enterasys® Secure Networks™

DATASHEET

Enterasys K-Series™

Flexible, Modular Switch With Premium Features, for Enterprise Edge to Small Core Deployments

Versatile, high density edge to small core switching with flexible connectivity and power options reduces cost of ownership

Advanced automated network provisioning maximizes the efficiency and reliability of supporting new IT services such as virtualized desktops

Integrated visibility, granularity and control delivers significant cost savings and premium security for mission critical networks

Easy to deploy access controls and prioritization provides more robust location, identification and overall management capabilities including support for "bring your own device" programs

Product Overview

The Enterasys K-Series™ is the most cost-effective, flow-based switching solution in the industry. Providing exceptional levels of automation, visibility and control from the network edge to the small enterprise core, these flexible, modular switches significantly reduce operational costs while still offering premium features.

The K-Series is built upon the Enterasys CoreFlow2 custom ASIC. This cornerstone switching technology provides greater visibility into critical business applications and the ability to enable better controls to meet the Service Level Agreements (SLAs) demanded by the business.

Designed to address the challenges associated with a growing demand for access to new applications and services, the K-Series protects businesses traffic and supports changing operational needs. This includes the consumerization of IT and "bring your own device" programs that require more robust location, identification, visibility and overall management capabilities. The K-Series is uniquely suited to intelligently manage individual user, device and application conversations, as well as to provide the visibility and management to troubleshoot connectivity issues, locate devices, and ensure protection of corporate data.

Enterasys K-Series switches are available in the following form factors:

- 6-slot chassis offering up to a maximum of 144 triple-speed ports and (4) 10Gb uplinks
- 10-slot chassis offering up to a maximum of 216 triple-speed ports and (8) 10Gb ports

The K-Series supports up to (12) 10Gb uplinks, including four ports on the fabric card and 8 ports on (2) 10Gb IOMs.

The K-Series makes forwarding decisions and enforces security policies and roles while classifying/prioritizing traffic at wire speed. All I/O modules provide the highest Quality of Service (QoS) features for critical applications such as voice and HD video even during periods of high network traffic load while also proactively preventing Denial of Service (DoS) attacks and malware propagation.

The K-Series implements an industry-leading, flow-based switching architecture to intelligently manage individual user and application conversations — far beyond the capabilities of switches that are limited to using VLANs, ACLs, and ports to implement role-based access controls. Users

Benefits

Business Alignment

- Ensures each end-user receives the information, services and applications needed to achieve their business goals through extensive network visibility and control capabilities
- Green and efficient power system modularity drives down power and cooling costs by providing optimal incremental power consumption
- Consistent end user experience and network protection by effectively allocating critical network services while blocking suspicious traffic

Operational Efficiency

- High-density, small form factor chassis provides up to (216) 10/100/1000 ports with (8) 10Gb uplinks in a standard rack, significantly reducing footprint costs
- Management automation and built-in resiliency features drive down operational costs and maximize uptime

Security

- Reduces risk and simplifies network administration with built-in, not bolted on security
- Protects business traffic from malicious attacks and maintains information confidentiality, integrity and availability
- Extends network access control and security to existing edge switches and wireless access points, meeting the challenges associated with the consumerization of IT

Support and Service

- Industry-leading customer satisfaction and first call resolution rates

There is nothing more important than our customers.

are identified and roles are applied to ensure each individual user can access their business-critical applications no matter where they connect to the network. K-Series policy rules combined with deep packet inspection can intelligently sense and automatically respond to security threats while improving reliability and quality of the user experience. A significant differentiator for the K-Series is the ability to collect NetFlow data at wire-speed providing total visibility into network resource consumption for users and applications. The K-Series joins the S-Series as the only enterprise switches to support multi-user, multimethod authentication on every port — absolutely essential when you have devices such as IP phones, computers, printers, copiers, security cameras, badge readers, and virtual machines connected to the network.

These new modular switches deliver flexible connectivity, premium features and integrated security that enable the network to quickly adapt to changing business requirements.

Hardware-Based High Availability Features

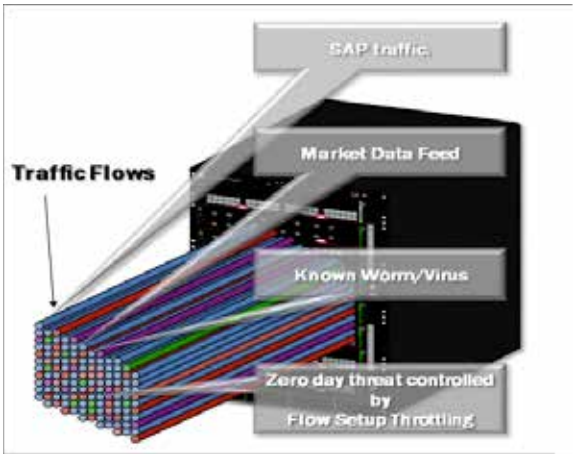
The K-Series includes many standard high availability features. These hardware-based high availability features allow the K-Series to be deployed in mission critical environments that require 24/7 availability.

The K-Series supports the following hardware-based high availability features:

- Passive chassis backplane
- Hot swappable fan trays with multiple cooling fans
- Hot swappable and load-sharing power supplies
- Multiple AC input connections for power circuit redundancy
- Up to 36 groups of eight Ethernet ports can be grouped together to create a multi-link aggregation group (LAG)

Flow-Based Architecture

In order to ensure granular visibility and management of traffic without sacrificing performance, the Enterasys K-Series deploys a flowbased architecture. This architecture ensures that when a specific communications flow is being established between two end points, the first packets in that communication are processed through the multilayer classification engines in the switch and the I/O fabric module. In this process, the role is identified, the applicable policies are determined, the packets are inspected and the action is determined. After the flow is identified, all subsequent packets associated with that flow are automatically handled in the Enterasys ASICs without any further processing. In this way the Enterasys K-Series is able to apply a very granular level of control to each flow at full line rate.



