
User Manual

2.4GHz 802.11b/g Outdoor

Access Point – Repeater - Bridge

Professional Speed - 54Mbps

AP-2010



Revision : 1-01

Updated : 02 Oct 09

Federal Communication Commission Interference Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

Important Note

- 1) The transmitter module may not be co-located with any other transmitter or antenna.
- 2) This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Contents

1	INTRODUCTION	1
	THE PRODUCT	1
	KEY FEATURES	1
2	PACKAGE CONTENTS.....	2
	CONTENT OF PACKAGE	2
	SYSTEM REQUIREMENTS FOR CONFIGURATION	2
3	CONNECTION.....	3
4	BASIC IP NETWORKING.....	3
	WIRELESS LAN BASICS.....	4
5	GETTING STARTED.....	5
6	CONFIGURATION WIZARD.....	8
7	CONFIGURATION MENU.....	11
	SYSTEM SUMMARY > CONFIGURATION	11
	SYSTEM SUMMARY > ASSOCIATIONS.....	12
	SYSTEM SUMMARY > STATISTICS	12
	SYSTEM SUMMARY > SITE SCAN	13
	BASIC SETTING > SNTP	13
	BASIC SETTING > LAN SETTING	14
	BASIC > VLAN SETTING	15
	WIRELESS > BASIC SETTING	16
	SECURITY MODE > OPEN-SYSTEM/SHARED KEY	18
	SECURITY MODE > WPA 2-PSK	20
	WIRELESS > ADVANCE SETTING.....	21
	WIRELESS > MAC ACCESS CONTROL.....	22
	WIRELESS > BANDWIDTH CONTROL	23
	SYSTEM TOOLS > SYSTEM LOG.....	24
	SYSTEM TOOLS > SYSTEM ADMIN	25
	SYSTEM TOOLS > LICENSE KEY.....	25
	SYSTEM TOOLS > SNMP CONFIGURATION	26
	SYSTEM TOOLS > BACKUP/RESTORE SETTINGS	27
	SYSTEM TOOLS > FIRMWARE UPDATE	28
	SYSTEM TOOLS > REBOOT	29

8	ACCESS POINT MOUNTING GUIDE	29
9	VIPER QUICKSTART INSTALLATION	30
10	VIPER QUICKSTART USER GUIDE.....	31
11	TECHNICAL SUPPORT	33
11	DISCLAIMER	34

1 INTRODUCTION

The Product

The product is based on the IEEE 802.11b/g standard, which is the latest 54Mbps Wireless LAN (WLAN) standard. Having this wireless protocols in one product ensure that your investments are protected, while enabling you to enjoy the fastest Wireless LAN speed.

This product model AP-2010 could operate as either one of the following modes:

- a. Wireless LAN Access Point (AP) mode.
- b. Wireless Ethernet Bridge mode.
- c. Repeater mode.

Key Features

- Support up to four distinct SSID
- Fully compatibility with **IEEE 802.11b/g** WLAN standard
- Utilize OFDM (Orthogonal Frequency Division Multiplexing)
- With independent 802.1Q VLAN Tagging
- Operates in the 2.4GHz license-free frequency band
- Industrial grade IP67 Casing
- Power over UTP cable DC supply
- **WEP** (Wired Equivalent Privacy). A simple WLAN encryption standard to protect wireless data from sniffers.
- **WPA** (WiFi Protected Access), for AP mode only. An improved WLAN encryption standard where the secret key renew automatically at regular intervals.
 - ▶ **TKIP** (Temporal Key Integrity Protocol). A new encryption key will be generated by corporate RADIUS server when a authorized wireless adaptor/user associate with the Access Point. This encryption key renew automatically at regular intervals. This is normally used in high security enterprise networks.
 - ▶ **Pre Shared Key (WPA-PSK)**. A new key is generated each time a wireless adaptor connects to the Access Point. This normally used for home user without a RADIUS server.
- **Remote AP list** provides added security for AP mode.
- **Protocol Filters** provides security to the network
 - ▶ **IPX Filter**
 - ▶ **Wireless Isolation**. Each wireless user would not be able to see each other even though they are in the same subnet. This is to protect the privacy of each user.
 - ▶ **Broadcast Filter**

▶ Multicast Filter

- User-friendly web-based interface for managing and configuring the Access Point.
- QoS features for multimedia support - voice, video and audio.

2 PACKAGE CONTENTS



Content of Package

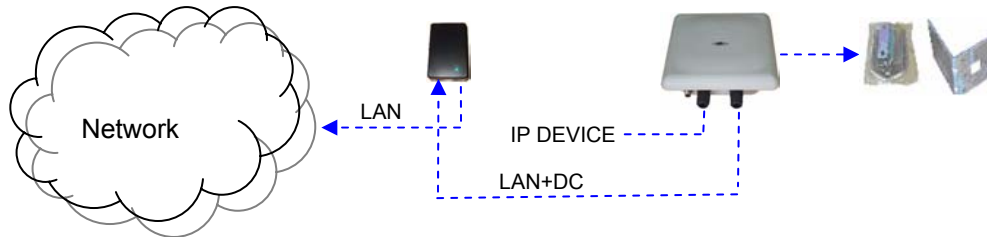
1. AP-2010
2. 48V DC combiner adaptor (Power Over Ethernet)
3. screws, washers, nuts, U-bolt
4. mounting bracket (pole)

Note: Standard package may vary with model type and country. Using a combiner adaptor with a power rating other than the one included in the package will cause serious damage to the Access Point and void the warranty for this product.

System Requirements for Configuration

- Computers with Windows, Macintosh or Linux-based operating systems and with an Ethernet adaptor
- Internet Explorer version 5.5 and above or Netscape Navigator that supports Java

3 CONNECTION



4 BASIC IP NETWORKING

IP = Internet Protocol

IP stands for Internet Protocol. In an IP network, every device has a **unique** IP Address (For example: 192.168.1.35) to identify itself. There are two ways of assigning an IP address to a PC or AP: Static and Automatic (DHCP). Static IP addresses are keyed-in manually, while Dynamic IP's are distributed by a DHCP Server.

Ports

Every packet of traffic is identified by its Source and Destination Addresses, which would ensure that the packet arrives at the correct destination. A Port Number is also embedded in each packet; to identify which software application that generated and uses that packet. Therefore, if it blocks a certain port number, it denies the particular software from using the connection.

