

Global PCS Inc.

SS0001

Bluetooth Access Point

User Guide

Version: 1.1.2

December 12, 2002

Document Number: BTAP-UM-0001



台揚企業集團

Global PCS Inc.

1, Innovation Road II

Hsinchu Science-Based Industrial Park

Hsinchu 300, Taiwan, R.O.C.

Phone: 886-35771155

Fax: 886-35772578

<http://www.g-pcs.com.tw/>

E-mail : divg_sales@mti.com.tw

1. Product Introduction

G-PCS Bluetooth Access Point (SS0001) is a universal adapter for Ethernet, cable modem and xDSL. SS0001 provides the low cost solution for point-to-point/point to multi points links at a 2.4GHz band, which covers unlicensed band in worldwide comply Bluetooth Specification 1.1. Devices can access the network through SS0001 using PPP Profile (LAP). The compact design makes SS0001 easy for desktop or wall mounted installation.

Feature:

- Access to Internet by xDSL modem and Cable modem
- Access to Local Area Network by Ethernet port (RJ45).
- LAN Access: point to point operation to provide Local Area Networking.
- High performance antenna.
- Dynamic Host Configuration Protocol (DHCP).
- Technique operating in the unlicensed 2.4Ghz ISM band.
- 10/100Mbps Auto-sensing Ethernet.
- Easy to install and user friendly.
- Provides Internal Web server and Telnet setup and configuration.
- Network Address Translation (NAT)

Specification:

Transmitter Output Power:	15dBm ~ 40mWatt
Power Requirement:	110V/60Hz
Frequency	2.4GHz Unlicensed band
Data Rate:	Up to 721Kbps
Range:	Up to 100M free space
Interfaces:	RS232 or 10/100 Base T Ethernet Port
Sensitivity:	-70dBm@0.1%BER
Dimensions(mm):	203mm x 130mm x 40mm
Weight:	275g

2. Install Hardware

- Global PCS Bluetooth Access Point x 1
- 6V Power Adapter x 1

3. Network Setup

SS0001 is setup and configured through an internal Web server.

3.1 Internet Explorer Setup

- (1) You can connect to web server using any of the three methods, the default Access Point IP address is **1.1.1.1**
- I. After connecting to Access Point via dongle, you can use Internet Explorer and key-in <http://1.1.1.1:5000> or the physical Access Point IP address <http://xxx.xxx.xxx.xxx:5000> to connect to web server.
 - II. Using any PC in Internet and key-in the physical Access Point IP address <http://xxx.xxx.xxx.xxx:5000>
 - III. Using a RJ-45 cross line which connects the Access Point and a PC, then key-in <http://1.1.1.1:5000> or the Access Point IP address <http://xxx.xxx.xxx.xxx:5000>. Note that the PC and Access Point must in the same subnet.
- (2) After connecting to the web server, you must enter the login ID and password.
(Default ID: BT, Password: access_point)

