康景科技有限公司
CONJING NETWORKS INC.

CJM210EC/CJM210ECI

802.11 b/g/n High Performance Embedded WiFi Module User Guide

Ver. 1.1

Revision History

Revision	Date	Description
1.0	October 2015	Initial release
1.1	November 2015	Add FCC warning statement

1. General Description

The CJM210EC/CJM210ECI WiFi module provides quick, easy and cost effective way to enable WiFi connectivity for all kinds of products. The module is based on single chip Atheros AR9341 which is a highly integrated IEEE 802.11n 2.4 GHz SoC. The CJM210EC/CJM210ECI supports radio data rate up to 150 Mbps. Besides, the module is integrated with 8MB flash and 32 MB DDR1 RAM and support rich I/O interfaces for variety of applications.

2. Hardware Features

2.1 Module SKUs

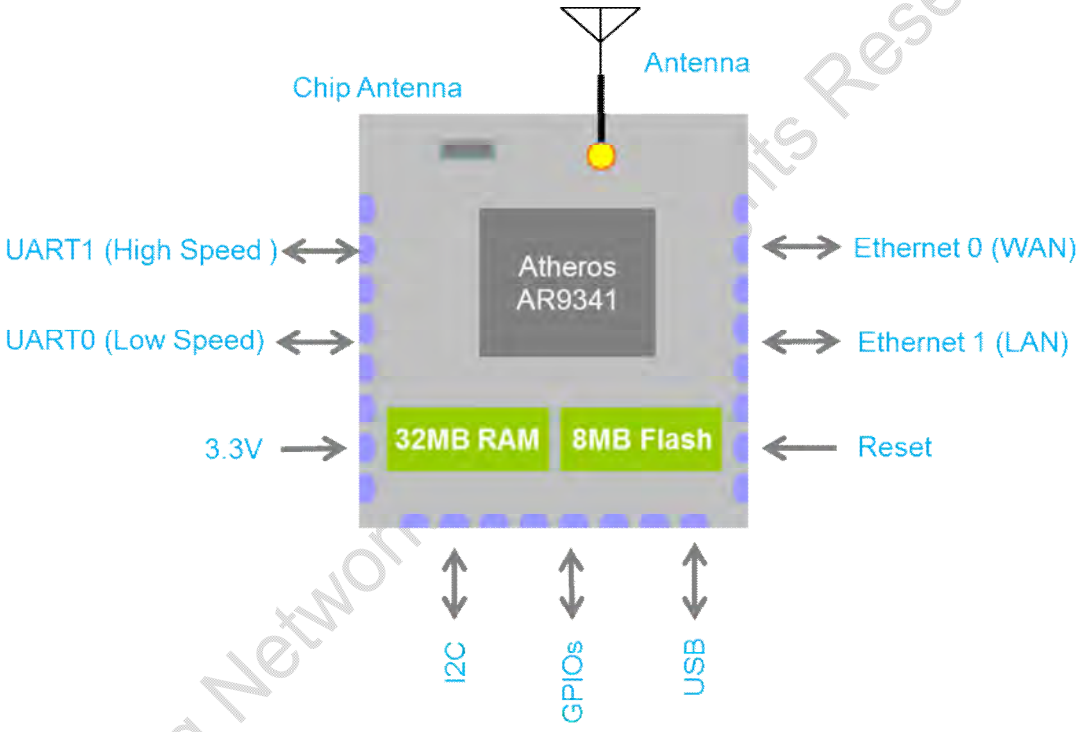
Model Name	Radio	Antenna Option
CJM210EC	802.11 b/g/n 1T1R	1 MMCX port / Chip antenna
CJM210ECI	802.11 b/g/n 1T1R	1 IPEX port / Chip antenna

2.2 Hardware Specification

RF characteristics	
Standard	IEEE 802.11 b/g/n 1x1
Operating Frequency	2.412 GHz ~ 2.484 GHz
Supported Data Rates	• 802.11n: 6.5Mbps ~ 75Mbps (CJM210EC) 6.5Mbps ~ 144.4Mbps (CJM220E) • 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps • 802.11b: 1, 2, 5.5, 11 Mbps
Transmit Power (Typical) (±2 dBm)	• 802.11b: 18dBm • 802.11g: 18dBm@6Mbps, 13dBm@54Mbps • 802.11n: 17dBm@MCS0, 12dBm@MCS7
Receiver Sensitivity	• 802.11b: -93dBm • 802.11g: -90dBm@6Mbps, -75dBm@54Mbps • 802.11n: -90dBm@MCS0, -71dBm@MCS7
Antenna Options	On-board chip antenna or MMCX/IPEX connector for external antenna
Hardware Characteristics	
Chipset	Qualcomm Atheros AR9341 SoC, MIPS74Kc processor up to 533 MHz
Memory	Flash: 8 MB nor flash, RAM: 32 MB DDR1
I/O Interfaces	• Low speed UART x 1: up to 115.2 Kbps

	• High speed UART x 1: up to 3Mbps with RTS/CTS flow control • Ethernet x 2, I^2C x 1, USB x 1, GPIOs
Operating Temperature	-40℃ ~ 70℃
Storage Temperature	-40℃ ~ 85℃
Power source	3.3 V DC
Dimension	47(l) mm x 33(w) mm x 8(h) mm

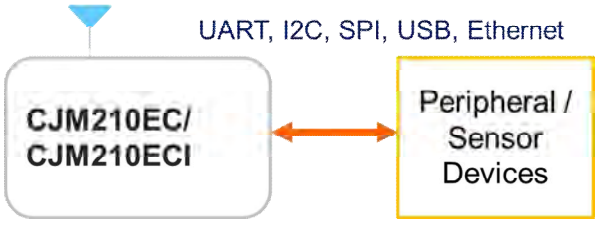
2.3 Block Diagram



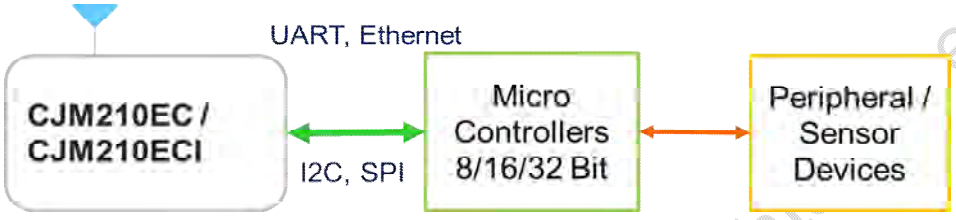
2.4 Embedded System Design

The modules support two integrated methods for embedded system, and user can depend on their product design to integrate with the WiFi module:

- Integrate with peripheral or sensor devices.

