WAVE CAST

MW-1500AP(H) Manual

SineDIGITAL

We Make the Internet Good.

The specifications and information herein are subject to change without notice. Please download the latest driver software or manual free of charge from the sinedigital,Inc.homepage at http:// www.sinedigital.com

WaveCast is a trademark of SineDigital,Inc.

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, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

FCC RF INTERFERENCE STATEMENT

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

■ RF Exposure

This device has been evaluated for compliance with FCC RF Exposure limits.

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

■ User Notice

Do not change or modify the product without permission or authority of manufacturer. It may cause undesirable operations, permanent damages or harmful interferences.

■ Product Notice

·Design and specification are subject to change without notice for product improvement purposes.

Send questions to:

SineDigital,Inc.
E-mail: support@sinedigital.com
Homepage:http://www.sinedigital.com

Product integrity issues:

- Do not open the case or modify contents of the MW-1500AP(H). Seek the assistance of a qualified professional if some problem occurs with the MW-1500AP(H).

- Do not expose the MW-1500AP(H) to dangerous environments such as fire, chemicals or explosives that may damage it.

- Do not use and disconnect all power and telephone cables from PC's and MW-1500AP(H) during severe thunderstorms or lightning.

- Make sure the MW-1500AP(H) will not cause hazardous effects to other equipment prior to operating it in hospitals, airplanes, etc. or other locations susceptible to radio wave interference.

- The MW-1500AP(H) and other wireless devices may cause interference on each other and as a result performance of the MW-1500AP(H) may be affected.

- To prevent the risk of losing important data saved in the PC during installation of the MW-1500AP(H), it is advised to backup all important data before installation.

- Moving the PC out of the access point's coverage during data transfer may damage the data being transferred.

- Make sure to stop all wireless data transfer prior to disconnecting from the MW-1500AP(H) in order to avoid damage to the transferred data.

List of Contents

1. THE WAVECAST ACCESS POINT

The MW-1500AP(H) is a wireless LAN (WLAN) equipment compliant to the IEEE 802.11b WLAN standard and will let you enjoy all the benefits of a regular wired network installation but with an added freedom of mobility.

The MW-1500AP(H) has powerful functions and features that make enjoying a wireless LAN secure and convenient.

Before you even start installing your MW-1500AP(H), there are a few issues to consider as shown below in order to ensure a trouble-free operation.

Issue	Description
Reduction of electronic waves	The WLAN system's electronic waves may be influenced by distance, interference from other equipment's electronic waves, obstacle, etc. Of special influence are concrete walls, metallic obstacles (e.g. metal doors and meshes) and equipment emitting electronic waves (e.g. microwave ovens). Please consider such sources of influences when choosing the location to install your MW-1500AP(H) or to operate your mobile PC (e.g. notebook PC).
Intensity of MW-1500AP(H)'s electronic wave	Strong electronic wave emission from the MW-1500AP(H) does not necessarily translate into smoother Internet access or faster data transfer rates since the connection's quality is also dependent on the electronic wave emission from the WLAN interface card the client is using.
Channels	There are thirteen (13) channels available in the MW-1500AP(H). However, different countries have different standard quantities of channels. For example, while the standard number of channels in Korea, China and most of Europe is thirteen (13) channels, it is eleven (11) channels in the U.S. When the product is sold in U.S., the channels will be limited to 1-11 through firmware.

MW-1500AP(H) Specification

Hardware Specification

- Ports: 1 x RJ-45 (WAN, Ethernet, 10/100 Base-T type)
  1 x DB-9 (COM, console port)
  1 x power connector
- Displays: 5 x status LED's
- Antenna: 2 x external 4dBi dipole (provision for antenna replacement)
- Power switch
- Init. switch (reset to factory default)
- Size: 146 x 186 x 41 mm
- Weight: 405g
- Temperature: -20 ~ 70 ^{o}C (storage)
  -10 ~ 55 ^{o}C (operation)
- Relative humidity: 0 ~ 95% non-condensing
- Power supply: 5V DC/2A
- Power consumption: max. 1.3A/5V DC

Software Specification

- IEEE 802.1d wired LAN to wireless LAN bridging
- Wired LAN standard: IEEE 802.3&3u (Ethernet, 10/100 Mbps)
- Works with ADSL (PPPoE), Cable modem and leased line
- Fixed IP, DHCP server, DHCP client, DHCP relay, etc.
- Roaming via IAPP
- Remote management via HTTP (Web Manager) and Telnet
- Security: static 64/128-bit WEP encryption
- IEEE 802.1x
- RADIUS authentication and accounting
- SNMP v1, v2c & MIB I, II, 802.11MIB
- Firmware upgrade function via TFTP or HTTP
- IP sharing via NAT
- Auto channel selection
- Load Balancing
- NetBIOS Filtering
- Broadcast Storming Control

Radio Specification

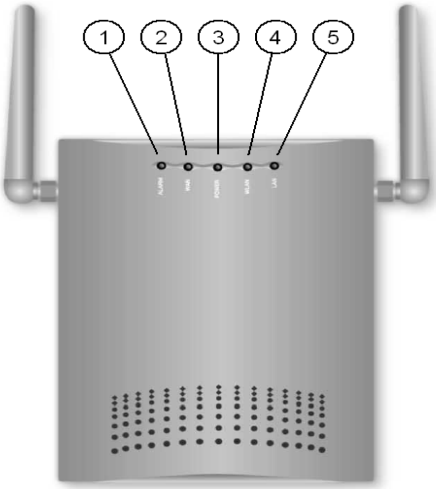
- Wireless LAN standard: IEEE 802.11b
- Frequency: 2.4GHz ISM band
- Modulation: Direct Sequence Spread Spectrum (DBPSK, DQPSK, CCK)
- Data rate: 1M, 2M, 5.5M, 11Mbps with auto fall-back
- 802.11b power save
- Receive sensitivity: min. -84dBm at 11Mbps
- Output power: typical 17dBm

