

**iChip and the
Internet Protocols:
Much More than Just TCP/IP**

A TCP/IP Primer



International:
Connect One Ltd.
2 Hanagar Street
Kfar Saba 44425, Israel
Tel: +972-9-766-0456
Fax: +972-9-766-0461
E-mail: info@connectone.com
<http://www.connectone.com>

USA:
Connect One Semiconductors, Inc.
15818 North 9th Ave.
Phoenix, AZ 85023
Tel: 408-986-9602
Fax: 602-485-3715
E-mail: info@connectone.com
<http://www.connectone.com>

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Executive Summary

The Internet is a complex, unpredictable, dynamic medium that is constantly evolving. New protocols and modifications to existing protocols are being introduced all the time, which demands that an Internet connectivity solution must be equally dynamic. ISPs and operators of wireless IP networks do not implement Internet protocols consistently, which requires that an Internet connectivity solution must also be reliable and robust.

Connect One's iChip Internet Controller is designed to operate flawlessly in this difficult environment. It is an adaptable, updateable, firmware-based Internet connectivity solution that enables customers to use a wide range of Internet protocols in order to access the Internet. iChip is easy to design-in, use and maintain, and assures reliable, seamless Internet connectivity. Not only does it give customers a great deal of flexibility in accessing the Internet, but it also enables the customer to fine-tune the Internet connection. iChip has been operating reliably in hundreds of thousands of devices since 1999, and has been deployed in more than 50 countries with hundreds of ISPs, telephone networks, and wireless operators.

In this White Paper, we will review the various protocols that are used to access the Internet and we will explain how iChip implements the Internet protocols. We will also highlight some iChip features that optimize and fine-tune the Internet connection. We will show that iChip is an excellent long-term investment, because it offers much more than just TCP/IP connectivity.

White Paper

*A TCP/IP Primer:
The Internet Protocols and their
Implementation in Connect One's iChip*

Table of Contents

Executive Summary	2
Table of Contents	3
Introduction	4
The Internet and the World Wide Web	4
Problems of Internet Connectivity	6
The Internet Protocols	6
PPP (Point-to-Point Protocol)	7
IP (Internet Protocol)	7
TCP (Transmission Control Protocol)	8
UDP (User Datagram Protocol)	8
SMTP (Simple Mail Transport Protocol)	8
POP3 (Post Office Protocol 3)	9
MIME (Multipurpose Internet Mail Extensions)	9
HTTP (Hypertext Transfer Protocol)	9
FTP (File Transfer Protocol)	9
TELNET	10
Internet Security	10
The iChip Internet Controller	10
The AT+i Command Set	11
Implementation of the Internet Protocols in iChip	11
TCP/UDP Sockets	11
SerialNET Mode	11
Email Send (SMTP and MIME)	12
Email Retrieve	13
HTTP (Web) Server	13
HTTP (Web) Client	13
FTP Client	13
TELNET Client	14
SSL3 (Secure Sockets Layer Version 3.0)	14
Other Value-Added Features	14
Remote Firmware and Parameter Updates	14
Automatic IP Registration	15
Always Online and Automatic Reconnect Modes	15
Interlaced AT Commands	16
RAS Server	16
Status Reports and Result Codes	16
Miscellaneous Features	16
Summary of Key iChip Functions	17
About Connect One	19

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Introduction

The scope of this document is to present an overview of the Internet protocols and to explain their use in Connect One's iChip™ Internet Controller™ for messaging for M2M (machine-to-machine) applications. This document is not intended to be a tutorial. Separate "Theory of Operation" documents describe in detail the use of the various protocols. Readers can also refer to the AT+i Programmer's Manual at <http://www.connectone.com/html/support.htm> to learn about the specific commands and parameter settings for using the Internet protocols in iChip.

iChip is family of updateable Internet communication chips that mediate the connection between a host device and the Internet. iChip is a complete, firmware-based, hardware and software solution that includes basic and upper layer Internet protocols and many features that optimize communication over IP-enabled networks. iChip uses onboard flash memory to store the Internet protocols and device configuration parameters, which are independent of the host application and can be updated locally or remotely over the Internet. iChip also includes ample buffers to ensure that data is not lost when initiating or terminating Internet sessions.

The logical interface between iChip and a device's host processor is Connect One's AT+i™ Application Programming Interface. AT+i is a high-level command set that enables manufacturers with limited Internet programming resources to quickly and easily Internet-enable their devices by writing just a few commands in their application. A common user interface and command set enables iChip to access the Internet via dial-up modems, cellular modems, 10/100BaseT Ethernet LANs and 802.11b Wireless LANs. Support for new physical media, Internet protocols, and other commands can easily be added to the AT+i command set and downloaded to iChip's flash memory.

In this document we will learn about the various protocols used to gain access to the Internet and how Connect One implements them in the iChip Internet Controller.

