
ShareTech AP-200

User Manual

Version 6.4.40

LAN 預設 IP 及帳密	
IP Address	192.168.1.21
Account / Password	admin / admin
Default 2.4GHz SSID	
Default SSID Name	AP-200
Security Account / Password	none

Contents

1. Introduction	3
2. Quick Setup Guide	3
3. Configuration Guide.....	7
4. Main Settings.....	8
5. Wireless Setup	10
6. Wireless Security	12
7. Network Settings	13
8. Wireless Advanced	16
9. Services	17
10. System	19

Introduction

This guide presents the description of the outdoor wireless CPE AP-200. AP-200 operates in IEEE 802.11a mode. The devices can operate in Client (Station), Access Point and WDS modes.

Quick Setup Guide

This Quick Setup Guide will guide you through quick and easy configuration of the subscriber station (client bridge) including:

- Changing of the IP settings (static or dynamic),
- Defining the SSID to which the subscriber station will be associated,
- Defining the IEEE 802.11 mode,
- Defining the wireless security (None, WEP, WPA™ or WPA2™),
- Changing the administrator's password.

For detailed setup and configuration instructions, please refer to the chapter *Configuration Guide*.

Follow these steps for subscriber station quick setup via web-browser interface:

Step 1 Login to the web management

Open the web browser and type the default IP address of the AP-200 device <http://192.168.1.21/> into the browser address field. You will be prompted to enter the administrator login credentials:

User Name: admin

Password: admin

After successful administrator log on you will see the main page of the subscriber station web management interface.

Step 2 Configure network settings

The IP configuration as described below is required for AP-200 management purposes. IP addresses can either be retrieved from a DHCP server or configured manually.

Use the Network menu to configure the IP settings:

Network Role

Network Mode: ▼

Disable Network: ▼

Network Settings

Bridge IP Address: DHCP Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Spanning Tree Protocol:

Auto IP Aliasing:

IP Aliases:

Network Mode: specify the *Bridge* operating mode (selected by default). Router operating mode configuration is described in the chapter 3 *Configuration Guide*.

Bridge IP Address: specify the IP mode:

DHCP – choose to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

Static – choose to assign a static IP address.

IP Address: enter IP address of the device.

Netmask: enter a subnet mask of the device.

Gateway IP: enter a Gateway IP address.

Primary DNS IP: enter a DNS IP address.
Click **Change** button to save the changes.

Step 3 Assign the SSID to subscriber station

Use **Wireless Setup** menu to specify the SSID of the wireless device (Access Point) to which the subscriber station will be associated:

The screenshot shows the 'Basic Wireless Settings' configuration page. A sidebar on the left contains navigation links: Main, **Wireless**, Network, Advanced, Services, System, and Logout. The main content area has the following settings:

- Wireless Mode: Access Point
- SSID: AP200 (highlighted with a red box) Hide SSID
- Country Code: Taiwan
- IEEE 802.11 Mode: B/G/N mixed
- Channel Width: Auto 20/40 MHz
- Frequency, MHz: Auto

Wireless Mode: specify the *Station WDS* wireless mode.

SSID: specify the SSID of the wireless network device which the AP-200 will be associated with. Refer to the section *Basic Wireless Settings* in the chapter *Wireless Setup* for more detailed configuration information.

Step 4 Specify the IEEE 802.11 mode

Specify the 802.11 wireless network mode by which the subscriber station will communicate with the wireless device:

The screenshot shows the IEEE 802.11 Mode configuration page with the following settings:

- Lock to AP MAC:
- Country Code: United States
- IEEE 802.11 Mode: A/N mixed
- Channel Width: Auto 20/40 MHz
- Frequency Scan List, MHz: Enabled
- Auto Adjust to EIRP Limit:
- Antenna Gain: 0 dBi
- Cable Loss: 0 dB
- Output Power: 27 dBm
- Max TX Rate, Mbps: MCS 15 - 130 [300] Automatic

IEEE 802.11 Mode: select the IEEE 802.11 mode of your wireless network. AP-200 supported IEEE 802.11 modes:

A/N – connect to a 802.11an network (selected by default).

Channel Spectrum Width: This is spectral width of the radio channel. Supported wireless channel spectrum widths:

- 5MHz – is the channel spectrum with the width of 5 MHz (known as Quarter-Rate mode).
- 10MHz – is the channel spectrum with the width of 10 MHz (known as Half-Rate mode).
- 20MHz – is the standard channel spectrum width (selected by default).
- 40MHz – the widest channel spectrum width required to connect to an 802.11a network which supports Static Turbo feature.

