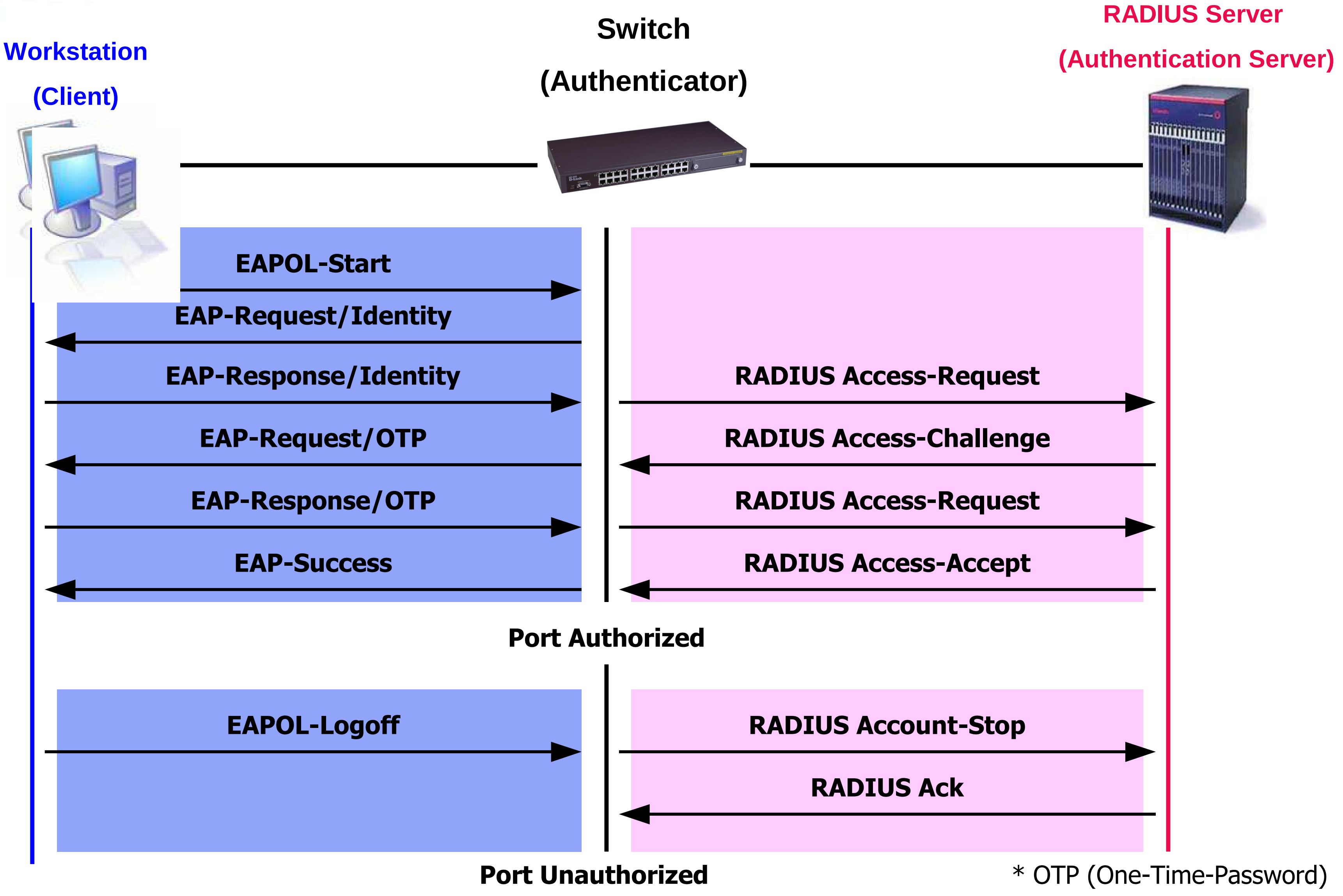
- *Device Roles: Authenticator*



Authenticator:

The Authenticator acts as an intermediary (proxy) between the Client and the Authentication Server, requesting identity information from the Client, verifying that information with the Authentication Server, and relaying a response to the Client.

802.1X Authentication process



Workstation

(Client)

Switch

(Authenticator)

RADIUS Server

(Authentication Server)

EAPOL-Start

EAP-Request/Identity

EAP-Response/Identity

RADIUS Access-Request

EAP-Request/OTP

RADIUS Access-Challenge

EAP-Response/OTP

RADIUS Access-Request

EAP-Success

RADIUS Access-Accept

Port Authorized

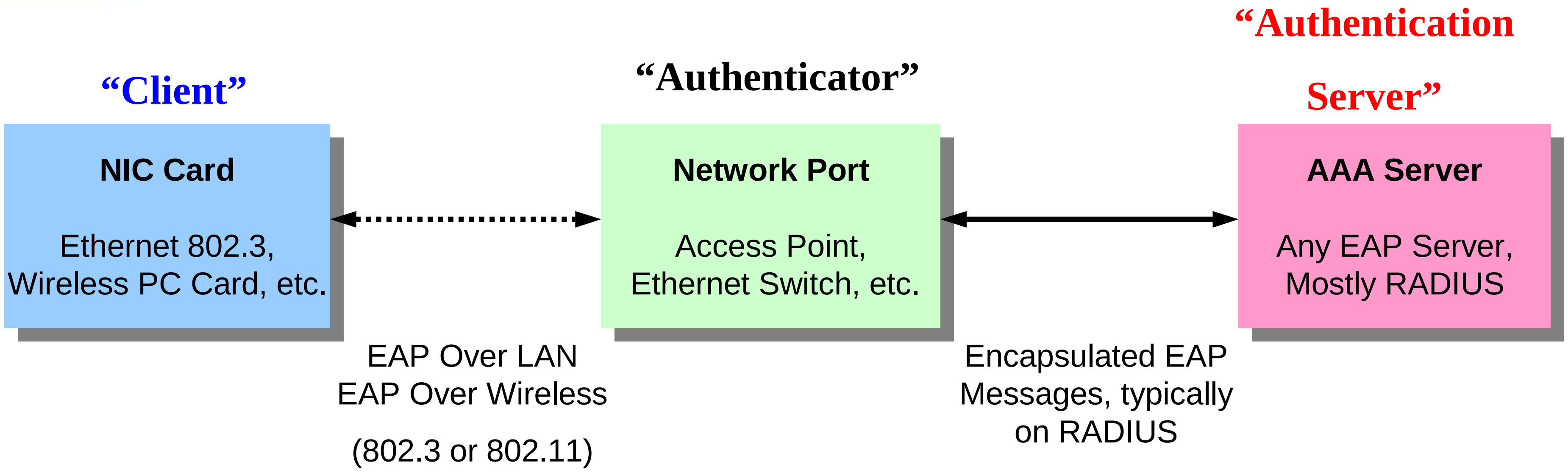
EAPOL-Logoff

RADIUS Account-Stop

RADIUS Ack

Port Unauthorized

* OTP (One-Time-Password)



