



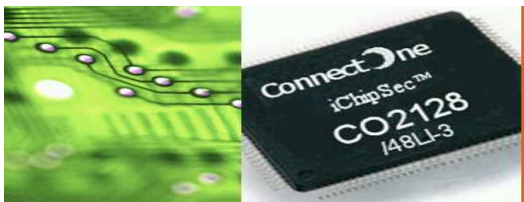
March 2010

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 i2128D807B06

Revision 1.00

PRELIMINARY

Reference Version: 806B05

Table of Contents

1.	WHAT IS NEW IN RELEASE 807B06?.....	3
1.1	ENHANCED HOST-USB THROUGHPUT	3
1.2	SUPPORT FOR ADDITIONAL USB MODEMS.....	3
1.3	IGNORE SSL SERVER CA VALIDATION	4
1.4	AT+I COMMANDS VIA LAN WHEN USING A MODEM	4
1.5	ENTERPRISE MODE ENLARGED USER NAME PARAMETER	4
1.6	GRATUITOUS ARP	4
1.7	REMOTE UPDATE OF SECURE FIELDS VIA HTTPS	5
1.8	BRIDGE MODE MAC-FILTER.....	5
1.9	IMPROVED PPP-OVER-USB PERFORMANCE	5
1.10	SUPPORT FOR EAP-TLS IN ENTERPRISE MODE	5
1.11	SUPPORT FOR WPS (WiFi PROTECTED SETUP) CONFIGURATION	6
	<i>AT+iWPSP – Configure WPS “push-button” PIN:</i>	7
	<i>At+iAWPS – Activate WPS using from Host:</i>	7
1.12	AUTO CONNECTION TO IP-ENABLED AP	8
1.13	NEW WiFi AD-HOC SETTING: “DO NOT MERGE”	9
1.14	SOCKET OPERATIONS VIA PROXY SERVER	9
1.15	ENHANCED RP2 REPORT IN BRIDGE MODE	10
2	LIMITATIONS SOLVED	11
3	KNOWN LIMITATIONS IN 807B06	15
4	SUPPORTED PLATFORMS	16
5	FIRMWARE FILE INFORMATION	16

1. What is New in Release 807B06?

1.1 Enhanced Host-USB throughput

iChip's USB Host previously operated in "Interrupt Mode". It has now been enhanced to operate in "Bulk Mode". Therefore, potential throughput performance has increased from 500Kb/Sec to 2Mb/Sec.

1.2 Support for Additional USB Modems

Additional USB modems are now supported by iChip's USB host. Following is the updated list of pre-qualified USB modems:

- SIMCON 5218E
- Siemens HC25
- Qualcomm 3G CDMA iCON 225
- HUAWEI EC1260
(E620 USB Modem)
- HUAWEI EC169
(E620 USB Modem)
- HUAWEI EM660
- HUAWEI EM770
- HUAWEI EM560
- ZTE MF622
- ZTE MF626
- ZTE MF636
- ZTE MF637
- ZTE MF626
- ZTE AC580
- ZTE AC2716
- ZTE AC8710
- ZTE AC2726
- ZTE AC2736
- ZTE AC8700 (EV-DO)
- ZTE AC8710
- ZTE HSDPA Z100M
(ZTE AD3801)
- DTmobile DTM6211
- U6100 LONGSUNG
- Longsung U5100
- LongCheer U5300
- Iridium Handset 9555
- Motorola H24
- Motorola C-Light
- Motorola Phone (H24)
- Motorola Phone (G24)
- One Touch X200

1.3 Ignore SSL Server CA validation

An additional configuration setting has been added to disable server certificate validation with a CA certificate while opening an SSL3/TLS1 socket. The new setting is implemented in the +iSDM (Service Disable Mask) parameter. To disable Server certificate validation, set the +iSDM bit 7 to '1' (bit 7 is the Eighth LSB, mask value 0x80).

The AT+iSDM=? Command shall now return 0-255 accordingly.