Notice:

Output Power: specify the output power (dBm) at which the wireless module is to

transmit data using the slider or entering the output power value manually. When using outdoors (open site), it is possible to use max output power (default): 27dBm; but, when using indoors for testing, must adjust the output power to below 20dBm to avoid saturation, which could influence the bandwidth and signal quality.

Data Rate: choose the data rate in Mbps at which the device should transmit wireless packets. If the device has trouble connecting or is losing data, then select “Auto”. This will automatically lower the data rates which will help alignment and successful linking.

Step 5 Specify the security mode

Choose the security method to protect your data to allow only authorized network users to access the network. You can choose **WEP**, **WPA**, **WPA2** or **None** security methods for your device.

If no security method is to be used, choose the **None** option (selected by default):

Wireless Security

Security: WEP

Authentication Type: Open Shared Key

WEP Key Length: 128 bit

WEP Key:

Key Type: HEX

Key Index: 1

Wireless Security

Security: WPA

WPA Authentication: PSK

WPA Preshared Key: Show

Security: select the security mode of your wireless network.

None – disable security.

WEP – enable WEP encryption.

WPA – enable WPA™i with Pre-shared Key encryption.

WPA2 – enable WPA2™ with Pre-shared Key encryption.

Authentication Type: choose one of the following authentication modes for WEP security method:

Open Authentication – station is authenticated automatically (more secure method).

Shared Authentication – station is authenticated after the challenge, generated

by AP (less secure method).

WEP Key Length: select the WEP Key length here, either 64-bit, or 128-bit.

Key Type: use the **HEX** or **ASCII** option to specify the character format for the WEP key.

WEP Key: enter the WEP encryption key to be used to encrypt and decrypt **Wireless traffic:**

For **64-bits** – specify pre-shared key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

For **128-bits** – specify pre-shared key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: specify the Index of the WEP Key used.

WPA Preshared Key: enter a passphrase for WPA™ or WPA2™ encryption. The preshared key is an alpha-numeric password between 8 and 63 characters long. Click **Change** button to save the changes.

Step 6 Change administrator password

For security reasons the default administrator's password should be changed immediately. Use the **System** menu and specify the parameters:

System Accounts

Administrator Username: 

Current Password:

New Password: Verify New Password:

Current Password: enter the current password (default administrators password is **admin**. (Default username is also **admin**)).

New Password: enter a new password value to be used for administrator authentication.

Verify Password: re-enter the new password to verify its accuracy. Click **Change** button to save the changes.

Step 7 Apply changes

After each configuration change, an informational message requesting application of the changes will appear:

Configuration contains changes. Apply these changes?

Network Role

Network Mode:

Disable Network:

Click **Apply** button to apply the changes and reboot the device.

Click **Discard** button to discard the changes.

Pop-up progress window will appear during the **Apply** operation:

Rebooting...

Device is rebooting, please stand by...

After the successful configuration of the general settings, the device is ready for basic operation. Web interface menu can be used for further device configuration. Please refer to the chapter *Configuration Guide* for detailed configuration instructions.

Configuration Guide

Each of the web management pages (listed below) contains parameters that affect a specific aspect of the device (see the relevant chapters below):

Main
Wireless Setup
Network
Wireless Advance
Services
System

Figure 1 – Configuration Management Menu

Main page displays current status of the device and the statistical information.

Wireless Setup page prepares the device for use in a wireless network, while covering basic wireless settings – i.e. controls how a subscriber station associates to an access point, authenticates to the wireless network, encrypts and decrypts data.

Network page covers the configuration of IP settings and network services (i.e. DHCP).

Wireless Advance page settings are dedicated for more precise wireless interface control. It also includes antenna polarity, traffic shaping and QoS settings.

Services page covers the configuration of system management services (i.e. SNMP, Ping Watchdog).

System page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

Main Settings

This page displays a summary of status information. It shows important information for the device operating mode and network settings as well as traffic statistics of the wireless and LAN interfaces.

In Access Point mode:

Figure 2 – Access Point mode

Status	
Device Name:	AP91
Network Mode:	Bridge
Wireless Mode:	Access Point WDS
SSID:	AP91
Security:	none
Version:	v6.0.3.oem
Uptime:	00:00:33
Date:	2011-12-07 01:12:30
Channel/Frequency:	161 / 5805 MHz
Channel Width:	40 MHz (Lower)
ACK/Distance:	43 / 1.5 miles (2.4 km)
TX/RX Chains:	2X2
WLAN MAC:	00:C0:CA:60:39:6E
LAN MAC:	00:C0:CA:60:39:6D
LAN:	100Mbps-Full
AP MAC:	00:C0:CA:60:39:6E
Connections:	0
Noise Floor:	-96 dBm
Transmit CCK:	-
TDMA:	Disabled

Base Station SSID: when operating in *Access Point* mode, displays the SSID of the device itself.

