Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.172 – 177

RESEARCH ARTICLE

Lightweight IP - The Network Protocol Its Features and Applications

Akshay Arunpant Nakade
Student of Master of Engineering in CSE
HVPM's College of Engineering and Technology
Amravati, India
aksnakade@gmail.com

Abstract:

With the advancement in the networking, a communications protocol or network protocol is the specification of a set of rules for a particular type of communication. In modern protocol design, protocols are "layered". Layering is a design principle which divides the protocol design into a number of smaller parts, each of which accomplishes a particular sub-task, and interacts with the other parts of the protocol only in a small number of well-defined ways. The dynamic nature of the Internet and the diversity of its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable. In this paper we are covering light weight Internet Protocol (lwIP) which is a widely used open source TCP/IP stack. Further we see the features of the lwIP and its applications. Most of its applications are designed for embedded systems.

Keywords: **lwIP, Datagram, Link-Local address, Berkeley sockets, Ethernet**

I. Introduction

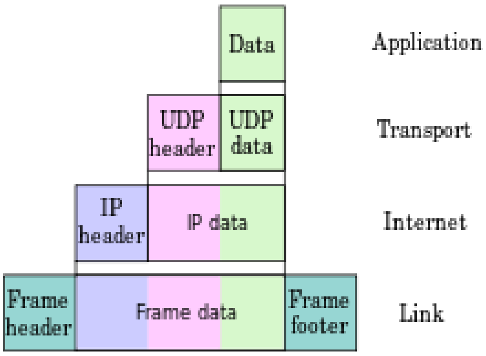
In the networking, a communications protocol or network protocol is the specification of a set of rules for a particular type of communication. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together are known as a protocol suite; when implemented in software they are a protocol stack. The terms are often intermingled; people may use the term "protocol" to refer to a software implementation, or use "protocol stack" to refer to the specification. Most recent protocols are assigned by the IETF for Internet communications, and the IEEE, or the ISO organizations for other types. The ITU-T handles telecommunications protocols and formats for the PSTN. As the PSTN and Internet converge, the two sets of standards are also being driven towards convergence.

lwIP (*lightweight IP*) is a widely used open source TCP/IP stack designed for embedded systems. lwIP was originally developed by Adam Dunkels at the Swedish Institute of Computer Science and is now developed and maintained by a worldwide network of developers.

The design of the Internet protocols is based on the end-to-end principle. The network infrastructure is considered inherently unreliable at any single network element or transmission medium and assumes that it is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the state of the network. For the benefit of reducing network complexity, the intelligence in the network is purposely mostly located in the end nodes of data transmission. Routers in the transmission path forward packets to the next known, directly reachable gateway matching the routing prefix for the destination address.

The focus of the lwIP TCP/IP implementation is to reduce resource usage while still having a full-scale TCP. [3] This makes lwIP suitable for use in embedded systems with tens of kilobytes of free RAM and room for around 40 kilobytes of code ROM. The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: identifying hosts; and providing a logical location service.

Datagram construction



Sample encapsulation of application data from UDP to a Link protocol frame

Each datagram has two components: a header and a payload. The IP header is tagged with the source IP address, the destination IP address, and other meta-data needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation.

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into networks and sub-networks, involving the designation of network or routing prefixes. IP routing is performed by all hosts, but most importantly by routers, which transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network.
IP routing is also common in local networks. For example, many Ethernet switches support IP multicast operations. [1] These switches use IP addresses and Internet Group Management Protocol to control multicast routing but use MAC addresses for the actual routing.

