Wireless LAN SOHO Router

User’s Manual

CONTENTS

Chapter 1 Introduction

1.1 Feature

- Fully interoperable with IEEE 802.11b compliant products.
- High-Speed data transfer rate up to 11Mbps.
- 64-bit and 128-bit WEP Encryption.
- MAC Address and TCP/UDP/IP filtering.
- Web-Based Network Manager/Telnet for Configuring and Managing Your access points.
- SNMP MIB I and MIB II supported.
- Capable of acting as a DHCP Server.
- Remote Management supported.
- Firmware Upgrade via WEB/TFTP
- Advanced Firewall features

1.2 Package Contents

- One CD-ROM with User Guide included
- One Power Adapter
- One CAT 5 UTP Cable
- One Fast Start Guide and One Registration Card

Chapter 2 Hardware Configuration

2.1 Hardware Configuration

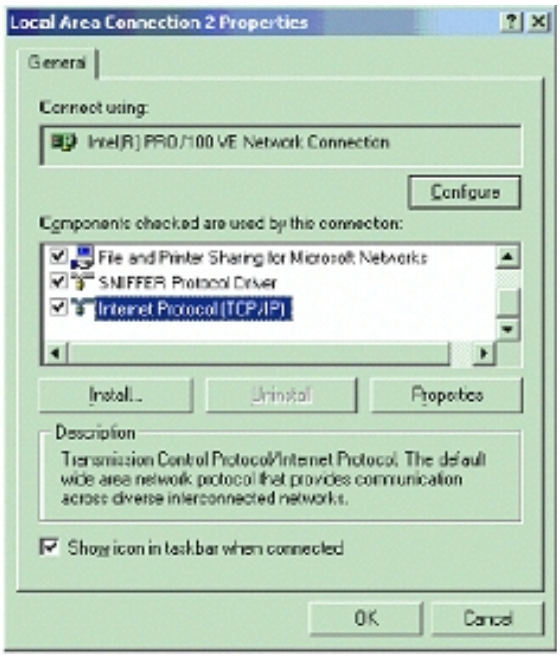
1. **RJ-45 Ethernet connector**
   Provides 10/100 Mbps connectivity to a wired Ethernet LAN.
2. **Reset Button**
   By pressing this button for over 3 seconds, the AP will be reset with factory default configuration.
3. **Power Supply connector**
   It is for connecting to the power adapter.

2.2 Hardware Installation

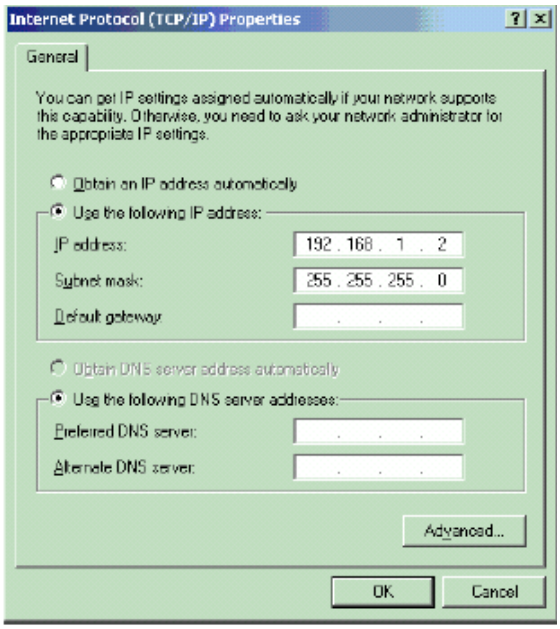
1. Configure your notebook or PC with Wireless LAN card.
2. For Wired LAN, connect your PCs' Ethernet port to any AP's LAN port by an Ethernet cable.
3. For WLAN, locate the AP to a proper position.
4. Plug the power cord into a power outlet.

Chapter 3 Configuring your PC

1. Change the TCP/IP setting of your managing computer. Select the TCP/IP line that has been associated to your network card. Click the **Properties** button.

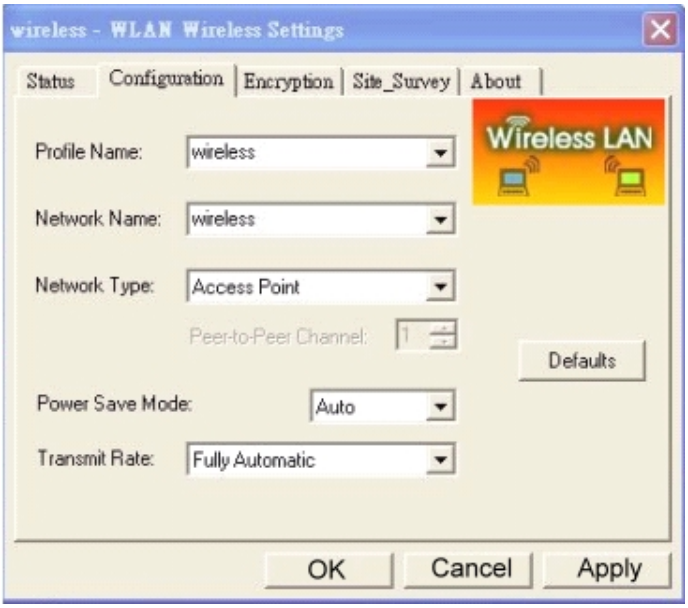


2. Make sure the IP address of your computer and the AP are in the same subnet. The default IP address of the access point is 192.168.1.1 and the default subnet mask is 255.255.255.0.



3. For WLAN, open the WLAN client utility. Click **Configuration** tab. Type default SSID (default SSID: wireless) in the Network Name field. Choose “Access Point” for Network Type, then click **OK** button.

   Note: the default channel is 6.Configuring the Router through Web Browser



Chapter 4 Initial Software Installation and Configuration

The access point can be configured through your web browser with the Web-Based Utility. Open your web browser and type the default IP address of the AP in the address field (default IP: 192.168.1.1) and press **Enter**. Make sure the IP address of AP and your computer are in the same subnet.

After the connection is established, you will see the User Login page as shown below. Leave the password field blank when the first time you open the Web-Based utility. You can change the password on the “Administrator settings” page.

The system will be time out after idling about 1 minute. You have to login again to re-enter the main setting page. You can change the idle time out period on the “Administrator settings” page.

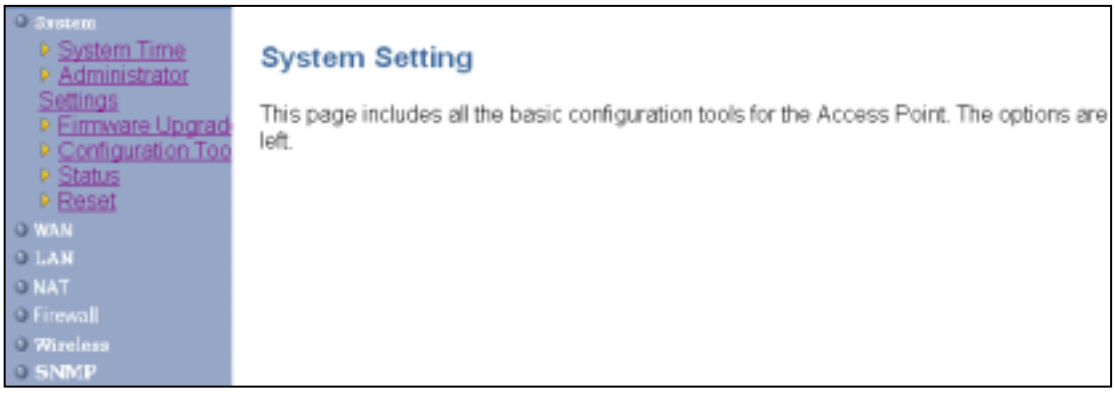
On any page, you can click **HELP** to obtain more descriptions and explanations. To clear any values you’ve entered on any page, click **CANCEL** and re-enter information.

There are three tabs on the upper right-corner of each page. To go back to the main setting page, press HOME tab. To log out of the web management, press EXIT tab. To complete any change you have made, press RESET tab after clicking APPLY button.

Chapter 5 Configuring the router through web browser

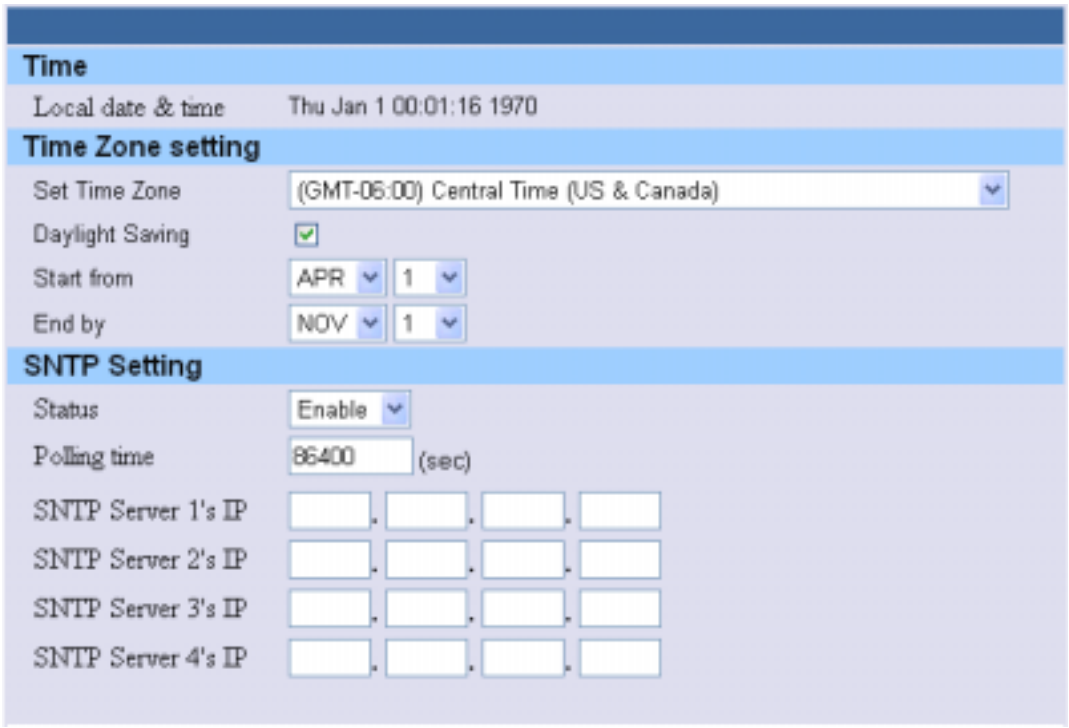
5.1 System Setting

The system setting contains all basic configuration of the access point. It includes System Time, Administrator Setting, Firmware Upgrade, Configuration Tools, Status, and Reset.



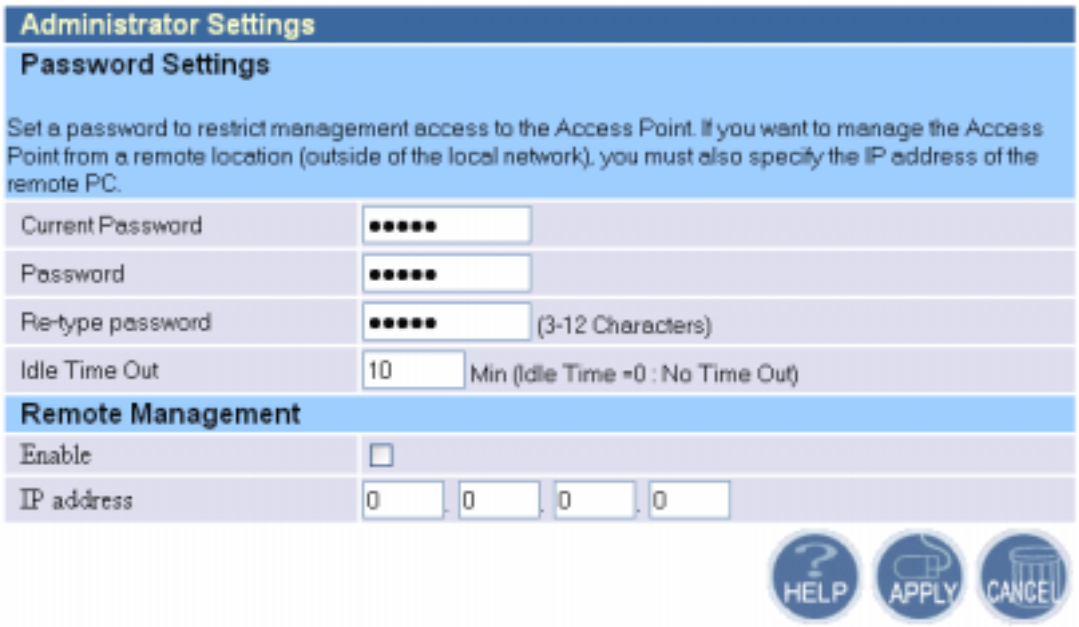
5.1.1 System Time

Connecting to a Simple Network Time Protocol (SNTP) server allows the AP to synchronize the system clock to the global internet. The synchronized clock in the AP is used to control client filtering. The polling time is the time period that the AP sends requests for the correct time. Note that the polling time can not be less than 3600 sec. Click **APPLY** to complete your change.



5.1.2 Administrator Setting

Set a password to restrict management access to the access point. If you want to manage the access point from a remote location (outside of the local network), you must also specify the IP



address of the remote PC.

Password Settings:

To change your password, enter your current password in the “Current Password” box. Enter new password in the “Password” box. Enter it again in the “Re-type password” box to confirm it. Click **APPLY** to complete your change.

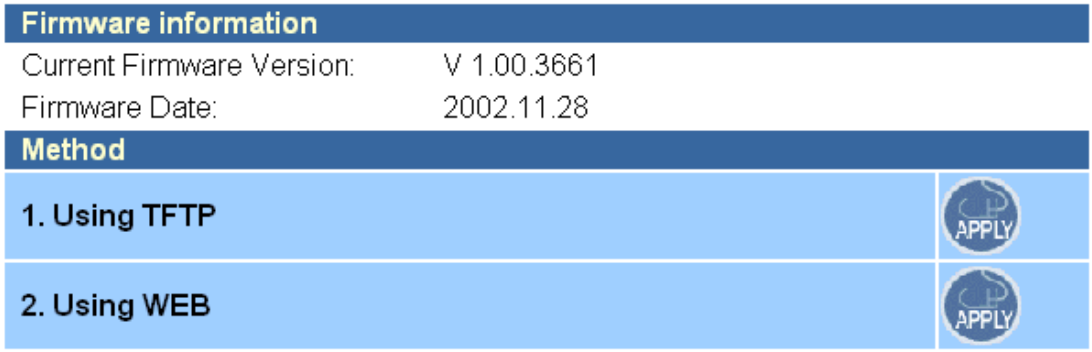
The “idle Time Out” is the amount of time of inactivity before the access point will automatically close the Administrator session. Set this to zero to disable it.