Static IP Address

Static IP addressing ensures that the device will always have the same IP address. Static addressing is commonly used for your servers.

Dynamic IP Address

A dynamic IP address is one that is automatically assigned to a PC. These IP addresses are "dynamic" because they are only temporarily leased to the PC when it connects to the network. This is the most convenient and common way of managing IP addresses in a network. The Server that manages this pool of IP addresses is called the DHCP Server. The product has a DHCP Server built-in to simplify the network management.

DHCP (Dynamic Host Configuration Protocol)

The PC obtaining an IP address from the Server is called the DHCP Client. If there is already a DHCP Server running on your network, you must disable one of the two DHCP servers. Running more than one DHCP server together will cause network problems!

Wireless LAN Basics

A Wireless LAN (WLAN) is a computer network that transmits and receives data with radio signals instead of using cables. WLANs have become common in homes, offices, airports and public Hotspots. WLAN can support the same applications and software that run on a wired network (LAN). Besides supporting the same software and functions, WLAN brings greater convenience and eliminates the need to lay Ethernet cables in a home or office.

WLAN networking involves a few additional parameters to be configured:

SSID

The SSID is the "network name" for the WLAN network. The SSID is any name, and can be any set of characters or numbers. The Client sniffs the radio frequencies for an AP with the same SSID with itself. The client locks onto the AP and they are "**associated**".

To enable plug-and-play convenience, most client cards can sniff the frequencies to extract the available SSIDs to let the user choose from.

Encryption

WLAN traffic can be captured by anybody to be read! The solution is to use encryption to make the traffic appear as random characters to the eavesdropper. Both the AP and client must use the same encryption standard and key to enable them to decode the "rubbish". If the encryption settings are mismatched, the client and AP cannot associate. WEP (Wired Equivalent Privacy) is the most common WLAN encryption standard.

Channel

There are a total of 13 channels in the 2.4GHz band. Depending on regulation, not all the frequencies may be available in every country. Frequency is configured on the AP only. The client searches for the AP and locks it into that AP's channel.

Signal Strength

Radio signals drop in power over a distance. Even if all the settings are correct, low signal strength makes association impossible. The usable distance between the AP and client can range from a few meters indoor to a few km. When setting up the client, make sure that you:

- Keep at a distance between the AP and the clients.
- Make sure that the WLAN signals do not have to pass through too many concrete walls and metal structures to reach the client.
- Make sure that clients are located far away from one another to avoid interference.
- Make sure that there is line of sight between the AP and client device.

Interference

Interference happens when 2 clients with the same channels are placed near to one another. The speed of the network drops and the signal strength fluctuates wildly.

Roaming

Association happens when the SSID, Encryption and MAC Address Control settings are correct between the AP and client. If 2 APs with these same settings are located in the same area, the client would choose to associate to the one which gives it a better signal strength. The client would roam over to the 2nd AP when he moves nearer to it. The client switches AP and frequency as he does so.

5 GETTING STARTED

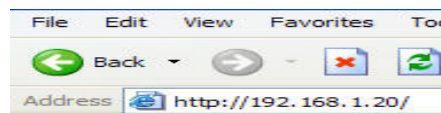
Connect the network as shown previously.



If your PC is **wireless**, check the PC's card utility to make sure that the signal strength is good.

Open a Web browser (Internet Explorer, Netscape etc.).

Type the AP LAN IP (**192.168.1.20**) address into the browser's Address field. The default LAN IP address is 192.168.1.20.



Note: If you have changed the default IP of the AP, make sure you enter the correct IP address.

Log On	
User Name:	<input type="text"/>
Password:	<input type="password"/>

- Type in **admin** for user name.
- Type in **admin** for the password
- Click on *Log In*

Note: If you have changed the default user name and password of the AP, make sure you enter the correct user name and password.

Once the login is successful, you'll see a configuration menu and a pop up window for wizard setup. The wizard is a quick guide to run you through the configuration process so as to setup your system in the shortest time. After the initial setup, you may wish to turn off the setup wizard by removing the tick on *Run This Wizard At Start*. Click on *Next* to proceed with the setup wizard.



Note: If you have pop-ups blocker installed on your computer, it may prevent the Wizard window from functioning properly.

Detailed configuration for the AP can be found at the System Summary menu. The System Summary menu consists of a navigation panel and a configuration panel. The configuration panel is a place to view the entire detailed configuration.

System Summary
Setup Wizard
Basic
Wireless
System Tools

System Summary > Configurations

LAN Settings	
LAN IP Mode	Static IP
System Name:	
IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Wireless Setting	
Wireless Mode:	Enable
SSID:	11g_1
Channel:	Current Channel 11: 2462MHz
Wireless Mode:	802.11g
Security Mode:	Disable
Authentication:	Open System
Data Rate (Mbps):	Best
Transmit Power:	Max
Preamble:	Short Preamble
Slot Time:	Short Slot Time
Wireless MAC Control:	Enable
Firmware Version	
Current Version:	M2010(S)-I00-C00-H00-V0.0.5B9P0

