

INTEGRITY



IPLITE

Ultra Compact IPv4/IPv6 Protocol Stack

IPLITE Overview

IPv6 support will be a requirement when the next generation of embedded devices enters the Internet. To meet this demand, Interpeak now introduces IPLITE, an ultra compact IPv4/IPv6 protocol stack, designed for minimum footprint and maximum performance.

In the next few years, billions of embedded devices are expected to enter the Internet. However, there is already an address shortage with just some hundreds of millions of human users. This means that the new IPv6 standard—the next generation Internet protocol—will be necessary for embedded systems.

Many embedded devices have limited resources in terms of memory and CPU power. Available networking solutions are simply too large and slow for such devices. In order to address these needs, Interpeak has developed IPLITE, the first extremely compact IPv6 implementation for resource constrained embedded devices.

Interpeak has used the experience from IPNET—the full featured IPv6 stack for embedded systems—to write a small, robust stack which is yet surprisingly powerful. With a footprint of only some 30 kBytes for a small IPv6 version, it can be used in just about every embedded device.

- IPv4
- IPv6
- IPSec*
- UDP
- TCP*
- PPP*
- ARP
- Ethernet
- ICMP
- ICMPv6/NDP

Supported protocols in IPLITE. An asterisk denotes that support for this protocol is available in an optional module.

Dual IPv4/IPv6 Stack

For several years to come, IPv4 and IPv6 systems will exist simultaneously. Many embedded applications must therefore be able to communicate with both types of nodes. IPLITE can handle both IPv4 and IPv6 traffic at the same time. It can be configured for IPv6 only, or for IPv4 only or for dual IPv4/IPv6 use.

Modular Design

The modular design of IPLITE permits the user to tailor it to the needs of the application, thus providing the smallest possible size. Hence, the PPP, TCP and IPSec protocols are provided as optional modules.

Interpeak will continuously add new modules to the IPLITE suite, with a roadmap that includes a number of interesting protocols such as ROHC, Multilink PPP and SCTP.

Applications

Interpeak has implemented a large number of security and networking applications like SSH, SSL, IKE, L2TP, RADIUS, PPPoE, RIP, SNMP, Telnet, FTP, TFTP, DHCP, HTTP, DNS, LDAP etc. For additional information about these networking applications, please visit www.interpeak.se/products.

The products are optimized for IPLITE and run out-of-the-box, allowing for rapid development of advanced networking equipment.

Footprint Optimizations

In order to achieve the smallest possible footprint, some features that are rarely used in minimal embedded systems are removed. Examples of these are support for multiple interfaces, routing and packet forwarding, jumbo-grams, etc. Networking applications that require more functionality will find a better match in IPNET—the full-featured dual IPv4/v6 stack.

Very High Performance

IPLITE has been designed specifically for high performance. Its zero-copy interface allows the highest possible bandwidth for performance critical applications. IPLITE is also particularly well suited to DSP applications with optimizations tailored to DSP designs.

- Raw IP/UDP/TCP BSD sockets
- Zero-copy API based on BSD sockets
- Dynamic configuration interface
- Link Layer Interface, enables additional link layer types, e.g. IEEE 802.11, ATM, etc.
- Driver Interface, using the RTOS BSP drivers