MW-1500AP(H) Contents

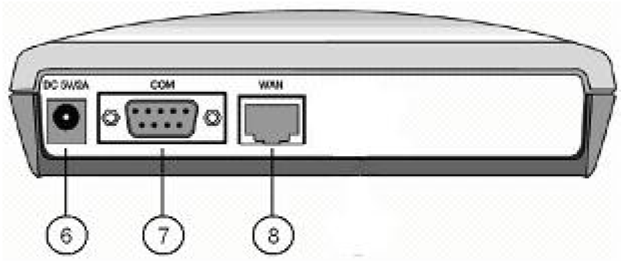
The following items should be included in the MW-1500AP(H) package:

- 1 x MW-1500AP(H)
- 1 x Ethernet cable (RJ-45)
- 1 x Power adapter (5V DC/2A)
- 2 x Antenna (4dBi dipole)

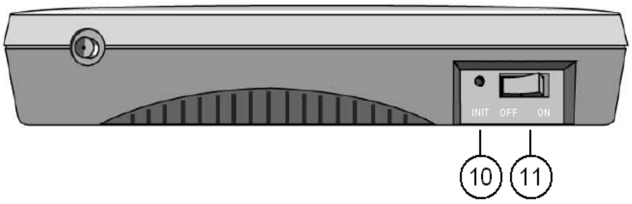
MW-1500AP(H) LED's, Ports and Switches



Item	Description
1	ALARM: This LED will turn green to indicate that there is a problem with the MW-1500AP(H). You should consult the Q&A in our website www.mmectech.com or contact us when this LED comes on.
2	WAN: This LED will turn green to indicate that the network's Ethernet cable is properly connected to the MW-1500AP(H) and will flash whenever there is data traffic.
3	POWER: This LED will turn red to indicate that electrical power is being properly supplied to the MW-1500AP(H).
4	WLAN: This LED will turn green to indicate that the WLAN link is properly established and will flash whenever there is data traffic.
5	LAN: This LED will turn green to indicate that the LAN link is properly established and will flash whenever there is data traffic. (MW-1500AP only)



Item	Description
6	DC 5V/2A: This jack is for connection with the power adapter. Do not use this jack when you are using the MW-1500AP(H) with a PoE power injector.
7	COM: This port is for the console cable that links the MW-1500AP(H) with the PC. This port is used for configuration purposes and is not necessary for normal use.
8	WAN: This port is for the Ethernet (10Mbps) cable. This port also supports use of PoE power injectors.



Item	Description
10	INIT: Pressing this button for about 1 second will reset the MW-1500AP(H) to the factory default settings. All LED's except the POWER LED will flash upon reset.
11	POWER SWITCH: Switches the MW-1500AP(H)'s power ON and OFF.

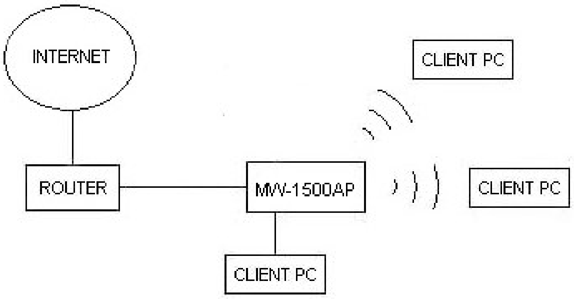
2. MW-1500AP(H) Installation

MW-1500AP(H) Layout

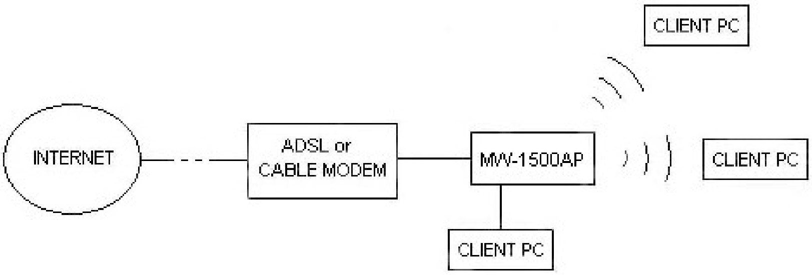
The following are some typical installation layouts for the MW-1500AP(H).

You might have to use either a direct cable or cross cable to connect the MW-1500AP(H) with a router, hub, ADSL or cable modem depending of each of these products' manufacturing convention (check with the each product's manufacturer). Nevertheless, you may verify that the correct type of cable has been used by doing the following: when connected with the correct cable, the MW-1500AP(H)'s WAN LED (item 2 in the above table) will light up.

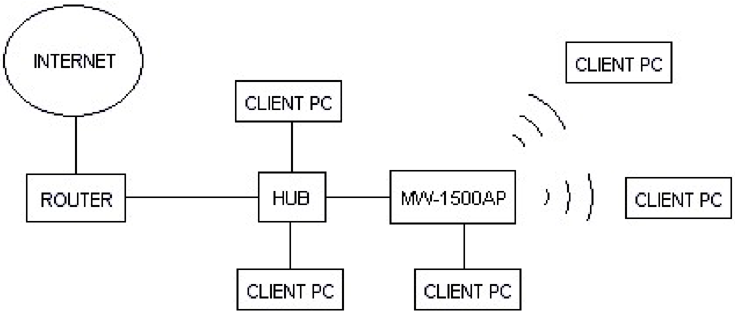
- MW-1500AP(H) Layout 1: Connecting With A Leased Line



- MW-1500AP(H) Layout 2: Connecting With External ADSL/Cable Modem



- MW-1500AP(H) Layout 3: Connecting With A Hub



MW-1500AP(H) Installation

Step 1: Make sure the MW-1500AP(H)'s "POWER SWITCH" is turned off. Connect the Ethernet cable (RJ-45) from router or ADSL modem, etc. into the MW-1500AP(H)'s "WAN" port.

Step 2: You may also connect another device such as a PC, printer, access point, etc. to the MW-1500AP(H)'s "LAN" port. Consult the manual of the device you wish to connect with the MW-1500AP(H).