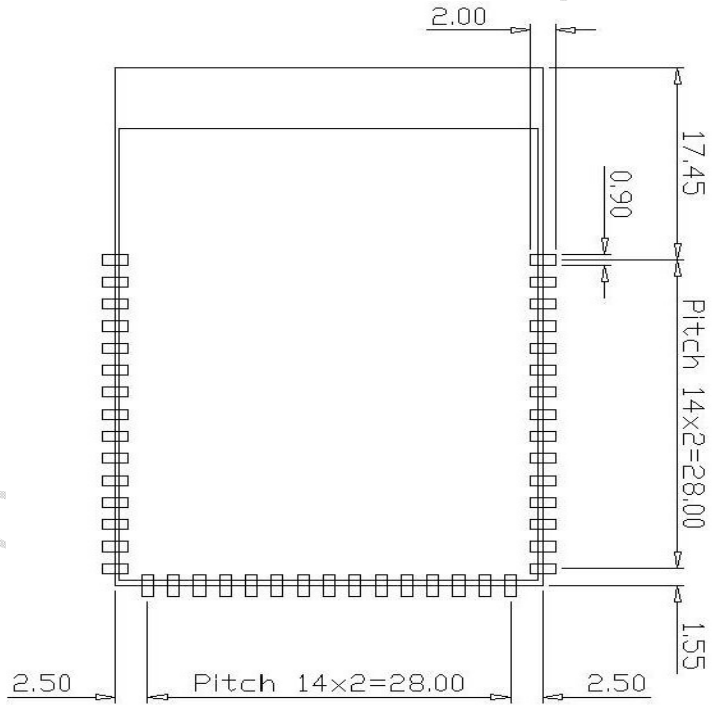


- Connect to another MCU

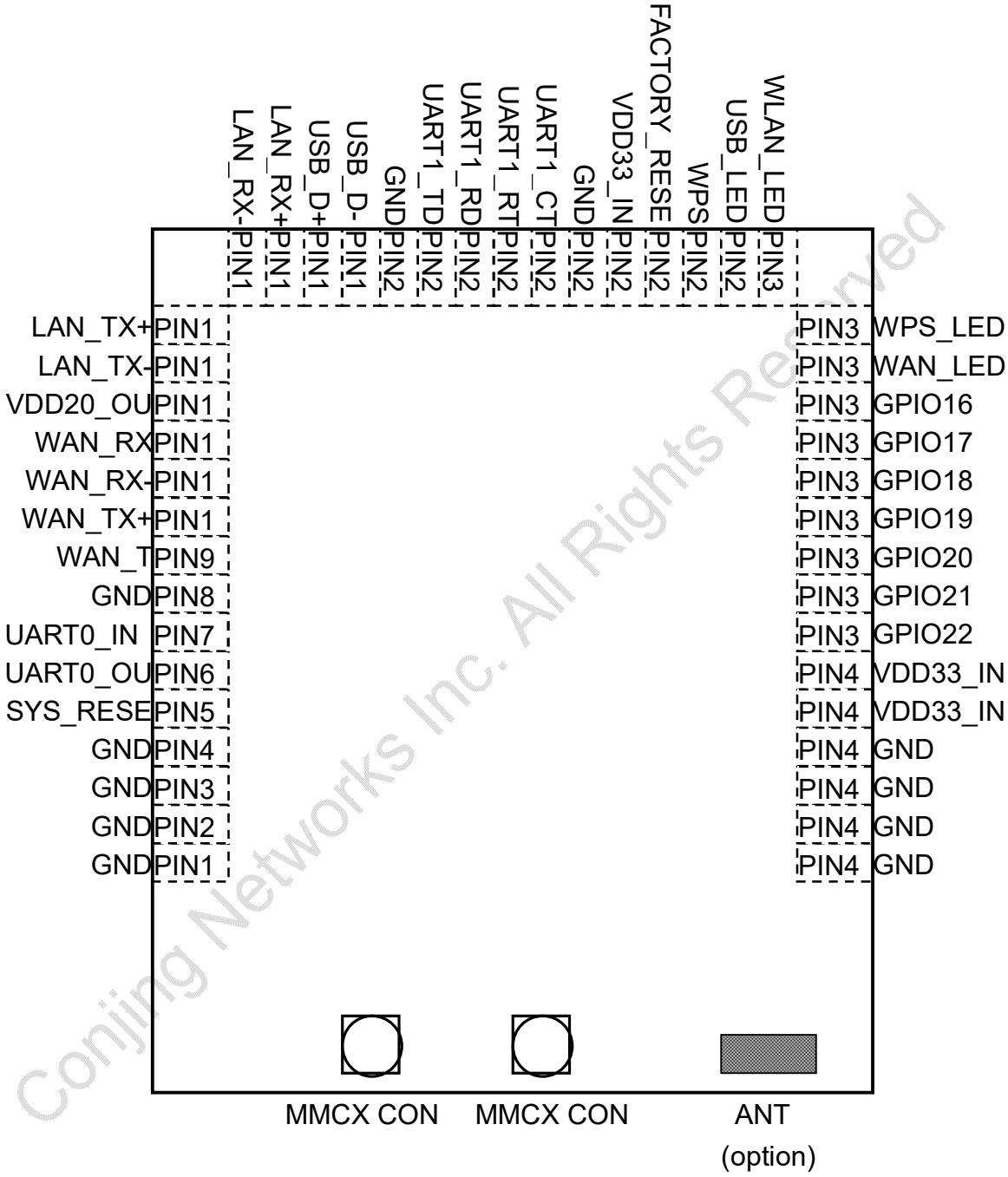


2.5 Module Dimensions

Unit: mm



2.6 Pinout and Signal Description



TOP VIEW

Pins Description

Pins	Name	Description	Note
1	GND	Ground	
2	GND	Ground	
3	GND	Ground	
4	GND	Ground	
5	SYS_RESET	Hardware reset	
6	UART0_OUT	Low speed UART serial out	Can be configured as GPIO function.
7	UART0_IN	Low speed UART serial in	
8	GND	Ground	
9	WAN_TX-	Ethernet0 Tx-	
10	WAN_TX+	Ethernet0 Tx+	
11	WAN_RX-	Ethernet0 Rx-	
12	WAN_RX+	Ethernet0 Rx+	
13	VDD20_OUT	2.0 V supply out	
14	LAN_TX-	Ethernet1 Tx-	
15	LAN_TX+	Ethernet1 Tx+	
16	LAN_RX-	Ethernet1 Rx-	
17	LAN_RX+	Ethernet1 Rx+	
18	USB_D+	USB D+ signal; carries USB data to and from the USB2.0 PHY	
19	USB_D-	USB D- signal; carries USB data to and from the USB2.0 PHY	
20	GND	Ground	
21	UART1_TD	High speed UART transmit data	Can be programmed to be GPIO function.
22	UART1_RD	High speed UART receive data	
23	UART1_RTS	High speed UART request to send	
24	UART1_CTS	High speed UART clear to send	
25	GND	Ground	
26	VDD33_IN	3.3 V supply input	
27	FACTORY_RESET	Restore system configuration to facroty default value	Can be programmed to be GPIO function. Open drain
28	WPS	WPS(WiFi Proected Setup) function	Can be programmed to be GPIO function.
29	USB_LED	USB LED	Can be programmed to be GPIO function.

30	WLAN_LED	WLAN LED	Can be programmed to be GPIO function.
31	WPS_LED	WPS LED	Can be programmed to be GPIO function.
32	WAN_LED	Ethernet0 LED	Can be programmed to be GPIO function.
33	GPIO16	GPIO pin	Open drain
34	GPIO17	GPIO pin	Open drain
35	GPIO18	GPIO pin	
36	GPIO19	GPIO pin	
37	GPIO20	GPIO pin	
38	GPIO21	GPIO pin	
39	GPIO22	GPIO pin	
40	VDD33_IN	3.3 V supply input	
41	VDD33_IN	3.3 V supply input	
42	GND	Ground	
43	GND	Ground	
44	GND	Ground	
45	GND	Ground	

NOTE: The I^2C interface can be supported by programming GPIO control and multiplexing.

