



June 2009

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

20 Atir Yeda Street
1st floor
Kfar Saba 44643 Israel
Te: +972-9-766-0456
Fax: +972-9-766-0461

www.connectone.com

Release Notes



iChip OS Version i2128D804B04

Revision 1.10

Reference Version: 802B03

Table of Contents

1.	WHAT WAS NEW IN RELEASE 804B01?	4
1.1	HARDWARE PIN SETTINGS RETAINED ACROSS FACTORY DEFAULTS.....	4
1.2	EXTENDED STOP BITS IN SERIALNET MODE.....	4
1.3	LAN TO WiFi BRIDGE.....	5
1.3.1	<i>Introduction</i>	5
1.3.2	<i>General Description</i>	5
1.3.3	<i>New AT+I Commands to support LAN-to-WiFi Mode</i>	9
1.3.4	<i>AT+iBRM – Bridge Mode</i>	9
1.3.5	<i>AT+iMACF – MAC Forward</i>	9
1.4	UDP BROADCAST TO SUBNET.....	9
1.5	USB MODEM SUPPORT.....	10
1.6	USE OF NAGLE ALGORITHM.....	10
	+iMSS — <i>Maximum Segment Size</i>	11
1.7	INCREASED SIZE FOR CA CERTIFICATES.....	11
1.8	PORT FORWARDING.....	12
1.8.1	<i>Introduction</i>	12
1.8.2	<i>Port Forwarding</i>	12
1.8.3	<i>Port Forwarding Rules</i>	12
1.8.4	<i>Port Forward Rules Report</i>	13
1.9	SKIP ENTERPRISE-MODE CERTIFICATE AUTHENTICATION.....	13
1.9.1	<i>Introduction</i>	13
1.9.2	<i>Skipping Certificate Authentication</i>	14
1.9.3	+iWSTn — <i>Wireless LAN WPA Security</i>	14
1.10	PARAMETER PROFILES.....	15
1.10.1	<i>Introduction</i>	15
1.10.2	<i>Parameter Profiles</i>	15
1.10.3	<i>Parameter Profile Full Command Syntax</i>	16
1.10.4	<i>Restoring a Parameter Profile with the MSEL signal</i>	17
1.11	NETWORK CONFIGURATION.....	17
1.11.1	<i>Introduction</i>	17
1.11.2	<i>Preliminary Network based Configuration</i>	18
1.11.3	<i>New iChip Facilities to support Network Configuration</i>	18
2	WHAT WAS NEW IN RELEASE 804B02?	21
2.1	HOST WEB SITE UP TO 256K.....	21
2.2	RS-485 HOST INTERFACE.....	21
2.2.1	<i>Introduction</i>	21
2.2.2	<i>Configuration</i>	21
3	WHAT IS NEW IN RELEASE 804B04?	23
3.1	EXTENDED URL PARAMETER TO 256 CHARACTERS.....	23
3.2	CHANGE OF ALLOWED VALUES FOR THE +IPGT (PING TIMEOUT) PARAMETER.....	23
3.3	CHANGE OF ALLOWED VALUES FOR THE +IWSRL AND +IWSRH (WiFi SNR THRESHOLDS).....	23
3.4	WiFi POWER-SAVE MODE.....	23
4	LIMITATIONS SOLVED	24
5	KNOWN LIMITATIONS IN 804B04	27

6	SUPPORTED PLATFORMS.....	28
7	FIRMWARE FILE INFORMATION.....	28

1. What was New in Release 804B01?

iChip firmware version i2128D804Bxx includes numerous features and fixes from previous versions. This section describes the new features that were added in this release.

1.1 Hardware Pin Settings Retained Across Factory Defaults

Several AT+i commands configure hardware pins. These are:

```
AT+iRRHW -- Defines the iChip Readiness signal
AT+iSPIP -- Defines the SPI Control signal
AT+iSLED -- Defines the SerialNET indicator pin
AT+iADCP -- Defines the A/D polling indicator signal
```

Since the settings of these parameters effects the utilization of physical pins, and would normally reflect the actual connections of these signals, the AT+iFD (Restore Factory Defaults) command will not alter their current settings.

1.2 Extended Stop Bits in SerialNET mode

The SerialNET mode COM interface parameter +iSNSI has been expanded to support 1.5 and 2 Stop Bits. The modified syntax for the +iSNSI parameter is:

Syntax: AT+iSNSI=*settings_str* Sets serial interface settings for SerialNET mode.

Parameters: *settings_str* = Serial link settings in SerialNET mode.

Command Options:

```
settings_str = "<baud>,<data_bits>,<parity>,<stop_bits>,<flow>"
```

where,

```
<baud>      = 0..9 or h
<data_bits> = 7 | 8
<parity>    = N | E | O
<stop_bits> = 1 | 1.5 | 2
<flow>     = 0 | 1
```

-or-

```
settings_str = <baud>
```

Where,

```
<baud>      = 0..9 or h
```

And the rest of port's characteristics will get their default value (8 data-bits, no parity, 1 stop-bit, no HW flow control).

1.3 LAN to WiFi Bridge

1.3.1 Introduction

The LAN to WiFi bridge mode enables users to design their application regardless of the network connection. Users can design their system to connect to a LAN infrastructure either by using a standard cable connection, WiFi to WiFi bridge or WiFi to AP bridge. The bridge mode enables users to use these three different connection types without any change to their application or to the LAN infrastructure.

In the LAN to WiFi bridge mode, iChip acts as layer 2 switch and emulating layer 2 packets from the user application toward the LAN and WiFi infrastructure.

1.3.2 General Description

What is LAN to WiFi Bridge?