The Internet and the World Wide Web

The most significant communication development in the second half of the 20th century is the Internet, which started out as a communication network for the US Department of Defense, and has evolved into the new global communication network. The Internet is a loosely organized, international collaboration of autonomous, interconnected networks that use TCP/IP as the protocol for host-to-host, peer-to-peer, and peer-to-host communication. To ensure interoperability, Internet connectivity requires conformity with Internet standards by hardware manufacturers, software developers, and Internet Service Providers (ISPs) who furnish Internet access.

The International Standards Organization created the Open Systems Interconnection Reference Model as a means to facilitate communication between two end users in a network. The model classifies communication protocols, applications and physical media into seven layers, built one on top of the other. It also helps in understanding networks and in developing products that can communicate with each other.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

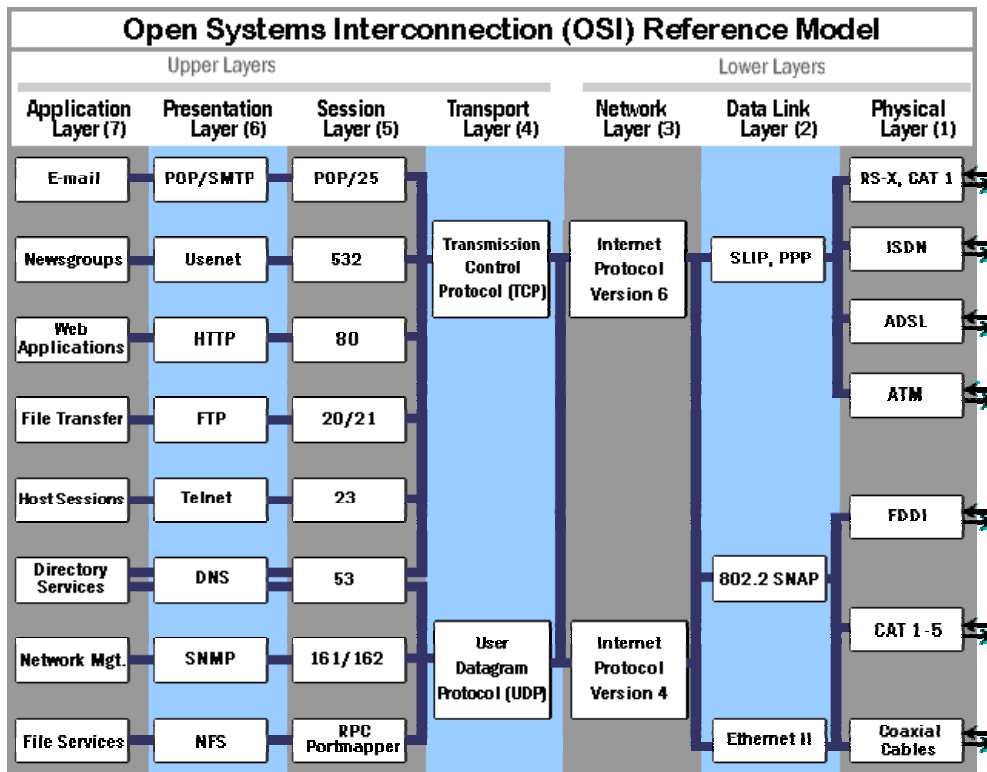


Figure 1: OSI Reference Model

The Internet offers many different methods to send and receive data, images, audio, video, and other files. The IETF (Internet Engineering Task Force) has created standards known as RFCs (Requests for Comment) that define ways of sending and receiving data over the Internet. For example, on the basic Transport Layer, a user can open TCP and UDP sockets between two points. On the Presentation Layer of the OSI Reference Model are “upper layer” protocols for transferring files, such as FTP; email protocols such as SMTP and POP3; Web protocols such as HTTP; and command protocols such as TELNET. Each protocol is advisable for certain applications.

The catalyst for the explosive growth of the Internet for personal and business applications was the introduction in the early 1990s of graphical, point-and-click network interfaces to access sites developed on the World Wide Web. Before the Web, personal computers had windowing and graphical capabilities, but networking applications (like email, FTP and TELNET) were still text-based. The rapid march of technology changed all that. Microprocessor computing power increased exponentially; operating systems became more powerful and user-friendly; and standard email programs, Web browsers and Web authoring tools were developed. Finally, the infrastructure of the “Internet Highway”—high-speed routers, switches and broadband “fat pipes”—was deployed on a massive scale worldwide during the high-tech boom at the end of the 1990s. The result is that the Internet has replaced many private communications networks. However, there are still many challenges to interoperability between devices and the Internet.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Problems of Internet Connectivity

Because the Internet is based on the use of open standards (as opposed to proprietary protocols), it offers the opportunity of a ubiquitous, low-cost, and accessible medium for communication. With TCP/IP as the basic communication protocol, any company can develop a product that can interoperate and “talk” with TCP/IP-enabled products developed by other companies.

Although there are standards for Internet connectivity, these standards are not implemented consistently from ISP to ISP, even from server to server. That is because (a) not all vendors support all the protocols required for Internet connectivity; and (b) the standards are evolving.