GPIO Electrical Characteristics

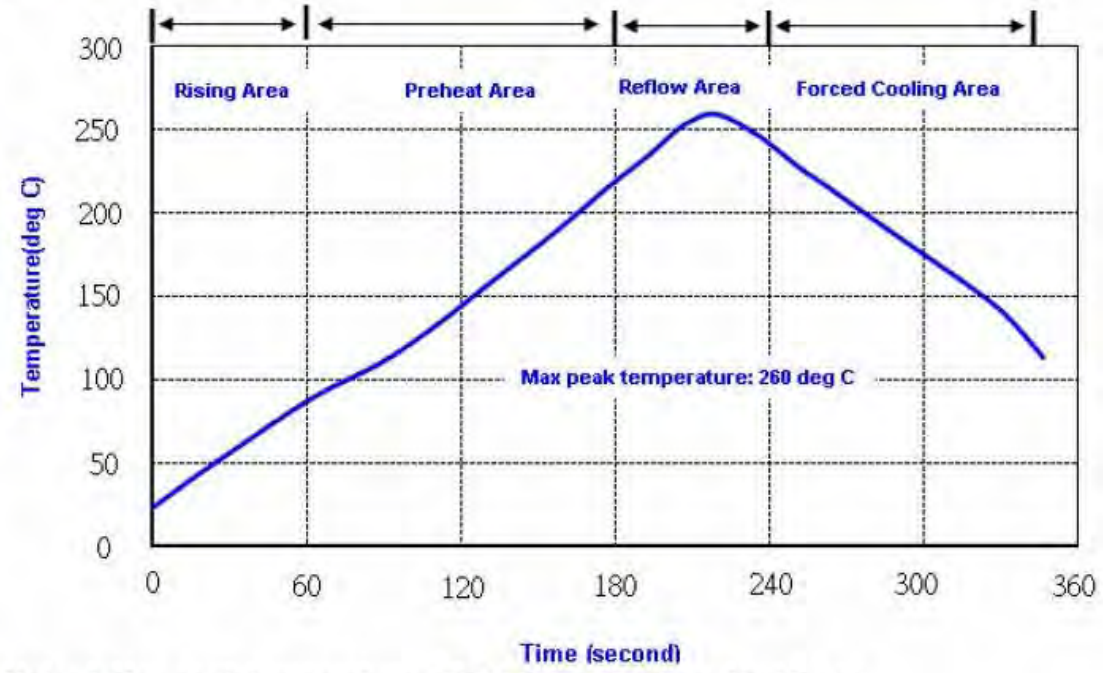
Symbol	Parameter	Min.	Max.	Unit
V_{IH}	High Level Input Voltage	1.8	2.8	V
V_{IL}	Low Level Input Voltage	-0.3	0.3	V
V_{OH}	High Level Output Voltage	2.2	2.8	V
V_{OL}	Low Level Output Voltage	0	0.4	V
I_{IL}	Low Level Input Current	-	15	μA
I_{OH}	High Level Output Current	-	8	mA
V_{IH}	High Level Input Voltage (GPIO11, GPIO16, GPIO17)	2.4	3.6	V
V_{IL}	Low Level Input Voltage (GPIO11, GPIO16, GPIO17)	-0.3	0.3	V
V_{OH}	High Level Output Voltage (GPIO11,GPIO16, GPIO17)	2.4	3.6	V
V_{OL}	Low Level Output Voltage (GPIO11, GPIO16, GPIO17)	0	-	V
I_{IL}	Low Level Input Current (GPIO11, GPIO16, GPIO17)	-	7	μA

2.7 Manufacturing Process Recommendations

The second wave soldering process depends on external factors like the choices of baseboard, soldering paste, size and thickness, etc. Exceeding the recommended

soldering temperature and time in this profile may damage the module permanently.

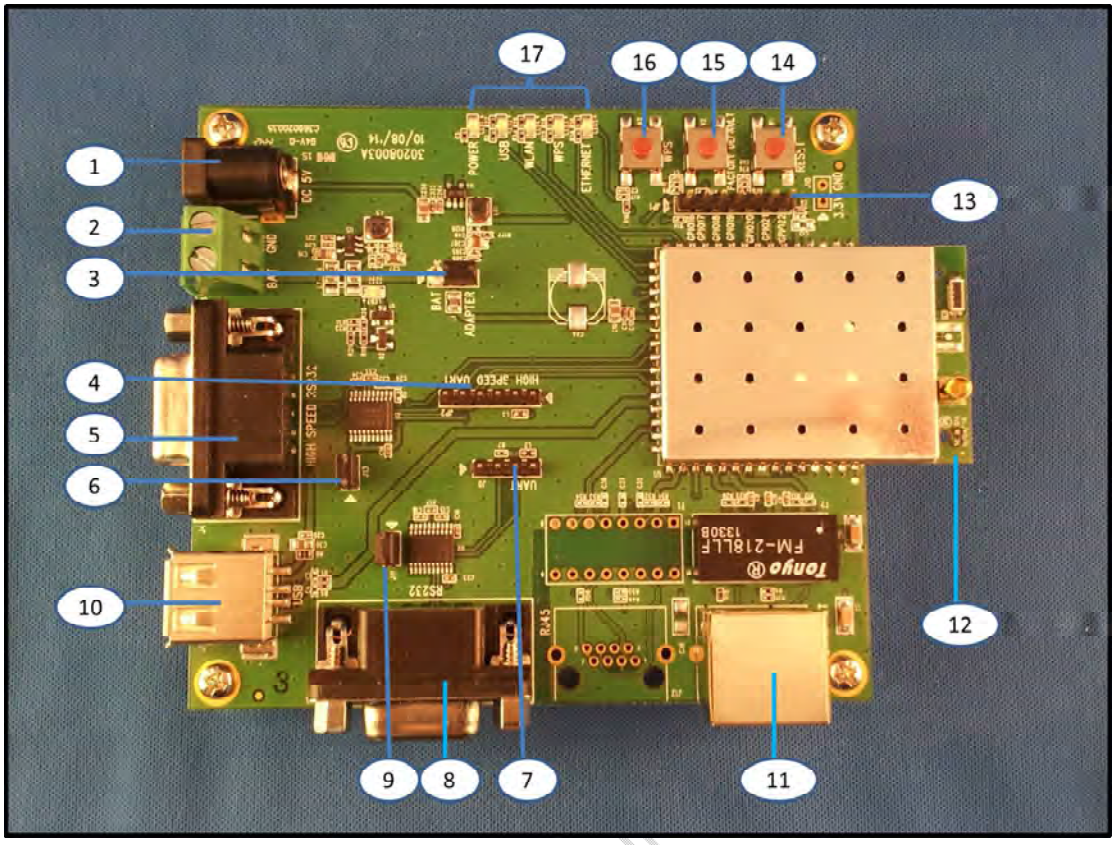
Reflow Profile:



Note: 1.Max peak temperature: 260+/-5 deg C; Time: 10+/-2 sec
2. Temperature: 217+/-5 deg C; Time: 90~100 sec

3. Evaluation Board

The CJM200-EVK evaluation board is used to evaluate the module functions and for the hardware reference design to integrate the module.



Where:

1	DC power connector (5V DC)	10	USB 2.0 for mass storage
2	Battery power connector (3.3V)	11	10/100 Mbps fast Ethernet
3	Power source switch	12	CJM210EC/CJM220E WiFi module
4	High speed UART	13	GPIOs Header
5	High speed RS232	14	Reset push button
6	High speed UART/RS232 switch	15	Factory default push button*
7	Low speed UART	16	WPS push button
8	Low speed RS232	17	LEDs
9	Low speed UART/RS232 switch		

NOTE: You have to press Factory default push button over 5 seconds to revert to factory default settings and reboot, otherwise it will act as Reset push button.