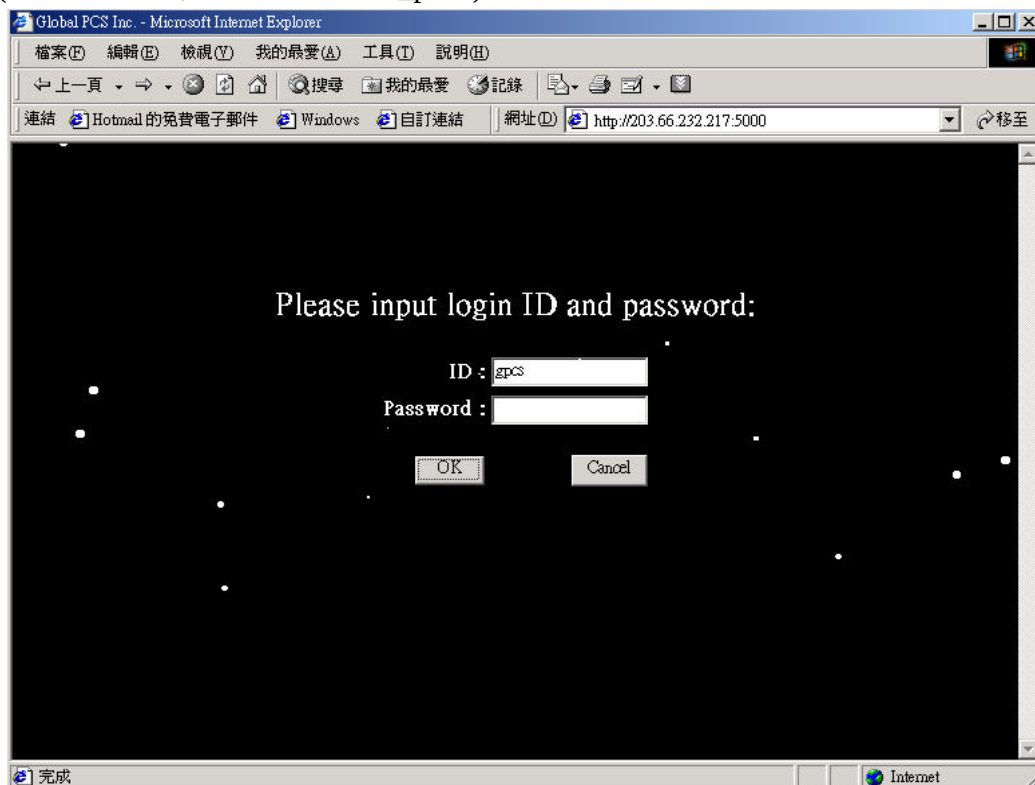


Figure 3.1 Login in

- (3) After entering the correct login ID and password, you can configure the Access Point, including change the login password, network type selection (Fixed IP address, DHCP or PPPoE), security level selection, enable data encryption or not. Figure 3.2 shows the description above.



Figure 3.2 Access Point Description

(3.1) Change password configuration:

When you click the “**Change password**” link, you can change the default password configuration as shown in figure 3.3. You must enter the old password and the new password, and figure 3.4 shows the result.

