

INTEGRITY



IPNET

—
IPv4/IPv6 Dual-Mode TCP/IP Stack

IPNET Overview

Many of the Internet protocols have traditionally only been available to workstation-class computers without any resource constraints. Interpeak now introduces IPNET, a full-featured IPv4/IPv6 dual-stack, specifically designed to be used in modern embedded real-time systems.

With the huge expansion of the Internet, TCP/IP has become the preferred protocol for local- and wide-area networks. The original design of the TCP/IP protocol surprisingly dates back to the early eighties, but new features are continuously added by the Internet Engineering Task Force (IETF).

TCP/IP is also widely used when connecting networked embedded real-time systems. TCP/IP stacks designed for use in embedded systems do however often have limitations in functionality. This is often caused by memory and timing constraints, but also by the fact that stack vendors have problems to keep up with the continuous flow of new protocols specified by the IETF.

The full set of TCP/IP protocols has therefore traditionally only been available to desktop computers and servers. Although the limited functionality of embedded TCP/IP stacks may have been sufficient in many cases, modern embedded real-time systems often demand a full-featured stack that supports a substantial part of the IETF protocols.

Interpeak, with its long experience of embedded networking products, therefore introduces IPNET—a full-

- IPv4
- IPv6
- IPSec
- PPP
- TCP
- UDP
- NAT
- ARP
- Ethernet
- ICMP
- ICMPv6/MLD/NDP
- IGMP/Multicasting

Supported Protocols

featured dual IPv4/IPv6 stack—specifically designed and implemented from the ground up to be used in modern embedded real-time systems.

Internet Protocol, Version 6

Interpeak IPNET supports IPv6, which extends the current IP protocol specification in a number of important aspects. The IPNET IPv6 implementation is RFC compliant and compatibility tested against major operating systems like Solaris, Linux, Windows XP, various BSD implementations etc.

Simultaneous Use of IPv4 and IPv6 Applications

The transition from IPv4 to IPv6 will take several years to finalize. During this period, a common situation will be that a TCP/IP stack has to support communication with both type of nodes. Interpeak IPNET is a true IPv4/IPv6 dual-stack that handles simultaneous use of IPv4 and IPv6 in a variety of configurations.

Packet Filtering

IPNET contains a packet filtering engine, allowing filtering of traffic based on interface, protocol, port, tos, ttl, source destination and many other factors. This can be used to implement security features like firewalls, and also for other types of customizations.

Security

In addition to the packet filtering, IPNET includes IPSec for both IPv4 and IPv6, as well as NAT.

IPSec—Internet Protocol Security—transparently secures applications by enabling authentication, integrity, encryption and replay protection.

NAT—Network Address Translation—makes it possible to hide the local network topology, as well as using a single public IP address for an entire LAN. The Firewall, NAT and IPSec functionality is tightly integrated with IPNET for optimum performance as well as guaranteed interoperability.

MIB-II Support

Remote management and control of the TCP/IP stack is allowed using the SNMP protocol. Necessary MIB-II statistics are gathered by the kernel for each access by SNMP agents. MIB-II tables include: Interfaces, IP, Address Translation, ICMP, TCP, and UDP.

- Raw IP/UDP/TCP BSD sockets
- Routing sockets, used by routing daemons
- PFKEYv2 sockets, used by key management daemons
- MIB control interface
- 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

IPNET Architecture

Routing Engine

IPNET contains a high-performance routing engine, using highly optimized Radix trees that allow both static and dynamic routes. There is also a standard BSD routing socket interface that enables the use of standard routing daemons, as well as allowing for dedicated routing devices to cooperate with the TCP/IP stack.

Furthermore, the IPNET stack supports full virtualization with multiple independent routing tables, used in Virtual Routers. The Virtual Routing support includes BSD socket extensions to manage the additional routing tables.

Highly Configurable

IPNET can be deployed in a variety of different configurations, which is often a requirement in embedded systems. Unused modules, protocols or features can be removed from the TCP/IP stack, thereby reducing memory footprint to as low as 40 kilobytes.