3.1 Switch Configuration

3.1.1 Power source switch

The power source switch is used to decide the power source supply is from DC or battery by jumper. The battery power only supplies to WiFi module, and the DC power supplies to the whole board.

3.1.2 UART/RS232 switch

Both high speed and low speed UART/RS232 switches are to enable UART or RS232 interface. If the jumper is used to connect switch header, the RS232 is enabled, otherwise the UART is enabled.

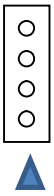
3.2 COM port configuration

The reference board supports two COM ports. The low speed UART/RS232 is used for console, and the high speed UART/RS232 is used for data transfer to WiFi or Ethernet. Please notice that the RS232 connection cable is not null modem.

3.2.1 Low speed UART/RS232

The settings:

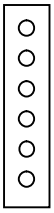
- Speed 115200 bits per second
- 8 data bits, 1 stop bit, 0 parity bit
- No flow control
- The definition of UART pin header is:



3.2.2 High speed UART/RS232

The settings:

- The default speed is 115200 bits per second, and is configurable up to 3 Mbps.
- 8 data bits, 1 stop bit, 0 parity bit
- RTS/CTS flow control, and is configurable to enable or disable.
- The definition of UART pin header is:



4. Navigating the Web Interface

You can connect to the device by Ethernet port or by WiFi. The default WiFi is enabled as AP mode, and the SSID is "**CJN-WiFi**" without security.

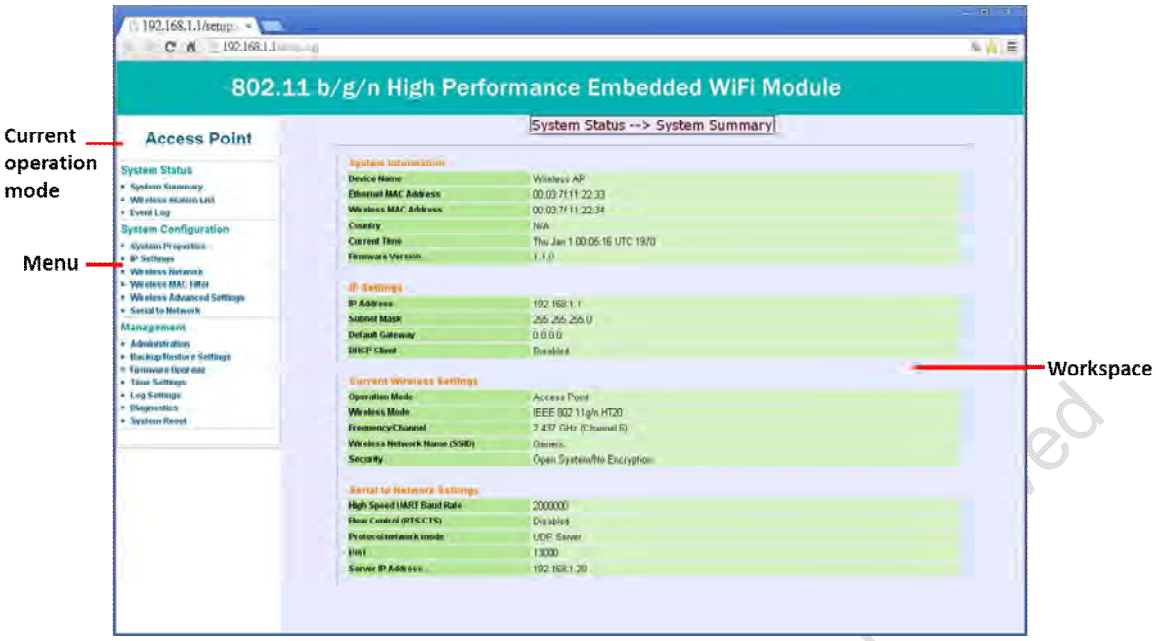
4.1 Logging into the Web Interface

You can log into the Web interface using a computer via a standard Web browser.

1. On the PC, open a Web browser window.
2. In the address or location bar, type the IP address of the AP. The default IP address is **192.168.1.1**.
3. Press <Enter> to connect to the Web interface.
4. If a Windows security alert dialog box appears, please enter the correct user name and password and click OK/Yes to proceed. The default use name is **Admin** and no password.

The wireless AP Web interface appears.

The Wireless AP's Web browser-based interface provides intuitive controls for viewing the status, making configuration changes, network administration and troubleshooting. The Web interface features that are identified as below.



Element	Description
Menu	Under each category (System Status, System Configuration, Management) are options that, when clicked, open the related workspace in the area to the right.
Current Operation Mode	Showing the current system operation mode. The options displayed in Menu bar are related to the current operation mode.
Workspace	This large area displays features, options and indicators relevant to the menu bar choices.

4.2 Viewing the Device Status

4.2.1 System Summary

The System Status --> System Summary page displays the main information on the AP's settings.

The System Information section displays a general overview of the AP's current status, including Device Name, MAC address, current time, current firmware version, etc.

The IP Settings section displays the information on the AP's network settings, including current AP's IP address, subnet mask, gateway, and the method of obtaining the IP address (DHCP or fixed IP).

The Current Wireless Settings displays the common wireless settings that the AP is using, including operation mode, wireless mode (802.11 b/g/n, HT20), frequency/channel, SSID, and security etc.

The Serial to Network Settings displays the current settings for COM port and network port, including UART speed, flow control, TCP or UDP network mode and port number.

You can click the refresh button to refresh the information immediately.

4.2.2 Wireless Station List

This option will be showed in Status group of menu bar when the operation mode is configured to be Access Point mode.

The System Status --> Wireless Station List page is to help you monitor wireless clients that are associated with your wireless network. The information displays each associated client's MAC address and signal strength. You can click the refresh button to refresh the status of client list or it will refresh automatically per 30 seconds.

4.2.3 Connection Status

This option will be showed in Status group of menu bar when the operation mode is configured to be Wireless Client mode.

The System Status --> Connection Status page is to view the connection status while the system is connecting to the wireless network. The status information includes AP's SSID and BSSID, current channel, connection status, wireless mode, security, Tx Data rate, current noise level and signal strength, etc. You can click the refresh button to refresh the connection status or it will refresh automatically per 30 seconds.

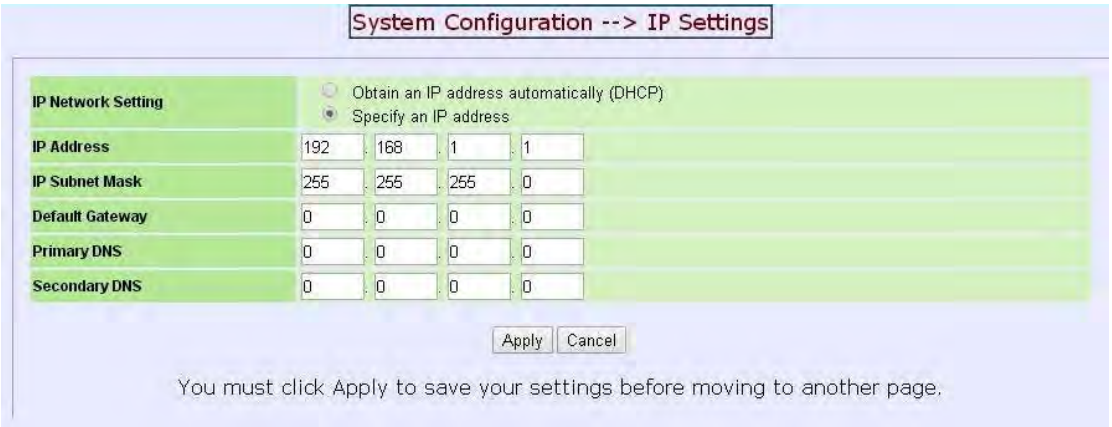
4.3 Configuring the Device Settings

4.3.1 System Properties

To configure the system settings:

1. Go to System Configuration--> System Properties. The System Setting page appears.
2. In **Device Name**, type a new name for the device or leave as is to accept the default device name. The device name identifies the AP among other devices on the network.
3. In **Country/Region**, select a country code to conform to local regulations. The usable channel list that shows in wireless network page is depended on the selected country code.
4. In **Operation Mode**, select one of supported operation mode (Access Point, Wireless Client, and Repeater).
5. Click Apply button to take effect the new settings, or Cancel button to revert to the original settings.

4.3.2 IP Settings



By default, the device is configured to assign the static IP address **192.168.1.1**. You can change the IP address by specifying the other static IP address for your network deployment or obtaining an IP address from DHCP server on network.

To review and configure the IP Settings

1. Go to System Configuration--> IP Settings. The IP Settings page appears.
2. Verify that the IP Network Setting is to obtain the IP address from DHCP server or set to static IP address.
3. When the Specify and IP address is selected, you can change the following settings

- IP Address: Assign an IP address for the device.
- IP Subnet Mask: Specify the subnet mask for your network segment deployment.
- Default Gateway: This is the gateway IP address of the internet interface.
- Primary DNS: The IP address of the primary Domain Name System (DNS) server.
- Secondary DNS: The IP address of te secondary Domain Name System (DNS) server.

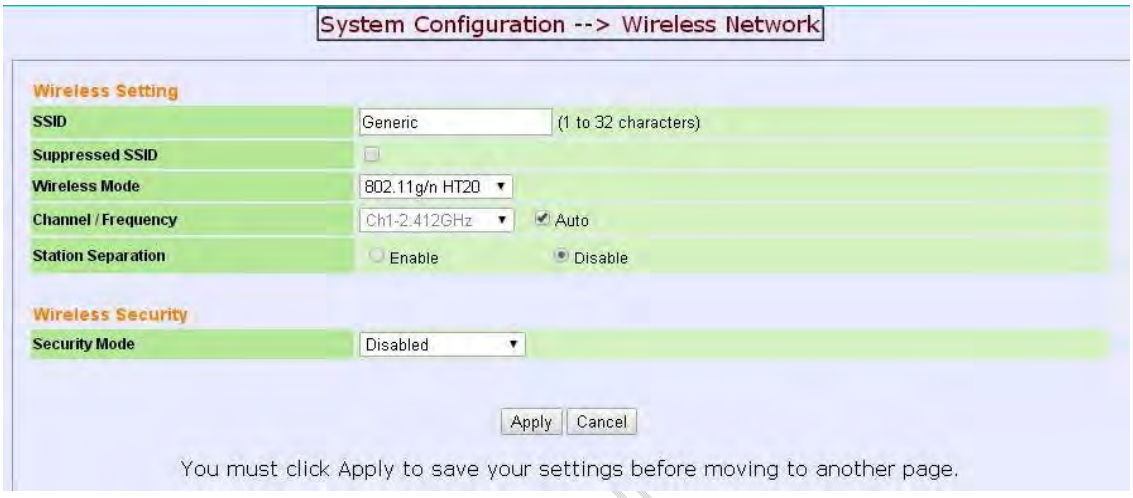
4. Click Apply button to take effect the new settings, or Cancel button to revert to the original settings.

4.3.3 Configuring the Wireless Basic Settings

The device supports 3 wireless operation modes: Access Point, Wireless Client and Repeater. Different operation mode will have different wireless settings for configuration. The operation mode is configured in System Configuration--> System Properties page.

Go to System Configuration-- > Wireless Network. The Wireless Network page appears.

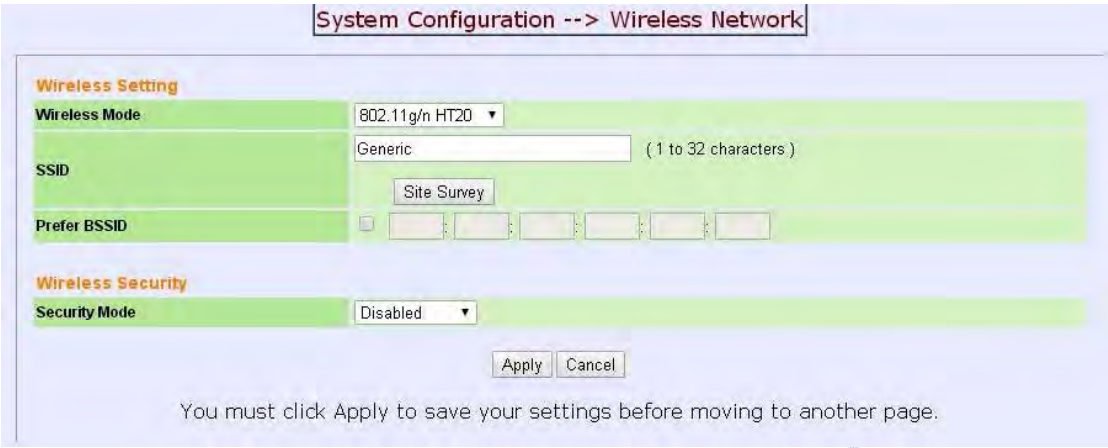
Access Point Mode



The basic wireless settings used for Access Point mode are listed below.

Setting	Description
SSID	This is the name of your wireless network. The "name" can be up to 32 characters in length, and contain letters and numbers.
Suppressed SSID	This option controls whether or not the SSID is visible to anyone looking for wireless networks.
Wireless Mode	Support 802.11 g/n HT20 and 802.11 b/g modes.
Channel/Frequency	Select the channel used by the wireless network. You can choose Auto or choose one of a specific number of channels. If you choose Auto, the AP automatically selects the best channel that is the least interference.
Station Separation	If you enable this option, all the associated clients won't be able to communicate with each other.

Wireless Client Mode



The basic wireless settings used for Wireless Client mode are listed below.

Setting	Description
Wireless Mode	Support 802.11 g/n HT20 and 802.11 b/g modes.
SSID	You can specify the Access Point SSID directly, or use **site survey** feature to select the specified Access Point.
Prefer BSSID	This setting is to let the wireless client always connect to the Access Point with specific MAC address, and won't roam to other Access Point with the same SSID.

Repeater Mode

The repeater mode is AP mode + client mode. After the client side connecting to remote AP is successful, the AP side will act as the remote AP to extend the wireless range.