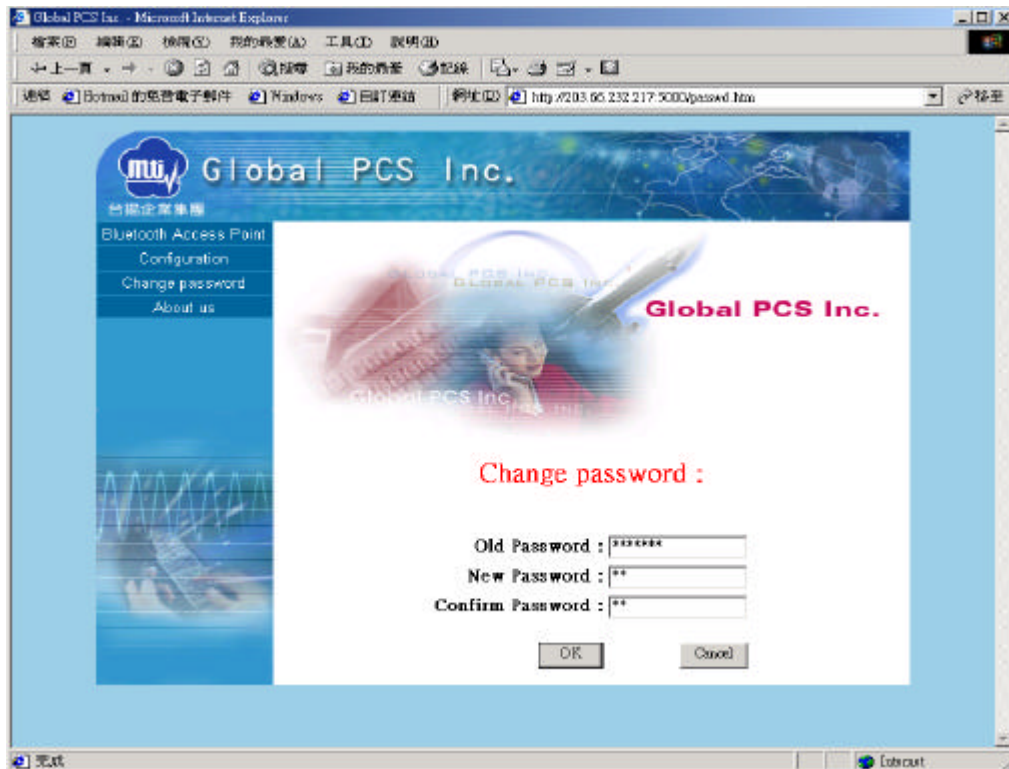


Figure 3.3 Change Password

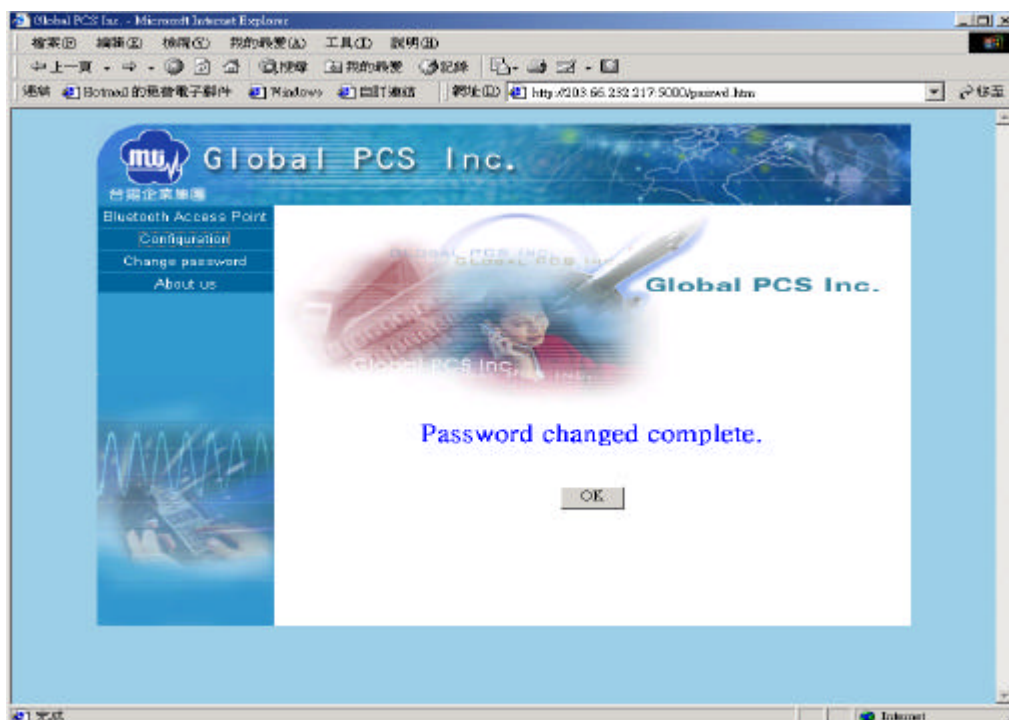


Figure 3.4 Change Password Complete

(3.2) Network configuration:

After you click the “**Configuration**” link, you can configure the network setting. Figure 3.5 shows the configuration. You can select **security level** from level 1 to level 3, and if you select level 3, you must enter the **PIN code**. You also can enable data encryption or not.

