Cisco IOS Systems

Small Form Factor (SFF) Systems with Cisco IOS®

- Runs Cisco IOS® software
- Cisco® Unified Communications Manager Express (CME) support
- Cisco® Mobile Ready Net, which allows for mobile ad hoc networking and radio aware routing
- Hardware acceleration
- Hardware encryption
- Integrated threat control using Cisco IOS® Firewall, Cisco IOS® Zone-based Firewall, Cisco IOS® Intrusion Prevention System (IPS), and Cisco IOS® Content Filtering
- Identity management using authentication, authorization, and accounting (AAA) and public key infrastructure
- Military D38999, industrial IP66/67, or commercial RJ-45 connectors
- Four 10/100/1000 Ethernet ports
- Natural convection cooling, conduction cooling, or forced-air cooling

Cisco IOS Systems

These systems are based on X-ES routers that run Cisco IOS® Software with Cisco® Mobile Ready Net capabilities, providing highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links. The Cisco IOS® systems are high-performance, ruggedized, packaged routers designed for applications with the most severe Size, Weight and Power (SWaP) constraints often deployed in harsh environments.

The Cisco IOS® Systems use the same Cisco IOS® that IT staffs in the military, energy, public safety, and other industries are already trained on, enabling these organizations to expand their network to personnel, equipment, facilities, and vehicles at the edge of the network without any additional training. Cisco IOS® Systems can be connected to UHF, VHF, Wi-Fi, and other radio platforms to create the network nodes used to form mobile ad hoc networks (MANETs). Able to operate without a connection to central infrastructure, MANETs offer many advantages for military, public safety, and emergency response users. Cisco IOS® Systems extend the Cisco® enterprise infrastructure beyond the reach of traditional fixed-network infrastructure for oil and gas, mining, smart grid, heavy construction, transportation, homeland security, and public safety applications.

To meet the needs of demanding SWaP-constrained mobile and embedded networking applications, Cisco IOS® Systems provide four Gigabit Ethernet interfaces, hardware encryption, radio aware routing (RAR) with support for the latest Dynamic Link Exchange Protocol (DLEP), support for IPv6, integrated threat control with integrated Cisco IOS® firewalls and Intrusion Prevention System (IPS), and Quality of Service (QoS). Cisco IOS® Systems have packaging options to meet a wide range of application and industry needs. They are available in natural convection-cooled, conduction-cooled, or forced-air-cooled enclosures in either horizontal or vertical orientations with commercial RJ-45, industrial IP66/67, or military D38999 front-panel connectors. The rugged Cisco IOS® Systems have passed the appropriate environmental and EMI testing, so they can be deployed quickly. In addition to packaged Cisco IOS® systems, X-ES can integrate Cisco IOS®-based routers with customer, third-party, and X-ES modules (e.g., PMCs, XMCs, COM Express, 3U VPX) into SFF and ATR systems.

X-ES
Extreme Engineering Solutions

...Always Fast

Extreme Engineering Solutions
9901 Silicon Prairie Parkway • Verona, WI 53593
Phone: 608.833.1155 • Fax: 608.827.6171
sales@xes-inc.com • https://www.xes-inc.com

Hardware Encryption Support

- Onboard hardware encryption processor supporting IP Security (IPsec)
- Secure Sockets Layer with transparent LAN services (SSL/TLS)
- Secure Real-time Transport Protocol (SRTP)
- Triple Digital Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Internet Key Exchange (IKE)

Cisco® IP Multiplexing

- Improve bandwidth efficiency over pps-constrained links

Cisco® Wide Area Application Services (WAAS) Express

- Bandwidth optimization and application acceleration capabilities
- Increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco® WAAS infrastructure

Routing Protocols

- Routing Information Protocol (RIP)
- RIPv2
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)
- Cisco® Discovery Protocol
- IP Policy Routing
- IP Multicast Protocol Independent Multicast (PIM) Versions 1 and 2
- Internet Group Management Protocol (IGMP) Versions 1 and 2
- IP Multicast Load Splitting
- Four, 10/100/1000 Mbps, IEEE 802.3-compliant, Ethernet controllers
- Cisco® Group Management Protocol (GMP)

VLANs

- Up to 32 VLANs supported per router

IPv4 and IPv6

- IPv6 routing and Cisco® Express Forwarding switching
- IPv6 QoS
- IPv6 tunneling support
- Zone-based Firewall for IPv6 traffic