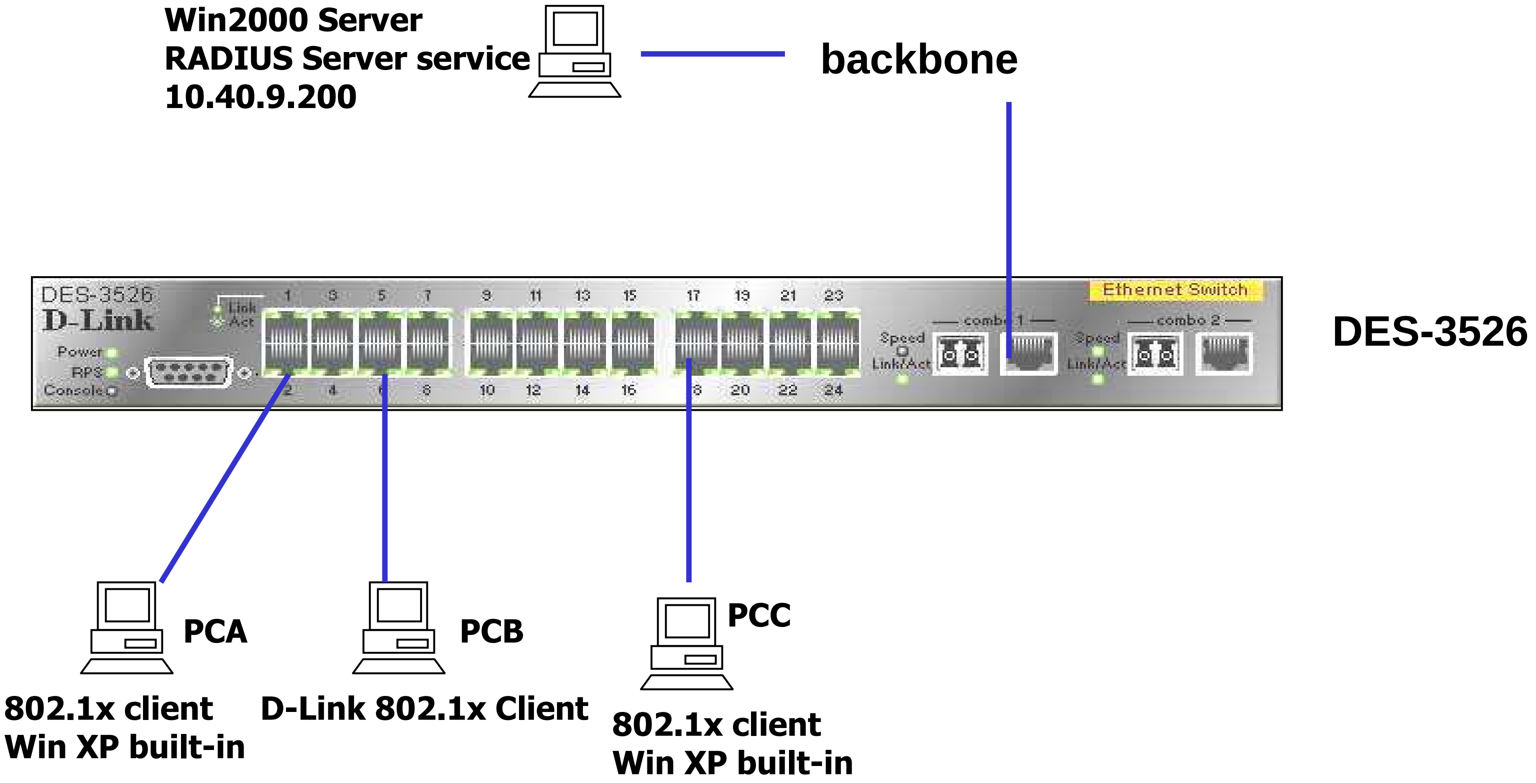
- ***The three different roles in IEEE 802.1x:***

Client, Authenticator and the Authentication Server.

Until the Client is authenticated, 802.1x access control allows only EAPOL traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

* *RADIUS* Server provides AAA service

802.1x Example



Win2000 Server
RADIUS Server service
10.40.9.200

backbone

DES-3526

PCA

802.1x client
Win XP built-in

PCB

D-Link 802.1x Client

PCC

802.1x client
Win XP built-in

Before passing the authentication using 802.1x client program with correct username/password, the port is locked. Port will be un-locked after passing the 802.1x client “dial-up.”

802.1x Configuration

- Workstation: 802.1x client is Window XP built-in. Otherwise, 802.1x client software is needed.

- Switch:

1. Enable 802.1x State by device

```
enable 802.1x
```

2. Setting 802.1x port setting by port

```
config 802.1x capability ports 1-24 authenticator
```

3. Configure Radius Server setting

```
config radius add 1 10.40.9.200 key 04009 default
```

- Radius: Windows NT/Windows 2000 Server Radius Server Service or third-party RADIUS server program.