Here are just a few examples of everyday problems faced when using the Internet. On the most basic level, it is impossible to log onto an ISP if the remote device and the ISP do not support the same authentication methods used in the PPP protocol. If a deployed device cannot be remotely updated to support the new IP version 6 when it becomes more widely used, the device will have to be recalled or retrofitted in the field in order to upgrade from the current IP version 4. If the email protocol known as IMAP (Internet Message Access Protocol) successfully challenges the popular POP3 protocol for retrieving email, both the ISP and the device will have to provide support this protocol. If the ISP’s dial-up number or mail server addresses change, these new parameters must be programmed into the application. If more ISPs require secure authentication of the user’s email account before sending email, then devices will have to include support for secure SMTP authentication in the application. If the device’s TCP/IP stack doesn’t enable flexibility in determining timeouts, the device may frequently disconnect from the network.

The Internet Protocols

The Internet offers the possibility to choose from a wide range of communication protocols that are suited for various applications. The basic protocol suite is referred to as the TCP/IP stack, because Internet communication is based on the Transmission Control Protocol (TCP), which, in turn, is based on the Internet Protocol (IP) that operates over the PPP protocol. These protocols together are known as the TCP/IP stack in a software application.

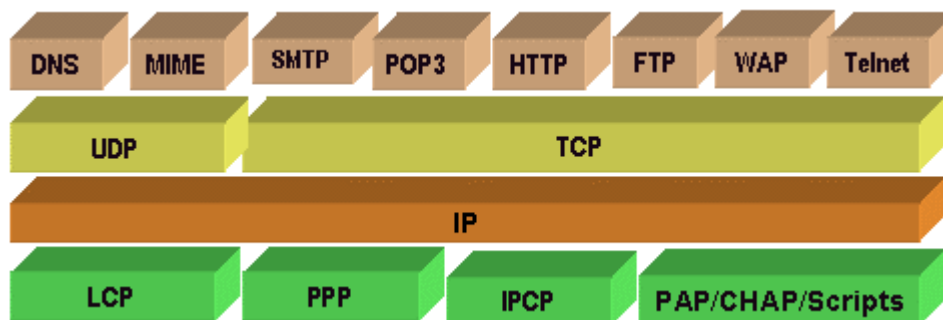


Figure 2: Internet Protocol stack for modem communication

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Following is a brief explanation of the key Internet communication protocols and how these protocols are used.

PPP (Point-to-Point Protocol)

PPP is a protocol for communication between two devices using a serial interface to connect by a modem to a server. PPP encapsulates a data message (in the form of TCP/IP packets) and forwards it to a remote server from where it will be routed over the Internet. PPP is a layered protocol, starting with a Link Control Protocol (LCP) for link establishment, configuration and testing. Once the LCP is initialized, a Network Control Protocol (NCP) is used to transport traffic for a particular protocol suite. The IP Control Protocol (IPCP) is an NCP that permits the transport of IP packets over a PPP link.

An Internet Server Provider provides a PPP connection so that its server can communicate with a device over the Internet using the Internet Protocol. In order to log onto the ISP and to access the Internet, PPP includes user account authentication. The most widely used authentication methods are the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP). Some PPP servers also support MS-CHAP (Microsoft CHAP) or scripts.

IP (Internet Protocol)

The Internet Protocol (IP) is the basic protocol used for all Internet-related communications. It is a “connectionless” protocol, meaning that there is no continuing connection between the end points that are communicating. Therefore it provides an unreliable method of delivering data from one host to another.

Data is packaged in a unit called a packet. Each packet is independent of any other packet of data. This means each packet must contain complete addressing information. Each sender and receiver of information (known as a host) on the Internet has an address known as an “IP address” that uniquely identifies it from all other hosts on the Internet. Each packet has an IP header that contains these addresses for identifying the sending and receiving hosts. Under IP version 4, which is in common use today, the IP address is a 32-bit number. Under IP version 6, which is slowly being introduced on a small scale, this is a 128-bit number. IP makes no attempt to determine if packets reach their destination or to take corrective action if they do not. IP only verifies successful transmission of the IP header, not the contents of a packet, and therefore is an unreliable delivery method.

IP provides all of the Internet’s data transport services, including addressing, fragmentation of IP packets, packet timeouts, and traffic prioritization. In order to function in a TCP/IP network, a network segment’s only requirement is to forward IP packets. Every other Internet protocol is ultimately either layered atop IP, or used to support IP from below.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Internet hosts use routers to select a path through the network to deliver packets, which include routing information in the IP header. The Internet uses a hop-by-hop routing model, which means that each host or router that handles a packet examines the Destination Address in the IP header, computes the next hop that will bring the packet one step closer to its destination, and delivers the packet to the next hop, until it reaches the Destination Address.

TCP (Transmission Control Protocol)

A message is divided into several packets that can be sent by different routes across the Internet and can arrive in a different sequence than they were sent. Each TCP peer must track its sequence numbering and the numbering used by the remote peer.

