

4.7.5 Routing Table

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [+ Basic Setting](#)
- [+ Forwarding Rules](#)
- [+ Security Setting](#)
- [- Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- [+ Toolbox](#)

Routing Table

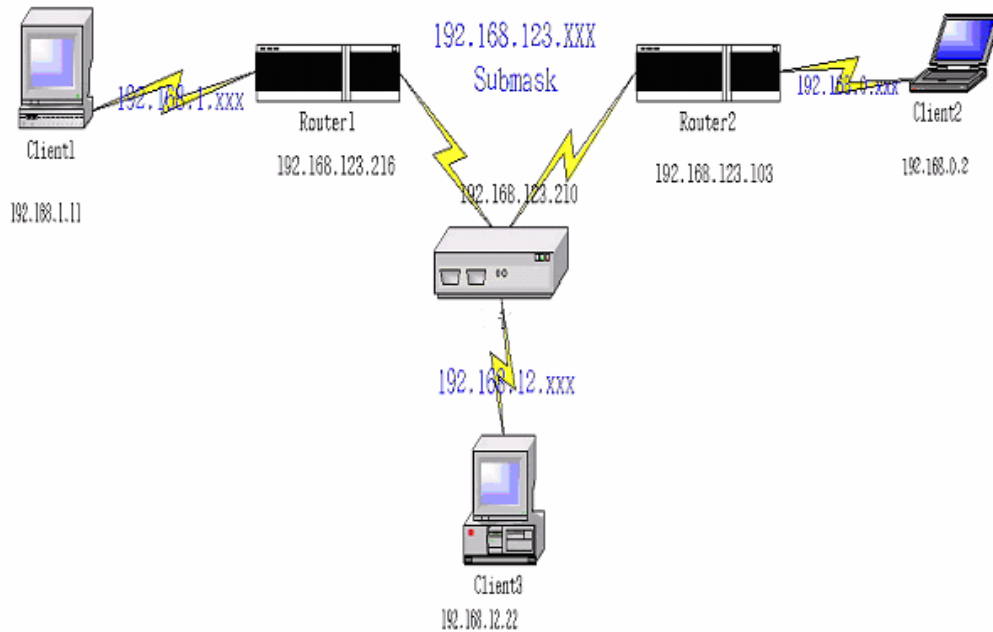
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

Example:



Configuration on NAT Router

Destination	SubnetMask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

4.7.6 Schedule Rule

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- [Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- + [Toolbox](#)

Log out

Schedule Rule

Item	Setting
► Schedule	☒ Enable

Rule#	Rule Name	Action
-------	-----------	--------

SaveAdd New Rule...Help

You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

Press “Add New Rule”

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- [Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- + [Toolbox](#)

Log out

Schedule Rule Setting

Item	Setting
▶ Name of Rule 1	ftp time

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:
Every Day	14 : 10	16 : 20

Save

Undo

Help

Back

After configure Rule 1→

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- [Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- + [Toolbox](#)

Log out

Schedule Rule

Item	Setting
► Schedule	☐ Enable

Rule#	Rule Name	Action
1	ftp time	EditDelete

Save

Add New Rule...

Help

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

Example1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- [Forwarding Rules](#)
 - [Virtual Server](#)
 - [Special AP](#)
 - [Miscellaneous](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.122.33	☒	1
2		192.168.122.	☐	0
3		192.168.122.	☐	0
4		192.168.122.	☐	0
5		192.168.122.	☐	0
6		192.168.122.	☐	0
7		192.168.122.	☐	0
8		192.168.122.	☐	0
9		192.168.122.	☐	0
10		192.168.122.	☐	0
11		192.168.122.	☐	0
12		192.168.122.	☐	0
13		192.168.122.	☐	0
14		192.168.122.	☐	0
15		192.168.122.	☐	0

Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- [Security Setting](#)
 - [Packet Filters](#)
 - [Domain Filters](#)
 - [URL Blocking](#)
 - [MAC Control](#)
 - [Miscellaneous](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

Outbound Packet Filter

Item
Setting

▶ Outbound Filter ☒ Enable

☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	:	: 20-21	☒	1
2	:	:	☐	0
3	:	:	☐	0
4	:	:	☐	0
5	:	:	☐	0
6	:	:	☐	0
7	:	:	☐	0
8	:	:	☐	0

Schedule rule (00)Always Copy to ID --

[Save](#)
[Undo](#)
[Inbound Filter...](#)
[MAC Level...](#)
[Help](#)

4.8 Toolbox

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- [Toolbox](#)
 - [View Log](#)
 - [Firmware Upgrade](#)
 - [Backup Setting](#)
 - [Reset to Default](#)
 - [Reboot](#)
 - [Miscellaneous](#)

Log out

Toolbox

- **View Log**
 - View the system logs.
- **Firmware Upgrade**
 - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
 - Save the settings of this device to a file.
- **Reset to Default**
 - Reset the settings of this device to the default values.
- **Reboot**
 - Reboot this device.
- **Miscellaneous**
 - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
 - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

4.8.1 System Log

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- [Toolbox](#)
 - [View Log](#)
 - [Firmware Upgrade](#)
 - [Backup Setting](#)
 - [Reset to Default](#)
 - [Reboot](#)
 - [Miscellaneous](#)

Log out

System Log

WAN Type: Dynamic IP Address (R1.9414vTIG)
Display time: Wed Oct 01 00:10:04 2003

2003年10月1日 上午 12:01:30 DOD:TCP trigger from 192.168.123.125:2288 to 207.46.104.20:186

2003年10月1日 上午 12:01:30 DHCP:discover()

2003年10月1日 上午 12:01:34 DHCP:discover()

2003年10月1日 上午 12:01:35 Admin from 192.168.123.125 login successfully

2003年10月1日 上午 12:01:42 DHCP:discover()

2003年10月1日 上午 12:01:58 DHCP:discover()

2003年10月1日 上午 12:02:47 DOD:triggered internally

2003年10月1日 上午 12:02:47 DHCP:discover()

2003年10月1日 上午 12:02:51 DHCP:discover()

2003年10月1日 上午 12:02:59 DHCP:discover()

2003年10月1日 上午 12:03:15 DHCP:discover()

2003年10月1日 上午 12:03:48 DOD:triggered internally

2003年10月1日 上午 12:03:48 DHCP:discover()

2003年10月1日 上午 12:03:52 DHCP:discover()

2003年10月1日 上午 12:04:00 DHCP:discover()

2003年10月1日 上午 12:04:16 DHCP:discover()

Back

Refresh

Download

Clear

You can View system log by clicking the **View Log** button

4.8.2 Firmware Upgrade

Administrator's Main Menu

- [Status](#)
- [Wizard](#)

+ [Basic Setting](#)

+ [Forwarding Rules](#)

+ [Security Setting](#)

+ [Advanced Setting](#)

- [Toolbox](#)

- [View Log](#)
- [Firmware Upgrade](#)
- [Backup Setting](#)
- [Reset to Default](#)
- [Reboot](#)
- [Miscellaneous](#)

Log out

Firmware Upgrade

Firmware Filename

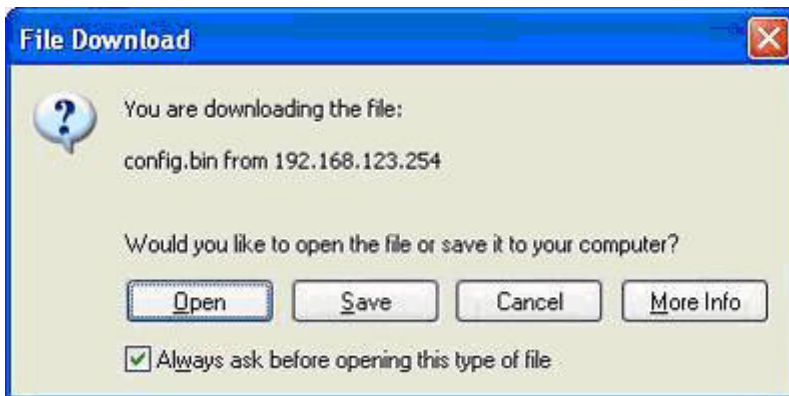
瀏覽...

Current firmware version is R1.9414vTIG. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

Upgrade Cancel

You can upgrade firmware by clicking **Firmware Upgrade** button.

4.8.3 Backup Setting



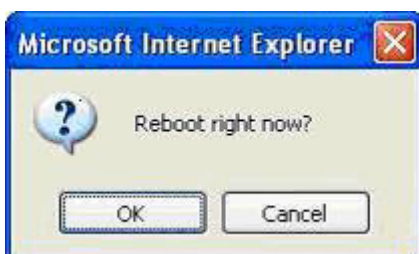
You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

4.8.4 Reset to default



You can also reset this product to factory default by clicking the **Reset to default** button.

4.8.5 Reboot



You can also reboot this product by clicking the **Reboot** button.

4.8.6 Miscellaneous Items

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- [Toolbox](#)
 - [View Log](#)
 - [Firmware Upgrade](#)
 - [Backup Setting](#)
 - [Reset to Default](#)
 - [Reboot](#)
 - [Miscellaneous](#)

Log out

Miscellaneous Items

Item	Setting
▶ MAC Address for Wake-on-LAN	Wake up

Save

Undo

Help

MAC Address for Wake-on-LAN

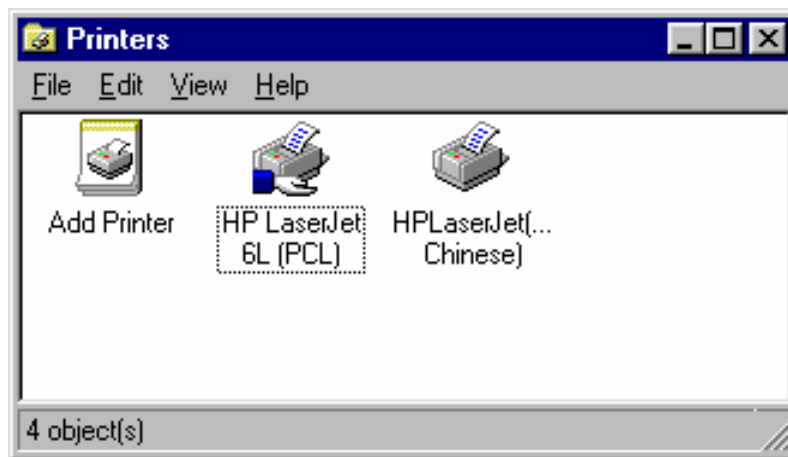
Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Chapter 5 Print Server

This product provides the function of network print server for MS Windows 95/98/NT/2000 and Unix based platforms. (If the product you purchased doesn't have printer port, please skip this chapter.)

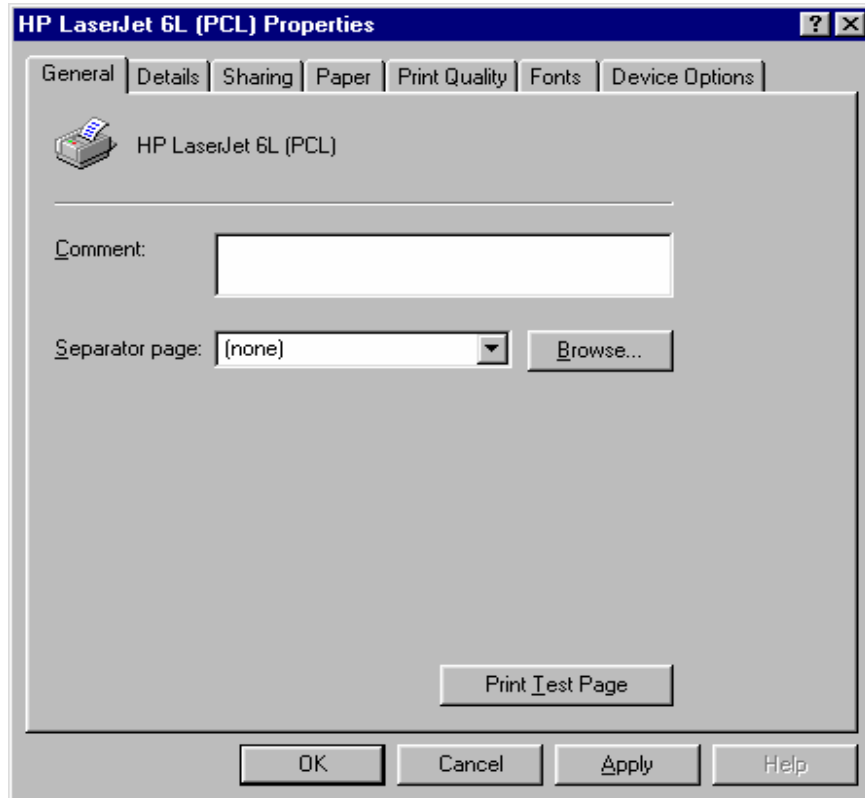
5.1 Configuring on Windows 95/98 Platforms