Frequency: displays the frequency used by device to transmit and receive data.

Channel: displays the channel used by device to transmit and receive data.

Security: displays the security method, which is set on the device.

ACK Timeout: displays current ACK Timeout value, which is set on the device manually or adjusted automatically.

Uptime: indicates the time, expressed in days, hours, minutes and seconds since last hard-reboot.

LAN Cable: displays the current status of the Ethernet port connection.

LAN MAC: displays the MAC address of the LAN (Ethernet) interface.

LAN IP Address: displays the current IP address of the LAN (Ethernet) interface while operating in *Router* mode.

WLAN IP Address: displays the current IP address of the WLAN (Wireless) interface while operating in *Router* mode.

Note: when operating in Bridge mode, the **LAN IP Address** and **WLAN IP Address** will display the same value – the current IP address of the virtual bridge interface.

Monitor

[Throughput](#) | [Stations](#) | [ARP Table](#) | [Bridge Table](#) | [Routes](#) | [Log](#)

IP Address	MAC Address	Interface
192.168.1.103	00:24:1D:13:73:55	BRIDGE

Figure 3 – Current Status of the system ARP tables

Tools: Use antenna alignment tool (see Figure 2) to adjust the device antenna to get better link with the wireless device. The antenna of wireless client has to be adjusted to get maximum signal strength. Click the **Align Antenna...** button and a new pop-up window with signal strength indicator will appear.

LAN Statistics: section displays detailed received and transmitted statistics (Bytes, Packets, Errors) of LAN (Ethernet) interface.

WLAN Statistics: section displays detailed received and transmitted statistics (Bytes, Packets, Errors) of wireless interface.

In Station Mode

Status	
Device Name:	AP91
Network Mode:	Bridge
Wireless Mode:	Station WDS
SSID:	AP91
Security:	none
Version:	v6.0.3.oem
Uptime:	00:02:13
Date:	2011-12-07 01:14:10
Channel/Frequency:	165 / 5825 MHz
Channel Width:	Auto 20 / 40 MHz
ACK/Distance:	43 / 1.5 miles (2.4 km)
TX/RX Chains:	2X2
WLAN MAC:	00:C0:CA:60:39:6E
LAN MAC:	00:C0:CA:60:39:6D
LAN:	100Mbps-Full
AP MAC:	Not Associated
Signal Strength:	-
Chain 0 / Chain 1:	0 / 0 dBm
Noise Floor:	-
Transmit CCQ:	-
TX/RX Rate:	- / -
TDMA:	-

Figure 4 – Station mode

Base Station SSID: when operating in Station mode, displays the SSID of the Access Point with which the device is associated.

AP MAC: displays the MAC address of the Access Point with which the device is associated while operating in *Station* mode.

Signal Strength, dBm: displays the received signal level (client-side) while operating in *Station* mode. The represented value coincides with the graphical bar.

TX Rate: displays the current data transmission rate while operating in *Station* mode.

RX Rate: displays the current data reception rate while operating in *Station* mode.

Transmit CCQ: displays the transmit successful rate. Just for reference.

QoS Status: displays the QoS Status, which is set on the device.

Uptime: indicates the time, expressed in days, hours, minutes and seconds since last hard-reboot.

Wireless Setup

The **Wireless Setup** page allows you to manage general wireless connection parameters of the device.

Basic Wireless Settings

The general wireless settings, such as wireless device SSID, country code, output

power, 802.11 mode and data rates can be configured in this section:

Basic Wireless Settings

Wireless Mode: [?] Access Point WDS Auto

WDS Peers:

SSID: AP91 Hide SSID

Country Code: United States

IEEE 802.11 Mode: A/N mixed

Channel Width: [?] 40 MHz

Frequency, MHz: Auto

Extension Channel: None

Frequency List, MHz: Enabled

Auto Adjust to EIRP Limit:

Antenna Gain: 0 dBi Cable Loss: 0 dB

Output Power: 27 dBm

Max TX Rate, Mbps: MCS 15 - 300 Automatic

Figure 5 – Basic Wireless Settings

Wireless Mode: specify the operating mode of the device. The mode depends on the network topology:

Station – in this mode the device acts as Subscriber Station, while connecting to Access Point defined by SSID.

Station WDS – in this mode the device acts as Subscriber Station, while connecting to Access Point using the WDS protocol.

Access Point – in this mode the device acts as Access Point.

Access Point WDS – in this mode the device acts as Access Point with the WDS protocol support.