802.1x
Port-based vs. MAC-based

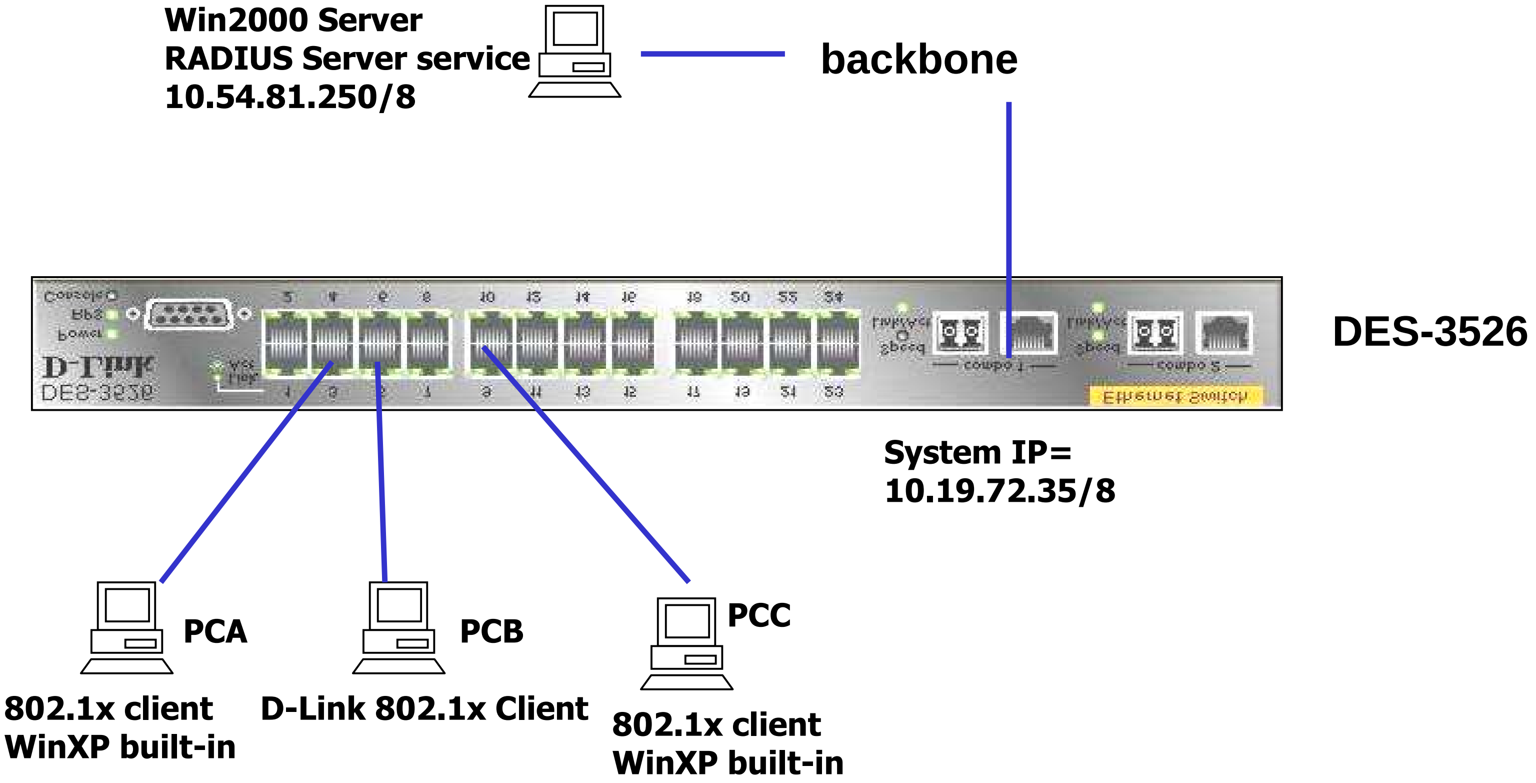
Port-based 802.1x

Once a port is authorized by a client, every user connecting to the same hub/switch can pass.

MAC-based 802.1x

Not only check the username/password, but also check whether the max. MAC allowed is reached or not. If reached, deny new MAC.

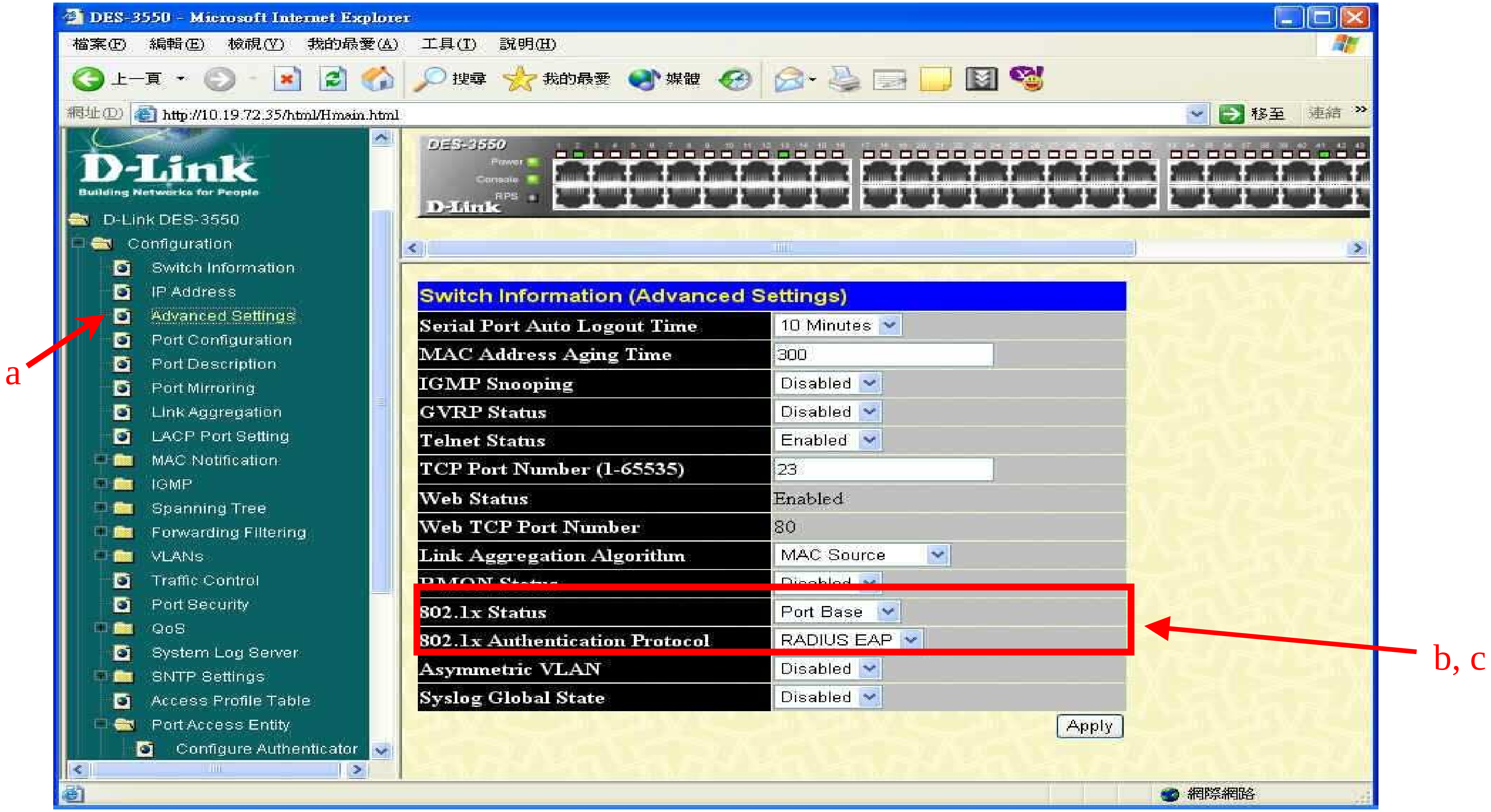
Port-based 802.1x example – Web GUI



Before passing the authentication using 802.1x client program with correct username/password, the port is locked. Port will be un-locked after passing the 802.1x client "dial-up."

Port-based 802.1x example – Web GUI

1. Enable 802.1x State by device, and change to port_based mode.
   a. Configuration →Advanced Settings
   b. Set 802.1X status as ***Port Base*** to enable 802.1X.
   c. Set protocol as ***RADIUS EAP.***



Switch Information (Advanced Settings)

Serial Port Auto Logout Time	10 Minutes
MAC Address Aging Time	300
IGMP Snooping	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
TCP Port Number (1-65535)	23
Web Status	Enabled
Web TCP Port Number	80
Link Aggregation Algorithm	MAC Source
RMON Status	Disabled
802.1x Status	Port Base
802.1x Authentication Protocol	RADIUS EAP
Asymmetric VLAN	Disabled
Syslog Global State	Disabled