After you finished the software installation procedure described in Chapter 3, your computer has possessed the network printing facility provided by this product. For convenience, we call the printer connected to the printer port of this product as server printer. On a Windows 95/98 platform, open the **Printers** window in the **My Computer** menu:

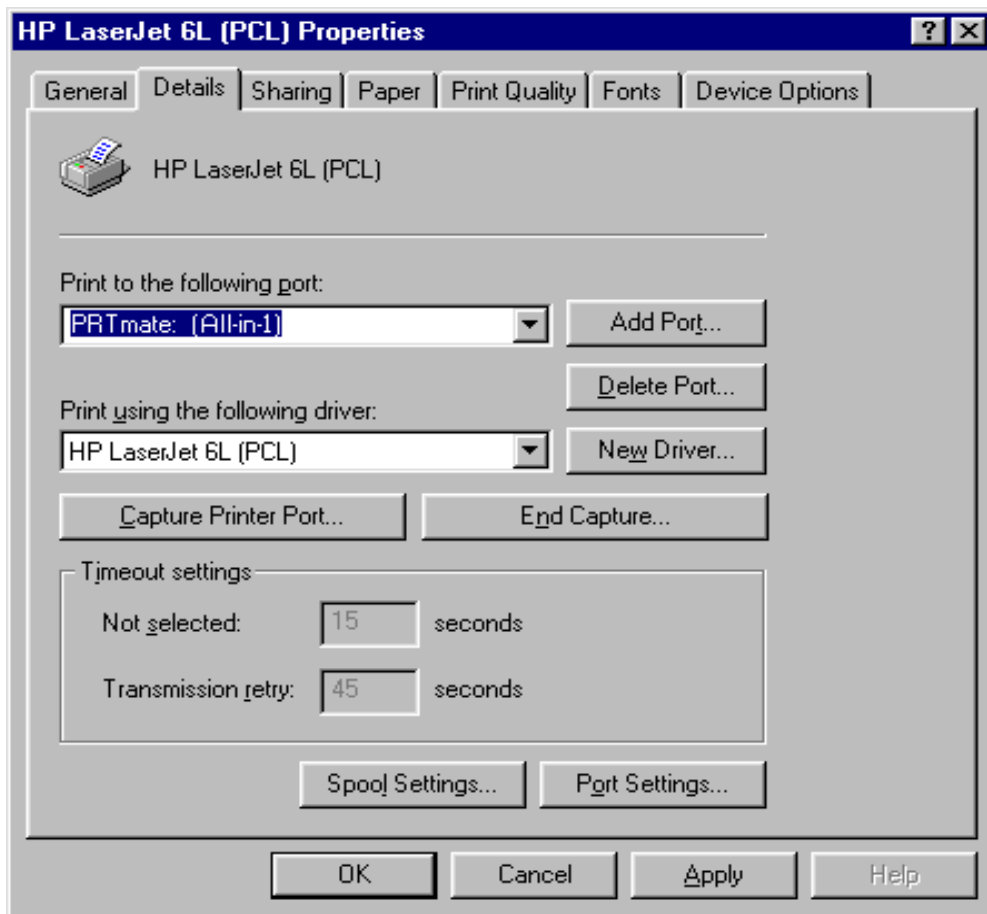


Now, you can configure the print server of this product:

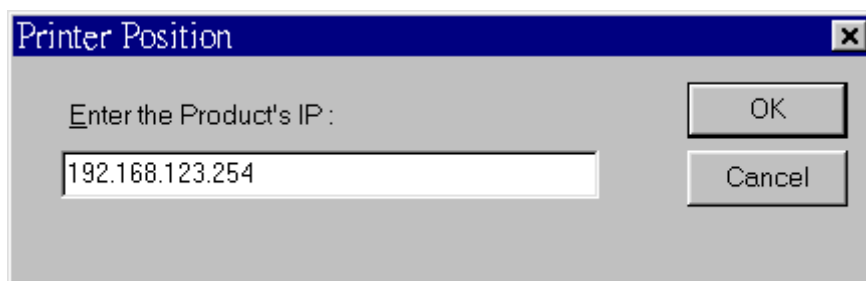
1. Find out the corresponding icon of your server printer, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the **Properties** item:



2. Click the **Details** item:



3. Choose the "PRTmate: (All-in-1)" from the list attached at the **Print To** item. Be sure that the **Printer Driver** item is configured to the correct driver of your server printer.
4. Click on the button of **Port Settings**:

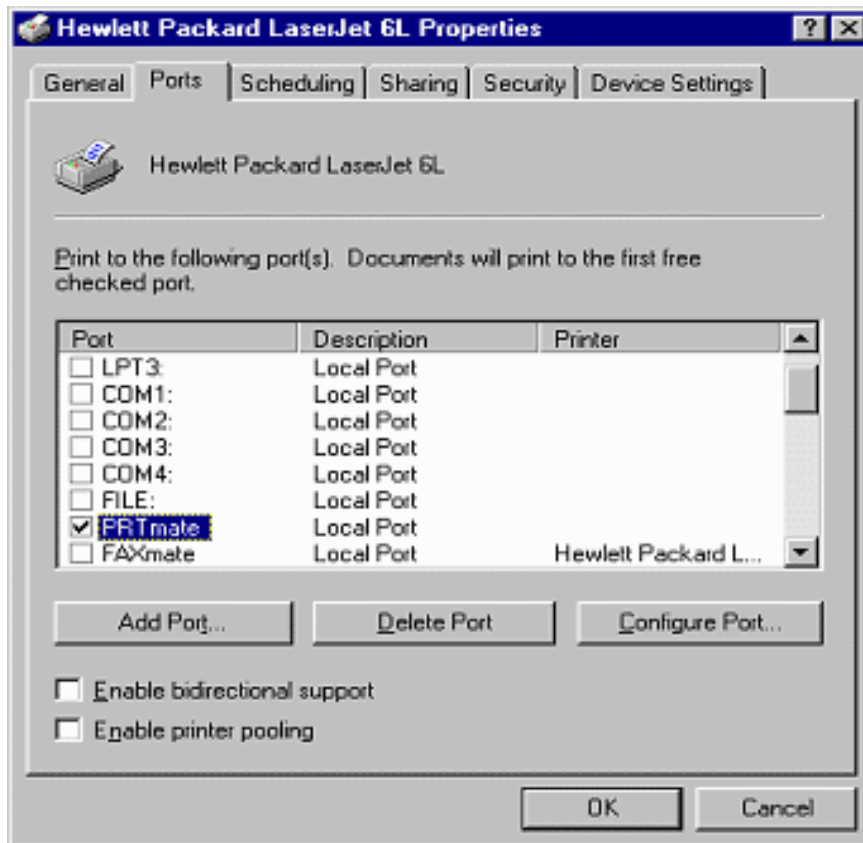


Type in the IP address of this product and then click the **OK** button.

6. Make sure that all settings mentioned above are correct and then click the **OK** button.

5.2 Configuring on Windows NT Platforms

The configuration procedure for a Windows NT platform is similar to that of Windows 95/98 except the screen of printer **Properties**:



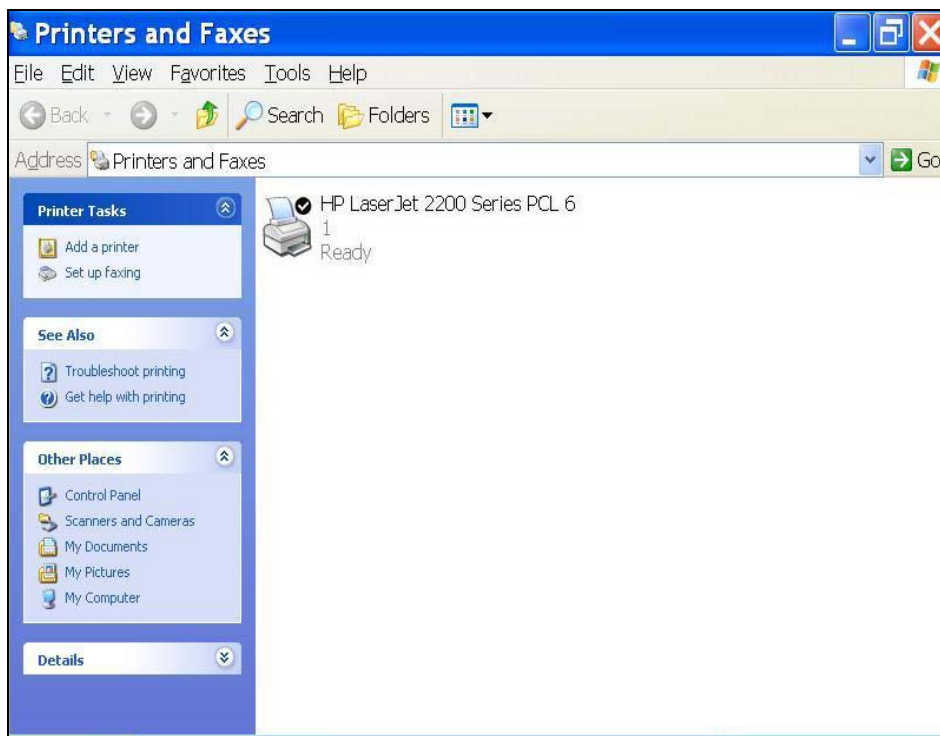
Compared to the procedure in last section, the selection of **Details** is equivalent to the selection of **Ports**, and **Port Settings** is equivalent to **Configure Port**.

5.3 Configuring on Windows 2000 and XP Platforms

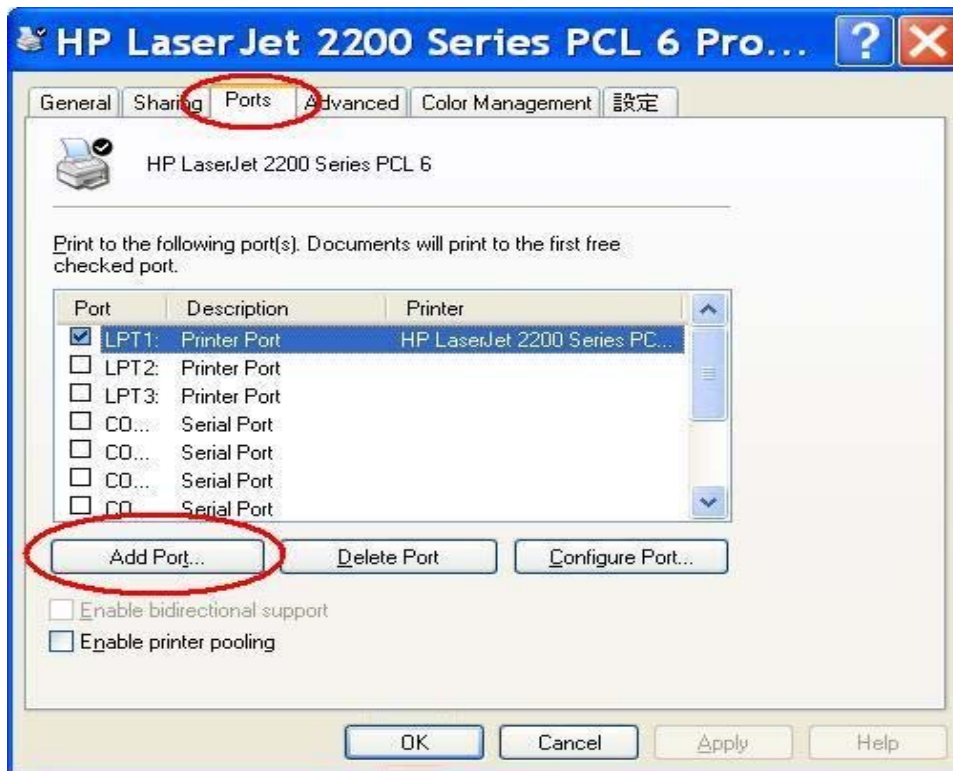
Windows 2000 and XP have built-in LPR client, users could utilize this feature to Print.

You have to install your Printer Driver on LPT1 or other ports before you preceed the following sequence.

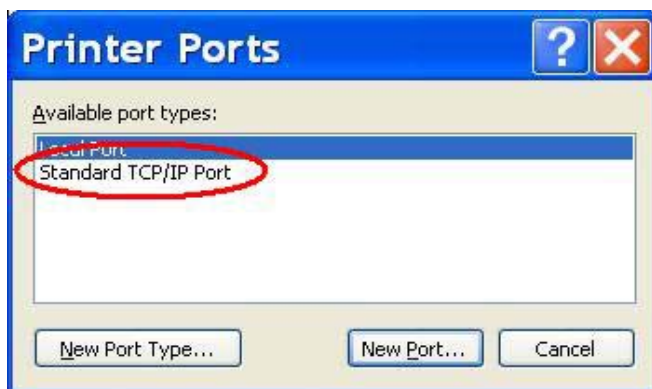
1.Open Printers and Faxes.