Because it is a connection-oriented protocol, the Transmission Control Protocol keeps track of the packet sequence in a message and puts the data back in the right order. TCP data is organized as a stream of bytes. TCP assures reliable data delivery by adding sequence numbers to coordinate which data has been transmitted and received. TCP will arrange for retransmission if it determines that data has been lost. TCP also provides flow control, manages data buffers, and coordinates traffic so that its buffers will not overflow.

TCP opens a connection to a port on a remote host computer, using the IP protocol to actually transfer the packets. Ports are numbers ranging from 0 to 65,000 that allow transmissions to be sent directly to a particular application that is “listening” to the specified port on a particular machine. Port numbers below 1024 are known as “well-known ports” and are reserved for predefined applications as assigned by the administrator of a machine. Typical ports are port 21 for listening by an FTP server, port 25 for sending email, and port 80 for a Web (HTTP) server. A port on a machine is usually specified by the IP address of the machine on which the port is active, followed by a colon, and the number of the port, such as 128.192.1.5:80.

UDP (User Datagram Protocol)

UDP is an alternative to TCP, but is a connectionless protocol that offers a limited amount of service. Like TCP, UDP uses the Internet Protocol to move a packet (also known as a datagram) from one computer to another. Also like TCP, but unlike IP, UDP does checksum its data, thus ensuring data integrity. Unlike TCP, however, UDP does not divide a message into packets, sequence and reassemble it at the other end. This means that packets may get lost before reaching their destination. The application must make sure that the entire message has arrived complete and in the right order. Network applications with very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. UDP is useful when TCP would be too complex or too slow.

SMTP (Simple Mail Transport Protocol)

SMTP is the Internet’s standard host-to-host mail transport protocol for email, which is ideal for non-time-sensitive applications, as it is an off-line medium. SMTP usually operates over TCP, port 25. SMTP uses TCP packets to transport its data from

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

the sending machine to the receiving machine. An SMTP conversation is carried on by two pieces of software running on two machines connected to the Internet. A new innovation is the use of secure SMTP servers, which requires authenticating the sender's user name and password. By 2005, International Data Corporation (IDC) forecasts that 11.5 billion emails will be sent each day on average in the US and 26.1 billion worldwide. This includes emails sent by individuals for business and personal purposes, but not mass emails sent to large lists. Data messaging is expected to add billions to these numbers.

POP3 (Post Office Protocol 3)

POP3 is the Internet standard for user-to-mailbox access. It is designed to manage checking, retrieving and deleting electronic mail from a mail server. Facilities are provided for user authentication.

MIME (Multipurpose Internet Mail Extensions)

MIME is used with SMTP and also is a non real-time protocol. It defines the standard representation for "complex" message bodies. A complex message body doesn't conform to the default of a single, human-readable, ASCII mail message. Examples of complex message bodies include messages with embedded graphics or audio clips, messages with file attachments, messages in foreign languages, or signed messages.

HTTP (Hypertext Transfer Protocol)

HTTP is the de facto standard for transferring documents on the World Wide Web and for building a Web site. Web pages usually are written in HTML (Hyper Text Markup Language), which is a way of constructing documents that reference other documents. Within a hypertext document, a block of text can be tagged as a hypertext link pointing to another document. When viewed with a hypertext browser like Internet Explorer or Netscape Communicator, the link can be activated to view the other document. HTTP operates over TCP, usually port 80.

Universal Resource Locators (URLs) are strings that name pages and specify how to access network resources, such as HTML documents. When viewed by a Web browser, every highlighted region on a Web page has an associated URL (hyperlink), that can be accessed when the hyperlink is activated by a mouse click.

Web sites are usually known by their domain name, such as www.connectone.com. The Internet uses the Domain Name System (DNS) is used to associate and convert domain names into IP addresses. This is a hierarchy of logical names called "domain names", used for remembering a host's domain name, instead of its IP address. A DNS server is used for this address conversion.

FTP (File Transfer Protocol)

FTP is earliest means of publishing information online. FTP was designed to let a user connect a remote system on which he had an account, authenticate himself using a user ID/password combination, then navigate a directory hierarchy and retrieve files. FTP uses separate command and data connections. The FTP protocol and the data

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

transfer use entirely separate TCP sessions. Data connections are initiated by the server from its port 20 to a port on the client identified in a PORT command. FTP servers listen on port 21.

TELNET

The TELNET protocol is designed for terminal-oriented remote login. TELNET allows a user at a remote computer to log on to another computer over a network and enter commands at a prompt as if they were directly connected to the remote computer. TELNET requires commands for specific functions.

Internet Security

A major drawback to widespread deployment of low-cost devices on the Internet is the concern about security. This is particularly true for medical applications and financial applications, such as electronic payment processing, which require encryption. Standards such as AES, SSL3 and IPSEC provide various levels of security, but may be costly and complicated to implement on an embedded device. As more devices start to use the Internet for communication, the demand will increase for low-cost, effective embedded encryption.