1.4 AT+I Commands via LAN when using a Modem

When the +iLATI parameter contains a port number, a remote user may open a socket to this port on the iChip's IP and manage an AT+I session across this socket. In previous versions the +iLATI parameter could have been used only through the communication platform selected by the +iCPF parameter. Now, a new feature allows connecting to the +iLATI port for AT+I command exchange through either the LAN/WiFi or the Dialup communication platform regardless the setting of the +iCPF parameter. As a result, iChip will attempt to resolve an IP address on the LAN end even when +iCPF is set to 0 (Modem) and will support setting up a TCP socket to the +iLATI port if it contains a port value (>0).

1.5 Enterprise Mode Enlarged User Name Parameter

The +iEUSN (Enterprise User Name) parameter has been enlarged to contain a string of up to 64 characters. In previous versions this parameter size was limited to 20 characters.

1.6 Gratuitous ARP

The purpose of Gratuitous ARP is mainly to inform routers and stations of a new LAN client that has joined the network or of a client whose MAC address or IP address has changed. This way other stations and routers / switches can update their ARP tables with the new data to save time and traffic later when they need to access that LAN client.

Clients usually send this message when they are assigned an IP address, recover from a Link Lost condition or undergo any change in their MAC / IP address.

Starting from this version, iChip shall send a Gratuitous ARP immediately upon going online and establishing a new IP on its LAN end. iChip shall also send a Gratuitous ARP after regaining the LAN link from a Link-Lost condition.

iChip sends Gratuitous ARP packets only when connected to an Ethernet or Wireless LAN.

1.7 Remote Update of Secure Fields via HTTPS

In previous versions iChip did not have provisions to remotely update secure fields (such as passwords and security keys) via its configuration Web site. The rationale behind this was to eliminate an obvious security hole if clear-text updates would have been allowed.

Since iChip now has an HTTPS secure configuration Web site, an additional tab has been added to the secure site, which allows remote submittal of secure fields.

When using iChip's non-secure HTTP configuration Web site, this tab shall be disabled.

1.8 Bridge Mode MAC-Filter

When iChip is configured to operate in Bridge mode (LAN↔WiFi Bridge), iChip expects packets from only a single Ethernet MAC address on the Ethernet connection. If more than one system is connected on the Ethernet end, iChip may become confused and results are undetermined.

A new feature has been added which allows iChip to operate as a LAN↔WiFi bridge in an environment where several LAN devices exist on the Ethernet side, while iChip bridges only packets from one specific MAC address and disregards the rest.

When the iChip's +iMACF (MAC Address Filter) parameter contains an Ethernet MAC address in association with Bridge modes 2 or 4 (LAN↔WiFi), iChip will use the MAC address value in this parameter to restrict bridging of packets to/from this MAC address only. Other packets shall be discarded.

1.9 Improved PPP-over-USB Performance

This version contains a complete overhaul of the PPP and USB drivers used in communicating via USB cellular modems. As a result, performance has been significantly boosted.

iChip can now provide as much as 2Mb/s download and 1Mb/s upload sustained throughput when working with a USB 3G cellular modem.

1.10 Support for EAP-TLS in Enterprise Mode

iChip now supports the EAP-TLS convention when connecting to a RADIUS server to complete its WiFi Enterprise-mode security.

1.11 Support for WPS (WiFi Protected Setup) Configuration

WPS (WiFi Protected Setup) is a standard endorsed by the WiFi alliance for easy and secure establishment of a wireless network. Traditionally, users need to manually create a wireless network name (**SSID**), and then manually enter a creative, yet sometimes predictable, security key on both the AP and clients to prevent unwanted access to their wireless network. This process requires the users to have the background knowledge related to WiFi device configuration.

With WPS, users can automatically configure a wireless network with a network name (**SSID**) and strong WPA data encryption and authentication.

Several methodologies are available to carry out the WPS negotiation. iChip implements the PBS method which specifies that a physical or virtual push-button is depressed in both the AP and the client, allowing for a 2-minute window within which the WPS negotiation must be completed. The WPS negotiation is managed entirely automatically over the wireless medium and results in the WiFi station fully configured for communications through the AP.

A new parameter, +iWPSP (WPS Pin) has been added to iChip to allow configuring a HW pin that will be referenced as the WPS physical Push-Button, to activate a WPS session. Furthermore, a new command, AT+iAWPS (Activate WPS) has been added to activate a WPS session from the host processor.

