



Monarch® 9485
Portable Printer

System Administrator Manual



Table of Contents

1. INTRODUCTION	3
1-1 Using This Manual	3
1-2 Using the Menu Chart	3
1-3 Using the Display and Buttons	4
1-3-1 Selecting a Menu	5
1-3-2 Exiting a Menu	5
1-3-3 Printing	5
1-4. Selecting a Language	6
2. USING DIAGNOSTICS	7
2-1 Diagnostics	7
2-1-1 Printer	8
2-1-2 Display	14
2-1-3 Buttons	15
2-1-4 RAM	16
2-1-5 Data Dump	17
2-1-6 About	18
3. SETTING UP THE PRINTER	19
3-1 SETUP	19
3-1-1 Stock PWR	20
3-1-2 Backlight	21
3-1-3 Contrast	22
3-1-4 Printer	23
3-1-5 Serial Communications	35
3-1-6 Power Management	39



Disposal of Old Electrical&Electronic Equipment(Applicable in the European Union and other European countries with separate collection systems)

This symbol on the product or on its packaging indicates that this product shall not be treated as household waste.

Instead it shall be handed over to the applicable collection point for the recycling of electrical and electronics equipment. For more detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

4. Wi-Fi	41
4-1 RF Network	41
4-2 Using the Wi-Fi Settings Dialog	50
4-3 Using the Web Interface	52
4-4 Wi-Fi Glossary	82
4-5 Wi-Fi specifications	87
5. Bluetooth	88
5-1 Using the Bluetooth Settings Dialog	88
5-2 Bluetooth Interface	91

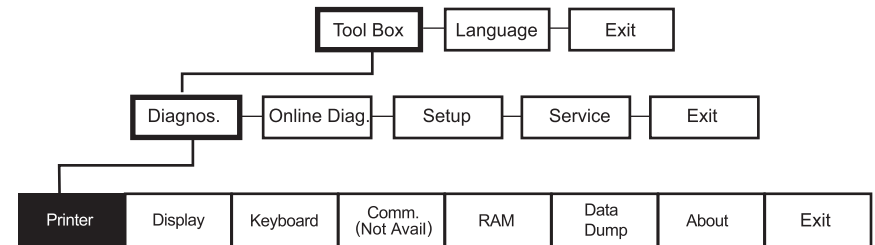
1. INTRODUCTION

1-1. Using This Manual

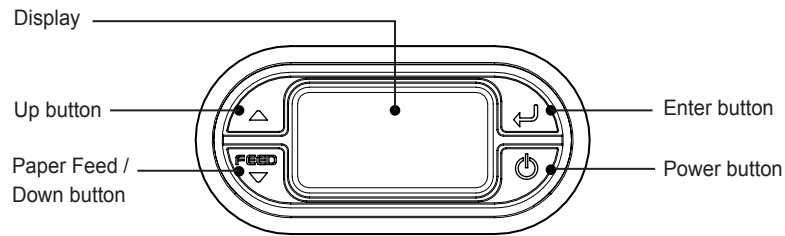
	Subjects	Contents
1	Introduction	Notes before using printer
2	Diagnostics	How to print test label, check sensor, check print position, etc.
3	Setting Up the Printer	How to use the Setting Menu to adjust stock and printer settings

1-2. Using the Menu Chart

The black boxes show present position, the boxes with a thick line show how you got there.



1-3. Using the Display and Buttons



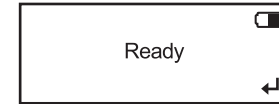
NOTE

button operates as feed button in ready condition only.

Screen displays	Meaning
↵	Selects the highlighted option.
▲	Moves position of Menu upwards by one step.
FEED ▼	Moves position of Menu downwards by one step
▶	Moves the cursor to the position to change.
+	Increases set value
-	Decreases set value
X	Returns to higher Menu without saving the setting
Y	Returns to higher Menu after saving the setting

1-3-1. Selecting a Menu

1. Press Enter(↵) button to enter the Menu



2. Move cursor to the menu using Up(▲) / Down(▼) buttons, and select the Menu by pressing Enter(↵) button.



1-3-2. Exiting a Menu

Select Exit Menu or press the power (⏻) button to return to the previous menu.

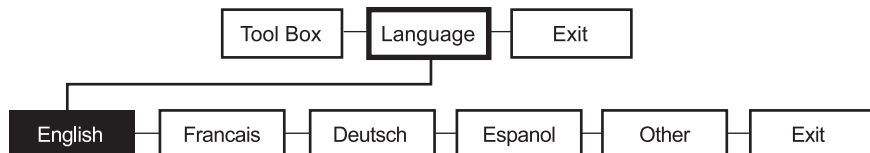
1-3-3. Printing

There are three ways to print.

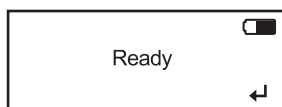
1. When turning on the printer, press and hold the power (⏻) button and the Down(▼) button. The printer prints a batch (if sent) or prints the printer status information.
2. Select a test label from the Diagnostics menu.
3. Send batch data to the printer.

1-4. Selecting a Language

You can read Menu names or messages of the printer in English, French, Spanish, German.



1. Turn on the printer. The printer name and software version information are displayed. Then you see



2. Press Enter(↵) button.



3. Move cursor to language by pressing Down(▼)button and then press Enter(↵) button.



4. Move the cursor to the language you want by pressing Up(▲)/Down(▼) button then press Enter(↵) button.



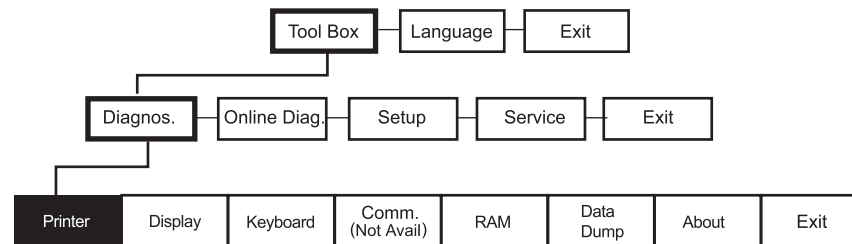
5. The selected language is displayed on the screen.
6. Select exit to return to the diagnostics menu or press the power button to return to the ready screen

2. Using Diagnostics

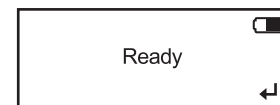
This chapter describes how to use Diagnostics in the Tool Box.

You can view test results through this Menu; however, you cannot change the setting.

2-1. Diagnostics



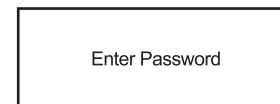
1. Turn on the printer. The printer name and software version information are displayed. Then you see



2. Press Enter(↵) button and then you see



3. Enter(↵) button and you see



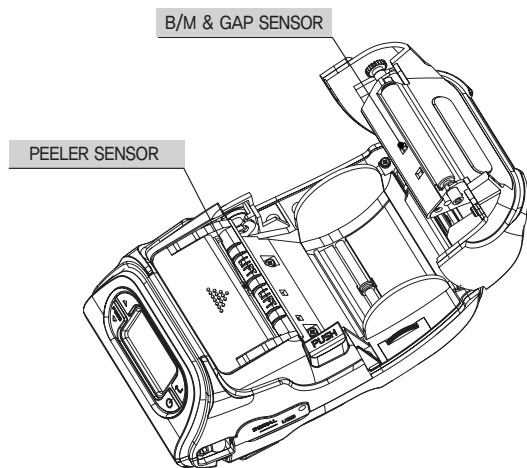
4. Press Up(▲) and Enter(↵) button in the sequence of ↵,▲, ▲, ▲,↵
5. If correct password is typed in then you see



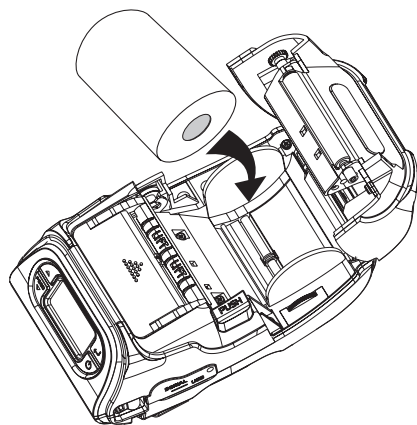
6. Cursor is positioned on the Diagnostics Menu. Enter into Diagnostics Menu by pressing Enter(↵) button.

**Sensors

In this Menu, you can read each A/D value of the Black Mark, Gap, or Peeler, Peel-SW sensors. Position of each sensor is as shown in following picture.



1. Load stock in the printer.

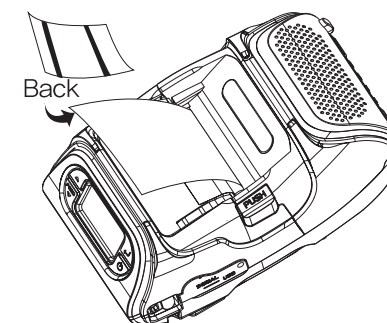
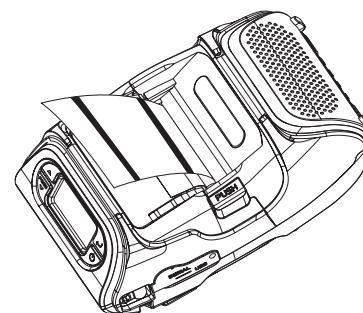


2. Select **Printer – Sensors – Black Mark** in the Diagnostics Menu.

Check whether A/D value is changing in Black Mark sensor position while feeding Black Mark stock manually.

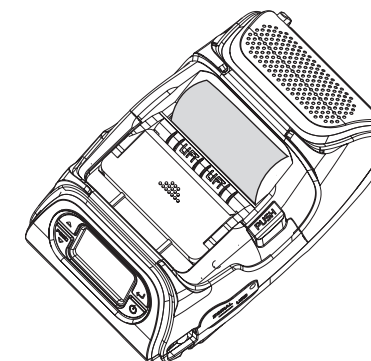
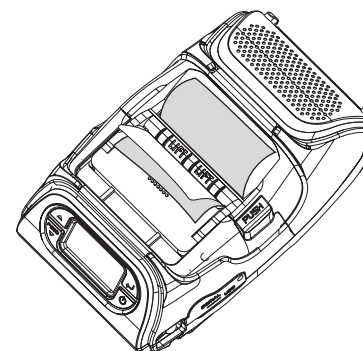
Black Mark
A/D Value = 16

Make sure the stock is loaded in line with upper/lower Black Mark sensor.



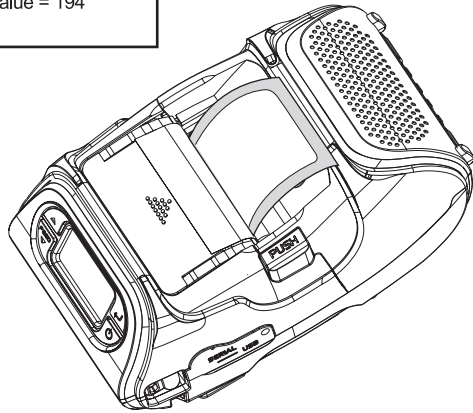
3. Select **Printer – Sensors – Peeler** in Diagnostics Menu. Check whether A/D value is changing by covering the Peeler Sensor with stock

Peeler
A/D Value = 255



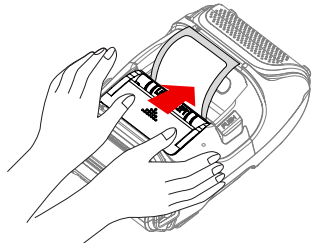
4. Select **Printer – Sensors – Gap** in Diagnostics Menu.
Check whether A/D value is changing in Gap sensor position by feeding Gap stock manually.

Gap
A/D Value = 194

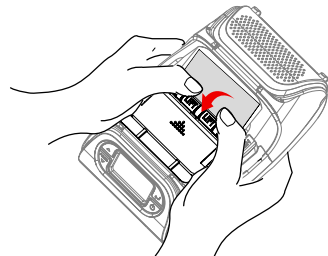


5. Select **Printer – Sensors – Gap** in Diagnostics Menu.
Check whether A/D value is changing by Peeler S/W position.

Peel-SW
A/D Value = 194



With a roll of stock installed, slide the peeler body towards the back of the printer.



Lift the peeler wing and slide the peeler body towards the front of the printer.

6. Press Enter(↵) button to return to the previous menu.

**Printhead

In this Menu, You can check Printhead temperature(TPH) in °C(Centigrade) unit.

1. Select **Printer – Printhead – Temperat** in the Diagnostics Menu.

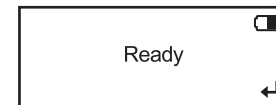
Temperature
Degree C = 32

The temperature of Printhead must be lower than 60°C to print.
Press Enter(↵) button to return to the previous menu.

**Battery

There are two ways to check the battery level.

1. You can check it in the battery shape located at upper right side of the ready screen.



NOTE Remaining electricity of battery

2. Select **Printer – Battery** in the Diagnostics Menu Battery level is displayed in voltage on the screen

Battery
Voltage = 7.74

Press Enter(↵) button to return to the previous menu.