The iChip Internet Controller

iChip is a family of Internet controller chips that works with *any* host processor and *any* (or no) host operating system, and can be designed into a product within one month typically. As a communication coprocessor, iChip negotiates the connection between a host CPU and the Internet. iChip can access the Internet via any cellular or dial-up modem that uses standard AT commands, and via 10/100BaseT or 802.11b wireless LAN controllers. Connect One developed its own Internet protocol stack and RTOS to run the Internet protocols on iChip. The result is a robust, highly optimized, efficient, and portable TCP/IP communication controller that enables the user to fine-tune the Internet connection and ensure seamless connectivity.

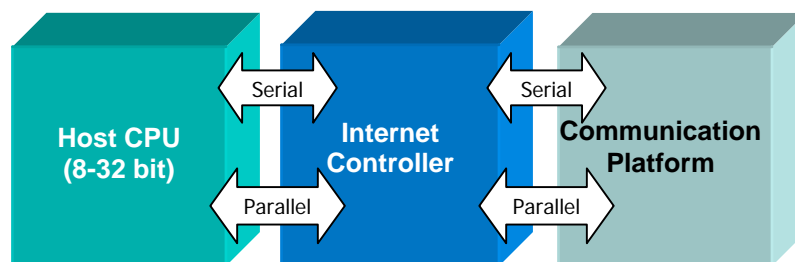


Figure 3: Internet Controller block diagram

iChip includes on-board, updateable flash memory that stores the protocols that are used for accessing the Internet, including PPP, IP, TCP, UDP, SMTP, POP3, MIME, HTTP, WAP, FTP and TELNET. In addition, iChip's flash memory stores the parameters that are required for configuring the host device to access the Internet. With the exception of CO110PC (whose firmware is locally updateable), the firmware in all iChips also is remotely updateable over the Internet.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

The AT+i Command Set

Connect One has defined a high-level Application Programming Interface (API), known as the AT+i™ command set, which is the logical interface between iChip and the host processor. Developed and pioneered by Connect One, this API enables an application to become IP-enabled with minimal or *no* modifications. AT commands written for existing applications transparently pass through iChip to the communication platform. Commands for accessing the Internet are written with the “AT+i” prefix in simple ASCII text, and instruct iChip to operate in Internet mode. The same AT+i command set is common to all iChips and communication platforms, so that once an application includes AT+i commands, it can work with any iChip with minimal or no changes. The AT+i command set is expandable, enabling Connect One to add new functionality, protocols, bug fixes, and customer requests, and to update the firmware on installed iChip-enabled devices.

Implementation of the Internet Protocols in iChip

Here is a description and explanation of how iChip implements the Internet protocols:

TCP/UDP Sockets

iChip includes commands to open and close, and send to and receive from, up to 10 simultaneous TCP or UDP sockets. In addition to 10 active sockets, iChip can open and close up to two simultaneous TCP listening sockets, enabling iChip to act as a server. When using the listening sockets, iChip can have up to 10 active sockets in backlog. iChip uses hardware interrupt and software mechanisms to inform the host of the status of a single active socket or a listen socket. iChip will dump and flush an active socket's buffer, and can check on the status of an open socket. iChip also will report how much data is being buffered and if sent data was not acknowledged.

iChip enables the user to fine-tune the TCP or UDP connection. For example, it is possible to control the maximum transfer unit (MTU) by limiting the size of outgoing PPP packets; to enforce flow control on TCP windows; to control the maximum segment size (MSS) of the packets to be received; to set the timeout to retransmit unacknowledged TCP packets; and to specify the local port for a TCP session.

Typical applications for TCP: remote control; data collection; financial transactions; home automation; accessing secure servers.

Typical applications for UDP: video monitoring; audio streaming; image transfer.

SerialNET Mode

A key feature of the AT+i protocol is a plug-and-play operating mode called SerialNET, which is perfect for retrofitting installed legacy devices with IP capability. When iChip enters this mode, *absolutely no modifications are required on the host application*. The benefit is that, in SerialNET mode, the host does not need to be AT+i aware. SerialNET is a two-way mode. The host processor can stream data to iChip, which packetizes it and sends it via TCP or UDP to a remote IP address.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Alternatively, data coming from a remote system over the Internet is de-packetized by iChip and streamed to the host.

In SerialNET mode, iChip routes a local asynchronous serial device across the Internet to a remote IP address and TCP or UDP port. iChip can function in SerialNET mode as a server or client. As a client, the iChip-enabled device initiates communications by sending service requests to a server. As a server, iChip responds to client requests. When a client device initiates communications in SerialNET mode, iChip establishes a network connection to a remote server before data flows between the two systems. When a remote client needs to access a device, the remote client contacts iChip and invokes SerialNET mode in order to create a communication flow to the local server device.

SerialNET mode is established by first defining all related parameters using AT+i commands, followed by a special AT+i command to enter SerialNET mode. Once in SerialNET mode, no additional AT+i commands may be sent, as the host serial link becomes a pipeline for streaming raw serial data to iChip. Data will continue to flow freely between the local and remote devices until a predefined activity occurs to terminate the remote connection.