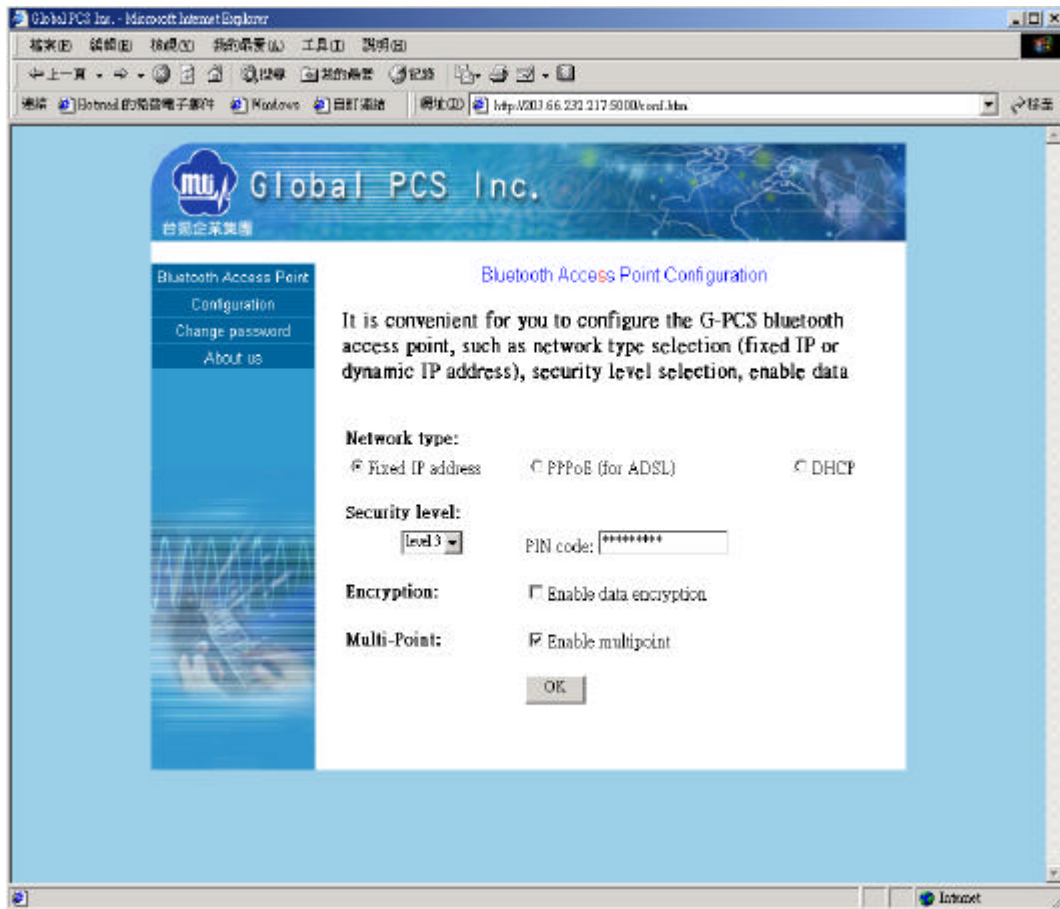


Figure 3.5 Configuration

Note: Bluetooth Security level

Level 1 (Non-secure): a device will not initiate any security procedure.

Level 2 (Service-level enforced security): a device does not initiate security procedures before channel establishment at L2CAP level.

Level 3 (Link-level enforced security): a device initiates security procedures before the link set-up at LMP level is completed.

(3.2.1) Network configuration (fixed IP address):

If you select fixed IP address, they will show the IP setting screen. You may key in the network setting information such as the IP address, Subnet mask, Gateway address, and DNS address in Figure 3.6.

Figure 3.7 shows the configuration you enter in figure 3.6. You can check the information you input.