2. Select “Ports” page, Click “Add Port...”

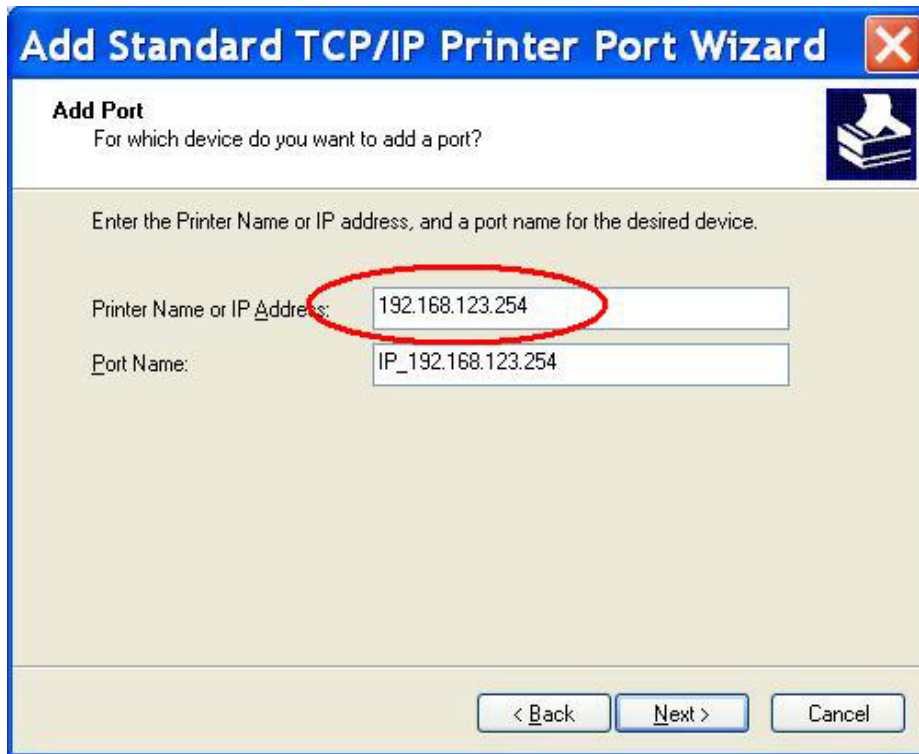


3. Select “Standard TCP/IP Port”, and then click “New Port...”



4. Click Next and then provide the following information:

Type address of server providing LPD that is our NAT device: 192.168.123.254



Add Standard TCP/IP Printer Port Wizard

Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.123.254

Port Name: IP_192.168.123.254

< Back Next > Cancel

1. Select Custom, then click “Settings...”



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required
The device could not be identified.

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

☐ Standard Generic Network Card

☒ Custom Settings...

< Back Next > Cancel

6. Select "LPR", type "lp" lowercase letter in "Queue Name:"

And enable "LPR Byte Counting Enabled".

Configure Standard TCP/IP P...

Port Settings

Port Name: IP_192.168.123.254

Printer Name or IP Address: 192.168.123.254

Protocol

☐ Raw ☒ LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: lp

☒ LPR Byte Counting Enabled

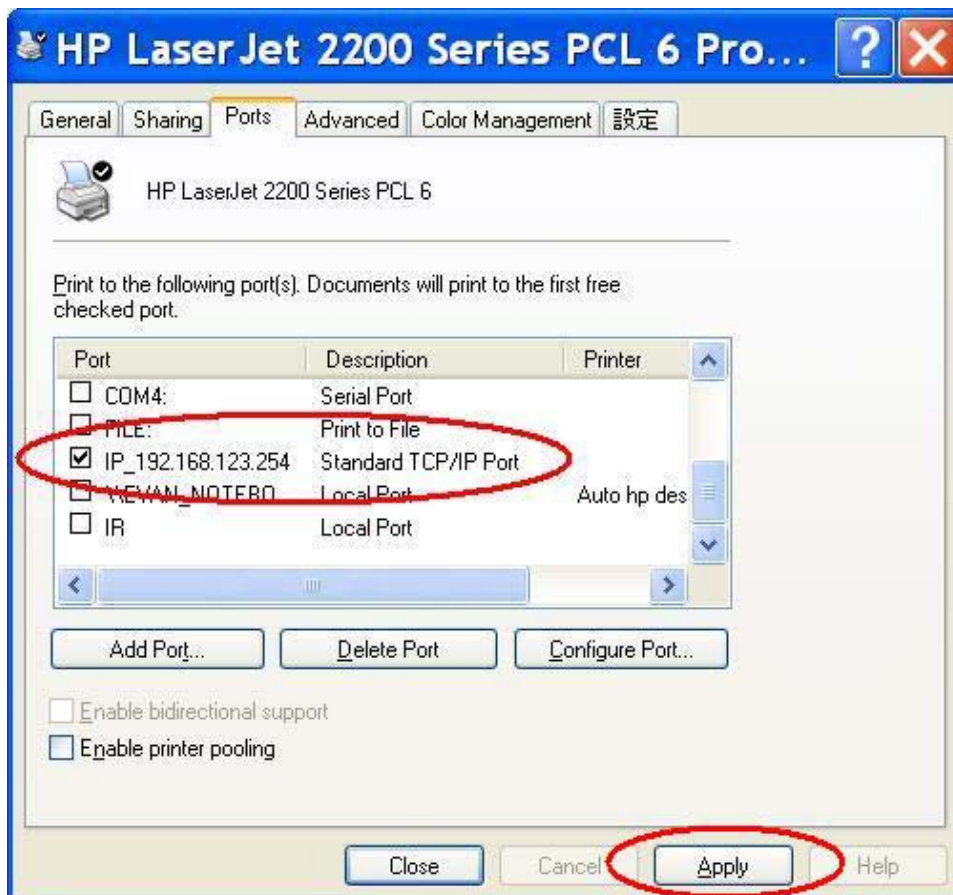
☐ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

OK Cancel

7. Apply your settings



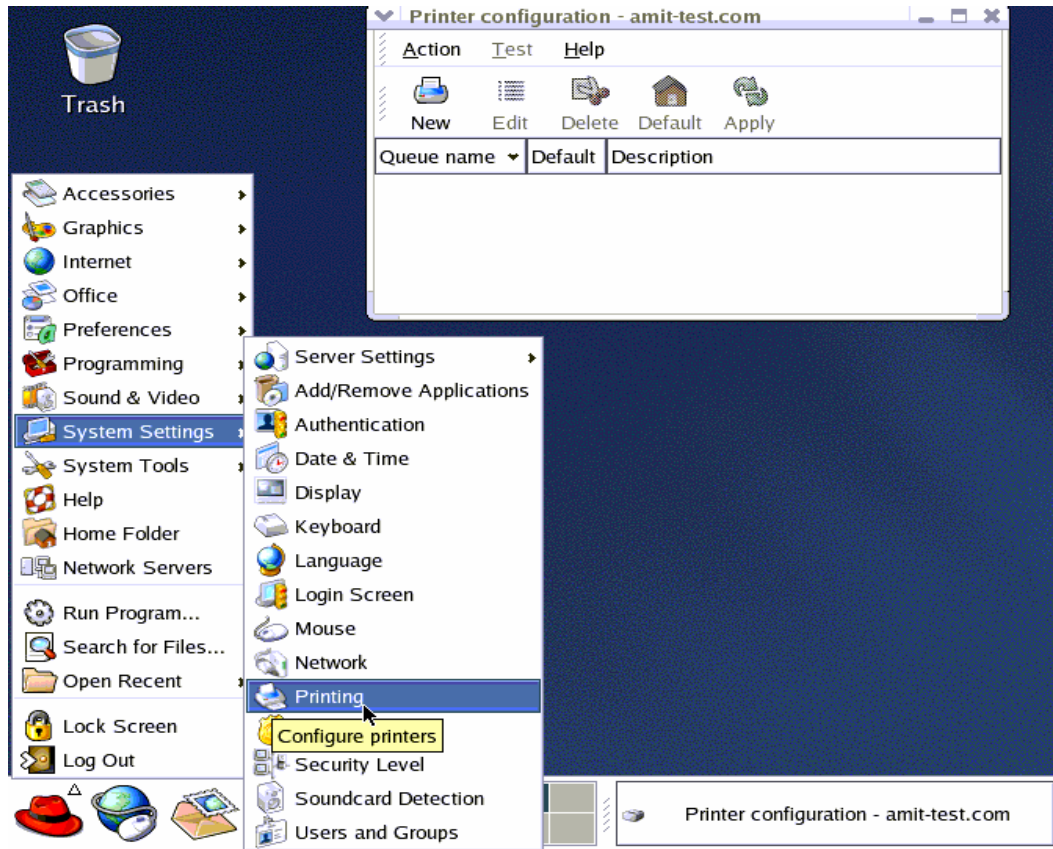
5.4 Configuring on Unix-like based Platforms

Please follow the traditional configuration procedure on Unix platforms to setup the print server of this product. The printer name is “lp.”

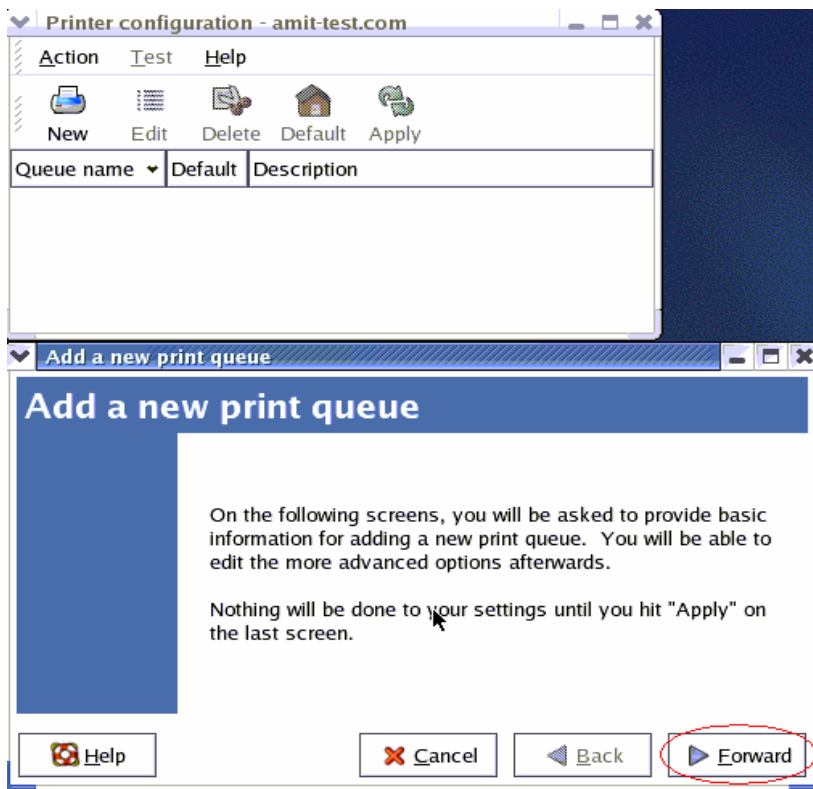
In X-Windows, for example, In Redhat Platforms,

Please follow the below steps to configure your printer on Red Hat 9.0.1. Start from the Red Hat--->

System Setting---> Printing.



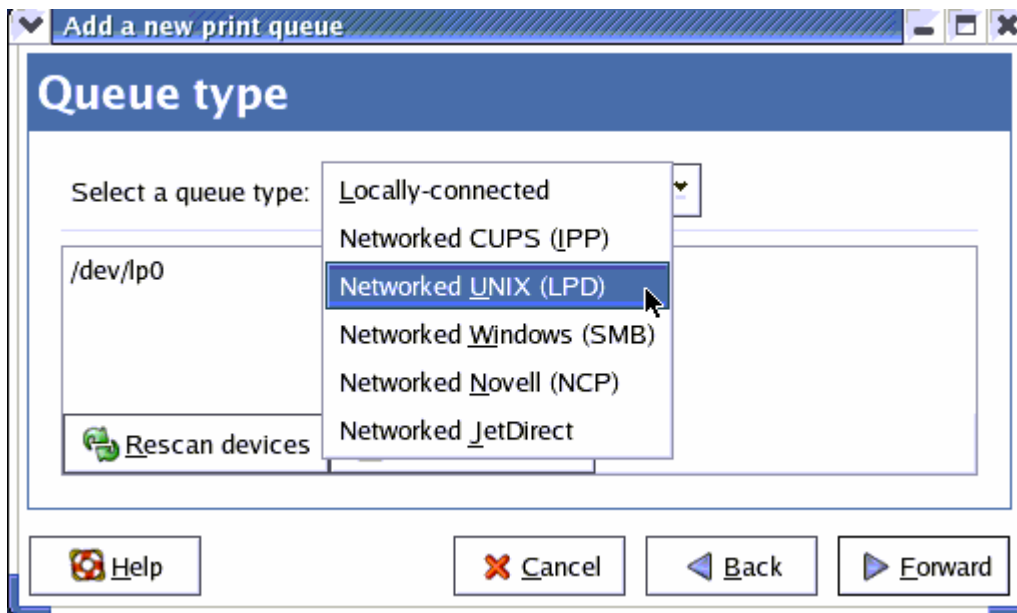
2. Click New---> Forward.