Remote Management:

By default, management access is only available to users on your local network. However, you can also manage the access point from a remote host. Just check the Enable check box and enter the IP address of an administrator to this screen.

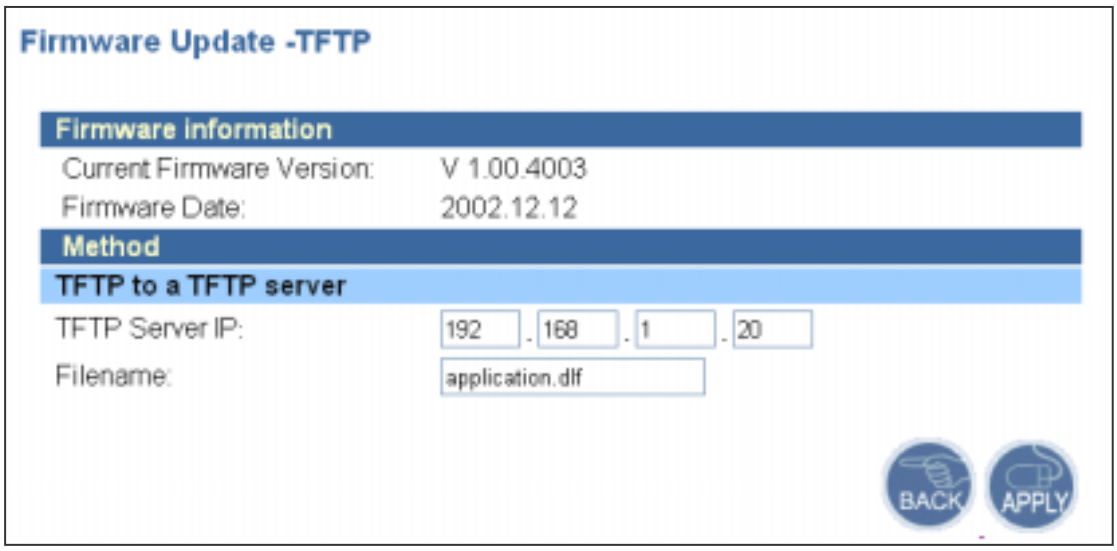
5.1.3 Firmware Upgrade

The firmware information is displayed on this page. You can find firmware version and firmware date here. There are two ways to upgrade the firmware: “Using TFTP” and “Using WEB”. Click **APPLY** to choose the one you want.



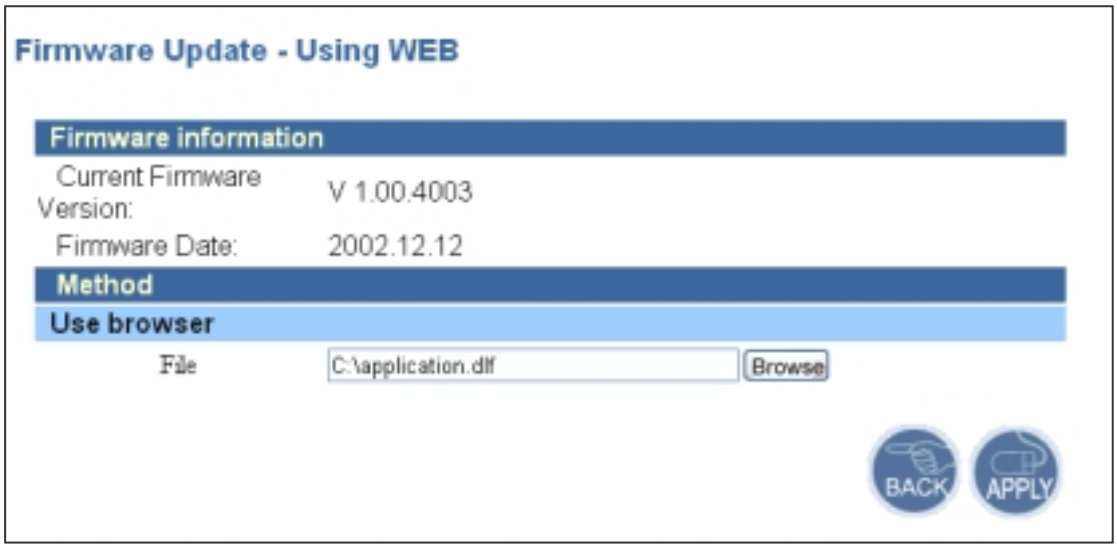
- **Using TFTP**

On the managed computer, run the TFTP Server utility. And specify the folder in which the firmware file resides. After running the TFTP server, enter the TFTP server IP and the filename on the following page. Click on **APPLY** to complete your change.



- **Using WEB**

Type the correct firmware file path and file name on the File field. You can click Browse to select the file location. Click on **APPLY** to complete your change.

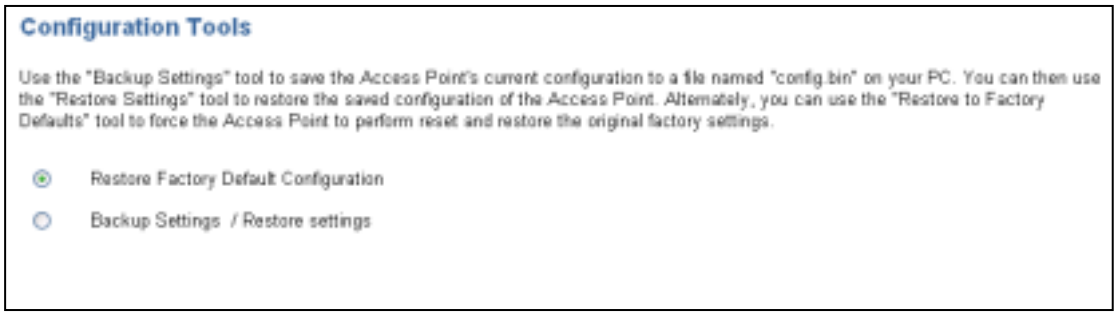


5.1.4 Configuration Tools

This tool can backup or restore the AP's configuration. It can also restore the original factory default settings.

- **Restore Factory default configuration:**

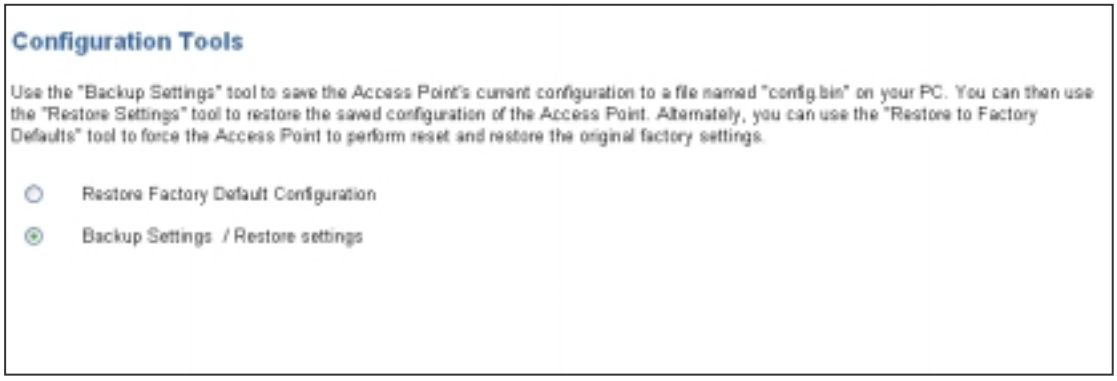
(1) Check the "Restore Factory Default Configuration**"** radio button and then click **APPLY**.



(2) Click **Restore** button to force the access point to perform reset and restore the original factory settings.

- **Backup Setting/Restore Settings:**

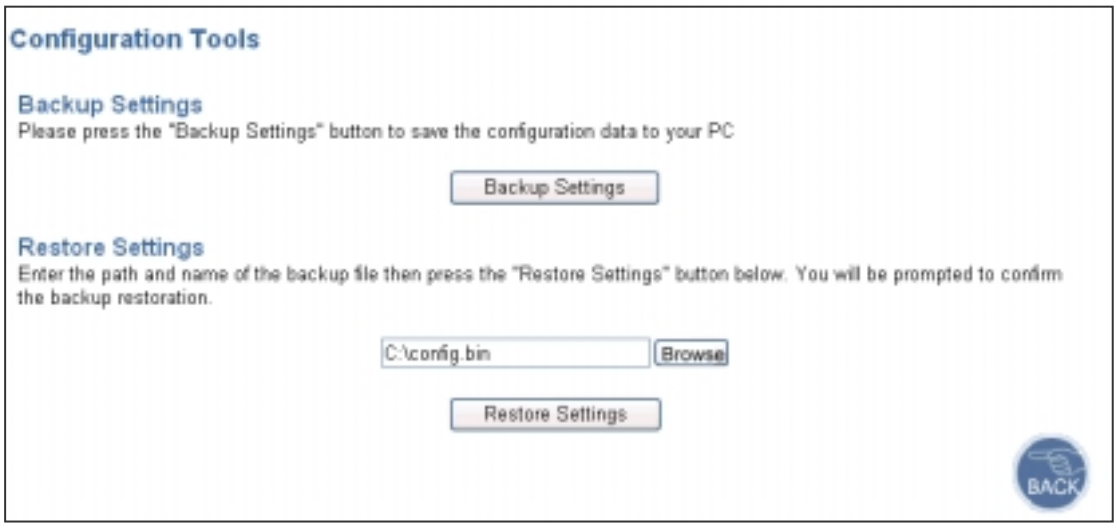
(1) Check the **"**Backup Settings/Restore Settings**"** radio button and click **APPLY**.



(2) To save the access point's current configuration to a file named "config.bin" on your PC, click **Backup Settings** button.

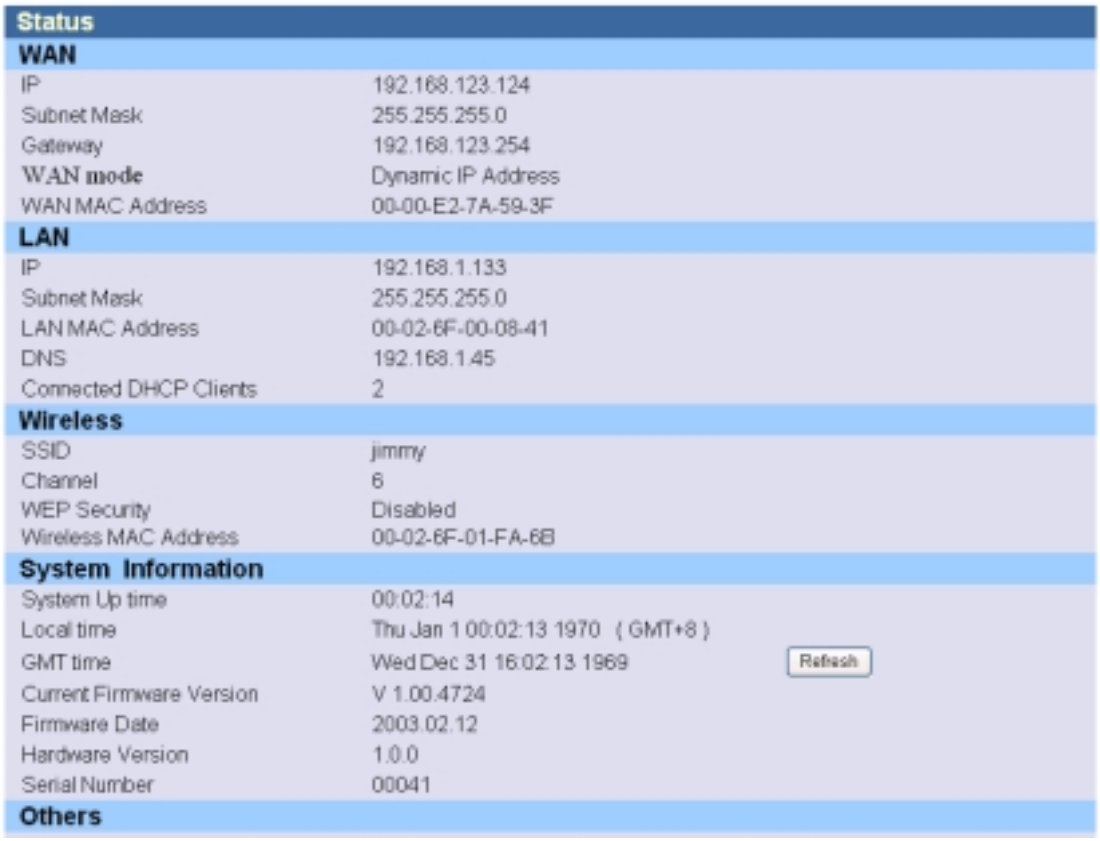
(3) To restore configuration, you can use the "Restore Settings" tool to restore the saved configuration of the access point.

(4) Enter the path and file name then click **Restore Settings** button. You can also click **Browse** to locate and select the previously saved backup file.



5.1.5 Status

The Status window displays current information and settings for your AP. It has five main parts – WAN, LAN, Wireless, System Information, and Others.



For WAN, it display the IP address, Subnet Mask, and Gateway of WAN. It also displays WAN mode and WAN MAC Address.

For LAN, it displays AP's IP address, MAC address, and Subnet Mask. It also displays the IP address of the DNS and the number of clients connected by DHCP server.

For Wireless, it displays SSID, Channel, WEP security status, and wireless MAC address.

For System Information, it displays system time, firmware version, firmware date, hardware version, and serial number.

For others, it displays the power level of the AP.