Typical applications: Internet-enabling deployed vending machines, utility meters, security systems, Point-of-Sales (POS) terminals, programmable logic controllers (PLCs), and fleet management terminals.

Email Send (SMTP and MIME)

Each iChip can have its own unique email address or shared address. There is no limit on the number of emails that can be sent with iChip. It is also possible to send an unlimited number of emails with MIME binary attachments. There is no limit to the size of the binary attachment, which makes iChip excellent for audio, video, and large data files. The body of an email can contain up to 18 kB of text. Email can be sent to 50 addresses and to four CC addresses.

For security reasons, many Internet Service Providers now use SMTP servers that require authentication of the user account before enabling the user to send email. iChip's SMTP client has been enhanced to support SMTP servers that require clients to authenticate their user name and password before being granted service.

Typical applications for SMTP: Send daily sales transactions for POS terminals; fleet management assignments and reporting; remote status reporting; data collection.

Typical applications for MIME: Send firmware updates; large data files; audio files; maps; video clips; high-resolution photographs.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Email Retrieve

iChip will download emails from a POP3 mailbox upon command. All emails or specific emails can be downloaded, as well as a list of the email headers. Emails may remain or be deleted from the server after download.

Typical applications: Remote firmware updates; download data files for host system; receiving text and binary files.

HTTP (Web) Server

All iChips, except CO110PC (which does not include a Web server), contain two independent Web sites, both stored in iChip's non-volatile memory. One Web site is the iChip configuration site, which is bundled in iChip's firmware and is dedicated to iChip configuration and maintenance. This site supports remote iChip parameter configuration, iChip firmware upload, and application Web site upload.

The second site is the application Web site that allows system designers to build Web-based products for device application use. This Web site may include multiple linked HTML pages, links to external pages, images, graphics, and Java applets. The application site may also incorporate a WAP (Wireless Access Protocol) server that can be browsed by Internet-enabled cellular handsets or PDAs.

The application Web site can be created by standard Web authoring tools and uploaded to iChip via iChip's Web site packing tool inside the bundled Windows-based iChip Config utility. Application Web sites can be remotely monitored, configured, and managed via the Internet by up to three concurrent remote Web browsers with MD-5 password-encrypted access authentication.

Typical applications: link information to a page in a Web site; firmware downloads; remote control and monitoring; graphical display of location, data or status.

HTTP (Web) Client

iChip supports retrieval of HTML pages and data files from standard Web servers with its HTTP client protocol.

FTP Client

In addition to basic commands such as opening and closing an FTP socket to a remote FTP server, and sending or retrieving a file, iChip includes a rich set of commands for FTP, including: retrieval of the remote FTP server's file directory listing and name list; the ability to create a directory on the remote server; the ability to change the server's current directory; and opening, closing, appending or deleting a file on the remote server.

Typical applications: real-time transfer of large files; firmware download; data collection; medical imaging.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

TELNET Client

iChip offers the ability to open and close a TELNET session, to send a line or a data stream, to flush the socket's outbound data, and to receive data. iChip also supports TELNET binary send.

Typical applications: accessing legacy systems that use TELNET.

SSL3 (Secure Sockets Layer Version 3.0)

Two iChip models (CO210AG and CO710AG) will implement an SSL3 client socket-layer in Q1, 2005, starting with FTP and followed by other protocols later in 2005. iChip will support a connection to an SSL3 server socket and allow transfer of encrypted data over the socket. The iChip implementation will include support for a subset of the cipher suites in SSL3. It will use RSA to encrypt the Public-Key exchange process, MD-5 or SHA1 for calculating Message Digests, and 3DES, AES, or ARC4 for data encryption. Initially iChip will accept only a single certificate (X.509 self-signed certificate or a single-level certificate chain) from the server. Future implementations may add support for multiple certificate chains.

Other Value-Added Features

iChip includes many features designed especially to optimize Internet connectivity. These features have been added as a result of experience gathered from customers who have deployed hundreds of thousands of iChip-enabled units.

Remote Firmware and Parameter Updates

In addition to local firmware and configuration parameter updates using the YMODEM protocol via a local serial port or a dial-up modem, both email and the Web can be used to remotely update iChip's firmware and configuration parameters.

iChip's remote firmware update methodologies are especially handy for a large installed base. iChip firmware can be uploaded using a standard Web browser through the internal configuration Web site. This is convenient when iChip is online and its IP address is known. The iChip configuration site includes an authentication form that automatically pops up on the remote browser when parameter updates are attempted. Remote iChip parameter updates are password-protected using MD-5 encryption.