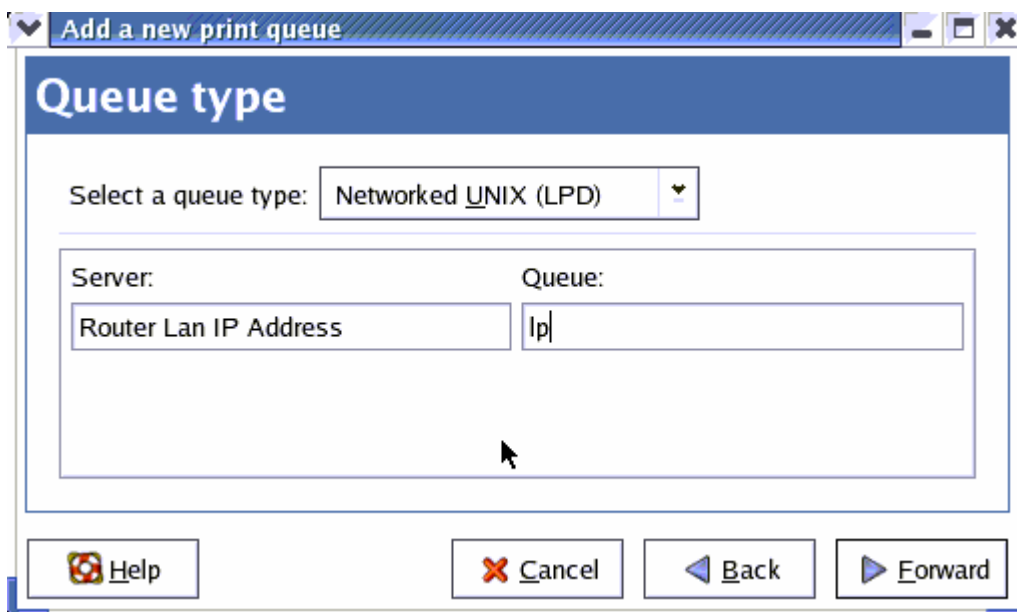
1. Enter the Pinter Name, Comments then forward.

The screenshot shows the 'Add a new print queue' dialog box at the 'Queue name' step. The dialog has a blue header bar with the title 'Queue name'. Below the header, the text reads: 'Please enter a name for this queue. Choose a short name that begins with a letter and contains no spaces.' There is a text input field labeled 'Name:' containing the text 'printertest'. Below this is a section titled 'About' with the text: 'If you like, you can enter a description of the printer to help you identify it more easily.' There is a text input field labeled 'Short description:' containing the text 'test'. At the bottom of the dialog are four buttons: 'Help' (with a question mark icon), 'Cancel' (with a red X icon), 'Back' (with a left arrow icon), and 'Forward' (with a right arrow icon).

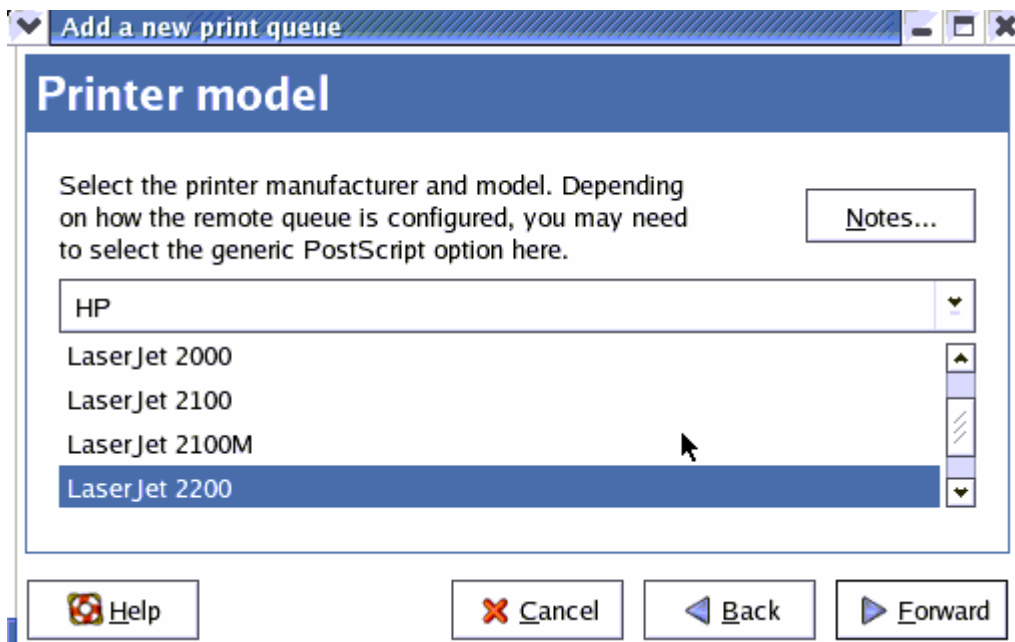
4. Select LPD protocol and then forward.



5. Enter Router LAN IP Address and the queue name "lp". Then forward.



6. Select the Printer Brand and Model Name. Then Forward.



7. Click Apply to finish setup.



8. At last you must click Apply on the toolbox to make the change take effective.

In Command Mode:

Linux has built-in LPR client ,You can utilize it for printing.

You can manual set it or via the tool "printtool" in X-windows.

PS: The spool name is "lp"-----all lowercase letter.

Below is my setting.

/etc/printcap

```
-----  
lp:\  
:sd=/var/spool/lpd/lp:\  
:mx#0:\  
:sh:\  
:rm=192.168.123.254:\  
:rp=lp:\ ----->key point  
:if=/var/spool/lpd/lp/filter:  
-----
```

Then add the corresponding directory

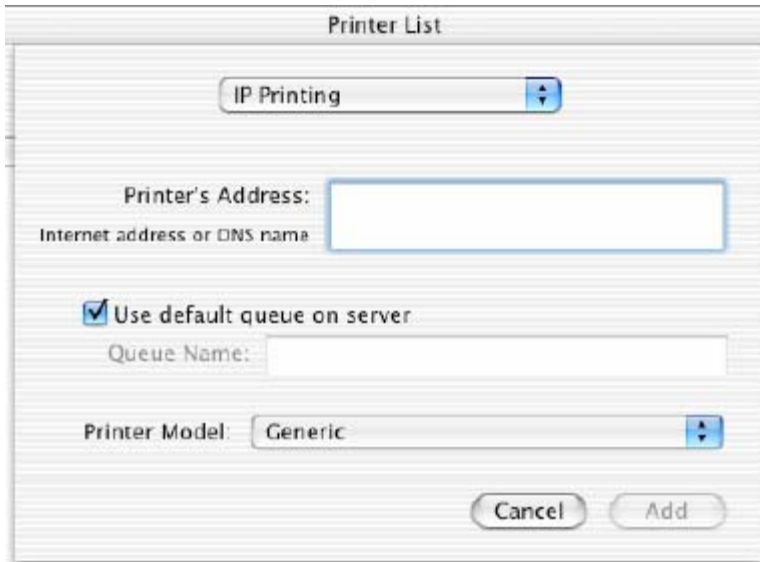
```
#mkdir /var/spool/lpd/lp
```

Too see the detail ,please refer to the online manual in linux.

```
#man printcap
```

5.5 Configuring on Apple PC

1.First, go to Printer center (Printer list) and add printer



Printer List

IP Printing

Printer's Address:

Internet address or DNS name

☒ Use default queue on server

Queue Name:

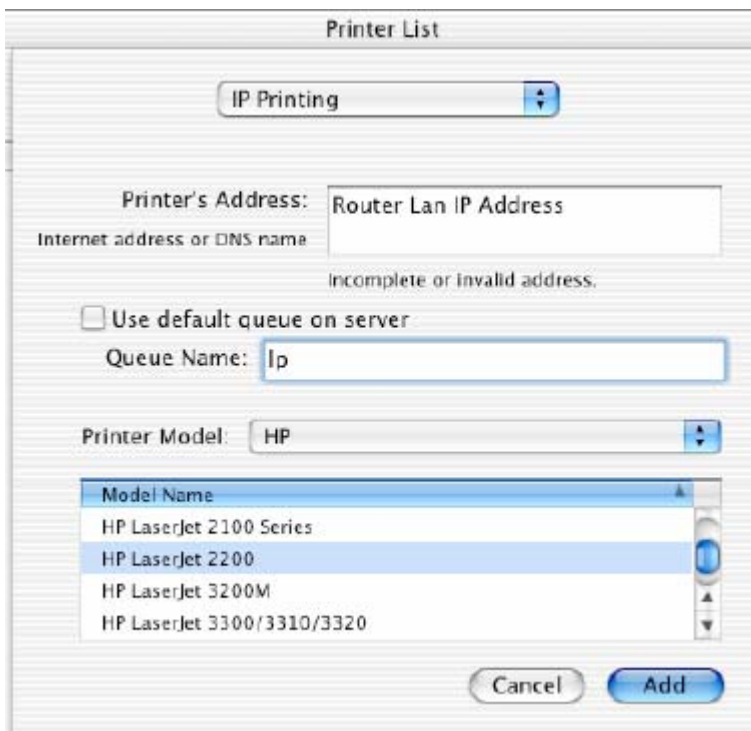
Printer Model: Generic

Cancel Add

2.Choose [IP print](#) and setup [printer ip address](#) (router Lan ip address).

3.Disable “[Default Queue of Server.](#)” And fill in ‘ [Ip](#) ‘ in Queue name item.

4.Printer Model: Choose “[General](#)” or Printer as below.



Printer List

IP Printing

Printer's Address: Router Lan IP Address

Internet address or DNS name

Incomplete or invalid address.

☐ Use default queue on server

Queue Name: Ip

Printer Model: HP

Model Name

- HP LaserJet 2100 Series
- HP LaserJet 2200
- HP LaserJet 3200M
- HP LaserJet 3300/3310/3320

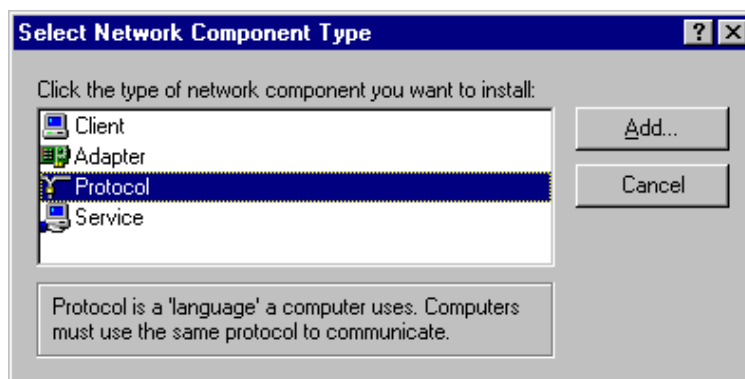
Cancel Add

Appendix A TCP/IP Configuration for Windows 95/98

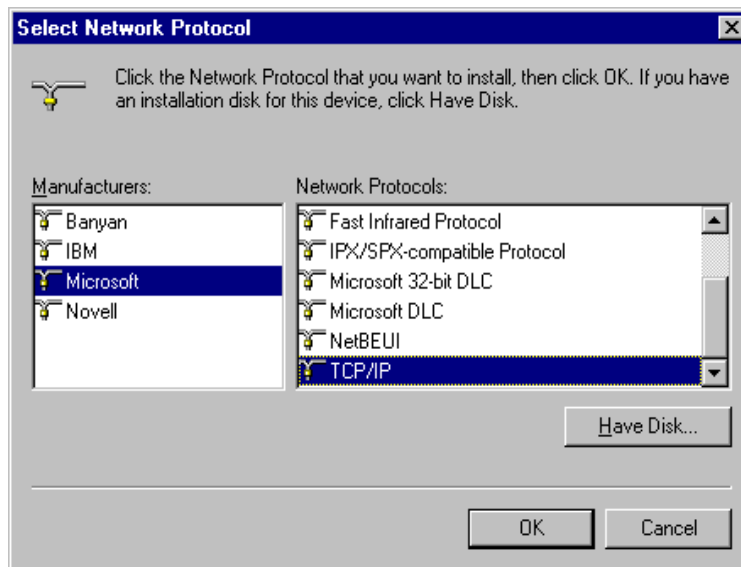
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



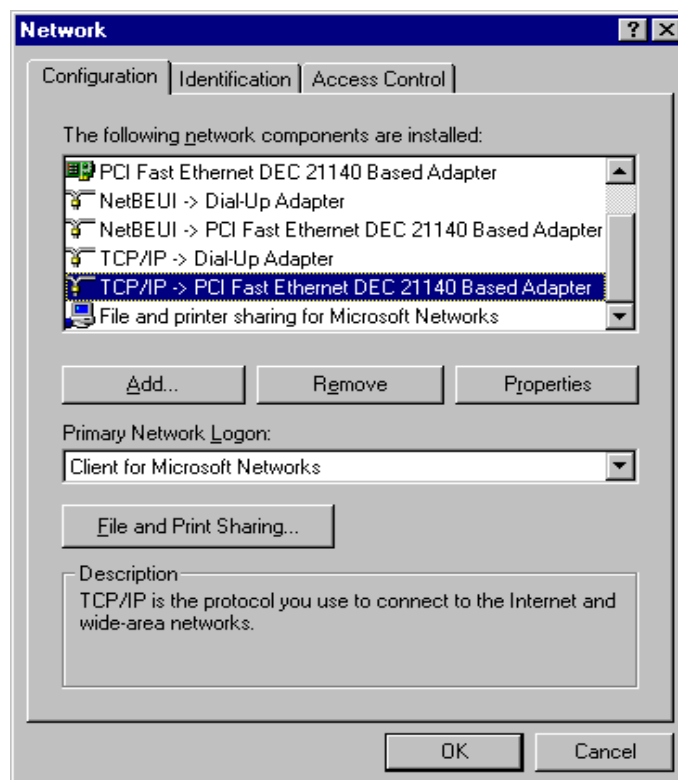
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.



3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:

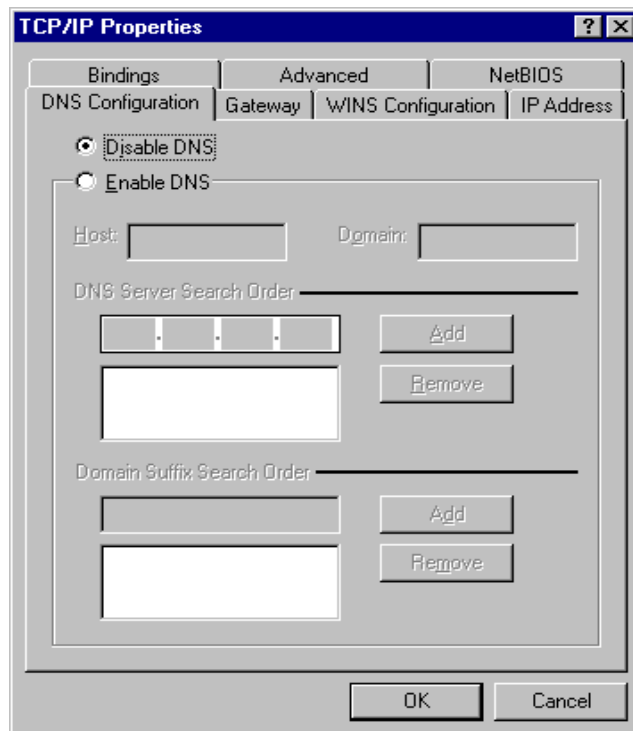
- a. Select **Obtain an IP address automatically** in the IP Address tab.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'IP Address' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are tabs for 'Bindings', 'Advanced', and 'NetBIOS'. Under 'Advanced', there are sub-tabs for 'DNS Configuration', 'Gateway', 'WINS Configuration', and 'IP Address'. The main area contains a text box with the following text: 'An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.' Below this text are two radio buttons. The first radio button is selected and is labeled 'Obtain an IP address automatically'. The second radio button is labeled 'Specify an IP address:'. Below the second radio button is a group box containing two input fields: 'IP Address:' and 'Subnet Mask:'. Each input field is a four-part box with dots, currently empty. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- b. Don't input any value in the Gateway tab.

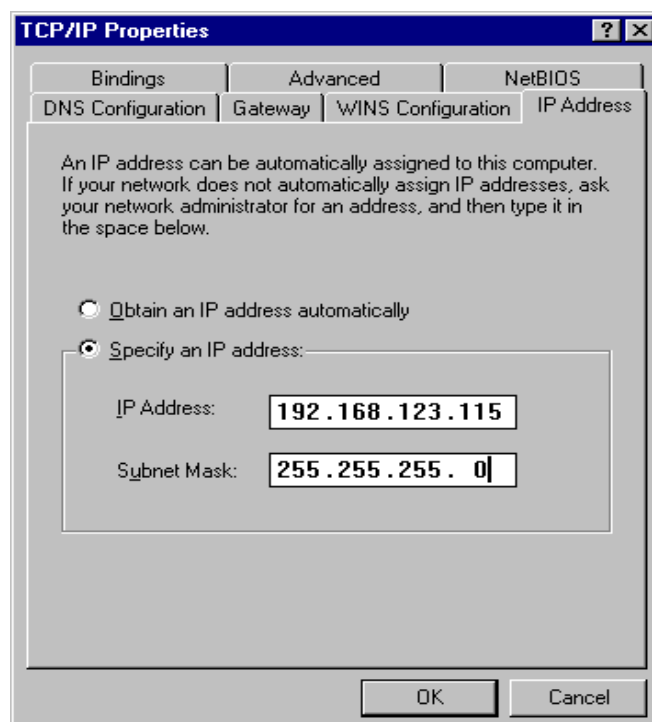
The screenshot shows the 'TCP/IP Properties' dialog box with the 'Gateway' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are tabs for 'Bindings', 'Advanced', and 'NetBIOS'. Under 'Advanced', there are sub-tabs for 'DNS Configuration', 'Gateway', 'WINS Configuration', and 'IP Address'. The main area contains a text box with the following text: 'The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.' Below this text is a section labeled 'New gateway:' with a four-part input field (dots) and an 'Add' button. Below this is a section labeled 'Installed gateways:' with a large empty rectangular box and a 'Remove' button. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- c. Choose **Disable DNS** in the DNS Configuration tab.



B. Configure IP manually

- a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



- b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'Gateway' tab selected. The 'New gateway:' field contains the IP address '192.168.123.254'. Below it, the 'Installed gateways:' list is empty. The 'Add' button is visible next to the 'New gateway:' field, and the 'Remove' button is next to the 'Installed gateways:' list. The 'OK' and 'Cancel' buttons are at the bottom right.

- c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'DNS Configuration' tab selected. The 'Enable DNS' radio button is selected. The 'Host:' field contains 'MyComputer' and the 'Domain:' field is empty. The 'DNS Server Search Order' list contains the IP address '168.95.1.1'. The 'Add' button is visible next to the 'DNS Server Search Order' list, and the 'Remove' button is next to the list. The 'OK' and 'Cancel' buttons are at the bottom right.

Appendix B 802.1x Setting

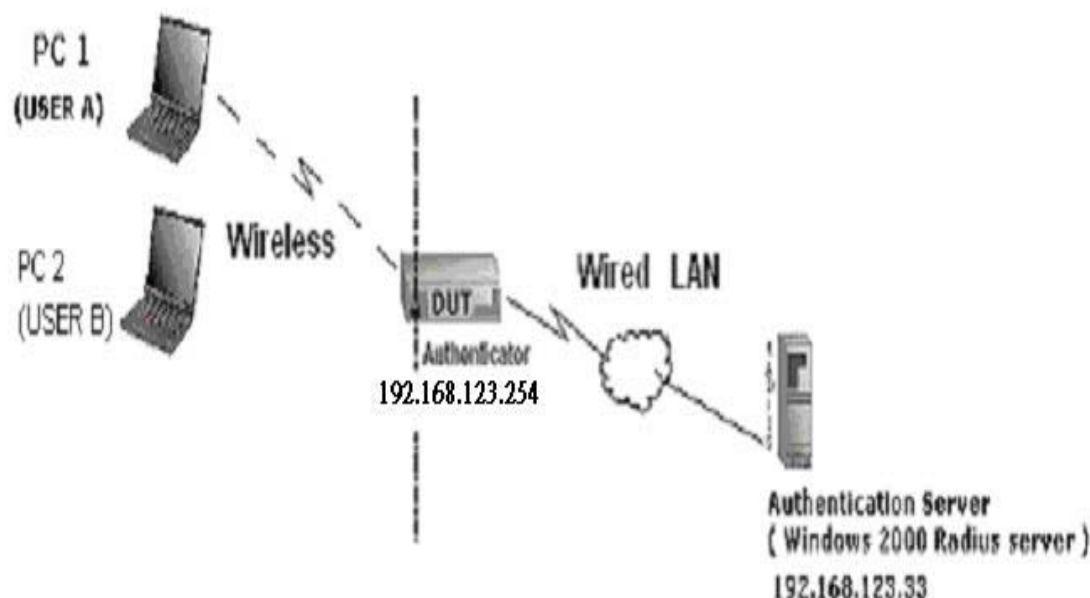


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

1 Equipment Details

PC1:

Microsoft Windows XP Professional without Service Pack 1.

D-Link DWL-650+ wireless LAN adapter

Driver version: 3.0.5.0 (Driver date: 03.05.2003)

PC2:

Microsoft Windows XP Professional with Service Pack 1a.

Z-Com XI-725 wireless LAN USB adapter

Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 (You can get more information from <http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>)

2 DUT

Configuration:

- 1.Enable DHCP server.
- 2.WAN setting: static IP address.
- 3.LAN IP address: 192.168.123.254/24.
- 4.Set RADIUS server IP.
- 5.Set RADIUS server shared key.
- 6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

3. DUT and Windows 2000 Radius Server Setup

3-1-1. Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

3-1-2. Setup DUT

- 1.Enable the 802.1X (check the “Enable checkbox“).
- 2.Enter the RADIUS server IP.
- 3.Enter the shared key. (The key shared by the RADIUS server and DUT).
- 4.We will change 802.1X encryption key length to fit the variable test condition.

3-1-3. Setup Network adapter on PC

- 1.Choose the IEEE802.1X as the authentication method. (Fig 2)

Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

- 2.Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
- 3.If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)

4. We will change EAP type to fit the variable test condition.

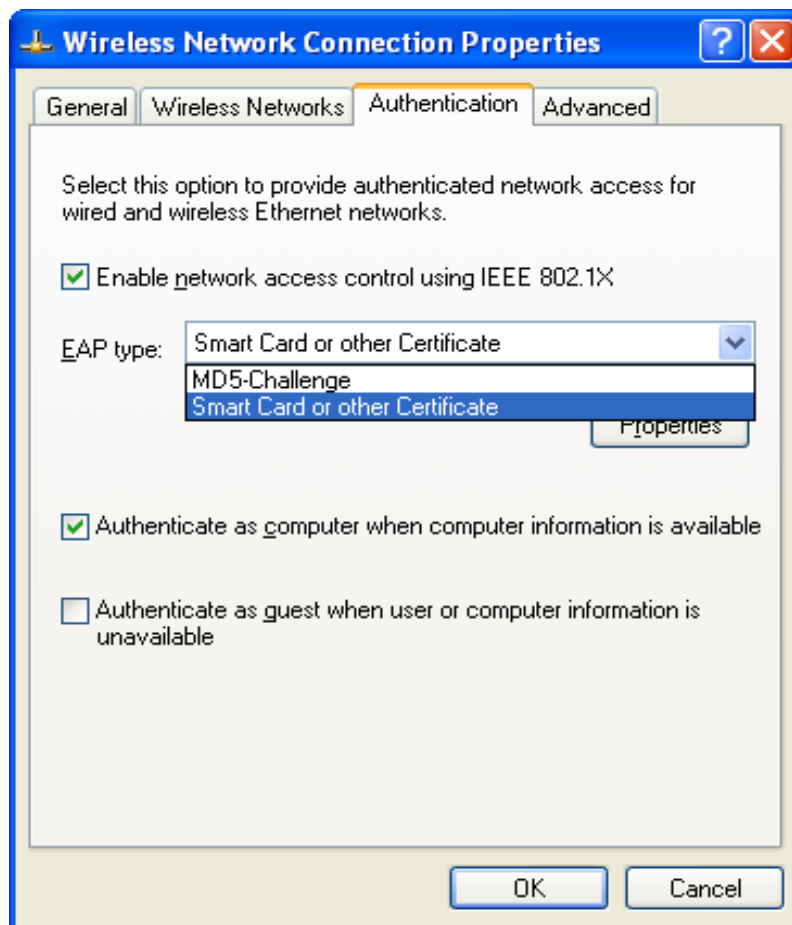


Figure 2: Enable IEEE 802.1X access control

Figure 3: Smart card or certificate properties

4. Windows 2000 RADIUS server Authentication testing:

4.1 DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 choose the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