Supported APIs

IPLITE Architecture

Socket API

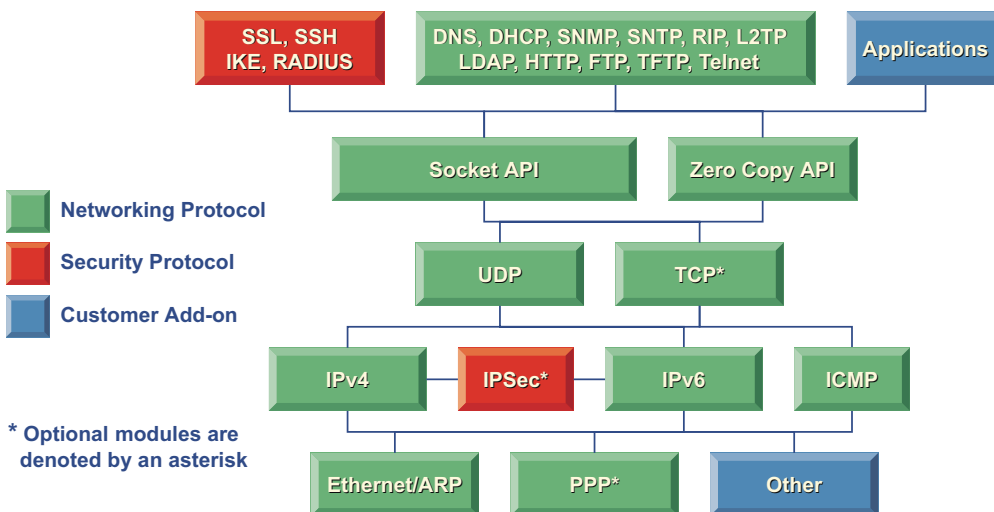
In addition to the proprietary zero-copy API, IPLITE has a subset of the familiar, easy-to-use BSD socket API, comprising the functions most commonly used in embedded devices. Even the BSD API is optimized for high performance, with only one data copy for incoming and outgoing packets.

Available on Many Platforms

Interpeak IPLITE is closely integrated with several major real-time operating

systems, utilizing the same network drivers and board support packages as the RTOS. This makes IPLITE readily available on all platforms and devices supported by the RTOS.

Since IPLITE only requires a minimum of operating system services, it may also be used when a commercial RTOS is not available. IPLITE can thus operate in combination with a proprietary RTOS, and other types of basic control software such as schedulers, monitors etc.



The architecture of IPLITE and additional Interpeak networking products. Due to its modular design, it is easy to customize IPLITE to a specific application by removing unused protocols and features.

IPv6 Protocol Features

Around year 1992, the Internet Engineering Task Force (IETF) became aware of shortage of IPv4 addresses in the world, and technical obstacles in deploying new protocols due to limitation imposed by IPv4. IPng (IP next generation) effort was started to solve these issues. After large amount of discussions, around year 1995, IPv6 (IP version 6) was picked as the final IPng proposal.

Larger IP Address Space

IPv4 uses only 32 bits for IP address space, which allows only 4 billion nodes to be identified on the Internet. 4 billion may look like a large number, however, it is less than the human population on the earth. IPv6 allows 128 bits for IP address space, allowing three hundred forty undecillion nodes to be uniquely identified on the Internet. Larger address space allows true end to end communication, without NAT or other short term workaround against IPv4 address shortage.

Deploy New Technologies

After IPv4 was specified 20 years ago, we have seen a plethora of technical improvements in networking. IPv6 covers a number of those improvements in its base specification, allowing users to assume these features available everywhere, anytime.

Autoconfiguration

With IPv4, DHCP has been available, but only as an option. The novice user can go into trouble when visiting an offsite without DHCP server. With IPv6, the stateless host autoconfiguration mechanism is mandatory.

Security

With IPv4, IPSec is optional and you need to ask the peer if it supports IPSec or not. With IPv6, IPSec support is mandatory. By mandating IPSec, you can secure your IP communication whenever talking to IPv6 devices.

Multicast

Multicast is mandatory in IPv6, which was optional in IPv4. IPv6 base specifications also extensively use multicast.

Ad-Hoc Networking

Scoped addresses allow better support for ad-hoc or *zeroconf* networking configuration. IPv6 supports anycast addresses, which can also contribute to service discoveries.

Protocol Extensions

IPv6 allows a more flexible protocol extension than IPv4 does. This is without imposing any overhead to intermediate routers. It is achieved by splitting headers into two flavours: the headers intermediate routers need to examine, and the headers the end nodes will examine. This also eases hardware acceleration for IPv6 routers.

No Routing Table Growth

IPv4 backbone routing table size has been a big headache to ISPs and backbone operators. The IPv6 addressing specification restricts the number of backbone routing entries by advocating route aggregation.