Step 3: Connect the power adapter into the MW-1500AP(H)'s "DC 5V/2A" jack and then into the power outlet. Turn the MW-1500AP(H)'s "POWER SWITCH" to ON. Use only the power adapter (5V DC/2A) supplied with the MW-1500AP(H).

Step 4: After proper configuration setup of the MW-1500AP(H), wirelessly connect the client PC (equipped with a WLAN interface card, such as a WaveCast client card) with the MW-1500AP(H). Consult the WLAN interface card's instructions.

Although you can wirelessly connect with the MW-1500AP(H) without having to perform any prior configuration settings on it, you will still need to make sure your wireless network interface card (e.g. WaveCast PCMCIA cards and USB dongles) is properly configured to successfully connect with the MW-1500AP(H). Consult your wireless network interface card and configure it based on the MW-1500AP(H)'s factory default values shown below.

- Operation mode: AP mode (compliant to IEEE 802.1d). This means that each client PC that connects wirelessly with the MW-1500AP(H) needs to have its own IP address.
- SSID: wavecast
- Channel: 3
- WEP Encryption: off

3. Configuration And Management Via Console Commands

Console commands are used to control the MW-1500AP(H)'s configuration and management functions when you link with the MW-1500AP(H) directly via a serial cable.

You will need to use console commands mostly when you first set-up your MW-1500AP(H) for your particular network or when something happens that prevents you from communicating with the MW-1500AP(H) remotely.

The following will show you how to establish a wired connection between your PC and MW-1500AP(H), followed by some of the most significant console commands.

Your screens may be different from the screens used at the time of this manual's writing according to the firmware version you are actually using.

Establishing A Console Link With The MW-1500AP(H)

Step 1: In order to access the MW-1500AP(H) via its console port, you will need a RS-232 serial cable (crossed) with the following connector pin arrangement:

PC side: DB-9 (female)	AP side: DB-9 (male)
Pin No. 2	Pin No. 3
Pin No. 3	Pin No. 2
Pin No. 5	Pin No. 5

Step 2: Connect the PC side of the RS-232 serial cable into the PC's serial port (refer to your PC's manual). The other end of the RS-232 serial cable should be connected into the MW-1500AP(H)'s console port (labeled "COM").

Step 3: On the PC, run a terminal emulation program (e.g. Windows HyperTerminal) and configure it to the following values:

```
> Bits per second   : 57600
> Data size         : 8
> Parity            : none
> Stop bits         : 1
> Flow control      : none
```

Step 4: Establish a link between the terminal emulation program and the MW-1500AP(H) (consult the manual of your terminal emulation program). Once connected with the MW-1500AP(H), you will be prompted for a User name and Password. The factory default values are shown below.

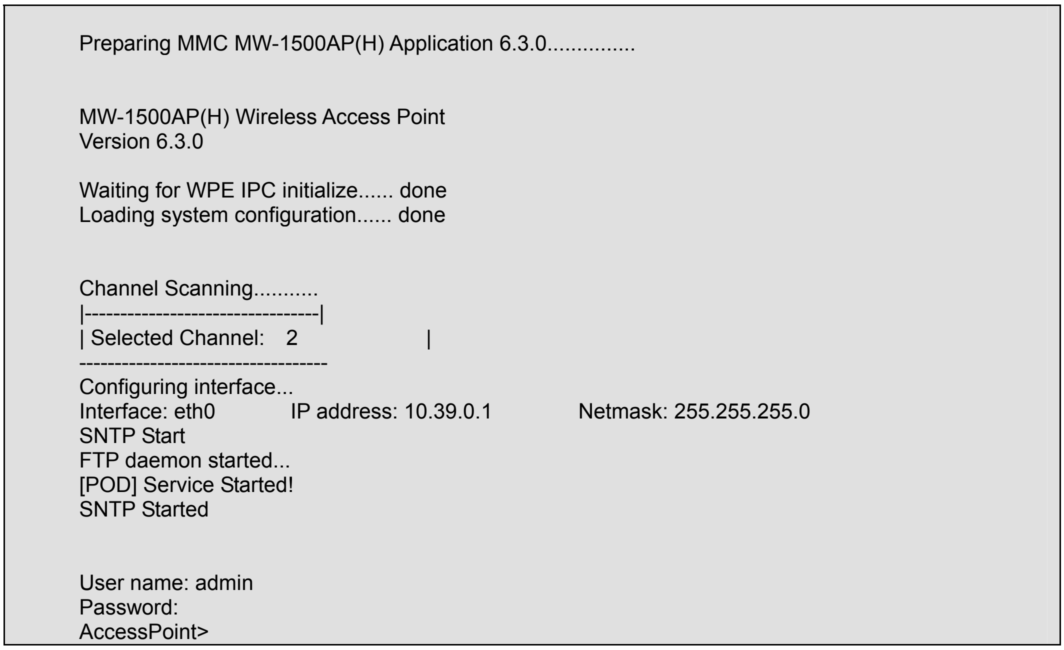
- User name: admin

- Password: password

```
User name: admin

Password: ********
```

Step 5: After entering the correct User name and Password, the command prompt "AccessPoint>" will appear and the MW-1500AP(H) will be ready to receive command input, as shown in the figure below.



```
Preparing MMC MW-1500AP(H) Application 6.3.0..............


MW-1500AP(H) Wireless Access Point
Version 6.3.0

Waiting for WPE IPC initialize...... done
Loading system configuration...... done


Channel Scanning...........
|---------------------------------|
| Selected Channel:    2                    |
-----------------------------------
Configuring interface...
Interface: eth0          IP address: 10.39.0.1           Netmask: 255.255.255.0
SNTP Start
FTP daemon started...
[POD] Service Started!
SNTP Started


User name: admin
Password:
AccessPoint>
```

Console Commands

Available console commands are explained below. Many of the commands listed in here have modifiers, which in turn are shown within brackets (i.e. [ ]). Multiple choices of modifiers are separated by slashes (i.e. /). Alphanumerical or hexadecimal values are shown within angle brackets (i.e. < >).

