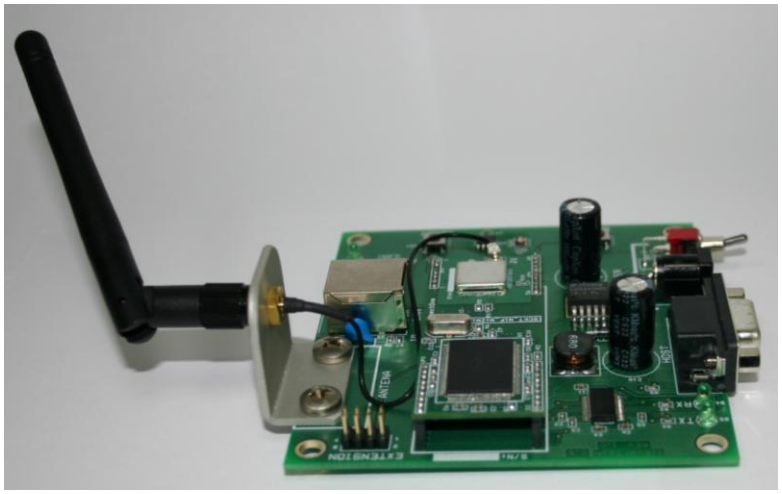
Instant Internet Evaluation Board II-EVB-361MW

User Manual

Version 1.3



International:
Connect One Ltd.
20 Atir Yeda Street
Kfar Saba 44643, Israel
Tel: +972-9-766-0456
Fax: +972-9-766-0461
E-mail: sales@connectone.com
http://www.connectone.com

Connect One Semiconductors, Inc.
560 S. Winchester Blvd.
Suite 500
San Jose, CA 95128
Tel: (408) 572-5675
Fax: (408) 572-5601

Information provided by Connect One Ltd. is believed to be accurate and reliable. However, Connect One assumes no responsibility for its use, nor any infringement of patents or other rights of third parties, which may result from its use. No license is granted by implication or otherwise under any patent rights of Connect One other than for circuitry embodied in Connect One's products. Connect One reserves the right to change circuitry at any time without notice. This document is subject to change without notice.

The software described in this document is furnished under a license agreement and may be used or copied only in accordance with the terms of such a license agreement. It is forbidden by law to copy the software on any medium except as specifically allowed in the license agreement. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including but not limited to photocopying, recording, transmitting via fax and/or modem devices, scanning, and/or information storage and retrieval systems for any purpose without the express written consent of Connect One.

iChip, Secure Socket iWiFi, Internet Controller, SerialNET, AT+i, and Connect One are trademarks of Connect One Ltd.

TABLE OF CONTENTS

International:
Connect One Ltd.
20 Atir Yeda Street
Kfar Saba 44643, Israel
Tel: +972-9-766-0456
Fax: +972-9-766-0461
E-mail: sales@connectone.com
http://www.connectone.com

Connect One Semiconductors, Inc.
560 S. Winchester Blvd.
Suite 500
San Jose, CA 95128
Tel: (408) 572-5675
Fax: (408) 572-5601

Introduction

This manual is intended to familiarize prospective customers with Connect One's Instant Internet Evaluation Board II-EVB-361MW. The II-EVB-361MW is an evaluation platform for the Secure Socket iWiFi™ Internet Controller. Secure Socket iWiFi is a secure serial-to-Wireless LAN device server module that also acts as a bridge to connect serial devices to 802.11b/g wireless LANs. Secure Socket iWiFi fits into a socket form-factor and utilizes Connect One's iChip CO2128SEC Internet communications coprocessor and the AT+i™ command set, a powerful set of Internet protocol commands developed by Connect One to manage Internet connectivity through a wireless LAN connection.

Secure Socket iWiFi enables sending and receiving textual and binary data, MIME-encoded email messages; downloading HTML pages or files from a Web server, or items from within a page; Web serving, as well as managing TCP or UDP socket communications (with or without SSL3) over the Internet. It also includes an FTP client and a Telnet client.

Secure Socket iWiFi supports numerous security protocols like SSL3/TLS1, 64/128-bit WEP encryption, AES-CCM and TKIP encryption, WPA (including AES) and WPA2.

Unpacking

Take the II-EVB-361MW out of its box. Included in the box are:

- The II-EVB- 361MW motherboard including Secure Socket iWiFi (iW-SM2128MW)
- A serial cable with two DB-9 connectors
- Antenna
- Power supply adaptor (110V/220V)

Connections

1. Connect one end of the RS232 cable to the serial port on the II-EVB-361MW (J1) and connect the other DB-9 connector to the COM1 or COM2 serial port on your PC, or to the serial port of your embedded device.
2. Connect the II-EVB- 361MW to the power supply.