After activating a WPS session, iChip de-authenticates from current AP and starts scanning for WPS-enabled APs in the surroundings. iChip maintains this scan for a maximum of two minutes. If within this period time, iChip does not find a WPS-enabled AP, it will exit WPS mode and reconnect to the last AP.

According to WPS specifications, the Scan results should contain only **ONE** valid AP. Otherwise, iChip must exit WPS mode and reconnect to the last AP.

When iChip finds a single valid AP, it starts the WPS session negotiation. The WPS session will run on the wireless medium as a series of EAP request/response messages, which is successfully concluded with iChip updating its parameters in flash with the new AP credentials. iChip will then connect to the AP using the new credentials.

IMPORTANT NOTE: If the WPS AP credentials contain a WPA pass-phrase, iChip shall automatically calculate the PSK according to the new SSID and pass-phrase. Hence, iChip will not respond to AT+i commands for about 25-30 seconds (as is the case when changing +iWLSI or +iWLPP parameters).

Following are the full AT+I syntax for the new parameter and new command:

AT+iWPSP – Configure WPS “push-button” PIN:

Syntax: AT+iWPSP=<pin>

Defines which of iChip’s general-purpose I/O pins (GPIO) will be used as a push-button for activating WPS.

Parameters:

pin=0 WPS mode is disabled.
pin=1-6 Pins 0-5 of PIOC (general-purpose I/O pins group C)
Default: 0 (port disabled)

Result Code:

I/OK If *pin* is within limits
I/ERROR Otherwise

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

AT+iWPSP=? Returns the message “**0-6**” followed by **I/OK**.

Note: The setting will take effect only after a SW or HW reset.

At+iAWPS – Activate WPS using from Host:

Syntax: AT+iAWPS

Activates a WPS configuration session regardless of the +iWPSP setting. iChip’s communication platform must be WiFi for this command to perform correctly.

Parameters: None

Result Code: **I/OK** If iChip’s Communication platform is WiFi
I/ERROR Otherwise

1.12 Auto Connection to IP-Enabled AP

iChip contains an elaborate scheme according to which it selects the most appropriate AP to connect with, given an SSID setting and relative transmission strengths. A new feature has now been added, that adds an additional criterion to decide on an appropriate AP. The criterion is that the AP is Internet enabled. In other words, an AP that can be used to access the public internet.

The modified selection procedure contains two phases. The first phase includes locating an AP in the normal manner. The second phase includes attempting a PING to a well-defined system on the Internet. If the PING command succeeds, iChip shall remain connected to that AP, otherwise it will continue searching for another AP. Two existing parameters are utilized to contain the PING destination addresses to use. These parameters are +iPDSn (n=1..2). The +iPDSn parameters are also used for a similar purpose, when verifying that the modem is ONLINE.

A new parameter, +iWIAP (Wireless Internet-Enabled AP) has been added to enable this type of AP search.

The new parameter shall have a default value of 0 (disabled). When assigned with a value in the range 1-255, the Internet-Enabled AP seek mode shall be enabled and the +iWIAP value shall indicate the maximum time in seconds to wait for an IP assignment from a DHCP server. When in Internet-enabled AP seek mode, while seeking for an Internet-Enabled AP, the AT+i!RP10 shall report:

“Scanning for IP-Enabled AP”

Since the +iPDSn parameters are used to verify that the AP tested is Internet-Enabled, if both are empty the test cannot be performed. Therefore, if +iWIAP>0 and both +iPDSn parameters are empty, iChip will not connect to any AP.

Changes to the +iWIAP parameter require a SW reset to take affect.

The full syntax of the new parameter is:

+iWIAP — Enable Seeking Internet-Enabled AP

Syntax: AT+iWIAP=<*n*>

Sets iChip to Internet-Enabled AP seek mode.

Requires SW reset to take affect

Parameters: *n*=0 - 255

n=0 Disable seek mode.

n>0 Enable seek mode. *n* value indicates the maximum time in seconds to wait for an IP assignment from a DHCP server.

Default: *n*=0

Result Code:

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

I/ERROR Otherwise

AT+iWIAP? Returns the current WIAP value followed by **I/OK**.

AT+iWIAP=? Returns the message “**0-255**” followed by **I/OK**.