(1) aaa

This command is used to configure the IEEE 802.1x authentication (RADIUS authentication) functions of the MW-1500AP(H). The command *show aaa* will display the IEEE 802.1x's current configuration status. In addition, the authentication server and accounting server can each be configured separately. Below is a list of commands related to MW-1500AP(H)'s authentication function.

aaa: Shows a list of possible *aaa* commands

aaa [enable / disable]: Enables/disables operation of AAA functions.

aaa eap [enable / disable]: Enables/disables operation of EAP-MD5 (i.e. 802.1x) authentication at the RADIUS server.

aaa macauth [enable / disable]: Enables/disables operation of MAC address authentication at the RADIUS server.

aaa session max <number>: Defines the maximum number of AAA sessions (i.e. users).

aaa session idle <sec>: Defines the AAA session's idle timeout in seconds. The idle timeout is how much time will be allowed for the client to successfully pass authentication.

The authentication process in the MW-1500AP(H) when it is operating the MAC authentication function starts at the moment wireless connection is established between client and MW-1500AP(H). Whereas, the authentication process in the MW-1500AP(H) when its is operating the 802.1x authentication function starts at the moment the client tries to login with its user ID and password.

There are three (3) possible types of values you can assign for the idle timeout (the factory default setting is *300 seconds*):

Negative (-): Entering a negative value (e.g. -100), the MW-1500AP(H) will not even start a session if the client fails authentication, thus not even allowing for a "wait period" in which the client may try to re-authenticate.

Zero (0): Entering a zero value (i.e. 0), the MW-1500AP(H) will start a session for the connecting client and allow for an infinite "wait period" (i.e. the MW-1500AP(H) will not delete the unauthenticated client's session information).

Positive (+): You may also manually determine the idle time period (from 60 to 2,147,483,647 seconds) during which the MW-1500AP(H) will wait for the client to re-authenticate. If the client fails to authenticate until the specified idle time terminates, that client's session information will be immediately deleted from the MW-1500AP(H)'s memory. The factory default for this setting is *60 seconds*.

aaa session delete: Shows a list of AAA sessions currently in progress. Selecting a session's number will delete that session.

aaa auth ip<number> <IP address>: Defines the RADIUS authentication server's IP address. An example would be "aaa auth ip1 10.0.0.3".

aaa auth port<number> <port number>: Defines the RADIUS authentication server's port number. An example would be "aaa auth port1 1812".

aaa auth secret<number> <name>: Defines the shared secret name to be used with the RADIUS authentication server. An example would be "aaa auth secret1 test".

aaa auth retry **<number>**: Defines how many times upon failure the MW-1500AP(H) will retry connection with the RADIUS authentication server. An example would be "aaa auth retry 3".

aaa auth timeout **<sec>**: Defines the time span (in seconds) in which the MW-1500AP(H) will try to connect with the RADIUS authentication server. An example would be "aaa auth timeout 5".

aaa auth nas_id **<name>**: Defines the MW-1500AP(H)'s NAS Identifier, which is the name that the RADIUS server will see. An example would be " aaa auth nas_id MMC-WL-AP1500".

aaa acct [enable / disable]: Enables/disables client accounting management by the MW-1500AP(H).

aaa acct ip<number> <IP address>: Defines the RADIUS accounting server's IP address. An example would be "aaa acct ip1 10.0.0.3".

aaa acct port<number> <port number>: Defines the RADIUS accounting server's port number. An example would be "aaa acct port1 1813".

aaa acct secret<number> <name>: Defines the shared secret name to be used with the RADIUS accounting server. An example would be "aaa acct secret1 test".

aaa acct retry **<number>**: Defines how many times upon failure the MW-1500AP(H) will retry connection with the RADIUS accounting server. An example would be "aaa acct retry 3".

aaa acct timeout **<sec>**: Defines the time span (in seconds) in which the MW-1500AP(H) will try to connect with the RADIUS accounting server. An example would be "aaa acct timeout 5".

aaa acct interim **<sec>**: Defines the cyclic time period after which the MW-1500AP(H) will send each client's accounting information to the RADIUS accounting server (i.e. the interim interval). There are three possible types of values you can assign for the interim value:

-1: Setting it to -1 (negative one) will have the MW-1500AP(H) not send out clients' accounting information to the RADIUS accounting server.

Zero (0): In case the RADIUS accounting server does not specify a interim interval, the MW-1500AP(H) will send the client's accounting information to the RADIUS accounting server only once when the client logs-in and then once again when the client logs-out.

However, if the RADIUS accounting server specifies a interim interval, the MW-1500AP(H) will send clients' accounting information to the RADIUS accounting server according to that specified time value.

Positive (+): You may define the interim interval manually to any positive value from 60 to 2,147,483,647 seconds (you must input without the commas).

aaa pod [enable / disable]: Enables/disables operation of the MW-1500AP(H)'s POD function (refer to chapter 3.2.3.12).

aaa pod checkpoll <sec>: Defines the check poll period, which is the cyclic time period after which the MW-1500AP(H) will check for data traffic activity with the client.

aaa pod idlepoll <sec>: Defines the idle poll period, which is the time period of continuous data traffic inactivity between the MW-1500AP(H) and client after which the MW-1500AP(H) will start checking the client to confirm whether the it (the client) is still wirelessly linked.

aaa pod deadthreshold <sec>: Defines the dead threshold period, which is the time period of continuous non-responsiveness from client after which the MW-1500AP(H) will, if confirmed there is no longer wireless link connectivity with client, automatically stop the client's accounting and delete the client's session information.

(2) channel

```
AccessPoint> channel
SSID (current: wavecast) : testssid
 Automatic Channel Configuration Enable? (CURRENT:enabled) [Y/N]:
Channel (current: 2) [1~13] : 9


 Change the configuration options as below.

 SSID             : testssid
 Channel          : 9

 Proceed?   (Y/N)


Changes will effect after save and reboot.
Reboot the system with "[~@home]" command.
AccessPoint> save

Configuration saved successfully

AccessPoint>
```

This command is used to configure the SSID and channel used by the MW-1500AP(H). Typing this command at the prompt will display the current SSID followed by the message:

Automatic Channel Configuration Enable? (CURRENT:disabled) [Y/N]

The current status of the automatic channel function is displayed within the parentheses "( )". The line also asks for an input of Y (yes: enable the automatic channel function) or N (no: disable the automatic channel function).