Testing the Secure Socket iWiFi Wireless LAN Connection

To test the wireless LAN connection, you need to configure the Secure Socket iWiFi to connect to an Access Point:

1. Make sure the Access Point is connected and configured properly.
2. Invoke the iChip Config Utility on your PC.
3. In the main window of the utility, click the Dumb Terminal icon.
4. In the Dumb Terminal window, enter the **AT+i** command to verify that the iChip is communicating with your PC. You should receive an I/OK in response.

5. Enter the **AT+iRP11** command to obtain a report of all the Access Points available in your area.
6. Enter **AT+iWLSI**=<*ssid*>. *ssid* is the ID of the Access Point you connect to. Note that *ssid* is a case-sensitive string.
7. If you want to enable WEP encryption, configure the following parameters:
   - **AT+iWLWM**=<*n*> where *n*=0 means no security, *n*=1 means 64-bit key, and *n*=2 means 128-bit key
   - **AT+iWLKI**=<*n*> where *n* is the WEP key index (*n*=1..4)
   - **AT+iWLK**<*n*>=<*keyString*> where *n* is an index between 1 and 4, and *keyString* is the WEP key string in the n^{th} position.
8. If you want to enable WPA encryption, configure the following parameter: **AT+iWLPP**=<*passphrase*> where *passphrase* is the pass-phrase to be used in generating the WPA1-PSK encryption key

   At this stage a connection to the Access Point is established. To test the connection, use the iChip Config Utility to perform any activity that requires network connection such as retrieving a web page, sending an email, or opening a socket.

Installing the II-EVB-361MW Utility and Evaluation Program

II-EVB-361MW enables you to evaluate the Secure Socket iWiFi without changing anything in your current development environment. Using a simple terminal program on a PC, you can issue AT+i commands to the iChip and get responses.

AT+i commands are used to configure parameter values into iChip's flash memory and activate Internet tasks such as email send, sockets, FTP sessions, configuration, and more.

A full description of the AT+i protocol can be found in the *AT+i Programmer's Manual* on the Connect One website in the *Documentation* section at http://www.connectone.com.

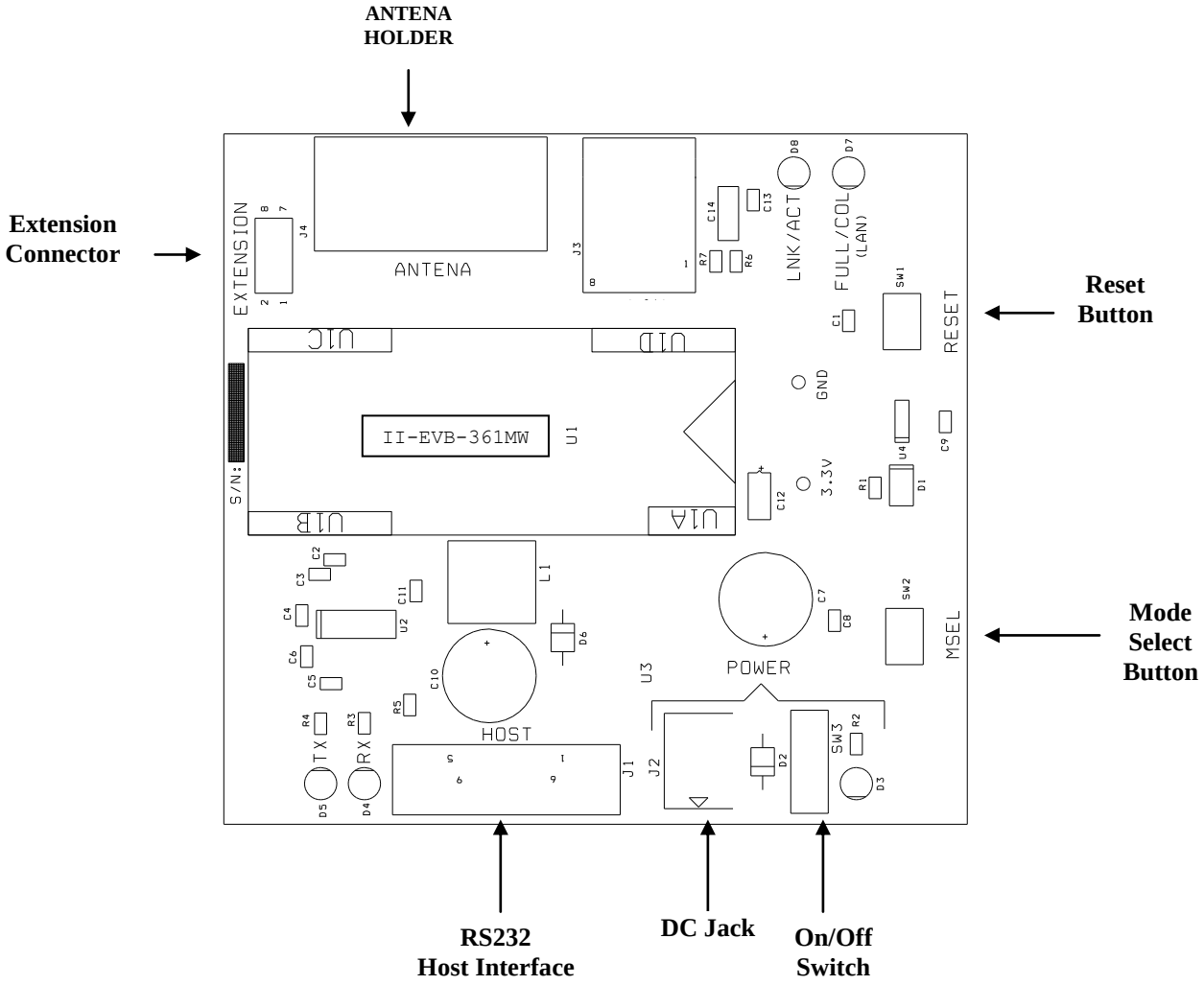
To help you evaluate the iChip, Connect One supplies the iChip Config Utility. This is a Windows-based GUI program that contains intuitive dialog boxes to fully configure iChip. It doesn't require any knowledge of AT+i commands. It also contains local firmware upgrade functionality.