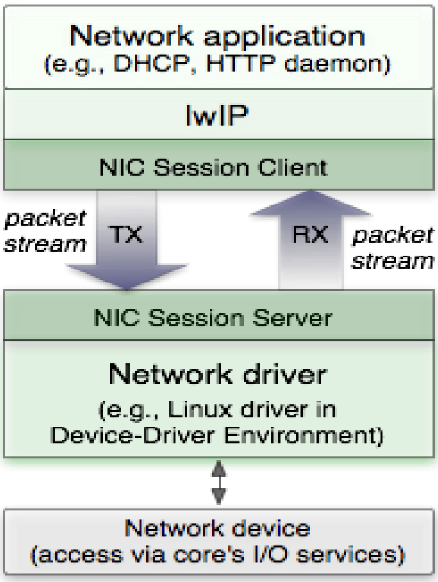


Fig. LwIP implementation in network layers

LwIP is used by many manufacturers of embedded systems. Examples include Altera (in the Nios II operating system), Analog Devices (for the Blackfin DSP chip), Xilinx, [2] Honeywell (for some of their FAA certified avionics systems) and Freescale Semiconductor (Ethernet Streaming SW for Automotive microcontrollers). And many other applications we will see latter in this paper.

II. LWIP Features

A. Features supported at layer format

Internet layer

- IP (Internet Protocol) including packet forwarding over multiple network interfaces
- ICMP (Internet Control Message Protocol) for network maintenance and debugging
- IGMP (Internet Group Management Protocol) for multicast traffic management

Transport layer

- UDP (User Datagram Protocol) including experimental UDP-lite extensions
- TCP (Transmission Control Protocol) with congestion control, RTT estimation and fast recovery/fast retransmit

Application layer

- DNS (Domain names resolver)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Configuration Protocol)

Link layer

- PPP (Point-to-Point Protocol)
- ARP (Address Resolution Protocol) for Ethernet

B. Implementation Features

1) Link-Local Address :

In a computer network, a link-local address is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to. Link-local addresses are usually not guaranteed to be unique beyond a single network segment. Routers therefore do not forward packets with link-local addresses.

For protocols that have only link-local addresses, such as Ethernet, hardware addresses that the manufacturer delivers in network circuits are unique, consisting of a vendor identification and a serial identifier. Link-local addresses for IPv4 are defined in the address block 169.254.0.0/16, in CIDR notation. In IPv6, they are assigned with the fe80::/10 prefix [4].

- Address assignment

Link-local addresses may be assigned manually by an administrator or by automatic operating system procedures. For Internet Protocol (IP) networks, they are assigned most often using stateless address auto-configuration. In IPv4, [5] they are normally only used to assign IP addresses to network interfaces when no external, stateful mechanism of address configuration exists, such as the Dynamic Host Configuration Protocol (DHCP), or when another primary configuration method has failed. In IPv6, [6] link-local addresses are mandatory and required for the internal functioning of various protocol components. Automatic address configuration of link-local addresses is often non-deterministic as the resulting address cannot be predicted. However, in IPv6 it is usually derived automatically from the interface media access control (MAC) address in a rule-based method.

- IPv4

In RFC 3927, the Internet Engineering Task Force has reserved the address block 169.254.0.1 through 169.254.255.254, for link-local addressing in Internet Protocol Version 4. Link-local addresses are assigned to interfaces by host-internal, i.e. stateless, address auto-configuration when other means of address assignment are not available. [5] RFC 3927 warns against the simultaneous use of IPv4 addresses of different scope, such as configuring link-local addresses as well as globally routable addresses on the same interface. Therefore, hosts search for a DHCP server on the network before assigning link-local addresses.

In the automatic address configuration process, network hosts select a random candidate address within the reserved range. This uses Address Resolution Protocol (ARP) probes to ascertain that the address is not in use on the network. If a reply is received to the ARP, it indicates the candidate IP address is already in use; a new random candidate IP address is then created and the process repeated. The process ends when there is no reply to the ARP, indicating the candidate IP address is available.

When a globally routable or a private address becomes available after a link-local address has been assigned, the use of the new address should generally be preferred to the link-local address for new connections but communication via the link-local address is still possible. Microsoft refers to this address auto-configuration method as Automatic Private IP Addressing (APIPA). [7] It is sometimes also casually referred to as auto-IP. Which is also somehow possible by LWIP implementation.