**View Total

In this Menu, you can view Total inches printed

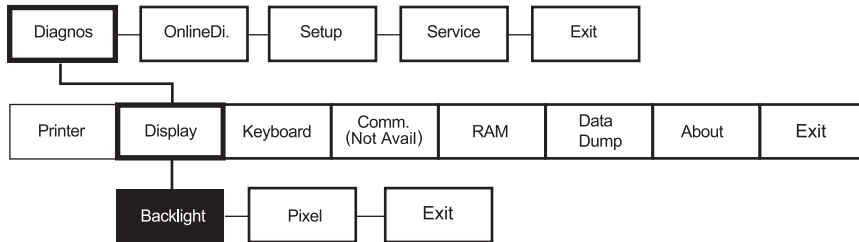
1. Select **Printer – View Total – Print Inch** in Diagnostics Menu.

Prt Inches
0000060

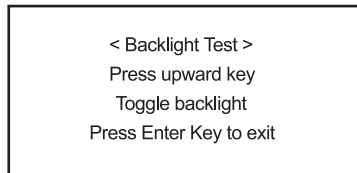
Press Enter(↵) button to return to the previous menu.

2-1-2. Display

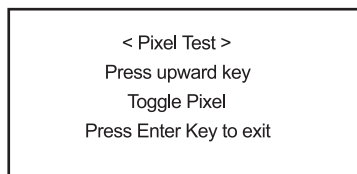
You can check the display in this Menu.



1. Select **Display – Backlight** in the Diagnostics Menu

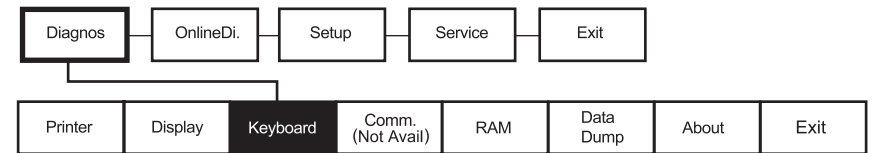


2. Press the Up(▲) button Backlight is turned off, if the same button is pressed once more then it is turned on.
3. Press Enter(↵) button to exit from Backlight Test.
4. Select **Display – Pixel** in the Diagnostics Menu.

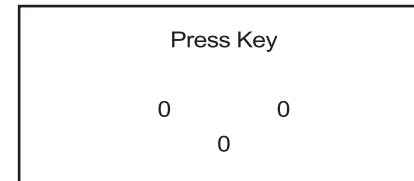


5. Press the Up(▲) button all Pixels on the screen are changed into black color and if it is pressed once more then all Pixels are changed into white color.
6. Press Enter(↵) button to exit from Pixel Test.

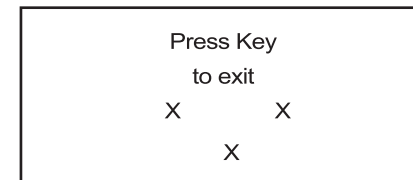
2-1-3. Buttons



1. Select Keyboard in Diagnostics Menu.

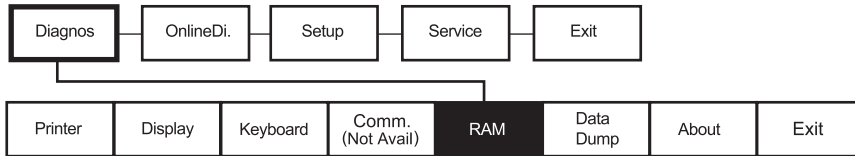


2. Press the upper left Up(▲) button, press the Down(▼) button, and press Enter(↵) button.
3. Each should change from O shape to X shape when pressed.
4. Press Enter(↵) button to from keyboard test.



2-1-4. RAM

Select this Menu and check memory of the printer.



1. Select **RAM** in Diagnostics Menu.
2. The message of RAM test running is displayed

```
RAM test running...
```

3. If RAM test result is okay, then you see:

```
RAM test passed
Press any Key
to exit
```

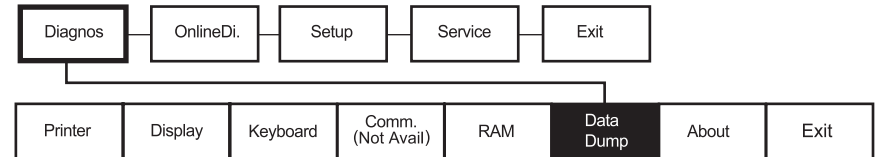
4. If RAM test result is not okay, then you see:

```
RAM test failed
Press any Key
to exit
```

5. Press Enter(↵) button to return to the previous menu.

2-1-5. Data Dump

Use this menu if you are having problems with a data stream. Data Dump captures the data from the communications port and prints that information to a label.



1. Select **Data Dump** in Diagnostics Menu.
2. The labels print with data from the communication port.

```
0 200 200 210 1
TEXT 4 0 0 100 I<-DATE
FORM
PRINT
```

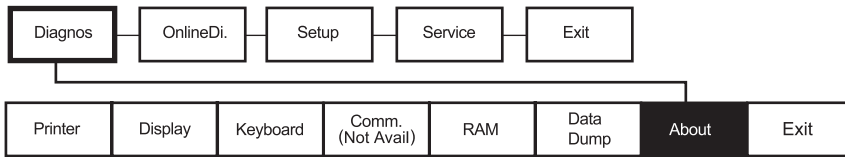
For CPCL, previous command data printed on the paper

```
1,0: T,08,1,v,195,182,0,,1,1,0
B,0,1,0: T,09,1,V,215,182,0,,1,
1,0,B,0,1,0: T,10,1,V,235,182,0
,,1,1,0,B,0,1,0: }B,3,N,1: 01,
"~128": 02, "~129": 03, "~130
": 04, "~131": 05, "132": 06
, "~133": 07, "~134": 08, "~13
5": 09, "~136": 10. "~137": }
```

For MPCL, previous command data printed on the paper

2-1-6. About

You can see the model name of the printer and H/W and S/W version in this Menu.



1. Select **About** in Diagnostics Menu.
2. Then you can check information of the printer

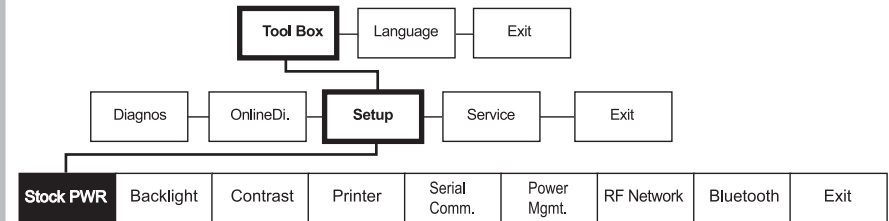
```
ABOUT LK-P12
S/W VER. v0.02a
H/W REV. v0.2
```

3. Press any key to exit

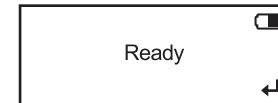
3. SETTING UP THE PRINTER

3-1. SETUP

This chapter describes, how to set up the printer



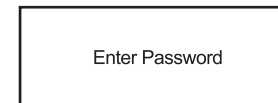
1. Turn on the printer.



2. Press Enter(↵) button.



3. Press Enter(↵) button then enter the password.



4. Press Up(▲) and Enter(↵) button in the sequence of ↵, ▲, ▲, ▲, ↵

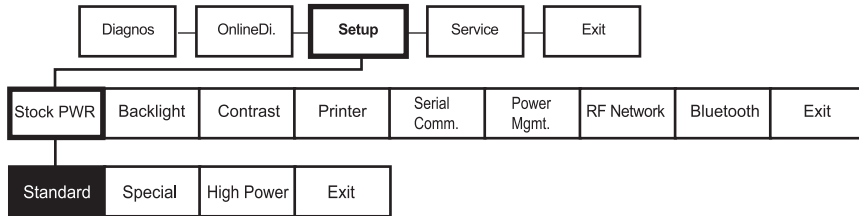
5. If password is entered correctly, you see:



6. Press Up(▲) / Down(▼) button to select Setup Menu and press Enter(↵) button

3-1-1. Stock PWR

Using this Menu, you can set stock type. This printer uses two kinds of stock, Standard and High Power. Standard supports tag, label, or receipt and High Power supports linerless and synthetic



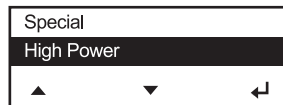
NOTE

The "special" setting is reserved for future supply types. Do not use this setting.

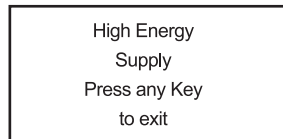
1. In Setup Menu, select **StockPWR.**



2. Select stock type.



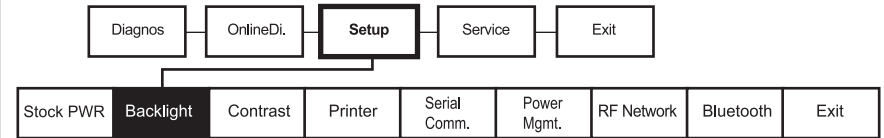
3. You see..



4. Press any key to exit. Set Values is stored.

3-1-2. Backlight

This Menu can activate or deactivate Backlight of LCD.



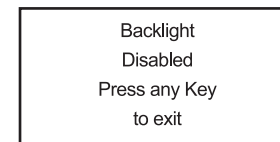
1. In Setup Menu, select **Backlight.**



2. Select Disable or Enable



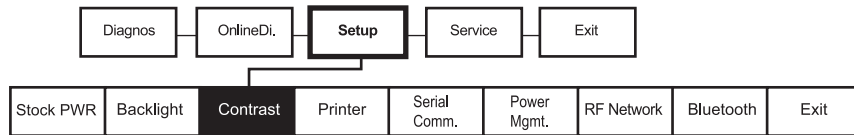
3. You see..



4. Press any key to exit. Set Values is stored.

3-1-3. Contrast

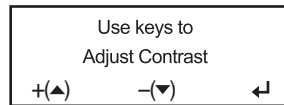
This Menu sets Contrast of LCD



1. Select Contrast in Setup Menu.



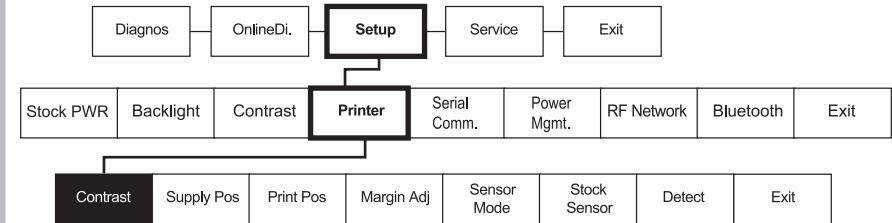
2. Press the Up(▲) button or Down(▼) button to adjust the contrast.



3. Press enter button (↵) to save and exit

3-1-4. Printer

In this Menu, you can set Print Contrast, Print Positions and use of various sensors.



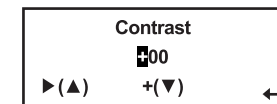
**Adjusting the Print Contrast

In this Menu, you can adjust print contrast.

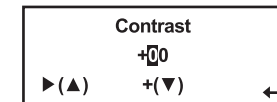
1. Select Setup **Menu – Printer – Contrast.**



2. Press Up(▲) button to move the cursor one step towards right side (selecting the +/-). Press Down(▼) button to change the positive/negative setting.



3. Press Up(▲) button to move the cursor one more step to the right. Press Down (▼) button to increase/decrease the print contrast setting (0 – 9).



Above key operations are described in following table.

▶	+	↵
Press Up(▲) button [Move cursor. (+00)]	Press Down(▼) button [Character is changed]	Press Enter(↵) button. [Exit after stored.]
First position(00)	It changes +/-.	Store the setting and then exit.
Second position(+00)	Changes second position.	
Third position (+00)	It changes third position.	

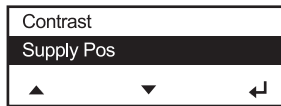
4. If you exceed the minimum/maximum range then following Menu appears and you must set the print contrast within the acceptable range.



**Adjusting the Supply Position

This Menu sets how much the paper is fed during printing.

1. Select Setup **Menu-Printer-Supply Pos**



2. In following picture, if Up(▲) button is pressed then position of cursor moves towards right side by one step. And if Down(▼) button is pressed then the level of character on which the cursor is presently positioned is increased. For example, if you press on + then it changes to -/If it is pressed on – then it is changed to +, if it is pressed on figure(Number) then the figure increases by 1(0~9). If it becomes the data desired by user then store it and exit by pressing Enter(↵) button.



3. Above key operations are described in following table.

▶	+	↵
Press Up(▲) button [Move cursor. (+00)]	Press Down(▼) button [Character is changed]	Press Enter(↵) button. [Exit after stored.]
First position(00)	It changes +/-.	Store the setting and then exit.
Second position(+00)	Changes 10 th digit.	
Third position (+00)	It changes 1 st digit.	

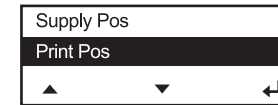
4. When to set, if you set exceeding minimum/maximum range then following Menu appears on the upper part and then returns to Setting Menu again.



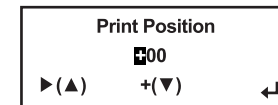
**Adjusting the Print Position

In this Menu, the position of printing material to be printed printing material will be adjusted towards Up/Down on the basis of present position.