If enabling the automatic channel function, the AP will, the next time it reboots, automatically scan the vicinity then decide on the most appropriate channel. If disabling the automatic channel function, you must manually select the channel the MW-1500AP(H) will operate in.

(3) csmac

This command configures the MW-1500AP(H)'s MAC filtering function. With this function, you can control the ability of each client to access the network via the MW-1500AP(H). After adding each client's MAC address into a list in the MW-1500AP(H)'s memory, you can either collectively allow or collectively negate network access to those clients in the list. The following is a list of possible commands to configure the MW-1500AP(H)'s MAC filtering function.

csmac show: Displays the current MAC Address List

csmac add <MAC address>: Adds a MAC address to the current list (e.g. *csmac add 00:30:0d:22:15:9c*).

csmac del <index number>: Deletes the MAC address corresponding to the index number in the list.

csmac disable: Disables the MAC filtering function and makes the network access independent of MAC address.

csmac enable [permit / deny]: When using the modifier *permit*, those stations in the list will be denied network access. When using the modifier *deny*, only those stations in the list will be allowed network access.

(4) dhcp

The following are possible commands related to the MW-1500AP(H)'s DHCP Client.

dhcp interface [start / stop / restart]: start / stop / restart the MW-1500AP(H) to be allocated an IP from a DHCP Server.

(5) dhcpr

The following are possible commands related to the MW-1500AP(H)'s DHCP Relay Agent.

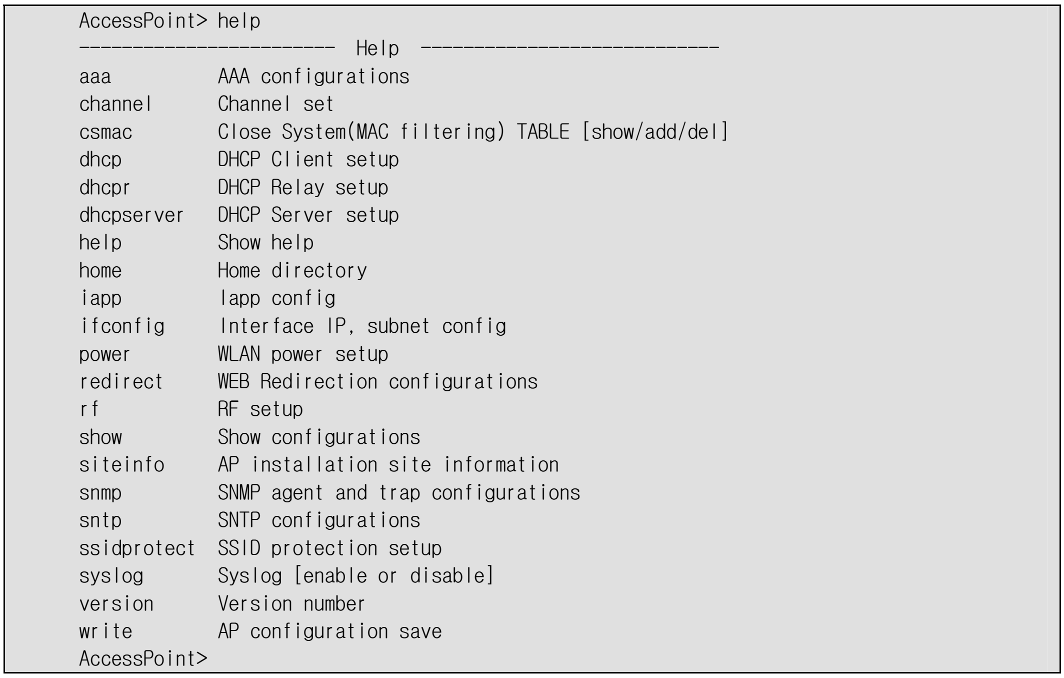
dhcpr [start / stop / status] –o [remote_server]: start / stop / status the MW-1500AP(H) to relay an IP address from a specified DHCP Server and allocate it to a client.

(6) exit

Typing the command *exit* at the command prompt will log out the user and return to the initial login screen.

(7) help

This command displays a list of some configuration commands available in the MW-1500AP(H) as shown in the figure below. Please refer to each command's section for detailed explanation.



```
AccessPoint> help
------------------------  Help  ----------------------------
aaa          AAA configurations
channel      Channel set
csmac        Close System(MAC filtering) TABLE [show/add/del]
dhcp         DHCP Client setup
dhcpr        DHCP Relay setup
dhcpserver   DHCP Server setup
help         Show help
home         Home directory
iapp         Iapp config
ifconfig     Interface IP, subnet config
power        WLAN power setup
redirect     WEB Redirection configurations
rf           RF setup
show         Show configurations
siteinfo     AP installation site information
snmp         SNMP agent and trap configurations
sntp         SNTP configurations
ssidprotect  SSID protection setup
syslog       Syslog [enable or disable]
version      Version number
write        AP configuration save
AccessPoint>
```

(8) http

This command configures the HTTP aspect of the MW-1500AP(H) and the following are the possible commands.

http: Displays the current configuration status of the MW-1500AP(H)'s HTTP function and a list of related commands.

http [enable / disable]: Enable/disable operation of the MW-1500AP(H)'s HTTP.

http port <number>: Defines the port the MW-1500AP(H) will use for HTTP (factory default is 80).

http filter [enable / disable]: When enabled, only the clients with the specified IP addresses are able to configure and manage the MW-1500AP(H) via HTTP. When disabled, any client will be able to configure and manage the MW-1500AP(H) via HTTP.

http permit add <first IP> <last IP>: Adds to the MW-1500AP(H)'s memory the IP address range that will be allowed to configure and manage the MW-1500AP(H) via HTTP by specifying the first and last IP addresses of that range. You can add up to five IP address ranges.

http permit del <number>: Deletes the IP address range of the specified index number from the MW-1500AP(H)'s memory.