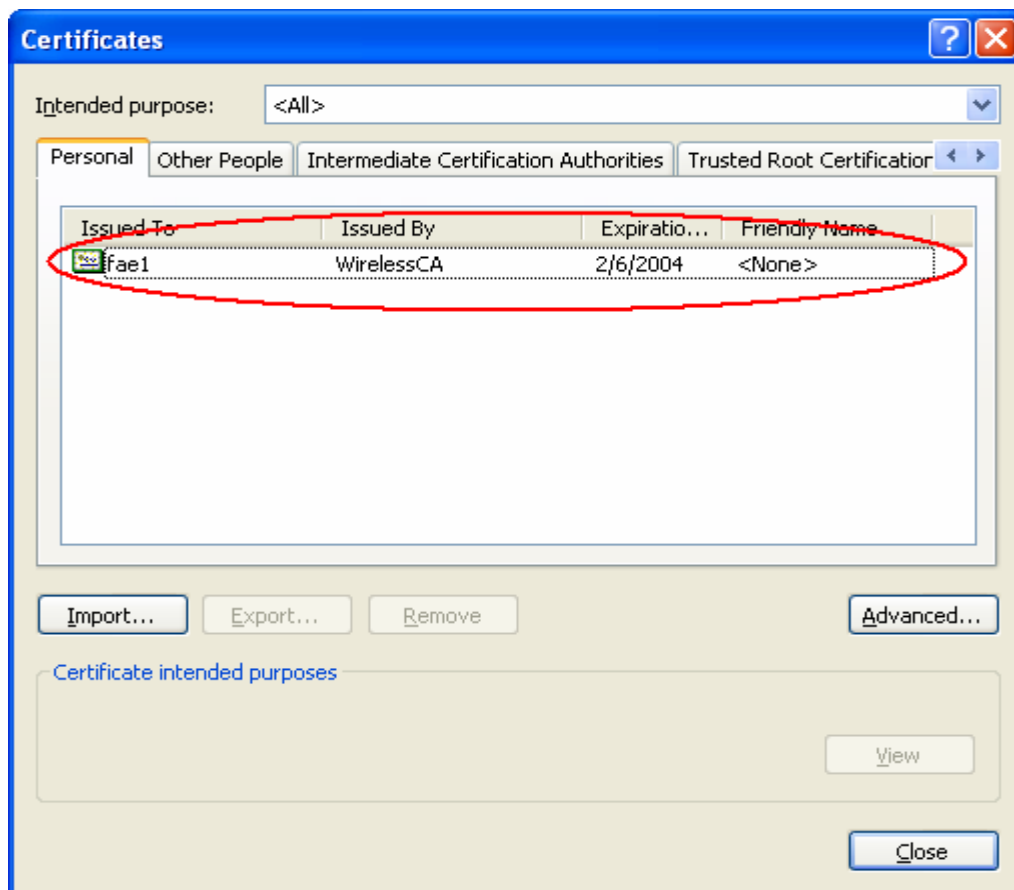


Figure 4: Certificate information on PC1

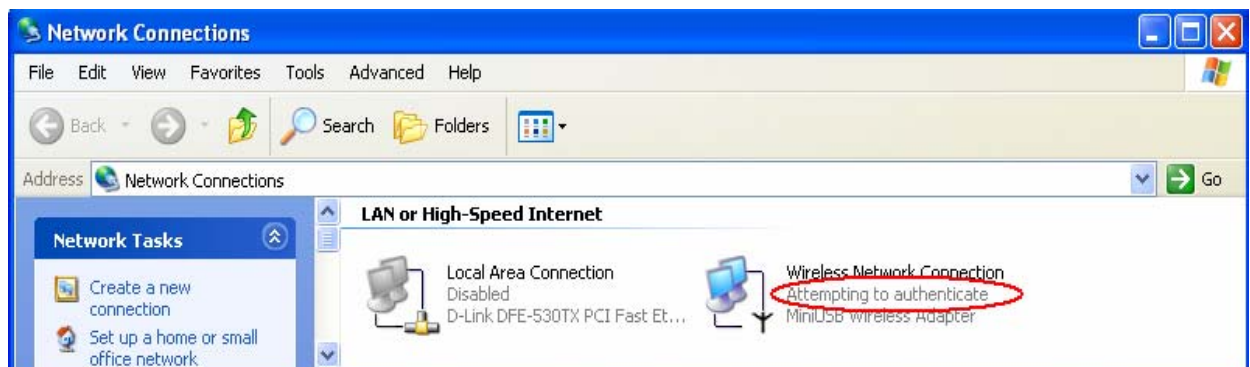


Figure 5: Authenticating

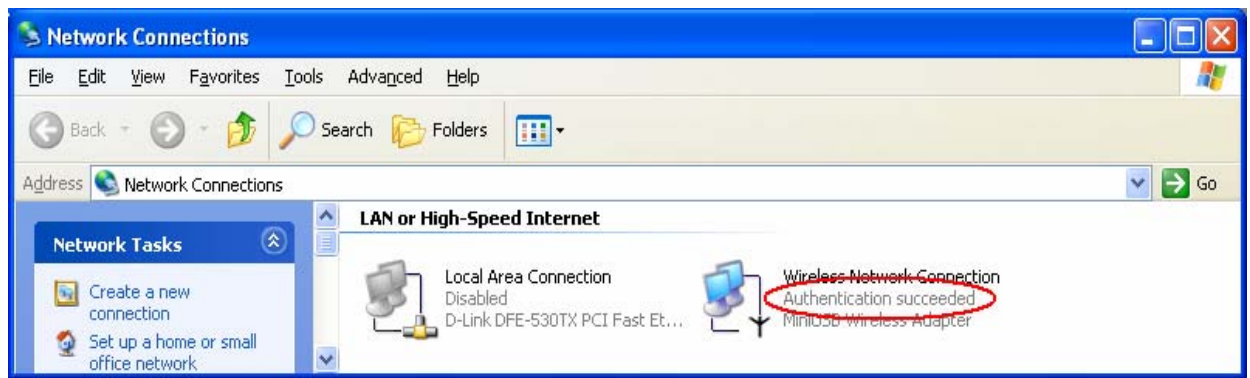


Figure 6: Authentication success

4.2DUT authenticate PC2 using PEAP-TLS.

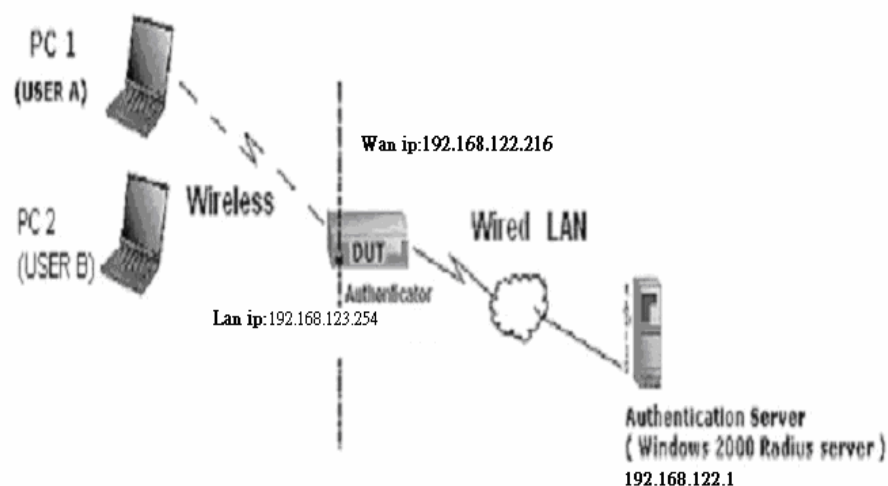
1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.
4. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.

Note.

1. PC1 is on Windows XP platform without Service Pack 1.
2. PC2 is on Windows XP platform with Service Pack 1a.
3. PEAP is supported on Windows XP with Service Pack 1 only.
4. Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

Appendix C WPA-PSK and WPA



Wireless Router: LAN IP: 192.168.123.254

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

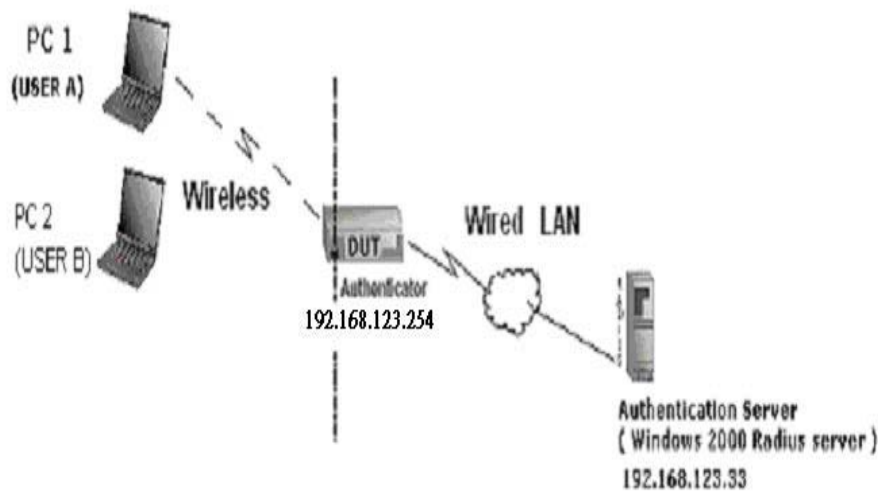
UserA : XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

Refer to: www.funk.com

Download: http://www.funk.com/News&Events/ody_c_wpa_preview_pn.asp

Or Another Configuration:



WPA-PSK

In fact, it is not necessary for this function to authenticate by Radius Server, the client and wireless Router authenticate by themselves.

Method1:

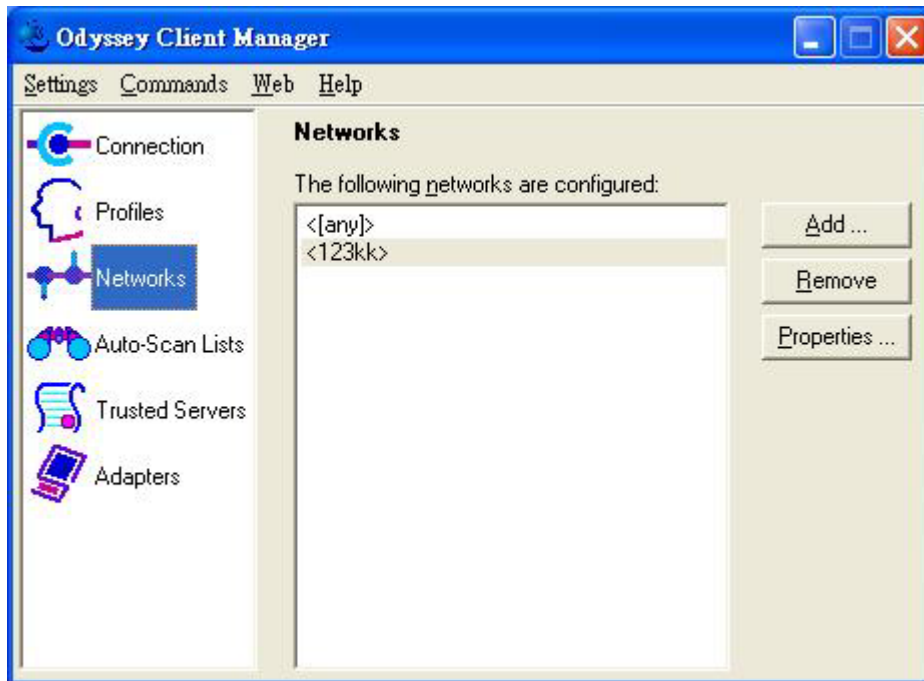
1. Go to the Web manager of Wireless Router to configure, like below:

Network ID(SSID)	123kk
Channel	8
Security	WPA-PSK
Key Mode	ASCII
Preshare Key	12345678

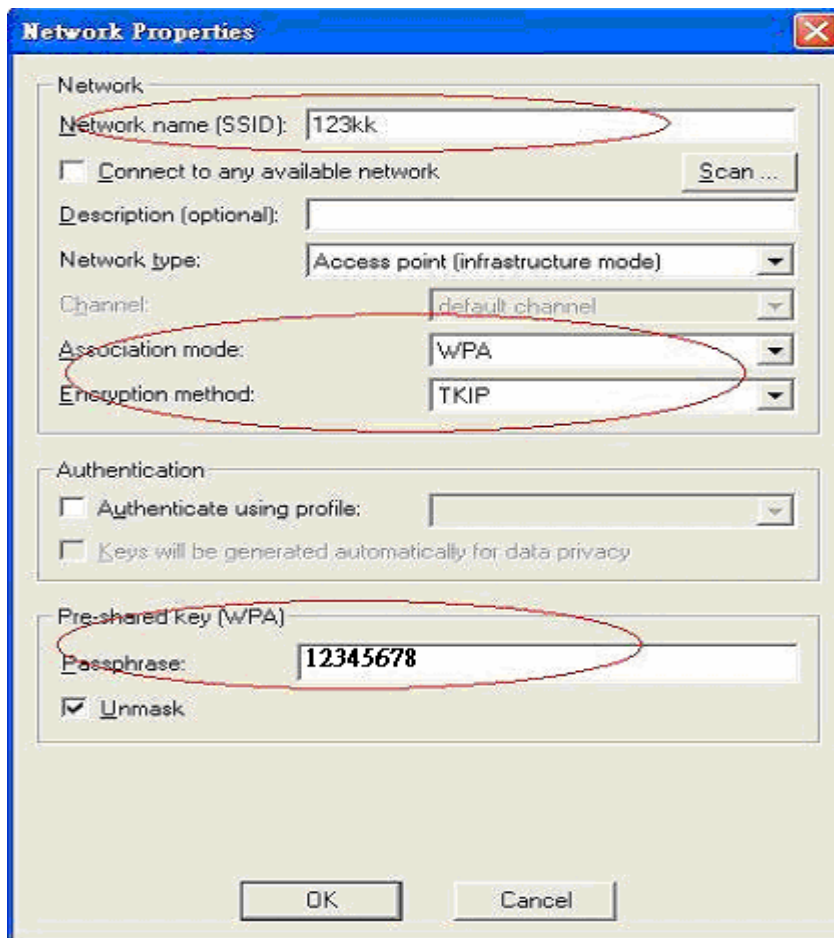
2. Go to Odyssey Client Manager, first choose "Network"

Before doing that, you should verify if the software can show the wireless card.