LAN to WiFi bridge, is a special iChip mode where iChip acts as layer 2 bridge between a LAN network on one side and a WiFi network on the other side. iChip FW is responsible for all the WiFi connectivity and security. iChip supports two modes of LAN to WiFi bridge:

- Cable replacement ADHOC Mode
- Cable replacement AP mode

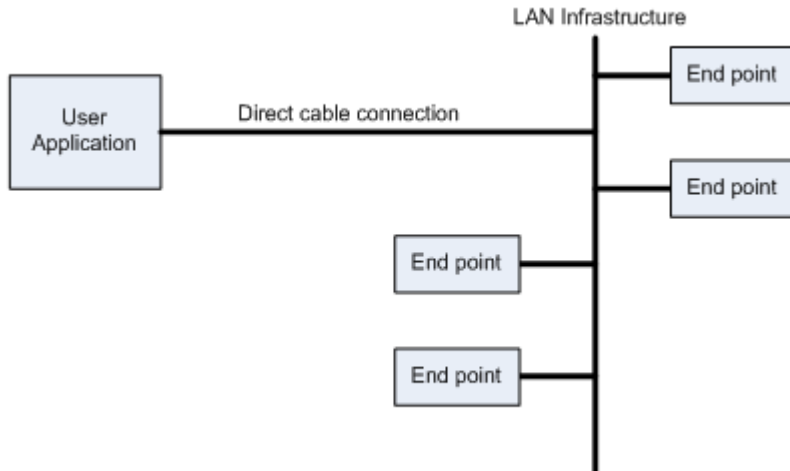
Cable replacement ADHOC mode

In this mode, two iChips are used to act as cable replacement. The connection between the two sides is done using WiFi ADHOC mode. In this mode iChip supports two types of LAN connections:

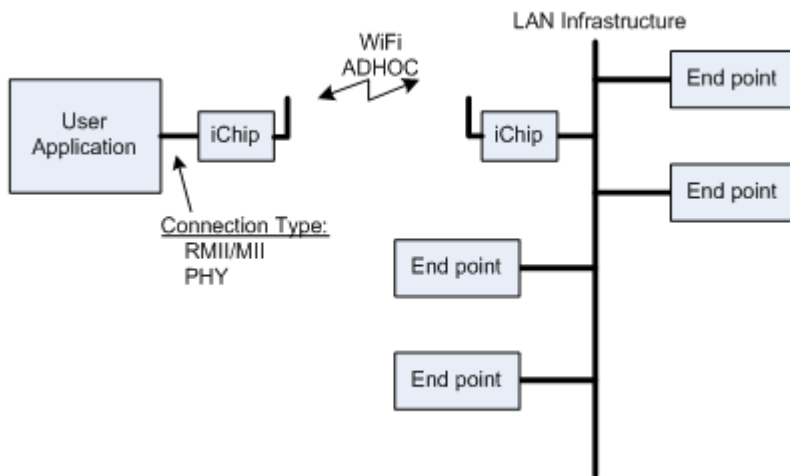
- RMII/MII connection to iChip
- PHY connection to iChip

Both sides of the line can be configured differently based on user requirements.

The diagrams below outline the iChip Cable replacement mode:



Drawing 1: Direct Cable connection (Original state)



Drawing 2: Cable replacement ADHOC mode

In cable replacement ADHOC mode, iChip supports two security layers. The first layer is the ADHOC WEP security and the second layer is MAC forwarding. When using MAC forwarding the user can configure both iChips to forward packets to a predefined MAC address as define in the MACF parameter. Without MAQ forwarding, iChip will need to broadcast outgoing packets. Broadcasting is slower than Unicasting and also has the disadvantage of being received by all systems on a specific AD-Hoc network.

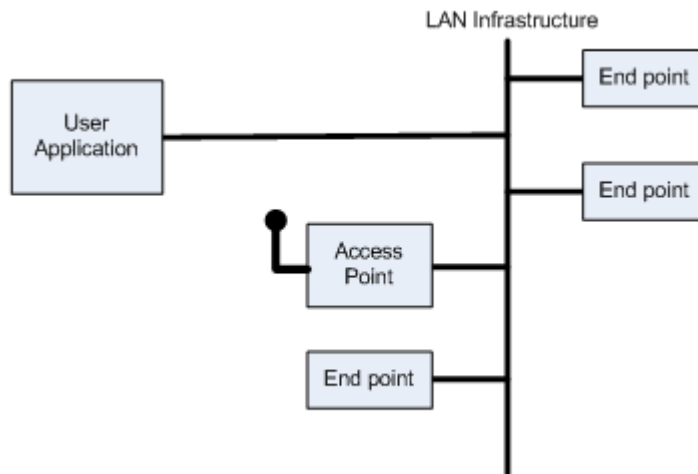
In this mode, all traffic from the LAN infrastructure is moved to the user application over the WIFI AD-HOC connection and all traffic sent from the user application is moved back to the LAN infrastructure.

To enter "Cable replacement ADHOC mode" the following parameters should be used:

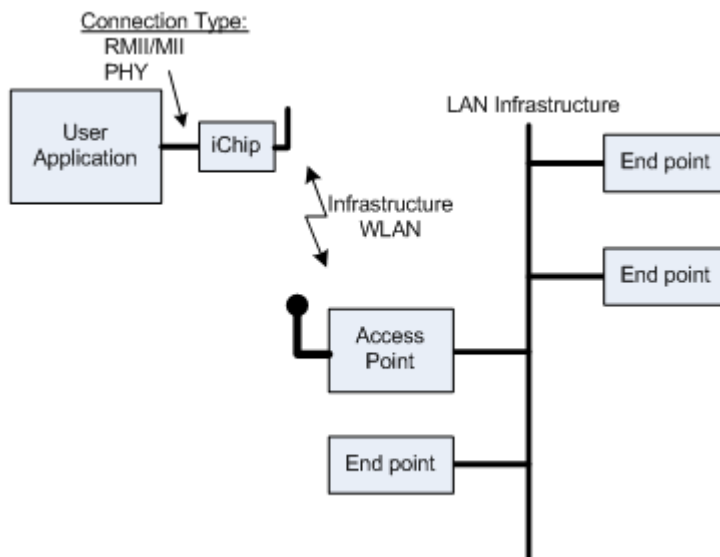
- +iWLCH - ADHOC wireless channel
- +iWLSI - ADHOC network SSID (prefix with '!')
- +iWST0 - WEP security type (64,128) - *optional*
- +iWKY0 - WEP security Key - *optional*
- +iBRM - LAN interface, MII/RMII or PHY - *1 or 3*
- +iMACF - MAC Forward on both sides - *optional*

Cable replacement AP mode

In this mode iChip replaces a direct LAN cable connection in the user application, by connecting the user application to an Accesses Point on the LAN infrastructure.