Firmware updates can also be sent as an email attachment, which is downloaded by the iChip through a POP3 session. iChip's bootblock includes a boot loader that facilitates a safe download mode. In this mode, iChip automatically recognizes a firmware update email and replaces its existing firmware with a new version. iChip can execute an email retrieve session that will download only a firmware update attachment, skipping other email messages. This methodology allows external events governed by the host to determine when and if to proceed with a firmware update. These events may be a time-schedule, a keystroke sequence applied to the host system, a message sent to the host via email or through a dedicated TCP socket, etc.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

It is possible to set up a dedicated mailbox for firmware updates. iChip can scan the update mailbox when responding to an initiated remote firmware update command. This methodology is especially useful when setting up a common firmware update mail account, to be shared by many devices with iChips. In addition, groups may be formed to access different update mailbox accounts. iChip controllers may each have their own mail account. A central management headquarters can issue the firmware attachment once to the dedicated mailbox, rather than sending individual mail attachments to each unit's mailbox. This also relieves the requirement to maintain a database of mailboxes used by the devices.

Automatic IP Registration

When iChip goes online in a modem environment, it is normally assigned a dynamic IP address during PPP negotiation. Because a different IP address is usually assigned every session, it is not practical to use iChip as a server, since clients do not know what IP address to use. Furthermore, under these restrictions, there is no practical way to know if a specific system is online or offline. To overcome this problem, iChip incorporates built-in procedures designed to register its IP address on a server system each time it goes online.

iChip can be instructed to go online automatically, create a PPP connection, register its IP address, and stay online. Once registered, client systems may interrogate the servers in order to verify the online status of a specific system and retrieve its currently assigned IP address. iChip can register itself by (a) sending an email, (b) opening a socket to a registration server, and (c) by submitting an entry to the URL of a registration Web server. This feature saves the customer the cost of buying a fixed IP address. iChip automatically reports its host name, port number and currently-assigned IP address to the registration page.

Once registered, client systems may interrogate the servers in order to verify the online status of a specific system and retrieve its currently assigned IP address. The IP registration process is governed by several AT+i parameters. Once these parameters are configured, iChip will register its IP address when it goes online.

Always Online and Automatic Reconnect Modes

iChip includes a "connectivity watchdog" that monitors the network connection in case it is lost. It also regularly pings a remote device to verify Internet connectivity. In the event that iChip goes offline or is disconnected by the service provider, it will constantly attempt to go online again. When in this mode, iChip immediately goes online after a power-up cycle and evokes the IP registration process (if configured to do so). iChip will not close any open Internet sessions (FTP or TELNET session, for example), nor release the handle of the active TCP sockets. This gives the host a chance to read the session errors and to get buffered incoming data from active TCP sockets. If listening sockets were active, iChip will restore them with the new IP address. After going online, iChip's Web server can be configured to activate automatically.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Interlaced AT Commands

AT commands can be sent to a modem during an Internet session. This is important if the modem is transmitting or receiving data via GPRS and new commands (such as SMS AT commands) must be sent. If this command is issued while iChip during an Internet session, iChip will put the modem into command mode. After the AT command is sent, iChip will wait for the modem reply and then restore online mode.

RAS Server

iChip features an internal RAS server, which makes it possible to dial into a device that has a modem. This feature allows a remote dialer to dial into iChip, which, when configured as a RAS (Remote Access Server), will answer the call and negotiate a PPP connection. iChip's RAS will acknowledge an IP address request from the remote dialer side and will acknowledge receipt of a default IP address. Since iChip is not connected to an actual ISP in this mode, iChip does not have access to the public Internet and thus only direct connections between the iChip and the connected PPP client will be possible.

After a RAS PPP connection is established, iChip can automatically open sockets to stream data to iChip or activate the internal Web server so that a remote client may browse iChip's Web or WAP site. All other iChip IP protocol functionality also will be enabled, allowing the host to issue Internet protocol AT+i commands via PPP.

Status Reports and Result Codes

iChip provides a wealth of information on the status of the Internet connection and setup parameters. These reports facilitate troubleshooting and informing current configuration status.

Miscellaneous Features

iChip includes many value-added features that fine-tune the Internet connection and ensure flexible and reliable Internet connectivity, including:

- ***Ring response server.*** This connects two devices that have dynamic IP addresses. This enables an iChip to wake-up upon receiving a call, dial a predetermined access number, and to register its IP address.
- ***Hardware and software flow control*** for the host-to-iChip and iChip-to-modem connection. This ensures that data is not lost during a session.
- ***Pinging a remote server.*** This is important for assuring an always-online connection and to know if a remote IP address is active. iChip has an adjustable Ping timeout.
- ***Setting the network time.*** This is important for stamping time and date on outgoing emails and for scheduling according to the correct time of day. iChip can retrieve the time of day from a network time server, and set the Greenwich Mean Time (GMT) offset for local time and daylight savings time (DST).
- ***Setting the number of ISP dialing retries.*** In case of an unsuccessful connection attempt, iChip will redial the ISP at a predetermined number of times with a predetermined time interval between each attempt.

White Paper

*iChip and the Internet Protocols:
Much More than Just TCP/IP*

Summary of Key iChip Functions

Following are some of the many iChip functions that enable flexible and reliable connectivity to IP networks. Complete information on these features can be read in the AT+i Programmer's Manual at www.connectone.com/html/manuals.asp.