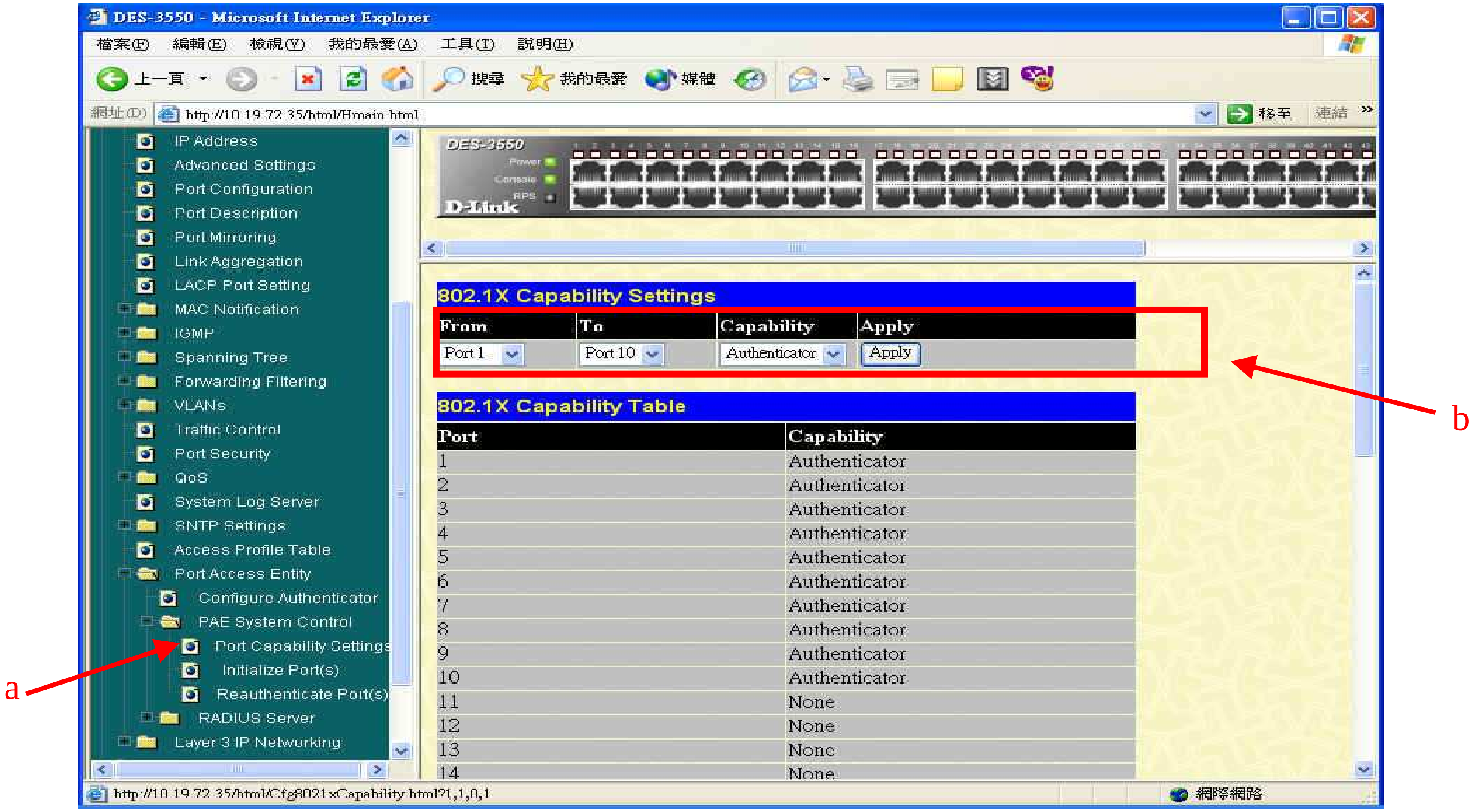
Apply

Port-based 802.1x example – Web GUI

2. Setting 802.1x port setting by port

   a. Configuration → Port Access Entity →PAE System Control →Port Capability Settings

   b. Set ports needing the 802.1x authentication as “authenticator.” In this example, ports 1-10. Others are non-authentication ports.



http://10.19.72.35/html/Hmain.html

802.1X Capability Settings

From	To	Capability	Apply
Port 1	Port 10	Authenticator	Apply

802.1X Capability Table

Port	Capability
1	Authenticator
2	Authenticator
3	Authenticator
4	Authenticator
5	Authenticator
6	Authenticator
7	Authenticator
8	Authenticator
9	Authenticator
10	Authenticator
11	None
12	None
13	None
14	None

http://10.19.72.35/html/Cfg8021xCapability.html?1,1,0,1

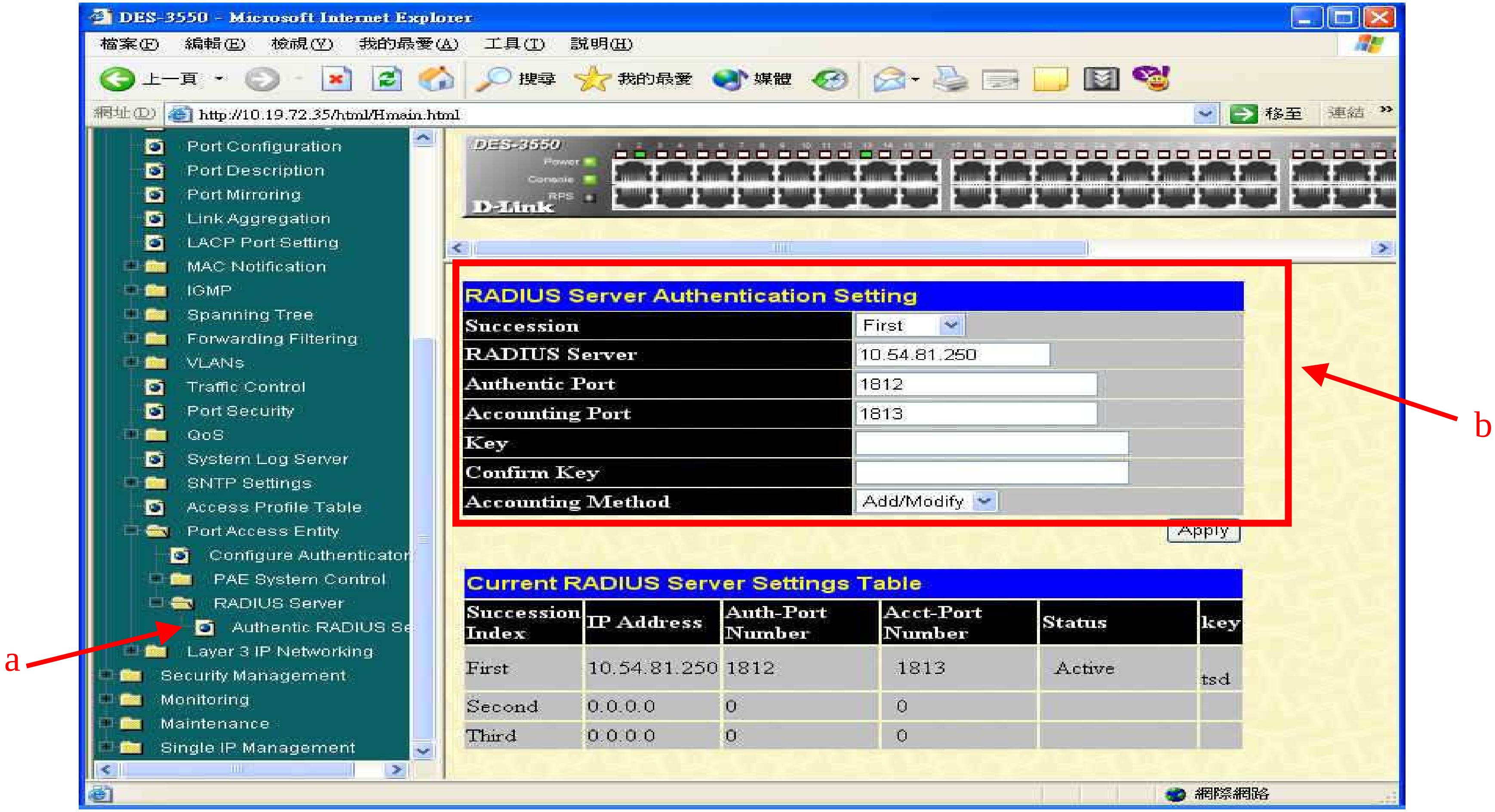
Port-based 802.1x example – Web GUI

3. Configure Radius Server setting

   a. Configuration → Port Access Entity →RADIUS Server →Authentic RADIUS Server

   b. set server IP, authentic port number and accounting port number, and Key for the server