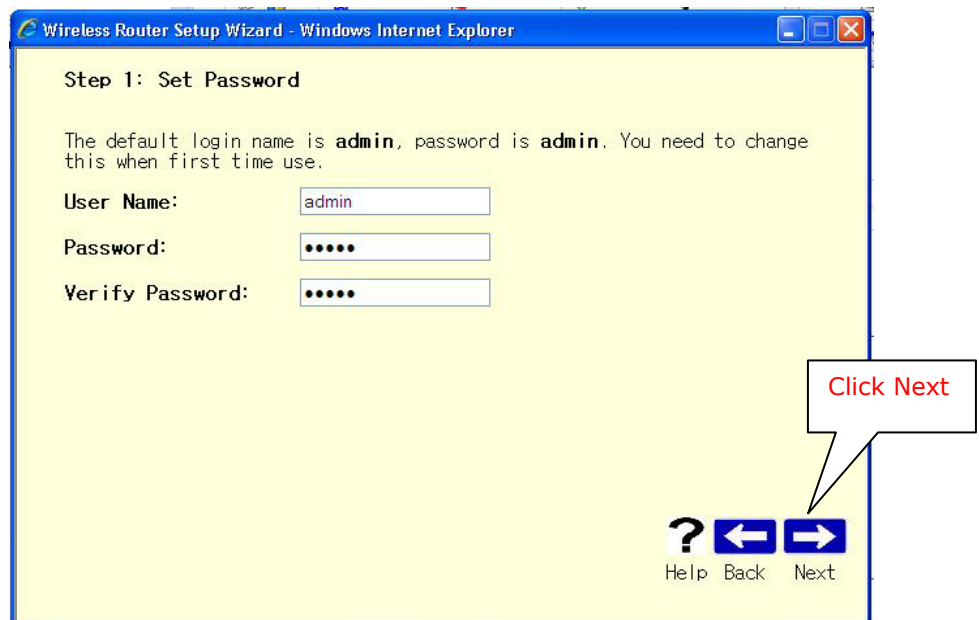
6 CONFIGURATION WIZARD



Once you have logged in, the Wizard screen will appear.

Set up your new password

The default User Name and password is **admin** and **admin**.



Choose your Time Zone

Enter the SNTP Server. If you do not know of any SNTP Server, you can use the default.

Choose your time zone from the drop down list.

The screenshot shows a web browser window titled "Wireless Router Setup Wizard - Windows Internet Explorer". The page content is as follows:

Step 2: Set Time Zone

The system gets the current time from SNTP server. Server Address can be a name or an IP address. For the time zone, select the local time zone.

SNTP Server Address:

Time Zone:

At the bottom right, there are three buttons: a question mark icon labeled "Help", a left arrow icon labeled "Back", and a right arrow icon labeled "Next". A red speech bubble with the text "Click Next" points to the "Next" button.

Wireless Setup

Enter the SSID you preferred for your network.

You can manually select the channel you wish to use or allow the AP to select a clean channel to use by selecting *smartSelect*.

The screenshot shows a web browser window titled "Wireless Router Setup Wizard - Microsoft Internet Explorer". The page content is as follows:

Step 3.1: Set the basic of Wireless

Enter the SSID and Channel to be used by the Wireless Access Point.

SSID:

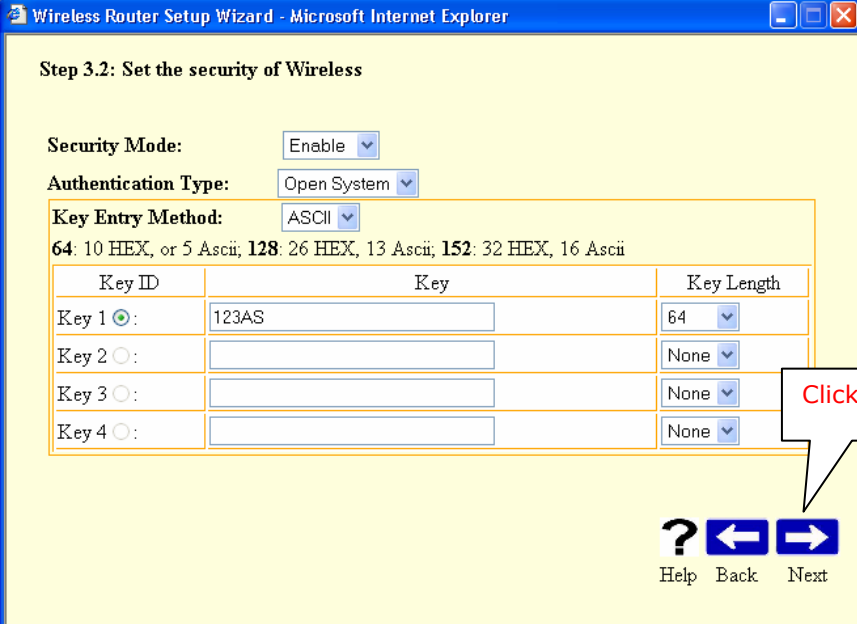
Channel:

At the bottom right, there are three buttons: a question mark icon labeled "Help", a left arrow icon labeled "Back", and a right arrow icon labeled "Next". A red speech bubble with the text "Click Next" points to the "Next" button.

Wireless Security

Enter the type of security mode you wish to use.

Take note that if you are using 802.11b card, it does not support WPA-PSK or WPA or WPA 2-PSK or WPA 2



Step 3.2: Set the security of Wireless

Security Mode:

Authentication Type:

Key Entry Method:

64: 10 HEX, or 5 Ascii; 128: 26 HEX, 13 Ascii; 152: 32 HEX, 16 Ascii

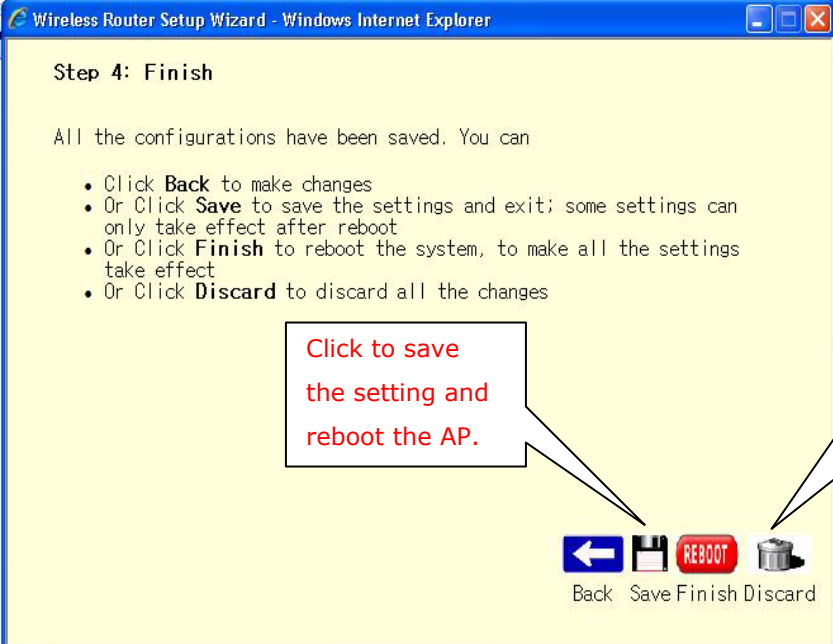
Key ID	Key	Key Length
Key 1 <input checked="" type="radio"/>	<input type="text" value="123AS"/>	<input type="button" value="64"/>
Key 2 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/>
Key 3 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/>
Key 4 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/>

Help Back Next

Click Next

End of Setup

Click on *Reboot* to save the setting and reboot the AP. If you wish to discard all the setting, click on *Discard*.