Simplified Header Structures

IPv6 has simpler packet header structures than IPv4. It will allow future vendors to implement hardware acceleration for IPv6 routers easier.

Smooth Transition From IPv4

Many IPv4 considerations were made during the IPv6 development. Also, there is a large number of transition mechanisms available which will allow smooth migration from IPv4 to IPv6.

Same Design Principles as IPv4

IPv4 was a very successful design, as proven by the ultra large-scale deployment in the world. IPv6 is the new version IP, and it follows many of the designs that made IPv4 very successful.

- ANSI C source code
- Small footprint
- DSP optimized
- Static and dynamic configuration
- Single interface for minimum stack overhead
- Add-on modules: PPP, TCP and IPSec

IPLITE Features.

IPLITE RFC Conformance

IPv4 and Base Conformance

- RFC 768 User Datagram Protocol
- RFC 791 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 826 An Ethernet Address Resolution Protocol
- RFC 894 Standard for the transmission of IP datagrams over Ethernet networks
- RFC 919 Broadcasting Internet Datagrams
- RFC 922 Broadcasting Internet datagrams in the presence of subnets
- RFC 950 Internet Standard Subnetting Procedure
- RFC 1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
- RFC 1071 Computing the Internet checksum
- RFC 1112 Host Extensions for IP Multicasting
- RFC 1122 Requirements for Internet Hosts - Communication Layers
- RFC 1191 Path MTU Discovery
- RFC 1518 An Architecture for IP Address Allocation with CIDR

IPv6 Conformance

- RFC 1886 DNS Extensions to support IP version 6 (future release)
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2373 IPv6 Addressing Architecture

- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 IPv6 specification
- RFC 2461 Neighbor discovery for IPv6
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 ICMPv6 for IPv6 specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2553 Basic Socket Interface Extensions for IPv6

TCP Conformance*

- RFC 793 Transmission Control Protocol
- RFC 2581 TCP Congestion Control

PPP Conformance*

- RFC 1321 The MD5 Message-Digest Algorithm
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2472 IP Version 6 over PPP

IPSec Conformance*

- RFC 1826 IP Authentication Header [old AH]
- RFC 1827 IP Encapsulating Security Payload (ESP) [old ESP]
- RFC 1828 IP Authentication using Keyed MD5
- RFC 1852 IP Authentication using Keyed SHA
- RFC 1853 IPIP - IP in IP tunneling
- RFC 2144 The CAST-128 Encryption Algorithm
- RFC 2367 PF_KEY Key Management API, Version 2 [+openbsd ext]
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2402 AH - IP Authentication Header
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406 ESP - IP Encapsulating Payload
- RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2451 The ESP CBC-Mode Cipher Algorithms (blowfish, cast, des, 3des)
- draft-ietf-ipsec-monitor-mib-03.txtIPSec Monitoring MIB
- draft-ietf-ipsec-auth-hmac-ripemd-160-96-02 HMAC-RIPE-MD-160-96

* Please note that an asterisk indicates that the group of RFCs is supported in an optional module.



Worldwide Headquarters

30 West Sola Street • Santa Barbara, California 93101
Tel: 805.965.6044 • Fax: 805.965.6343 • Email: sales@ghs.com • www.ghs.com

International Offices

France: +33 (0)1 46 96 07 00 • Germany: +49 (0)721 98 62 580
The Netherlands: +31 (0)33 4613363 • Sweden: +46 (0)46 211 33 70
United Kingdom: +44 (0) 1844 267950 • Japan (ADaC): +81.3.3576.5351

Interpeak Network Security

Interpeak AB, located in Stockholm, Sweden, specializes in network security software and new Internet communication protocols for embedded systems. Interpeak products include IPSec, IKE, SSH, SSL, Web Server Security and NAT. Internet protocols such as LDAP, L2TP, RADIUS, and PPPoE, as well as a dual-mode IPv4/IPv6 TCP/IP stack is also available. For additional information, please visit our homepage: www.interpeak.se, or send a mail to info@interpeak.se.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 2.10. Copyright © 2003, Interpeak AB. All rights reserved.