Open "Adapters"

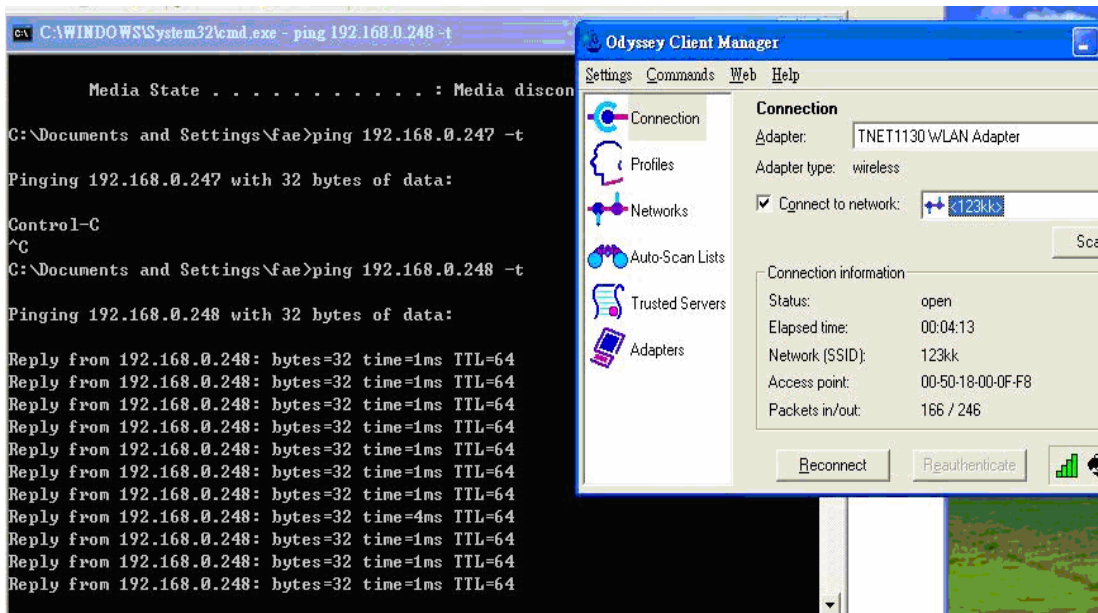


3. Add and edit some settings:



4. Back to Connection:

Then Select “Connect to network” You will see:



Method2:

1. First, patch windows XP and have to install “Service package 1”

Patch:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=5039ef4a-61e0-4c44-94f0-c25c9de0ace9>

2. Then reboot.
3. Setting on the router and client:

Router:

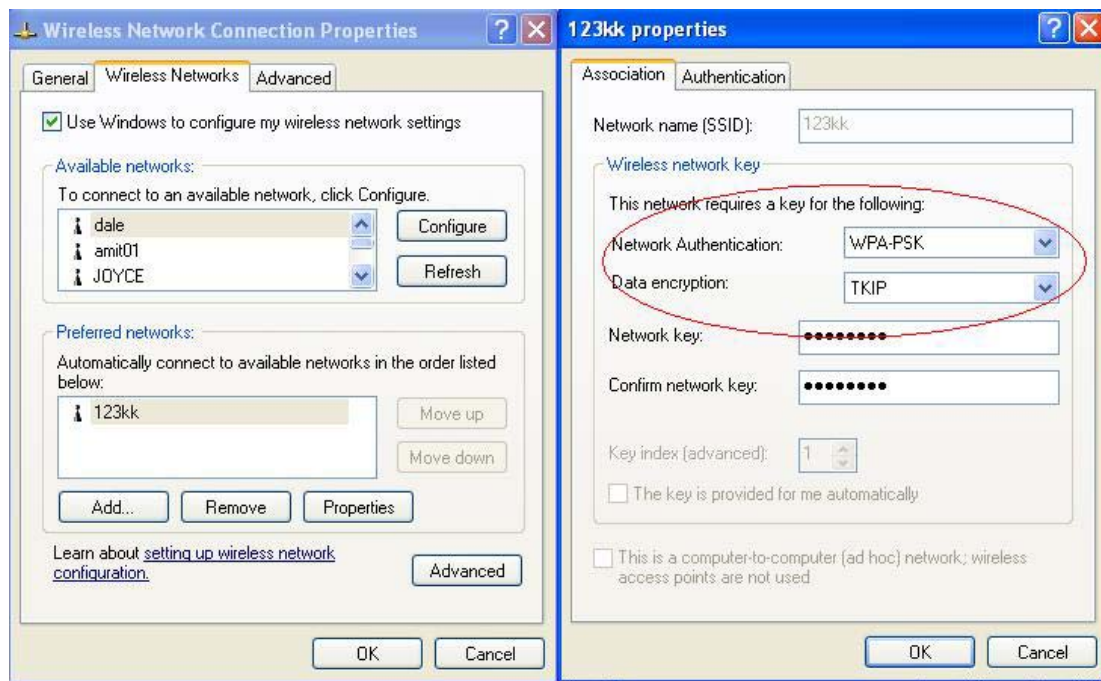
Network ID(SSID)	123kk
Channel	8
Security	WPA-PSK
Key Mode	ASCII
Preshare Key	12345678

Client:

Go to “Network Connection” and select wireless adapter.

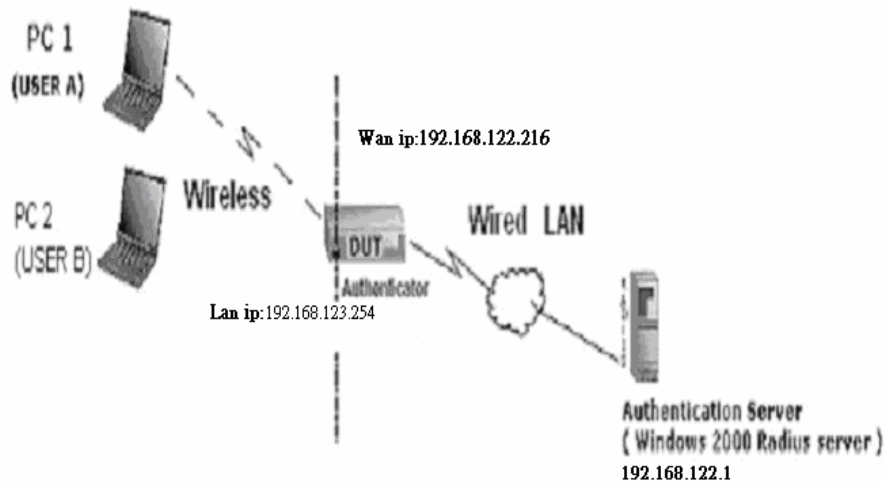
Choose “View available Wireless Networks” like below:

Advanced → choose “123kk”



WPA:

For this function, we need the server to authenticate. This function is like 802.1x.



The above is our environment:

Method 1:

1. The UserA or UserB have to get certificate from Radius, first.

<http://192.168.122.1/certsrv>

account : fael

passwd : fael



2. Then, Install this certificate and finish.

3. Go to the Web manager of Wireless Router to configure, like below:

Network ID(SSID)	123kk
Channel	8
Security	WPA

802.1X Settings

RADIUS Server IP	192.168.122.1
RADIUS port	1812
RADIUS Shared Key	costra

4. Go to Odyssey Client Manager, choose “Profiles” and Setup Profile name as “1”

Add Profile

Profile name: 1

User Info | Authentication | ITLS Settings | PEAP Settings

Login name: fae1

Password

☒ Permit login using password

☐ use Windows password

☐ prompt for password

☒ use the following password:

fae1

☒ Unmask

Certificate

☒ Permit login using my certificate:

fae1

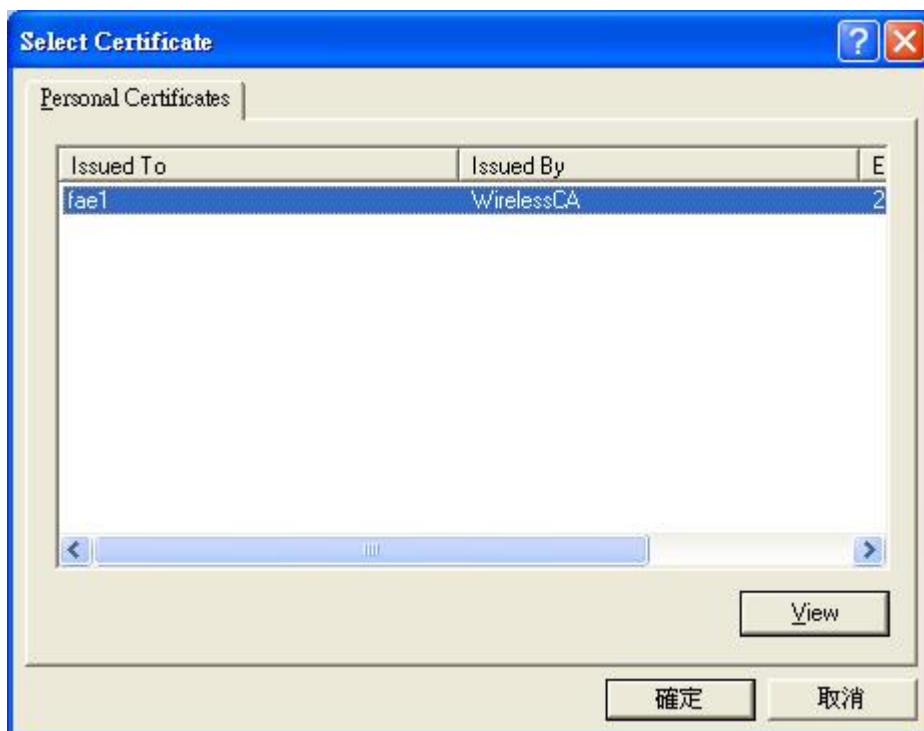
View ... Browse ...

OK Cancel

Login name and passwd are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

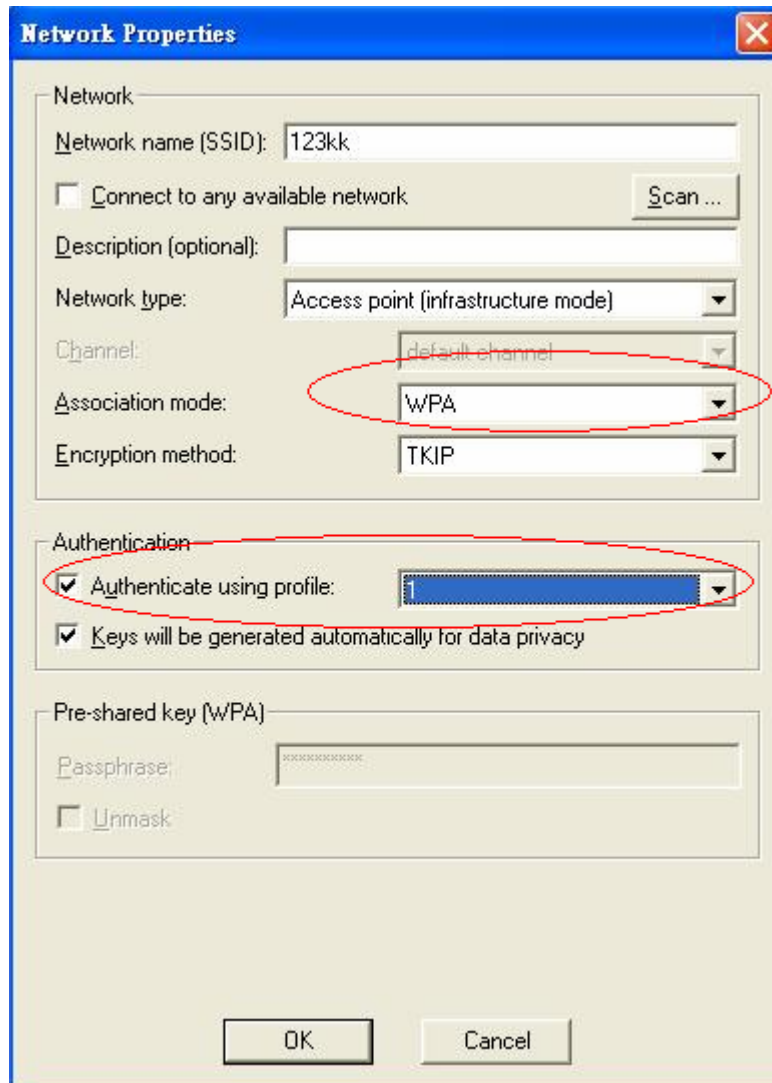
5. Then Choose “certificate” like above.