Station - Bridge mode has pass-through restrictions for Layer2 protocols while it is transparent for DHCP and PPPoE protocols.

Station WDS - Bridge mode is transparent for all the Layer2 protocols. Refer to the section *Network Settings* for detailed *Bridge* network mode configuration information.

SSID/ESSID:

While operating in *Access Point* mode, specify the SSID of the device itself.

While operating in *Station* mode, specify the ESSID of the Access Point with which the device will be associated.

Hide SSID: selected control will disable broadcasting of the SSID to wireless stations. Unselected control will make SSID visible during network scans on the wireless stations. Control is available while operating in *Access Point* mode.

Country Code: choose from drop-down list the country in which you will use the device.

IEEE 802.11 Mode: select the IEEE 802.11 mode of your wireless network.
AP-200 supported IEEE 802.11 modes:

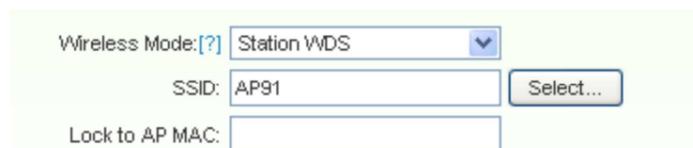
A – connect to a 802.11a network (selected by default).

Channel Spectrum Width: choose the channel width (**40 Mhz/Turbo**, **20 Mhz/Full Rates**, **10 MHz/Half Rates** or **5 MHz/Quarter Rates**) which will be utilized for data transmission.

Channel: select the operating channel while operating in *Access Point* mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected **country code** and **IEEE** mode.

Output Power: specify the output power (dBm) at which the wireless module is to transmit data using the slider or entering the output power value manually. When using outdoors (open site), it is possible to use max output power (default): 27dBm; but, when using indoors for testing, adjust the output power to below 20dBm to avoid saturation, which could influence the bandwidth and signal quality.

Data Rate: choose the data rate in Mbps at which the device should transmit wireless packets. If the device has trouble connecting or is losing data, then must select “Auto”. This will automatically lower the data rates which will help alignment and successful linking.



The screenshot shows a configuration window with a light green background. It contains three main input areas: a dropdown menu for 'Wireless Mode' currently set to 'Station WDS', a text field for 'SSID' containing 'AP91' with a 'Select...' button to its right, and a text field for 'Lock to AP MAC' which is currently empty.

Figure 6 – Locking the Station to Access Point specified by MAC

Use the **Select...** button next to **ESSID** entry field to load the **Site Survey** tool in pop-up window while operating in *Station* mode. Site Survey will search for all wireless networks in range and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in the wireless security section.

Site Survey

Scanned Frequencies:
5.745GHz 5.765GHz 5.785GHz 5.805GHz 5.825GHz

MAC Address	SSID	Device Name	Encryption	Signal / Noise, dBm	Frequency, GHz	Channel
<input type="button" value="Scan"/>						

Figure 7 – Site Survey Scan

Select the Access Point from the list and click **Select** button for association. Click **Scan** button to refresh the list of available wireless networks.

Close this window button closes Site Survey window.

Wireless Security

This section enables you to set parameters that control how the subscriber station associates to a wireless device and encrypts/decrypts data:

Wireless Security

Security: ▼

WPA Authentication: ▼

WPA Preshared Key: Show

Figure 8 – Wireless Security Settings

Security: select the security mode of your wireless network.

None – disable security.

WEP – enable WEP encryption.

WPA – enable WPA™ with Pre-shared Key encryption.

WPA2 – enable WPA2™ with Pre-shared Key encryption.

WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by

encrypting data being transferred over your wireless network. Enable WEP security:

Wireless Security

Security: WEP

Authentication Type: Open Shared Key

WEP Key Length: 64 bit

WEP Key:

Key Type: HEX

Key Index: 1

Figure 9 – Configuration of the WEP

Authentication Type: choose one of the following authentication modes for WEP security method:

Open Authentication – station is authenticated automatically.

Shared Authentication – station is authenticated after the challenge, generated by AP.

WEP Key Length: select the WEP Key length here, either **64-bit**, or **128-bit** (stronger).

Key Type: use the **HEX** or **ASCII** option to specify the character format for the WEP key.

WEP Key: enter the WEP key for wireless traffic encryption/decryption:
For **64-bits** – specify pre-shared key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.
For **128-bits** – specify pre-shared key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: select the Index of the WEP Key used.

WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods. WPA™ and WPA2™ support the following ciphers for data encryption:

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm. The device will use the strongest cipher (CCMP) in *Station* and *Access Point* wireless mode by default. If CCMP is not supported on the other side of the link the TKIP encryption will be used – such as in situations where the device acts as Access Point with WPA security enabled and at least one wireless station (without CCMP support) is connected to it. Enable WPA2™ (RSN) security:

Wireless Security

Security: WPA2
WPA Authentication: PSK
WPA Preshared Key: Show

Figure 10 – WPA Security Settings

WPA Preshared Key: enter a passphrase for WPA™ or WPA2™ encryption. The pre-shared key is an alpha-numeric password between 8 and 63 characters long. Click **Change** button to save the changes.

Network Settings

AP-200 can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the **Network** menu to configure the IP settings:

Network Role

Network Mode: Bridge
Disable Network: None

Network Settings

Bridge IP Address: DHCP Static
IP Address: 192.168.1.21
Netmask: 255.255.255.0
Gateway IP: 192.168.1.1
Primary DNS IP:
Secondary DNS IP:
MTU: 1500
Spanning Tree Protocol:
Auto IP Aliasing:
IP Aliases:

Figure 11 – Bridge mode Network Settings

Network Mode: specify the operating network mode for the device. The mode depends on the network topology:

Bridge operating mode is selected by default as it is widely used by the subscriber stations while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet. Router mode will block broadcasts while it is not transparent. The device can act as DHCP server and use Network Address Translation (Masquerading) feature in router mode which is widely used by the Access Points.

Bridge IP Address: specify the IP mode:

DHCP – choose to assign the dynamic IP settings by the DHCP server.

Static – choose to assign a static IP address.

IP Address: enter IP address of the device.

Netmask: enter a subnet mask of the device.

Gateway IP: enter a Gateway IP address.

Primary DNS IP: enter a DNS IP address.

Network Role

Network Mode: Router

Disable Network: None

WLAN Network Settings

WLAN IP Address: DHCP PPPoE Static

IP Address: 0.0.0.0

Netmask: 255.255.255.0

Gateway IP: 192.168.1.1

Primary DNS IP:

Secondary DNS IP:

MTU: 1500

Enable DMZ:

Auto IP Aliasing:

IP Aliases:

Change MAC Address:

LAN Network Settings

IP Address: 0.0.0.0

Netmask: 255.255.255.0

Enable NAT:

MTU: 1500

Enable DHCP Server:

Port Forwarding:

Auto IP Aliasing:

IP Aliases:

Figure 11 – Router mode Network Settings

There are two network segments (**WLAN** and **LAN**) configured separately when device

is operating in **Router** mode.

Wireless network segment can be configured in **WLAN Network Settings** section:

IP Address: enter IP address of the WLAN interface.

Netmask: enter a subnet mask of the WLAN interface.

Enable NAT: control will enable Network Address Translation (Masquerading) feature between WLAN and LAN interfaces.

Enable DHCP Server: control will enable DHCP Server feature on WLAN interface. The DHCP options should be configured while **DHCP Server** is enabled:

Range Start: Enter the IP address that begins the range of IP address space

reserved for DHCP.

Range End: Enter the IP address that ends the range of IP address space reserved for DHCP.

Netmask: Enter the subnet mask of IP address space reserved for DHCP.

Lease Time: Enter the lease period (in seconds) during which DHCP guarantees that the IP address assigned to one particular client is not reassigned to another client. LAN (Ethernet) connection settings can be configured in **LAN Network**

Settings section which is identical to the bridge mode Network Settings section described above. LAN IP settings can be assigned automatically using the **DHCP** or **PPPoE**. If **PPPoE** mode is selected, the **Username** and **Password** credentials are required for PPPoE authentication. Click **Change** button to save the changes.

Wireless Advanced

The **Wireless Advanced** options page allows you to manage advanced settings that influence the device's performance and behavior.

Excepting the Distance setting, the advanced wireless settings are designed for more technically advanced users who have sufficient knowledge of wireless LAN technology. These settings should not be changed unless the user knows what effect the changes will have on the device.

Advanced Wireless Settings

RTS Threshold: Off

Fragmentation Threshold: Off

Distance: miles (2.4 km)

ACK Timeout: Auto Adjust

Aggregation: Enable

Frames Bytes

Multicast Data: Allow All

Enable Installer EIRP Control:

Enable Extra Reporting:

Sensitivity Threshold, dBm: Off

Figure 12 – Advanced Wireless Settings

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word “off”. The default value is 2347 which means that RTS is disabled.

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word “off”. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended while default setting of 2346 should remain in most cases.

Distance: The distance value should be adjusted during installation. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance as this will enhance performance and provide the best signal quality and bandwidth.