The iChip Config Utility also allows you to perform specific Internet communication tasks such as sending and receiving emails, activating iChip's websites, entering SerialNET mode, and more.

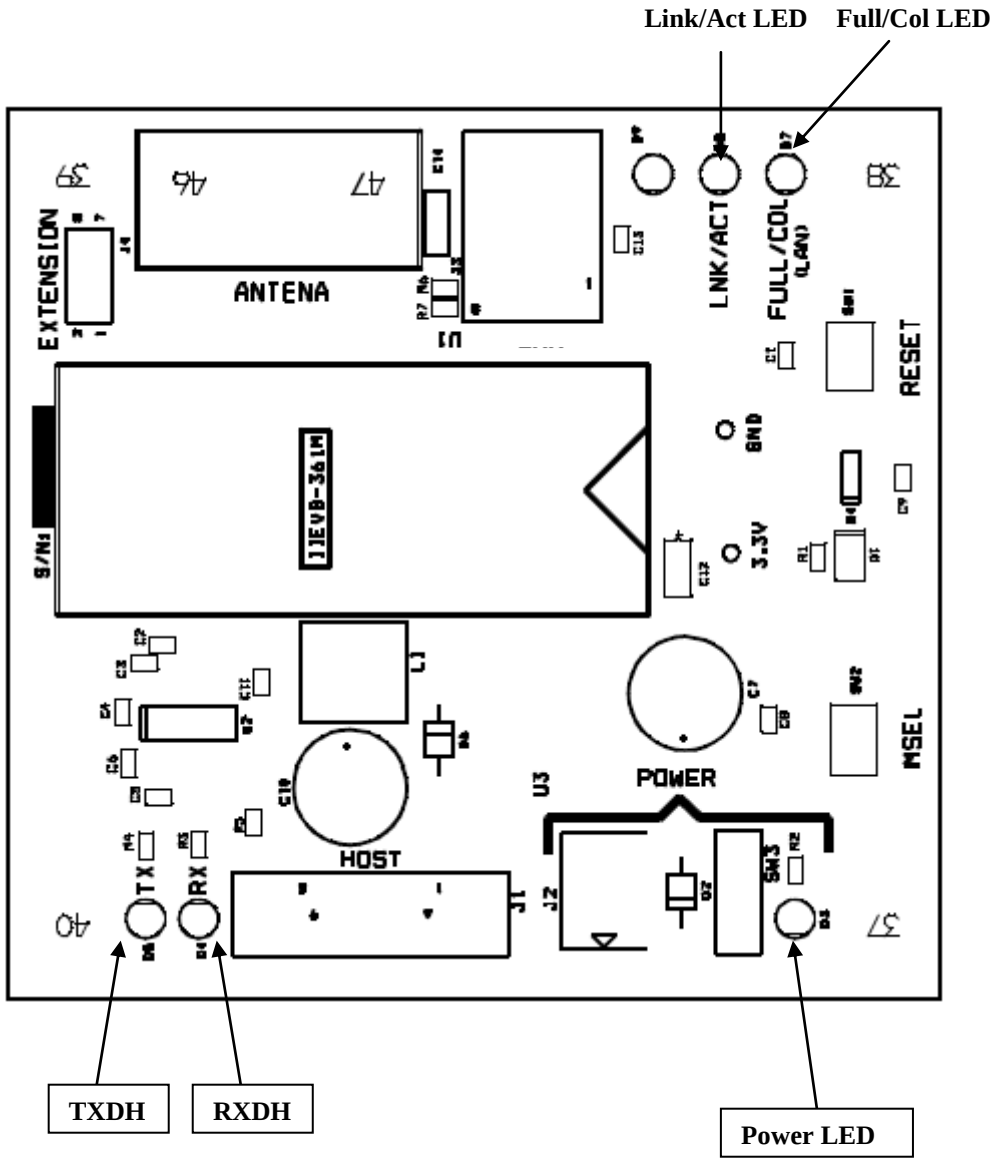
The latest iChip Config Utility version and user manual can be found on the Connect One website at http://www.connectone.com in the *Support* section.