Wireless Security Settings:

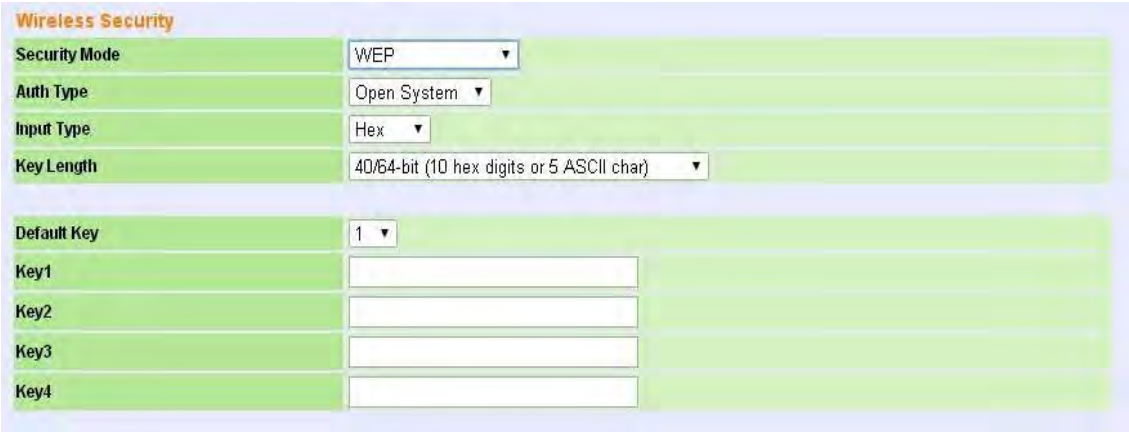
In the security mode option, there are WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2 and WPA Mixed listed.

CAUTION: Setting the security mode to WEP or setting the WPA algorithm to TKIP will result in

	decreased performance, as these settings are not supported by the 802.11n standard.

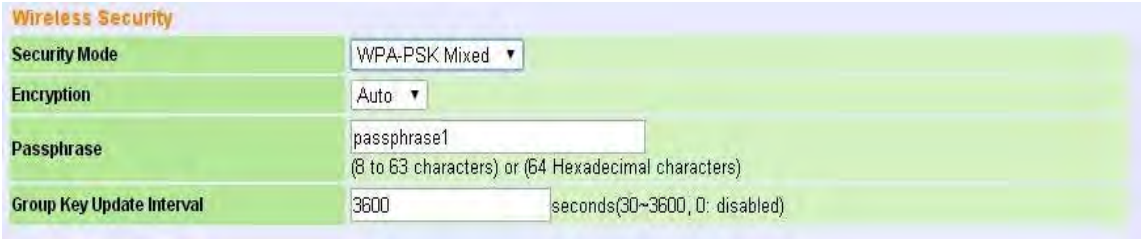
Access Point Mode

WEP



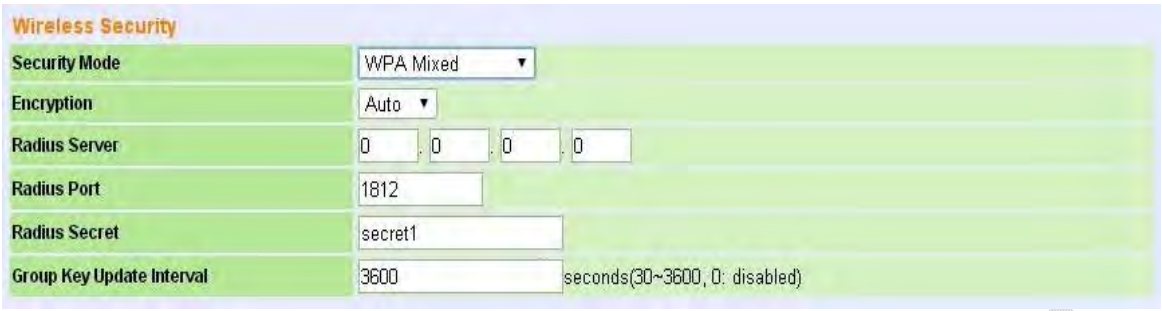
Setting	Description
Security mode	Enable WEP encryption
Auth. Type	Open System: No security measure is enforced. Shared: The selected Default Shared Key is used.
Input Type	Hex: The encryption key only accepts hexadecimal characters. ASCII: The encryption key accepts ASCII characters.
Key Length	Specify the key length with 64/126/152 bit
Default Key	Select the key index that WEP key is used
Key1/Key2/Key3/Key4	Enter the key according to Input Type and Key Length settings.

WPA-PSK/WPA2-PSK/WPA-PSK Mixed



Setting	Description
Security mode	The security uses the entered pre-shared key to produce a security key between AP and client. WPA2 is the strongest security and is supported in 802.11n standard. WPA provides stronger security than WEP, but less than WPA2. The WPA is greater compatibility than WPA2. WPA-PSK Mixed allows clients to use WPA-PSK or WPA2-PSK based on the client's capabilities.
Encryption	AES offers the strongest encryption, and is the only option supported by the 802.11n standard. TKIP will result in decreased performance but is for compatibility. Auto is automatically selects AES or TKIP based on client's capabilities.
Passphrase	Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters.
Group Key Update Interval	Group key is used for multicast packets, and this setting is used to update new group key periodically with associated clients. The value should be between 30 to 3600 seconds, and 0 is to disable the update.

WPA/WPA2/WPA Mixed



Setting	Description
Security mode	The security uses EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method to get a security key from Radius server. This method is commonly used in Enterprise networks. WPA2 is the strongest security and is supported in 802.11n standard. WPA provides stronger security than WEP, but less than WPA2. The WPA is greater compatibility than WPA2. WPA Mixed allows clients to use WPA or WPA2 based on the client's capabilities.
Encryption	AES offers the strongest encryption, and is the only option supported by the 802.11n standard. TKIP will result in decreased performance but is for compatibility. Auto is automatically selects AES or TKIP based on client's capabilities.
Radius Server	Radius server IP address
Radius Port	Radius server port number. The default port number is 1812
Radius Secret	Enter the radius secret key that is specified in radius server.
Group Key Update Interval	Group key is used for multicast packets, and this setting is used to update new group key periodically with associated clients. The value should be between 30 to 3600 seconds, and 0 is to disable the update.

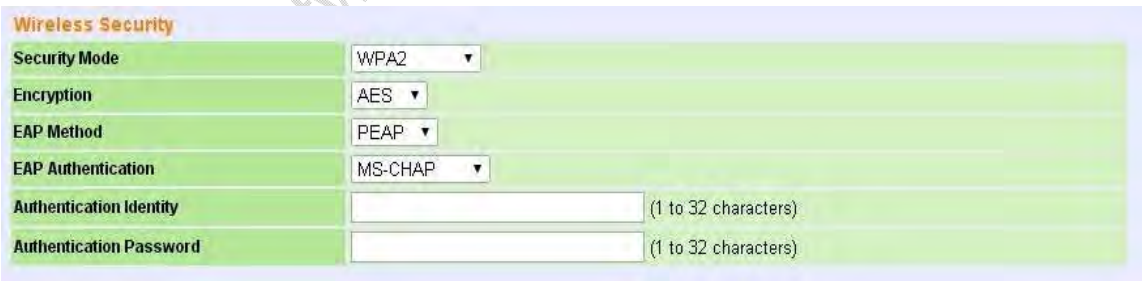
Wireless Client Mode

In wireless client mode, the wireless security settings are depended on the connecting Access Point's security settings. The WEP security settings are the same as in Access Point mode, and other security modes are described as below.

WPA-PSK/WPA2-PSK

Setting	Description
Security Mode	Select WPA-PSK or WPA2-PSK according to connecting AP's security mode setting
Encryption	Select TKIP or AES depending on connecting AP's settings. TKIP will decrease the performance, so only if AP's encryption setting is TKIP, otherwise it is not recommended.
PassPhrase	Enter the passphrase key the same as AP's setting.

WPA/WPA2



Setting	Description
Security Mode	Select WPA or WPA2 according to connecting AP's security mode setting
Encryption	Select TKIP or AES depending on connecting AP's settings. TKIP will decrease the performance, so only if AP's encryption setting is TKIP, otherwise it is not recommended.