Drawing 3: Direct cable connection to LAN infrastructure



Drawing 4: Cable replacement AP Mode

In Cable replacement AP mode, the iChip enables the user application to connect to an existing AP on the LAN infrastructure. The iChip connects to the AP using the same MAC address of the user application which enables the LAN infrastructure to maintain that same connection rules for the user application.

The following parameters should be used in order to set "Cable replacement AP mode" (WPA Security):

- +iWLSI - WIFI network SSID
- +iWST0 - WIFI security type - *optional*
- +iWLPP - WIFI WPA security Key - *optional*
- +iBRM - LAN interface, MII/RMII or PHY - *2 or 4*

1.3.3 New AT+I Commands to support LAN-to-WiFi Mode

1.3.4 AT+iBRM – Bridge Mode

Syntax: AT+iBRM=<n> Sets iChip bridge mode

Parameters: n=0..4

Command Options:

n=0 Bridge mode disable

n=1 Cable replacement PHY to WIFI ADHOC mode

n=2 PHY LAN to WiFi AP mode

n=3 Cable replacement MII/RMII to WIFI ADHOC mode

n=4 MII/RMII LAN to WiFi AP mode

1.3.5 AT+iMACF – MAC Forward

Note - This parameter takes effect only in cable replacement mode (BRM= 1, 3)

Syntax: AT+iMACF= <mac> Sets MAC forwarding in ADHOC bridge mode. This MAC will be used as the destination MAC address of the transmitted packets. If left empty Broadcast is used.

Parameters: *mac*="hhhhhhhhhhhh" 12 HEX digits of MAC address

Command Options:

mac = "" No MAC forwarding. Packets will be Broadcast.

mac = *mac_address*

Valid 12 HEX digit representation of MAC destination address.

In case of invalid value – MAC forwarding will not work.

1.4 UDP Broadcast to Subnet

The iChip Open UDP socket command (AT+iSUDP) will now accept a subnet directed Broadcast address as the destination. This allows broadcasting a UDP packet to the immediate subnet (without crossing gateways). For example, assuming that the local

subnet is 192.168.x.x, a UDP Broadcast to the subnet for UDP port 1234 may be achieved in iChip by opening a UDP socket using the following command:

```
AT+iSUDP:192.168.255.255,1234
```

1.5 USB Modem Support

Support for the following USB cellular modems has been added to this firmware version:

Longsung U5100 HSDPA and U6100 HSDPA

ZTE HSDPA Z100M, DTM6211 and AC8710

The complete list of the supported USB cellular modems is now:

- *Datang DTM6211,*
- *LongSung U6100*
- *LongSung U6500,*
- *EVDO AC8710,*
- *Motorola C-Light Modem,*
- *Motorola G24 Modem,*
- *Motorola Zbm (H24-Light)*
- *Siemens HC25*
- *ZTE CDMA Tech,*
- *ONDA CDMA Technologies MSM,*
- *ZTE HS-USB Modem*
- *AIKO 83D*

1.6 Use of Nagle Algorithm

When exchanging information over TCP/IP, iChip makes use of the Nagle algorithm (http://en.wikipedia.org/wiki/Nagle's_algorithm), which defines that transmit data should be coalesced until receiving an ACK from the remote peer. A new packet of the accumulated data is sent after the ACK is received or when a full sized packet that contains MSS bytes, is ready to be sent.

To disable iChip's use of the Nagle algorithm, the second bit of the +iMSS parameter may be set.

The complete syntax of the +iMSS command is:

+iMSS — Maximum Segment Size

Syntax: AT+iMSS=*b*

Permanently sets the maximum segment size that iChip will negotiate with the Peer and defines the use of the Nagle algorithm.

Parameters: *b* is a bitmapped value

Command

Options:

Bit 1 0 – Use MSS=536

1 – Use MSS=1460

Bit 2 0 – Use Nagle Algorithm

1 – Disable Nagle Algorithm

Default: 0 (MSS=536 with Nagle Algorithm)

Result Code:

I/OK If *b* is within limits

I/ERROR Otherwise

AT+iMSS~*b* Temporarily sets the MSS bitmapped value for one session. The permanent value will be restored after completing the next session, both if the session was successful or not.

AT+iMSS? Reports the current MSS bitmapped value.

The reply is followed by **I/OK**.

AT+iMSS=? Returns the message “0-3”.

The reply is followed by **I/OK**.

1.7 Increased Size for CA Certificates

The CA certificate related parameters in iChip have been enlarged in capacity to contain certificates of up to 1500 bytes. Previously, the CA parameters were limited to 1300 bytes. Note that CA files contain Base64 encoding which stores 1500 bytes in roughly 2000 bytes. The iChip CA related parameters are:

- CA -- Major Certificate Authority Certificate
- CA2, CA3, CA4 -- Alternate Certificate Authority Certificates
- CERT -- iChip's Certificate
- PKEY -- iChip's Private Key

1.8 Port Forwarding

1.8.1 Introduction

iChip may be configured as a router using the so-called iRouter mode. This mode is established by issuing the AT+iSTRR (Start Route) or setting +iARS=1 (Auto Router Start). In iRouter mode iChip has a local (LAN or WiFi) connection and a dial-up (PPP) connection via a dial-up modem or Cellular modem. The iChip maintains a NAT table to manage a plurality of IP addresses on the local subnet, each having access to the WAN through the single IP address assigned on the dialup/cellular side.

1.8.2 Port Forwarding

The use of the NAT table provides the ability of each IP node on the local subnet to create a connection to an IP on the WAN. However, none of the local systems may be approached from the WAN.