The following is an example of the usage of the *http* command.

```
AccessPoint> http
  HTTP Server [ENABLED].
  HTTP Port:80
  HTTP Filtering [DISABLED].

--------------------HTTP Permit No List.--------------------
Insufficient parameters.
ex) http enable
        http disable
        http port 8080
        http filter enable
        http filter disable
        http permit
        http permit add 10.0.0.1 10.0.0.127
        http permit del 1
AccessPoint>
```

(9) ifconfig

This command lets you configure MW-1500AP(H)'s interface parameters. Possible commands are shown in the figure below.

Ifconfig –o <interface_name> inet <address> [netmask <mask>] [broadcast <addr>] [up/down] [mtu <n>]

(10) iapp

Operation of the MW-1500AP(H)'s IAPP (Inter-Access Point Protocol) function must be enabled in order to allow roaming amongst various MW-1500AP(H)'s that are located in a certain area (e.g. Hot Spot sites) and operating with their authentication function enabled.

```
AccessPoint> iapp
Insufficient parameters.
ex) iapp [enable]
ex) iapp [disable]
ex) iapp [list]
ex) iapp [show]
ex) iapp [waittime] [second]
ex) iapp [sender] [old/new]
ex) iapp [rcvtime] [enable/disable]
ex) iapp [synctime]
AccessPoint>
```

In very simple terms, this is how roaming takes place: when a client moves from site A to site B, the MW-1500AP(H) at site A reports the client's information to the authentication server, which in turn authenticates the client again via the MW-1500AP(H) at site B, thus allowing the client to roam. A necessary condition for roaming to take place is that both MW-1500AP(H)'s at site A and B must be in the same subnet.

Possible commands are shown in the figure above. **Do not use** the modifiers *waittime*, *sender*, *rcvtime* and *synctime* (leave them at their default values).

(11) ping

When the MW-1500AP(H) is allocated with an appropriate IP address, you can verify whether it is properly linked to the network by using this command to ping a specified IP Address.

```
AccessPoint> ping 172.16.0.80

Pinging 172.16.0.80 (172.16.0.80) with 56 bytes of data

64 bytes from 172.16.0.80: icmp_seq= 0 ttl=128 time=2.000 ms
64 bytes from 172.16.0.80: icmp_seq= 1 ttl=128 time=1.000 ms
64 bytes from 172.16.0.80: icmp_seq= 2 ttl=128 time=1.000 ms
64 bytes from 172.16.0.80: icmp_seq= 3 ttl=128 time=1.000 ms

--- 172.16.0.80 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.000/1.250 ms/2.000

AccessPoint>
```

(12) rf

Typing this command at the prompt will present you with a series of prompts where you can configure settings for RTS Threshold, Fragment Threshold, Power Save Mode, Beacon Interval, Basic Rates, Supported Rates, Tx Control Rates, etc. The factory default settings for these parameters are already at their optimum settings and it is recommended that you **do not modify** them. But in case you do, please proceed with caution.

```
AccessPoint> rf
RTS Threshold (current: 2432)  [0~3000] :
Fragment Threshold (current: 2346)  [256~2346 EVEN NUMBER only!] :
Beacon Interval (current: 100) :
Transmit Rate Control(current: f) [HEX] :
Basic Rates(current: 3) [HEX] :
Supported Rates(current: f) [HEX] :
DTIM Period(current: 1) [DECIMAL] :
Preamble (current: 1) [1.long, 2 short, 3 auto] :
PM Multicast Buffering (current: Yes) [y/n] :


 Change the configuration options as below.

 RTS Threshold          : 2432
 Fragment Threshold     : 2346
 Beacon Interval        : 100
 Transmit Rate Control  : 0xf
 Basic Rates            : 0x3
 Supported Rates        : 0xf
 DTIM Period            : 1
 Preamble: : 1
 PM Multicast Buffering: Yes

 Proceed?  (Y/N)
Configuration saved successfully.


Changes will effect after reboot.
Reboot the system with "[~@home]" command.
AccessPoint>
```

(13) reboot

This command restarts the MW-1500AP(H)'s system (reboot). Rebooting the MW-1500AP(H) is necessary for any configuration changes to take effect.

(14) redirect

This command is only applicable when operation of the MW-1500AP(H)'s 802.1x function is enabled. The redirect function allows either or both of the following functions to operate:

Just Enrollment: Redirection of client that either fails authentication or tries to access the Internet without authenticating to a specified homepage.

Just First Browsing: Redirection of client to a specified homepage right after successfully passing authentication.

The above can also be used in combination.

Typing the command *redirect* at the prompt, you will be presented with the *redirection menu*, where you will be able to configure its parameters by entering the number of your choices.

```
AccessPoint> redirect

---------------------------
          REDIRECTION MENU
---------------------------
   1. Show Current Setting
   2. Set New Configuration
   3. Flush IPs for Redirect URLs
   4. Use Private IP for Redirection
---------------------------
   Enter the Index of MENU :    2

---------------------------------------------
                        REDIRECTION MODE
---------------------------------------------
   Index    Just Enrollment    Just First Browsing
---------------------------------------------
     [1]              OFF                         OFF
     [2]              ON                          OFF
     [3]              OFF                         ON
     [4]              ON                          ON
---------------------------------------------
   Enter the Index ?    2

   Enter the new URL    : http://www.mmctech.com
   More Sub-Server IP ? (y/n)
"write config" and "reboot" to confirm
AccessPoint>
```

The figure above illustrates the configuration of the redirection function using the command *redirect*. In case redirection will be done to multiple homepages, enter *Y* to the prompt "*More Sub-Server IP? (y/n)*" (You can enter up to four different homepages).