- IPv6

In the Internet Protocol Version 6 (IPv6), the address block fe80::/10 has been reserved for link-local unicast addressing. [6] The actual link local addresses are assigned with the prefix fe80::/64.[8] They may be assigned by automatic (stateless) or stateful (e.g. manual) mechanisms. Unlike IPv4, IPv6 requires a link-local address to be assigned to every network interface on which the IPv6 protocol is enabled, even when one or more routable addresses are also assigned. [9] Consequently, IPv6 hosts usually have more than one IPv6 address assigned to each of their IPv6-enabled network interfaces. The link-local address is required for IPv6 sub-layer operations of the Neighbor Discovery Protocol, as well as for some other IPv6-based protocols, like DHCPv6.

In IPv6, stateless address autoconfiguration is performed as a component of the Neighbor Discovery Protocol (NDP), [10] as specified in RFC 4862. The address is formed from its routing prefix and the MAC address of the interface.IPv6 introduced additional means of assigning addresses to host interfaces. Through NDP routing prefix advertisements, a router or a dedicated server host may announce configuration information to all link-attached interfaces which causes additional IP address assignment on the receiving interfaces for local or global routing purposes. This process is sometimes also considered stateless, as the prefix server does not receive or log any individual assignments to hosts. Uniqueness is guaranteed automatically by the address selection methodology in combination with the duplicate address detection algorithm.

- Media access control

Media access control (MAC) addresses used in local broadcast networks, such as Ethernet, are link-local addresses. Such devices are configured with an address in hardware by the manufacturer. However, operating system utilities, such as ifconfig may be used to assign or change these addresses. This is essential when an operating system is running in a virtual machine environment.

2) Berkeley-like socket API :

All modern operating systems now have some implementation of the Berkeley socket interface, as it became the standard interface for connecting to the Internet. Even the Winsock implementation for MS Windows, developed by unaffiliated developers, closely follows the Berkeley standard. [11]

Berkeley sockets (or **BSD sockets**) is a computing library with an application programming interface (API) for internet sockets and Unix domain sockets, used for inter-process communication (IPC). As the API has evolved with little modification from a *de facto* standard into part of the POSIX specification. **POSIX sockets** are basically Berkeley sockets. [12]

This list is a summary of functions or methods provided by the Berkeley sockets API library mainly used for Networking :

- Socket () creates a new socket of a certain socket type, identified by an integer number, and allocates system resources to it.
- Bind () is typically used on the server side, and associates a socket with a socket address structure, i.e. a specified local port number and IP address.
- Listen () is used on the server side, and causes a bound TCP socket to enter listening state.
- Connect () is used on the client side, and assigns a free local port number to a socket. In case of a TCP socket, it causes an attempt to establish a new TCP connection.

- Accept () is used on the server side. It accepts a received incoming attempt to create a new TCP connection from the remote client, and creates a new socket associated with the socket address pair of this connection.
- Send () and recv (), or write () and read (), or sendto () and recvfrom(), are used for sending and receiving data to/from a remote socket.
- Close () causes the system to release resources allocated to a socket. In case of TCP, the connection is terminated.
- Gethostbyname () and gethostbyaddr () are used to resolve host names and addresses. IPv4 only.
- select() is used to spend, waiting for one or more of a provided list of sockets to be ready to read, ready to write, or that have errors.
- Poll () is used to check on the state of a socket in a set of sockets. The set can be tested to see if any socket can be written to, read from or if an error occurred.
- Getsockopt () is used to retrieve the current value of a particular socket option for the specified socket.
- Setsockopt () is used to set a particular socket option for the specified socket.