This problem can be remedied by defining Port-Forward rules, that set aside designated ports on the WAN IP and automatically forward them to specific IP nodes on the local subnet. This firmware version introduces the Port-Forward feature in iChip's iRouter mode and provides maintenance for up to 10 Port-Forwarding rules. Port Forward rules may be restricted to either TCP or UDP or non restricted and forward either.

1.8.3 Port Forwarding Rules

A new AT+I command has been added to configure and manage Port-Forward rules. The command syntax is:

```
AT+iPFWn="w-port,<l-IP:l-port>[,<type>]"
```

Where,

- | | |
|---------------|--|
| <i>n</i> | - Index in the range 0..9 |
| <i>w-port</i> | - The WAN port. i.e., The port on the Public-IP end. |
| <i>l-IP</i> | - An IP on the local LAN (or WiFi network) |
| <i>l-port</i> | - A port on l-IP. |
| <i>type</i> | - Optional: 0-TCP, 1-UDP restriction. Not specified: Both. |

Note that the Port-Forward rule must be enclosed in double-quotes.

For example, given a iRouter system with WAN IP 10.0.0.100 and a Port-Forward rule: AT+iPFW0="8000,192.168.0.1:80", a packet (either TCP or UDP) to 10.0.0.100:8000 arriving at iChip from the WAN end shall cause iChip to route the packet to 192.168.0.1:80 on the local LAN and then route the response packet back to the originating system on the WAN.

The parameter polling command for +iPFWn parameters shall return a formatted report of the rule: *w-port,l-IP:l-port*

For example, given the previous example setting:

AT+iPFW0?

8000,192.168.0.1:80

I/OK

The same Port Forwarding rule that is restricted to TCP shall be:

AT+iPFW0="8000,192.168.0.1:80,0"

The polling command shall return the appropriate response:

AT+iPFW0?

8000,192.168.0.1:80,0

I/OK

Newly assigned Port Forwarding rules take effect only after power cycling or soft-resetting the iChip with AT+iDOWN.

1.8.4 Port Forward Rules Report

A new Report: AT+iRP22 shall be added to return all PFW rules.

The report shall display each Port-Forwarding Rule in a separate line, prefixed with the Rule index number. Only non-empty rules shall be returned.

The report line syntax shall be:

#- <w-port>,<l-IP:l_port><CR/LF>

For example,

AT+iRP22

0- 8000,192.168.0.1 :80,0

3- 8800,192.168.0.5 :80

I/OK

1.9 Skip Enterprise-Mode Certificate Authentication

1.9.1 Introduction

When iChip negotiates Enterprise mode security with a RADIUS server it normally verifies the RADIUS server's credentials by comparing the CA that has signed the RADIUS server's certificate with one of its internal CA certificates. However, in some cases the end-user may decide to skip this requirement in favor of simplicity – though it

may have a negative effect on the total security. When the iChip is configured to skip CA authentication, a CA certificate (in the +iCA parameter) is not required.

1.9.2 Skipping Certificate Authentication

A new feature in this version allows configuring iChip to skip the RADIUS authentication and in effect, accept any RADIUS server it was configured for. To disable the authentication add +100 to the +iWST n parameter Enterprise mode values. In other words specify values of 105 or 106 instead of 5 or 6 to specify WPA or WPA2 Enterprise mode without RADIUS CA authentication. In this case, configuring a CA certificate in iChip is not required.

The full +iWST n syntax is:

1.9.3 +iWST n — Wireless LAN WPA Security

Syntax: `AT+iWST n =sec`
 Sets the Wireless LAN security type for each individual SSID in the array. For $n > 0$ this parameter takes effect following either a hardware or software reset (AT+iDOWN) only. A change of +iWST0 during iChip operation affects the current connection immediately.

Parameters: $n=0-9$
 $sec=0$, no security.
 $sec=1$, WEP 64.
 $sec=2$, WEP 128.
 $sec=3$, WPA-TKIP-PSK.
 $sec=4$, WPA2-AES-PSK.

 $sec=5$, WPA-TKIP Enterprise PEAP-MSCHAPv2.
If CA parameter is empty, returns ERROR 222.
 $sec=6$, WPA2-AES Enterprise PEAP-MSCHAPv2.
If CA parameter is empty, returns ERROR 222.

 $sec=105$, WPA-TKIP Enterprise PEAP-MSCHAPv2 without RADIUS Authentication.
 $sec=106$, WPA2-AES Enterprise PEAP-MSCHAPv2 without RADIUS Authentication.

NOTE: In order to nullify CA, all WST n parameters need to be set to values other than 5 or 6.

Default: 0 (No Security)

Result code:

I/OK If sec is within limits provided that when sec equals 5 or 6 the CA parameter is defined.

I/ERROR Otherwise

AT+iWST0? Reports the current value followed by I/OK.

AT+iWST0=? Returns the message — 0-6,105,106 followed by I/OK.

1.10 Parameter Profiles

1.10.1 Introduction

iChip contains an internal database of non-volatile environmental parameters, which store a configuration that is used by iChip to determine its operation in the network environment it is configured for.

Each iChip parameter has a “Factory Default” value, which it is assigned to that parameter as a default, before any other value is assigned to it. The AT+iFD command is available to restore all iChip parameters to their Factory Default at any given time.

A new feature in this version is introduced to allow OEM manufacturers or iChip users to define a different set of default values, described as a “Profile”. The Profile may then be restored at any given time.

1.10.2 Parameter Profiles

A new AT+i command has been added that may be used to store the current “snap shot” of iChip parameter values as a Profile. Currently only 1 profile is supported, however in future versions support for additional profiles shall be added. The command syntax is:

AT+iSPRF[:*n*], Where *n* is the optional profile number to store (currently can only be 1).

The command stores the current values of all iChip parameters in a separate storage, which may be referenced at a later time to Load the stored profile into the active iChip parameters. Profile loading is achieved with the new AT+i command:

AT+iLPRF[:*n*] Where *n* is the optional stored profile number (currently must be 1).