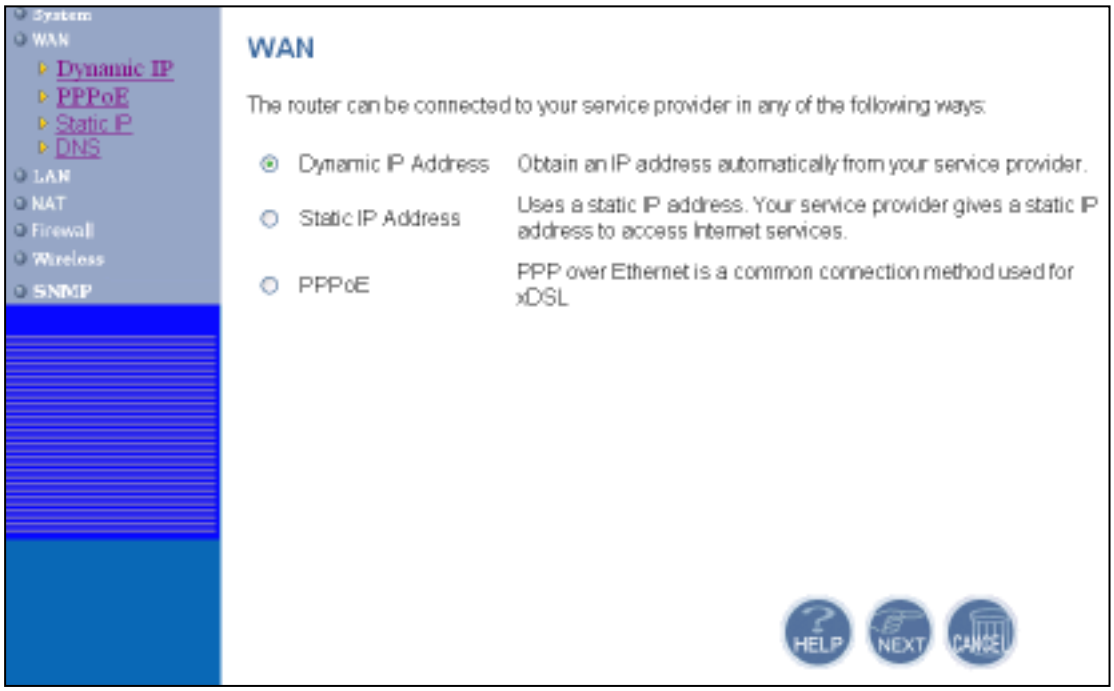
You can obtain the most up-to-date information by pressing the "Refresh" button.

5.1.6 Reset

In the event that the access point stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the **Reset** button below. You will be asked to confirm your decision. The reset will take about 18 seconds.

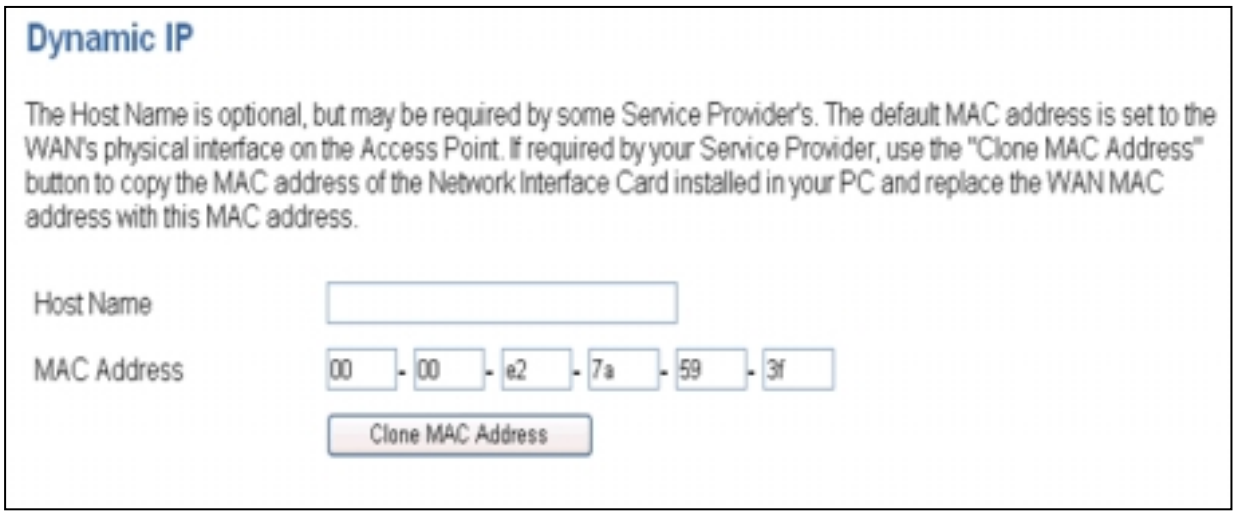
5.2 WAN Setting

The router can be connected to your internet service provider (ISP) via dynamic IP Address, static IP Address, and PPPoE. Select the way you want to connect to your internet service provider and click "NEXT" to continue setting. Remember to reset the Router after making any change of WAN setting. The WAN mode is displayed in the status page.



5.2.1 Dynamic IP Address

By select this way, the router obtains an dynamic IP address assigned by your ISP when connecting to the internet. Click “APPLY” to complete your change.



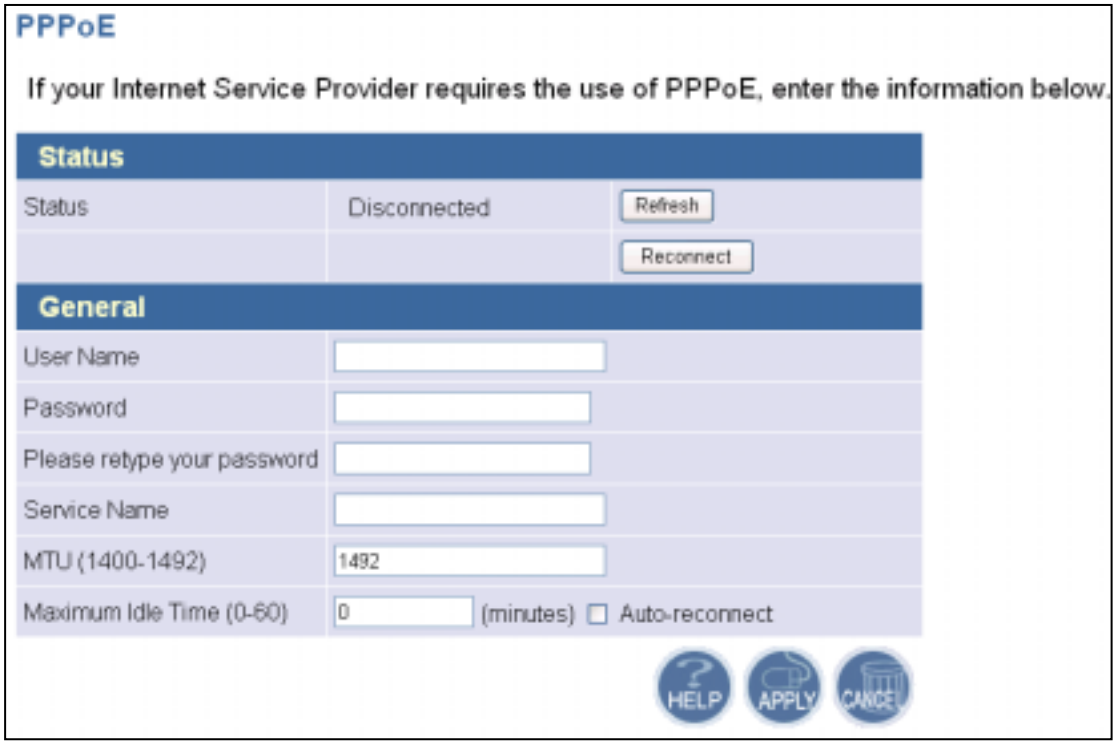
(1) **Host Name:** This is optional but may be required by your ISP.

(2) **MAC Address:** The default MAC address is set to WAN’s physical interface on the Access Point. By cloning MAC address, you can replace the WAN MAC address with the MAC address of your network interface card/adapter. Just click “Clone MAC

Address” button.

5.2.2 PPPoE Settings

PPP over Ethernet is a common connection method used for xDSL. Choose PPPoE if your ISP uses a PPPoE connection.



Status:

It displays the connection status of WAN. Click “Refresh” to check the up-to –date connection status. You can click “Reconnect” if the PPPoE connection is dropped.

General:

(1) **User Name:** Your PPPoE User Name provided by your ISP.

(2) **Password:** Enter your PPPoE password.

(3) **Retype your password:** Re-enter your PPPoE password.

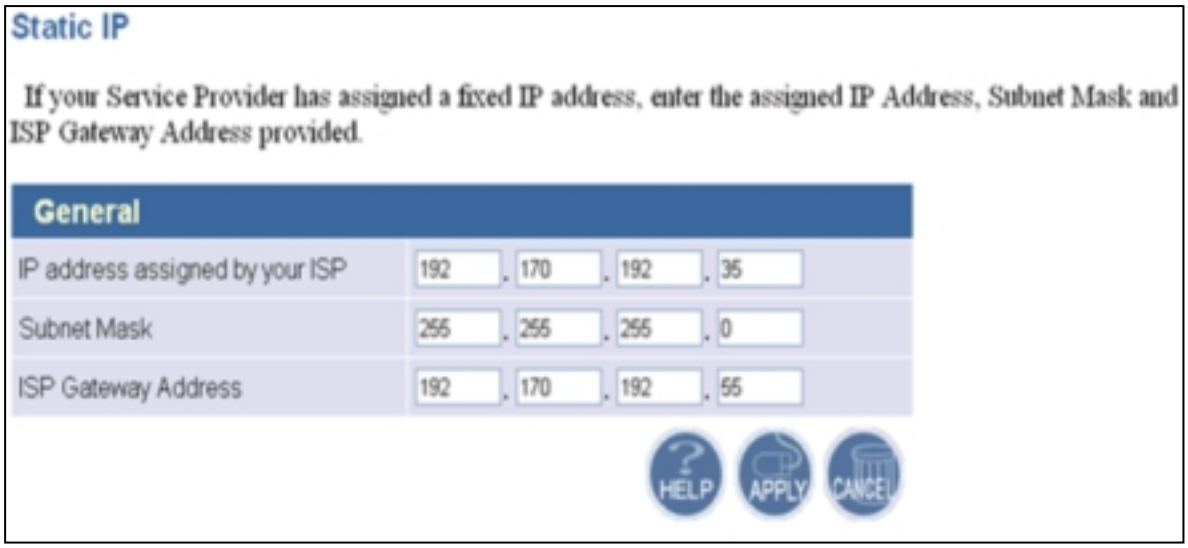
(4) **Service Name:** Enter the service name provided by your ISP.

(5) **MTU:** Maximum Transmission Unit-1492 is the default setting-you may need to change the MTU for optimal performance with your specific ISP.

(6) **Maximum Idle Time:** The amount of time of inactivity before disconnecting your PPPoE session. If you check the Auto-reconnect check box, the access point will automatically connect to your ISP after your system is restarted or if the PPPoE connection is dropped.

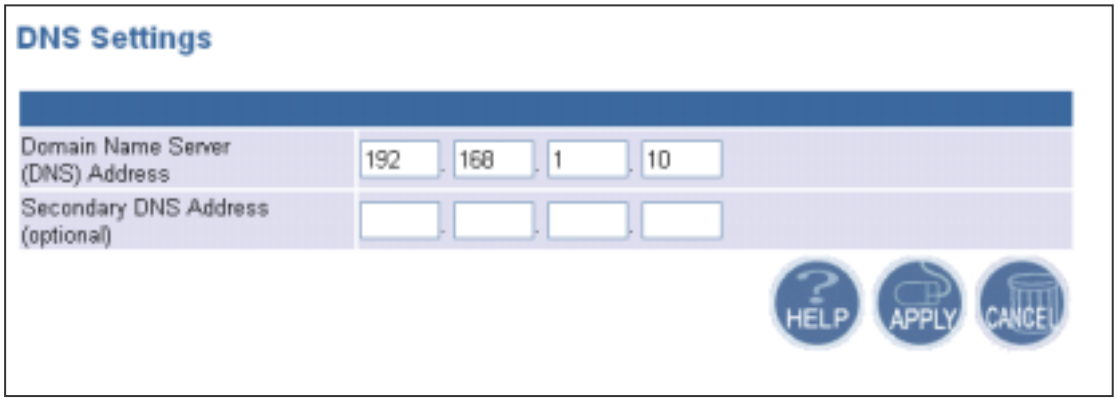
5.2.3 Static IP

If your Service Provider has assigned a fixed IP address, enter the assigned IP Address, Subnet Mask and ISP Gateway Address provided.



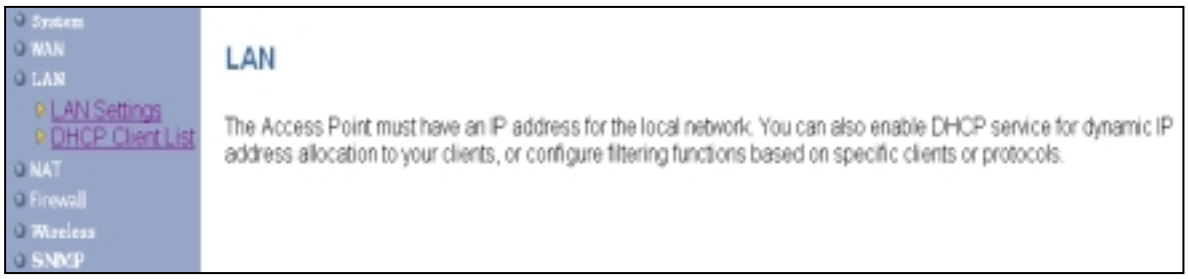
5.2.4 DNS Settings

Domain Name Servers are used to map an IP address to the equivalent domain name. Your ISP should provide the IP address for one or more domain name servers. The access point can be a DNS relay to send clients' request to the Domain Name Server. You can do a DNS lookup to find the IP address of some specific servers. Click **APPLY** to complete your change.



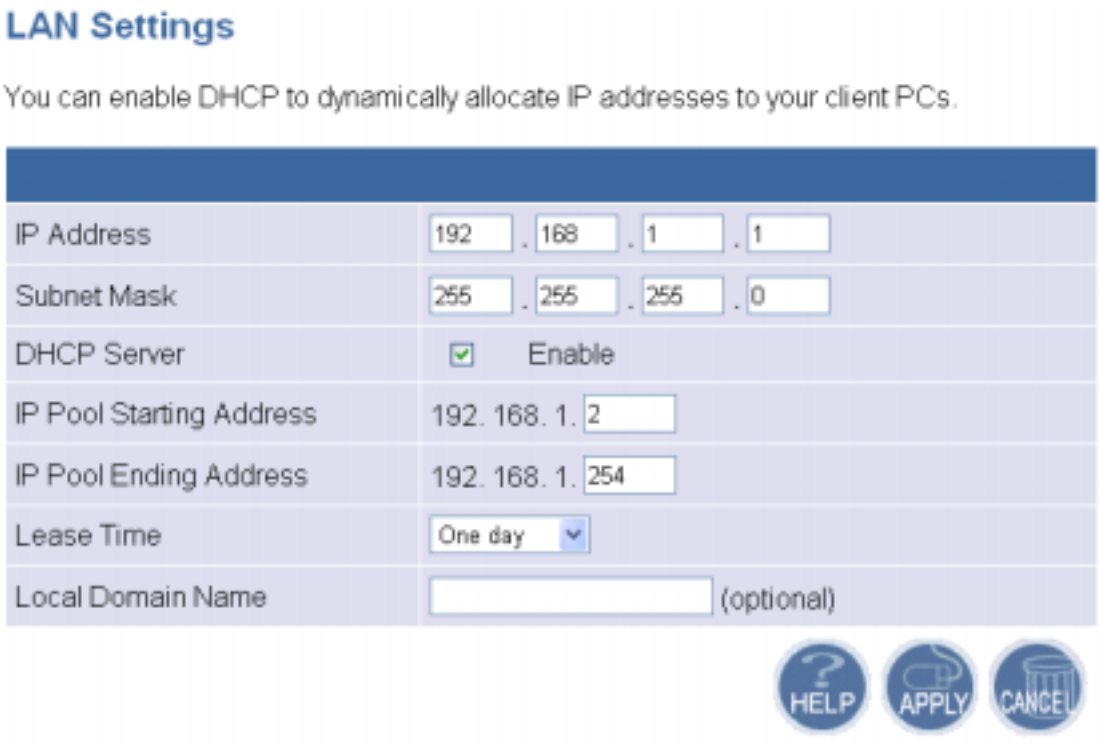
5.3 LAN Setting

The access point must have an IP address for the local network. You can enable DHCP service for dynamic IP address allocation to your clients, or configure filtering functions based on specific clients or protocols.



5.3.1 LAN Settings

You can change the basic settings of AP here, including IP address, Subnet mask, IP Pool Address, Lease Time, and Local Domain Name. Click **APPLY** to complete your change.



(1) **IP Address:** The IP address of the AP. You should have a unique IP address to your network. The default value is 192.168.1.1.

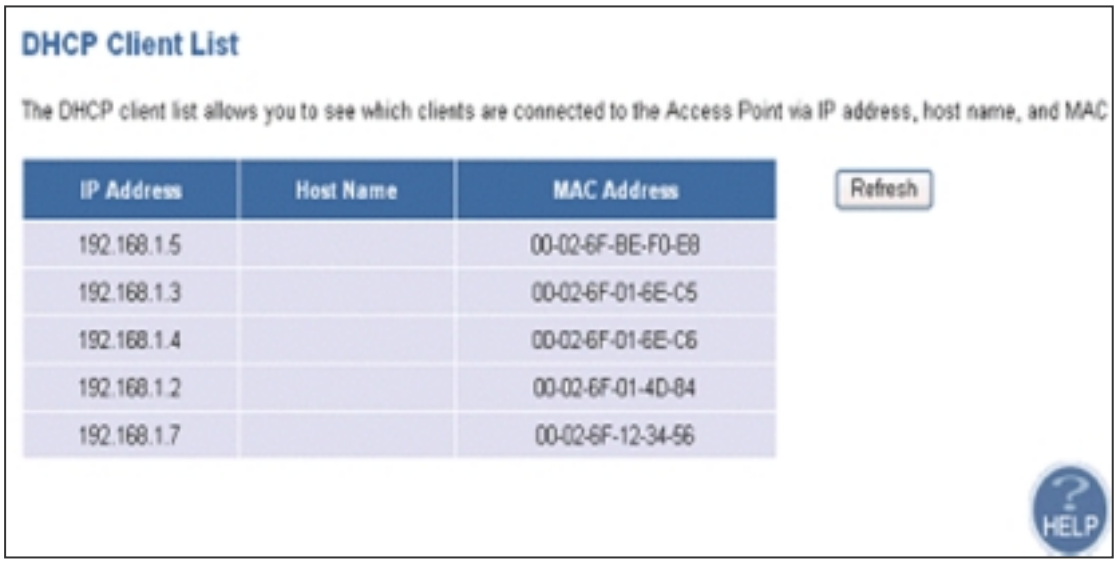
(2) **Subnet Mask:** The Subnet Mask of your access point. The default value is 255.255.255.0.

(3) **DHCP Server:** By default, the AP can function as a DHCP server. The AP can automatically

assign an IP address to a client. To enable this function, clear the “Enable” check box.
(4) **IP Pool Starting Address & IP Pool Ending Address:** The first and the last address in the IP address pool.
(5**) Lease Time:** The period client can have the IP address assigned by DHCP server.
(6) **Local Domain Name:** It’s optional.

5.3.2 DHCP Client Lists

This page lists clients that are connected to the access point via IP address, host name, and MAC address. You can click **Refresh** button to obtain most up-to-date information.



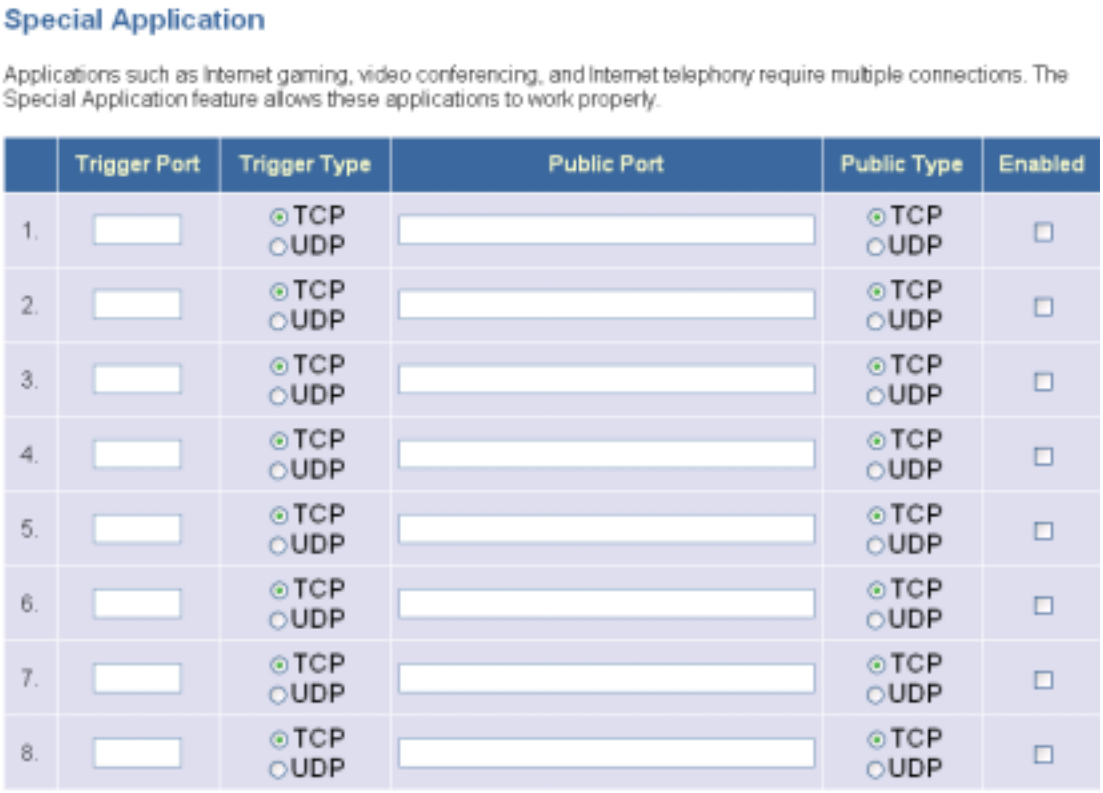
5.4 NAT Setting

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

5.4.1 Special Application

Applications such as Internet gaming, video conferencing, and Internet telephony require multiple

connections. The Special Application feature allows these applications to work properly.



(1) **Trigger Port:** The port will be used to trigger the application. This allows the Router to watch out-going data for specific port numbers.
(2) **Trigger Type:** The protocol will be used to trigger the special application.
(3) **Public Port:** This is the port number on the WAN side that will be used to access the application.
(4) **Public Type:** The protocol for special application.
(5) **Enabled:** Check “Enable” to enable special application of corresponding items.

5.4.2 Virtual Server

You can configure the access point as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the access point redirects the external service request to the appropriate server (located at another internal IP address).

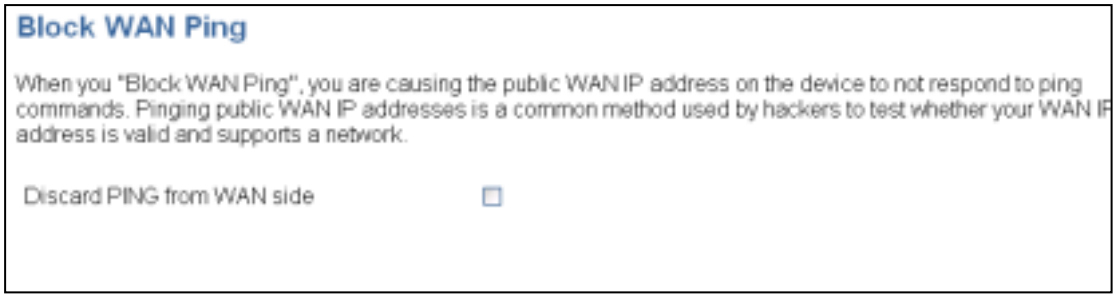
	Mapping Ports	Server IP	Enabled
1.	21, 40	192. 168. 1. 2	☑
2.	41-60, 70-90	192. 168. 1. 4	☑
3.		192. 168. 1.	☐
4.		192. 168. 1.	☐
5.		192. 168. 1.	☐
6.		192. 168. 1.	☐
7.		192. 168. 1.	☐
8.		192. 168. 1.	☐
9.		192. 168. 1.	☐
10.		192. 168. 1.	☐

(1) **Mapping Ports:** The port number of the service used by the server computer. You can use a comma to add multiple ports or use a dash to give port ranges.
(2) **Server IP:** The IP address of server computer that provides the services.
(3) **Enable:** Check “Enable” to enable corresponding items.

5.5 Firewall Setting

5.5.1 Block WAN Ping

Check the “Discard PING from WAN side” to enable blocking WAN ping. When you “Block WAN Ping”, you are causing the public WAN IP address on the device to not respond to ping commands. Pinging public WAN IP address is a common method used by hackers to test whether you WAN IP address is valid and supports a network. Click APPLY to complete your change.



5.5.2 MAC Control

You can block certain clients PCs accessing the internet based on MAC address.

When you enable “MAC Address Control” without allowing unspecified MAC address connect to internet, you will block all client PCs accessing the internet. The clients whose MAC addresses listed in the “MAC Address Control List” can access the internet only if the “Allow Connect to Internet is checked.

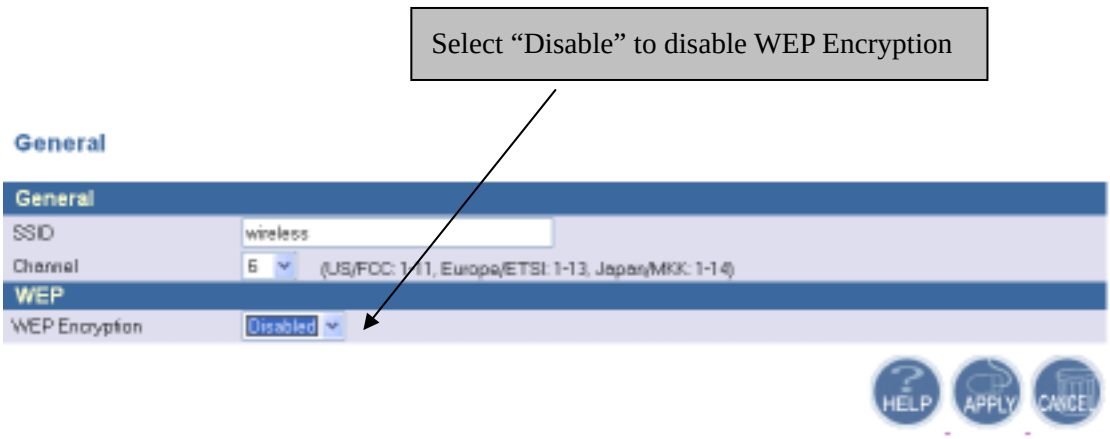
5.5.3 Client Filtering

You can block certain client PCs accessing the internet based on time. IP Filtering can filter the packets sent from clients. For example, you can ban WEB browsing by setting the port to “80”. Remember to select the Check box in the “Enable”. Click **APPLY** to complete your change.

5.6 Wireless Setting

5.6.1 General

In this window you can make changes to the default wireless settings. For communicating, all computers on the network must be within the same IP Address range, and have the same settings for the Radio channel and SSID. If you don't want to utilize WEP Encryption, select "Disable" to disable this function.

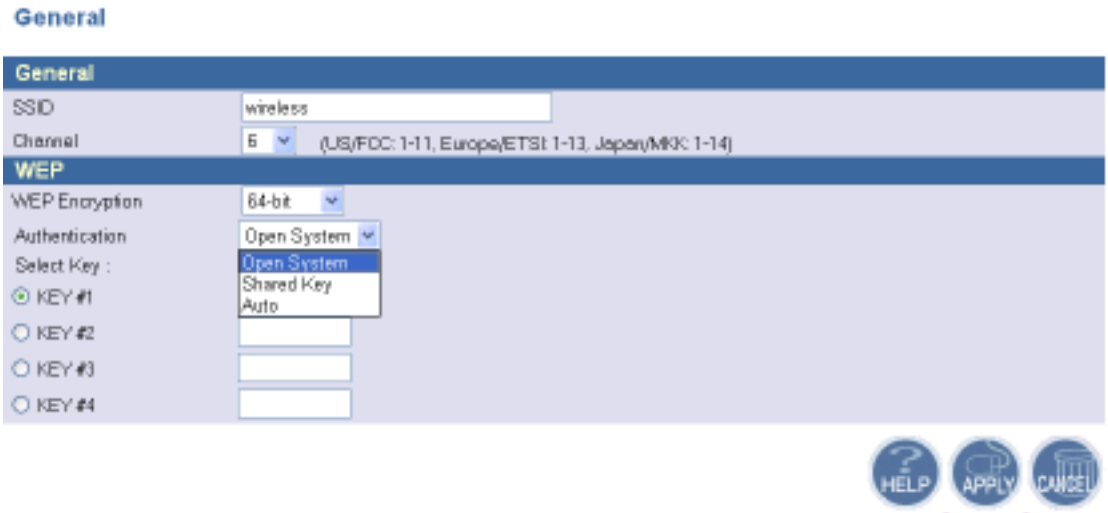


General:

1. **SSID**: The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed

32 characters.

2. **Channel**: The channel shared by all wireless devices. The range of channel is 1~14.



WEP:

Short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. Select **Disabled** to disable this function.

There are two WEP Encryption key length: 64-bit(10 hex digits) and 128 bit(26 hex digits). For Authentication type, you can choose between **Open System**[1]**, Shared Key**[2] **,** and **Auto**[3]**.** All station on your network must use the same authentication type. Check your wireless card's documentation to see what type to use.

Following are the combinations of WEP encryption and authentication type:

(1) If you want to enable WEP encryption with **Open System** for your authentication type, select a key length in WEP encryption field and select **Open System** in Authentication field.

(2) If you want to disable WEP encryption with **Open System** for your authentication type, just select **Disable** in WEP encryption field to disable WEP encryption.

(3) If you want to enable WEP encryption with **Shared Key** for your authentication type, select a key length and select **Shared Key** in Authentication field.

(4) If you want to enable WEP encryption with **Auto** for your authentication type, select a key

---

[1] **Open System -** An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption.

[2] **Shared Key -** when both the sender and the receiver share a secret key. When "Shared Key" is checked, the AP sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate.

[3] **Auto** – No matter the authentication packets with encryption or not, the access point allows the requesting device to authenticate.

length in WEP encryption field and select **Auto** in Authentication field.

(5) Note that there is no way to disable WEP encryption with **Shared Key** or **Auto** for your authentication type.

Enhanced Features

Enhanced Security:

1. **Hide SSID name in Beacon frame:** By selecting this function , AP will not broadcast it's SSID in the beacon frame.
2. **Block Responds to "Unspecified-SSID"**: By selecting this function **,** AP will not respond wireless client's association requests using "ANY" as the AP's SSID.
3. **Wireless Client isolation**: By selecting this function , the AP will not forward uni-cast, multi-cast and broadcast packets to clients sent from any client.

Power Control: If you select MAX(Original), **t**hen the power is the same as the network card's power.

802.11 Enhancement: The setting is listed below.

Field	Ranges	Default value
Fragment Threshold	256 – 2346 (bytes)	2346
RTS Threshold	0 – 3000 (ms)	2432
Beacon Period	Up to 4095 ms	4095

Load Balance: This is the maximum number of users that can associate to this AP. The new client's association will not be accepted when the number of associated clients reaches this number.

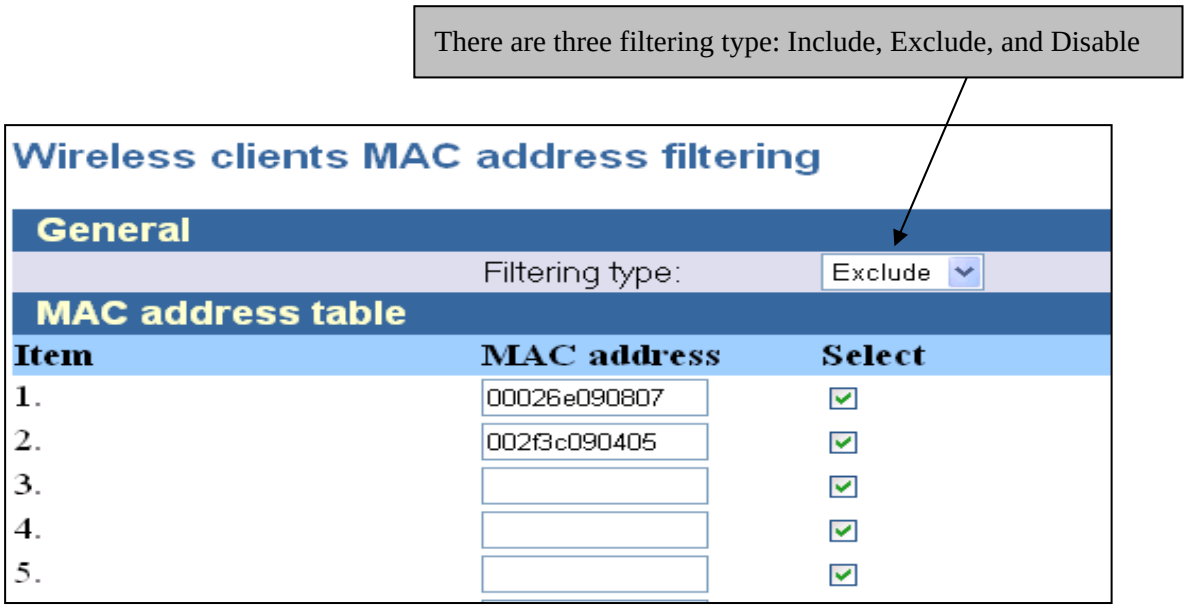
AP Link Completeness: If this function is enabled, the AP will disassociated all associated clients and ban all new association requested when the LAN Ethernet port gets no signals (e.g. it is unplugged).

5.6.2 Associated Clients

This page lists all the associated clients. Click **Refresh** to obtain the most up-to-date information.

5.6.3 Wireless clients MAC Filtering

The maximum number of items is 64. Check the **select** check box to include or exclude corresponding items. The wireless clients whose MAC addresses listed in the "MAC address table" cannot get associations to the AP while the "Filtering type" is chosen to **"**Include**".** On the other hand, only those wireless clients' with MAC addresses listed in the "Exclude" filtering list can associate to the AP. The MAC address filtering function can be disabled by choosing the "Filtering type" to "Disable". Click **APPLY** to complete your change.



5.7 SNMP

Short for Simple Network Management Protocol, a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

5.7.1 SNMP Community

SNMP Community provides a simple kind of password protection. Access to the SNMP device is controlled through community names. The community name can be thought of as a password. If you don't have the correct community name you can't retrieve any data (get) or make any changes (sets). Multiple SNMP managers may be organized in a specified community. You can change your SNMP community settings on this screen. Check the "Enable" check box to enable the SNMP function. Click **APPLY** to complete your change.

Validity: You can enable or disable the SNMP function of the corresponding community item.
Access Right: Select a access right for the corresponding SNMP community (Deny[4]/Read[5]/Write[6]).
Community: Specify the name of community for the SNMP manager(Private/Public). By convention, "Public" community is with a read-only access right.

[4] Deny community will not allow a remote device to read information from a device or to modify settings on that device.
[5] Read-only community enables a remote device to retrieve "read-only" information from a device.
[6] Read-Write community allows a remote device to read information from a device and to modify settings on that device.

5.7.2 SNMP Trap

Traps can be used by network entities to signal abnormal conditions to management stations. SNMP TRAP message can be sent to a host. Click **APPLY** to complete your settings.

Version: Select the SNMP Version.

Select “Disable” to disable the snmp trap function of the corresponding item.

Version1: SNMP Version1

Version2: SNMP Version2

IP Address: Specify the IP Address of the SNMP Manager for SNMP Trap Report.

Community: Specify the name of community (public/Private) for SNMP manager.

Following are the traps supported in the access point:

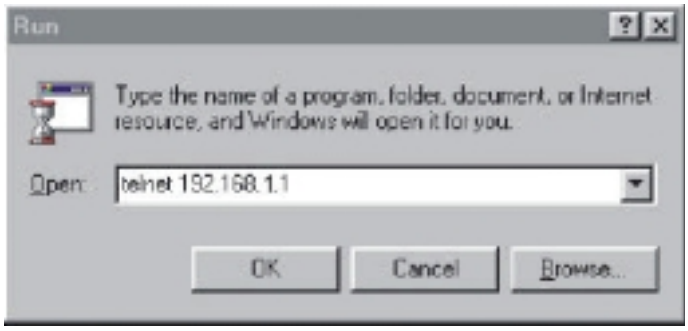
Cold-start trap:

This trap indicates that the specified node’s power has just come on. The cold-start trap is generated every time the access point is power-cycled. Cold-start traps are not generated until three seconds after the access point is power-cycled. This allows time for the hardware providing the low-level IP network interface to start up and stabilize before attempting to send a packet.

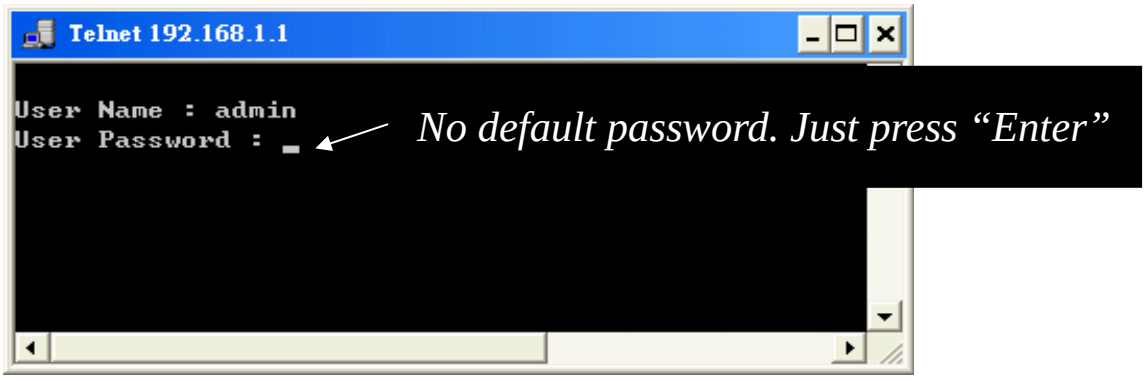
Chapter 6 Configuring the Router through Telnet

6.1 Enter the Telnet session

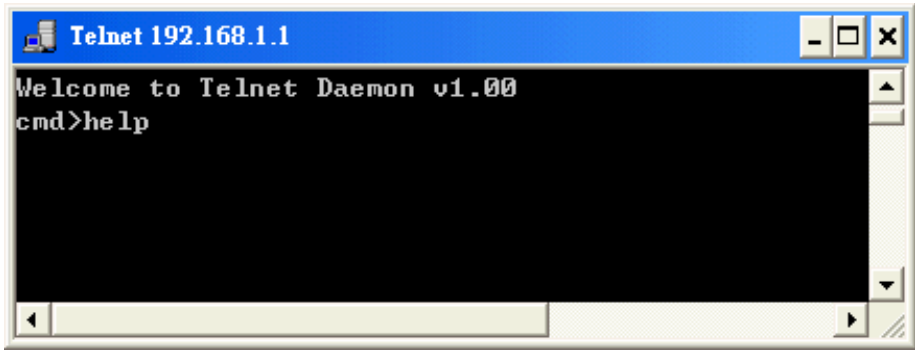
1. Click **Start** button, select **Run** to open the Run dialog box as shown below. Enter telnet **192.168.1.1** (default IP address of AP is 192.168.1.1) in the Open field. Then click **OK** button.



2. After entering the telnet session, enter the User Name and User Password as shown below. (Default User Name is **admin** and there is no default User Password).



3. After entering the telnet daemon, you can first type **help** to see the available commands.



```
                    Command Line Interface v 1.0
================================================
time          : Get current system time.
        Usage: time
settime      : Set system time.
        Usage: settime <hh:mm:ss> [yy/mm/dd] [TZ(GMT +/- hour)]
help          : List all commands.
        Usage: help
ifShow       : Dispaly network interface.
        Usage: ifShow <ifname>
ipConfig    : Configure interface address and subnet mask.
        Usage: ipConfig [ifname] [ip] [subnet mask]
ping          : Ping a host..
        Usage: ping [ip]
routeShow : Show Route.
        Usage: routeShow
dhcpsStart: Start DHCP Server..
        Usage: dhcpsStart
dhcpsStop : Stop DHCP Server..
        Usage: dhcpsStop
exit          : exit this telnet session.
        Usage:    Exit
wlanShow    : Show the WLAN config.
        Usage: wlanShow
reset         : reset the system.
        Usage: reset
wlanSet      : configure the wireless part.
        Usage: wlanset ACTION [arg1], [agr2], ...
```

```
status       : Show the AP status.
        Usage: status
sysSet       : Change the System Configuration.
        Usage: sysSet ACTION [arg1], [agr2], ...
lanShow      : Show the LAN setting.
        Usage: lanShow
lanSet       : Change the LAN Configuration.
        Usage: lanSet
snmpShow     : Show the SNMP setting.
        Usage: snmpShow
snmpSet      : Change the SNMP setting.
        Usage: snmpSet
fwShow       : Show the Firewall setting.
        Usage: fwShow
fwSet        : Change the Firewall setting.
        Usage: fwSet
pppoeShow : Show the PPPoE setting.
        Usage: pppoeShow
pppoeSet     : Change the PPPoE setting.
        Usage: pppoeSet
wanShow : Show the WAN setting.
        Usage: wanShow
wanSet       : Change the WAN setting.
        Usage: wanSet
```

6.2 Command Line for Telnet daemon

1.“time” command shows current system time. Just type “time” at command line prompt.

```
cmd>time
Time zone:        GMT+6
Local time:       Thu Jan    1 00:59:10 1970
GMT time:         Thu Jan    1 06:59:10 1970
cmd>
```

7. Use “settime” to change the current system time.
   Usage: settime <hh:mm:ss> [yy/mm/dd] [TZ(GMT +/- hour)]

```
cmd>settime 15:50:00 2002/12/13
cmd>time
Time zone:      GMT+6
Local time:     Fri Dec 13 15:50:02 2002
GMT time:       Fri Dec 13 21:50:02 2002
cmd>
```

(4) “ifShow” command shows all network interface information, including IP address, subnet mask, and information of packets.

Usage: ifShow [ifname]

To show all network interface, just type “ifShow” at command line prompt.

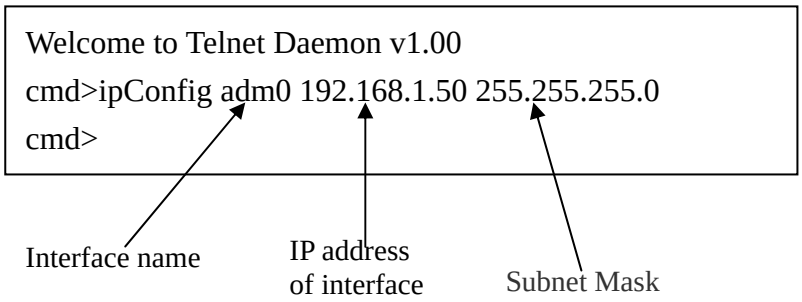
Lo – Loopback interface.
adm – LAN interface.
wlan – Wireless LAN interface.

```
cmd>ifShow
lo (unit number 0):
Type: SOFTWARE_LOOPBACK
Internet address: 127.0.0.1
Netmask 0xff000000 Subnetmask 0xff000000
Metric is 0
Maximum Transfer Unit size is 1536
0 packets received; 0 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped

adm (unit number 0):
Type: ETHERNET_CSMACD
Internet address: 192.168.1.1
Broadcast address: 192.168.1.255
Netmask 0xffffff00 Subnetmask 0xffffff00
```

Ethernet address is 00:01:02:03:04:05
Metric is 0
Maximum Transfer Unit size is 1500
1016 packets received; 686 packets sent
189 multicast packets received
21 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
wlan (unit number 0):
Type: ETHERNET_CSMACD
Netmask 0x1114 Subnetmask 0x111c
Ethernet address is 00:02:6f:01:c0:3f
Metric is 0
Maximum Transfer Unit size is 1500
0 packets received; 209 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
cmd>

(5) "ipConfig" command is used to configure interface address and subnet mask.
Usage: ipConfig [ifname] [ip] [subnetMask]



(6) "ping" command is used to p
Usage: ping [IP address

cmd>ping 192.168.1.20
Start time 14671
Reply from 192.168.1.20
End time 14673
Ping statics for 192.168.1.20:
Packets: Sent = 1, Received = 1, Lost = 0

(7) “exit” command exit the telnet session. Type “exit” at command line prompt.

```
cmd>exit
Exit this telnet session
```

(8) “wlanShow” command shows the wireless LAN configuration, including SSID, Channel, WEP Encryption information, threshold information, and security information. Just type “wlanShow” at command line prompt.

```
cmd>wlanShow
------- AP configuration ---------
MAC address 00:02:6f:01:c0:3d
SSID: Candice
Channel: 6
WEP: Disable
Authentication algorithm: Open System
```

```
Default Wep key Id(1-4): 1
WEP key len: 64-bit
Key 1: 0000000000000000000000000
Key 2: 0000000000000000000000000
Key 3: 0000000000000000000000000
Key 4: 0000000000000000000000000
--- Wireless Enhanced Features ---
Power Level: MAX(original)
Fragment Threshold: 2346
RTS Threshold: 2432
Beacon Interval 100 (max: 4095 ms default :100ms)
Max associated stations: 250
Wireless Client Isolation: Disable
Hide SSID: Disable
Block Responds to 'Unspecified-SSID': Disable
AP Link Completeness: Disable
```

8.“reset” command can reboot the system. Just type ”reset” at command line prompt.

(9) “status” shows current information and settings for your AP.

```
cmd>status
---===== WAN configuration ====---
WAN mode: 1
WAN mode: DHCP client
IP Address: 192.168.123.157
Subnet Mask: 255.255.255.0
Gateway: 192.168.123.254
MAC address: 00:d0:59:13:3e:92
--------- LAN    -----------------
IP: 192.168.1.133
Subnet Mask: 255.255.255.0
Gateway: 192.72.9.250
LAN MAC Address: 00:02:6f:00:08:41
--------- Wireless    -----------------
SSID: [jimmy]
Channel: 6
WEP Security: [Disable]
Wireless MAC address 00:02:6f:01:fa:6b
--------- System Information -----------------
System Up time: 00:14:16
Local time: Thu Jan    1 00:14:16 1970
GMT time: Wed Dec 31 16:14:16 1969
Current Firmware Version: [1.00.4753]
Firmware Date: [2003.02.12]
Hardware Version: [1.0.0]
Serial Number: [00041]
```

10. “routeShow” shows the network routing table, host routing table and the ARP table.

```
cmd>routeShow

Net Routing Table:
Destination       Gateway          NetMask          Flags     Used Hops Interface
192.168.3.0       192.168.3.1      255.255.255.0    U     C   0        0      adm0

Host Routing Table:
Destination       Gateway          NetMask          Flags     Used Hops Interface
127.0.0.1         127.0.0.1                         U H       0        0      lo0

ARP Table:
Destination       Gateway          NetMask          Flags     Used Hops Interface
192.168.3.20      00:00:e2:7ª:59:3f                  U H   L   3377 0      adm0
192.168.3.25      00:02:6f:01:c0:3d                  U H   L   3142 0      adm0
cmd>
```

11.“dhcpsStart” command enables the DHCP server function. The AP can function as a DHCP server and automatically assign an IP address to a client.

```
cmd>dhcpsStart
DhcpsStart: successful!
```

12. “dhcpsStop” command can stop the DHCP server function.

```
Welcome to Telnet Daemon v1.01
cmd>dhcpsStop
cmd>
```

13. “lanShow” command shows the LAN configuration and DHCP configuration, including IP address, Subnet Mask, DHCP status, and IP pool information.

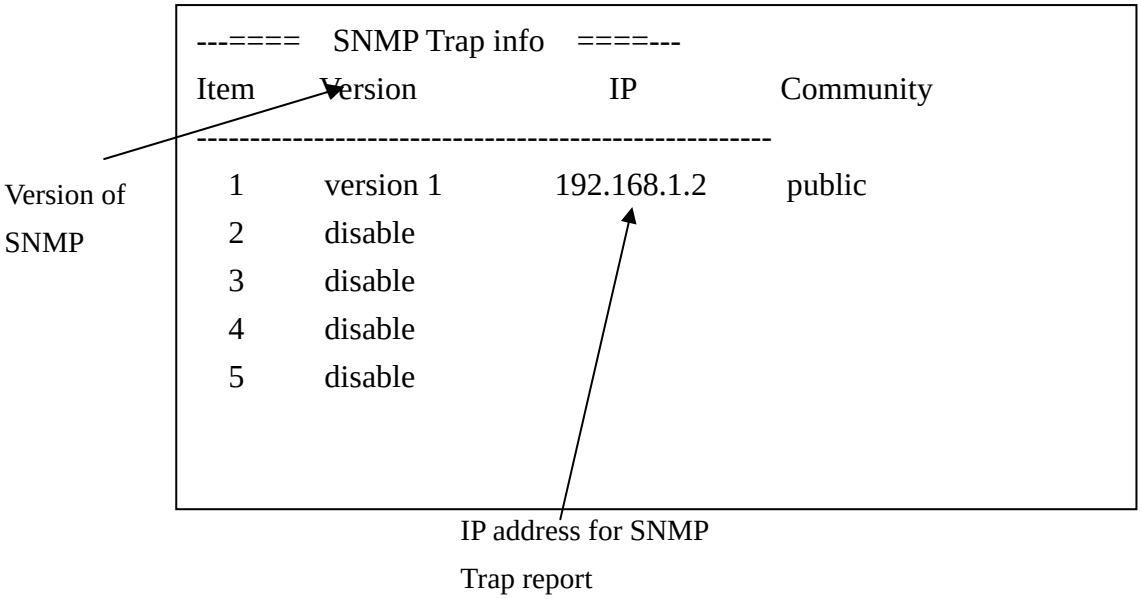
```
Welcome to Telnet Daemon v1.01
cmd>lanShow
---==== LAN configuration ====---
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
MAC address 00:02:6f:00:08:41
DHCP Server: Enabled
IP Pool Starting Address:    192.168.1.2
IP Pool Ending Address:    192.168.1.254
Lease Time:    One day
Local Domain Name:
---==== DHCP configuration ====---
Item       IP                    MAC Address              Host name
```

14.“wanShow” displays the WAN configuration, including IP address, subnet mask, MAC address, gateway, and WAN mode.

```
cmd>wanShow
---==== WAN configuration ====---
WAN mode: DHCP client
IP Address: 192.168.123.156
Subnet Mask: 255.255.255.0
Gateway: 192.168.123.254
MAC address: 00:d0:59:13:3e:91
```

15. “snmpShow” shows SNMP configuration. It displays the information of SNMP Community and SNMP Trap. Type “snmpShow” at the command line prompt.

```
cmd>snmpShow
---==== SNMP Information ====---
SNMP Status: Enable
---==== SNMP Community info ====---
-------------------------------------------------------------------------
Item       Access Right       Community            Validity
1          WRITE                public               Enable
2          CREATE               private              Enable
3          DENY                                      Enable
5          DENY                                      Enable
```



16. “fwShow” shows firewall configuration. It displays the information of Blocking WAN ping, MAC control, and client filtering.

```
Welcome to Telnet Daemon v1.01
cmd>fwShow
----===== Block WAN Ping setting ====----
Block WAN Ping: Enable

----===== MAC Control setting ====----
MAC Address Control: Enabled
Unspecified MAC address connect to Internet: Allow
  ---- Mac control list ----
item      Allow          MAC Address      Validity
  1       Allow          0000e27a593f     Enable
  2       Allow          026f01c03d44     Enable
  3       Allow          00043f253f55     Disable
  4       Disallow       000000000000     Disable
  5       Disallow       000000000000     Disable
  6       Disallow       000000000000     Disable
  7       Disallow       000000000000     Disable
  8       Disallow       000000000000     Disable
```

---===== IP Filter Configuration ====---

IP		Port	Type	Block	Day	Time	
192.168.1.2-	2	21-	21 TCP	Always	N/A- N/A	N/A- N/A	Disable
192.168.1.3-	3	21-	21 TCP	Time	MON-TUE	1:00am- 4:00am	Enable
192.168.1.0-	0	0-	0 TCP	Always	N/A- N/A	N/A- N/A	Disable
192.168.1.0-	0	0-	0 TCP	Always	N/A- N/A	N/A- N/A	Disable
192.168.1.0-	0	0-	0 TCP	Always	N/A- N/A	N/A- N/A	Disable
192.168.1.0-	0	0-	0 TCP	Always	N/A- N/A	N/A- N/A	Disabl

17. “pppoeShow” displays PPPoE configuration.

```
Welcome to Telnet Daemon v1.01
cmd>pppoeShow
---===== PPPoE configuration ====---
PPPoE Status: Disconnected
User Name: s004282
User password: winnie6511
Service Name:
MTU (1400-1492): 1492
Maximum Idle Time: 0
Auto-reconnect: Selected
cmd>
```

6.3 Configuring Wireless LAN through Telnet

The command “wlanSet” can configure the Wireless LAN part. Type “wlanSet” and the action you want to perform. You need to know actions for the Wireless LAN setting.

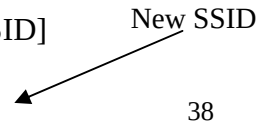
Usage: wlanSet [ACTION] [arg1] [arg2] ….

ACTION	Description	Usage
ssid	Change the SSID	wlanSet ssid [SSID]
channel	Change the wireless channel[1-14]	wlanSet channel [channel number]

ACTION	Description	Usage
frag	Change the fragment Threshold	wlanSet frag [fragment threshold]
rts	Change the RTS Threshold	wlanSet rts [RTSThreshold]
keyid	Change the WEP default key id [1-4]	wlanSet keyid [solate key id]
beacon	Change the beacon Period [0-4095ms]	wlanSet beacon [beacon period]
maxass	Change the max associated stations [1-300]	wlanSet maxass [number of stations]
wepkey	Change the WEP key	wlanSet wepkey [keyid] [key(hex format)]
wep	wlanSet wep [0|64|128]	wlanSet wep [0|64|128]
isolate	Change the Wireless Client Isolation: 0:disable, 1:enable	wlanSet solate [0|1]
hidessid	Change the Hide SSID: 0:disable, 1:enable	wlanSet hidessid [0|1]
block	Change the Block Responds to 'Unspecified-SSID': 0:disable, 1:enable	wlanSet block [0|1]
power	Change the Outpower level: 0:Original, 1: 100mW, 2: 50mW, 3: 20mW	wlanSet power [0|1|2|3]
aplink	Change the AP Link Completeness: 0:disable, 1:enable	wlanSet aplink [0|1]
authalgo	Change Authentication algorithm: 1:Open system, 2: Shared key, 3:Auto	wlanSet authalgo [1|2|3]
mac	Change the MAC address filtering.	WlanSet mac [disable|include|exclude|select|unselect|setmac|clear|clearall]
macShow	Show the MAC filtering setting.	WlanSet macshow

1. The "ssid" action can change the SSID

   Usage: wlanSet ssid [New SSID]



```
cmd>wlanSet ssid WirelessLAN
Old SSID: Wireless
New SSID (after reset): WirelessLAN
(Please remember to reset the Access Point if you made any change).
```

2. The “channel” action can change the wireless channel.
   Usage: wlanSet channel [New channel number]

```
cmd>wlanSet channel 5
Old Channel: 6
New Channel (after reset): 5
(Please remember to reset the Access Point if you made any change).
```

3. The “frag” action can change the frame’s fragment threshold.
   Fragment Threshold: 256~2346 bytes , default is 2346
   Usage: wlanSet frag [New fragment threshold]

```
cmd>wlanSet frag 2000
Old Fragment Threshold: 2346
New Fragment Threshold (after reset): 2000
(Please remember to reset the Access Point if you made any change).
```

4. The “rts” action can change the frame’s RTS threshold.
   RTS Threshold: 0~3000 ms, default is 2432
   Usage: wlanSet rts [Nes RTS threshold]

```
cmd>wlanSet rts 2500
Old RTS Threshold: 2432
New RTS Threshold (after reset): 2500
(Please remember to reset the Access Point if you made any change).
```

5. The “keyid” action can change the WEP default ID(the default is from 1 to 4).
   Usage: wlanSet keyid [New key default ID]

```
cmd>wlanSet keyid 2
Old WEP default key id: 0
New WEP default key id (after reset): 2
(Please remember to reset the Access Point if you made any change).
```

6.

Usage: wlanSet beacon [New beacon period]

7. The “maxass” action can set the maximun number of users that can associate the AP.

```
cmd>wlanSet maxass 20
Old Maximum Assocated Stations: 250
New Maximum Assocated Stations (after reset): 20
(Please remember to reset the Access Point if you made any change).
```

8. The “wepkey” action can change the WEP key.
   Usage: wlanSet wepkey [keyid] [key(hex format)]

```
cmd>wlanSet wepkey 1 1122334455
CmdWlanSetKey() key 1122334455
Old Key 1: 0011223344
New Key 1: 1122334455
(Please remember to reset the Access Point if you made any change).
```

9. The action “wep” is for changing the WEP key length (0:disable/64 bit/128 bit).
   Usage: wlanSet wep [New key length]

Example:

```
cmd>wlanSet wep 128
Old WEP Encryption: 64-bit
New WEP Encryption (after reset): 128-bit
(Please remember to reset the Access Point if you made any change).
```

To disable the WEP key, type following command:

```
cmd>wlanSet wep 0
Old WEP Encryption: 64-bit
New WEP Encryption (after reset): Disabled
(Please remember to reset the Access Point if you made any change).
```

10. The “isolate” action can enable/disable the wireless client isolation function.
    0: Disable
    1: Enable
    Usage: wlanSet isolate [0|1]

```
cmd>wlanSet isolate 1
Old Wireless Client Isolation: Disable
New Wireless Client Isolation (after reset): Enable
(Please remember to reset the Access Point if you made any change).
```

11. The “hidessid” action can enable/disable the “Hide SSID in beacon frame” function.
    0: Disable
    1: Enable
    Usage: wlanSet hidessid [0|1]

```
cmd>wlanSet hidessid 1
Old Hide SSID: Disable
New Hide SSID (after reset): Enable
(Please remember to reset the Access Point if you made any change).
```

12. The “block” action can enable/disable the ”Block responds to Unspecified-SSID” function.
    0: Disable
    1: Enable
    Usage: wlanSet block [0|1]

```
cmd>wlanSet block 0
Old Block Responds to 'Unspecified-SSID': Enable
New Block Responds to 'Unspecified-SSID' (after reset): Disable
(Please remember to reset the Access Point if you made any change).
```

13. The “power” action can change the power level 0:Original, 1: 100mW, 2: 50mW, 3: 20mW
    0:Original
    1: 100mW
    2: 50mW
    3: 20mW
    Usage: wlanSet power [0|1|2|3]

```
cmd>wlanSet power 2
Old Power Level: MAX(original)
New Power Level (after reset): 50mW
(Please remember to reset the Access Point if you made any change).
```

14. The “aplink” action can change the AP Link Completeness. If enable this function, the WLAN interface will be disabled when plug off the cable of LAN interface,
    0: Disable
    1: Enable
    Usage: wlanSet aplink [0|1]

```
cmd>wlanSet aplink 1
Old AP Link Completeness: Disable
New AP Link Completeness (after reset): Enable
(Please remember to reset the Access Point if you made any change).
```

15. The “authalgo” action can change the authentication algorithm.
    1: Shared key
    2: Open system
    3: Auto
    Usage: wlanSet authalgo [1|2|3]

```
Welcome to Telnet Daemon v1.01
cmd>wlanSet authalgo
Current Authentication algorithm: Open System
cmd>wlanSet authalgo 3
Old Authentication algorithm: Open System
New Authentication algorithm (after reset): Auto
(Please remember to reset the Access Point if you made any change).
```

(10) [illegible]

Description	Usage
Set filtering type to ‘disable’	filterSet mac disable
Set filtering type to ‘include’	filterSet mac include
Set filtering type to ‘exclude’	filterSet mac exclude
Set mac address	filterSet mac setmac [index] [MAC address]

	index: 1…1291632, MAC address format : 00-00-01-02-03-04-05
Select a mac address	filterSet mac select [index] index: 1…64
Unselect a mac address	filterSet mac unselect [index] index: 1…64
Clear a mac address	filterSet mac clear [index] index: 1…64
Clear all mac addresses	filterSet mac clearall

(11) The “macshow” action can display the MAC filtering configuration.

Usage: wlanSet macshow

```
cmd>wlanSet macshow
---======= MAC control list ---======
Filtering type: Disabled (Any station can access)
Item      MAC                  Select
-------------------------------------------
1         00:00:00:00:00:00        Selected
2         00:00:00:00:00:00        Selected
3         00:00:00:00:00:00        Selected
4         00:00:00:00:00:00        Selected
5         00:00:00:00:00:00        Selected
6         00:00:00:00:00:00        SELECTED
```

6.4 Configuring LAN through Telnet

The command “lanSet” can configure the LAN part. Type “lanSet” and the action you want to perform. You need to know actions for the LAN setting.

Usage: lanSet [ACTION] [arg1] [arg2] ….

ACTION	Description	Usage

ACTION	Description	Usage
ip	Change the LAN's IP and mask	lanSet ip [IP] [mask]
dhcp	Change the DHCP server setting.	LanSet dhcp ['disable'|start ip] [end ip] [lease time] [domain name]

1. The "ip" action can change the LAN's IP address and Subnet Mask.

Usage: lanSet ip [IP] [mask]

Example:

```
cmd>lanSet ip 192.168.3.1 255.255.255.0
argc 3, ip [192.168.3.1] mask [255.255.255.0]
(Please remember to reset the Access Point if you made any change).
```

2. The "dhcp" action can change the dhcp server setting.

Usage: lanSet dhcp ['disable' | start ip] [end ip] [lease time] [domain name]

Argument Description	Usage
'disable'|start ip	disable: to disable the DHCP server function start ip: the start IP address of the IP pool
end ip	The ending IP address of the IP pool
lease time: The period client can have the IP address assigned by DHCP server.	0: Half hour, 1: One hour, 2: Two hours, 3:Half day, 4: One day, 5: Two days, 6: One week, 7:Two weeks 8: Forever
domain name: the domain name (needed by some applications)	

Usage: To disable the dhcp server, type: lanSet dhcp 'disable'

To enable the dhcp server, type:

lanSet dhcp ['disable' | start ip] [end ip] [lease time] [domain name]

Example:

```
cmd>lanSet dhcp disable
disable the DHCP server
(Please remember to reset the Access Point if you made any change).
cmd>
```

```
cmd>lanSet dhcp 55 66 1 domainname
LAN set DHCP ok!
(Please remember to reset the Access Point if you made any change).
cmd>
```

6.5 Configuring System through Telnet

The command “sysSet” can change the settings of system, including time and administrator settings. Type “sysSet” and the action you want to perform. You need to know actions for filter setting.

Usage: sysSet [ACTION] [arg1][arg2]…..

ACTION	Description	Usage
passwd	Change the password.	SysSet passwd
idletime	Change the IdleTimeOut.	SysSet idletime [idle time (mins)]
remote	Change the Remote Management status	sysSet remote [0|1][IP]
fwupgrade	firmware upgrade.	SysSet fwupgrade [IP] [file]
setdefault	Set to default system configuration.	SysSet setdefault
reset	reset the system.	SysSet reset
sntppoll	Change the SNTP polling time	sysSet sntppoll
sntp	Change the SNTP setting	sysSet sntp [0|1] [IP]

ACTION	Description	Usage
sntpchangeip	Change a SNTP server's IP.	SysSet sntpchangeip [INDEX] [IP], index: 1-4

7. The "passwd" action can change the system password.
   Usage: sysSet passwd

Example:

```
Welcome to Telnet Daemon v1.01
cmd>sysSet passwd
**** Change password ****
Please enter current password:
Please enter new password: ****
Please re-enter new password: ****
New password is set
cmd>
```

8. The "idletime" action can change the system idle time out.

Usage: sysSet idletime [idle time(min)]

```
cmd>sysSet idletime 98
New Idle time value out is 98 min(s)
(Please remember to reset the Access Point if you made any change).
cmd>
```

9. The "remote" action can enable or disable the remote management function. You can enter the IP address of the remote manager.
   Usage: sysSet remote [0|1] [IP of remote manager]

   0: disable
   1: enable

Example:

cmd>sysSet remote

Current Remote Management status: Disabled
cmd>sysSet remote 1 192.168.3.25
New Remote Management status: Enabled
(Please remember to reset the Access Point if you made any change).
cmd>

10. The ”fwupgrade” action can do the firmware upgrade.
    Usage: sysSet fwupgrade [IP] [file]

Example:

Welcome to Telnet Daemon v1.01
cmd>sysSet fwupgrade 192.168.3.20 application.dlf
Current Firmware Version: 1.00.4431
Firmware Date: 2003.01.02
TFTP download start
TFTP download successed
(Please remember to reset the Access Point if you made any change).
cmd>

11. The “setdefault” action can reset system to factory default configuration. This command is the same as the “Restore Factory Default Configuration” function of the Web-Based utility.
    Usage: sysSet setdefault

    Example:
    Welcome to Telnet Daemon v1.01
    cmd>sysSet setdefault
    Load default system configuration
    Load default system configuration finished

    Note: You have to reset system to let this change effective.

12. The “reset” action can reboot the system and refresh the AP’s connection.
    Usage: sysSet reset

13. The “sntppoll” action can change the SNTP pooling time.
    Usage: sysSet sntppoll [polling time(sec)]

Example:

```
cmd>sysSet sntppoll
Current SNTP polling time value is 86400 second(s)
cmd>
```

```
Welcome to Telnet Daemon v1.01
cmd>sysSet sntppoll 11000
New SNTP polling time value is 11000 second(s)
(Please remember to reset the Access Point if you made any change).
cmd>
```

(12) The “sntp” action can change SNTP function and set SNTP server.

Usage: sntp [0|1] [IP]

0: Disable 1: Enable

```
cmd>sysSet sntp 0
New SNTP status: Disabled
(Please remember to reset the Access Point if you made any change).
cmd>sysSet sntp 1 192.168.3.20
New SNTP configuration
Usage: sntp [0|1] [IP], 0:disable, 1:enable
---===== SNTP configuration ===---
Status: Enable
Polling time: 86400 seconds
Server #1's IP: 192.168.3.20
Server #2's IP: 0.0.0.0
```

(13) The “sntpchangeip” action can change SNTP server’s IP.

Usage: sntpchangeip [Index] [sntp server’s IP]

index: 0-4

Example:

cmd>sysSet sntpchangeip 1 192.168.3.25

New setting:

---==== SNTP configuration ===---
Status: Enable
Polling time: 86400 seconds
Server #1's IP: 192.168.3.25
Server #2's IP: 0.0.0.0
Server #3's IP: 0.0.0.0
Server #4's IP: 0.0.0.0
(Please remember to reset the Access Point if you made any change).
cmd>

6.6 Configuring Firewall through Telnet

The command “fwSet” can change the settings of blocking WAN ping, MAC control, and IP filtering. Type “fwSet” and the action you want to perform. You need to know actions for firewall setting.

Usage: fwSet [ACTION] [arg1][arg2]…..

ACTION	Description	Usage
ip	Set the IP filtering setting.	FwSet ip ….
Ipdaytime	Change the daytime part	fwSet ipdaytime
ipstatus	Enable or Disable the IP filtering function.	FwSet ipstatus
blockping	Block pings from WAN	fwSet blockping [0|1]
macctrladd	Add address to MAC Control	fwSet macctrladd [mac address] [0|1]
macctrlallow	Set mac control to allow	fwSet macctrlallow [index]
macctrldis	Set mac control to disallow	fwSet macctrldis [index]
macctrldel	Delete an MAC control entry	fwSet macctrldel [index]
macctrl	Set MAC access control status	fwSet macctrl [0|1]
macctrlunspc	Set MAC access connect to Internet	fwSet macctrlunspc [0|1]

1. The “ip” action can set the IP and port to be block. You can set the protocol type to be block.

Usage: fwSet ip [Index] [Start IP] [End IP] [Start port] [End port] [Protocol]

Argument	Description
index: the (index)th item to be modified	index : 1 .. 8
Start IP	the last byte of the Start IP
End IP	the last byte of the End IP
Start port	the first port being blocked
End port	the last port being blocked
Protocol: the protocol type	Type “tcp” or “udp”

Example:

```
cmd>fwSet ip 2 45 78 21 21 udp
Set to index 2 Source IP Start: 45 Source IP end: 78 PortStart 21 PortEnd 21 pro
tocol 2
Ok
```

2. The “ipdaytime” can set the day and time to block the IP address.
   Usage: fwSet ipdaytime index [Start day] [End day] [Start hour] [End hour]
   Example: fwSet ipdaytime 1 MON FRI 9am 6pm

Argument Description	Usage
index: the (index)th item to be modified	index : 1 .. 8
Start day: the day start to block	SUN, MON, TUE, WED, THU, FRI, SAT
End day: the day stop to block	SUN, MON, TUE, WED, THU, FRI, SAT
Start hour: the time start to block	0am, 1am, 2am, 3am, 4am, 5am, 6am, 7am, 8am, 9am, 10am,11am, 12am, 1pm, 2pm, 3pm, 4pm, 5pm, 6pm, 7pm, 8pm, 9pm,10pm, 11pm
End hour: the time stop to block	0am, 1am, 2am, 3am, 4am, 5am, 6am, 7am, 8am, 9am, 10am 11am, 12am, 1pm, 2pm, 3pm, 4pm, 5pm, 6pm, 7pm, 8pm, 9pm,10pm, 11pm

3. The “ipstatus” action can enable and disable the IP filtering function.
   Usage: fwSet ipstatus [index] [status]

Example: fwSet ipstatus 1 2

Argument Description	Usage
index: the (index)th item to be modified	index : 1 .. 8
status	0: disable, 1:enable, 2:always block, 3:block on time

Note: If you choose 3 (block on time) for status, you have to indicate the day and time by using the “ipdaytime” action.

4. The “blockping” action can block pings from WAN.

Usage: fwSet blockping [0|1]

0: Disable

1: Enable

```
Welcome to Telnet Daemon v1.01
cmd>fwSet blockping 0
Old Block WAN Ping: Enable
New Block WAN Ping: Disable
cmd>
```

5. The “macctrladd” action can add address to MAC Address Control list.

Usage: macctrladd [mac address] [filter action],

mac address format: xx-xx-xx-xx-xx-xx

filter action: 0:disallow connect to internet, 1:allow connect to internet

Example:

```
cmd>fwSet macctrladd 00-02-3c-4a-09-08 1
finished.
```

6. y index.

Usage: macctrlallow [index], index: 1.. 32

Example:

```
cmd>fwSet macctrlallow 1
Old: index #1 is dis-allowed to connect to internet
Current: index is #1 allowed to connect to internet
```

7. The “macctrldis” action can set mac address to disallow connecting to internet by index.

```
cmd>fwSet macctrldis 1
Old: index #1 is allowed to connect to internet
Current: index is #1 dis-allowed to connect to internet
```

8. The “macctrldel” action can delete an MAC control entry of MAC Address Control List.

```
cmd>fwSet macctrldel 2
        finished.
```

9. The “macctrl” action can enable or disable the MAC Access Control.
   Usage: fwSet macctrl [0|1]
   0: disable MAC Access Control
   1: enable MAC Access Control

```
cmd>fwSet macctrl 0
Old MAC Address Control Status: Enable
New MAC Address Control Status: Disable
```

10. The “ macctrlunspc” action can enable or disable the “Allow unspecified MAC address connect to Internet”.
    Usage: fwSet macctrlunspc [0|1]
    0: disable
    1: enable

```
cmd>fwSet macctrlunspc 0
Old unspecified MAC address connect to Internet: Allow
!!!Warning!!! Your PC may be no longer to connect to the AP.
Are you sure to make this change? [Y/N]
Y
New unspecified MAC address connect to Internet: Disallow
cmd>
```

6.7 Configuring SNMP through Telnet

The command “snmpSet” can change the settings of SNMP. Type “snmpSet” and the action you want to perform. You need to know actions for snmp setting.