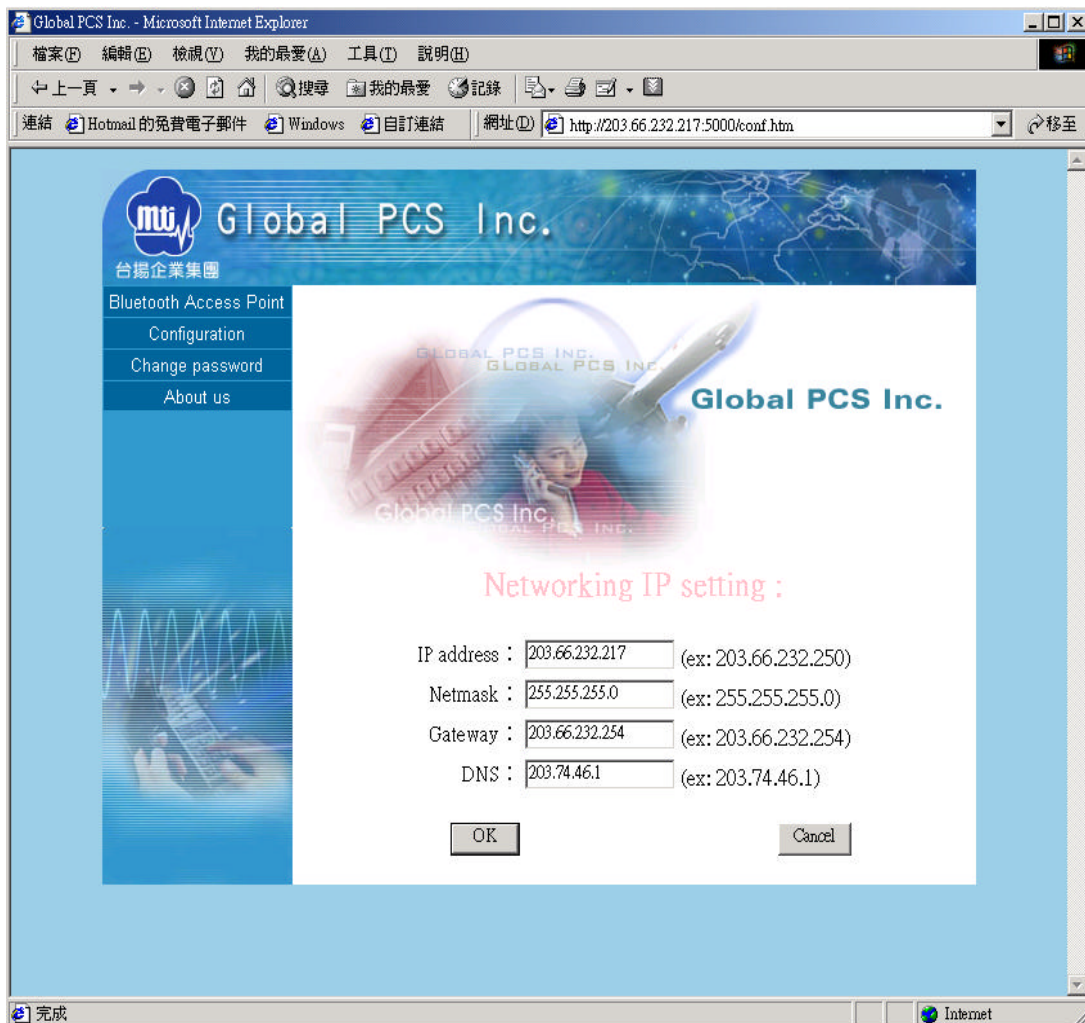


Figure 3.6 Network Configuration (fixed IP address)

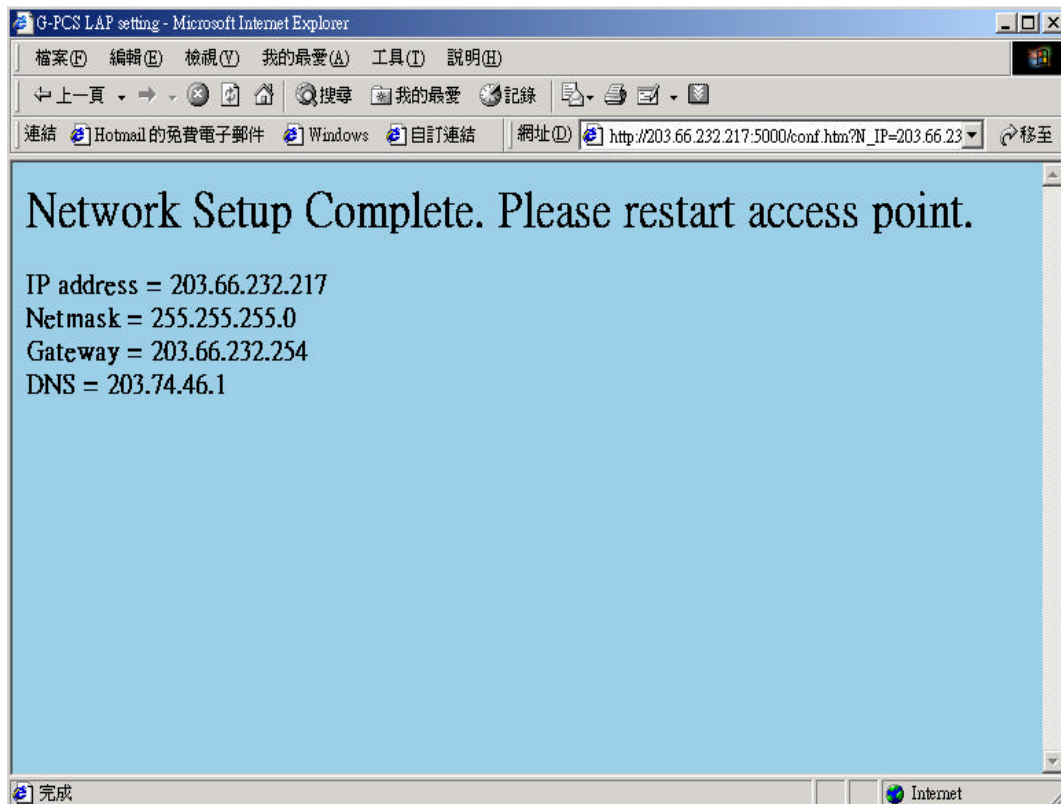


Figure 3.7 Network Configuration Complete (fixed IP address)

(3.2.2) Network configuration (PPPoE):

If you select PPPoE, you must input the PPPoE login ID and password. Figure 3.8 shows this situation and figure 3.9 shows the result.