4. Other 802.1x related setting are using default.



RADIUS Server Authentication Setting

Succession	First
RADIUS Server	10.54.81.250
Authentic Port	1812
Accounting Port	1813
Key	
Confirm Key	
Accounting Method	Add/Modify

Current RADIUS Server Settings Table

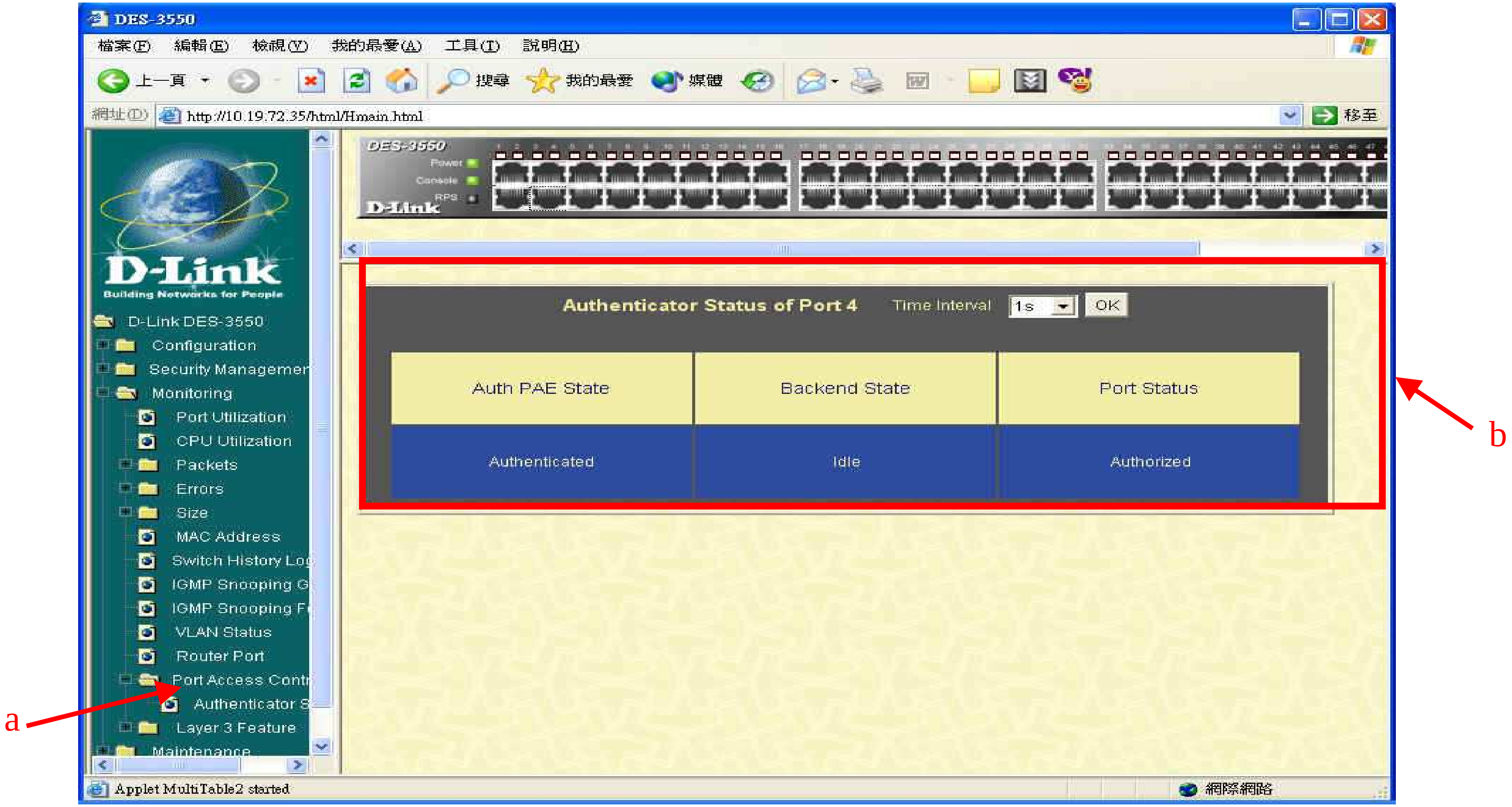
Succession Index	IP Address	Auth-Port Number	Acct-Port Number	Status	key
First	10.54.81.250	1812	1813	Active	tsd
Second	0.0.0.0	0	0		
Third	0.0.0.0	0	0		

Port-based 802.1x example – Web GUI

4. Check if the port which connects to client PC is authorized

   a. Monitoring → Port Access Control →Authenticator Status

   b. click on the port which connects client PC connect to, and you will see the port status ia "Authorized"