An additional command has been added to display a report of the profile. The report includes one line for each iChip parameter with the syntax:

<Parameter Name>=<Value> where, *Parameter Name* is the AT+i name code used.

The syntax of the profile display command is:

AT+iDPRF[:*n*] where, *n*=0 displays the current (active) iChip parameters and *n*=1 displays the stored Profile values.

1.10.3 Parameter Profile Full Command Syntax**1.10.3.1 +iSPRF**

Syntax: AT+iSPRF[:<*n*>]

Store the current system state (all the parameters values) as parameters' profile *n*.

Parameters: *n* – Optional Profile number
 n=1 Parameters' profile #1

Default: 1

Result code:

I/OK If *n* is a legal value.

I/ERROR Otherwise

1.10.3.2 +iLPRF

Syntax: AT+iLPRF[:<*n*>]

Load parameters' profile *n* and restore it as the system state. This operation is destructive – it will change the values of the system parameters with out an option for rolling back.

Parameters: *n* – Optional Profile number
 n=1 Parameters' profile #1

Default: 1

Result code:

I/OK If *n* is a legal value.

I/ERROR Otherwise

1.10.3.3 +iDPRF

Syntax: AT+iDPRF[:<*n*>]

Display the context of profile *n* by displaying pairs of name and value. Each pair will be displayed in a new line. Note that passwords are displayed in plaintext.

Parameters: *n* – Optional Profile number

n=0 Current System state

n=1 Parameters' profile #1

Default: 1

Result code:

I/OK If *n* is a legal value.

I/ERROR Otherwise

1.10.4 Restoring a Parameter Profile with the MSEL signal

A stored Parameter Profile may be restored with the MSEL signal (CO2128 pin 60; CO2064 Pin 26; CO2144 Ball L9).

While iChip is operating pull the MSEL signal LOW (0VDC) for at least 30 seconds continuously, iChip shall restore Parameter Profile #1, thereby overriding all its current parameter values (nonreversible).

The effect is equivalent to issuing the AT+iLPRF command, detailed above.

1.11 Network Configuration**1.11.1 Introduction**

iChip may be configured using a combination of the following methods:

1. Issue AT+i commands to the iChip Host port (Serial, USB or SPI). AT+i commands allow setting each individual parameter value. Since the iChip parameters are non-volatile, this setting may be a one-time procedure.
2. Connect the iChip Serial Host port to a PC running Windows and activating the iChipConfig GUI application. This application provides a convenient GUI with which to configure iChip. The actual configuration is done by issuing AT+i commands in the background.

3. Activate iChip's Web server and use a standard Browser to surf to iChip's configuration Web site, where most of iChip's parameters may be viewed and changed.
4. Upload an RPF file via the iChip's Configuration Web site. The iChip Webserver must be active. An RPF file contains iChip parameter names and value settings. Loading an RPF has the equivalent affect of setting the iChip's parameters to the specified values.

Methods 1 and 2 require a physical connection to the iChip Host port (Serial, USB or SPI). Methods 3 and 4 require an active IP connection to the network in order to properly allow parameter configuration.

In many cases, neither of these connections is available **before** a preliminary configuration is made. Therefore, an additional method is required to bridge the gap and allow a preliminary configuration.

1.11.2 Preliminary Network based Configuration

This firmware supports a methodology for a preliminary easy-configuration capability, where the physical iChip Host port is not available and iChip needs to be configured (in at least several parameters) in order to connect to the network. The methodology is based on the Parameter Profile feature, also added to this firmware version.

It is assumed that in the cases where iChip's Host port is not available and at least several parameters need to be configured in order for iChip to connect to the network – a Parameter Profile may be devised and stored in iChip to allow an improvised (temporary) IP connection for preliminary configuration purposes. For example, given a WPA secured WiFi network requires the configuration of an SSID and Pass-Phrase to connect to the Access point. A temporary network connection may be devised to support an Ad-Hoc connection on a specific (pre-known) channel and SSID. The SSID and Pass-Phrase may then be configured through that network.

1.11.3 New iChip Facilities to support Network Configuration

Several new iChip facilities have been added in this firmware version to support Easy-Network-Configuration:

1.11.3.1 Auto Start Web Server

The +iAWS (Auto Web Server) parameter behavior has been changed. When +iAWS>0 iChip will enable its Web Server under all circumstances. Previously, iChip enabled the Web server only in some special modes, such as SerialNET, and iRouter modes and only after it had assigned IP addresses for all interfaces.

1.11.3.2 Network Configuration Mode

A new mode of operation has been defined. This mode is governed by a special set of values that may be assigned to the +iAWS parameter:


- 200 -- Use SSL3 Secure Web Server
- 201, 202 or 203 -- Use Web Server with 2, 4 or 6 sockets respectively.

When +iAWS≥200 the iChip Configuration Web site (which is part of the iChip firmware) returns a special Network Configuration page. This page is dedicated to configuring only the required parameters that need to be defined to connect to a specific network.

It is envisioned that this configuration shall be a one-time configuration, under a temporary profile, which shall be used only a first time configuration to get iChip connected to a specific network, whose configuration is unknown at the time of manufacturing the product.

After the one-time configuration, it is assumed that the +iAWS parameter is assigned a value less than 200 and therefore iChip will connect to the required network and the regular iChip Configuration Web site shall be displayed and used to fully configure the iChip.