6. Then go to Authentication and first Remove EAP/ TLS and Add EAP/TLS again.



7. Go “Network” and Select “1” and ok



The image shows a Windows XP-style dialog box titled "Network Properties". It contains several sections for configuring a network connection. The "Network" section includes fields for "Network name (SSID)" (123kk), a checkbox for "Connect to any available network", a "Scan ..." button, a "Description (optional)" field, a "Network type" dropdown (Access point (infrastructure mode)), a "Channel" dropdown (default channel), an "Association mode" dropdown (WPA), and an "Encryption method" dropdown (TKIP). The "Authentication" section has a checked checkbox for "Authenticate using profile:" (with a blue dropdown arrow), a checked checkbox for "Keys will be generated automatically for data privacy", and a "Pre-shared key (WPA)" section with a "Passphrase" field (containing 20 asterisks) and an unchecked "Unmask" checkbox. Red circles highlight the "Association mode" dropdown and the "Authenticate using profile:" checkbox. At the bottom are "OK" and "Cancel" buttons.

Network Properties

Network

Network name (SSID): 123kk

☐ Connect to any available network Scan ...

Description (optional):

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: WPA

Encryption method: TKIP

Authentication

☒ Authenticate using profile: [blue dropdown arrow]

☒ Keys will be generated automatically for data privacy

Pre-shared key (WPA)

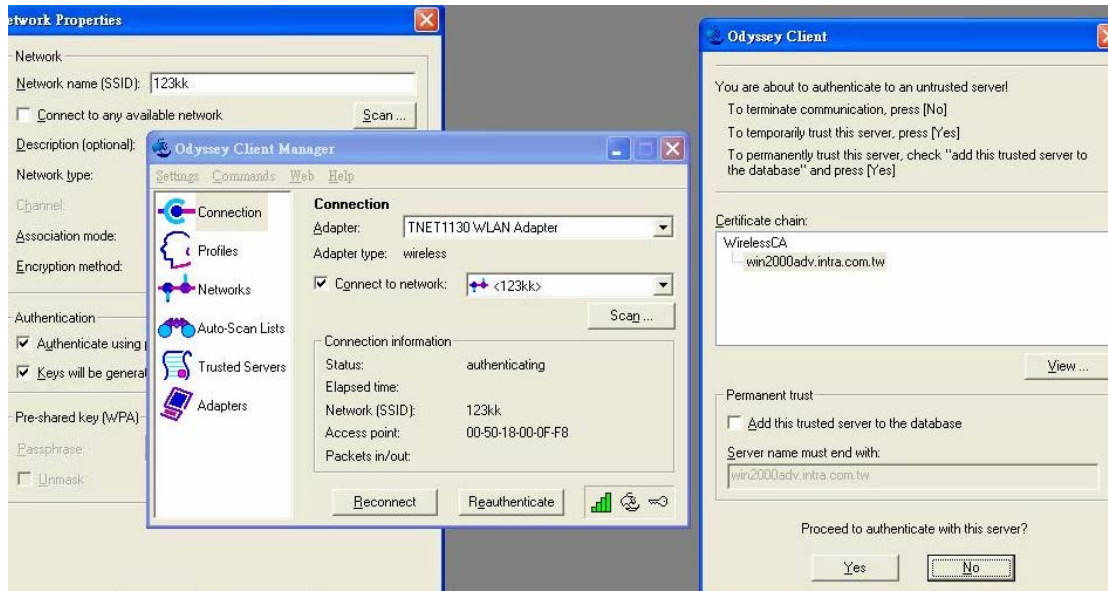
Passphrase: 20 asterisks

☐ Unmask

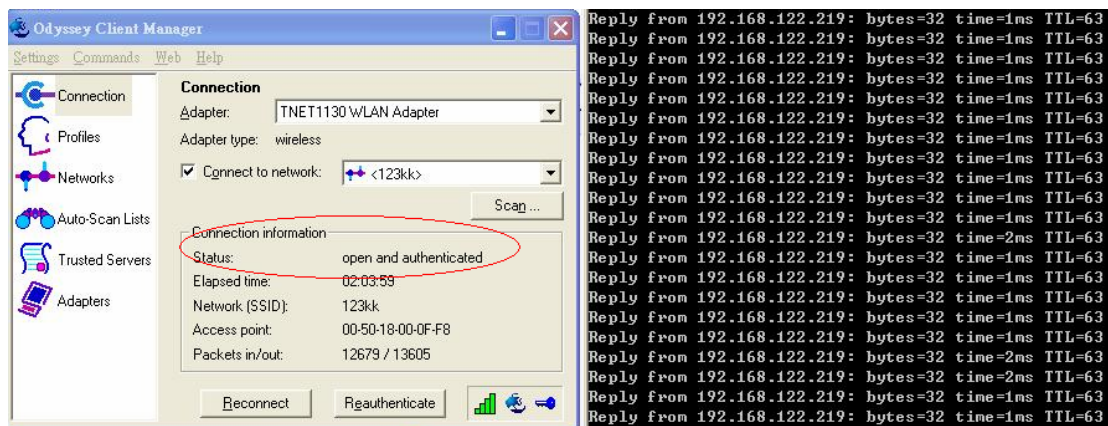
OK Cancel

8. Back to Connection and Select “123kk.

If **successfully**, the wireless client has to authenticate with Radius Server, like below:



9.Result:



Method 2:

1. The UserA or UserB have to get certificate from Radius,first.

<http://192.168.122.1/certsrv>

account:fael

passwd:fael



2. Then Install this certificate and finish.

3. Setting on the router and client:

Router:

Network ID(SSID)	123kk
Channel	8
Security	WPA

802.1X Settings

RADIUS Server IP	192.168.122.1
RADIUS port	1812
RADIUS Shared Key	costra

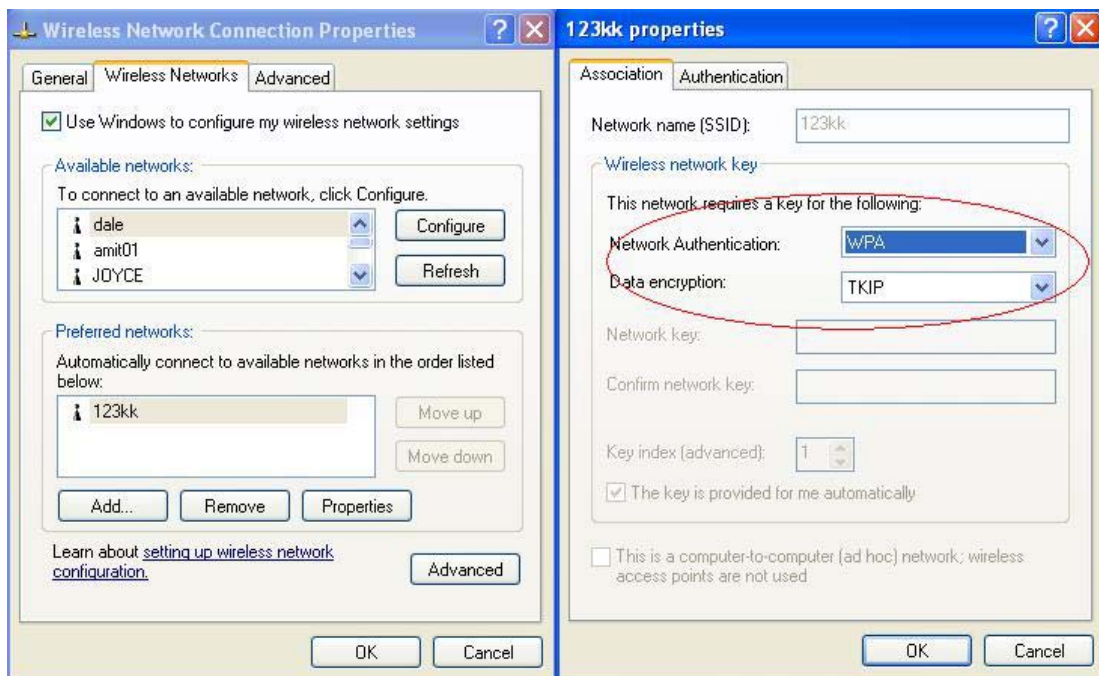
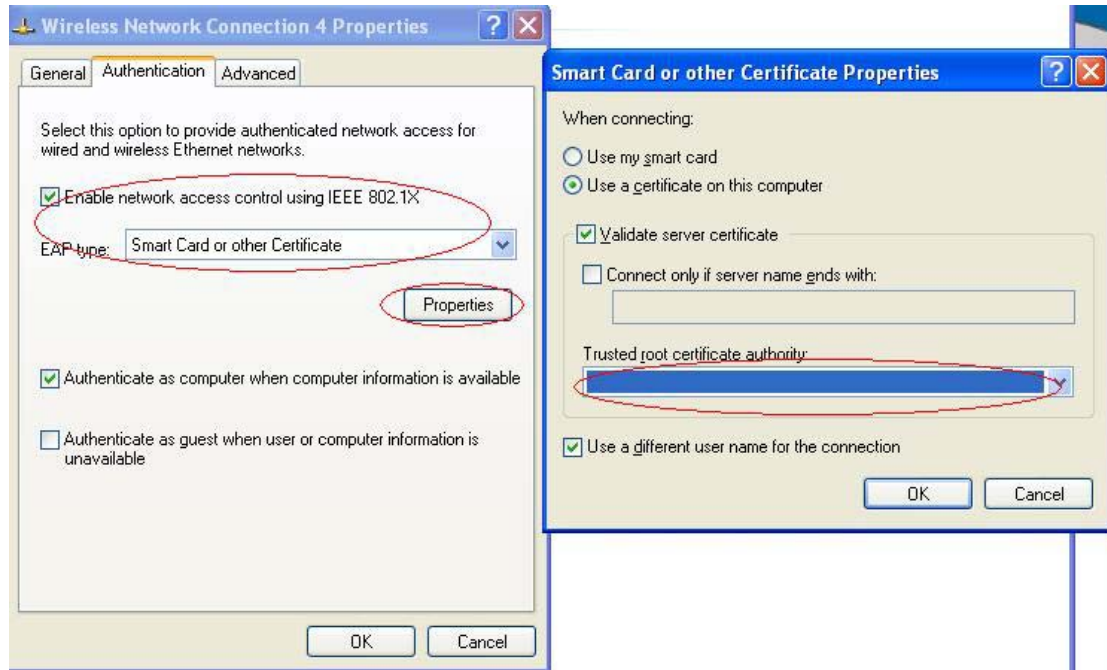
Client:

Go to “Network Connection” and select wireless adapter.

Choose “View available Wireless Networks” like below:

Advanced → choose “123kk”

Select “WirelessCA and Enable” in Trusted root certificate authority:



Then, if the wireless client wants to associate, it has to request to authenticate.

Appendix D FAQ and Troubleshooting

Reset to factory Default

There are 2 methods to reset to default.

1. Restore with RESET button

First, turn off the router and press the RESET button in. And then, power on the router and push the RESET button down until the M1 and or M2 LED (or Status LED) start flashing, then remove the finger. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

2. Restore directly when the router power on

First, push the RESET button about 5 seconds (M1 will start flashing about 5 times), remove the finger . The RESTORE process is completed.

FCC Channel selection disabled attestation:

The Channels 1-11 is just for USA used, other channels will be disabled by software. the end user can not provide with any controls or software to allow operation outside the USA frequency band for all future applications when selling this product in USA.

FCC Caution

1. The device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
2. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
3. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
4. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.