EAP Method	Select PEAP or TTLS depending on Radius server's settings.
EAP Authentication	MS-CHAP/MS-CHAP2
Authentication Identity	Identification credential used for EAP authentication
Authentication Password	Password credential used for EAP authentication

4.3.4 Wireless MAC Filter

The Wireless MAC Filter is used to control access to the wireless network by clients' MAC address. You can restrict the access permission by allowing or denying only stations explicitly listed in the access control table. This function is only supported in Access Point operation mode.

1. Go to System Configuration > Wireless MAC Filter. The Wireless MAC Filer page appears.
2. In ACL Mode, you can decide the wireless access control policy by select the Deny MAC in the list, or Allow MAC in the list. The default is disabled.
3. You can specify the MAC address manually and press Add button to new add the MAC address to the MAC address table.
4. Click Apply button to take effect the new settings.

4.3.5 Wireless Advanced Settings

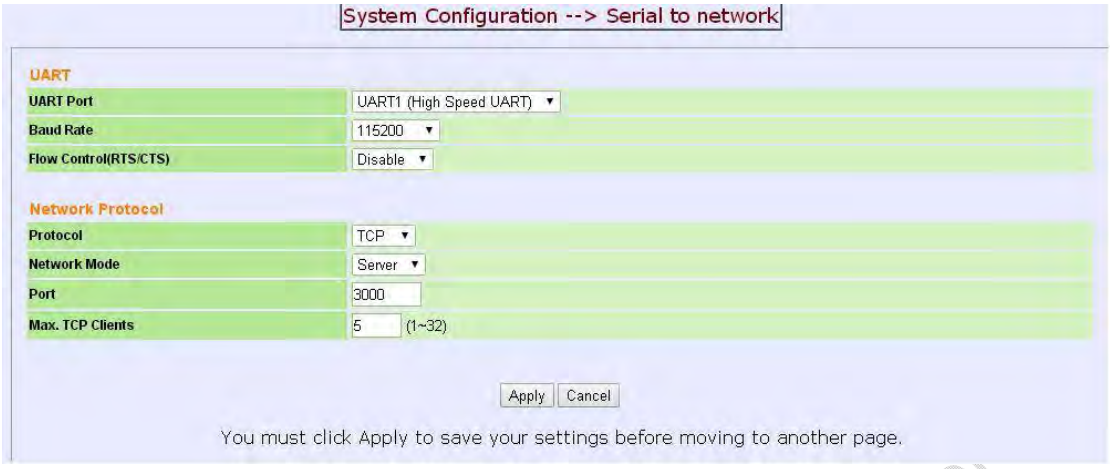
The wireless advanced settings are common to any operation mode.

1. Go to System Configuration--> Wireless Advanced Settings. The Wireless Advanced Settings page appears.
2. After finishing the following settings, click Apply button to take effect the new settings, or Cancel button to revert to the original settings.

Setting	Description
Data Rate	This defines the data rare (in Mbps) which the device should transmit wireless packets. Higher data rates will get higher throughput but be achieved at closer distances. You can fix a specific data rate (MCS0 to MCS15) or select the **Auto** option to get the best data rate dynamically according to link quality condition. It is recommended to use the Auto option, especially if you are having trouble getting connected or losing data at higher data rate.
Transmit Power	This will configure the maximum average transmit power (in dBm) of the wireless device. The transmit power will affect the wireless coverage; however, setting higher transmit power may cause connecting issue in indoor environment or the distance is not long enough between two devices.
Antenna	This option is supported for CJM210EC to use

	internal chip antenna or external antenna.
Aggregation	A part of 802.11n standard. It creates the larger frame by combing smaller frames with same physical source and destination and QoS into one large frame with a common MAC header. **Frames:** the number of frames combined on the new large frame. **Bytes:** The size of the large frame
WMM	Part of the 802.11e QoS enhancement to the Wi-Fi standard. It is recommended to enable this setting for 802.11n wireless mode to enhance traffic throughput.

4.3.6 Serial to Network

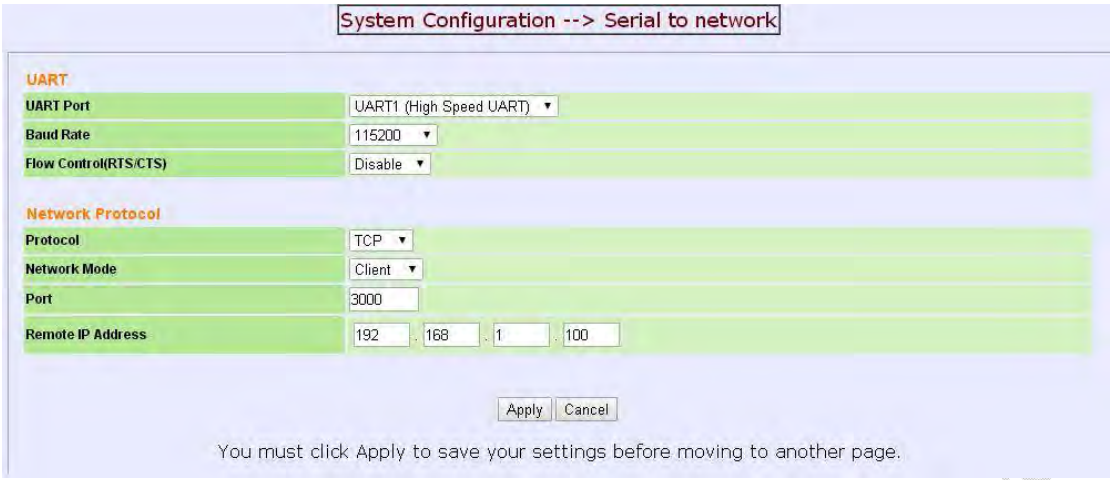


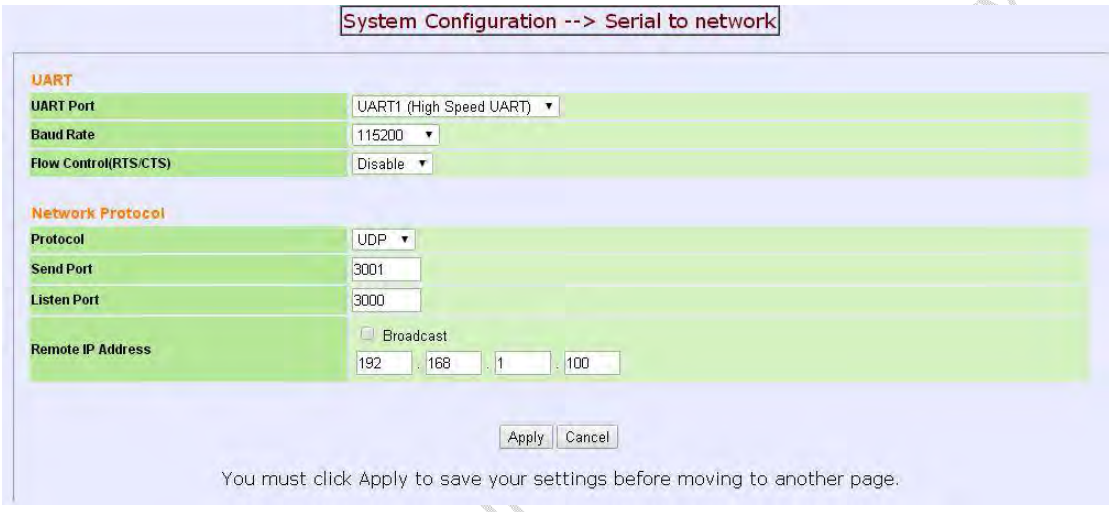
This device supports the communication between COM port and wireless or Ethernet interface. This page is to configure the UART/RS232 port and the TCP/UDP network settings.