1.13 New WiFi Ad-Hoc Setting: “Do Not Merge”

A new setting added to this version allows configuring iChip in Ad-Hoc mode but eliminating the Ad-Hoc network merging procedure. To do this the +iWLCH (Wireless LAN Channel number) must contain a +100 offset. For example, instead of setting to channel 6, set +iWLCH to channel 106.

With this setting iChip shall setup an Ad-Hoc network (Assuming +iWLSI is preceded with an ‘!’) on channel 6 and network merging is disabled.

The network merging procedure occurs when 2 individual Ad-Hoc networks with the same SSID come dynamically into range and merge into one large Ad-Hoc network.

1.14 Socket Operations via Proxy Server

A new feature has been added to iChip to support working through a Proxy server. To support this feature a new parameter, +iPRXY, has been added. When this parameter contains a non-empty value, it is interpreted as an <IP>:<port> of a proxy server through which communications to the outside world must be routed.

The full syntax of this parameter is:

+iPRXY — Define Proxy Server

Syntax: AT+iPRXY="<IP>:<Port>"

Sets the IP address and port of the Proxy to use for all subsequent socket communications.

Parameters:

<IP>:<Port> *IP* has the format x.x.x.x
Port is 0..65535

Default: Empty (Do not use a Proxy server)

Result Code:

I/OK If parameter is a single string

I/ERROR Otherwise

AT+iPRXY? Returns the current PRXY value followed by **I/OK**.

AT+iPRXY=? Returns the message "**string**" followed by **I/OK**.

Note: In version 807, +iPRXY is an alias to +iUF12. Therefore, values set to +iPRXY or +iUF12 shall be stored in the same memory element. This situation shall be ratified in the next FW version (808), where +iUF12 and +iPRXY shall be individual, mutually exclusive, parameters.

1.15 Enhanced RP2 report in Bridge Mode

The AT+iRP2 report reply has been enhanced when iChip is operating under Bridge-mode (+iBRM > 0). The motivation for this is to allow the host processor to inspect and supervise the quality of the LAN and WiFi connections.

When under Bridge mode, iChip shall reply to the AT+iRP2 command with:

LAN/WIFI Bridge Mode,<LAN Status>,<WIFI status>

Where,

LAN Status: 0 – NO Link
1 – Link OK

WIFI Status: 1 – Not connected
2 – Connecting
4 – Connected

2 Limitations Solved

<i>Reference</i>	<i>Description</i>
1712	Previously, after disconnecting and then reconnecting a working USB device to the iChip (e.g. a USB modem) no data could have been exchanged between the USB device and the iChip. This problem was fixed and now you can disconnect and reconnect USB devices without affecting iChip functionality.
1763	Previously, iChip may not have recovered from power failure that had happened during an RFU (Remote FW Update) process. This problem was fixed and now iChip always recovers, even if a power failure occurs during an RFU process.
1783	Previously, when iChip was defined to go on-line automatically on the modem end (e.g. ARS=1), and the modem did not respond, iChip would fail to go on-line and could never recover from this state. This problem was fixed and now iChip will go on-line as soon as it detects a modem.
1791	Previously, the IP Readiness indication might not have work properly when multiple SSID's were defined and the iChip could not connect to the first SSID (WLSI), which was defined with WPA or WPA2 security, but did connect to one of the other SSID's. This problem was fixed and now the IP Readiness indication will work properly regardless of the configuration of the SSID list and the connected SSID.
1802	Previously, the data flow control protocol, used by iChip when working with SPI as a host interface was not stable. This problem was fixed and now the SPI protocol is fully and properly implemented.
1819	Previously, when iChip was on-line (connected to ISP), the AT+iFU command did not respond. This phenomenon was fixed and now iChip always responds to the +iFU command. When iChip is connected to an ISP, iChip will respond with "/I/ERROR (112)".
1825	Previously, iChip occasionally crashed while processing incoming PPP packets while in iRouter mode when the modem interface was USB (iMIF=5). This phenomenon was fixed.
1836	Previously, iChip failed to receive a file larger than 20KB using FTP over SSL when connecting over LAN. This problem was fixed.
1838	Previously, the Port Forwarding parameters (iPFWn) were not exposed in the iChip configuration WEB site. This problem was fixed and now the iPFWn parameters can be accessed and changed via the iChip WEB site.
1845	Previously, when iChip used its USB Device Port as its host interface and it was not connected to the host, the DHCP Server did not work. This problem was fixed and now the DHCP Server works regardless of the host interface connectivity status.
1846	Previously, when iChip used a USB modem as its cellular modem, iChip might have exited auto-host and auto-baud-rate detection mode before a host was actually detected. This phenomenon is fixed and now iChip exits the auto-detection mode only after detecting a "real" host.
1847	Previously, iChip stopped responding to AT+I commands after disconnecting a