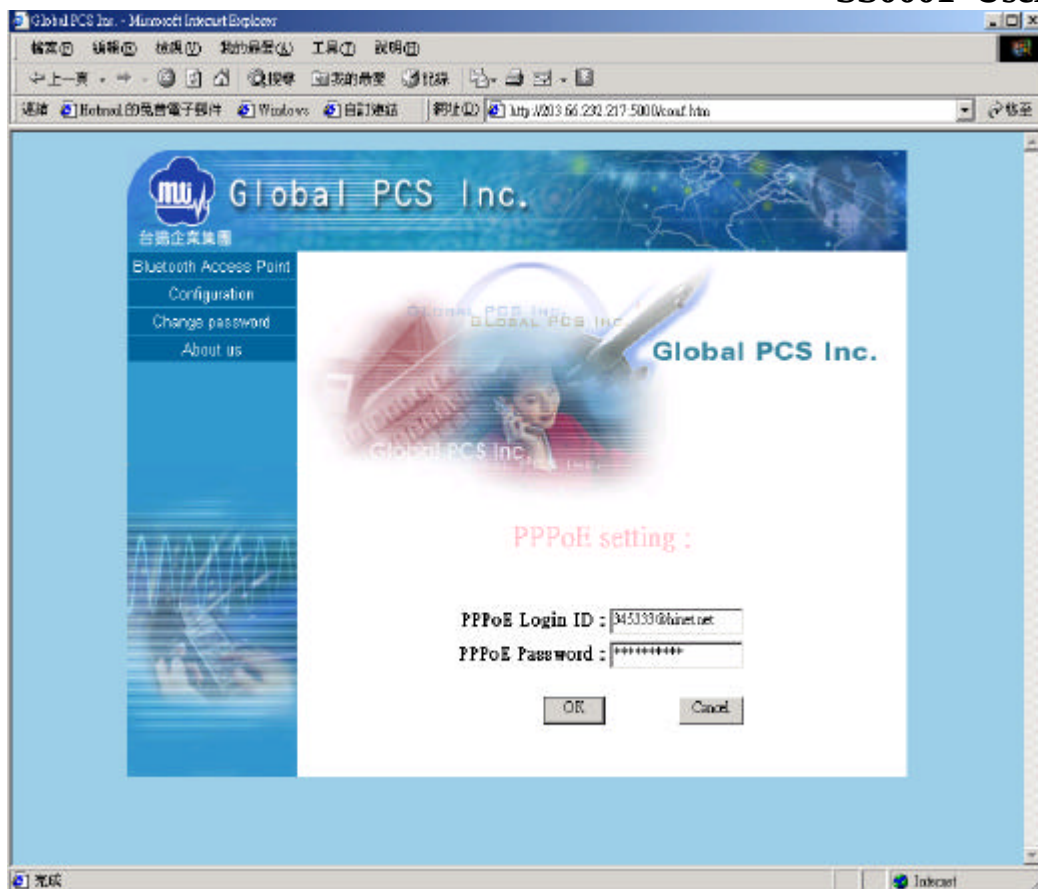


Figure 3.8 Network configuration (PPPoE)

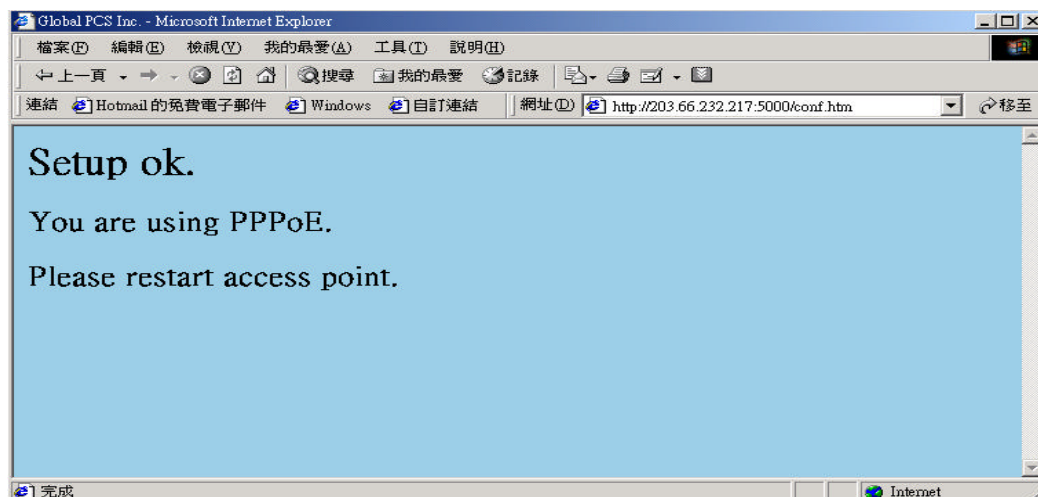


Figure 3.9 Network configuration Complete (PPPoE)

(3.2.2) Network configuration (DHCP):

The configuration of DHCP is very easy, Figure 3.10 shows the result.