For more information on the iChip Config Utility and its usage, see the *iChip Config Utility User's Manual*.

Connectors and Switch Positions



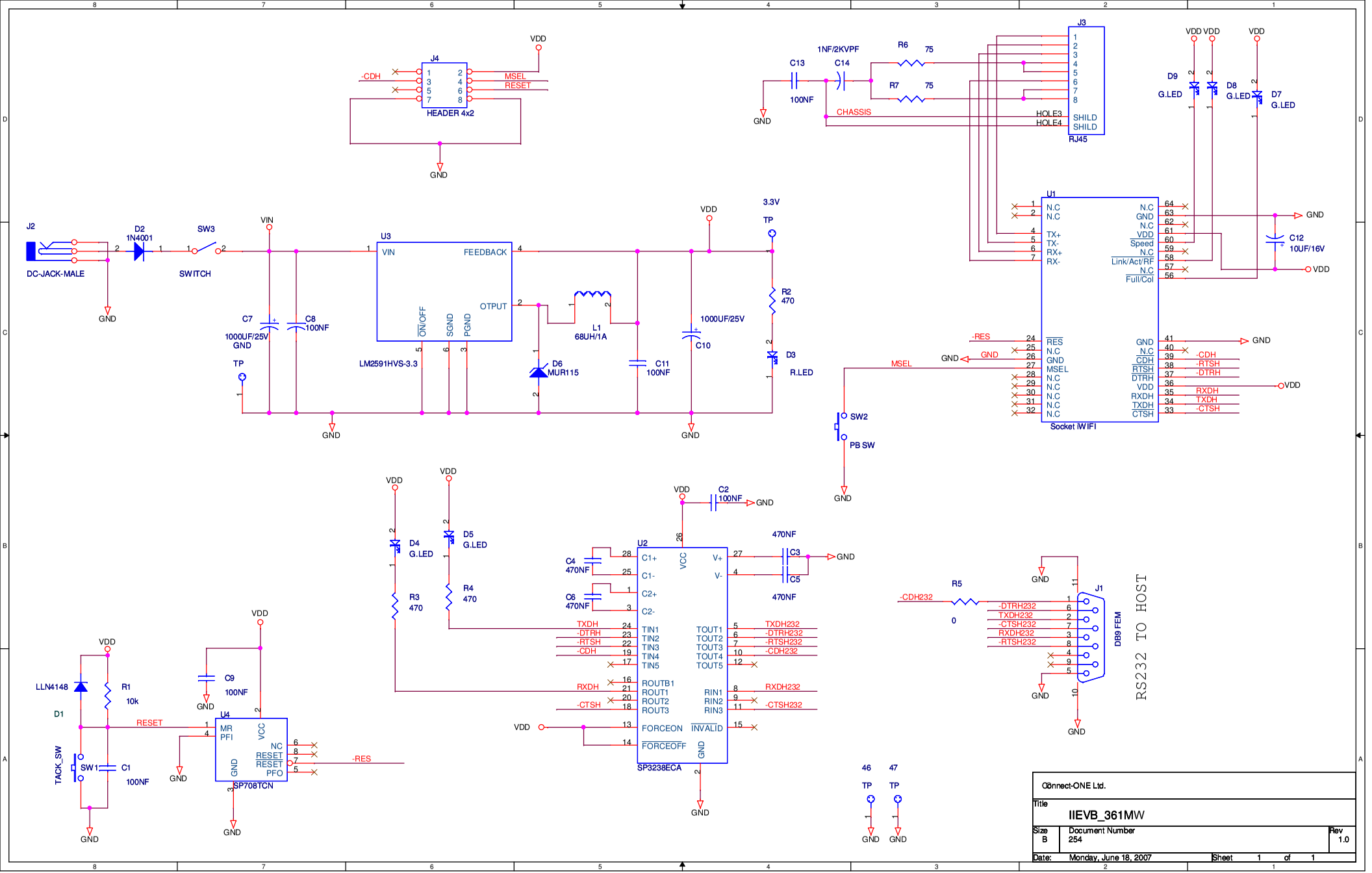
LED Positions



Bill of Materials

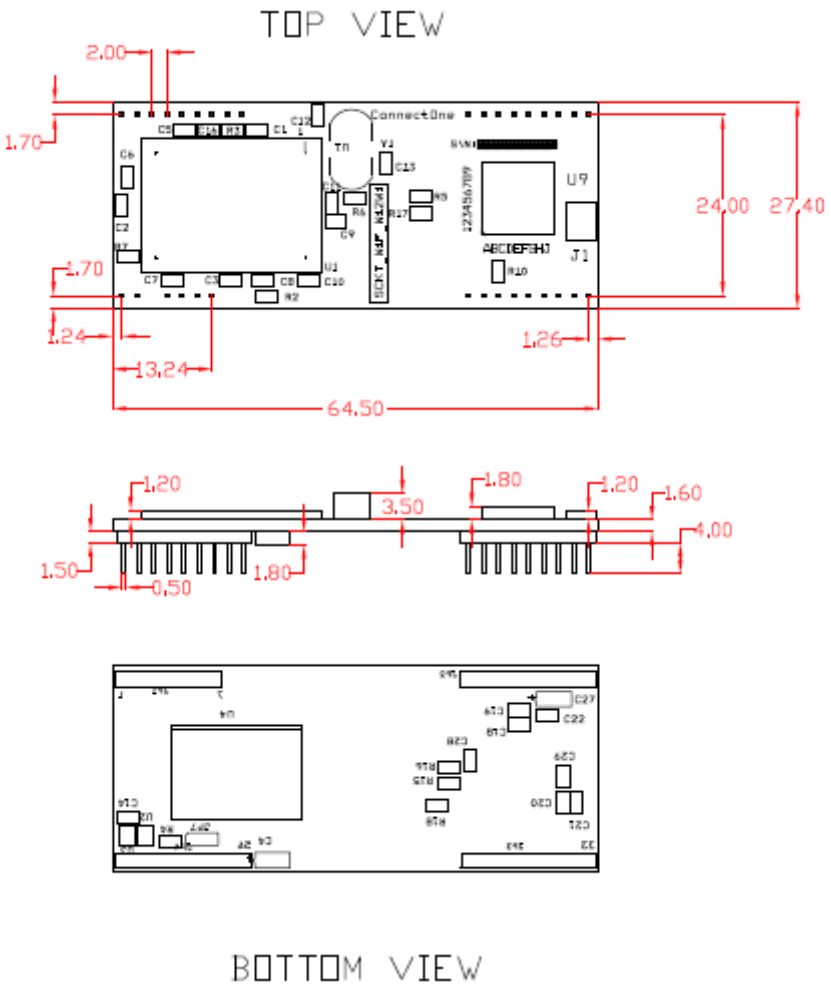
#	Qty	Reference	Description	Manufacturer
1	6	C1,C2,C8,C9,C11,C13	100NF	Any
2	4	C3,C4,C5,C6	470NF	Any
3	2	C7,C10	1000UF/25V	Any
4	1	C12	10UF/16V	Any
5	1	C14	1NF/2KVPF	Any
6	1	D1	LLN4148	Any
7	1	D2	1N4001	Any
8	1	D3	R.LED	Any
9	5	D4,D5,D7,D8,D9	G.LED	Any
10	1	D6	MUR115	Any
11	4	3.3V,46,47,GND	TP	Any
12	1	J1	DB9 FEM	Any
13	1	J2	DC-JACK-MALE	Any
14	1	J3	RJ45	Any
15	1	J4	HEADER 4x2	Any
16	1	L1	68UH/1A	Any
17	1	R1	10k	Any
18	3	R2,R3,R4	470	Any
19	1	R5	0	Any
20	2	R6,R7	75	Any
21	1	SW1	TACK_SW	Any
22	1	SW2	PB SW	Any
23	1	SW3	SWITCH	Any
24	1	U1	Secure Socket iWiFi	Connect One
25	1	U2	SP3238ECA	Any
26	1	U3	LM2591HVS-3.3	Any
27	1	U4	SP708TCN	Any

Appendix 1: II-EVB-361MW Schematic



Connect-ONE Ltd.		
Title: IIEVB_361MW		
Size: B	Document Number: 254	Rev: 1.0
Date: Monday, June 18, 2007	Sheet 1 of 1	

Appendix 2: Secure Socket iWiFi Mechanical Views



Appendix 3: WiFi Configuration Notes

Introduction

Wireless LAN stations operate in one of two modes: Infrastructure or Ad-Hoc.

In Infrastructure mode, wireless LAN stations connect to a wireless LAN Access Point (AP), which acts as a hub. Wireless LAN stations may connect to each other through the AP. If the AP is connected to LAN, it allows wireless LAN stations to connect to other stations on the LAN. When a gateway is in place, it enables wireless LAN stations to connect to systems across the gateway, as well.

In Ad-Hoc mode, two or more wireless LAN stations communicate directly with each other.

The Secure Socket iWiFi supports the 802.11b/g wireless LAN communication platform. It uses the iChip™ CO2128 communication controller chip and Marvell 88W8686 WiFi chipset. It incorporates several dedicated AT+i configuration parameters to support the wireless LAN environment. See the table below for a detailed list of WiFi configuration parameters.

AT+i Parameter Name	Description
WLCH	Wireless LAN Communication Channel
WLSI	Wireless LAN System-Set ID
WLWM	Wireless LAN WEP Mode
WLKI	Wireless LAN Transmission WEP Key Index
WLKn	Wireless LAN WEP Key Array
WLPS	Wireless LAN Power Save
WLPP	Personal Shared Key Pass Phrase
WLRS	Wireless LAN Rescan Interval

Table 1: AT+i Wireless LAN Configuration Parameters

The Secure Socket iWiFi may also be configured to exploit WEP security. iChip supports configuration of both 64-bit or 128-bit WEP keys.

In Infrastructure mode, Power Save mode is supported. When activated, Power Save shuts down the station for a limited period of time, during which the Access Point buffers incoming packets destined for the deactivated WiFi station. The station periodically wakes up to retrieve all the buffered packets stored in the Access Point. In this mode, total power consumption is lowered at the expense of higher response latency. The Secure Socket iWiFi may be configured to put the WiFi chipset in Power Save mode in conjunction with iChip's inherent Power Save mode.

iChip Wireless LAN Environment Configuration Parameters

WLCH (Factory Default: 0)
In Infrastructure mode, the WLCH parameter **must** be set to 0. Other available values (1..13) designate the preferred communication channel while in Ad-Hoc mode.

WLSI (Factory Default: Empty)
This parameter **must** be assigned with the System-Set-ID string (SSID), which is identical to that configured in the Access Point(s) through which the WiFi station needs to connect. An exception to this is the "Any SSID" configuration, which is configured by simply leaving this parameter empty (or setting to NULL string with AT+iWLSI=""). In the "Any SSID" configuration, the WiFi station will connect to any available Access Point. If more than one Access Point is active, it will choose the one with the stronger radio signal.

WLWM (Factory Default: 0)
Configure this parameter to designate WEP security usage mode. If WEP is disabled, the WLKI and WLK*n* parameter settings are irrelevant. Note that WEP settings (with the exception of WLKI) **must** be identical to those configured in the Access Point device. Possible settings are:

WLWM Setting	WEP Security
0	Disabled
1	Enabled, using 64 bit keys
2	Enabled, using 128 bit keys

Table 2: WEP Security Mode Settings

WLKI (Factory Default: 1)
If WEP is enabled, this parameter defines the key index of the WEP key to be used when encoding outgoing WiFi packets. Since WEP includes configuration for an array of four possible keys, WLKI can receive a value in the range [1..4]. The value of this parameter **need not** be the same as that configured in the Access Point.

WLKn (Factory Default: All Empty)
These are four consecutive parameters (with *n* ranging from 1 to 4). The parameters define an array of 4 WEP security keys, which are used to encode outgoing WiFi packets (using the key defined by WLKI) and decode incoming packets according to the key issued by the Access Point device. Key size is 64- or 128-bits, according to the WLWM setting. The parameter values are used only if WEP security is enabled (WLWM > 0). The key values **must** be identical to those configured in the Access Point device.

WLPS (Factory Default: 0)
This parameter defines the chipset Power Save mode. When configured for Power Save mode, iChip links its own internal Power-Save mode with that of the Marvell chipset. When iChip's Power Save mode is activated (AT+iPSE=1), and when WLPS is greater than 0, iChip will force the chipset into Power Save mode. The value stored in WLPS defines the maximum length of time (in milliseconds) during which the Marvell chipset will snooze, before waking up to download any available packets that may have been buffered for it in the Access Point. WLPS may be set in the range:

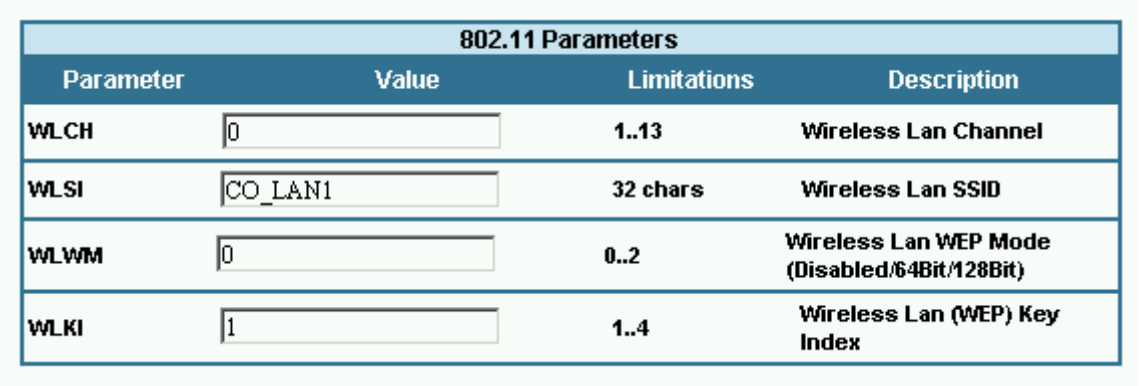
[0..3600]. When WLPS is set to 0, the Marvell chipset Power Save is disabled, even if iChip enters Power Save mode.

WLPP (Factory Default: Empty)
This parameter sets the wireless LAN WPA1-PSK pass-phrase to be used in generating the WPA1-PSK encryption key. When empty, WPA security is disabled. If WLSI (SSID) is not empty, WPA1-PSK security is enabled for WiFi connections and *WLPP* is used in generating the WPA1-PSK encryption key. The allowed value for *WLPP* is an ASCII string containing 8-63 characters.

WLRS (Factory Default: 0)
This parameter sets the interval between consecutive scans that iChip performs in search for nearby ad-hoc networks. Scan duration is two beacon periods (200 ms). WLRS may be set in the range: 0-65535 milliseconds.

Wireless LAN Configuration Web Site Page

iChip's configuration website includes two views that support configuration and status retrieval of related Wireless LAN parameters. The configuration view displays the configurable Wireless LAN AT+i parameters (WLCH, WLSI, WLWM, and WLKI). New values may be defined and submitted to iChip from the browser.



802.11 Parameters

Parameter	Value	Limitations	Description
WLCH	0	1..13	Wireless Lan Channel
WLSI	CO_LAN1	32 chars	Wireless Lan SSID
WLWM	0	0..2	Wireless Lan WEP Mode (Disabled/64Bit/128Bit)
WLKI	1	1..4	Wireless Lan (WEP) Key Index

Figure 1: Wireless LAN Web Configuration

Wireless LAN Status Report

The Wireless LAN AT+i Report (AT+iRP10) returns pertinent status information regarding the active 802.11b/g Wireless LAN link. In response to issuing the report command, iChip will reply with the following syntax:

I/(<port stat>, <xfer rate>, <sig level>, <lnk qual>)

Where,

port stat -- Port Status:
- 0: Wireless LAN adapter not present
- 1: Wireless LAN adapter Disabled
- 2: Searching for initial connection
- 4: Connected
- 5: Out of range

xfer rate -- Transfer Rate, in the range 1..4
(1 =>1 Mbps; 2 =>2 Mbps; 3 =>5.5 Mbps; 4 =>11 Mbps)

sig lvl	--	Signal Level [%], in the range 0..100
lnk qual	--	Link Quality [%], in the range 0..100

The Configuration website contains a live status page with this and some additional status information:

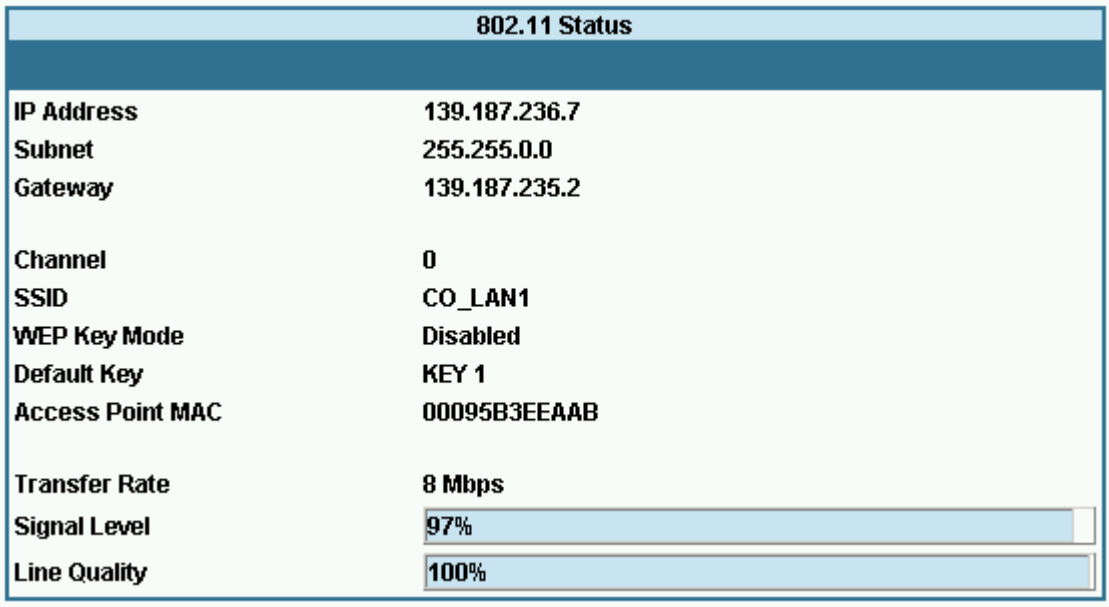


Figure 2: Wireless LAN Web Status Display

iChip Wireless LAN Test Mode

WLTR
This command limits the wireless LAN transmission rate according to the specified command parameter. The table below details the possible parameter values:

Maximum Transmission Rate	Detail
0	Maximum possible transmission rate for the current chipset.
1	1 Mbps
2	2 Mbps
3	5.5 Mbps
4	11 Mbps

Table 3: Maximum Transmission Rate Command Parameter

When AT+i WLTR is issued, transmission rate is limited for the duration of the session until another AT+iWLTR command is issued, or iChip is power-cycled.

Placement and Range Guidelines

802.11b/g wireless LAN devices connect to wireless LAN Access Points over a maximum range of 300 feet. Actual transmission rate and service quality may vary significantly as a result of environmental obstacles and physical placement of the Access Point and station devices.

For best results, refer to the following guidelines:

1. Locate the wireless LAN equipment away from sources of interference, such as PCs, large metal surfaces, microwaves, and cordless phones.
2. Position the wireless LAN access point at an elevated position and as close as possible to the center of the area in which the wireless LAN devices will operate.

Wireless LAN Data Privacy/Security Considerations

The fact that wireless LAN devices transmit data over a radio link makes them vulnerable to electronic eavesdropping, tampering, and information theft. There are several means by which you may strengthen your wireless LAN access security:

- Change the factory default SSID setting of the wireless LAN Access Point and station devices. Enable WEP or WPA encryption of the wireless LAN data communications. If you use WEP, it is recommended that you use 128-bit WEP keys.
- Restrict 802.11b/g wireless LAN access based on MAC address. This is configurable in most Access Point devices.
- Place the 802.11b/g Wireless Access Point in a location where it cannot be physically tampered with.
- Store printed SSID and WEP or WPA key settings in a safe place.