1. Select Setup **Menu – Printer – Print Pos.**



2. In flowing picture, if you press Up(▲) button then the position of cursor moves towards right side by one step. And if you press Down(▼) button then the level of character on which cursor is located increases. For example, if you press it on + then it changes to -/ If you press it on – then it changes to +, and if you press it on figure(Number) then the figure increases by 1(0~9). If it becomes the data desired by user, then store it and exit by pressing Enter(↵) button.



3. Above key operations are described in following table.

▶	+	↵
Press Up(▲) button [Move cursor. (+00)]	Press Down(▼) button [Character is changed]	Press Enter(↵) button. [Exit after stored.]
First position(00)	It changes +/-.	Store the setting and then exit.
Second position(+00)	Changes 10 th digit.	
Third position (+00)	It changes 1 st digit.	

4. When to set, if you set exceeding minimum/maximum range then following Menu appears on the upper part and then returns to Setting Menu again.



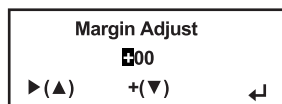
**Adjusting the Margin Adjust

In this Menu, the position to be printed can be adjusted in left/right on the basis of present position.

1. Select Setup Menu – Printer – Margin Adj.



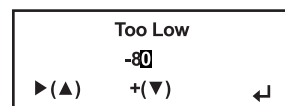
2. In flowing picture, if you press Up(▲) button then the position of cursor moves towards right side by one step. And if you press Down(▼) button then the level of character on which cursor is located increases. For example, if you press it on + then it changes to -/If you press it on – then it changes to +, and if you press it on figure(Number) then the figure increases by 1(0~9). If it becomes the data desired by user, then store it and exit by pressing Enter(↵) button.



3. Above key operations are described in following table.

▶	+	↵
Press Up(▲) button [Move cursor. (+00)]	Press Down(▼) button [Character is changed]	Press Enter(↵) button. [Exit after stored.]
First position(+00)	It changes +/-.	Store the setting and then exit.
Second position(+00)	Changes 10 th digit.	
Third position (+00)	It changes 1 st digit.	

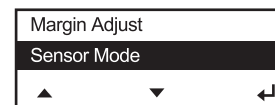
4. When to set, if you set exceeding minimum/maximum range then following Menu appears on the upper part and then returns to Setting Menu again.



**Setting the Sensor Mode

This Menu sets sensor according to presently loaded paperstock (Gap, BlackMark).

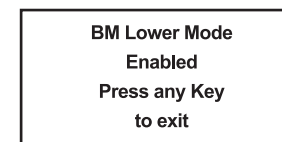
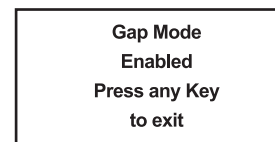
1. Select Setup **Menu – Printer – Sensor Mode.**



2. Select one of four sensor modes of Gap, BM Lower, BM Upper, Non-indexed.



3. You see:



4. Exit from the screen by pressing any key. The set value is saved.

Depending on your supply, set the sensor mode accordingly:

Gap	Use for die cut (no black mark) supplies. If your supply is die cut, with black marks, select BM Upper.
BM Lower	Use for supplies with black marks on the front (printing side) of the supply.
BM Upper	Use for supplies with black marks on the back (non-printing side) of the supply.
Non-indexed	Use for receipt paper.

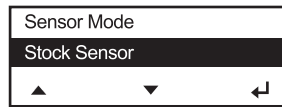
✓ NOTE

Our supplies are usually black mark on the back (non-printing side), so select BM Upper.

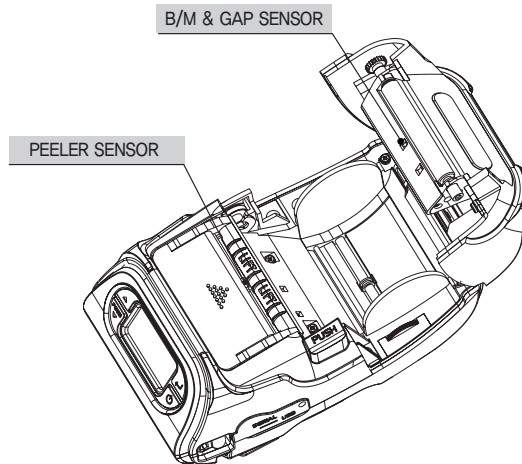
**Setting the Stock Sensor

This Menu sets DAC value per for each sensor (Gap, BlackMark).

1. Select Setup **Menu- Printer – Stock Sensor.**

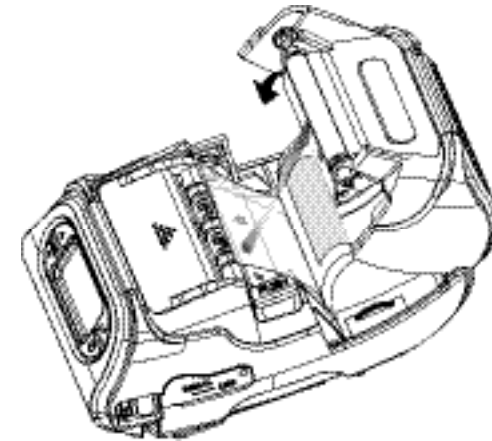


2. Conduct testing referring to following picture.

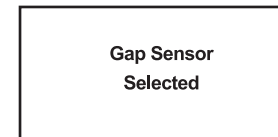


Gap Mode

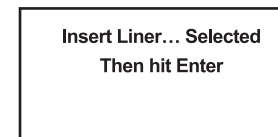
1. With the printer turned off, remove one or two labels from the liner.
2. With the printer in peel mode, place the liner over the sensor.



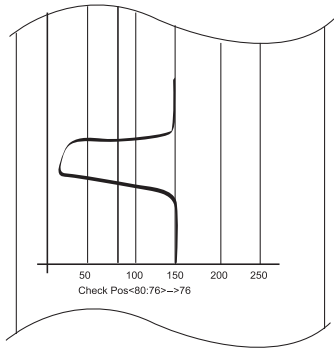
3. Press Enter(↵) button when you see:



4. Following message appears, Press Enter(↵) button to continue.



5. The information label prints.



6. Following message appears

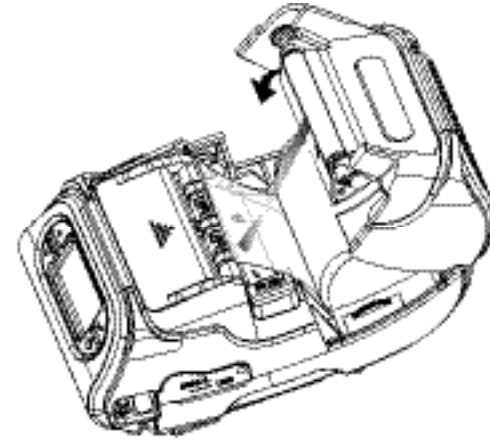
Successful

Failed

7. Press any key to exit from the Menu.

Black Mark Lower Mode

1. Cover the lower black mark with a label,



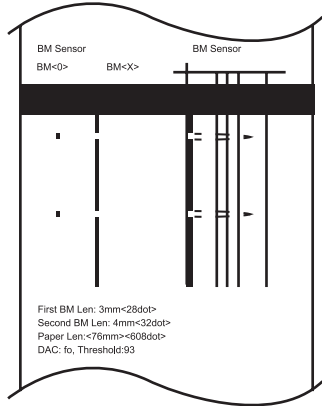
2. Press Enter(↵) button

**BM Sensor
Selected**

3. Following message appears, pressEnter(↵) button to continue.

**Insert Liner... Selected
Then hit Enter**

4. The information label prints.



5. Following message appears according to the result.

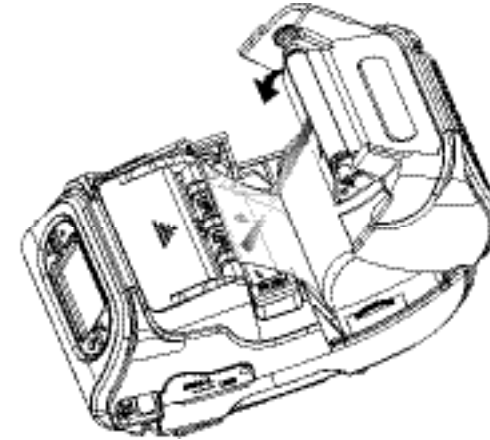
Successful

Failed

6. Press any key to exit from the Menu.

Black Mark Upper Mode

1. Cover the upper black mark with a label. BM Upper is recommended for our supply.



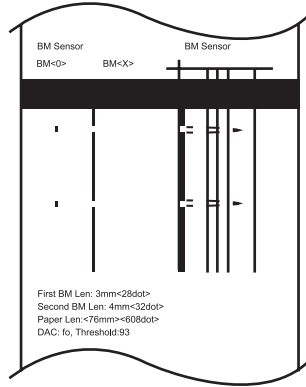
2. Move to next step by pressing Enter(↵) button in following screen.

**BM Sensor
Selected**

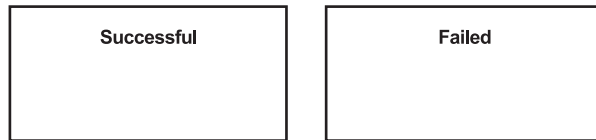
3. Following message appears and if Enter(↵) button is pressed then test will be started

**Insert Liner... Selected
Then hit Enter**

4. The information label prints.



4. Following message appears according to the result.



5. Press any key to exit from the Menu.

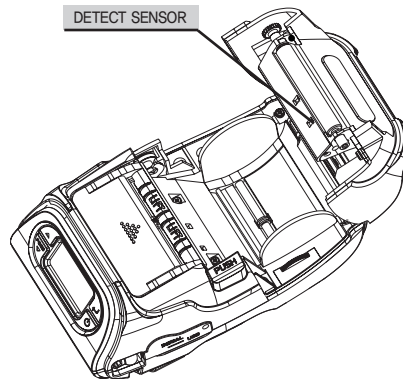
****Setting the Detect**

This Menu can activate or deactivate Width-Detect Function.

1. Select Toolbox – Setup – Printer – Detect.

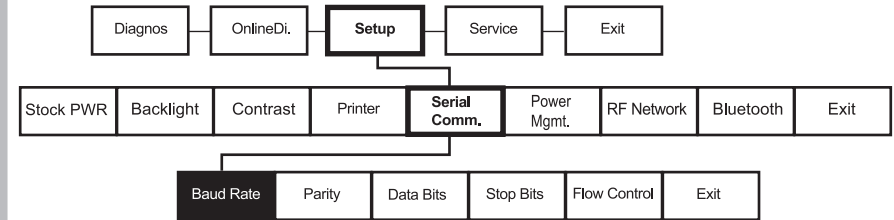
If "Enable" is selected and the supply less than 1 inch-width is detected, printing speed is reduced.

(Default : Disable)



3-1-5. Serial Communications

You can set serial communication using this Menu.



The following values must be set for serial communication with PC.

Option	Choices	Default
Baud Rate	1200/2400/4800/9600/ 19200/38400/57600/115200	9600
Parity	None/Odd/Even	None
Data Bits	7/8	8
Stop Bits	1/2	1
Flow Control	No Flow/DTR Flow/ RTS Flow/Xon/Xoff/Special	DTR

**Baud Rate

1. Select Setup **Menu – Serial Comm – Baud Rate.**

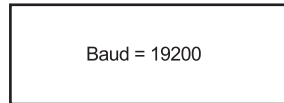


2. Select among 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.



(※BPS=Bit Per Second)

3. Save the setting by pressing Enter(↵) button.



4. Select exit to return to the Serial Comm menu.

**Parity

1. Select Setup **Menu – Serial Comm – Parity.**



2. Select among No Parity, Odd Parity, Even Parity.



3. Save the setting by pressing Enter(↵) button.



4. Select exit to return to the Serial Comm menu.

**Data Bits

1. Select Setup **Menu – Serial Comm – Data Bits.**



2. Select one of 7 Data Bits, 8 Data Bits.



3. Save the setting by pressing Enter(↵) button.



4. Select exit to return to the Serial Comm menu.

**Stop Bits

1. Select Setup **Menu – Serial Comm – Stop Bits.**



2. Select one of 1 Stop Bit, 2 Stop Bits.



3. Save the setting by pressing Enter(↵) button.



4. Select exit to return to the Serial Comm menu.

**Flow Control

1. Select Setup **Menu – Serial Comm – Flow Ctrl.**

Stop Bits
Flow Ctrl
▲ ▼ ↵

2. Select among No Flow, DTR Flow, RTS flow, Xon/Xoff, Special.

NOTE

The “special” setting is reserved for future supply types. Do not use this setting.

DTR Flow
RTS Flow
▲ ▼ ↵

3. Save the setting by pressing Enter(↵) button.

DTR Flow Ctrl

4. Return to previous Serial Comm Menu using Exit.

Exit and Save

After setting all serial communications,select exit or press Power(⏻) button to exit. The selected values are displayed and asks whether to save it or not.