ACK Timeout: specify the ACK Timeout (20-520). This is the amount of time the subscriber station will wait to hear a acknowledgement response from the wireless device after the data packet is transmitted. If the timeout is set too short or too long, it will result poor connection and throughput performance. Changing the ACK Timeout value will change the **Distance** to the appropriate distance value for the ACK Timeout.

Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above.

Signal LED Thresholds

	LED1	LED2	LED3	LED4
Thresholds, dBm:	- 94	- 80	- 73	- 65

Figure 13 – RSSI LED Thresholds Configuration

RSSI LED Thresholds specify the marginal value of RSSI which will switch on LEDs indicating signal strength:

Configuration example: if the Signal Strength (displayed in the Main page) fluctuates around -63 dBm, the LED Thresholds can be set to the values -70, -65, -62, -60. Note: sign "-" character should not be used for the Signal Strength value specification.

Wireless Traffic Shaping

Wireless Traffic shaping feature is dedicated for upstream and downstream bandwidth control while looking from the client (connected on Ethernet interface) perspective.

Traffic Shaping

Enable Traffic Shaping:	<input checked="" type="checkbox"/>
Incoming Traffic Limit:	512 kbit/s
Incoming Traffic Burst:	0 kBytes
Outgoing Traffic Limit:	512 kbit/s
Outgoing Traffic Burst:	0 kBytes

Figure 14 – Wireless Traffic Shaping Setup

Enable Traffic Shaping: control will enable bandwidth control on the device.

Incoming Traffic Limit: specify the maximum bandwidth value in kbps for traffic passing from wireless interface to Ethernet interface.

Outgoing Traffic Limit: specify the maximum bandwidth value in kbps for traffic passing from Ethernet interface to wireless interface.

Services

This page covers the configuration of system management services SNMP and Ping Watchdog.

Ping Watchdog : Ping Watchdog is dedicated to continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP

“echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Traffic Shaping

Enable Traffic Shaping:

Incoming Traffic Limit: kbit/s

Incoming Traffic Burst: kBytes

Outgoing Traffic Limit: kbit/s

Outgoing Traffic Burst: kBytes

Figure 16 – Ping Watchdog configuration

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

IP Address To Ping: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

Ping Interval: specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool.

Startup Delay: specify initial time delay (in seconds) until first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Failure Count To Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Traffic Shaping

Enable Traffic Shaping:

Incoming Traffic Limit: kbit/s

Incoming Traffic Burst: kBytes

Outgoing Traffic Limit: kbit/s

Outgoing Traffic Burst: kBytes

Figure 17 – SNMP Agent Configuration

Enable SNMP Agent: control will enable SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access.

Contact: specify the identity or the contact who should be contacted in case an emergency situation arises.

Location: specify the physical location of the device.

System

This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.

Firmware

Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. When the device is updated with a newer version or the same version firmware builds, system configuration will be preserved.

Device Maintenance

Firmware Version: AP91.v6.0.3.oem.9036

Figure 18 – Firmware Upgrade. Step 1

Firmware version: displays version of the current firmware.

Upgrade...: click to load the device firmware upgrade window.

Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations.



The screenshot shows a configuration window with a light green header labeled "Device". Below the header, there is a text input field labeled "Device Name:" containing the text "AP91".

Figure 19 - Host Name Configuration

Host Name: specify the system identity. Click **Change** button to save the changes.

Administrative Account

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first setup:



The screenshot shows a configuration window with a light green header labeled "System Accounts". Below the header, there are four input fields: "Administrator Username:" with the value "admin" and a key icon; "Current Password:" which is empty; "New Password:" which is empty; and "Verify New Password:" which is empty.

Figure 20 - Change Administrator Settings

Administrator Username: displays name of the system user. The username is not a configurable parameter, so it cannot be changed.

Current Password: enter the current password value. Default administrator login credentials:

User Name: **admin**

Password: **admin**

New Password: enter a new password value used for administrator authentication.

Verify Password: re-enter the new password to verify its accuracy. Click **Change** button to save the changes.

Configuration Management

AP-200 configuration is stored in plain text file. Use the **Configuration Management** section controls to manage (backup, restore/update) system

configuration file:

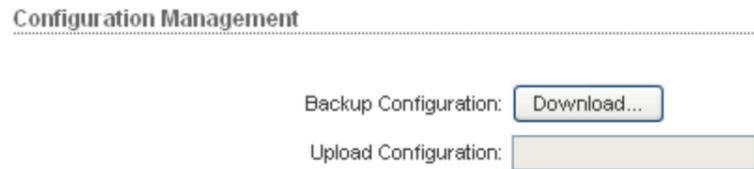


Figure 21 – Configuration Management

Backup Configuration: click **Download...** button to download the current system configuration file.