	USB modem. This phenomenon is now fixed.
1848	Previously, some USB modems (like the ZTE MF636) was overwrote firmware data during an RFU process. This phenomenon does not happen any more.
1849	Previously, iChip sometimes detected an Ethernet "Link Lost" condition for no apparent reason. This phenomenon is fixed and the Link Lost is asserted only when there is a real link lost event.
1850	Previously, iChip did not work properly in modem communication platform (+iCPF=0) when using SPI as its host interface (+iHIF=6). This problem is fixed and now the SPI interface is full functioning as a host interface even when +iCPF=0.
1851	Previously, when iChip was in bridge mode, data was not sent to WiFi clients which were defined with WEP security after disconnecting and then reconnecting the LAN client. This phenomenon is fixed and now data transfer continues regardless of the WiFi client security type.
1862	Previously, when iChip was in bridge mode, issuing a WiFi report caused iChip to stop responding. This phenomenon is fixed and now it is allowed to issue Wi-Fi report commands (+iRP10 and +iRP20) when iChip is in bridge mode.
1863	Previously, iChip failed to establish an SSL connection when the SSL server supports SSLv3 handshake only. This problem is fixed and now iChip can establish an SSL connection with servers that support SSLv3 handshake negotiation only.
1864	Previously, once iChip experienced problems sending an email, it repeatedly reported the error until the next reboot. This phenomenon is fixed and now iChip reports the error only once.
1866	Previously, iChip did not report I/ERROR(074) after a link lost condition when WIFI is used and an active TCP socket existed. This problem is fixed and now iChip reports "I/ERROR (074)" as a result of WiFi link lost regardless of socket status.
1871	Previously, when iChip was connected to an Ethernet 100BaseT switch, the commands +IETHD and +IETHU did not work as expected. This problem is fixed and now +IETHD shuts down the Ethernet PHY while +IETHU restarts the Ethernet PHY even when iChip is connected to an Ethernet 100BaseT switch.
1873	Previously, changing the WiFi security type while iChip was connected caused a mistaken report from iChip (as response to +iIRP10). This phenomenon is fixed and now iChip reports the correct security type.
1874	Previously, iChip did not properly handle a modem plug-out/plug-in cycle when the modem was in command mode. This problem was fixed and now USB modems can be plugged-out/plugged-in and iChip will detect and initialize the new modem.
1875	Previously, the "HW" parameters +iSPIP, +iRRHW, +iSLED, and +iADCP were not retain across a factory default restore. This problem is fixed and now the above parameter values are retained when issuing factory default restore (+iFD).
1876	Previously, iChip did not work properly, with the cellular networks, when the +iHIF parameter was USB Device (iHIF=4) and the MIF parameter was USB Host (iMIF=5). This problem is fixed and now the iChip works properly with the cellular networks regardless of the host interface setting.
1877	Previously, when the +iCPF parameter was 1 (LAN Communication Platform), iChip always responded with "I/ERROR (070)" when issuing the +iSTRR

	command to enter iRouter mode. This phenomenon is fixed and now the host can activate the iRouter mode even when the iCPF parameter is set to 1.
1880	Previously, the DIP parameter did not accept "000" as a valid value. This problem is fixed.
1882	Previously, trying to upload an RPF file via the iChip Configuration WEB site had failed. This problem is fixed.
1885	Previously, using POST method to set parameters in iChip did not always succeed and may have caused memory leakage problem. This problem is fixed and now iChip parameters may be set using the POST method.
1891	Previously, issuing an empty POST request to iChip caused iChip to stop responding. This phenomenon is fixed and now iChip can receive an empty POST command and continue normally.
1892	Previously, when issuing the command AT+iLSST for a socket created by a remote client (to an iChip LISTEN socket) the response may not have been correct. This has been fixed.
1896	Previously, iChip failed to connect to a WPA secured AP when the iMACF parameter was defined. This problem was fixed and now iChip with a MAC filter configuration can connect to an AP independent of the security setting.
1898	Previously, when issuing the command AT+iSNMD, while iChip was configured for Modem Communication Platform (+iCPF=0) with automatic WEB Server (+iAWS>0), it did not enable the WEB site on the LAN side. This has been corrected. Now the Web is enabled both on the Modem end and the LAN end.
1899	Previously, iChip failed to perform roaming between two AP's that were configured with WEP security. This problem was fixed and now iChip can perform roaming when the AP's are configured for WEP security.
1900	Previously, iChip failed to associate with an AP that was configured to use a shared WEP key. This problem was fixed.
1901	Previously, when setting iChip to host-auto-detection mode, iChip failed to detect a host that was connected to the iChip via the SPI interface. This has now been corrected.
1903	Previously, when working with the SPI host interface (+iHIF=6), the SPI_INT pin was not cleared after it was set due to flow-control. Now it is properly cleared.
1904	Previously, sometimes iChip stopped responding after performing a firmware update. This has been corrected.
1905	Previously, when pulling the MSEL signal LOW, while iChip was running, for more than 5 seconds did not cause iChip to enter host-auto-detect mode. This has been corrected. Now iChip always enters host-auto-detect-mode in this case.
1906	Previously, when iChip performed a SW reset (e.g. AT+iDOWN) the "special" PIOs (i.e. SPIP, RRHW, WPSP, etc.) may have experienced a "glitch". For example the SPI_INT pin may have been asserted high and then cleared.
1912	Previously, In LAN-to-WIFI bridge mode, iChip stopped passing data from the Ethernet side to the WIFI side when many "small" UDP packets were sent from the Ethernet side. This problem has been fixed and iChip continues transferring data in this scenario.
1919	Previously, Issuing the command at+iWRFD while iChip was defined as an Ad-Hoc member responded, after a "long" time, with I/ERROR (403). This

	phenomenon was fixed and now the iChip accepts the command and responses with I/OK.
1920	Previously, when the host issued the "AT+iPID?" command and the PID was set to 13, iChip responded with an erroneous string. This phenomenon was fixed and now iChip returns the correct response ("SCKT-WIFI-WI2WI-EU").
1928	Previously, when activating the PING Keep-Alive mechanism, iChip used a fixed value of 2-seconds as the timeout when waiting for the PING reply. This behavior was changed and now iChip uses the +iPGT parameter's value as the timeout for the PING reply.

3 Known Limitations in 807B06

<i>Ref.</i>	<i>Description</i>
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 files using FTP SSL at baud-rates of 9600 and less.
1533	Sometimes Error 051(Syntax error) or error 053 (Illegal command code) appears when setting the CA certificate parameter
1536	DNS values are not updated when the CPF parameter is changed
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)
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
1746	In response to the AT+iTOPN command, the iChip returns I/ONLINE instead of I/OK
1761	When connecting to a B-Mode AP, iChip tries to send packets at G-Mode rate before it shifts down to B-Mode rates.
1813	In case of EBI flash defects (i.e. write operation failure) iChip may stop responding
1832	When trying to set parameters (such as URL, whose size is limited to 256 characters) to a string longer than 256 characters via the iChip WEB site – iChip does not return an error indication but truncates the input string to 256 characters.
1869	When setting +iFLW=3, iChip does not transparently transfer the DSR(host) to DTR(modem)
1927	WiFi connection failure when connecting to a WPA-PSK AP when the WPA passphrase is set to “*****” (8 asterisks).
1930	FTP Receive (+iFRCV) over cellular network is very slow (several 10's KBits).

4 Supported Platforms

iChip OS i2128D807B06 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	

5 Firmware File Information

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

807B06	<i>File Name</i>	<i>File Size (bytes)</i>	<i>MD5 Checksum</i>
IMF (Local firmware update)	i2128d807b06.imf	622580	415b673f798d31bf4c65b257ca26b637
IMZ (Remote firmware update) Note: Only for 2Mb Flash	i2128d807b06.imz	407318	78ae198d1c405dd3dfc0cba874f0589f