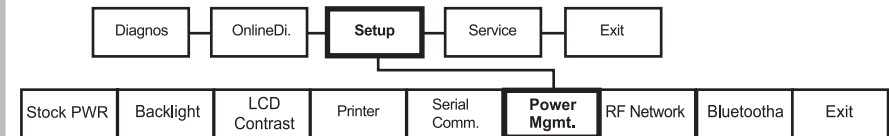
New Selection
9600, EVEN, 8, 1
Are you sure?
Y(▲) X(▼)

If you select Y by pressing Up(▲) button then it will be saved, and if you select X by pressing Down(▼) button then it exits from Menu without saving set values.

3-1-6. Power Management

This Menu sets Power Save Timeout.

(If USB cable is connected the printer does not go into Power Save). If the printer goes into Power Save Mode, wake-up the printer by connecting the USB cable, or pressing Power(⏻) button, or send data to the serial port.



1. Select Setup **Menu – Power MGMT - Low Power**

Serial Comm
Power Mgmt
▲ ▼ ↵

2. Select the Power Save Time among disable, 10 sec, 20 sec, 30 sec, 1 min, 2 min, 5 min, 10 min, 30 min, 1 hour.

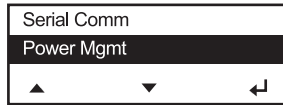
Disable
10 Sec
▲ ▼ ↵

3. Selected time is displayed and buzzer sounds short two times.

Low Power Mode
10 Seconds

4. Pressing Enter(↵) button.
5. Select Exit to return to the Setup menu.

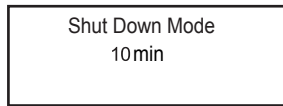
1. Select Setup **Menu – Power MGMT -Shut Down**



2. Select the Power Save Time among disable, 10min, 20min, 30 min



3. Selected time is displayed and buzzer sounds short two times.



4. Pressing Enter(↵) button.
5. Select Exit to return to the Setup menu.

4. Wi-Fi

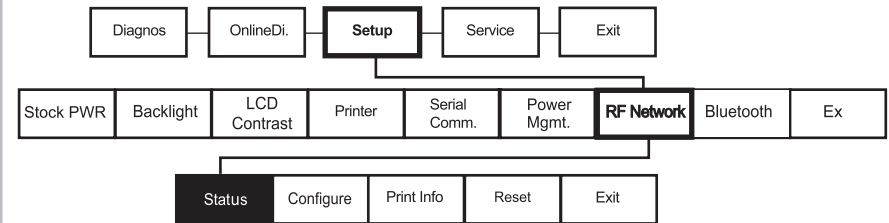
4-1. RF Network

Use these instructions to set up a printer using the printer's RF Network menu in the printer's Tool Box.

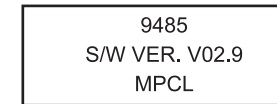
The RF Network menu allows you to check the printer's status, configure the RF network settings, and reset the radio.

NOTE

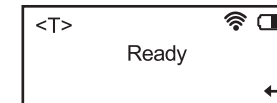
Refer to "4-3. Using the Web Interface" for the webpage configuration



1. Turn on the printer by pressing and holding the power button (⏻) until the display turns on. The display printer version information.



When you see this, the printer is waiting for the wireless print server to initialize. Next, you may see

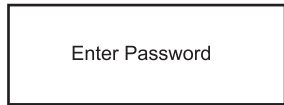


Display	Indicates
Ready	The printer is in Ready mode to send and receive data.
<T>	You can Press ▲ to display the printer's IP address. And then press ▲ again, you can return to Ready mode.
📶	The printer is connected to a Wi-Fi module.
📶	The printer is not connected to Wi-Fi module.
🔋	You can see the battery indicator. When the indicator seems to be empty, you have to recharge the battery.

2. Press Enter(↵) Button.



3. Press Enter(↵)Button then enter the password.



4. Press Up(▲) and Enter(↵) button in the sequence of ↵, ▲, ▲, ▲, ↵



5. If password is entered correctly, you see.



6. Press Up(▲)/Down(▼) button to select Setup menu and press Enter(↵) button

****Checking the Printer**

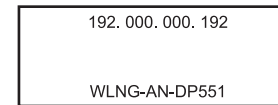
To check the printer's network status, use this menu.
To exit, press ⏏ at any time.

Checking the network status

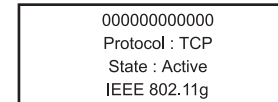
This option check the printer's IP address.

1. In Setup menu, Select RF Network.
2. From the RF Network menu, select Status.
3. Check your printer's IP address.

The display printer's IP address



4. Press ▲ to check other information



****Configuring the Printer**

The Configure menu allows you to set the printer's IP address, subnet mask, gateway, power mode, protocol, SSID, and escape character.

To exit, press ⏏ at any time.

Setting the IP Address

This option sets the printer's IP address.

1. From the RF Network menu, select Configure.
2. From the Configure menu, select IP Address.

IP Address 192.0.0.192 ▶(▲) +(▼) ↵
--

For: Select:
BOOTP 0.0.0.0
DHCP 0.0.0.1
Static IP nnn.nnn.nnn.nnn

Use the buttons as shown in the following table:

▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Increments the current position setting by 1	Saves the setting

3. When the setting you want is displayed, press ↵ to save the setting. You return to the Configure menu.

Setting the Subnet Mask

This option sets the printer's subnet mask.

1. From the Configure menu, select Subnet Mask.

Subnet Mask 255.255.000.000 ▶(▲) +(▼) ↵

Use buttons as shown in the following table:

▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Increments the current position setting by 1	Saves the setting

2. When the setting you want is displayed, press ↵ to save the setting. You return to the Configure menu.

Setting the Gateway

This option sets the printer's router (gateway) address.

1. From the Configure menu, select Gateway.

Gateway 000.000.000.000 ▶(▲) +(▼) ↵

Use buttons as shown in the following table:

▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Increments the current position setting by 1	Saves the setting

2. When the setting you want is displayed, press ↵ to save the setting. You return to the Configure menu.

Setting the Power Mode

This option sets the power mode.

1. From the Configure menu, select Power Mode.



The choices include CAM (Continuous Awake Mode) or PSP (Power Save Protocol). PSP conserves battery power. CAM means the printer is continuously receiving and transmitting data. This mode uses battery power quickly.

2. When the setting you want is displayed, press **↵** to save the setting. You return to the Configure menu.

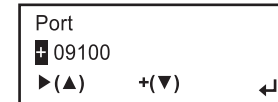
Setting the Protocol

This option sets the Protocol.

1. From the Configure menu, select Protocol : TCP or LPD. (TCP Fixed)



2. Use **▼** to select the protocol you want. For example, if you select LPD, you must specify a raw printer port:



Use buttons as shown in the following table:

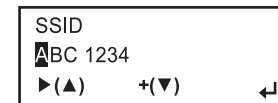
▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Toggles between + or – also increments the current position setting by 1	Saves the setting

3. Press **↵** to save the setting. You return to the Configure menu.

Setting the SSID

This option sets the SSID. The SSID is case-sensitive.

1. From the Configure menu, select SSID.



Use buttons as shown in the following table:

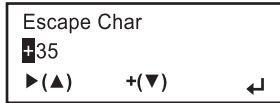
▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Increments the current position setting by 1 and scrolls through alpha/special characters	Saves the setting

2. When the setting you want is displayed, press **↵** to save the setting. You return to the Configure menu.

Setting the Command Escape Character

This option allows you to set or view the Command Escape Character (CEC). Run-time messages from the radio begin with the CEC and the default is the pound sign (#), which has a decimal value of 35. You may need to change the default CEC character if it conflicts with other data, because an unexpected operation could occur. The range is a decimal value between 1 and 255.

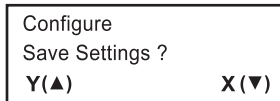
1. From the Configure menu, select Escape.



Use buttons as shown in the following table:

▶(▲) Press ▲ to	+(▼) Press ▼ to	↵ Press ↵ to
Scrolls through the positions from left to right	Increments the current position setting by 1	Saves the setting

2. When the setting you want is displayed, press ↵ to save the setting. You return to the Configure menu.
3. Press ⏻ to exit. When you select "Exit" after configuring, you will see



To save all the configuration settings, press Y(▲). To exit without saving the configuration settings, press X(▼). Press ⏻ until you see "Ready."

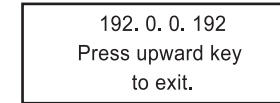
NOTE

You must reset the RF network before your changes take effect.

**Network Information

You can see a network IP address.

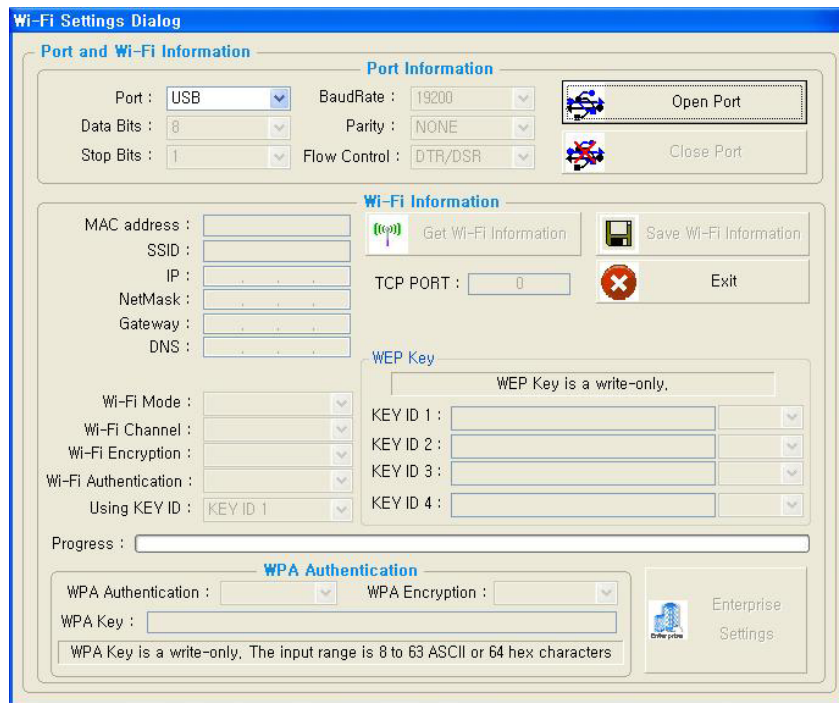
1. Turn on the printer.
2. Press ▲ under <T>. You see the printer's IP address. For example,



3. Press ⏻ or ▲ to exit.

4-2. Using the Wi-Fi Settings Dialog

After Executing Utility, please click 'Start Wi-Fi Settings'



4-2-1. Port Information

You can connect the printer to PC by Serial (COM1 – COM9) or USB port. When you use Serial Port, you have to check the Baud Rate setting between the printer & PC.

After Baud Rate setting, please click "Open Port".

When you click 'Get Wi-Fi Information', you can see Wi-Fi information of the printer.

You also can change the setting data of Wi-Fi of the printer and you can save it by clicking 'Save Wi-Fi Information'. You can disconnect printer from the PC by clicking 'Close Port'.

4-2-2. Wi-Fi Information

You can set SSID, IP, Net Mask, Gateway and DNS value according to your network environment.

And you can configure

- Wi-Fi Mode (Ad-Hoc or Infrastructure)
- Wi-Fi Channel
- Wi-Fi Encryption mode
- Wi-Fi Authentication mode
- Using KEY ID

4-2-3. WPA Authentication

Our printer supports WPA PSK(TKIP) or WPA2 PSK(AES).

4-2-4. Enterprise

Our tool supports peap, tis, ttis, wep-leap, wpa-leap, wpa-fast, wpa2-fast.

4-3. Using the Web Interface

To use the web interface follow the steps outlined in section 8.0 to establish the IP address of the module. Once the IP address is known open a web browser and enter the IP address of the module in the URL window.

The web interface currently supports Internet Explorer v6.0 thru 8.0, Firefox v3.x, Opera v9.6+ and Chrome v1.0+. When the authentication request is returned enter

Figure 1 - Website Login



Username: user

Password : password

After successfully authenticating with the module, you will be logged into the web server and allowed to browse and update module settings if required. A quick overview of the web interface follows.

4-3-1. Navigation Bar

Figure 2 - Website Navigation Bar

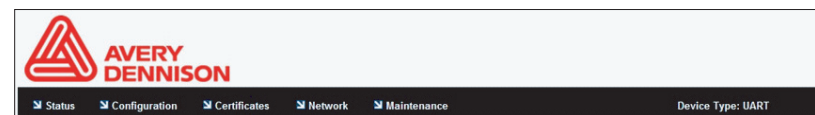


Table 1 - Navigation Bar Items

Title	Description
Status	Provides status and performance characteristics for the network interfaces available. Includes connection status.
Configuration	Allows viewing and configuration of all the interface settings including wireless LAN, network connectivity, security, and web server. Includes the interface for delivery of OEM and user configuration files, as well as management and viewing of current configurations.
Certificates	This menu items provides the interface for certificate delivery and management. Included in this section are the abilities upload and delete certificates.
Network	It is possible to scan for available Access Points.
Maintenance	This section allows the updating of the modules firmware. You can restart the module remotely. The module locate function is also enabled in this section.

4-3-2. Status

Status menu includes "Module Status" .

Module Status

As shown Figure 3, the "Module Status" will be shown when you select the "Status" in "Website Navigation Bar". This will show the Firmware or IP information for the module.