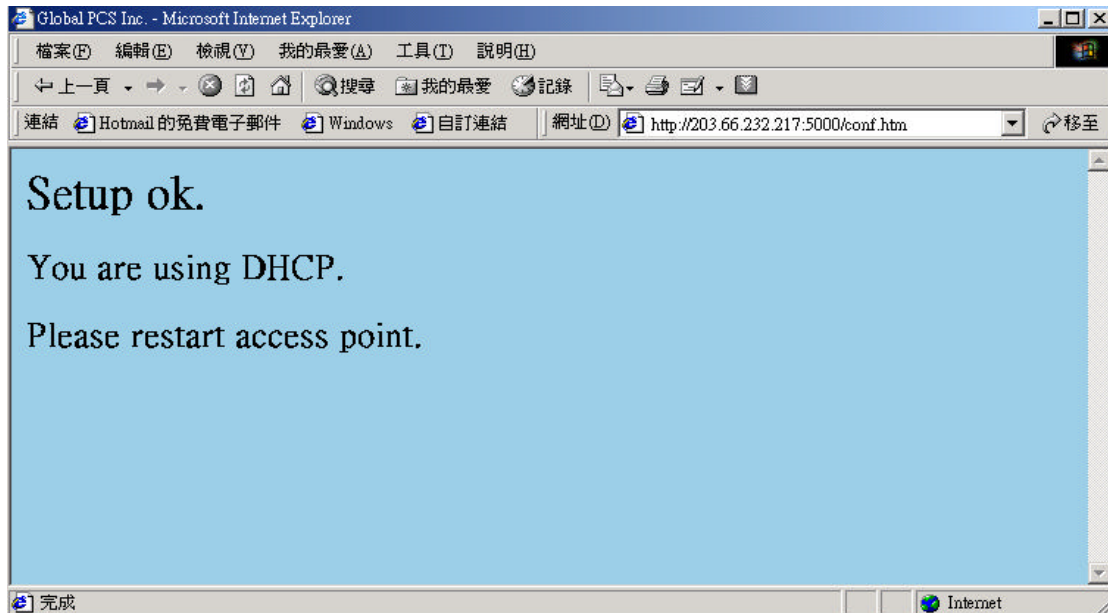
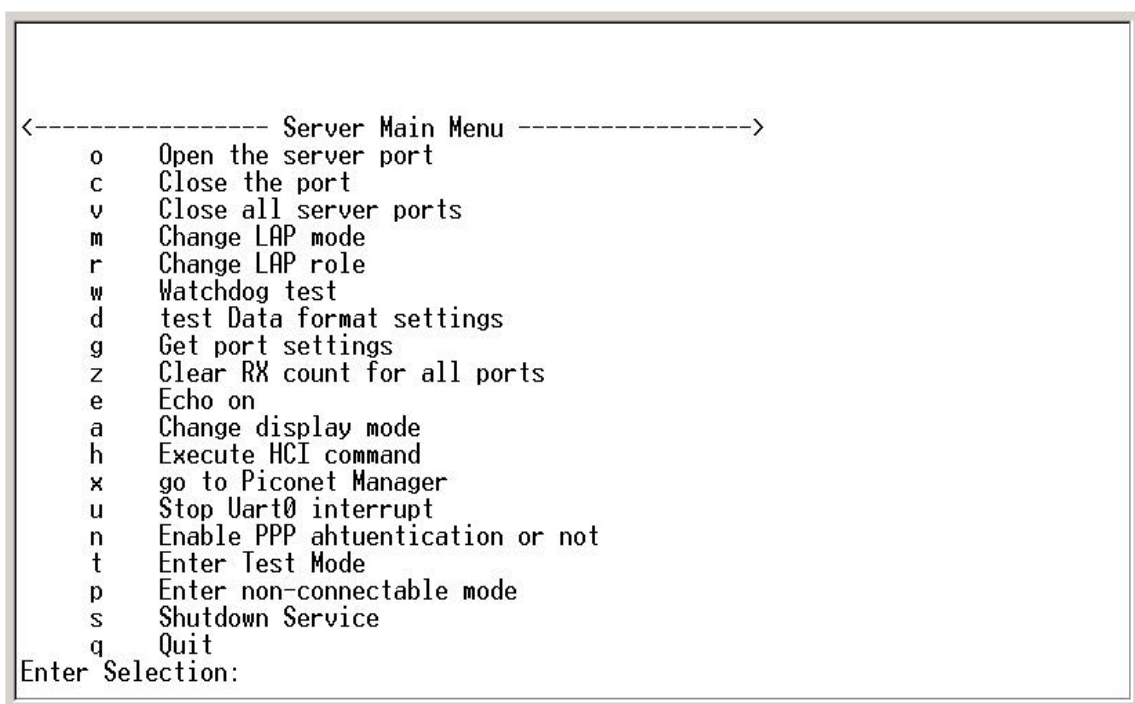