1. Go to System Configuration--> Serial to Network. The Serial to Network page appears.
2. After finishing the following settings, click Apply button to take effect the new settings, or Cancel button to revert to the original settings.

UART

Setting	Description
UART Port	The UART0 is low speed UART port and UART1 is high speed UART port.
Baud Rate	The low speed UART port supports the baud rate from 300 to 115200 and the high speed UART port supports the baud rate from 115200 to 3000000. You have to select the right one for communication, depends on the capability of the other side. The default is 115200.
Flow Control (RTSCTS)	To enable or disable the hardware flow control RTSCTS. This option is only supported by high speed UART.



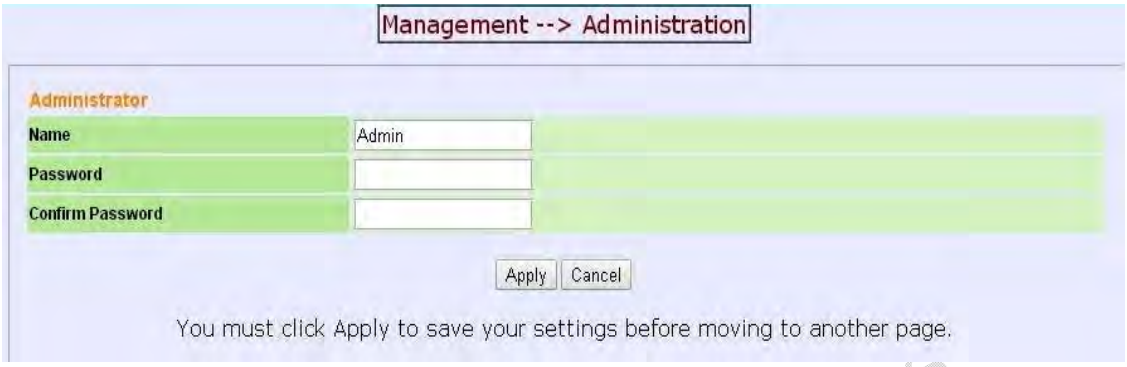


Network Protocol

Setting	Description
Protocol	To establish TCP or UDP connection.
Network Mode	To be server or client mode.
Port	For TCP protocol, the port number is as listen port when the Network Mode is server, and is as send port when the Network Mode is client.
Send Port	The send port for UDP protocol.
Listen Port	The listen port for UDP protocol.
Max. TCP Clients	When configured as TCP server, the max. TCP clients are accepted. This option is for the function of multiple TCP connections.
Remote IP Address	When the Network Mode is client, you have to indicate the server side IP address. The broadcast option is only supported for UDP protocol.

4.4 Managing the Device

4.4.1 Administration



The Web management is only allowed the authorized user to login. The default user name is Admin, and default password is empty. You can change the administrative login settings in this page.

1. Go to Management --> Administration. The Administration page appears.
2. In Name, type a new user name that you will use to log in to the Web interface.
3. In New Password, type a new password to replace the old one.
4. In Confirm New Password, re-type the new password.
5. Click Apply button to take effect the new settings, or Cancel button to revert to the original settings.

4.4.2 Backup/Restore Settings

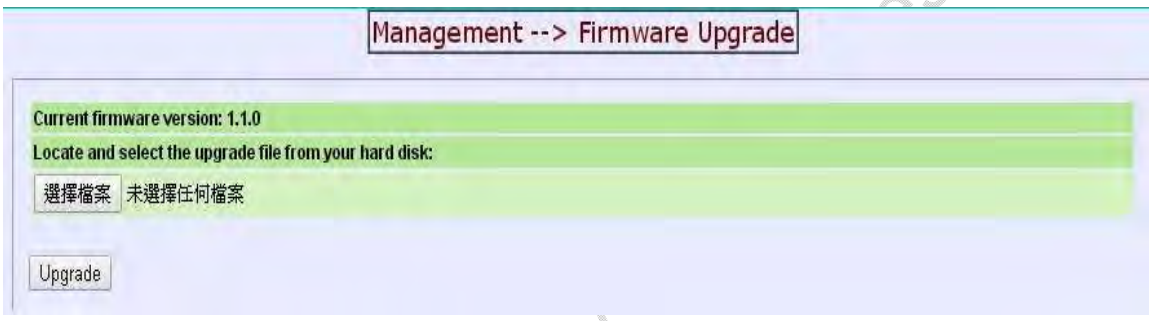
You can save the current device settings to a file or restore the saved settings file to the device to revert the old settings.

1. Go to Management --> Backup/Restore Settings. The Backup/Restore Settings page

appears.

2. Click on Backup button to save the current device settings.
3. In Restore Saved Settings from A File, click the browse button to select the saved settings file and click Restore button to load the file. After rebooting the device, the new settings will take effect.
4. Click Factory Default button to reset all the settings to factory default values. After rebooting the device, the default settings are reverted.

4.4.3 Firmware Upgrade



1. Go to Management --> Firmware upgrade. The Firmware Upgrade page appears.
2. Click the Browse button to select the firmware image file, and click the Upgrade button to proceed the update of firmware. It will take around 90 seconds to finish the firmware update. Once the firmware is updated successfully, the device will reboot automatically.

4.4.4 Time Settings

The device supports two ways to configure the system time. The first is to configure the date and time manually, and once the device is rebooted, the current time will revert to the default value, and it is needed to re-configure the date and time again. The other way is to use NTP protocol to get the date and time automatically. If you don't specify the IP address of NTP server, the system will get the date and time from public NTP server via internet.

1. Go to Management --> Time Settings. The Time Settings page appears.
2. Decide which option you want to take:
   - Manually Set Date and Time.
   - Automatically Set Date and Time
3. If the Manually Set Date and Time is selected, input the current date and time, and click Apply button to take effect.
4. If the Automatically Set Date and Time is selected, specify the Time Zone that your country is located. If you don't specify the IP address of NTP server, the system will get the date and time automatically from internet. Click Apply button to take effect the time settings.

NOTE: If the NTP server is located on internet, please make sure the device is able to connect to the internet via the deployed network.

4.4.5 Diagnostics

The Diagnostics is to provide tools to understand the network connecting status. The Ping utility is used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets. The Traceroute utility is used for tracing the hops route from the device across the network to a selected outgoing IP address.

1. In Ping test, specify the following parameters:

Parameter	Description
Target IP	The IP address of the other network device
Ping packet size	Specify the packet size of each ICMP packets
Number of Pings	Specify the ping packet numbers for the test

2. Click the Start Ping button; it will pop up a window to show the test result.
3. In the Traceroute test, specify the target IP address and click the Start Traceroute button to start the test.

4.4.6 System Reset

You can use this function to reboot the system without changing any of the current settings or reset to factory default settings and reboot the system.

FCC Warning Statement

1. 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.
2. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.
3. 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.
4. FCC RF Radiation Exposure Statement
   - This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
   - This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
5. This module is intended for OEM integrator. The OEM integrator is responsible for the compliance to all the rules that apply to the product into which this certified RF module is integrated. Additional testing and certification may be necessary when multiple modules are used.