Figure 3 – Module Status Web Page

Module Status	
Module Firmware Version:	2.11F
Radio Firmware Version:	2.2.146.14
Link Status:	Connected
SSID:	sewoo-wifi-quat
MAC Address:	000B6B7ECC57
BSSID:	8E016B7E685D
Transmit Rate (Mb/s):	54
Signal Level (dBm):	-37
Noise Level (dBm):	-96
IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.10.1
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Up Time (Sec):	23879

4-3-3. Navigating the Website

A standard web page looks like Figure 4. The navigation bar runs along the top of the page, page specific feature groups are list in the left hand pane of the page and the specific parameters are shown in the main display pane.

Figure 4 - Web Page

The screenshot shows the Avery Dennison website interface. At the top is the logo and a navigation bar with links: Status, Configuration, Certificates, Network, and Maintenance. On the right of the navigation bar, it says "Device Type: UART". Below the navigation bar is a left-hand sidebar with two links: "Module Status" (selected) and "Radio Statistics". The main content area is titled "Module Status" and contains the following information:

Module Firmware Version:	2.11F
Radio Firmware Version:	2.2.146.14
Link Status:	Connected
SSID:	sewoo-wifi-qua
MAC Address:	000B6B7ECC57
BSSID:	82016B7E085D
Transmit Rate (Mb/s):	54
Signal Level (dBm):	-37
Noise Level (dBm):	-96
IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.10.1
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
Up Time (Sec):	557

At the bottom of the page, there is a red footer bar with links for "Quatech", "Contact us", and "Technical Support".

To select any of the items, move your cursor over the item and press the Left Hand mouse button. The items in the Navigation bar and the Feature bar are hyperlinks and will cause the mouse cursor to change form an arrow pointer to a finger pointer when placed over them.

To find out what a specific field does move the cursor over the field and hold of approximately a second. A help balloon will appear and will provide details on the function of the field and its valid range of values.

4-3-4. Configuration

Configuration menu includes all the menus for Wireless LAN setting.

Express Setup

As shown Figure 5, this can set the parameters in "Express Setup" menu.

Figure 5 – Express Setup Web Page

Express Setup	Current Values
Discovery OEM Device Name:	<input type="text" value="OEM-Cfg1"/>
Radio Startup Mode:	<input type="button" value="On"/>
WLAN Parameters	
WLAN Connection Type:	<input type="button" value="AdHoc"/>
SSID:	<input type="text"/>
WLAN Security Type:	<input type="button" value="Disabled"/>
IP Address Parameters	
WLAN DHCP:	<input type="button" value="Disabled"/>
WLAN Static IP Address:	<input type="text"/>
WLAN Subnet Mask:	<input type="text"/>
WLAN Gateway Address:	<input type="text"/>
<input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/>	

Discovery OEM Device Name

Configures the Discovery OEM Device Name. Name can be up to 31 characters with no spaces. Default is OEM-Cfg1.

Radio Startup Mode

Sets the startup state for the radio.

On = Normal mode (radio attempts to associate).

Off = Radio does not attempt to associate until an explicit radio-on command is given.

Sleep = Radio immediately goes to sleep at startup. Radio will wakeup via a pass mode connection attempt or the pm-mode wakeup command.

Default is On.

WLAN Connection Type

Configures the wireless interface operation type to participate in an infrastructure or peer-to-peer network.

Infrastructure = Infrastructure (AP) mode.

AdHoc = AdHoc (peer-to-peer) mode.

Unique AdHoc = Generate unique SSID in AdHoc (peer-to-peer) mode based on MAC address.

Access Point = Infrastructure (AP) Access Point mode.

Default is Infrastructure.

When Infrastructure / AdHoc →

SSID

Applies the SSID used for 802.11 association. SSID can be up to 32 characters.

In Infrastructure mode, the SSID controls which AP the module connects to and affects the module's roaming behavior. In AdHoc mode, the SSID defines the network name for the AdHoc devices.

Only the devices with the same SSIDs can connect to each other.

any = The module associates with the AP that has the best signal quality.

(other) = The module associates with the AP matching the SSID that has the best signal quality.

Default is any.

WLAN Security Type

Selects the Wireless Security Method for Authentication and Encryption.

Disabled = Wireless security is disabled.

WEP64 = WEP with 64-bit key length (sometimes referred to as 40-bit).

WEP128 = WEP with 128-bit key length.

WPA-LEAP* = WPA CISCO LEAP. Requires LEAP username and password.

WPA-PSK = WPA Pre-Shared Key. Requires WPA Passphrase.

WPA2-PSK = WPA2 Pre-Shared Key (WPA2-Personal). Requires WPA Passphrase.

PEAP* = EAP-PEAP with tunnelled EAP authentication.

Default is Disabled.

NOTE

Security methods marked with a * are not available in AP mode.

When WEP64 / WEP128 →

WEP Key 1

Sets WEP Key #1 to binary value. Can be 10 or 26 hex digits (10 digits for 64 bits, 26 digits for 128 bits).

Default is 000000000000000000000000.

When WPA-LEAP →

LEAP User Name

Configures the WPA-LEAP username. The LEAP username can be 1 to 32 characters and must match the LEAP username assigned on the LEAP server.

Default is admin.

LEAP Password

Configures the WPA-LEAP password. The LEAP password can be 1 to 32 characters and must match the LEAP password assigned to the LEAP user on the LEAP server.

The LEAP password cannot contain spaces.

Default is admin.

When WPA-PSK / WPA-PSK2 →

WPA / WPA2 Pre Shared Key (PSK)

Configures the Pre-Shared Key used with WPA-PSK or WPA2-PSK security. The input range is 8 to 63 ASCII characters or 64 hex characters. This key must match the key on the AP.

Default is "passphrase".

When PEAP →

PEAP Identity

Identity string for EAP. This field is also used to configure user NAI for EAP-PSK/PAX/SAKE/GPSK.

PEAP Password

Password string for EAP. This field can include either the plaintext password (using ASCII or hex string) or a NtPasswordHash (16-byte MD4 hash of password) in hash:(32 hex digits) format.

NtPasswordHash can only be used when the password is for MSCHAPv2 or MSCHAP (EAP-MSCHAPv2, EAP-TLS/MSCHAPv2, EAP-TTLS/MSCHAP, LEAP). EAP-PSK (128-bit PSK), EAP-PAX (128-bit PSK), and EAP-SAKE (256-bit PSK) is also configured using this field. For EAP-GPSK, this is a variable length PSK.

WLAN DHCP

Configures the DHCP Client to be enabled or disabled for the wireless interface. If the DHCP Client is enabled, the module will use DHCP to obtain an IP configuration. If DHCP fails to obtain the IP configuration, the module's IP address will be 0.0.0.0. However, if wl-dhcp-fb is enabled, then the values from wl-dhcp-fbip, wl-dhcp-fbsubnet, and wl-dhcp-fbgateway will be used as the IP address, subnet mask and gateway address until the module is power cycled.

If eth-role is bridge, this field specifies whether the Bridge Client is using DHCP. If enabled, the bridge will wait to configure itself until the client issues a DHCP request. If disabled, the bridge will attempt to pre-configure itself for the Client based upon the settings for wl-ip and br-client-mac. MSCHAPv2, EAP-TLS/MSCHAPv2, EAP-TTLS/MSCHAP, LEAP). EAP-PSK (128-bit PSK), EAP-PAX (128-bit PSK), and EAP-SAKE (256-bit PSK) is also configured using this field. For EAP-GPSK, this is a variable length PSK.

NOTE

DHCP can only be enabled for the wireless interface if the WLAN Connection Type is not Access Point.

Disabled = Use static IP

Enabled = Use DHCP

When DHCP Disable →

WLAN Static IP Address

Configures the static IP address of the wireless interface of the module if the DHCP Client is disabled. If the Ethernet Role is Router and the WLAN Connection Type is Access Point, this field configures the IP address of the first wireless client that associates to the module. If the wireless client is not using DHCP, this address must also be configured on the wireless client for IP routing to work correctly. If the Ethernet Role is Bridge and the WLAN Connection Type is not Access Point, this field pre-configures the IP address expected to be used by the Bridge Client and the Module if that Client uses static IP configuration. If the Ethernet Role is Bridge and the WLAN Connection Type is Access Point, this field is ignored. This is also the first IP address handed out by the module's internal wireless DHCP Server (if enabled).

Default is 192.168.1.99.

WLAN Subnet Mask

Configures the static subnet mask of the wireless interface of the module if the DHCP Client is disabled. If the Ethernet Role is Router and the WLAN Connection Type is Access Point, this field configures the subnet mask of the wireless client devices that associate to the module. If the wireless clients are not using DHCP, this subnet mask must also be configured on the wireless clients for IP routing to work correctly. If the Ethernet Role is Bridge and the WLAN Connection Type is Access Point, this field is ignored.

Default is 255.255.255.0.

WLAN Settings

Setting the WLAN Setting as follows

Figure 6 – WLAN Settings Web Page

WLAN Parameters	Current Values
Radio Startup Mode:	On <input type="checkbox"/>
WLAN Connection Type:	AdHoc <input type="checkbox"/>
SSID:	<input type="text"/> <input type="checkbox"/>
WLAN Channel:	1 <input type="checkbox"/>
WLAN TX Power (dBm):	15 dBm <input type="checkbox"/>
WLAN Beacon Interval:	100 <input type="checkbox"/>
Maximum Wireless Data Rate:	Auto <input type="checkbox"/>
Use Fixed Data Rate:	Disabled <input type="checkbox"/>
WLAN Region:	United States <input type="checkbox"/>

Radio Startup Mode

Sets the startup state for the radio.

On = Normal mode (radio attempts to associate).

Off = Radio does not attempt to associate until an explicit radio-on command is given.

Sleep = Radio immediately goes to sleep at startup. Radio will wakeup via a pass mode connection attempt or the pm-mode wakeup command.

Default is On.

WLAN Connection Type

Configures the wireless interface operation type to participate in an infrastructure or peer-to-peer network.

Infrastructure = Infrastructure (AP) Client mode.

AdHoc = AdHoc (peer-to-peer) mode.

Unique AdHoc = Generate unique SSID in AdHoc (peer-to-peer) mode based on MAC address.

Access Point = Infrastructure (AP) Access Point mode.

Default is Infrastructure.

When Infrastructure / AdHoc →

SSID

Applies the SSID used for 802.11 association. SSID can be up to 32 characters. In Infrastructure mode, the SSID controls which AP the module connects to and affects the module's roaming behavior. In AdHoc mode, the SSID defines the network name for the AdHoc devices. Only the devices with the same SSIDs can connect to each other.

any = The module associates with the AP that has the best signal quality.

(other) = The module associates with the AP matching the SSID that has the best signal quality. Default is any.

When AdHoc / Unique Adhoc →

WLAN Channel

Configures the wireless interface AdHoc channel number. The channel number is only applicable in AdHoc or Access Point mode.

Some channels are restricted in certain countries. OEMs must use only unrestricted channels. Channel range is 1 - 14.

WLAN TX Power (dBm)

Configures the wireless interface transmit power in dBm. This value has a range of 5 – 15 dBm. Default is 15.

When AdHoc / Unique Adhoc →

WLAN Beacon Interval

Configures the wireless interface beacon interval in milliseconds. This value is only applicable in AdHoc or Access Point mode. The range is 100 – 65535 milliseconds.

Default is 100.

Maximum Wireless Data Rate

Configures the maximum wireless data rate for the module (in Mbps). For rates above 1 Mbps, the module may fall back to a lower rate. Lower data rates may result in better range. Auto selects the best rate that gives acceptable performance.

Default is Auto.

Use Fixed Data Rate

Transmits at only the selected data rate. Default is Disabled

WLAN Region

Specifies the wireless channels allowed based on the region. Default is United States.

WLAN Security Settings

Setting the security configurations in Wireless LAN

Figure 7 – WLAN Security Settings Web Page

WLAN Security Parameters	Current Values
WLAN Security Type:	WPA2-FAST
Authentication Type:	Auto
EAP Settings	
Basic/Advanced Settings:	Basic
EAP Identity:	
EAP Password:	
CA Certificate File Name:	
EAP-FAST Settings	
EAP-FAST Provisioning Type:	Authenticated
Maximum Number of EAP-FAST Servers:	10
<input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/>	

WLAN Security Type

Selects the Wireless Security Method for Authentication and Encryption.

Disabled = Wireless security is disabled.

WEP64 = WEP with 64-bit key length (sometimes referred to as 40-bit).

WEP128 = WEP with 128-bit key length.

WEP-LEAP* = LEAP with WEP encryption.

WPA-LEAP* = WPA CISCO LEAP. Requires LEAP username and password.

WPA-LEAP64* = Migration mode w/ Cipher suite TKIP+40-bit WEP using EAP (LEAP).

Requires LEAP username and password.

WPA-LEAP128* = Migration mode w/ Cipher suite TKIP+128-bit WEP using EAP (LEAP).

Requires LEAP username and password.

WPA-PSK = WPA Pre-Shared Key. Requires WPA Passphrase.

WPA-PSK64* = Migration mode w/ Cipher suite TKIP+40-bit WEP using WPA PSK.

Requires WPA Passphrase.

WPA-PSK128* = Migration mode w/ Cipher suite TKIP+128-bit WEP using WPA PSK.