Function	Benefit
TCP/UDP Sockets	Ten simultaneous active TCP or UDP sockets enable many concurrent tasks.
Listening Sockets	Two simultaneous TCP listening sockets enable iChip to act as a server. Up to 10 active sockets in backlog.
SerialNET Mode	Plug-and-play mode for IP-enabling any RS232 device without modifying the host application or hardware.
Textual Email Send	Send standard ASCII text emails.
Binary Email Send	Send standard MIME-encoded attachments. No limit on number or size of binary attachments.
Email Receive	Retrieve entire message with or without headers, leave message on server or delete from server.
Web Server ¹	Includes two internal Web sites: one used by the application and one to configure and update iChip firmware. Web/WAP sites can be created by standard Web authoring tools, and can be uploaded to iChip via iChip's Web site packing tool. Web sites are password-protected by MD-5 encryption.
RAS Server	Dialing into iChip enables remote client to connect over PPP, browse iChip's Web site and open sockets to exchange data with iChip.
FTP Client	Enables transfer of large files and accessing/modifying directories and files on remote FTP servers.
TELNET Client	Open a TELNET session, send a line or a data stream, flush the socket's outbound data, or receive data.
Remote Firmware and Parameter Updates ¹	Use sockets, email or the Web to update firmware and parameter settings. Remote iChip parameter updates are password-protected using MD-5 encryption.
Dialer Scheduling	Schedule the number of redial attempts and time interval between each attempt.
Status Reporting	iChip provides detailed status reports.
PING	Assures the "always-online" connection and informs whether a remote device is online.
Hardware and Software Flow Control	Balances data flow over host-to-iChip and iChip-to-modem connections.
Ring Response Server	Enables iChip with a dynamic IP address to wake-up upon receiving a call and to dial a predetermined access number and to notify its IP address.
Network Time	Gets network time from standard time servers. Important for stamping time and day on outgoing emails, for scheduling according to the correct time of day, and for synchronizing host clocks across the Internet.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

Function	Benefit
Automatic IP Registration	Overcomes the problem of dynamic IP addresses. When going online, iChip automatically reports its host name, port number and dynamic IP address to a socket server, mailbox or Web registration page. Once registered, clients may query the servers in order to retrieve iChip's current IP address.
Always On-line Mode	iChip includes a "connectivity watchdog" that monitors the cellular network connection and automatically reconnects if necessary.
Automatic Reconnect	In case of a lost carrier, iChip establishes a new PPP link. iChip immediately goes online after a power-up cycle and can register its IP address. After going online, iChip's Web server can be configured to activate automatically.
Interlaced AT Commands	AT commands can be sent to the modem during an Internet session, without interrupting the session. iChip will wait for the modem to reply before restoring online mode.
Remote AT+i Commands	Send AT+i commands to an iChip from a remote device across the Internet. Enables remote configuration.

Note 1: Available on all chips except CO110PC.

White Paper

iChip and the Internet Protocols: Much More than Just TCP/IP

About Connect One

Connect One was established in 1996 with the goal of simplifying the task of connecting non-PC devices to the Internet. To implement this vision, Connect One includes a team of experts in embedded systems, networking, Internet connectivity and data communications protocols, whose expertise is in interfacing data communication protocols with Internet protocols. By enabling devices to tap into the Internet's ubiquitous global infrastructure, Connect One makes it possible for manufacturers, system integrators, wireless operators, and end-users to eliminate the time, cost and complexity of connecting their devices to the Internet.

Unlike other companies in the embedded Internet sphere, Connect One's IP expertise derives having spent almost all of its initial four years in development of an Internet fax appliance. Connect One understands the complexity of connecting a device to a myriad of Internet Server Providers, wireless operators, and telephone systems worldwide. The company has applied this knowledge on the system and embedded level, embodied in the most robust, flexible and economical Internet chips and plug-and-play, stand-alone products available today.

Connect One's products have been designed into products that usually have limited internal resources (e.g. processing power and memory). Typical products include point-of-sales (POS) terminals, fleet management terminals, fax machines, security systems, medical devices, data loggers, programmable logic controllers, HVAC systems, environmental monitors, vending machines, and utility meters.

Connect One's technology provides these and other devices with a wide range of benefits, such as remote diagnostics, maintenance, firmware downloads, data collection, remote monitoring and management. The benefit to manufacturers and consumers is that products that are Internet-enabled offer enhanced functionality, longer product lives, reduced infrastructure, and lower operating costs.

The company's products are distributed worldwide by leading distributors of electronic components and wireless modems. Connect One is privately owned, with offices in Phoenix, AZ and Kfar Saba, Israel. For further information, please visit the company's Web site at <http://www.connectone.com> or send an email to info@connectone.com. iChip, Internet Controller, AT+i, SerialNET, iConnector, Instant Internet, and Connect One are trademarks of Connect One Ltd.