III. Applications of lightweight (LwIP) protocol

A. Embedded Ethernet

With the development of embedded technology, embedded system in industrial control applications more and more widely, and the embedded Ethernet technology is particularly important, LwIPprotocol stack, Ethernet in low-end embedded system applications may be provided, STM32 interconnected ARM processor and its official software for Embedded Ethernet application development offerred convenience condition. By Embedded Ethernet mainly introduces the LwIP in hardware platform applications. [13]

B. Embedded sensors network

The embedded sensor network has to evaluate the performance of the lightweight TCP/IP protocol stack using the digital signal processor. The applications of such embedded system are in sensor networking, voice over IP (VoIP) communications and process control in industrial environments. The performance of LwIP stack has been evaluated using the evaluation board EZ-KIT. The LwIP stack has good performance and applications, comparable with the TCP/IP stack implementation in operating systems like Linux or Windows. Furthermore, a framework for developing embedded networking applications is provided. [14]

C. Smart home design

This work is based on the Internet of Things and ZigBee wireless sensor network technology. A kind of smart home design based on ZigBee wireless sensor network was proposed mainly for this. Texas Instruments MCU device LM3S9B96, which is the ARM Cortex-M3 based controllers, was used in this system. The entire system is running on the μC/OS-II embedded real-time multitasking operating system. Users can access this system by a dynamic webpage of LwIP TCP/IP protocol stack or GSM SMS. Using these system users can conveniently know the environment parameters of home, such as temperature, humidity, meter readings, light, and control the home electronic equipments, such as light, air condition, heater, by ZigBee wireless sensor network. [15]

D. The Porting and Implementation for Embedded Web Server

The development trend of embedded technology need the web/server technology applies into embedded fields and provides a flexible remote device monitoring and management function based on Internet browser. But, due to the limitation of hardware resource and the low-efficiency of general purpose TCP/IP protocol stacks and protocol models, it is quite difficult to implement full TCP/IP protocol into embedded system when accessing to Internet. [16] The paper analyses the Light-Weight TCP/IP and gives the detailed processing of every layer first, then designed the hardware platform and the software platform with muC/OS- II, porting the LwIP based on them. A thin server is designed based on LwIP, and the state transform of client and server when they were communicating was analyzed. At last, the EWS was tested on the Production of Storage Battery Control System, the result indicated the EWS can long-distance monitor the devices real-timely and perfectly.

IV. Conclusion

In inter-networking, a communications protocol or network protocol is the specification of a set of rules for a particular type of communication. Multiple protocols often describe different aspects of a single communication Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. Layering also permits familiar protocols to be adapted to unusual circumstances. For example, the mail protocol above can be adapted to send messages to aircraft. As we see the lwIP support all the layering features, hence it is simple. So, by using this we can develop reliable, cheaper and simple protocol stack.

References

[1] "Building Complex VDK/LwIP Applications Using Blackfin Processors ", Kaushal Sanghai, Analog Devices Inc. September 2008

[2] Siva Velusamy, LightWeight IP (lwIP) Application Examples, Xilinx Inc. June 2009

[3] Yanwen Wu (2010). *Software engineering and knowledge engineering : theory and practice*. Berlin: Springer. p. 639. ISBN 978-3-642-03717-7.

[4] http://tools.ietf.org/html/rfc4291#section-2.5.6

[5] *a b* RFC 3927, *Dynamic Configuration of IPv4 Link-Local Addresses*, S. Cheshire, B. Aboba, E. Guttman, The Internet Society (May 2005)

[6] *a b* RFC 4291,*IP Version 6 Addressing Architecture*, R. Hinden, S. Deering, The Internet Society (February 2006)

[7] "APIPA". Microsoft. Retrieved 2010-08-02.

[8] RFC 4291, section 2.5.6. *Link-Local IPv6 Unicast Addresses*

[9]RFC 4291, section 2.8. *A Node's Required Addresses*

[10] RFC 4862, *IPv6 Stateless Address Autoconfiguration*, S. Thompson, T. Narten, T. Jinmei (September 2007)

[11] *UNIX Network Programming* Volume 1, Third Edition: The Sockets Networking API, W. Richard Stevens, Bill Fenner, Andrew M. Rudoff, Addison Wesley, 2003.

[12] "— POSIX.1-2008 specification". Opengroup.org. Retrieved 2012-07-26.

[13] Electrical and Control Engineering (ICECE), 2011 International Conference on

[14] Communications (COMM), 2012 9th International Conference on

[15] Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on

[16] Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference