

Wireless Access Point

User Guide

Contents

1.	<u>Overview -----3</u>
1.1	<u>Feature and Benefits -----5</u>
1.2	<u>Applications -----6</u>
1.3	<u>Network Configurations -----6</u>
2.	<u>Hardware Configuration ----- 11</u>
2.1	<u>Hardware Configuration ----- 11</u>
2.2	<u>Hard ware Installation ----- 11</u>
3.	<u>Initial Software Installation and Configuration ----- 12</u>
4.	<u>Configuring the Access Point through Web Brower -- 15</u>
4.1	<u>System Setting----- 17</u>
4.1.1	<u>System Time----- 18</u>
4.1.2	<u>Administrator Setting ----- 19</u>
4.1.3	<u>Firmware Upgrade ----- 20</u>
4.1.4	<u>Configuration Tools ----- 23</u>
4.1.5	<u>Status----- 25</u>
4.1.6	<u>Reset----- 26</u>
4.2	<u>LAN Setting ----- 27</u>
4.2.1	<u>LAN Settings ----- 28</u>
4.2.2	<u>DHCP Client List ----- 29</u>
4.2.3	<u>DNS Settings ----- 30</u>
4.3	<u>Filtering Setting ----- 31</u>
4.3.1	<u>MAC Filtering----- 31</u>
4.3.2	<u>IP Filtering----- 32</u>

4.4	<u>Wireless Setting-----</u>	<u>33</u>
4.4.1	<u>General-----</u>	<u>33</u>
4.4.2	<u>802.1X-----</u>	<u>36</u>
4.4.3	<u>Enhanced Features-----</u>	<u>39</u>
4.4.4	<u>Associated Clients-----</u>	<u>41</u>
4.5	<u>SNMP-----</u>	<u>41</u>
4.5.1	<u>SNMP Community-----</u>	<u>42</u>
4.5.2	<u>SNMP Trap-----</u>	<u>43</u>
5.	<u>Configuring the Access Point through Telnet-----</u>	<u>45</u>
5.1	<u>Enter the Telnet session-----</u>	<u>45</u>
5.2	<u>Command Line Interface list-----</u>	<u>47</u>
5.3	<u>Command Line for Telnet daemon-----</u>	<u>48</u>
5.4	<u>Configuring Wireless LAN through Telnet-----</u>	<u>63</u>
5.5	<u>Configuring LAN through Telnet-----</u>	<u>74</u>
5.6	<u>Configuring System through Telnet-----</u>	<u>78</u>
5.7	<u>Configuring Filtering through Telnet-----</u>	<u>86</u>
5.8	<u>Configuring SNMP x through Telnet-----</u>	<u>92</u>
5.9	<u>Configuring 802.1x through Telnet-----</u>	<u>95</u>
5.10	<u>Upgrading Firmware through Telnet-----</u>	<u>100</u>
6.	<u>The Changed History-----</u>	<u>104</u>

1. Overview

The Wireless Access Point is 11Mbps (802.11b) wireless networking in homes, businesses, and public wireless hotspots around anywhere.

The Access Point can serve as a DHCP Server, Load Balance function, Watch Dog, 802.1x technology to protect against Internet intruders. Besides, it can be configured to filter internal users' access to the Internet. The configuration uses the web browser-based configuration management system. More features and benefits are shown as below:

1-1 Features and Benefits

Feature	Benefit
Up to 23dBm(200mW) RF Output Power (depends on different countries)	9 times coverage of regular Access Point
11Mbps IEEE 802.11b Compliant	Fully interoperable with IEEE 802.11b compliant products
IEEE802.1x/RADIUS Client	Provide mutual authentication

(EAP-MD5/TLS/TTLS) Support	(Client and Server Site) and dynamic encryption keys to enhance security
Power Over Ethernet(POE)	Supplying power to a wireless advanced AP over an Ethernet cable
TCP/IP/UDP/Port/MAC address filtering	Firewall functions ensure secure network connection
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

1-2 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LAN.

1. Difficult-to-wire environments

There are many situations where wires cannot or cannot easily be laid. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

2. Temporary workgroups

Consider situations in parks, athletic arenas, exhibitions, disaster-recovery, temporary office and construction sites where one wants a temporary WLAN established and removed.

3. The ability to access real-time information

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

4. Frequently changed environments

The show rooms, meeting rooms, retail stores, and manufacturing sites are where the workplace is frequently rearranged.

5. Small Office and Home Office (SOHO) networks

SOHO users need a cost-effective, easy and quick installation of a small network.

6. Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

7. Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

8. Training/Educational Facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1-3 Network Configurations

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN products network configurations. The wireless LAN products can be configured as:

1. Ad-hoc (peer-to-peer) for departmental or SOHO LANs.
2. Infrastructure for enterprise LANs.
3. IP Sharing for 56K/ISDN TA/Cable/DSL Modem – Connect Internet and your SOHO network.

Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration that several computers equipped with the PC cards that form a wireless network whenever they are within range of one another (**Figure 1-2**). In ad-hoc mode, each client is linked peer-to-peer and would only have access to the resources of the other client, this requires no access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.

Peer to Peer

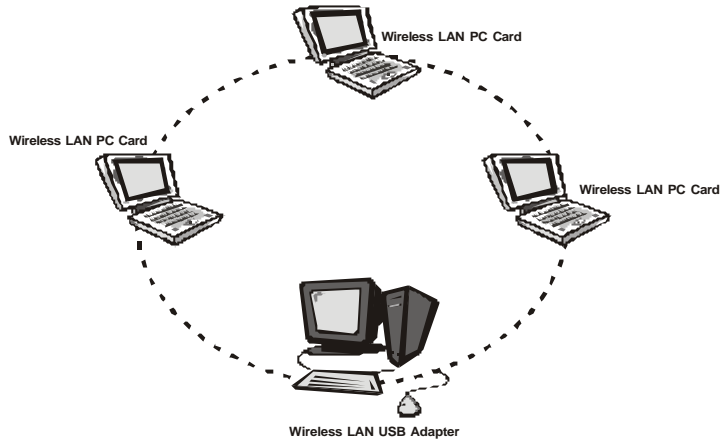


Figure 1-2 A wireless ad-hoc network

Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP whether the AP is wired to an Ethernet network or stands alone. If used as a stand-alone, the AP can extend the range of independent wireless LANs by acting a repeater, which effectively doubles the distance between wireless stations

If wired to an Ethernet network, the AP serves as a bridge and provides the link between the server and the wireless clients. The wireless clients can move freely throughout the coverage area of the AP while remaining connected to the server. Since the AP is connected to the wired network, each client would have access to server resources as well as to other clients.

In a very large facility such as an enterprise, a warehouse, or on a college campus, it will probably be necessary to install more than one access point to cover an entire building or campus. In this scenario, access points hand the client off from one to

another in a way that is invisible to the client, ensuring unbroken connectivity. Wireless clients can roam seamlessly between different coverage areas and remain connected to the network.

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.

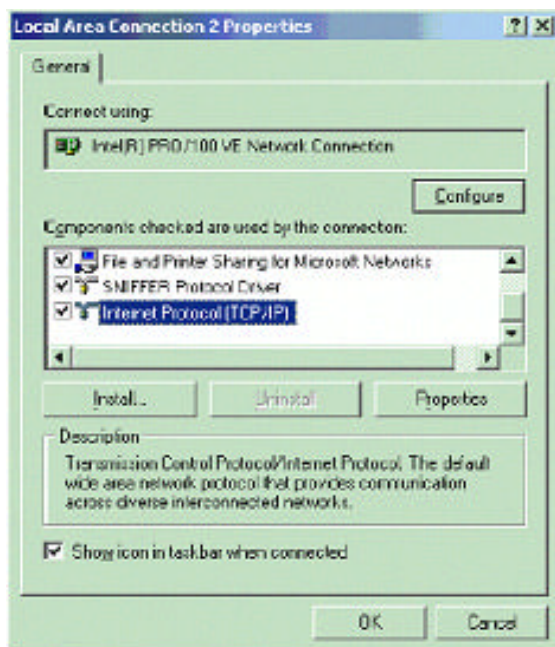
2.2 Hardware Installation

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.

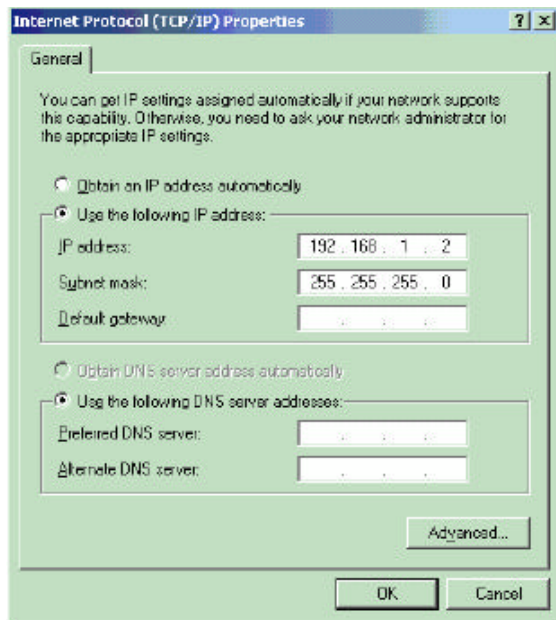
3 Initial Software Installation and

Configuration

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.

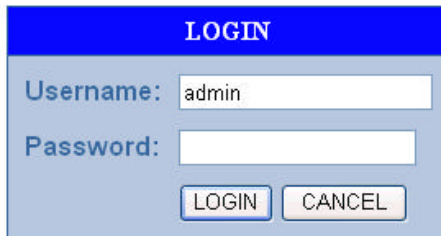
Note: the default channel is 6.



4 Configuring the Access Point through Web Browser

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.



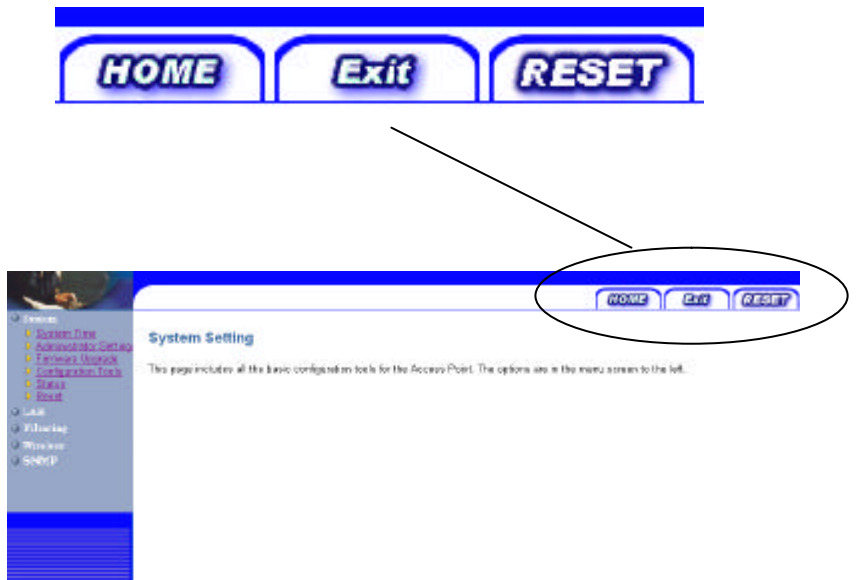
The image shows a web browser login interface. At the top, there is a blue header with the word "LOGIN" in white capital letters. Below the header, the page has a light blue background. There are two input fields: "Username:" followed by a text box containing the word "admin", and "Password:" followed by an empty text box. At the bottom of the form, there are two buttons: "LOGIN" and "CANCEL", both with a light blue background and a thin border.

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

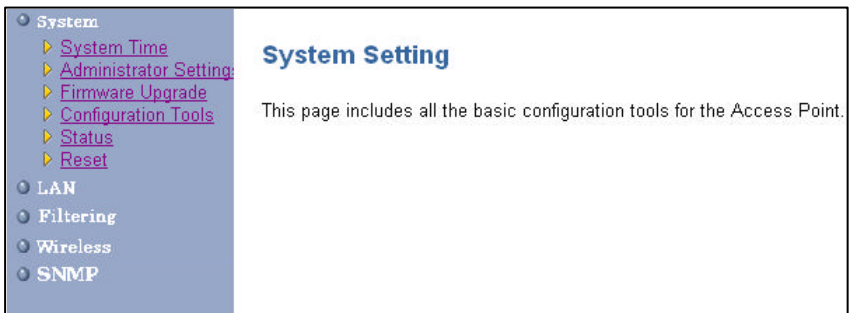
descriptions and explanations. To clear any values you've entered on any page, click **CANCEL** and re-enter information.

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.



4.1 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.



The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu is a vertical list of items, each preceded by a small circular icon. The 'System' item is selected and highlighted in a light blue background. Underneath 'System', there are five sub-items, each preceded by a right-pointing triangle icon: 'System Time', 'Administrator Setting', 'Firmware Upgrade', 'Configuration Tools', and 'Reset'. Below these are four other main menu items: 'LAN', 'Filtering', 'Wireless', and 'SNMP'. The main content area on the right has a blue heading 'System Setting' and a paragraph of text below it.

- System
 - System Time
 - Administrator Setting
 - Firmware Upgrade
 - Configuration Tools
 - Status
 - Reset
- LAN
- Filtering
- Wireless
- SNMP

System Setting

This page includes all the basic configuration tools for the Access Point.

4.1.1 System Time




Connecting to a Simple Network Time Protocol (SNTP) server allows the AP to synchronize the system clock to the global internet. The synchronizes 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.

Time	
Local date & time	Thu Jan 1 00:01:16 1970
Time Zone setting	
Set Time Zone	(GMT-06:00) Central Time (US & Canada) ▼
Daylight Saving	<input checked="" type="checkbox"/>
Start from	APR ▼ 1 ▼
End by	NOV ▼ 1 ▼
SNTP Setting	
Status	Enable ▼
Polling time	86400 (sec)
SNTP Server 1's IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
SNTP Server 2's IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
SNTP Server 3's IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
SNTP Server 4's IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

4.1.2 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.

Administrator Settings	
Password Settings	
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.	
Current Password	<input type="password" value="•••••"/>
Password	<input type="password" value="•••••"/>
Re-type password	<input type="password" value="•••••"/> (3-12 Characters)
Idle Time Out	<input type="text" value="10"/> Min (Idle Time =0 : No Time Out)
Remote Management	
Enable	<input type="checkbox"/>
IP address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

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.

4.1.3 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.



Firmware information	
Current Firmware Version:	V 1.00.3661
Firmware Date:	2002.11.28
Method	
1. Using TFTP	
2. Using WEB	

- **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.

Firmware Update -TFTP

Firmware information	
Current Firmware Version:	V 1.00.4003
Firmware Date:	2002.12.12
Method	
TFTP to a TFTP server	
TFTP Server IP:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="20"/>
Filename:	<input type="text" value="application.dff"/>





- **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.

Firmware Update - Using WEB

Firmware information	
Current Firmware Version:	V 1.00.4003
Firmware Date:	2002.12.12
Method	
Use browser	
File	<input type="text" value="C:\application.dif"/> <input type="button" value="Browse"/>

4.1.4 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 then click **APPLY**.

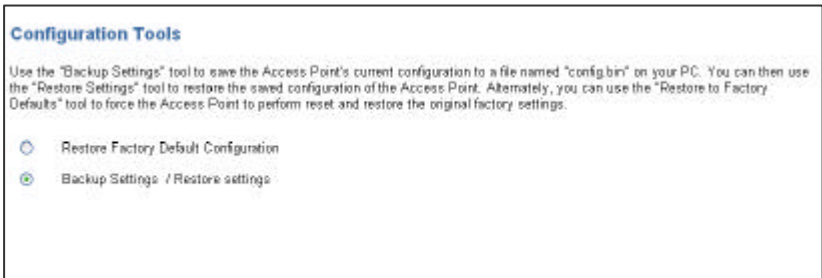


- (2) Click **Restore** button to force the Access Point to perform reset and restore the original factory settings.



- **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.

Configuration Tools

Backup Settings
Please press the "Backup Settings" button to save the configuration data to your PC.

Restore Settings
Enter the path and name of the backup file then press the "Restore Settings" button below. You will be prompted to confirm the backup restoration.



4.1.5 Status

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

Status	
LAN	
IP	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
MAC Address	00-02-4E-09-08-07
DHCP	0.0.0.0
Connected DHCP Clients	4
Wireless	
SSID	wireless
Channel	6
WEP Security	Disabled
Authentication type	None
System Information	
System Up time	01:25:30
Local time	Thu Jan 1 01:25:30 1970
GMT time	Thu Jan 1 07:25:30 1970 : (GMT+6)
Current Firmware Version	V 1.00.3661
Firmware Date	2002.11.26
Hardware Version	100
Serial Number	1234
Others	
Power level	Max(Original)

For LAN, it displays AP's IP address, MAC address, Subnet Mask, and Gateway. 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 Authentication type.

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.

4.1.6 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 completes when the power light stops blinking.

Reset Access Point

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 be complete when the power light stops blinking.

Reset



4.2 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.

A screenshot of a web interface showing a navigation menu on the left and a main content area on the right. The menu includes "System", "LAN", "Filtering", "Wireless", and "SNMP". Under "LAN", there are sub-links for "LAN Settings", "DHCP Client List", and "DNS Settings". The "LAN" sub-link is highlighted. The main content area has the heading "LAN" and the text: "The Access Point must have an IP address for the local network. You can also enable DHCP for your clients, or configure filtering functions based on specific clients or protocols."/>

System

LAN

- LAN Settings
- DHCP Client List
- DNS Settings

Filtering

Wireless

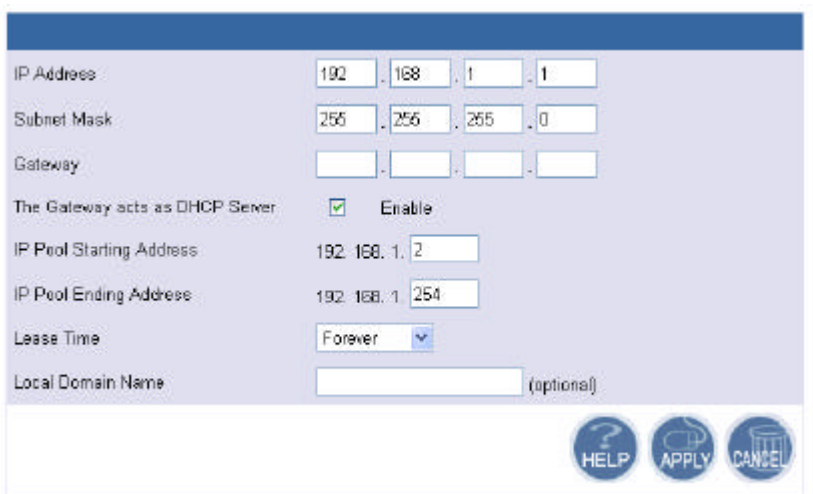
SNMP

LAN

The Access Point must have an IP address for the local network. You can also enable DHCP for your clients, or configure filtering functions based on specific clients or protocols.

4.2.1 LAN Settings

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



IP Address	192	.	168	.	1	.	1
Subnet Mask	255	.	255	.	255	.	0
Gateway		.		.		.	
The Gateway acts as DHCP Server	<input checked="" type="checkbox"/>	Enable					
IP Pool Starting Address	192	.	168	.	1	.	2
IP Pool Ending Address	192	.	168	.	1	.	254
Lease Time	Forever <input type="button" value="v"/>						
Local Domain Name	<input type="text"/> (optional)						

HELP APPLY CANCEL

- (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) Gateway: It indicated the Network's Gateway. It's optional.
- (4) The Gateway acts as the DHCP Server: By default, the AP can function as a DHCP server. The AP can automatically assign an IP address to a client. To disable this function, clear the "Enable" check box.
- (5) IP Pool Starting Address & IP Pool Ending Address: The first and the last address in the IP address pool.
- (6) Lease Time: The period client can have the IP address assigned by DHCP server.
- (7) Local Domain Name: It's optional.

4.2.2 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.

Note: The DHCP server only serves wireless clients. So LAN users cannot get IP address through DHCP server.

DHCP Client List

The DHCP client list allows you to see which clients are connected to the Access Point via IP address, host name, and MAC

IP Address	Host Name	MAC Address
192.168.1.5		00-02-6F-8E-F0-E8
192.168.1.3		00-02-6F-01-6E-C5
192.168.1.4		00-02-6F-01-6E-C6
192.168.1.2		00-02-6F-01-4D-84
192.168.1.7		00-02-6F-12-34-56

Refresh

HELP

4.2.3 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.

DNS Settings

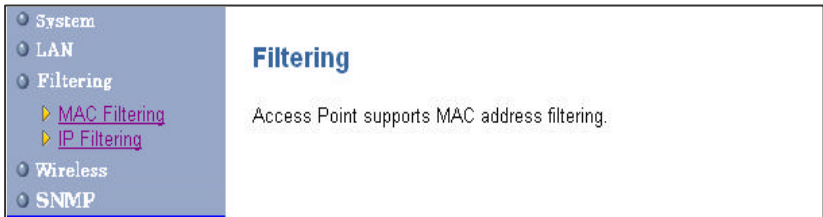
Domain Name Server (DNS) Address:

Secondary DNS Address (optional):

HELP APPLY CANCEL

4.3 Filtering Setting

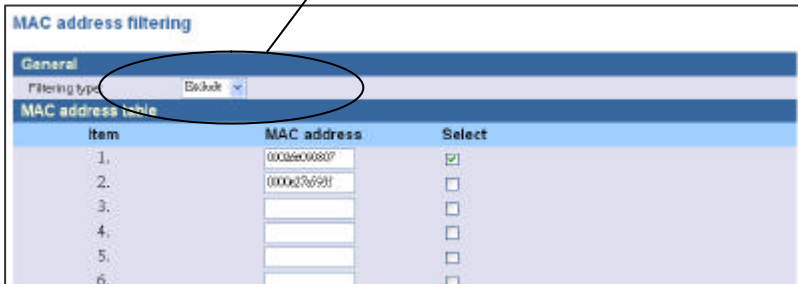
The Access Point provides filtering function via MAC address or IP address for wireless interface.



4.3.1 MAC Filtering

The maximum number of items is 64. Check the **select** check box to include or exclude corresponding items. The 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 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.

There are three filtering type: Include, Exclude, and Disable



4.3.2 IP 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.

	IP	Port	Type	Block Time	Day	Time	Enable
1.	192.168.1.20 - 25	80 - 80	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="radio"/> Always <input checked="" type="radio"/> Block	MON WED	0:00am 11:00pm	<input checked="" type="checkbox"/>
2.	192.168.1. -	-	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="radio"/> Always <input type="radio"/> Block	~	~	<input type="checkbox"/>
3.	192.168.1. -	-	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="radio"/> Always <input type="radio"/> Block	~	~	<input type="checkbox"/>
4.	192.168.1. -	-	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="radio"/> Always <input type="radio"/> Block	~	~	<input type="checkbox"/>
5.	192.168.1. -	-	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input checked="" type="radio"/> Always <input type="radio"/> Block	~	~	<input type="checkbox"/>

4.4 Wireless Setting

- System
- LAN
- Filtering
- Wireless
 - [General](#)
 - [Enhanced](#)
 - [Associated clients](#)
- SNMP

Wireless

You can set the wireless related setting here.

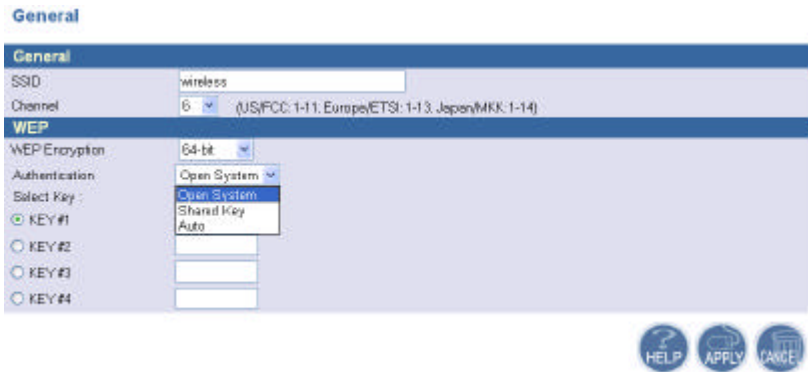
4.4.1 General

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.

Select "Disable" to disable WEP



- (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.



- (3) **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.

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.

4.4.2 802.1X

The 802.1X standard is designed to enhance the security of wireless local area networks that follow the IEEE 802.11 standard. 802.1X uses an existing protocol, the Extensible Authentication Protocol (EAP) for message exchange during the authentication process.

In a wireless LAN with 802.1X, a user requests access to an access point (known as the *authenticator*). The access point forces the user into an unauthorized state that allows the client to send only an EAP-start message. The AP replies with an EAP-request identify message to obtain the clients identity. The clients EAP-response packet containing the clients identity is forwarded to the authentication server. The authentication server is configured to authenticate clients with a specific authentication algorithm. The result is an accept or reject packet from authentication server to AP. Once authenticated, the AP opens the client's port and traffic will be forwarded.

802.1x

General	
Authentication type	NONE (NONE: disable 802.1x)
Reauthentication Time	seconds
Radius Server	
Primary Radius Server:	
IP Address:	192 . 170 . 1 . 1 Port: 1812 Shared Secret: hello
Backup Radius Server (Optional):	
IP Address:	192 . 170 . 1 . 66 Port: 1813 Shared Secret:
Dynamic WEP keys	
Enable	<input type="checkbox"/> Use Dynamic WEP Keys (Valid Only if Authentication is EAP-TLS or EAP-TTLS)
Rekeying Time:	100 seconds



(1)General:

1. **Authentication type:** There are three EAP (Extensible Authentication Protocol) types supported. You can choose between EAP-TLS⁴, EAP-MD5⁵, and EAP -TTLS⁶. You can choose NONE to disable the 802.1X.

⁴ TLS- Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

⁵ MD5- provides basic security and is analogous to the challenge handshake authentication protocol (CHAP). MD5 is intended for use with signal signature applications, which require that large files must be compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.

⁶ TTLS- provides mutual authentication, supports legacy password protocols and does not require clients to have certificates. As a result, enterprises can reduce the costs associated with operating a certificate authority to distribute and revoke user certificates.

2. **Reauthentication time:** The time period that AP informs clients to re-authenticate.

(2)Radius Server:

1. **Primary Radius Server:** The IP address and port number of Primary Radius Server. You need to know the shared secret between AP and Radius Server. The default port number is 1812.
2. **Backup Radius Server:** The IP address, shared secret, and port number of backup Radius Server. It is optional.

(3)Dynamic WEP keys:

1. **Enable:** Check the Enable box to enable using dynamic WEP keys. This function only valid if authentication type is EAP-TLS or EAP-TTLS.
2. **Re-keying Time:** The time period that AP informs clients to change the WEP key.

Note: After enabling the dynamic WEP key function , the default WEP key will change to 3 and the authentication type for WEP will automatically change to Open System.

4.4.3 Enhanced Features

Wireless Enhanced Features

Enhanced Security	
Hide SSID name in Beacon frame	<input checked="" type="checkbox"/>
Block Responds to "Unspecified-SSID"	<input checked="" type="checkbox"/>
Wireless Client Isolation	<input type="checkbox"/>
Power Control	
Power Level	MAX(original) ▾
802.11 Enhancement	
Fragment Threshold	2345
Rts Threshold	2432
Beacon Period	100
Load Balance	
Maximum number of users	280
AP Link Completeness	
Enable	<input type="checkbox"/>

(1) 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.

(2) **Power Control:** If you select MAX(Original), then the power

is the same as the network card's power.

(3) **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

(4) **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.

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

4.4.4 Associated Clients

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

Associated Clients

MAC address table	
Item	MAC address <input type="button" value="Refresh"/>
1	00026301c034



4.5 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.

4.5.1 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.

SNMP Community

SNMP			
Enable	<input checked="" type="checkbox"/>		
Item	Access Right	Community	Validity
1	READ	public	<input checked="" type="checkbox"/>
2	DENY	private	<input checked="" type="checkbox"/>
3	READ		<input checked="" type="checkbox"/>
	WRITE		<input checked="" type="checkbox"/>
	CREATE		<input checked="" type="checkbox"/>
4	DENY		<input checked="" type="checkbox"/>
5	DENY		<input checked="" type="checkbox"/>

HELP APPLY CANCEL

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 (Deny⁷/Read⁸/Write⁹).

Community: Specify the name of community for the SNMP manager(Private/Public). By convention, "Public" community is with a read-only access right.

4.5.2 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.

SNMP Trap

Item	Version	IP Address				Community
1	Version 1	152	169	1	2	public
2	Disable					
3	Version 1					
	Version 2					
4	Disable					
5	Disable					

HELP APPLY CANCEL

⁷ Deny community will not allow a remote device to read information from a device or to modify settings on that device.

⁸ Read-only community enables a remote device to retrieve "read-only" information from a device.

⁹ Read-Write community allows a remote device to read information from a device and to modify settings on that device.

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 type of community (public/Private) for SNMP manager.

Following are the traps supported in the access point:

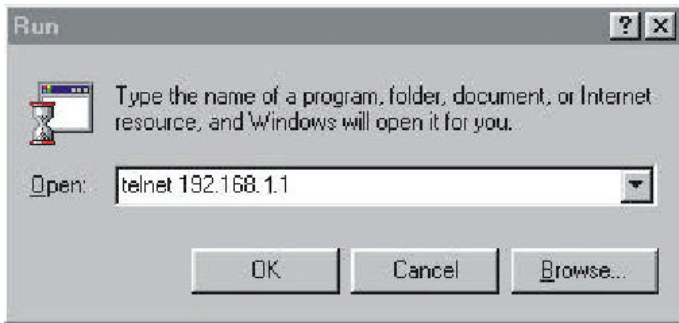
Cold-start trap:

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.

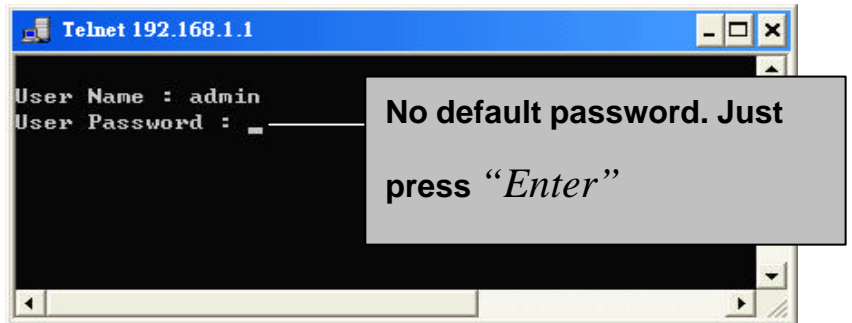
5 Configuring the Access Point through Telnet

5.1 Enter the Telnet session

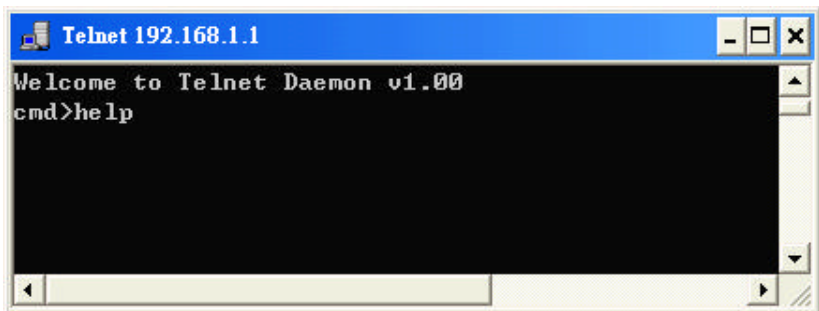
3. Click **Start** button, select **Run** to open the Run dialog box as shown below. Enter telnet **192.168.1.1** (default IP address of AP is 192.168.1.1) in the Open field. Then click **OK** button.



4. 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).



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



5.2 Command Line Interface list

CLI	Description	Usage
time	Get current system time	time
settime	Set system time	settime <hh:mm:ss> [yy/mm/dd] [TZ (GMT +/- hour)]
help	List all commands	help
ifShow	Display network interface	ifShow <ifname>
ipConfig	Configure interface address and subnet mask	ipConfig [ifname] [ip] [subnet mask]
ping	Ping a host...	ping [ip]
routeShow	Show Route	routeShow
dhcpsStart	Start DHCP Server	dhcpsStart
dhcpsStop	Stop DHCP Server	dhcpsStop
exit	Exit this telnet session	exit
wlanShow	Show the WLAN config	wlanshow
reset	Reset the system	reset
wlanSet	Configure the wireless part	Wlanset ACTION [arg1], [agr2],...
status	Show the AP status	status
sysSet	Change the System Configuration	sysSet ACTION [arg1], [agr2],...
lanShow	Show the LAN setting	lanShow
lanSet	Change the LAN Configuration	lanSet
filterShow	Show the Filter setting	filterShow
filterSet	Change the Filter setting	filterSet
snmpShow	Show the SNMP setting	snmpShow
snmpSet	Change the SNMP setting	snmpSet

5.3 Command Line for Telnet daemon

2. “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>
```

3. 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 0xfffff00 Subnetmask 0xfffff00

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>

4. “ipConfig” command is used to configure interface address and subnet mask.

Usage: ipConfig [ifname] [ip] [subnetMask]

```
Welcome to Telnet Daemon v1.00
cmd>ipConfig adm0 192.168.1.50 255.255.255.0
cmd>
```

Interface name

IP address of interface

Subnet Mask

5. “ping” command is used to ping a host.

Usage: ping [IP address]

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

6. “exit” command exit the telnet session. Type “exit” at command line prompt.

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

7. “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: 00000000000000000000000000000000
Key 2: 00000000000000000000000000000000
Key 3: 00000000000000000000000000000000
Key 4: 00000000000000000000000000000000
--- 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
----- LAN -----
IP: 192.168.1.98
Subnet Mask: 255.255.255.0
Gateway: 0.20.247.208
LAN MAC Address: 00:01:02:03:04:10
Connected DHCP Clients: 1
----- Wireless -----
SSID: [(null)]
Channel: 6
Authentication type: None
Wireless MAC Address: 00:02:6f:01:c0:3dWireless MAC
Address:
```

----- System Information -----

System Up time: 01:26:55

Local time: Thu Jan 1 01:26:55 1970

GMT time: Wed Dec 31 17:26:55 1969

Current Firmware Version: [1.00.4455]

Firmware Date: [2003.01.06]

Hardware Version: [1]

Serial Number: [0000011118]

cmd>

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>
```

1. "lanShow" command shows the LAN configuration and DHCP configuration, including IP address, Subnet Mask, DHCP status, and IP pool information.

```
cmd>lanShow
----- LAN configuration -----
IP Address: 192.168.1.98
Subnet Mask: 255.255.255.0
Gateway: 0.0.0.0
DHCP Server: Enabled
IP Pool Starting Address: 192.168.1.2
IP Pool Ending Address: 192.168.1.254
Lease Time: One hour
Local Domain Name:
----- DHCP configuration -----
Item   IP           MAC Address   Host name
  1    192.168.1.2  00:02:6f:01:c0:3e  wlan-w2k
cmd>
```

14. "filterShow" displays the MAC address filtering table, filtering type, and the information of IP filtering.

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

----- MAC control list -----
Filtering type: Disabled (Any station can access)
Item   MAC                Select
-----
1      00:02:6f:01:c0:3f   Selected
2      00:00:00:00:00:00   Unselect
3      00:00:00:00:00:00   Unselect
4      00:00:00:00:00:00   Unselect
.....
.....
.....

----- IP Filter Configuration -----
-----
          IP          Port Type  Block  Day      Time
192.168.3.0- 0    0- 0  TCP  Always  N/A- N/A  N/A- N/A
Disable
192.168.3.0- 0    0- 0  TCP  Always  N/A- N/A  N/A- N/A
Disable
```

```
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
192.168.3.0- 0 0- 0 TCP Always N/A- N/A N/A- N/A
Disable
cmd>
```

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
4	DENY		Enable
5	DENY		Enable

----- SNMP Trap info -----

Item	Version	IP	Community
1	version 1	192.168.1.2	public
2	disable		
3	disable		
4	disable		
5	disable		

Version of SNMP

**IP address for
SNMP Trap report**

5.4 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]
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 [default key id]
beacon	Change the beacon Period [0-4095ms]	wlanSet beacon [beacon period]

ACTION	Description	Usage
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 isolate [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]

ACTION	Description	Usage
aplink	Change the AP Link Completeness: 0:disable, 1:enable	wlanSet amlink [0 1]
authalgo	Change Authentication algorithm: 1:Open system, 2: Shared key, 3:Auto	wlanSet authalgo [1 2 3]

1. The “ssid” action can change the SSID

New 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 [New 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. The “beacon” action can change the beacon period.
Beacon Period: Default is 100 ms. The maximum is 4095.

Usage: wlanSet beacon [New beacon period]

```
cmd>wlanSet beacon 3000  
Old Beacon Period: 100  
New Beacon Period (after reset): 3000  
(Please remember to reset the Access Point if you made any change).
```

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

```
cmd>wlanSet maxass 20  
Old Maximum Associated Stations: 250  
New Maximum Associated 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]

If plug off the cable of LAN interface,

```
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 amlink [0|1]

```
cmd>wlanSet amlink 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).
```

```
cmd>
```

5.5 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
ip	Change the LANs IP and mask	LanSet ip [IP] [mask]
gateway	Change the AP IP, mask, Gateway, DHCP	lanSet gateway [gateway]
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 “gateway” action can set the network's gateway.

Usage: lanSet gateway [gateway IP]

Example:

```
cmd>lanSet gateway 192.168.3.47
Change gateway success.
(Please remember to reset the Access Point if you made any change).
cmd>
```

3. 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>
```

5.6 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]

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

1. 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>
```

2. 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>
```

3. 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>
```

6. 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 succeeded
(Please remember to reset the Access Point if you made any change).
cmd>
```

7. 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.

8. The “reset” action can reboot the system and refresh the AP’s connection.

Usage: sysSet reset

9. The “sntp” action can change the SNTP polling 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).
```

10. The “sntp” action can change SNTP function and set SNTP server.

Usage: sntp [0|1] [IP]

0: Disable

1: Enable

Example:

```
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
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).
```

11. 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>
```

5.7 Configuring Filtering through Telnet

The command “filterSet” can change the settings of MAC filtering and IP filtering. Type “filterSet” and the action you want to perform. You need to know actions for filter setting.

Usage: filterSet [ACTION] [arg1][arg2]

ACTION	Description	Usage
macshow	Show the MAC filtering setting.	filterSet macshow
mac	Change the MAC address filtering.	filterSet mac
ip	Show the IP filtering setting.	filterSet ip
ipdaytime	Change the daytime part	filterSet ipdaytime
ipstatus	Enable or Disable the IP filtering function.	filterSet ipstatus

1. The “macshow” action shows the filtering type and MAC address table of MAC filtering.

Usage: filterSet macshow

```
cmd>filterSet macshow
----- MAC control list -----
Filtering type: Disabled (Any station can access)
Item      MAC                      Select
-----
1         00:02:6f:01:c0:3f        Unselect
2         00:00:00:00:00:00        Unselect
3         00:00:00:00:00:00        Unselect
4         00:00:00:00:00:00        Unselect
.....
.....
.....
```

2. “mac” action can change the settings of MAC address filtering. You can change filtering type. You can select ,unselect or clear those MAC address item.

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

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

Usage: filterSet 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>filterSet 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
```

4. The “ipdaytime” can set the day and time to block the IP address.

Usage: filterSet ipdaytime index [Start day] [End day]
[Start hour] [End hour]

Example: filterSet 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

5. The “ipstatus” action can enable and disable the IP filtering function.

Usage: filterSet ipstatus [index] [status]

Example: filterSet 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.

5.8 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).
```

5.9 Configuring 802.1x through Telnet

The command “8021xSet” can change the settings of 802.1x. Type “8021xSet” and the action you want to perform. You need to know actions for 802.1x setting.

Usage: 802.1xSet [ACTION] [arg1] [arg2]

ACTION	Description	Usage
authtype	Change 802.1x authentication type.	8021xSet authtype [none md5 tls ttls]
authtime	Change 802.1x authentication time.	8021xSet authtime [time]time: 100 ~ 255
rekeytime	Change 802.1x dynamic WEP key re-key time.	8021xSet rekeytime [time] time: 100...
dymkey	Change 802.1x dynamic WEP status	8021xSet dymkey [0 1]0:disable, 1:enable
primrad	Change the Primary Radius Server setting.	8021xSet primrad [IP] [Port] [Shared secret]
secrad	Change the Secondary Radius Server setting.	8021xSet secrad [IP] [Port] [Shared secret]

1. The “authtype” action can change the type of EAP.

Usage: 8021xSet authtype [none|md5|tls|ttls]

none: disable the 802.1x function

md5: EAP-MD5

tls: EAP-TLS

ttls: EAP-TTLS

```
cmd>8021xSet authtype md5
```

```
Current Authentication type is EAP_TLS
```

```
Warning: Since 802.1x dynamic key can only be used with TLS or TTLS,  
the dynamic key setting is set to disabled
```

```
New Current Authentication type is EAP_MD5
```

```
(Please remember to reset the Access Point if you made any change).
```

Note: If you choose MD5 or NONE with dynamic WEP key enabled, the dynamic WEP key will automatically set to disable after reset.

Note: If you choose TLS or TTLS for EAP type, you will not be able to change the authentication type of WEP key to “Shared key” or “Auto”.

2. The “authtime” action can change the time period that AP informs clients to re-authenticate.

Usage: 8021xSet authtime [time]

The unit of time is second and the range is 100~255 sec

```
cmd>8021xSet authtime 200  
Old Reauthentication Time: 100(seconds)  
New Reauthentication Time(after reset): 200(seconds)  
(Please remember to reset the Access Point if you made any change).
```

3. The “rekeytime” action can change the re-key time of dynamic WEP key.

Usage: 8021xSet rekeytime [time]

The unit of re-key time is seconds and the range is equal to or bigger than 100 (seconds)

```
cmd>8021xSet rekeytime 200  
Old Dyanmic WEP key re-keying Time: 100(seconds)  
New Dyanmic WEP key re-keying Time(after reset): 200(seconds)  
(Please remember to reset the Access Point if you made any change).  
cmd>
```

4. The “dymkey” action can enable or disable the dynamic WEP key.

Usage: 8021xSet dymkey [0|1]

0: disable

1: enable

Note: If the authentication type is NONE or MD5, you will not be able to enable the dynamic WEP key.

Note: After enabling the dynamic WEP key, the authentication type of WEP key will automatically change to “Open System” and the default key will automatically change to 3.

```
cmd>8021xSet dymkey 1
```

```
Old Dyanmic WEP key status: Disabled
```

```
New Dyanmic WEP key status: Enabled
```

```
(Please remember to reset the Access Point if you made any change).
```

5. The “primrad” action can change the settings of primary Radius Server, including IP address, port number, and shared secret key.

Usage: 8021xSet primrad [IP] [Port] [Shared secret]

```
Welcome to Telnet Daemon v1.01
cmd>8021xSet primrad 192.170.1.2 1812 chair
Old: Primary Radius server IP: 192.170.1.1, Port 1812, shared secret hello
New: Primary Radius server IP: 192.170.1.2, Port 1812, shared secret chair
(Please remember to reset the Access Point if you made any change).
cmd>
```

6. The “secrad” action can change the settings of backup Radius Server.

Usage: 8021xSet secrad [IP] [Port] [Shared secret]

```
Welcome to Telnet Daemon v1.01
cmd>8021xSet secrad 192.170.1.66 1813 book
Old: Secondary Radius server IP: 192.170.1.1, Port 1812, shared secret hello
New: Secondary Radius server IP: 192.170.1.66, Port 1813, shared secret
book
(Please remember to reset the Access Point if you made any change).
```

5.10 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
```

IP address of TFTP

Firmware file name

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>
```

6. The Changed History

Date	Subject/Comment	Old Version	New Version
12/16/02		N/A	V1.0
12/16/02	WEP(auto), FW upgrade through telnet	V1.0	V1.01
1/03/02	Telnet	V1.01	V1.02
1/06/03		V1.02	V1.03
1/07/03	correction	V1.03	V1.04