Usage: snmpSet [ACTION] [arg1] [arg2]…..

ACTION	Description	Usage
comstatus	Enable or disable the SNMP community function	snmpSet comstatus [0|1]
community	Change the SNMP community setting.	SnmpSet community [index] [access right] [community] [validatiy]
trap	Change the SNMP trap setting.	SnmpSet trap [index] [version] [IP] [community]

1. The “comstatus” action can enable or disable the community status.
   Usage: snmpSet comstatus [0|1]
   0: Disable
   1: Enable
2. The “community” action can change the settings of SNMP community.
   Usage: snmpSet community [item] [Access Right] [Community] [Validity]

Argument Description	Usage
item	item: 1 .. 5
Access Right: Select a access right for the corresponding SNMP community	Type “deny”, “read”, “write”, “create” for different access right
Validity: enable or disable the SNMP function of the corresponding community item.	0:disable, 1:enable

Example:

```
Welcome to Telnet Daemon v1.01
cmd>snmpSet community 1 read public 1
SNMP community set ok.
(Please remember to reset the Access Point if you made any change).
```

3. The “trap” action can change the settings of SNMP trap.
   Usage: snmpSet trap [item] [version] [ip] [community]

Argument Description	Usage
item	item: 1 .. 5
Version: the version of SNMP	0:disable, 1: Version 1, 2: Version 2

Example:

```
cmd>snmpSet trap 3 2 192.168.1.1 public
SNMP trap set ok.
(Please remember to reset the Access Point if you made any change).
```

6.8 Configuring WAN through Telnet

The command “wanSet” can change the settings of WAN. Type “wanSet” and the action you want to perform. You need to know actions for WAN setting.

Usage: wanSet [ACTION] [arg1] [arg2]…..

ACTION	Description	Usage
dnsprm	Change the Primary DNS IP	wanSet dnsprm [IP]
dnssec	Change the Secondary DNS IP	wanSet dnssec [IP]
mode	Change the WAN mode	wanSet mode [1|2|3], 1: DHCP client, 2: Static IP, 3:PPPoE
static	Change the WAN IP and mask for static mode	wanSet ipmask [IP address] [netmask] [gateway]
dhcpchost	Change the DHCP client host name	wanSet dhcpchost [hostname]
macaddr	Change the WAN MAC address	wanSet macaddr [mac address]

1. The “dnsprm” action can set the primary DNS address.

Example:

```
cmd>wanSet dnsprm 192.168.192.74
Old primary DNS IP: 192.72.9.45
New primary DNS IP: 192.168.192.74
(Please remember to reset the Access Point if you made any change).
```

2. The “dnssec” action can set the secondary DNS address.

Example:

```
cmd>wanSet dnssec 192.168.192.55
Old secondary DNS IP: 192.72.9.46
New secondary DNS IP: 192.168.192.55
(Please remember to reset the Access Point if you made any change).
cmd>
```

3. The “mode” action can change the WAN mode.

1: DHCP client

2: Static IP

3: PPPoE

Example:

```
Welcome to Telnet Daemon v1.01
cmd>wanSet mode 2
Old WAN mode: DHCP client
New WAN mode: Static IP
(Please remember to reset the Access Point if you made any change).
cmd>wanSet mode
Current WAN mode: Static IP
```

4. The ”static” action can the WAN IP and Subnet Mask for static mode.

Usage: wanSet static [IP address] [netmask] [gateway]

Example:

```
cmd>wanSet static
Usage: WANSet ip [IP address] [netmask] [gateway]
Current WAN IP: 192.72.9.20, mask:255.255.255.0, gateway: 192.72.9.250
cmd>wanSet static 192.72.9.20 255.255.255.0 192.72.9.250
Old WAN IP: 192.72.9.20, mask:255.255.255.0, gateway: 192.72.9.250
New WAN IP: 192.72.9.20, mask:255.255.255.0, gateway: 192.72.9.250
(Please remember to reset the Access Point if you made any change).
```

5. The “dhcpchost” action can set the DHCP client host name.
   Usage: wanSet dhcpchost [hostname]

Example:

```
cmd>wanSet dhcpchost hello
Old host name:
New host name: hello
(Please remember to reset the Access Point if you made any change).
```

6. The “macaddr” action can set the WAN MAC address.
   Usage: wanSet macaddr [mac address]
   MAC address format: xx-xx-xx-xx-xx-xx
   Example:

```
cmd>wanSet macaddr 00-d0-59-13-3e-92
Old WAN MAC address: 00-d0-59-13-3e-91
New WAN MAC address: 00-d0-59-13-3e-92
(Please remember to reset the Access Point if you made any change).
```

6.9 Configuring PPPoE through Telnet

The command “pppoeSet” can change the settings of PPPoE. Type “pppoeSet” and the action you want to perform. You need to know actions for PPPoE setting.

Usage: pppoeSet [ACTION] [arg1] [arg2]…..

ACTION	Description	Usage
name	Change the PPPoE user name	pppoeSet name [name]
password	Change the PPPoE password	pppoeSet password [password]
srvname	Change the Service name	pppoeSet srvname [service name]
mtu	Change the MTU	pppoeSet mtu [mtu] Mtu: 1400 – 1492
idletime	Change the maximum idle time	pppoeSet idletime [idle time] Idletime: 0 – 60 min
autoconn	Enable or disable the auto-reconnect	pppoeSet autoconn [0|1] 0: unselected 1: selected

1. The “name” action can change the PPPoE name.

Usage: pppoeSet name [name]

Example:

```
Welcome to Telnet Daemon v1.01
cmd>pppoeSet name guest
Old User name: s004282
New User name: guest
cmd>
```

2. The “ password” action can change the PPPoE password.

Usage: pppoeSet password [password]

Example:

```
cmd>pppoeSet password guest1
Old Password: test1
New Password: guest1
```

3. The “srvname” action can change the service name.

Usage: pppoeSet srvname [service name]

Example:

```
cmd>pppoeSet srvname http
Old Service name: ftp
New Service name: http
```

4. The “mtu” action can change the maximum transmission unit.

Usage: pppoeSet mtu [mtu]

Example:

```
cmd>pppoeSet mtu 1422
Old MTU: 1432
New MTU: 1422
```

Note: the default mtu is 1492.

5. The “ idletime” action can change the maximum idle time.

Usage: pppoeSet idletime [idle time]

Example:

```
cmd>pppoeSet idletime 30
Old idle time: 40
New idle time: 30
```

6. The “autoconn” action can enable or disable the auto-reconnect function.

Usage: pppoeSet autoconn [0|1]

0: Unselected (disable)

1: Selected (enable)

Example:

Welcome to Telnet Daemon v1.01
cmd>pppoeSet autoconn 1
Old auto reconnection: Unselect
New auto reconnection: Selected

6.10 Upgrading Firmware through Telnet

If problem happens during firmware upgrading (e.g.. Power off abnormally), the AP may not work normally. If this is the case, the AP will start a Telnet Daemon on the LAN interface. After that, user can telnet to the AP and make a firmware upgrade using TFTP method. By doing so, user can make AP works again.

1. You will see the warning message shown as below:

```
Verifying product code.....FAIL

***** WARNING *****

Need to reprogram the Flash. Telnet init
Enter into daemon : Telnet listen Port 23
```

2. Connect the managed computer and the AP's **LAN** port with an Ethernet cable.

3. Telnet to the AP. Make sure the AP's IP Address is the one when problem happened.

```
***** WARNING *****
Need to reprogram the Flash!
User Name :
```

4. Type the fixed User Name and Password (User Name: root / Password: tftp) to enter the telnet session.

```
***** WARNING *****
Need to reprogram the Flash!
User Name : root
User Password : tftp
```

5. Type **help** to list all command.

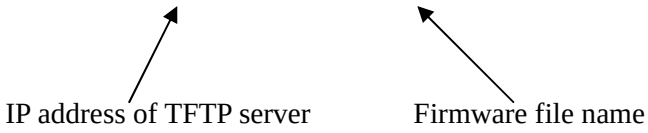
```
cmd>help
                    Command Line Interface v 1.0
==============================================
time           : Get current system time.
        Usage: time
help           : List all commands.
        Usage: help
tftp           : tftp download.
        Usage: tftp [IP] [file]
ipConfig    : Configure interface address and subnet mask.
        Usage: ipConfig [ifname] [ip] [subnet mask]
ifShow        : Dispaly network interface.
        Usage: ifShow <ifname>
reset         : reset the system.
        Usage: reset
ping           : Ping a host..
        Usage: ping [ip] [ms]
```

6. On the managed computer, run the TFTP Server utility. Make sure to specify the folder in which the firmware files reside.

7. To perform the firmware upgrade, use **tftp** command.

Usage: tftp [IP Address] [File Name]

```
Welcome to Telnet Daemon v1.00
cmd>tftp 192.168.1.20 application.dlf
```



8. After downloading successfully, the AP will be reset and start running normally. Telnet session will be closed after downloading successfully.

```
Welcome to Telnet Daemon v1.00
cmd>tftp 192.168.1.20 application.dlf
TFTP download start
TFTP download succeed

cmd>
```

Appendix A: Glossary

- **Ad-hoc Network** - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode.
- **Beacon Interval** - A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).
- **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)** - In local area networking, this is the CSMA technique that combines slotted time-division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.
- **Default Gateway** - The routing device used to forward all traffic that is not addressed to a station within the local subnet.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. DHCP supports static addresses for computers containing Web servers that need a permanent IP address.
- **BSS (Basic Service Set)** - An infrastructure network connecting wireless devices to a wired network using a single access point.
- **Dynamic IP Address** - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such

as servers and printers, are usually assigned static IP addresses.

- **Encryption** - A security method that applies a specific algorithm to data inorder to alter the data's appearance and prevent other devices from reading the information.
- **ESS (Extended Service Set)** - A set of more than two or more BSSs (multiple access points) forming a single network.
- **DNS** - The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.
- **DSSS (Direct-Sequence Spread Spectrum)** - DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN end-point), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).
- **DTIM (Delivery Traffic Indication Message)** - A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages
- **Fragmentation** - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
- **Gateway** - A device that interconnects networks with different, incompatible communications protocols.
- **Infrastructure Network** - An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infra-structure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.
- **MAC (Media Access Control) Address** - A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.
- **NAT (Network Address Translation)** - The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.
- **Ping (Packet INternet Groper)** - An Internet utility used to determine whether a particular IP

address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.
- **PPTP (Point-to-Point Tunneling Protocol)** - A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network.
- **Roaming** - In an infrastructure mode wireless network, this refers to the ability to move out of one access point's range and into another and transparently re-associate and re-authenticate to the new access point. This re-association and re-authentication should occur without user intervention and ideally without interruption to network connectivity. A typical scenario would be a location with multiple access points, where users can physically relocate from one area to another and easily maintain connectivity.
- **RTS (Request To Send)** - An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.
- **SNMP (Simple Network Management Protocol)** - A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the net-work. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).
- **Spread Spectrum** - Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).
- **SSID (Service Set IDentifier)** - A unique name shared among all points in a wireless network. The SSID must be identical for each point in the wireless net-work and is case-sensitive.

- **Static IP Address** - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.
- **TCP (Transmission Control Protocol)** - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.
- **TCP/IP (Transmission Control Protocol/Internet Protocol)** - The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.
- **Telnet** - A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.
- **TFTP (Trivial File Transfer Protocol)** - A version of the TCP/IP FTP protocol that has no directory or password capability.
- **Throughput** - The amount of data moved successfully from one place to another in a given time period.
- **UDP (User Datagram Protocol)** - A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram)between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64- bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **WINIPCFG** - Configuration utility based on the Win32 API for querying, defining and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

Appendix B Specification

Feature	Benefit
Up to 23dBm(200mW) RF Output Power (depends on different countries)	9 times coverage of regular wireless Router
11Mbps IEEE 802.11 b Compliant	Fully interoperable with IEEE 802.11 b compliant products
Three built-in 10/100Mbps Switch Ports	Scalability, able to extend your network
NAT/PAT support	Shares single Internet account and providing a natural firewall
TCP/IP/UDP/Port/MAC address filtering	Firewall functions ensure secure network connection
Virtual Server Mapping	Allows some of computers in wireless LAN network to be accessible from outside network
IP Sec Pass through / PPTP	Provides special pass-through support for common VPN implementations
64 /128-bit WEP data encryption	Powerful data security
DHCP client/server/relay	Simplifies network administration, the software keeps track of IP addresses rather than administrators to manage the task
SNMP/Telnet/Web configuration	Helps administrators to remotely configure or manage the Router via SNMP/Telnet/Web browser
PPPoE	Dial-Up connects the users to the Internet through a shared DSL/Cable modem
Seamless Roaming	Allows users to travel between Routers without losing their network connection

General	
Data Transfer Rate	11, 5.5, 2 and 1 Mbps, Auto Fall-Back
Frequency Band	2.400～2.484 GHz
Range (open environment)	11 Mbps –300m/450m (23 dBm output power) 5.5 Mbps –400m/600m (23 dBm output power) 2 Mbps – 500m/750m (23 dBm output power) 1 Mbps –800m/1200m (23 dBm output power)
Radio Type	Direct Sequence Spread Spectrum (DSSS)
Operation Channels	11 for North America, 14 for Japan, 13 for Europe, 2 for Spain, 4 for France
Modulation	CCK(11 Mbps / 5.5 Mbps), DQPSK(2 Mbps), DBPSK (1Mbps)
Antenna	High sensitivity diversity antenna
RF Output Power	23dBm(200mW)--FCC 20dBm(100mW)--CE
Security	64/128-bit WEP data encryption, hide SSID in beacons, stations can not use “any” SSID
Compatibility	IEEE 802.11b compliant
Regulation Certifications	FCC Part 15/UL, ETSI 300/328/CE
Network	
Interface	One 10/100Mbps RJ-45 for DSL/Cable modem Three 10/100Mbps RJ-45 Switch Port
Firewall	- NAT/PAT - TCP/IP/UDP/Port/MAC address filtering - Virtual server mapping
Dial-up connection	PPPoE
VPN Support	IP Sec pass-through / PPTP
Management	Telnet/Web/SNMP(v1/v2, 802.11MIB) configuration

Firmware Upgrade	Upgrade firmware via TFTP/Web-based
Environment	
Temperature Range	0 to 55° C (32 °F to 131 °F) - Operating, -20 to 80 ° C(-4 °F to 176 °F) - Storage
Humidity (non-condensing)	5%～95% typical
Physical	
Dimensions	145(L)mm x 210(W)mm x 40(H)mm 5.7(L)in x 8.3(W)in x 1.6(H)in
Weight	500g(1.1 lb)