Encapsulations

- Point-to-Point Protocol (PPP)
- PPP over Ethernet (PPPoE) client and server for Fast Ethernet
- 802.1q VLAN trunking support
- Generic Routing Encapsulation (GRE)
- Additional protocol support

Radio Aware Routing

- Optimizes IP routing over fixed or temporary radio networks
- Factors radio link metrics into route calculations
- Immediately recognizes and adapts to changes in network neighbor status
- Dynamic Link Exchange Protocol (DLEP)
- Router Radio Control Protocol (R2CP)
- RFC 5578 (authored by Cisco®)

Mobile Ad Hoc Networks

- OSPFv3 enhancements for mobile ad hoc networks

Mobile IP

- Home agent and mobile router redundancy
- Mobile router preferred interfaces
- Mobile router reverse tunneling
- Mobile router asymmetric links
- Mobile router static and dynamic networks
- Static co-located care-of address
- Authentication, authorization, and accounting (AAA) server
- Cisco® Mobile Networks Network Address Translation (NAT) Traversal over Mobile IP
- Support for Mobile IP tunnel templates, allowing configuration of IP Multicast and IPsec on Mobile IP tunnels
- Mobile IP foreign agent local routing optimization

Next Generation Encryption

- Suite-B support in IOS® SW crypto including Suite-B-GCM-128, Suite-B-GCM-256, Suite-B-GMAC-128, Suite-B-GMAC-256 as described in RFC-4869

Authentication

- Route and router authentication
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP) local password
- IP basic and extended access lists
- Time-based access control lists (ACLs)

Secure Connectivity

- Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN

Integrated Threat Control

- Responding to sophisticated network attacks and threats using Cisco IOS® Firewall, Cisco IOS® Zone-based Firewall, Cisco IOS® IPS, Cisco IOS® Content Filtering, and Flexible Packet Matching (FPM)

Identity Management

- Intelligently protecting endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI)

Traffic Management

- QoS
- Generic traffic shaping
- Class-based Ethernet matching and mobile access routing (802.1p Class of Service [CoS])
- Committed access rate
- Flow-based Weighted Random Early Detection (WRED)
- Class-based Weighted Fair Queuing (WFQ)
- Low Latency Queuing (LLQ)
- Priority Queuing
- Weighted Fair Queuing (WFQ)
- Link Fragmentation and Interleaving (LFI)
- Traffic Policing Resource Reservation Protocol (RSVP)

Security Protocols

- IP Security (IPsec)
- Secure Sockets Layer with transparent LAN services (SSL/TLS)
- Secure Real-time Transport Protocol (SRTP)
- Triple Digital Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Internet Key Exchange (IKE)

Unified Communications

- Cisco® Unified Communications Manager Express with support for up to 150 phones

Management Services

- Simple Network Management Protocol (SNMP) Versions 2 and 3
- Telnet
- Console port
- RADIUS
- TACACS+
- Cisco® Service Assurance Agent
- Syslog
- Response Time Reporter
- Network Time Protocol (NTP) Client
- Trivial File Transfer Protocol (TFTP) Client and Server
- Dynamic Host Configuration Protocol (DHCP) Client and Server
- DHCP Relay
- Hot Standby Router Protocol (HSRP)

Tool Command Language (Tcl) scripts

- Tcl script support

Address Conservation

- NAT Many-to-One (Port Address Translation [PAT])
- NAT Many-to-Many (Multi-NAT)
- DHCP Client Address Negotiation
- Easy IP Phase I

I/O Interfaces

- Four 10/100/1000 routed Gigabit Ethernet ports supporting auto-negotiation
- One console port supporting RS-232 signaling
- One AUX serial port supporting RS-232/422 signaling plus handshaking

Enclosure and Front Panel I/O options

- XPand6000 Series enclosures with two D38999 connectors
- XPand6100 Series enclosures with industrial IP66/67 or commercial, e.g. RJ-45, connectors

Power

- MIL-STD-704 28 VDC or 100 VAC input voltage
- MIL-STD-461 EMI filtering
- Integrated internal hold-up (optional)
- Additional power supply options available

Environmental

- XPand6000 Series versions designed to meet the rigorous standards of MIL-STD-810