
TCP/IP Module

Overview

IP Infusion's ZebOS® Network Platform TCP/IP Module is a dual stack that supports simultaneous use of IPv4 and IPv6 in a variety of configurations. ZebOS control plane software communicates via standard routing sockets with the TCP/IP module to install routes into the Forwarding Information Base (FIB); send and receive packets; and configure interfaces. Other levels of communication use various sockets and/or a set of standard TCP/IP stack APIs [such as, `ioctl()`]. Clients can deploy the ZebOS TCP/IP Module in a variety of different configurations, which is often a requirement for embedded systems. In addition, clients can remove unused features from the TCP/IP stack, thereby reducing memory footprint.

To implement security features and other customizations, the TCP/IP Module contains a packet-filtering engine that allows filtering of traffic based on interface, protocol, port TOS, TTL, source, destination and many other factors. Clients can use the SNMP protocol for remote management and control of the TCP/IP. MIB-II tables include Interface, IP, Address Translation, ICMP, TCP, and UDP.

In addition to standard functionality, ZebOS TCP/IP supports Virtual Routing (VR) and multiple FIBs simultaneously by partitioning resources per FIB. In order to support VR, ZebOS TCP/IP can be used in conjunction with ZebOS BGP-4+, OSPFv2, OSPFv3, or RIP/RIPng.

Features

- Simultaneous support of IPv4 and IPv6
- Packet Filtering
- MIB-II Support
- Ad-Hoc Networking
- Highly Configurable
- Flexible Protocol Extensions
- Virtual Routing Support
- Support of VxWorks® real-time operating systems

Benefits

- Stable, robust implementation of TCP/IP
- Smooth transition from IPv4 to IPv6

Standards Support

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 sub-nets
- 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 Internet: MIB-II
- RFC 1518 — An Architecture for IP Address Allocation with CIDR
- RFC 1812 — Requirements for IP Version 4 Routers
- RFC 2113 — Router Alert Option
- 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 Auto-configuration
- 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 — IP in IP (IPIP) 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 — IP Authentication Header
- RFC 2403 — The Use of HMACMD5- 96 within ESP and AH
- RFC 2404 — The Use of HMACSHA- 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 — IPsec Monitoring MIB
- draft-ietf-ipsec-auth-hmac-ripemd 160-96-02 — The use of HMAC-RIPEMD-160-96 within ESP and AH

NAT Conformance

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

Standard Deliverables

- Source Code (written in ANSI compliant C)
- Installation Guide
- Configuration Guide
- Command Reference Guide
- Ported on VxWorks® Operating Systems