Authenticator Status of Port 4 Time Interval 1s OK

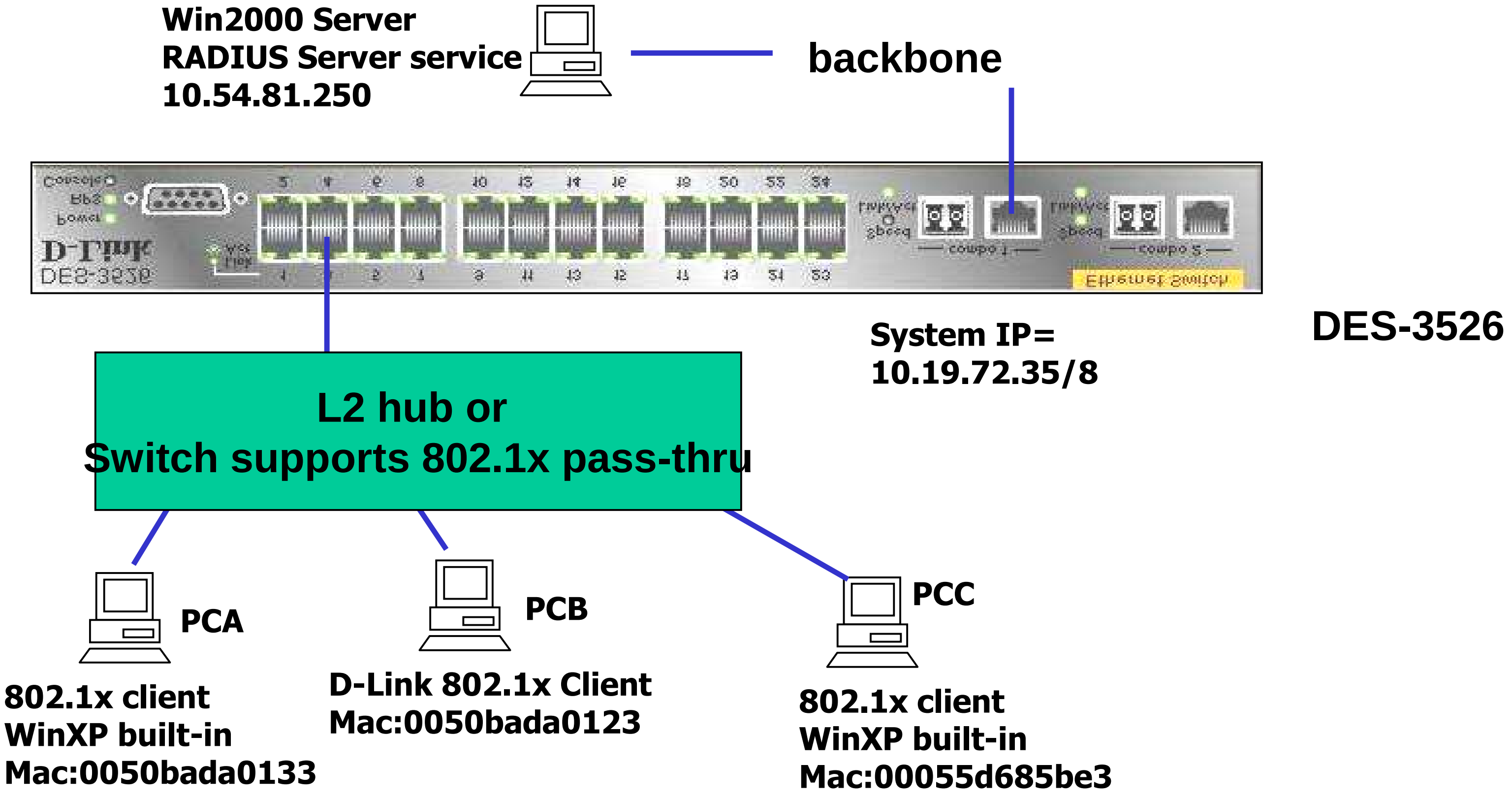
Auth PAE State	Backend State	Port Status
Authenticated	Idle	Authorized

Port-based 802.1x example – Web GUI

Notice:

- Radius: Windows NT/Windows 2000 Server Radius Server Service or third-party RADIUS server program.
- Workstation: 802.1x client is Window XP built-in. Otherwise, 802.1x client software is needed.

MAC-based 802.1x example



Each client needs to provide correct username/password to pass the authentication so that it can access the network.

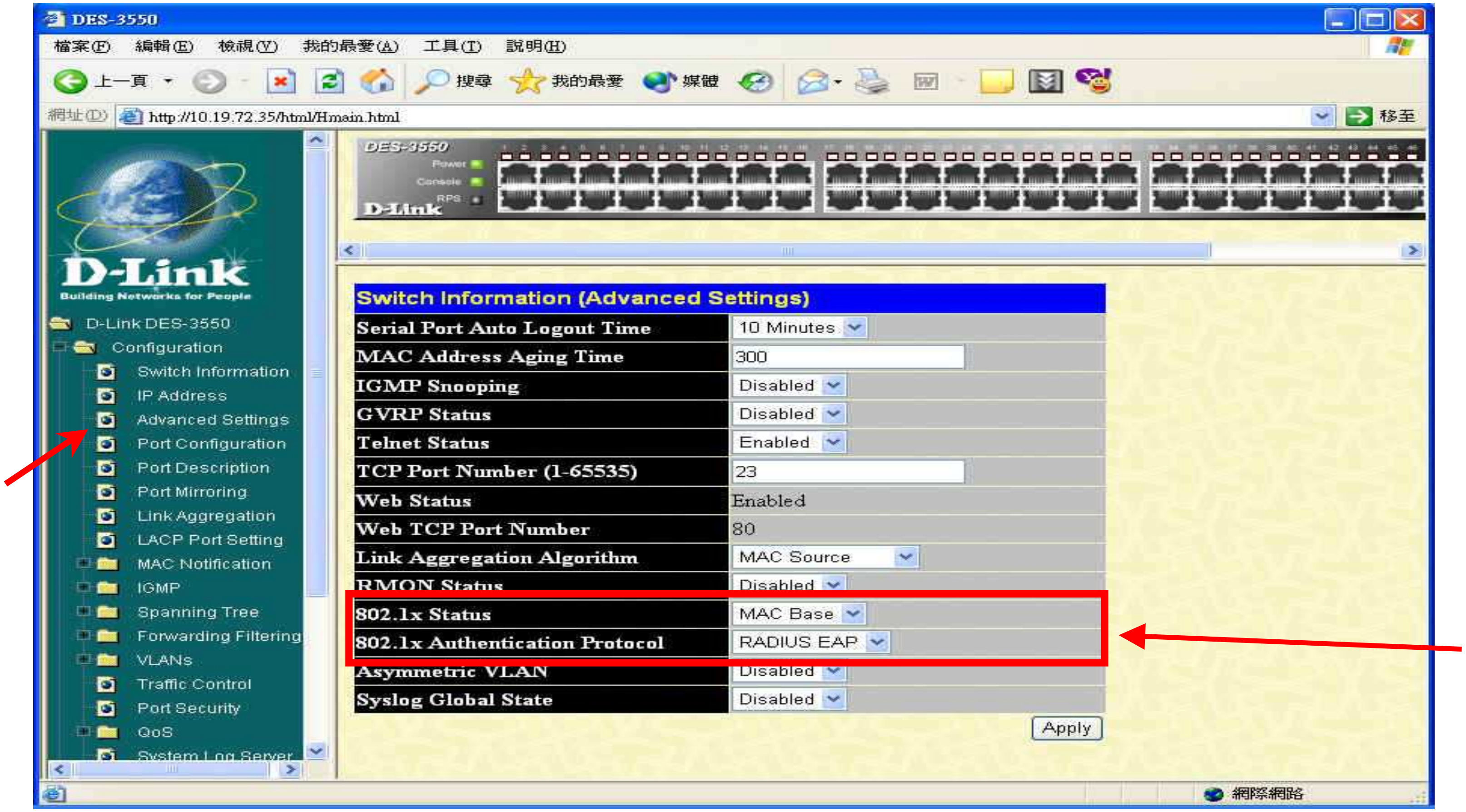
MAC-based 802.1x example – Web GUI

1. Enable 802.1x State by device, and change to port_based mode.

   a. Configuration →Advanced Settings

   b. Set 802.1X status as ***MAC Base*** to enable 802.1X.

   c. Set protocol as ***RADIUS EAP***



Switch Information (Advanced Settings)