(15) show

This command is used to verify the configuration status and statistical information of various functions and parameters of the MW-1500AP(H). The available commands are shown below.

show aaa: Shows information regarding 802.1x authentication.

show http: Shows configuration status of the MW-1500AP(H)'s HTTP.

show interface: Shows overall information of the MW-1500AP(H)'s interface.

show rf: Shows configuration status of the MW-1500AP(H)'s RF.

show snmp: Shows configuration status of the MW-1500AP(H)'s SNMP.

show syslog: Shows MW-1500AP(H)'s current System Log.

show systime: Shows MW-1500AP(H)’s current System time.

show trap: Shows transmission status of each SNMP TRAP in the MW-1500AP(H).

(16) snmp

The following are commands for the configuration of the MW-1500AP(H)'s SNMP (Simple Network Management Protocol) function. Typing the command *show snmp* will display the current configuration status of the MW-1500AP(H)'s SNMP.

snmp manager <primary server(trap destination) ip> <secondary server ip>: Up to two SNMP Managers can be configured. Only configured SNMP Managers can access the SNMP Set operation.

snmp community <read-community> <write-community> <trap-community>: SNMP community can be configured. Only those clients with the same community name as the one configured will be able to connect with the MW-1500AP(H).

snmp off: Disables the MW-1500AP(H)'s SNMP function.

snmp trap: Displays a menu where you can enable/disable SNMP trap and assigns how many times the trap message will be sent.

snmp trapoff: Disables SNMP trap function.

snmp trap all: Enable/disable each SNMP trap transmission the MW-1500AP(H) can send.

```
AccessPoint> snmp
Insufficient parameters.
ex) snmp manager <primary server(trap destination) ip> <secondary server ip>
    snmp manager 211.50.55.210 0
    snmp manager 211.50.55.210 211.50.55.211
ex) snmp community <read-community> <write-community> <trap-community>
    snmp community public1 public2 public3
ex) snmp on
ex) snmp off
ex) snmp trap
ex) snmp trapon
ex) snmp trapoff
ex) snmp trap all
ex) snmp filter enable/disable
ex) snmp filtermanager <server ip 1> <server ip 2>
    snmp filtermanager 211.50.55.210 0
    snmp filtermanager 211.50.55.210 211.50.55.211
AccessPoint>
```

(17) sntp

The SNTP (Simple Network Time Protocol) function is used to synchronize the MW-1500AP(H)'s time with the time received from a specified time server. With the command *sntp*, you will be able to configure whether or not to use the SNTP function, the time server's IP address, and the time period loop (in seconds) after which the MW-1500AP(H) will receive such time information.

```
AccessPoint> sntp
Insufficient parameters.
ex) sntp [enable/disable]
ex) sntp addr [server ip]
ex) sntp time [time interval to get time from time server]
ex) sntp timeoffset [time offset value in hours from GMT]
AccessPoint>
```

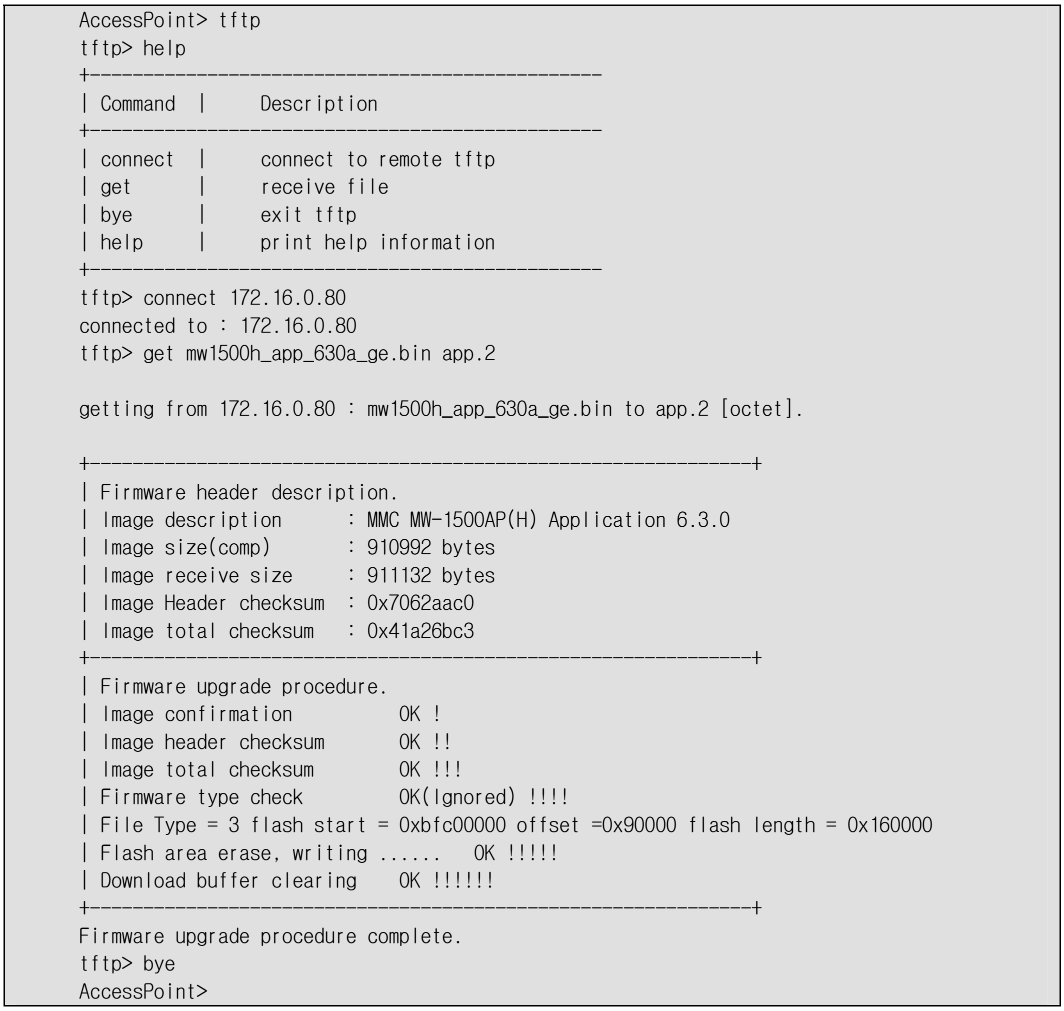
(18) syslog

This command determines whether or not to save the MW-1500AP(H)'s System Log. The saved System Log can be displayed by typing the command *show syslog* at the prompt.

```
AccessPoint> syslog
Syslog enable
Insufficient parameters.
ex) syslog [enable/disable]
AccessPoint>
```