Requires WPA Passphrase.

WPA-PSK128-TKIP* = Migration mode w/ Cipher suite TKIP and/or 128-bit WEP for the Group Cipher using WPA PSK. Requires WPA Passphrase.

WPA2-PSK = WPA2 Pre-Shared Key (WPA2-Personal). Requires WPA Passphrase.

WPA2-PSK-TKIP* = WPA2-PSK Migration mode w/ Group Cipher suites TKIP and/or WPA2 Pre-Shared Key (WPA2-Personal). Requires WPA Passphrase.

PEAP* = EAP-PEAP with tunnelled EAP authentication.

TLS* = EAP-TLS. Requires both a Client and Server (CA) certificate.

TTLS* = EAP-TTLS with tunnelled EAP or PAP/CHAP/MSCHAP/MSCHAPV2 authentication.

WPA-FAST* = EAP-FAST w/ Cipher suite TKIP.

WPA2-FAST* = EAP-FAST w/ Cipher suite AES-CCMP.

Default is Disabled.

NOTE

Security methods marked with a * are not available in AP mode.

Authentication Type

Configures the authentication type.

Auto = Authenticate using Open Key algorithm.

Open = Authenticate using Open Key algorithm.

Shared = Authenticate using Shared Key algorithm.

Default is Auto.

When WEP64 / WEB128 →

Default WEP Key

Configures the default WEP key index. This must match the key index configured on the AP.

Range is 1 - 4.

Default is 1.

WEP Key 1~4

Sets WEP Key 1~4 to binary value. Can be 10 or 26 hex digits

(10 digits for 64 bits, 26 digits for 128 bits).

Default is 00000000000000000000000000000000.

When WEP-LEAP →

LEAP User Name

Configures the WPA-LEAP username. The LEAP username can be 1 to 32 characters and must match the LEAP username assigned on the LEAP server.

Default is admin.

LEAP Password

Configures the WPA-LEAP password. The LEAP password can be 1 to 32 characters and must match the LEAP password assigned to the LEAP user on the LEAP server. The LEAP password cannot contain spaces.

Default is admin.

When WPA-LEAP / WPA-LEAP64 / WPA-LEAP128 →

WPA Protocol Version

Selects the preferred WPA protocol.

Selecting a specific protocol helps speed up roaming versus automatic selection.

Auto = Automatically negotiate the protocol for WPA.

WPA = Use WPA for the protocol.

RSN = Use RSN (WPA2) for the protocol.

Default is Auto.

LEAP User Name

Configures the WPA-LEAP username. The LEAP username can be 1 to 32 characters and must match the LEAP username assigned on the LEAP server.

Default is admin.

LEAP Password

Configures the WPA-LEAP password. The LEAP password can be 1 to 32 characters and must match the LEAP password assigned to the LEAP user on the LEAP server. The LEAP password cannot contain spaces.

Default is admin.

When WPA-PSK / WPA-PSK64 / WPA-PSK128 / WPA-PSK128-TKIP / WPA2-PSK / WPA2-PSK-TKIP →

PA / WPA2 Pre Shared Key (PSK)

Configures the Pre-Shared Key used with WPA-PSK or PA2-PSK security. The input range is 8 to 63 ASCII characters or 64 hex characters. This key must match the key on the AP.

Default is "passphrase".

When PEAP →

WPA Protocol Version

Selects the preferred WPA protocol. Selecting a specific protocol helps speed up roaming versus automatic selection.

Auto = Automatically negotiate the protocol for WPA.

WPA = Use WPA for the protocol.

RSN = Use RSN (WPA2) for the protocol.

Default is Auto.

Basic/Advanced Settings

Selects from a basic or advanced WPA/WPA2/EAP settings page.

Basic = Basic WPA/WPA2/EAP parameters are displayed.

Advanced = The entire list of WPA/WPA2/EAP parameters are displayed.

Default is Basic.

EAP Identity EAP Identity

Identity string for EAP. This field is also used to configure user NAI for EAP-PSK/PAX/SAKE/GPSK.

EAP Password

Password string for EAP. This field can include either the plaintext password (using ASCII or hex string) or a NtPasswordHash (16-byte MD4 hash of password) in hash:(32 hex digits) format.

NtPasswordHash can only be used when the password is for MSCHAPv2 or MSCHAP (EAP-MSCHAPv2, EAP-TLS/MSCHAPv2, EAP-TTLS/MSCHAP, LEAP). EAP-PSK (128-bit PSK), EAP-PAX (128-bit PSK), and EAP-SAKE (256-bit PSK) is also configured using this field.

For EAP-GPSK, this is a variable length PSK.

CA Certificate File Name

The CA certificate file name. (PEM/DER) This file can have one or more trusted CA certificates. A trusted CA certificate should always be configured when using EAP-TLS, TTLS, or PEAP.

When Advanced →

EAP Anonymous Identity

Anonymous identity string for EAP (to be used as the unencrypted identity with EAP types that support different tunnelled identity, e.g., EAP-TTLS).

EAP Phase 1 String

Phase1 (outer authentication, i.e., TLS tunnel) parameters (string with field-value pairs, e.g., "peapver=0"). 'peap_outer_success=0' can be used to terminate PEAP authentication on tunneled EAP-Success. This is required with some RADIUS servers that implement draft-josefsson-pppext-eap-tls-eap-05.txt (e.g., Lucent NavisRadius v4.4.0 with PEAP in "IETF Draft 5" mode url : <http://www.watersprings.org/pub/id/draft-josefsson-pppext-eap-tls-eap-05.txt>). 'include_tls_length=1' can be used to force pa_suppllicant to include LS Message Length field in all TLS messages even if they are not fragmented. 'sim_min_num_chal=3' can be used to configure EAP-SIM to require three challenges (by default, it accepts 2 or 3). 'result_ind=1' can be used to enable EAP-SIM and EAP-AKA to use protected result indication. 'crypto_binding' option can be used to control PEAPv0 cryptobinding behavior:
0 = Do not use cryptobinding.
1 = Use cryptobinding if server supports it (default).
2 = Require cryptobinding.

EAP Phase 2 String

Phase2 (inner authentication with TLS tunnel) parameters (string with field-value pairs, e.g., "auth=MSCHAPV2" for EAP-PEAP or "autheap=MSCHAPV2 autheap=MD5" for EAP-TTLS). The following certificate/private key fields are used in inner Phase2 authentication when using EAP-TTLS or EAP-PEAP.

ca-cert2-filename: File path to CA certificate file. This file can have one or more trusted CA certificates. If ca-cert2-filename is not included the server certificate will not be verified. This is insecure and a trusted CA certificate should always be configured.

client-cert2-filename: Client certificate file name.

priv-key2-filename: Path to client private key file name.

priv-key2-password: Password for private key file name.

dh-param2-filename: DH/DSA parameters file name (in PEM format).

subject_match2: Substring to be matched against the subject of the authentication server certificate.

altsubject_match2: Substring to be matched against the alternative subject name of the authentication server certificate.

EAP Subject Match String

Substring to be matched against the subject of the authentication server certificate. If this string is set, the server certificate is only accepted if it contains this string in the subject.

The subject string is in following format:

/C=US/ST=CA/L=San Francisco/CN=Test AS/emailAddress=as@example.com

EAP Alternate Subject Match/Match2 String

Semicolon separated string of entries to be matched against the alternative subject name of the authentication server certificate. If this string is set, the server certificate is only accepted if it contains one of the entries in an alternative subject name extension.

altSubjectName string is in TYPE:VALUE format.

Example:

EMAIL:server@example.com

Example:

DNS:server.example.com;

DNS:server2.example.com Following types are supported:

EMAIL, DNS, URI

CA Certificate 2 File Name

The CA certificate 2 file name. (PEM/DER) This file can have one or more trusted CA certificates. A trusted CA certificate should always be configured when using EAP-TLS, TTLS, or PEAP.

Client Certificate/Certificate2 File Name

The client certificate/certificate2 file name. (PEM/DER)

Private Key File Name

The client private key file name. (PEM/DER/PFX) When PKCS#12/PFX files are used the client-cert-filename should not be used.

Private Key File Password

The password for the private key file.

Private Key 2 File Name

The password for the private key file.

Private Key File 2 Password

The client private key 2 file name. (PEM/DER/PFX) When PKCS#12/PFX files are used the client-cert2-filename should not be used.

DH Parameter/Parameter2 File Name

DH/DSA parameters/parameters2 file name (in PEM format). This is an optional configuration file for setting parameters for an ephemeral DH key exchange. In most cases, the default RSA authentication does not use this configuration. However, it is possible to setup RSA to use ephemeral DH key exchange. In addition, ciphers with DSA keys always use ephemeral DH keys. This can be used to achieve forward secrecy. If the file is in DSA parameters format, it will be automatically converted into DH params.

Network Settings

Setting the DHCP or IP configuration in Wireless LAN.

Figure 8 – Network Settings Web Page

Network Parameters	Current Values
WLAN Specific Settings	
WLAN DHCP:	Disabled <input type="button" value="info"/>
WLAN DHCP Client Name:	Airborne7ECC57 <input type="button" value="info"/>
WLAN Static IP Address:	<input type="text"/> <input type="button" value="info"/>
WLAN Subnet Mask:	<input type="text"/> <input type="button" value="info"/>
WLAN Gateway IP Address:	<input type="text"/> <input type="button" value="info"/>
Common Settings	
DNS Server1 IP Address:	0.0.0.0 <input type="button" value="info"/>
DNS Server2 IP Address:	0.0.0.0 <input type="button" value="info"/>
WINS Server1 IP Address:	0.0.0.0 <input type="button" value="info"/>
WINS Server2 IP Address:	0.0.0.0 <input type="button" value="info"/>
<input type="button" value="Commit"/> <input type="button" value="Cancel"/> <input type="button" value="Defaults"/>	

WLAN DHCP

Configures the DHCP Client to be enabled or disabled for the wireless interface. If the DHCP Client is enabled, the module will use DHCP to obtain an IP configuration. If DHCP fails to obtain the IP configuration, the module's IP address will be 0.0.0.0. However, if wl-dhcp-fb is enabled, then the values from wl-dhcp-fbip, wl-dhcp-fbsubnet, and wl-dhcp-fbgateway will be used as the IP address, subnet mask and gateway address until the module is power cycled. If eth-role is bridge, this field specifies whether the Bridge Client is using DHCP. If enabled, the bridge will wait to configure itself until the client issues a DHCP request. If disabled, the bridge will attempt to pre-configure itself for the Client based upon the settings for wl-ip and br-client-mac.

NOTE

DHCP can only be enabled for the wireless interface if the WLAN Connection Type is not Access Point.

Disabled = Use static IP

Enabled = Use DHCP

WLAN DHCP Client Name

Configures the DHCP Client Host Name to use in the DHCP requests for the wireless interface. On some APs, this name is displayed along with the MAC address in the list of attached devices. Name can be up to 31 characters. Default is Airbornexxxxxx, where xxxxxx are the last six hexadecimal digits of the module's MAC address.

When DHCP Disable →

WLAN Static IP Address

Configures the static IP address of the wireless interface of the module if the DHCP Client is disabled. If the Ethernet Role is Router and the WLAN Connection Type is Access Point, this field configures the IP address of the first wireless client that associates to the module. If the wireless client is not using DHCP, this address must also be configured on the wireless client for IP routing to work correctly. If the Ethernet Role is Bridge and the WLAN Connection Type is not Access Point, this field pre-configures the IP address expected to be used by the Bridge Client and the Module if that Client uses static IP configuration. If the Ethernet Role is Bridge and the WLAN Connection Type is Access Point, this field is ignored. This is also the first IP address handed out by the module's internal wireless DHCP Server (if enabled).

Default is 192.168.1.99.

WLAN Subnet Mask

Configures the static subnet mask of the wireless interface of the module if the DHCP Client is disabled. If the Ethernet Role is Router and the WLAN Connection Type is Access Point, this field configures the subnet mask of the wireless client devices that associate to the module. If the wireless clients are not using DHCP, this subnet mask must also be configured on the wireless clients for IP routing to work correctly. If the Ethernet Role is Bridge and the WLAN Connection Type is Access Point, this field is ignored. Default is 255.255.255.0.

WLAN Gateway IP Address

Configures the static gateway IP address of the module if the DHCP Client is disabled.

If the Ethernet Role is Router and the WLAN Connection Type is Access Point, this field configures the static IP address of the wireless interface of the module. This address also configures the default gateway address of the wireless client devices that associate to the module.

If the wireless clients are not using DHCP, this gateway address must also be configured on the wireless clients for IP routing to work correctly.

If the Ethernet Role is Bridge and the WLAN Connection Type is Access Point, this field is ignored.

Default is 0.0.0.0.

When DHCP Enable →

WLAN DHCP Acquire Limit

Configures the number of seconds that the module should wait to acquire its IP configuration using DHCP before applying the DHCP fallback algorithm (if enabled) for the wireless interface. This is an integer with a range of 1-255 seconds.

Default is 150.

NOTE

"0" will turn off IP Fallback.

WLAN DHCP Fallback

Configures the DHCP fallback algorithm. When the DHCP fallback algorithm is enabled, the module will apply the configuration from wl-dhcp-fbip, wl-dhcp-fbgateway, and wl-dhcp-subnet as the static IP configuration, if the DHCP client has not received its IP configuration after wl-dhcp-acqlimit seconds.

Disabled = Disable DHCP fallback (default for UART, Direct Serial)

Enabled = Enable DHCP fallback (default for SPI, Direct Ethernet)

When DHCP Fallback Enable →

WLAN Fallback to Last DHCP IP Address

Enabling this will cause the module to set the wl-dhcp-fbip, wl-dhcp-fbgateway, wl-dhcp-fbsubnet, dns-server1, and dns-server2 to their current values each time an IP address is successfully acquired using DHCP. This will only occur if wl-dhcp-fb is set and the wl-dhcp-acqlimit is not 0 (zero). If wl-dhcp-fbper is not enabled, the current fallback IP address will not be saved across reboots.

Default is Disabled.

When WLAN Fallback to Last DHCP IP Address Enable →

Save Last WLAN DHCP IP Address as Fallback IP Address

Enabling this will cause the wl-dhcp-fbip, wl-dhcp-fbgateway, wl-dhcp-fbsubnet, dns-server1, and dns-server2 to be saved to flash memory each time it changes. This will make these values persistent across restarts or power cycles. This will only occur if wl-dhcp-fb and wl-dhcp-fbauto are enabled and the wl-dhcp-acqlimit is not 0 (zero).

Default is Disabled.

WLAN Fallback IP Address

Configures the IP address used by the DHCP fallback algorithm.

Default (UART, Direct Serial) is 192.168.10.1. Default (SPI, Direct Ethernet) is 0.0.0.0.

WLAN Fallback Subnet Mask

Configures the Subnet Mask used by the DHCP fallback algorithm.

Default is 255.255.255.0.

WLAN Fallback Gateway IP Address

Configures the gateway address used by the DHCP fallback algorithm.

Default is 0.0.0.0.

DNS Server1 IP Address

Configures the Primary DNS Server Address. This value is used for DNS lookups. If the DHCP Client is enabled, the dns-server1 value will be updated if the DHCP Server provides one.

Default is 0.0.0.0.

DNS Server2 IP Address

Configures the Secondary DNS Server Address. This value is used for DNS lookups, if the lookup fails using the value from dns-server1. If the DHCP Client is enabled, the dns-server2 value will be updated if the DHCP Server provides one.

Default is 0.0.0.0.

WINS Server1 IP Address

Configures the Primary WINS Server Address. This value is used for WINS lookups. If the DHCP Client is enabled, the wins-server1 value will be updated if the DHCP Server provides one. Default is 0.0.0.0.

WINS Server2 IP Address

Configures the Secondary WINS Server Address. This value is used for WINS lookups, if the lookup fails using the value from wins-server1. If the DHCP Client is enabled, the wins-server2 value will be updated if the DHCP Server provides one. Default is 0.0.0.0.

When DHCP Enable →

DHCP Request Retransmission Mode

Configures the DHCP request retransmission mode to either Exponential Interval or Fixed Interval. Default is Exponential Interval.

DHCP Request Retransmission Interval

Configures the DHCP request retransmission interval (in seconds) to use when wl-dhcp-mode is set to fixed. This is an integer with a range of 1-64. Default is 15.

Upload Configuration Files

The Airborne Device Server module supports both OEM and User configuration files for provisioning the module. Delivery of these configuration files can be performed through the web interface.

To upload configuration files follow the steps in Table 2.

In this menu, you can load the Configuration file and save to the Module.

Figure 9 - Upload Configuration Files Web Page

Upload a Configuration File to the Module

Select a Configuration File to upload and save on the module:

Select the destination filename:

User Configuration
 Encrypted Configuration
 OEM Configuration

Table 2 - Uploading Configurations

Step	Description
Navigation Bar Select Configuration	You will see major WLAN parameters displayed.
Feature Bar Select Upload Configuration File	You will see a window open with field to enter the location of the configuration you want to upload, along with a choice of OEM or User Configuration.
Press Browse... Button	This will open a dialog box in which you can locate the certificate you wish to upload to the module. Select the configuration file and press Open . This will return you to the Configuration Upload window and will have entered the location and file name of the certificate you wish to upload in the field next to the Browse... button.
Select User or OEM Configuration	This defines the configuration you are installing. OEM Configurations will survive a factory reset, User Configurations will not.
Press Upload Configuration	You will then see a notice that the configuration has been successfully uploaded to the module.

Uploading a configuration file will overwrite any configuration file already stored on the module. This will cause a change in configuration when a module restart is performed.

IMPORTANT!!

Confirm that the OEM or USER settings in the configuration files will allow the user to communicate with the module after the upload and a restart has been completed.

Delete Configuration File

You can delete the configuration files saved in the Module.

Figure 10 – Delete Configuration File Web Page

Delete a Configuration File From Flash

Choose a Configuration File to Delete:

Choose a Configuration File... Delete File

4-3-5. Certificates

Upload Certificate

Adding certificates to the Airborne Device Server module is very easy when using the web interface. See Figure11 and Table3.

Figure 11 - upload Certificate Web page

The screenshot shows a web interface for uploading certificates. At the top, there is a navigation menu with the Avery Dennison logo and links for Status, Configuration, Certificates, Network, and Maintenance. The current page is titled "Upload a Certificate to the Module". Below the title, there is a section for selecting a certificate file to upload, with a text input field and a "찾아보기..." (Find) button. Below this are "Upload Certificate" and "Cancel" buttons. On the left side, there is a sidebar menu with options: "Upload Certificate", "List Certificates", and "Delete Certificate". At the bottom of the page, there is a red footer bar with the text "Avery Dennison", "Contact us", and "Technical Support".

Table 3 - Uploading Certificates

Step	Description
Navigation Bar Select Configuration	You will see a list of certificates currently resident on the module when you enter the Certificate File List window.
Feature Bar Select Upload Certificates	You will see a window open with field to enter the location of the certificate you want to upload.
Press Browse... Button	This will open a dialog box in which you can locate the certificate you wish to upload to the module. Select the Certificate file and press Open . This will return you to the Certificate Upload window and will have entered the location and file name of the certificate you wish to upload in the field next to the Browse... button.
Press Upload Certificate	You will then see a notice that the certificate has been successfully uploaded to the module.

Delete Certificate

Delete a security certificate from the module.

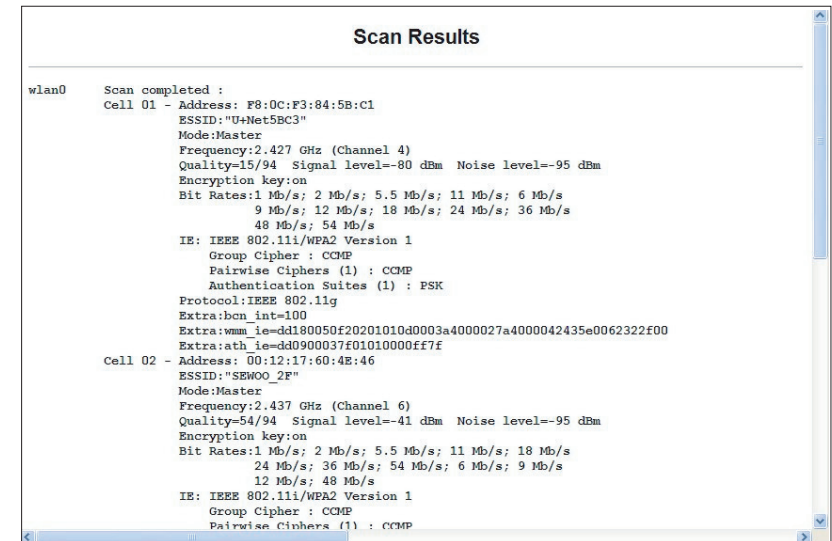
Figure 12 – Delete Certificate



4-3-6. Network

The “Scan for Access Points” are in the “Network” menu.
“Scan for Access Points” shows “MAC Address, ESSID, Mode, Frequency, Quality, Signal level, Noise level, Encryption key, Bit rates, Protocol, Extra” information for the terminals which are connected the AP linked to the Module.

Figure 13 – Scan Results



4-3-7. Maintenance

Maintenance menu includes "Update Module Firmware, Reset to Factory Defaults, Restart Module" functions.

Update Module Firmware

The module's firmware may be updated using the web interface; please refer to Table 5 for the procedure to do this.

Updating the firmware will not alter any existing configuration files or certificates loaded on the module.

You will first need to obtain the version of firmware you wish to install from the Quatech website or Quatech technical support. The firmware will be a binary image file (.img) and indicate the version of the firmware in the file name.

Once you have obtained the firmware, save the firmware image to a location on the system you are browsing the module from, or a location accessible to the system you are browsing the module from.

Figure 14 - Firmware Update Page

Upload Firmware to the Module

Current Firmware Version = 2.11F

Select the firmware image file to load and then click "Load New Firmware"

Figure 15 - Firmware Update in Progress

Flashing Firmware in the Module

Transferring the firmware file
File retrieved successfully - Flashing the module

This should take approximately 90 seconds

Do not turn off the power!

Figure 16 - Firmware Update Complete

Flashing Firmware in the Module

Transferring the firmware file
File retrieved successfully - Flashing the module

This should take approximately 90 seconds

Do not turn off the power!

Firmware flashing completed successfully.

Table 4 - Updating Firmware

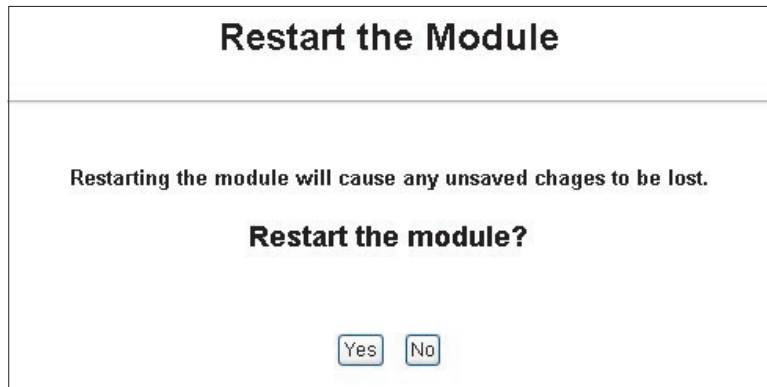
Step	Description
Navigation Bar Select Maintenance	This will open a window showing the current module status.
Feature Bar Select Update Module Firmware	You will see a window open with field to enter the location of the module firmware you want to upload. The current firmware version number is displayed at the top of the page.
Press Browse... Button	This will open a dialog box in which you can locate the firmware image you wish to upload to the module. Select the firmware image file and press Open . This will return you to the Upload Firmware window and will have entered the location and file name of the firmware image you wish to upload in the field next to the Browse... button.
Press Load New Firmware	You will then see a notice that the firmware upload has begun (Figure 20). When the upload has been completed successfully and the firmware updated w window indicating this will be shown (Figure 21).
Press Reboot	This will restart the module and the new firmware will be loaded.

DO NOT REMOVE POWER FROM THE MODULE DURING THE FIRMWARE UPDATE CYCLE. This may cause the device to become non-operational. If this happens please contact Quatech Technical Support.

Restart Module

Select reboot module, the following message is shown. Select "Yes", the Module is reset.

Figure 17 – Module Reset



4-3-8. Updating a Field

To update a field, select the field by pressing the Left Hand mouse button. Then either type in the appropriate content or select from the pull down menu.

Once you have finished modifying parameters, scroll to the bottom of the page and press the Commit button. The page will then indicate the changes have been completed successfully, you can then return to the configuration page by pressing the Reload button or restart the module by pressing the Reboot button

Figure 18 – Updating a field



NOTE

The changes to the parameters will not be applied until a module restart has been completed.

Before the Commit button has been pressed, all modified fields can be returned to their original state by pressing the Cancel button.

4-4. Wi-Fi Glossary

Access Point

An interface between a wireless network and a wired network. Access points can be used with Ethernet or other communications to enable roaming throughout a facility.

Ad-Hoc Mode

A wireless network composed of devices that contain a network interface card and no access point. Ad-Hoc mode is also called peer-to-peer (point-to-point) communications or BSS network. As long as the devices are in range and are on the same channel and SSID, they connect and communicate. Use this mode if a wireless infrastructure does not exist or where services are not required.

Authentication Method

Identifies users on a network, based on a username and password. There are two types, open and shared. Authentication protocols include LEAP, PEAP, TLS, TTLS, EAP-FAST, and PSK.

Auto Method

One of the available boot methods. Auto tries DHCP, BOOTP, and RARP, then sets to the last IP address used if the IP address is not automatically set using any of the previous methods.

BOOTP or Bootstrap Protocol

One of the available boot methods. It is a protocol used by devices that know their MAC address, but do not know their IP address. The device broadcasts its hardware address and the BOOTP server responds with the IP address for it. The network administrator must enter the MAC address in the BOOTP Config file to obtain the IP address from the server.

Boot Method

The wireless print server uses this method to obtain an IP address. Can be set to Auto, DHCP, BOOTP, RARP, or Static. Boot Tries The number of times the device tries to get an IP address from the server when using the BOOTP and DHCP methods.

BSS or Basic Service Set

A set of 802.11b/g devices operating as a fully connected wireless network.

BSSID : See MAC Address.

Channel or RF Channel

You can select which channel your network devices use to communicate. All devices must be on the same channel to communicate in Ad-Hoc mode. Other radio devices such as Bluetooth® wireless devices, microwave ovens, or 2.4-GHz cordless phones may operate/interfere if they are on the same channel as your network.

DHCP or Dynamic Host Configuration Protocol

One of the available boot methods. It is a protocol that issues IP addresses automatically within a specified range to devices (such as printers) when they are first turned on. The device keeps the IP address for a defined period of time set by your System Administrator; however, a device could have a different IP address every time it connects to the network.

EAP (Extensible Authentication Protocol)

Defines how to pass authentication information between the device and authentication server. The authentication is handled by the EAP type: FAST, TLS, TTLS, etc.

FAST (Flexible Authentication via Secure Tunneling)

Cisco Systems® developed this authentication protocol. It does not use certificates to authenticate, but a PAC (Protected Access Credential), which is managed dynamically by the server. The PAC is distributed one at a time to the client manually or automatically.

Gateway

Allows connections (communications) between different subnets on a network.

Infrastructure Mode

Requires an access point to communicate with other devices on the network. In infrastructure mode, wireless devices can communicate with each other or with a wired network.

IP Address

One of the available boot methods. It is a protocol used by devices that know their MAC address, but do not know their IP address. The device broadcasts its hardware address and the BOOTP server responds with the IP address for it. The network administrator must enter the MAC address in the BOOTP Config file to obtain the IP address from the server.

Boot Method

The wireless print server uses this method to obtain an IP address. Can be set to Auto, DHCP, BOOTP, RARP, or Static. Boot Tries The number of times the device tries to get an IP address from the server when using the BOOTP and DHCP methods.

LEAP (Lightweight Extensible Authentication Protocol)

Cisco Systems® introduced this authentication protocol and provides mutual authentication with unique WEP keys for each user. New keys are issued based on a time limit. Changing the WEP key time limits provides additional security.

LPD/LPR

A printer protocol that uses TCP/IP to establish connections between printers on a network. Also known as Line Printer Daemon/Line Printer Remote.

MAC Address or Media Access Control

A hardware address (6-byte) that uniquely identifies each node of a network. The MAC address is set during manufacturing and does not change. Also, two Network Interface Cards (NIC) will not have the same value.

MSCHAPv2

The Microsoft® version of CHAP. It is a three-way handshake protocol that is more secure than PAP. It provides mutual authentication between devices.

NIC or Network Interface Card

An adapter (board or card) that can be inserted into a device, so the device can be connected to a network. The NIC converts data from the device into the form transmitted or received from the network.

Node

A processing location on a network. The location can be a workstation, computer, or printer. Each Node has a unique MAC address.

Open Authentication

This allows any device to authenticate and then attempt to communicate with the access point. Any wireless device can authenticate with the accesspoint, but if WEP is used, the device can communicate only if its WEP keys match the access point's. There is no challenge that occurs, you either have the correct key or not when you communicate with the access point. By eliminating the challenge process, it actually makes this more secure than shared key authentication

PAP (Password Authentication Protocol)

A simple authentication protocol used with PPP (Point-to-Point Protocol). It is a plain text password system, which is not very secure. Pathname/The location of a particular file or directory that includes the full path to the needed filename or directory. This is a combination of path and filename.

PEAP (Protected Extensible Authentication Protocol) :

Authenticates clients into a network using only server-side certificates, which makes implementing and administering a wireless LAN easier.

Ping

A way to determine if a device is accessible. It sends a packet to the specified address and waits for a reply.

Protocol

This is the way two devices transmit data between each other, including error checking, data compression, and how messages start and end.

PSK (Pre-Shared Key)

Authentication mode of WPA used in SOHO environments. The key value(or pass-phrase) is used for network authentication only (not data encryption). It does not use a RADIUS server like the other modes, but uses a shared key to provide the initial authentication with the access point or host.

RADIUS (Remote Authentication Dial-In Server)

This is an authentication server, such as the Cisco® ACS, Microsoft® IAS, etc.

RARP

One of the available boot methods. The device sends an RARP request and the RARP server responds with an IP address. The device knows its MAC address and the server responds with the IP address for it.

Router

Any device that forwards data along networks. Routers are located at gateways.

Shared Authentication

The access point sends an unencrypted challenge text string to any device attempting to communicate with it. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored; however, this leaves the access point open to attack. Because of this weakness, shared key authentication can be less secure than open authentication.

Signal Strength

A percentage (1 to 100) of the connection between the device and access point. If the signal strength is 0, there is no connection with the access point; 30 or less indicates you may be experiencing interference or close to being out of access point range, and below 50, printing performance could be affected. To improve the signal strength, try moving the printer closer to the access point and away from other radio devices such as Bluetooth® wireless devices, microwave ovens, or 2.4-GHz cordless phones.

Speed or Transmit Rate

Sets the maximum rate of communication between the devices on the network. It is also called transmit rate. The speeds are in megabits per second (Mbps) and include: 1, 2, 5.5, 11, 12, 18, 24, 36, 48, and 54.

SSID or Service Set Identifier

A unique identifier that must match for all nodes on a subnetwork to communicate with each other. It consists of up to 32 characters (any printable character, including spaces). If using the space character, it must be enclosed in quotation marks. It is case-sensitive.

Static Method

One of the available boot methods. Use static if your network uses fixed configuration. The IP address remains the same every time the device connects to the network.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with the same prefix. For example, all devices that start with 192.192.192 are part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons.

Subnet Mask

A mask is used to determine what subnet an IP address belongs to. Companies often have ranges of IP addresses that can be described by one or more masks. For example, a mask of 255.255.255.0 allows variation in the last position only, because the first three positions are fixed.

TCP/IP

A way that two devices can transmit data between each other. TCP/IP (Transmission Control Protocol/ Internet Protocol) is generally the standard for transmitting data over a network.

TKIP (Temporal Key Integrity Protocol)

Changes the encryption keys regularly and has time limits before new keys are created. Changing the key periodically provides additional security.

TLS (Transport Layer Security)

A cryptographic protocol that uses client-side and server-side certificates to authenticate users on the Web. It can dynamically create user-based and session-based keys.

TTLS (Tunneled Transport Layer Security)

Provides certificate-based, server-side, mutual authentication of the client and network through an encrypted channel (or tunnel). It can dynamically create user-based and session-based keys.

WEP or Wired Equivalent Privacy

A security protocol for wireless local area networks. WEP was designed to provide the same level of security as that of a wired network, which is inherently more secure than a wireless network because wired networks are easily protected against unauthorized access. Wireless networks use radio waves to communicate and can be vulnerable to unauthorized users. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted. However, it has been found that WEP is not as secure as once believed

NOTE

If one part of a wireless network has WEP enabled, they all must have it enabled with the same key or they cannot communicate.

128 Bit / 64 Bit WEP Key

This is the 64 or 128 bit WEP key that must match other Nodes' encryption keys to communicate: 10 hex characters for 64 bit (40 serspecifiedcharacters), or 26 hex characters for 128 bit (104 user-specified characters). You must use the same key values for devices to communicate with each other

WLAN or Wireless Local Area Network

A LAN that uses high-frequency radio waves to communicate between nodes, rather than telephone wires, etc

WPA (Wi-Fi Protected Access)

A network security protocol that uses improved authentication and temporal keys. It was created to address the weaknesses of WEP encryption.

WPA2(or IEEE 802.11i) :

A network security protocol with stronger encryption than WPA. It was created to address the weaknesses of WEP encryption.

4-5. Wi-Fi Specifications

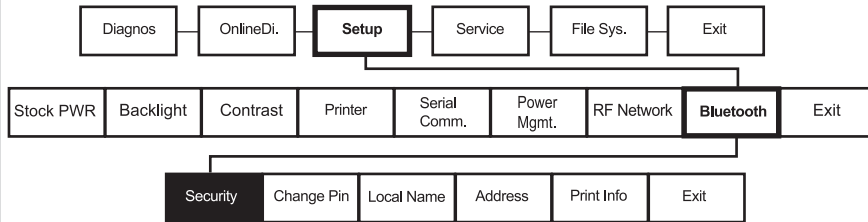
- Frequency 2.4 ~ 2.4835 GHz (US/Canada/Europe), 2.4 ~ 2.497 GHz (Japan)
- Communication Rate : 802.11b = 11, 5.5, 2, 1 Mbps
802.11g = 54, 48, 36, 24, 18, 12, 9, 6 Mbps
- Channels : USA/Canada: 11 channels
Europe: 13 channels
France: 7 channels
Japan: 14 channels (13 channels for 802.11g)
- Mode : Ad-Hoc or infrastructure
- Receive Sensitivity : 54Mb/s = -75dBm
36Mb/s = -82dBm
18Mb/s = -88dBm
6Mb/s = -93dBm
11Mb/s = -88dBm
1Mb/s = -98dBm
- Network Protocol : TCP/IP, ARP, ICMP, DHCP, DNS, UDAP, TFTP, UDP, PING
- Security Protocols :

Personal	Disabled, WEP 64 & 128bit, WPA (TKIP), WPA (AES), WPA2(AES), 802.1x (EAP) Supplicant 802.11i
WPA & WPA2 Enterprise supplicants	EAP-TLS, EAP-TTLS(MSCHAPv2), EAPTTLS(MD5), EAP-PEAPv0(MSCHAPv2), EAP-FAST, LEAP
Supports Certificates and Private Key Upload and Storage (Multiple)	

5. Bluetooth

5-1. Using the Bluetooth Settings Dialog

This Menu sets Bluetooth communication.



5-1-1. Enabling the Security

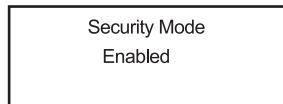
1. Select Setup **Menu – Bluetooth – Security.**



2. Select one of Enable and Disable.



3. Selected option is displayed as shown below



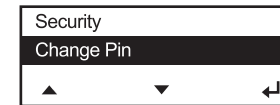
4. Press Enter(↵) button to exit.

NOTE

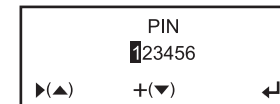
Refer to “3-1-14. Bluetooth Interface” for the Bluetooth configuration.

5-1-2. Change Pin

1. Select Setup **Menu – Bluetooth – Change Pin.**



2. Screen to set PIN appears as shown below.



3. On above screen, if Up(▲) button is pressed then the position of cursor moves towards right side by one step. If Down(▼) button is pressed then the selected character is increased.

4. Press Enter(↵) button to save and exit.

5-1-3. Local Name

1. Select Setup **Menu- Bluetooth – Local Name**



2. The screen to set Local Name appears as shown below.



3. On above screen, if Up(▲) button is pressed then the position of cursor moves towards right side by one step. If Down(▼) button is pressed then the selected character is increased.

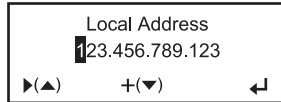
4. Press Enter(↵) button to save and exit.

5-1-4 Local Address

1. Select Setup **Menu – Bluetooth – Local Address.**



2. The screen to set Local Name appears as shown below.



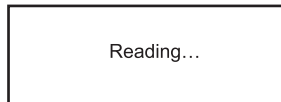
3. On above screen, if Up(▲) button is pressed then the position of cursor moves towards right side by one step. If Down(▼) button is pressed then the selected character is increased.
4. Press Enter(↵) button to save and exit.

5-1-5 Printing Info

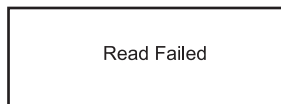
1. Select Setup **Menu – Bluetooth – Printing Info.**



2. You may see:



3. If it is successful, it starts to print, and if not, you see:



4. Press any key to exit

5-2. Bluetooth Interface



5-2-1. Printer Connection Settings

Printer Connection Settings

Port : COM1

BaudRate : 19200

Data Bits : 8

Parity : NONE

Stop Bits : 1

Open Port Close Port

Save Serial Port Configuration

You can connect the printer to PC by Serial (COM1 – COM9) or USB port. When you use Serial Port, you have to check the BaudRate setting between the printer & PC. When the printer is connected with PC, you can change the BaudRate setting of the printer. You can save the changed BaudRate to the printer by executing 'Save Serial Port Configuration'. You can disconnect printer from the PC by clicking 'Close Port'.

5-2-2. Get Bluetooth Information

Get Bluetooth Information

BT Address : 00:13:7b:52:f5:f0

You can get 12 characters Bluetooth Address.

5-2-3. PIN Code Information

PIN Code Information

PIN Code : 0000

Save Bluetooth PIN Code

You can register Bluetooth PIN Code by inputting PIN Code and execute "Save Bluetooth PIN Code"

5-2-4. Discoverable Mode Information

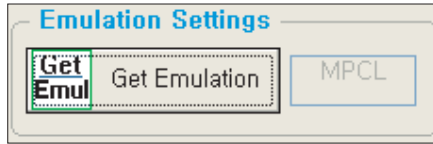
Discoverable Mode Information

ON OFF

Save Discoverable Mode

When you set "Discoverable Mode" as ON, the printer can be detected by other Bluetooth devices(PDA, Smart Phone...) and when you set it as "Off", the printer can not be detected by other devices.

5-2-5. Emulation Settings



When you click "Get Emulation", you can see the current emulation setting of the printer.