Step 4: Finish

All the configurations have been saved. You can

- Click **Back** to make changes
- Or Click **Save** to save the settings and exit; some settings can only take effect after reboot
- Or Click **Finish** to reboot the system, to make all the settings take effect
- Or Click **Discard** to discard all the changes

Click to save the setting and reboot the AP.

Click if you wish to discard changes

Back Save Finish Discard

7 CONFIGURATION MENU

System Summary > Configuration

This page presents a convenient overview of the overall status of the AP. The most common configuration parameters are shown here, for a quick look.

System Summary	Setup Wizard	Basic	Wireless	System Tools
-----------------------	------------------------------	-----------------------	--------------------------	------------------------------

System Summary > Configurations

LAN Settings	
LAN IP Mode	Static IP
System Name:	
IP Address:	192.168.1.20
Subnet Mask:	255.255.255.0
Wireless Setting	
Wireless Mode:	Enable
SSID:	11g_1
Channel:	Current Channel 11: 2462MHz
Wireless Mode:	802.11g
Security Mode:	Disable
Authentication:	Open System
Data Rate(Mbps):	Best
Transmit Power:	Max
Preamble:	Short Preamble
Slot Time:	Short Slot Time
Wireless MAC Control:	Enable
Firmware Version	
Current Version:	M2010(S)-I00-C00-H00-V0.0.5B9P0

System Summary > Associations


This page allows you to view the MAC address of all the wireless laptop and PC connected to the AP. ID of AP is the MAC address of the AP itself. Any wireless computers or laptop associated with the AP will have an ID of STA.

ID	MAC Address	Status	Signal Strength(RSSI)	NoiseFloor
AP	00:0A:06:FF:3E:BC	up	-94 dBm	0 dBm

ID	MAC Address	IP Address
----	-------------	------------

System Summary > Statistics

This page allows you to view the packets and bytes receive and transmit by the Access Point.

Wireless	Recieved	Transmitted
Total Bytes:	0	2123277
Broadcast Packets:	0	6681
Multicast Packets:	0	6251
Unicast Packets:	0	1520
RTS Failed:	0	
Ack Rcv Failures:	33009	
FCS Failures:	96779	
Tx Multiple Retries		0
Ethernet	Recieved	Transmitted
Ethernet Status		
Total Bytes:	2253916	6526708
Unicast Packets:	3981	6104
Multicast Packets:	12943	

Up Time: Day 0, 1:26:12

System Summary > Site Scan

Using the site scan, you can scan for the presence of other AP near you. The ESSID, BSSID, wireless mode, channel, signal strength, security mode and network mode of the surrounding AP will be display in the table. You can use this function to select a clean channel for your AP. Take note that there would not be any result if the wireless function of the AP is set to disable.

ID	ESSID	BSSID	Wireless Mode	Channel	Signal Strength (RSSI)	Security Mode	Network Mode
1	DCDC1	00:06:C7:05:08:59	802.11g	1	37	NONE	Infrastructure
2	PM-WR	00:14:BF:7F:01:BB	802.11g	1	21	WEP	Infrastructure
3	Asia_Medicine_Net	00:13:F7:44:15:67	802.11g	1	5	WEP	Infrastructure
4		00:06:C7:1F:25:9F	802.11g	1	12	WPA	Infrastructure

Basic Setting > SNTP

Simple Network Time Protocol (SNTP) allows the AP to set its internal clock based on periodic updates from the specified timeserver (SNTP or NTP). The time is useful in the IP filter section, where you can configure to block certain IP address daily at a certain time.

The system gets the current time from SNTP server.

SNTP Server Address:

Time Zone:

Basic Setting > LAN Setting

This page allows you to choose the type of IP mode

IP Mode	<input checked="" type="radio"/> Static IP <input type="radio"/> Dynamic IP (DHCP Client)
System Name:	<input type="text"/>
IP Address:	<input type="text" value="192.168.1.20"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="192.168.1.254"/>
<input checked="" type="checkbox"/> Manually Set DNS	
DNS Server:	<input type="text" value="0.0.0.0"/>

Static IP mode: When you boot up the AP for the first time, it is in Static mode. You can assign a Static IP to the AP.

DHCP mode: The AP will obtain an IP Address from an upstream DHCP Server.

System Name: This is to assign a name to the AP for system identification.

LAN IP address: This is where you assign a local IP address to your AP's LAN port. The factory default value is 192.168.1.20. If you give your computer a static IP address, the gateway of your computer must be set to this IP for you to access the Internet.

Subnet Mask: This is where you assign the corresponding subnet mask. The default subnet mask is 255.255.255.0.

(Note: When you change the LAN Setting of the AP, you need to reset/renew the Local computer IP address.)

Gateway Address: This displays the gateway address of your WAN as given by the ADSL modem.

DNS Server: This displays the IP address of the DNS server as given by the ADSL modem. You can manually set the DNS server if your ISP provides you with the IP address of the DNS server.

Take note:

User must un-tick the manually set DNS if your ISP did not provide the DNS IP address.

Basic > VLAN Setting

The VLAN provides broadcast filtering, security, address summarization, and traffic flow management. VLAN tagging is to control traffic flow patterns and react to port relocations.

The applications set vlan configurations.

VLAN Mode:

Remove Vlan Header of Trunk Link

Vlan Setting Table

Port	Vlan ID
Vap0	<input type="text" value="1"/>
LAN1	<input type="text" value="5"/>
Management	<input type="text" value="8"/>

You may also set LAN1 port to have the same VLAN ID as the management port to enable the PC connected to this port to get access to web or console.

This page lets you configure the wireless AP, VLAN tagging configurations and additional function of the wireless AP.

The features includes as follows:

1. VLAN Tagging function in Access Point mode
2. VLAN Tagging function in Ethernet Bridge mode
3. Management VLAN support for both AP and Ethernet Bridge mode

VLAN mode: Can be set as enabled or disabled.