(19) tftp

tftp <tftp server IP> <binary file name>: Use this command to upgrade the MW-1500AP(H)'s firmware by using TFTP to download the new firmware from the specified TFTP server.



```
AccessPoint> tftp
tftp> help
+-------------------------------------------------
| Command   |     Description
+-------------------------------------------------
| connect   |     connect to remote tftp
| get       |     receive file
| bye       |     exit tftp
| help      |     print help information
+-------------------------------------------------
tftp> connect 172.16.0.80
connected to : 172.16.0.80
tftp> get mw1500h_app_630a_ge.bin app.2

getting from 172.16.0.80 : mw1500h_app_630a_ge.bin to app.2 [octet].

+---------------------------------------------------------------+
| Firmware header description.
| Image description      : MMC MW-1500AP(H) Application 6.3.0
| Image size(comp)       : 910992 bytes
| Image receive size     : 911132 bytes
| Image Header checksum  : 0x7062aac0
| Image total checksum   : 0x41a26bc3
+---------------------------------------------------------------+
| Firmware upgrade procedure.
| Image confirmation         OK !
| Image header checksum      OK !!
| Image total checksum       OK !!!
| Firmware type check        OK(Ignored) !!!!
| File Type = 3 flash start = 0xbfc00000 offset =0x90000 flash length = 0x160000
| Flash area erase, writing ......   OK !!!!!
| Download buffer clearing   OK !!!!!!
+---------------------------------------------------------------+
Firmware upgrade procedure complete.
tftp> bye
AccessPoint>
```

(20) write config

In order to save new settings or firmware upgrades into the MW-1500AP(H)'s memory, you must type the command *write config* at the prompt after such actions.

Although the new configuration values have been saved into the MW-1500AP(H)'s memory with the *write config* command, they will not become effective until after you reboot the MW-1500AP(H). To reboot the MW-1500AP(H), type the command *reboot* at the prompt.

(21) wep

This command is used to configure the MW-1500AP(H)'s WEP (Wired Equivalent Privacy) function. The current configuration status of WEP can be verified by typing the command *show wep* at the prompt.

In order to control wireless access to the MW-1500AP(H), it must be configured to operate in either of two types of Authentication Algorithms: *Open System* and *Shared Key* (the factory default is *Open System*).

Open System: The Open System authentication is null authentication. The client can associate with any AP and listen to all data that are sent plaintext (non-encrypted). This is usually implemented where ease-of-use is the main issue, and the network administrator does not want to deal with security at all.

Shared Key: The Shared Key authentication approach provides a better degree of authentication than the Open System approach. For a client to utilize Shared Key authentication, it must implement WEP.

The following are the available commands.

***wep -o [enable/disable*]**: Enable/disable the MW-1500AP(H)'s WEP function.

wep -o [key1/key2/key3/key4] <xx xx xx xx xx>: Up to four default keys can be configured.

wep -o keylen [5/13]: Specifies the length of the WEP key to 5 or 13 bytes.

wep -o defaultkey <number>: Specifies which default key (1~4) will be used.

wep -o authtype <number>: Selects to use the Open System (1) or Shared Key (2) method of Authentication Algorithm.

wep -o intrablocking [enable / disable]: When set to *enable*, the MW-1500AP(H) will not allow different clients that are connected with the same MW-1500AP(H) to see each other.

APPENDIX A: ACRONYMS

AAA: Authentication, Authorization, Accounting
ADSL: Asymmetric Digital Subscriber Line
AP: Access Point
BSS: Basic Service Set
CCK: Complimentary Code Keying
CTS: Clear To Send
DBPSK: Differential Binary Phase Shift Keying
DC: Direct Current
DHCP: Dynamic Host Configuration Protocol
DMZ: Demilitarized Zone. In terms of this manual, DMZ means a neutral location where suspicious data coming from outside the network are sent.
DNS: Domain Name Service
DTIM: Delivery Traffic Indication Map
DQPSK: Differential Quadrature Phase Shift Keying
EAP: Extensible Authentication Protocol
ESSID: Extended Service Set Identity
GMT: Greenwich Mean Time
HTTP: Hypertext Transfer Protocol
IP: Internet Protocol
IAPP: Inter Access Point Protocol
ICMP: Internet Control Message Protocol
ID: Identity
IEEE: Institute of Electrical and Electronics Engineers
LAN: Local Area Network
LED: Light Emitting Diode
MAC: Media Access Control
MD: Message Digest
NAT: Network Address Translation
NAS: Network Access Server
PC: Personal Computer
PCMCIA: Personal Computer Memory Card International Association
PM: Power Management
POD: Power-off/Out-of-range/Detachment
PoE: Power over Ethernet
PPP: Point-to-Point Protocol
PPPoE: Point-to-Point Protocol over Ethernet
PS: Power Save
Q&A: Question & Answer
RADIUS: Remote Authentication Dial In User Service
RCV: Receive
RF: Radio Frequency
RTS: Request To Send
Rx: Receive
SNMP: Simple Network Management Protocol

SNTP: Simple Network Time Protocol
SSID: Service Set Identity
TCP: Transmission Control Protocol
TFTP: Trivial File Transfer Protocol
Tx: Transmit
UDP: User Datagram Protocol
USB: Universal Serial Bus
WAN: Wide Area Network
WEP: Wired Equivalent Privacy
WLAN: Wireless Local Area Network
XMIT: Transmit