1.11.3.3 New iChip Network Configuration Web Page (when +iAWS≥200)



Web Server Status Message: OK

Network Configuration			
Parameter	Value	Limitations	Description
WIFI			
WLCH	<input type="text" value="0"/>	1..13	Wireless Lan Channel (Ad-Hoc)
WST0	<input type="text" value="3"/>	0-6,105,106	Wireless Security Type
WLK1	<input type="text"/>	32 Chars	Wireless Lan WEP Key
WLPP	<input type="text" value="*****"/>	8-63 Chars	Wireless Lan WPA Passphrase
EUSN	<input type="text"/>	64 Chars	Enterprise Domain/Username
EPSW	<input type="text"/>	64 Chars	Enterprise Password
<input type="button" value="upload CA file"/>			
WLSI	<input type="text" value="INET"/>	32 Chars	Wireless Lan SSID
<small>Available APs and Ad-Hoc networks (SSID, ADHOC or AP, BSSID, Security Type, Channel, RSSI)</small> <small>RTL8188-default AP,00:E0:4C:81:86:86,NONE,1,62</small> <small>llat_adhoc,ADHOC,02:26:16:4C:F2:44,NONE,3,65</small> <small>Yuval,AP,00:18:4D:DE:D8:35,NONE,5,58</small> <small>Jetta,AP,08:14:5C:89:4A:7C,WPA2,6,49</small> <small>GANG_TEST,AP,00:17:3F:9F:89:0E,NONE,7,63</small> <small>Blue4 The Lab,AP,00:1B:2F:87:85:62,WEP,7,68</small> <small>Bora,AP,00:14:78:F7:11:BA,NONE,7,48</small> <small>Levanto,AP,00:14:D1:4A:4C:A3,WEP,7,57</small> <small>Sirocco,AP,00:18:4D:DE:D7:DF,WPA,7,58</small> <small>Ela,AP,00:0E:2E:EB:C0:87,WPA2_ENT,7,70</small> <small>INET,AP,00:14:7C:4D:22:F3,WPA,7,59</small> <small>Mistral,AP,00:11:8B:3B:55:E2,WEP,9,61</small> <small>Zohar,AP,00:0E:2E:C6:B8:E1,WPA_ENT,11,61</small> <small>INET,AP,00:0E:2E:FD:F0:69,WPA,11,49</small>			
LAN			
DIP	<input type="text" value="0.0.0.0"/>		Default IP
SNET	<input type="text" value="255.255.0.0"/>		Subnet
IPG	<input type="text" value="172.20.0.1"/>		IP Gateway
Dialup/Cellular			
ISP1	<input type="text"/>	96 Chars	ISP's Primary Phone Number
ATH	<input type="text" value="1"/>	0..2	Authentication
USRN	<input type="text"/>	64 Chars	ISP Username
PWVD	<input type="text"/>	63 Chars	ISP Password
MTYP	<input type="text" value="0"/>	0..12,100..112,98	Modem Type
MIS	<input type="text"/>	126 Chars	Modem Initialization String
PPP	<input type="text" value="0"/>	0..2	PPP ACFC Handling
Misc			
AWS	<input type="text" value="0"/>	0..3, 100	Automatic Web Server activation
LATI	<input type="text" value="0"/>	0..65,535	Listen port to enable remote AT+i

1.11.3.4 Summary of Network Configuration Methodology

The following guidelines summarize the Easy-Network-Configuration methodology:

- Create and store a temporary network configuration Parameter Profile in iChip
- Assign +iAWS=20x in the Parameter Profile
- When in the field pull the MSEL signal LOW for +30 seconds
- Use the temporary network configuration to browse to iChip's configuration Web site
- Because +iAWS \geq 200 you will receive the special Network-Configuration Web page discussed above
- Configure the relevant Network parameters for the specific environment
- Assign +iAWS<200 and SUBMIT the configuration
- iChip should reboot and connect to the specific network it was configured for
- Try accessing the iChip from the current network. Optionally continue configuring iChip using its normal configuration Web site
- If iChip did not successfully connect to the specific Network, pull MSEL LOW for +30 seconds to reinforce the parameter profile and start over from the 4th step.

2 What was New in Release 804B02?

2.1 Host Web Site up to 256K

Previously, the iChip's internal Host Web site was limited to a maximal size of 64K. This limitation has been alleviated to a maximal size of **256K**.

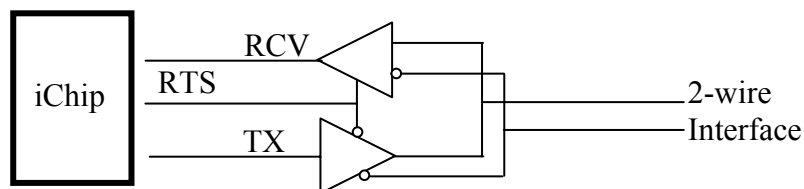
2.2 RS-485 host interface

2.2.1 Introduction

A new Host interface has been added to iChip to support a half-duplex, 2-wire, RS485 connection.

The 2-Wire RS485 interface is based on using the same 2 wires for send and receive. The potential interference between transmit and receive modes is resolved by toggling the wire use in the time-space. The RTS H/W flow control signal is used by the UART to signal the wire direction and can thus be used to gate the send/receive RS485 buffers.

The following block diagram depicts this:



Note that the 2-wire interface is connected to both the receive and transmit buffers. The RTS signal is used to gate the buffers so only one path (TX or RX) is active at one time.

When iChip is configured for half-duplex RS485, the iChip ECHO is automatically turned off, regardless of the AT+iEn command.

The half-duplex, 2-wire, RS485 setting is also available in SerialNET, however, if full-duplex exchange shall be attempted, data shall be lost.

2.2.2 Configuration

The iChip is configured for half-duplex, 2-wire, RS485 mode via the +iHIF parameter. A value of 101 defines the RS485 interface on iChip's COM0 while a value of 102 defines this interface on iChip's COM1. The full syntax of the +iHIF parameter now becomes:

Syntax: AT+iHIF=*n*

Specifies the interface to be used for communication between the host processor and iChip in subsequent sessions. This parameter takes effect only after power-up.

Parameters:

n=0 Automatic host interface detection. In this mode, the first character sent from the host over one of the supported interfaces sets the host interface to be used throughout that session until the next iChip power cycle.

n=1 USART0

n=2 USART1

n=3 USART2

n=4 USB Device

n=5 USB Host

n=6 SPI-1

n=101 Half-Duplex, 2-wire, RS485 on USART0

n=102 Half-Duplex, 2-wire, RS485 on USART1

Default: 0 (Automatic host interface detection)

Result Code:

I/OK If *n* is within limits

I/ERROR Otherwise

AT+iHIF? Reports the current value followed by **I/OK**.