Applications

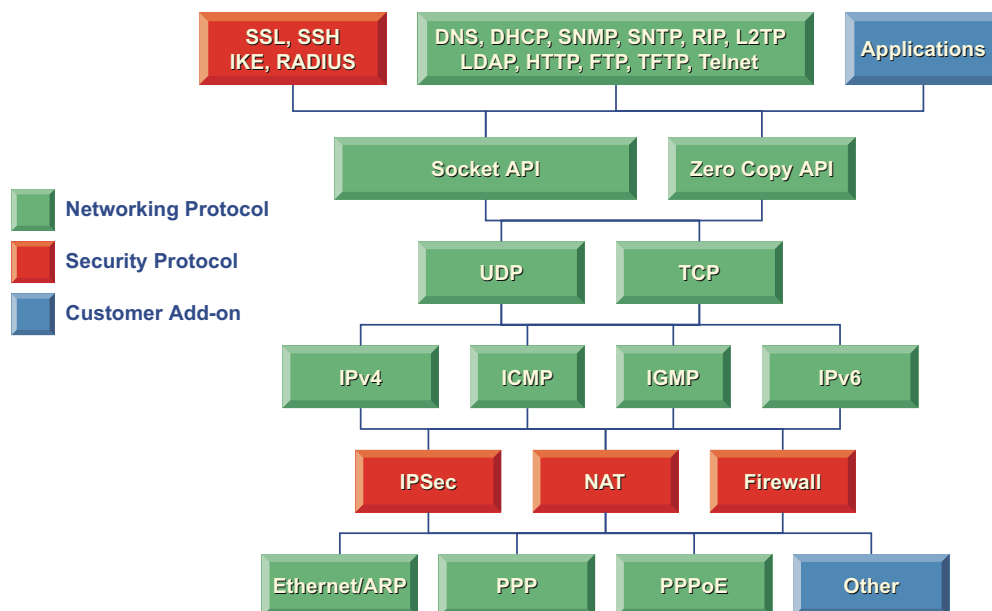
Interpeak has implemented a large number of security and networking applications like SSH, SSL, IKE, L2TP, RADIUS, PPPoE, RIP, SNMP, Telnet, FTP, TFTP, DHCP, HTTP, DNS, LDAP etc. For additional information about these networking applications, please visit www.interpeak.se/products.

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

Uses Existing Drivers and Board Support

Interpeak IPNET is closely integrated with several major real-time operating systems, utilizing the same network drivers and board support packages as the RTOS. This makes IPNET readily available on all platforms and devices supported by the RTOS.

Example target systems include both CISC, RISC and DSP architectures from e.g. ARM, Hitachi, Intel, MIPS, Motorola, Texas, etc.



The architecture of IPNET and additional Interpeak networking products. Due to its modular design, it is easy to customize IPNET 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
- Highly scalable
- Static and dynamic configuration
- Unlimited number of addresses, sockets, routes and interfaces
- Optimized radix routing trees
- Virtual routing support
- Built-in IPSec, NAT and Firewall
- Shell commands, e.g. `ifconfig`, `netstat`, `route` etc.

IPNET Features.

IPNET RFC Conformance

IPv4 and Base Conformance

- RFC 768 User Datagram Protocol
- RFC 791 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 Transmission Control Protocol
- 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 1213 Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 1518 An Architecture for IP Address Allocation with CIDR
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 2236 Internet Group Management Protocol, Version 2
- RFC 2581 TCP Congestion Control

IPv6 Conformance

- RFC 1886 DNS Extensions to support IPv6 (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 2465 MIB for IPv6: Textual Conventions and General Group
- RFC 2466 MIB for IPv6: ICMPv6 group
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2710 Multicast Listener Discovery for IPv6

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.txt IPsec Monitoring MIB
- draft-ietf-ipsec-auth-hmac-ripemd-160-96-02 MAC-RIPE-MD-160-96

NAT Conformance

- RFC 1631 The IP Network Address Translator (Nat)
- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations



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.