Figure 3.10 Network configuration Complete (DHCP)

3.2 Other function of SS0001

SS0001 LAP provides a COM port interface, you must have a RS-232 line to connect between SS0001 and DT (Data Terminal). After DT creates a connection with COM port (usually using windows HyperTerminal), it can send some commands to control SS0001 through the created COM port. Note that the COM port settings are non-parity check, data bit is 8, 1 stop bit, and baudrate is 57600 bps with hardware flow control off.

A screenshot of a terminal window showing the 'Server Main Menu' for the SS0001 device. The menu is enclosed in a rectangular box with a thin border. At the top, the title '<----- Server Main Menu ----->' is displayed. Below the title is a list of 17 options, each preceded by a single lowercase letter: 'o Open the server port', 'c Close the port', 'v Close all server ports', 'm Change LAP mode', 'r Change LAP role', 'w Watchdog test', 'd test Data format settings', 'g Get port settings', 'z Clear RX count for all ports', 'e Echo on', 'a Change display mode', 'h Execute HCI command', 'x go to Piconet Manager', 'u Stop Uart0 interrupt', 'n Enable PPP authentication or not', 't Enter Test Mode', 'p Enter non-connectable mode', 's Shutdown Service', and 'q Quit'. At the bottom of the menu, the text 'Enter Selection:' is shown, indicating where the user should input their choice.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
d   test Data format settings
g   Get port settings
z   Clear RX count for all ports
e   Echo on
a   Change display mode
h   Execute HCI command
x   go to Piconet Manager
u   Stop Uart0 interrupt
n   Enable PPP authentication or not
t   Enter Test Mode
p   Enter non-connectable mode
s   Shutdown Service
q   Quit
Enter Selection:
```

Figure 3.11 SS0001 Function Display

- (o) **Open the server port:** Open the server serial port for RFCOMM connection. All ports are opened by default for 7 connections.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: o
Server port0 is open.
```

- (c) **Close the port:** Close the server serial port for RFCOMM connection.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: c
Which server [0 ... 7]? 2
Server port2 is closed.
```

- (v) **Close all server ports:** Close the server serial port for all RFCOMM connection.

(m) **Change LAP mode:** Change LAP mode among general accessible mode, limit accessible mode, non-accessible mode and connectable mode only.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: m
PME: Changing Not Connected accessible mode.
PME: Change to Non-Accessible mode succeeded.
PME: Setting Non-Accessible mode.
m
PME: Changing Not Connected accessible mode.
PME: Change to General Accessible mode succeeded.
PME: Setting General Accessible mode.
m
PME: Changing Not Connected accessible mode.
PME: Change to Connectable Only mode succeeded.
PME: Setting Connectable only mode.
m
PME: Changing Not Connected accessible mode.
PME: Change to Limited Accessible mode succeeded.
PME: Setting Limited Accessible mode.
```

(r) **Change LAP role:** Change LAP role as master or slave.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: r
LAP is SLAVE role now.
r
LAP is MASTER role now.
```

- (w) Watchdog test: Check watchdog and to see if it works.
- (a) Change display mode: Display debug message on hyper terminal or not.
- (h) Execute HCI command: Enter an HCI command to execute.
- (s) Enable PPP authentication or not: Authenticate ID and password for PPP connection or not.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: n
PPP authentication is enable
n
PPP authentication is disable
```


(p) **Halt the PPP server:** Stop the PPP service. PPP now is not available.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: p
PPP service is halt
p
PPP service is open
```

(s) **Shutdown PPP:** Close all existing PPP connections.

```
<----- Server Main Menu ----->
o   Open the server port
c   Close the port
v   Close all server ports
m   Change LAP mode
r   Change LAP role
w   Watchdog test
a   Change display mode
h   Execute HCI command
n   Enable PPP authentication or not
p   Halt the PPP server
s   Shutdown PPP
q   Quit
Enter Selection: s
Shutdown PPP server
```

IMPORTANT NOTE

- 1.0 This 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.
- 2.0 The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- 3.0 To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

FCC INFORMATION

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval from Global Pcs. Inc. Modification could void authority to use this equipment.

" Importance Note: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."