AT+iHIF=? Returns the message “0-6,101,102” followed by **I/OK**.

3 What is New in Release 804B04?

3.1 Extended URL parameter to 256 characters

The URL argument in the AT+iRLNK command and the associated +iURL parameter have been extended to a maximum of 256 characters. In previous versions, these fields were limited to 128 characters.

3.2 Change of allowed values for the +iPGT (PING Timeout) parameter

The range of allowed values for the +iPGT parameter have been changed to: 0 (Disabled) or 50-65535 (timeout in mSec after which iChip will reissue a PING request). Previously, the allowed range was 0-65535.

3.3 Change of allowed values for the +iWSRL and +iWSRH (WiFi SNR thresholds)

The allowed range for the +iWSRL (SNR-Low) threshold has been changed to: 0 to 245.

The allowed range for the +iWSRH (SNR-High) threshold has been changed to: 10 to 255. This provides a minimum of 10 counts between the two thresholds at the two extreme ends.

3.4 WiFi Power-Save Mode

The iChip Power-save mode procedure has been updated so that iChip will not wakeup the WiFi module in order to scan for AP's if the +iWLSI parameter contains the '*' value. When the +iWLSI contains the '*' value it signals to iChip not to connect to AP's. Therefore, waking the WiFi module to scan in this case was redundant as well as wasteful.

4 Limitations Solved

<i>Reference</i>	<i>Description</i>
1635	Previously, the PPP connection with the host failed when HIF was 4 (USB Device). This has now been corrected.
1669	Corrected the SNSI parameter validity check. Previously, the host could set the "flow" field to any value without getting I/ERROR 042, although the flow field is restricted to values 0 or 1 only.
1674	Previously, when in modem platform (CPF=0), error 410 had been received when AT+iUP was issued after AT+iBDRA. This has been corrected.
1683	Previously, issuing the AT+iRP8 command caused a small accumulated delay in the iChip's internal clock. Now, this has been fixed and no delay occurs.
1686	Previously, issuing the command AT+iUP when a GPRS modem was connected to iChip and when iChip was configured with an invalid ISP number caused iChip to stop responding. This has now been corrected.
1689	Previously, when iChip received a file using FTP/SSL over WiFi, the I/ONLINE response arrived only about one minute after all the data was received. This has been corrected.
1695	Previously, iChip lost data when in SerialNET mode (SNMD was set to value 2 or 3) in a dial-up configuration if data was sent right after the SNMD command. This has been corrected.
1700	Previously, iChip failed to connect to an AP with WPA2-PSK Auto mode (both TKIP and AES). This has been corrected.
1701	Previously, when trying to clear an already empty PKEY (by issuing AT+iPKEY=<CR><CR>) iChip stopped responding. This has been corrected.
1702	Previously sending more than 65535 bytes using the SSND command over a UDP socket caused iChip to stop responding. Now, a new error code (230) will be returned in this case.
1703	Previously, iChip failed to connect to a Cisco ACS when the RADIUS server was configured with multiple authentication types. This has been corrected.
1704	Previously, when trying to upload an RPF file through the configuration website the process failed. This has been corrected.
1706	Previously, iChip did not accept a UDP broadcast packet, even when configured with a UDP "listen" socket. This has been corrected.
1709	Previously, when using a LAN platform (e.g. LTYP=2), the command AT+iRP2 had returned "Command mode" even when there was no Ethernet PHY connected. Now it returns "NO LAN" in this case.
1710	Previously, if terminating quotes (") were used when setting a parameter value to a string containing only one character, and setting this parameter occurs right after surfing to one of the parameter pages in the configuration website, the quotes were saved as the second character of the parameter. This has been corrected. Now the quotes are not stored in the parameter in this situation.

1713	Previously, when the iChip host interface is set to "USB Host" (AT+iHIF=5) – iChip did not detect its host (perform the enumeration process) after the host disconnected or reset. Now, iChip properly performs the enumeration process when the host is reconnected.
1717	Previously, in iChip versions 802Bxx, when a user entered the iChip password (RPG) in a host website (required when the host website allows updating internal iChip parameters), the password page and the updated values were not submitted to iChip's web server at all. This has been corrected.
1722	Previously, iChip returned a misleading error code (042) in response to the AT+iWWW:n (n≠0) command when the WEB server was already up with a different backlog. Now, in such a case, iChip returns error code 309.
1723	Previously, the command AT+iRP0 returned the same response for both CO2128 and CO2144 chips. Now the responses are appropriately different.
1724	Previously, when the iChip was set for Network-Configuration, +iAWS≥200, and the RPG parameter had a non-empty value – loading a CA via the Network Configuration page succeeded without submitting the password (even though an "iChip authentication error" is displayed). Now, when the RPG parameter has a non-empty value, iChip asks the user for a password before displaying the host or iChip WEB page.
1725	Previously, the SPI-1 chip-select pin (PIO-C #21) was configured without pull-up. Now, during auto host detection time, SPI-1 chip-select pin is configured with a pull-down.
1726	Previously, the DTM6211 USB modem did not work well with iChip. This problem has been fixed. Note: in order to use this specific modem it is not allowed to work in auto host or auto baud-rate detection mode.
1727	Previously, when iChip was configured for Modem Communication Platform (AT+iCPF=0) and iChip was set to Auto WEB Server mode (AT+iAWS=n, n≠0), iChip didn't go online after the AT+iWWW command. Now, after AT+iWWW iChip does go online.
1729	Previously, when setting the WPA parameter after the LTYP parameter was changed from 2 (LAN only) to 0 (auto-mode) or to 1 (WLAN only), without a software reset, it may have caused the PSK parameter to have a wrong value. This has been fixed.
1730	Previously, iChip failed to connect to an Access-Point (AP) with multiple authenticate key management ("mixed mode"). This problem is fixed and now the iChip establishes a connection with such an AP either when the iChip is set to WPA security or to WPA Enterprise security mode.
1731	Previously, when the UID field was empty the command "AT+iUID?" returned a non-empty string. This was fixed and now, in such a case, iChip returns an empty string.
1733	Previously, in LAN platform (AT+iCPF=1) when there were no open sockets, the "Link Lost event was not reported in response to the AT+iRP2 command. This problem was fixed.
1735	Previously, when using an AP that was configured to security-type WPA with encryption-type CCMP/AES, the iChip reported the security-type (AT+iRP20) as WPA2 instead of WPA. Now, iChip reports the correct security type.