Once the AP or Bridge is set to **Enabled mode**, use LAN1 as your uplink port to connect to your PC (for configuration use).

Wireless > Basic Setting

This page lets you configure the Wireless settings of the AP. There are 2 sections: Radio and Security.

<input checked="" type="checkbox"/> Enable Wireless	
<input type="checkbox"/> Enable Qos(SpectraLink) Support	
Operation mode:	<input checked="" type="radio"/> Access Point <input type="radio"/> Ethernet Bridge <input type="radio"/> Repeater
SSID:	<input type="text" value="11g_1"/>
	SSID suppressed: <input type="radio"/> Yes <input checked="" type="radio"/> No
Channel:	<input type="text" value="SmartSelect"/>
Wireless Mode:	<input type="text" value="2.4GHz 54Mbps (802.11g)"/>
Remote AP MAC Address	<input type="text" value="00:00:00:00:00:00"/>
	<input type="text" value="00:00:00:00:00:00"/>
	<input type="text" value="00:00:00:00:00:00"/>
Wireless Isolation:	<input checked="" type="checkbox"/>
<hr/>	
Security Mode:	<input type="text" value="Disable"/>

Enable Wireless: Tick to enable wireless function. With this function, laptop with card bus or in-built wireless function can access the AP wirelessly.

Enable QoS (SpectraLink) Support: Selecting this option will enable the 802.11e QoS support feature for VOIP and video data.

Operation mode: AP operates as Wireless LAN Access Point or Ethernet Bridge or Repeater. Wireless Bridge is used when it is not advisable to lay an Ethernet line over a distance. Two AP's can be set up to connect over this distance, acting as the wired backbone.

SSID: Service Set Identifier. It is a sequence of characters that uniquely names a Wireless LAN. This name allows PCs to connect to the correct Wireless Access Point when multiple Access Points operate in the same location.

The default SSID is **11g_1**

Channel: The radio channel number. You can select channel 1 to 11 or use SmartSelect, where the AP will select the cleanest channel to use upon booting up. The number of channels varies according to countries.

Wireless Mode: You can choose to operate the AP in **802.11g** or **802.11b** mode. The data rate for 802.11g is 54Mbps while the data rate for 802.11b is 11Mbps. 802.11g is backward compatible with 802.11b.

WDS: This feature is available for Ethernet bridge mode. Enable or disable or disable with multiple PC support. When WDS enabled, the bridge can support multiple PCs behind it. When WDS disabled, the bridge can support only one PC behind it. When disabled with multiple PCs support, the bridge can support multiple PCs behind it, even if the AP cannot support WDS.

Remote AP MAC List: The Bridge will only associate with AP whose MAC address is in the list. It is essential to type in the MAC address of the AP without any spacing in front or behind it.

Wireless Isolation: Selecting this option will disallow wireless clients associated with this device to communicate with each other.

Security Mode: This section allows you to configure wireless encryption to prevent unwelcome parties from reading your traffic. You must **Enable** the Security Mode before choosing the type of wireless security.

Security mode > Open-System/Shared key

Security Mode: ▾

Authentication Type: ▾

Key Entry Method: ▾

Key Entry Instruction:

- 64: 10 HEX, or 5 Ascii
- 128: 26 HEX, 13 Ascii
- 152: 32 HEX, 16 Ascii

Key ID	Key	Key Length
Key 1 <input checked="" type="radio"/>	<input type="text" value="asd12"/>	<input type="button" value="64"/> ▾
Key 2 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/> ▾
Key 3 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/> ▾
Key 4 <input type="radio"/>	<input type="text"/>	<input type="button" value="None"/> ▾

Open-System: When chosen, the Key is not used for authentication. It is only used for encryption. Open-System uses Static Keys for encryption. Static (Shared) Keys are never changed, and a hacker can crack the key after a period of time.

Shared-Key: When chosen, the encryption Key is also used for authentication between the AP and Client. Note that this system is also using Static Keys.

Key Entry Method: Choose **HEX** if you want to enter the Keys in hexadecimal format. Otherwise, enter in ASCII format. ASCII is also called Alphanumeric in some systems. Use the same key format for the AP and Client!

Key 1-4: The Key is to be entered in the boxes. The **SAME Key** must be entered in both the AP and Client. Take note that there is a different Key length for a different number of encryption bits. 152 bits is the most secure, but make sure that your Client card supports it. The last point to take note is that if you use Key 4 on the AP, you must also use Key 4 on the Client, for example. The same logic applies for Keys 1-3.

Security Mode > WPA-PSK

Security Mode:

Authentication Type:

Key Entry Method:

Passphrase:

Cipher:

WPA-PSK is also known as WPA-Preset-Key. This implementation is more secure than WEP as the encryption is automatically changed periodically. To configure this feature, just key in 8-63 ASCII character or 64 HEX character pass-phrase for both the AP and Cards.

Cipher: You can choose to use TKIP or AES for the cipher type.

Security Mode > WPA

Security Mode:

Authentication Type:

RADIUS Server: :

Shared Secret:

Confirm Secret:

WPA (WiFi Protected Access) is a standard where the Wireless Card has to authenticate to a RADIUS Server, through the Access Point. The Server can also manage the encryption keys such that they are changed dynamically. You need to have a RADIUS Server to be able to use this feature.

RADIUS Server: Enter the IP Address and the port of the RADIUS Server.

Shared Secret: Enter the Shared Secret of the RADIUS Server.

Confirm Secret: Enter the Shared Secret again to confirm.

Security Mode > WPA 2-PSK

Security Mode: ▾

Authentication Type: ▾

Key Entry Method: ▾

Passphrase:

Cipher: ▾

WPA 2-PSK is the enhancement of WPA-PSK which uses the AES encryption algorithm.

Cipher: You can choose to use TKIP or AES for the cipher type.

Security Mode > WPA 2

Security Mode: ▾

Authentication Type: ▾

RADIUS Server: :

Shared Secret:

Confirm Secret:

WPA 2 is the enhancement of WPA which uses the AES encryption algorithm.

RADIUS Server: Enter the IP Address and the port of the RADIUS Server.

Shared Secret: Enter the Shared Secret of the RADIUS Server.

Confirm Secret: Enter the Shared Secret again to confirm.

Wireless > Advance Setting

This page allows you to configure the advance wireless setting of the AP.

Data Rate(Mbps)	Best ▾
Transmit Power:	Max(20dBm) ▾
Distance:	4-6 Km ▾
Preamble:	Short Preamble ▾
Slot Time:	Short Slot Time ▾
Protection Mode:	None ▾
Protection Type:	<input checked="" type="radio"/> CTS-only <input type="radio"/> RTS-CTS
RTS/CTS Threshold:	2346

Data Rate (Mbps): You can set the wireless data rate from the available list or choose Best to allow the AP to choose the most appropriate data rate. When Best is used, the AP will determine the optimal data rate according to the environment.

Transmit Power: This will adjust the transmit power of the antenna. Sometimes, it is useful to decrease the coverage range of each AP, so that more AP can be located together without interfering one another.

Distance: This is to set the distance for bridging. The default distance is 4-6km.

Preamble: Choose Short Preamble or Long Preamble. Most manufacturers implement long preambles. Even if there is a mismatch between the AP and the client, they can still connect well and the mismatch may not be noticeable to most users. Do not change this setting without seeking advice.

Slot Time: Choose short or long slot time. The slot time is the amount of time a device waits after a collision before retransmitting.

Protection Mode: Select None, Always or Auto.

Protection Type: Select either CTS only or RTS-CTS.

RTS/CTS Threshold: Request to Send/Clear to Send. The primary use of RTS/CTS is to minimize collisions among hidden stations. Forcing the access point to implement the RTS/CTS handshake will significantly increase the overhead and reduce throughput. Once the RTS/CTS is set at the station, it initiates by sending a RTS frame. Upon receiving, the access point will responds by sending a CTS frame. Select the RTS/CTS radio button to enable this feature. Set a packet size threshold (2346 bytes) value to trigger this protection. If the packet that the station/access point is transmitting is larger than the threshold, it will initiate the RTS/CTS function.

Wireless > MAC Access Control

This page allows you to specify which **wireless** computer can access the Internet and which **wireless** computer cannot access the Internet. The specified MAC address and the policy for the computer are reflected in the table.

Users can control the access of other wireless devices to the router.
To do:

- Enable Wireless MAC Control
- Set the default policy
- Add the MAC address with the policy applied to the MAC

Enable Wireless MAC Control

Default Policy: Deny All Allow All Save

MAC Address: (Format: aa:bb:cc:dd:ee:ff)

Policy: Add Update

ID	MAC Address	Policy	
0	00:06:34:6ffd:43	Deny	Edit Delete

Help

Enable Wireless MAC Control: Tick to enable Wireless MAC Control.

Default Policy: This policy determines whether computers, whose MAC addresses are not in the table, are able to access the Internet. If you choose **Deny All**, all computer associated to the AP will not be able to access the Internet other than those specified in the table.

MAC Address: Enter the MAC address of the computer. The format for the MAC address is aa:bb:cc:dd:ee:ff.

Policy: Choose to deny or allow the computer to access the computer. Click on the *Add* button to add the policy.

Wireless > Bandwidth Control

This page allows you to control the bandwidth limit for broadcast/multicast/TCP and individual wireless client.

Bandwidth Control:	
<input checked="" type="checkbox"/> Broadcast Limit (F/s):	<input type="text" value="50"/>
<input checked="" type="checkbox"/> Multicast Limit (F/s):	<input type="text" value="50"/>
<input type="checkbox"/> TCP Limit (kbps):	<input type="text" value="1024"/>

Bandwidth Control for Each Wireless Client:	
<input type="checkbox"/> Upload Limit (kbps):	<input type="text" value="1024"/>
<input type="checkbox"/> Download Limit (kbps):	<input type="text" value="1024"/>

Enable Broadcast Limit: Selecting this option will filter off out broadcast storm.

Broadcast Box: Select a number in between 0 to 1000 F/s.

Enable Multicast Filter: Selecting this option will filter off out multicast storm.

Multicast Box: Select a number in between 0 to 1000 F/s.

Enable TCP Limit: Selecting this option will limit the bandwidth on TCP/IP data based on the number entered in the textbox.

TCP Limit: Select a number in between 48 to 55296 Kbps.

Enable Upload Limit: Selecting this option for bandwidth control of wireless Client uplink to AP.

Upload Box: Select a number in between 48 to 55296 Kbps.

Enable Download Limit: Selecting this option for bandwidth control of AP downlink to wireless Client

Download Box: Select a number in between 48 to 55296 Kbps.

System Tools > System Log

This page allows you to configure the AP to dump its status to a System Log Server.

Enable Remote System Log

Server IP:

Server Port:

Enable Local System Log

When log is full: Stop Logging Auto Delete

```
83: <6>00:00:11 Boot:  FFFFFFFD FFF7FFFF EFFFFFFF DF7FFFFF DFFFBFFF FFFFFFFF
82: <5>00:00:11 System: System Up From Cold Power Up FFFFFFF7 FFFFFFFF
81: <6>00:00:11 Boot:  FFBFFFD FFF7BFFF EFFFF7DF DD37FFDF DD7FBFFF F7F3FFFF
80: <5>00:00:11 System: System Up From Cold Power Up FDFF77F DFFF7F7F
79: <6>00:00:11 Boot:  FFFFFFFD FFF7BFFF EFFFFFFF DF7FFFFF DFFFBFFF FFFFFFFF
78: <5>00:00:11 System: System Up From Cold Power Up FFFFF77F FFFF7F7F
77: <5>00:00:13 System: System Up From Reset: sysFactoryInt
76: <6>00:00:11 Boot:  FFBFFFD FFF7BFFB EFEFF7FF DD377FDF DF7FBFFF F7F7FFFF
75: <5>00:00:11 System: System Up From Cold Power Up 5EADBAAE 00000000
74: <6>00:00:12 Boot:  FFBFFFD FFF7BFFF EFEFF7FF DD377FDF DF7FBFFF F7F7FFFF
73: <5>00:00:11 System: System Up From Cold Power Up DEADBEAF 00000000
72: <6>00:00:11 Boot:  FFBFFFD FFF7BFFF EFFFF7FF DD37FFDF DF7FBFFF F7F7FFFF
71: <5>00:00:11 System: System Up From Cold Power Up FFFFF77F DFFF7F7F
70: <6>00:00:11 Boot:  FFBFFFD FFF7BFFF EFFFF7FF DD77FFDF DF7FBFFF F7F3FFFF
69: <5>00:00:11 System: System Up From Cold Power Up FDFF77F DFFF7F7F
68: <5>00:00:11 System: System Up From Reset: ws_FacReset
67: <5>00:00:56 System: Reboot by Factory reset command
```

Available Entries Left: 117

Enable Remote System Log: Enable this feature to allow the AP to constantly update its status on a System log Server.

System Log Server IP: Enter the IP Address of the System Log Server if you had enabled Remote Logging.

System Log Server Port: Enter the port number the System Log Server is using.

Enable Local System Log: Enable this feature if you do not have a System log Server. The events would then be logged locally on the AP.

Log Management when log is full (Stop Logging): When this option is chosen, the AP will stop logging.

Log Management when log is full (Auto Delete): The maximum number of local log entry is 200. When all the 200 entries are used up, the AP will overwrite previous entries with new logs.

Remember to Apply and Reboot for the settings to take effect.

System Tools > System Admin

This page allows you to change the Administrator's Username and Password. The default username and password is admin / admin. After every **Factory Reset**, the AP reverts to this combination.

User Name:	<input type="text" value="admin"/>
Password:	<input type="password" value="password"/>
Verify Password:	<input type="password" value="password"/>

System Tools > License Key

License Key:	<input type="text"/>
--------------	----------------------

This page allows you to key in the license key to enable your request for additional features requirements. The license key can be obtained from our company at a certain fees and features request agreement.

System Tools > SNMP Configuration

Enable SNMP	<input checked="" type="checkbox"/>
Read Community String	<input type="text" value="public"/>
Write Community String	<input type="text" value="private"/>
System Contact	<input type="text"/>
System Location	<input type="text"/>

Enable SNMP: Selecting this option will enable the SNMP feature.

Read Community String: The password set for the SNMP Client for read access.

Write Community String: The password set for the SNMP Client for write access.

System Contact: To set the system contact for users.

System Location: To set the system location for users.

System Tools > Backup/Restore Settings

Use this page to preserve any good setting. You can save the configuration file into your computer and upload it back to the AP when the setting of your AP when necessary. In addition, you can do a factory reset and restore the AP back to factory default setting. The factory default setting is shown in the *Factory Reset* section.

Good Settings	
Save the Good Settings:	<input type="button" value="Save"/>
Restore to the Good Settings:	<input type="button" value="Restore&Reboot"/>
Configuration File	
Backup the current settings to a file. Click Here to save.	
Upload the Configuration File(apcfg):	
<input type="text"/>	<input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Factory Reset	
Press the button to set all the configurations to factory default settings.	
<input type="button" value="Factory Reset&Reboot"/>	
<input type="button" value="Help"/>	

Save configuration to local device: After you have successfully configured the AP, you can save this "Good Config" into device memory.

Restore configuration from local device: You can retrieve this "Good Config", if you have messed up some settings and do not know what the previous working setting is.

Save configuration to local PC: After successfully configured the AP, save this "Good Config" into the computer system.

Configuration file on local PC: Browse to the location of the saved "Good Config" in the computer system.

Restore configuration from local PC: Allow restoring back to the "Good Config" from the computer system.

Revert to factory setting: If you have even forgotten the password to get into the configuration pages, you would have to do a Factory Reset to the AP.

System Tools > Firmware Update

This page allows you to update the firmware (software) in the AP. New firmware is issued to improve the performance and add features to the product.

Attention:

- Please upload the **correct** firmware.
- Please **DO NOT** power off or disconnect during uploading. Improper actions will damage the system.
- Please **DO NOT** close the browser during uploading
- Upload will take around 3 minutes

File Name:

Current Version: *M2010(S)-100-C'00-H00-V0.0.5B9P0*

1. The new firmware is a file name "apimg1".
2. Save the file in your PC.
3. **Browse** and select the firmware file.

You will see the following page when firmware upgrading is successful.

Upload Succeeds.

The file has been uploaded.

[Back](#)



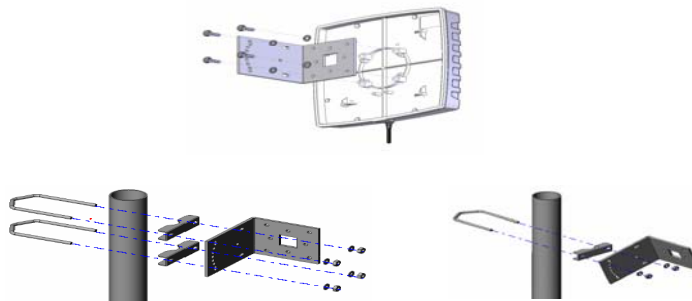
Do not close the browser or shutdown the AP during firmware upgrading. Failure to do so will cause serious damage to Access Point.

System Tools > Reboot

This page allows you to reboot the AP. You must reboot the AP after you have finished configuring the AP for the new setting to take effect.



8 ACCESS POINT MOUNTING GUIDE



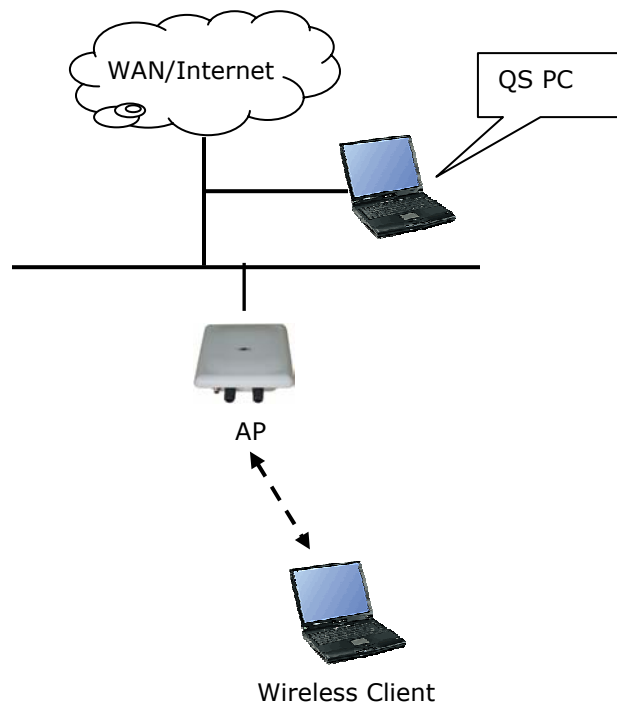
9 VIPER QUICKSTART INSTALLATION

Introduction

The Viper QuickStart Version 1.2 utility is an easy-to-use software that allows an Administrator to quickly configure the AP at first boot-up. The QS Utility only communicates with authorized Access Points and Bridge. The Utility allows the devices to be monitored and configured even if they all have the same default IP Address at first boot-up after installation.

Execution of viper

Double click on the viper program - **quickstart.exe** and it is ready for use.




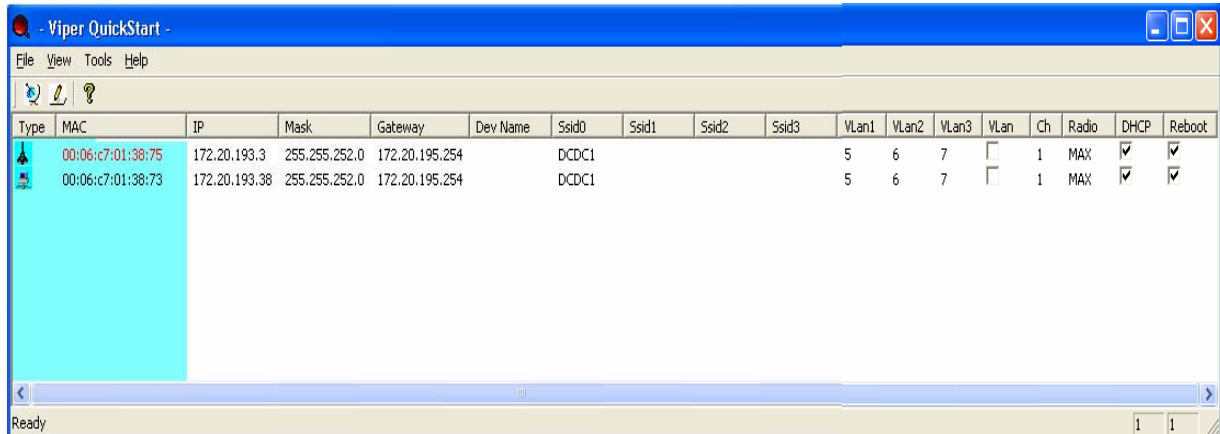
PC Requirement

- X86 based CPU, 600Mhz & above
- 128 MB RAM
- 1.5 MB hard disk space
- Ethernet port / Wireless LAN adapter
- Windows 2000 and above

10 VIPER QUICKSTART USER GUIDE

Viper QuickStart Icon

Click on the icon  quickstart.exe to start the application.



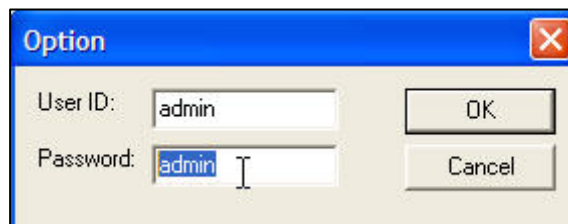
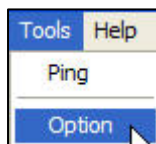
Parameters Display in Utility

The Utility displays the following basic parameters that can be changed.

1. MAC ID
2. IP Address
3. Subnet Mask
4. Gateway
5. Device Name
6. Channel
7. DHCP/Static IP

Username and Password of Utility

If the username/password of the Devices have been changed, the QS Utility has to be updated with the correct username and password. If the username/password of the QS Utility and the Device is different, QS Utility will not operate as desire.




Making Changes

The changes are directly applied in the Utility.

IP	Mask	Gateway
10.0.0.160	255.255.255.0	10.0.0

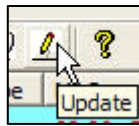
Dev Name	Ch	DHCP
	8	<input type="checkbox"/>
	7	<input type="checkbox"/>
	8	<input type="checkbox"/>
	9	<input type="checkbox"/>
	10	<input type="checkbox"/>
	11	<input type="checkbox"/>

It does not matter if all the devices have the same IP Address. The QS Utility identifies them uniquely by their MAC Addresses.

Type	MAC
	00:06:c7:14:08:73

Updating Changes

After the necessary changes have been made, the Administrator can apply the changes to the AP. Check on the **Reboot** Checkbox and click on the **Update** button to reboot the device.



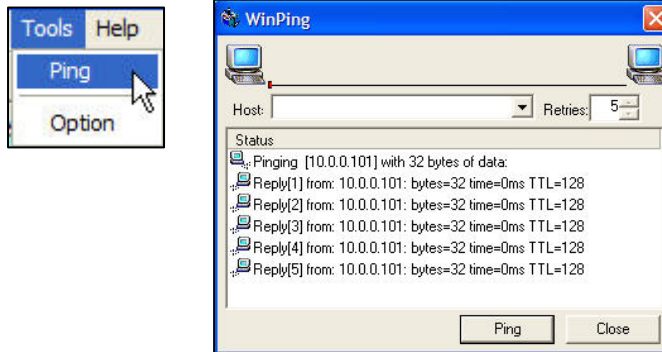
Multiple devices can be updated all at once. Use ctrl-left click to select multiple entries or type ctrl-A to select all entries. Click on Update button to begin the update process.



To refresh the view, use the **Find** button.

Pinging the Device

The QS Utility can also be used to ping a selected Device to check the connectivity.



11 TECHNICAL SUPPORT

For technical support, please contact the following local distributor or reseller.



11 DISCLAIMER

- Manufacturer assumes no responsibility for any damage or loss resulting from the use of this manual.
- Manufacturer assumes no responsibility for any loss or claims by third parties that may arise through the use of this product.
- Manufacturer assumes no responsibility for any damage or loss caused by incorrect use of the AP.
- The contents of this manual are subject to change without prior notice due to engineering improvement.
- No part of this manual may be reproduced in any form without the express written consent of the Manufacturer.
- Sample displays shown in this Manual may differ somewhat from the displays actually produced by the product.
- User Manual may differ for different firmware version.
- All brands and product names are trademarks or registered trademarks of their respective holders.