Serial Port Auto Logout Time	10 Minutes
MAC Address Aging Time	300
IGMP Snooping	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
TCP Port Number (1-65535)	23
Web Status	Enabled
Web TCP Port Number	80
Link Aggregation Algorithm	MAC Source
RMON Status	Disabled
802.1x Status	MAC Base
802.1x Authentication Protocol	RADIUS EAP
Asymmetric VLAN	Disabled
Syslog Global State	Disabled

Apply

a

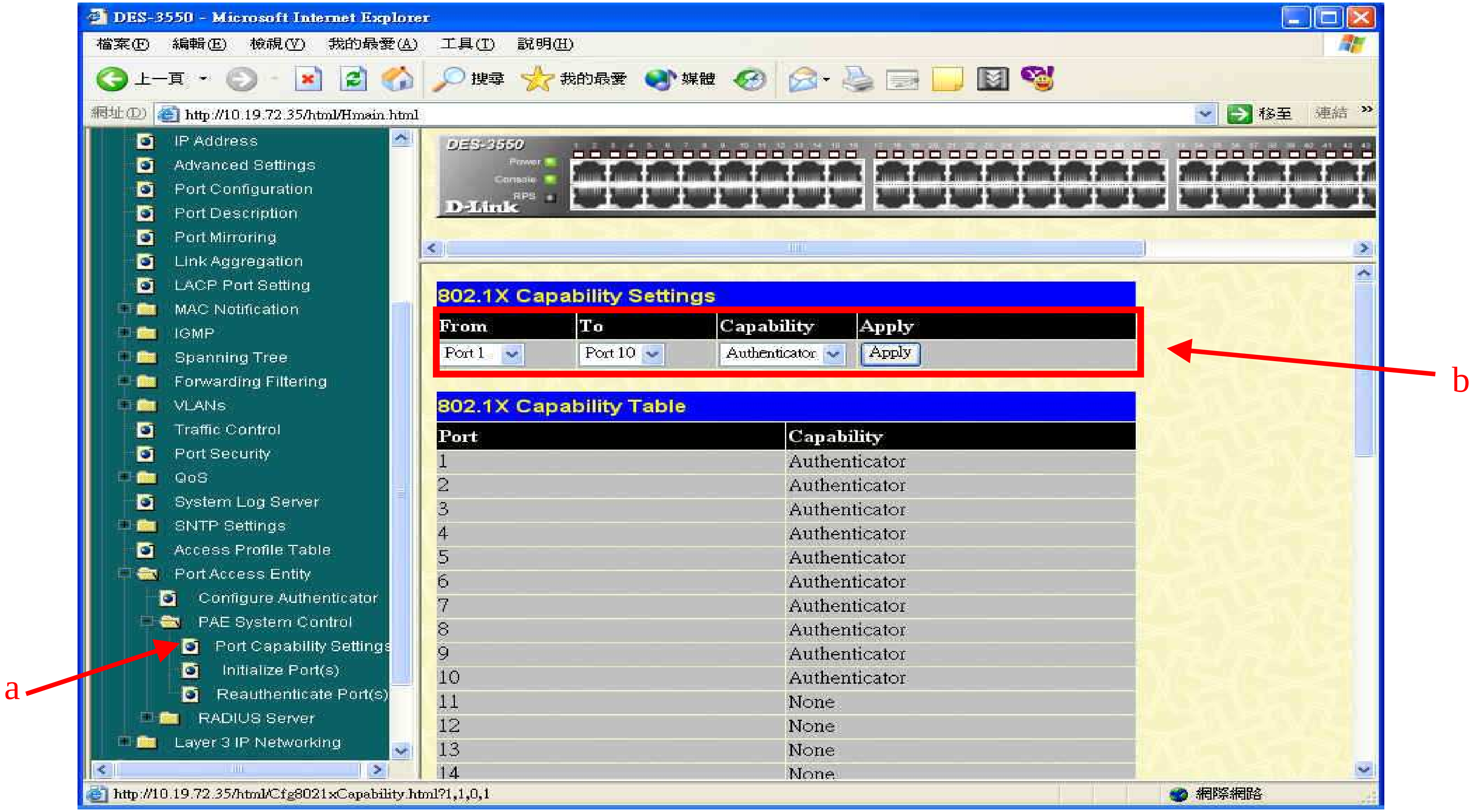
b, c

MAC-based 802.1x example – Web GUI

2. Setting 802.1x port setting by port

   a. Configuration → Port Access Entity →PAE System Control →Port Capability Settings

   b. set from port 1 to port 10 as authenticator



802.1X Capability Settings

From	To	Capability	Apply
Port 1	Port 10	Authenticator	Apply

802.1X Capability Table

Port	Capability
1	Authenticator
2	Authenticator
3	Authenticator
4	Authenticator
5	Authenticator
6	Authenticator
7	Authenticator
8	Authenticator
9	Authenticator
10	Authenticator
11	None
12	None
13	None
14	None