1738	Previously, iChip failed to connect to an AP that includes both WPA and WPA2 IE in its beacon. In this case it also returned an incorrect report. This has been fixed. Now iChip succeeds in this connection.
1742	Previously, when iChip was in the LAN to WiFi bridge mode (AT+iBRM) it had added the FCS bytes to the data causing the TCP connection to fail. Now, the FCS bytes are not transmitted at all.
1744	Previously, when iChip was configured to Ethernet LAN (LTYP=2) in a dialup environment (CPF=0), iChip did not respond to AT+iWWW:0 after a browser had surfed to its configuration site. This has been fixed.
1745	Previously, when In modem communication platform (CPF=0, dial-up + WLAN environment), iChip stopped responding when it received the command AT+iDOWN immediately after received the command AT+iWWW:0 after a browser had surfed to its configuration site. This has been fixed.
1747	Previously, when the LAN cable was disconnected, iChip did not respond to the AT+ISSL:0 command, This has been fixed.
1748	Previously, when the LTYP parameter was configured as Ethernet only (LTYP=2) issuing the command AT+iWRST caused iChip to stop responding. Now iChip responds correctly.
1751	Previously, receiving 2 files during the same FTP session, caused iChip to stay online after the AT+iFCLS command. Now iChip will correctly close the FTP session.
1752	Previously, iChip returned error 416 as a response to a WiFi command (e.g. AT+iRP11) even when the WLAN device was functioning well. This has now been corrected.
1759	Previously, iChip had sent ICMP replies to packets that were subnet directed broadcasts before it got an IP address. Now iChip does not reply to ICMP packets in this case.
1765	Previously, the AT+iRLNK command may have returned with error 300 ("bad host name") although the host name was legal and reachable (a secondary attempt usually succeeded). This has been corrected. Now RLNK commands to reachable host devices will always succeed.
1766	Previously, the first AT+iRLNK command, after a SW or HW reset, had failed for some URL addresses. This has been corrected.
1769	Previously, in version 804b03, trying to perform a remote firmware update over HTTP (AT+iRFU) has failed with I/ERROR (301). This has been corrected.
1770	Previously, in version 804b02, performing the command AT+iRFU failed with I/ERROR (205) although the update process completed successfully. The erroneous error message has been removed.
1772	Previously, the DHCP server failed when iChip was in SerialNET mode and the HSRV parameter was set to the same IP address as the IP address that was offered to the client. This has been corrected. Now the DHCP server will succeed to allocate the IP address in this case.
1773	Previously, the +iSPIP parameter did not retain its value after the AT+iFD (Factory Defaults) command was applied. This has been corrected. The +iSPIP parameter now retains its value.
1775	Previously, in LAN platform, after disconnecting and reconnecting the Ethernet cable, iChip remained in the "link lost" state. This has been corrected. Now it will restore the connection and return to "command mode".

1777	Previously, iChip certified a secured WEB server and received its HTTPS data even when it did not have a CA defined. This has been corrected. Now in the absence of a CA, iChip will never authenticate an HTTPS server.
------	--

5 Known Limitations in 804B04

Ref.	Description
General	
1385	Plugging-in the Wi-Fi antenna when iChip is working may cause the iChip to stop responding to incoming data (host and network data) for few seconds
1438	It is impossible to receive file using FTP SSL in baud-rate 9600 and less.
1462	TCP sending of a 1Mb file fails Error (111).
1463	TCP receiving file at 1.5Mbps fails
1536	When in iRouter mode, displayed DNS values (AT+iDNSn? commands) are not updated when the CPF parameter is changed. However, internally the DNS list is correct.
1547	Lack of sufficient memory causes severe limitations when working with FTP over SSL. This may cause, for example, inability to get a directory list (At+iFDL) or retrieving a file
1579	iChip crashed while receiving data in SerialNET mode with SSL when PTD=1 and MTTF=1000
1620	AT+I replies not received over LATI socket when the Serial port is disconnected and set to H/W flow control (FLW=3)
1673	iChip must be restarted (power recycled) when the GPRS modem is restarted (power recycle)
1684	Host web site authentication (WPWD) is per IP and not per browser session
1711	When USB Host is used as the host interface, the iChip “wake-up” indications (e.g. I/ONLINE) are lost
1712	After disconnecting and then reconnecting to iChip with a working USB device (HIF=5) -- no data is transferred
1746	In response to the AT+iTOPN command, iChip responds with I/ONLINE instead of I/OK
1761	When connecting to an AP operating in 802.11b, iChip tries to send packets in 802.11g mode before changing to 802.11b mode.

6 Supported Platforms

iChip OS i2128D804B04 supports the platforms listed below.

<i>Type</i>	<i>Model</i>	<i>Comments</i>
iChip	CO2128, CO2144	
Embedded Device Server	Secure Socket iWiFi	
Embedded Device Server	mini Socket iWiFi	
Embedded Device Server	Nano WiReach	
Embedded Device Server	Nano LANReach	
Embedded Device Server	Nano Socket iWiFi	
Embedded Device Server	Nano Socket LAN	
External Device Server	Secure iLAN	
External Device Server	Secure iWiFi	

7 Firmware File Information

The following table includes detailed information that can be used to verify the integrity of the downloaded firmware.

804B04	<i>File Name</i>	<i>File Size (bytes)</i>	<i>MD5 Checksum</i>
IMF (Local firmware update)	i2128d804b04.imf	563,412	2e3fd9ccc8d15cc6f8bd911cba880fd9
IMZ (Remote firmware update) Note: Only for 2Mb Flash	i2128d804b04.imz	372,573	7a8ccf50576a329321a2bf8eae588da1