Upload Configuration: click **Browse...** button to navigate to and select the new configuration file or specify the full path and click the **Upload** button.

Device Maintenance

Use this section to reboot device or reset all the system parameters to factory default values:



Figure 22 – Device Maintenance Settings

Reboot: click to hard-reboot the device in the current configuration. Any non-applied changes will be lost.

Reset to Defaults: click to reset the device to factory defaults.

Support Info: activate Support Info button in order to get system information file.

FAQ

1. Why the bandwidth is much lower while we test AP-200 indoor?

Ans> It caused by the signal saturation happen, please adjust below configurations:

In Basic wireless settings

Output Power: specify the output power (dBm) at which the wireless module is to transmit data using the slider or entering the output power value manually. When using outdoors (open site), it is possible to use max output power (default): 27dBm; but, when using indoors for testing, must adjust the output power to below 20dBm to avoid saturation, which could influence the bandwidth and signal quality.

Data Rate: choose the data rate in Mbps at which the device should transmit wireless packets. If the device has trouble connecting or is losing data, then select "Auto". This will automatically lower the data rates which will help alignment and successful linking.

In Advanced wireless settings

Distance: specify the real testing distance

2. How to optimize the performance outdoor?

Ans>

In Basic wireless settings

Wireless mode: specify "Access Point WDS" or "Station WDS", in WDS mode, it runs proprietary protocol, AP-200 system only could connect AP-200 system. It's performance is better than general mode "AP mode" and "Station mode" while it could connect other band system.

Output Power: specify the max output power (default): 27dBm

Data Rate: select "Auto"

In Advanced wireless settings

Distance: specify the real transmit distance

3. How to optimize AP-200 Wireless Link Quality in point to Multiple point application?

Ans>

While using point to Multiple point application, in order to decrease the hidden node impact to make system best performance, please follow below configuration:

About AP side configuration

Main
Wireless Setup
Network
Wireless Advance
Services
System

BASIC WIRELESS SETTINGS

Wireless Mode: 1 Auto

WDS Peers:

SSID: Hide SSID

Country Code:

IEEE 802.11 Mode:

Channel Spectrum Width: 2 Max Datarate: 54Mbps

Channel:

Output Power: 3 dBm

Data Rate, Mbps: 4 Auto

1. Choose AP+WDS to enable “transparent bridge”
2. Choose 20Mhz for PtMP.
3. Choose maximum output power 27dbm for outdoor
4. Chose maximum data rate and check “auto” tag

Main
Wireless Setup
Network
Wireless Advance
Services
System

ADVANCED WIRELESS SETTINGS

Rate Algorithm: 5

Noise Immunity: Enabled

RTS Threshold: 6 Off

Fragmentation Threshold: Off

Distance: 7 miles (0.6 km)

ACK Timeout: Auto Adjust

SuperAG Features: 8 Fast Frame Bursting Compression

Multicast Data: 9 Allow All

Multicast Rate, Mbps: 10

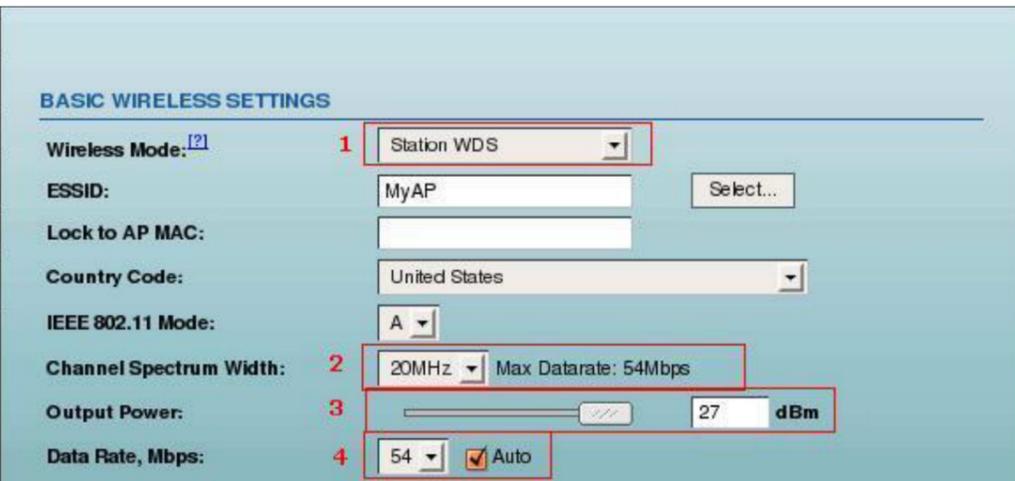
Enable Extra Reporting:

Enable DFS:

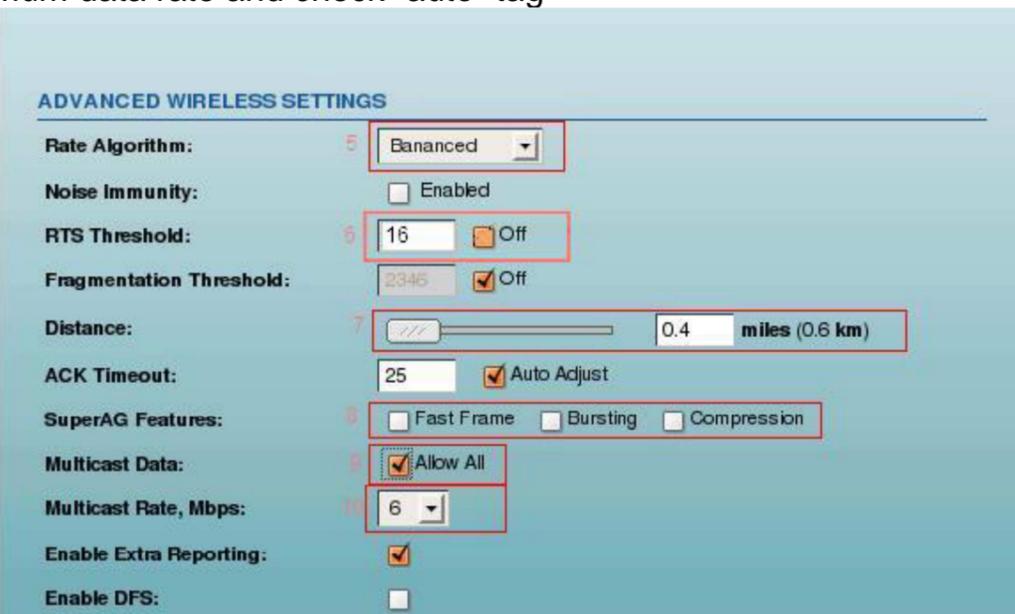
Enable Client Isolation:

5. Choose “Balanced” algorithm for outdoor
6. RTS Threshold: open CTS/RTS, and specify “16”
7. Choose the distance. (distance = client num x client distance.)
8. Disable “Fast Frame” and “Bust” for reducing hidden node effect
9. Enable “Allow All” to transmit all layer2 packet
10. Chose “6Mbps” to increase multicast packet receive successful probability

About Station Side configuration

Main	
Wireless Setup	
Network	
Wireless Advance	
Services	
System	

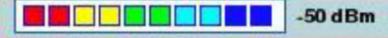
1. Choose “station+WDS” to enable “transparent bridge” and turn off “NAT 2.5” to increase packet forwarding rate
2. Choose 20Mhz for PtMP.
3. Choose maximum output power 27dbm for outdoor
4. Chose maximum data rate and check “auto” tag

Main	
Wireless Setup	
Network	
Wireless Advance	
Services	
System	

5. Choose “Balanced” algorithm for outdoor
6. RTS Threshold: open CTS/RTS, and specify “16”
7. Choose the distance (distance = client num x client distance.)
8. Disable “Fast Frame” and “Bust” for reducing hidden node effect
9. Enable “Allow All” to transmit all layer2 packet
10. Chose “6Mbps” to increase multicast packet receive successful probability

About Station Side CCQ/Signal Strength configuration

Main	
Wireless Setup	
Network	
Wireless Advance	
Services	
System	

Base Station SSID:	MyAP	AP MAC:	00:26:48:56:00:2B
Signal Strength:			
TX Rate:	48 Mbps	RX Rate:	48 Mbps
Frequency:	5180 MHz	Channel:	36
Security:	none	ACK Timeout:	25
Transmit CCQ:	88.8%	QoS Status:	No QoS
Uptime:	3 day(-s) 21:18:05	Date:	2011-04-06 21:51:01
LAN Cable:	OFF	Host Name:	AP4
LAN MAC:	00:26:48:5A:00:80	LAN IP Address:	192.168.1.21
WLAN MAC:	00:26:48:5A:00:81	WLAN IP Address:	192.168.1.21
Extra info:	----	Tools:	----

1. Signal strength: the bigger the better ex: -51dBm is better than -78dBm
2. CCQ: Transmit successful rate. The larger, the better ex: 100% is better than 50%
3. If Signal strength is high but CCQ is low decrease the tx power ex: signal strength is -20dBm, CCQ is 20%
4. If Signal strength is low and CCQ is low increase the tx power and align antenna ex: signal strength is -85dBm, CCQ is 10%