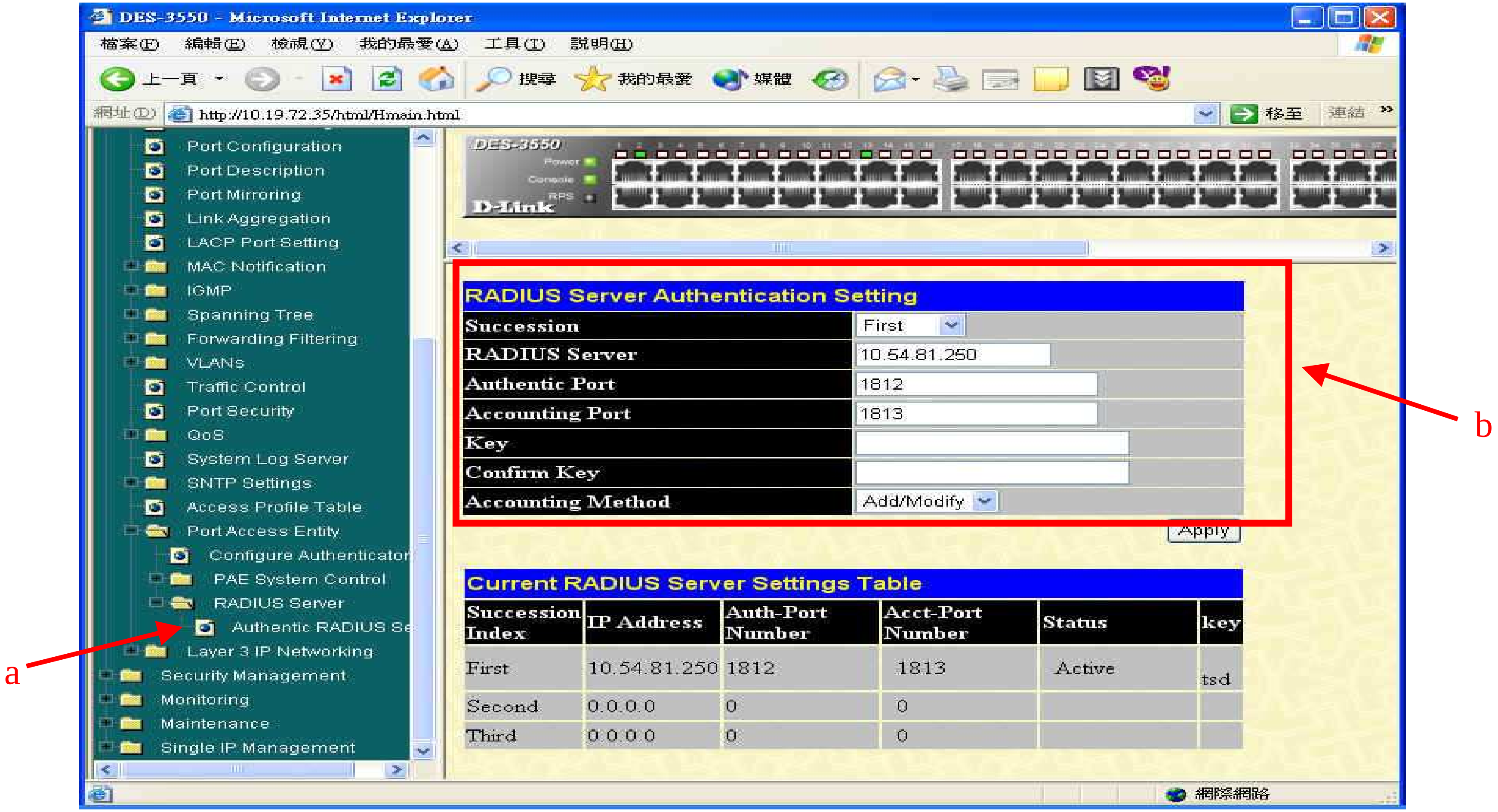
MAC-based 802.1x example – Web GUI

3. Configure Radius Server setting

   a. Configuration → Port Access Entity →RADIUS Server →Authentic RADIUS Server

   b. set server IP, authentic port number and accounting port number, and Key for the server.

4. **Other 802.1x related setting are using default.**



RADIUS Server Authentication Setting

Succession	First
RADIUS Server	10.54.81.250
Authentic Port	1812
Accounting Port	1813
Key	
Confirm Key	
Accounting Method	Add/Modify

Current RADIUS Server Settings Table

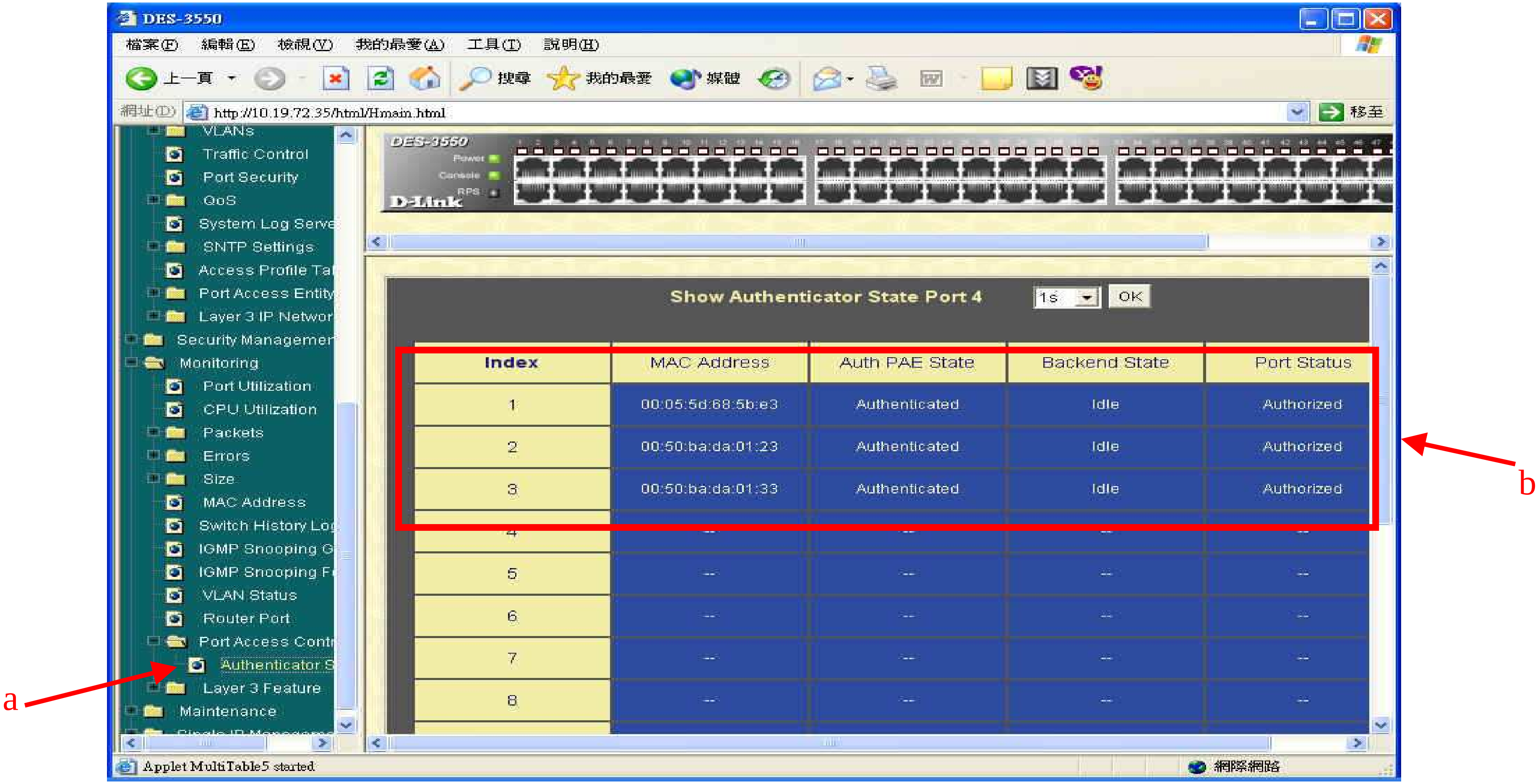
Succession Index	IP Address	Auth-Port Number	Acct-Port Number	Status	key
First	10.54.81.250	1812	1813	Active	tsd
Second	0.0.0.0	0	0		
Third	0.0.0.0	0	0		

MAC-based 802.1x example – Web GUI

4. Check if 3 client PC’s MAC are all learned into device

   a. Monitoring → Port Access Control →Authenticator Status

   b. click on the port which L2 hub connect to, and you will see the authenticator status(3 MAC addresses are learned)



Show Authenticator State Port 4

Index	MAC Address	Auth PAE State	Backend State	Port Status
1	00:05:5d:68:5b:e3	Authenticated	Idle	Authorized
2	00:50:ba:da:01:23	Authenticated	Idle	Authorized
3	00:50:ba:da:01:33	Authenticated	Idle	Authorized
4	--	--	--	--
5	--	--	--	--
6	--	--	--	--
7	--	--	--	--
8	--	--	--	--

MAC-based 802.1x example – Web GUI

Notice:

- Radius: Windows NT/Windows 2000 Server Radius Server Service or third-party RADIUS server program.
- Workstation: 802.1x client is Window XP built-in. Otherwise, 802.1x client software is needed.

THANK YOU