Multi-User/Method Authentication and Policy

Authentication allows enterprise organizations to manage network access and provide mobility to users and devices. It provides a way to know who or what is connected to the network and where this connection is at any time. The Enterasys K-Series has unique, industry leading capabilities regarding types of simultaneous authentication methods. K-Series modules can support multiple concurrent authentication techniques, including:

- 802.1X authentication
- MAC authentication, which is a way to authenticate devices on the network using the MAC address
- Web-based authentication, also known as Port Web Authentication (PWA), where a user name and password are supplied through a browser
- CEP, also known as Convergence End Point, where multiple vendors VoIP phones are identified and authenticated; this capability provides great flexibility to enterprises looking to implement access control mechanisms across their infrastructure

A significant additional feature of the K-Series is the capability to support multi-user authentication. This allows multiple users and devices to be connected to the same physical port and each user or device to be authenticated individually using one of the multi-method options (802.1x, MAC, PWA, or CEP). The major benefit of multi-user authentication is to authorize multiple users, either using dynamic policy or VLAN assignment for each authenticated user. In the case of dynamic policy, this is called Multi-User Policy. Multi-user port capacities with the K-Series are determined on a per port, per I/O module, and per multi-slot system basis.

Multi-user authentication and policy can provide significant benefits to customers by extending security services to users connected to unmanaged devices, third party switches/routers, VPN concentrators, or wireless LAN access points at the edge of their network. Using authentication provides security, priority, and bandwidth control while protecting existing network investments. The K-Series supports up to 8 users per port with a license option for 256 users per port. Total system capacity supports 1152 users on the K6 and 1920 users on the K10.

Dynamic, Flow-Based Packet Classification

Another unique feature that separates the Enterasys K-Series from all competitive switches is the capability to provide User-Based Multi-layer Packet Classification/QoS. With the wide array of network applications used on networks today, traditional Multi-layer Packet Classification by itself is not enough to guarantee the timely transport of business critical applications. In the K-Series, User-Based Multi-layer Packet Classification allows traffic classification not just by packet type, but also by the role of the user on the network and the assigned policy of that user. With User-Based Multi-layer Packet Classification, packets can be classified based on unique identifiers like “All Users”, “User Groups”, and “Individual User”, thus ensuring a more granular approach to managing and maintaining network confidentiality, integrity, and availability.

Network Visibility From High Fidelity NetFlow

Network performance management and security capabilities via NetFlow are available on Enterasys K-Series switch ports without slowing down switching and routing performance or requiring the purchase of expensive daughter cards for every module. Enterasys NetFlow tracks every packet

in every flow as opposed to more typical statistical sampling techniques or restrictive appliance-based implementations. The value of unsampled, real-time NetFlow monitoring is the visibility into exactly what traffic is traversing the network. If something abnormal occurs it will be captured by NetFlow and appropriate action can be applied. Additionally, NetFlow can be used for capacity planning, allowing the network manager to monitor the traffic flows and volumes of traffic in the network and understand where the network needs to be reconfigured or upgraded. This saves time and money by enabling administrators to know when and where upgrades might be needed.

Network Traffic Monitoring–Port Mirroring

Port mirroring is an integrated diagnostic tool for tracking network performance and security that is especially useful for fending off network intrusion and attacks. It is a low-cost alternative to network taps and other solutions that may require additional hardware, disrupt normal network operation, affect client applications or may introduce a new point of failure into your network.

Port mirroring is highly scalable and easy to monitor. It is especially convenient to use in networks where ports are scarce. Ports that can be configured to participate in mirroring include physical ports, virtual ports and host ports—VLAN interfaces, and intrusion detection ports. With this feature, analyzing bi-directional traffic and ensuring connectivity between, for example, a departmental switch and its high speed uplink to a backbone switch becomes simple and cost effective process.

K-Series port mirroring relationships can be set on inbound traffic, outbound traffic, or both for up to 4-port mirrors consisting of one-to-one, one-to-many, many-to-one, IDS or policy mirrors.

Feature Summary

Multi-layer packet classification - enables the delivery of critical applications to specific users via traffic awareness and control

- User, port, and device Level (Layer 2 through 4 packet classification)
- QoS mapping to priority queues (802.1p & IP ToS/ DSCP) up to 12 queues per port
- Multiple queuing mechanisms (SPQ, WFQ, WRR and Hybrid)
- Granular QoS/rate limiting
- VLAN to policy mapping

Switching/VLAN services–provides high performance connectivity, aggregation, and rapid recovery services

- Extensive industry standards compliance (IEEE and IETF)
- Inbound and outbound bandwidth rate control per flow
- VLAN services support
  - Link aggregation (IEEE 802.3ad)
  - Multiple spanning trees (IEEE 802.1s)
  - Rapid reconfiguration of spanning tree (IEEE 802.1w)
- Provider Bridges (IEEE 802.1ad), Q-in-Q
- Flow setup throttling
- DHCP Server

IP Routing - provides dynamic traffic optimization, broadcast containment and efficient network resilience

- Standard routing features include static routes, RIPv2, RIPng and Multicast routing support (DVMRP, IGMP v1/v2/v3), Policy Based Routing and Route Maps and VRRP
- Licensed routing features include OSPF v2/v3, VRF, IS-IS (via future FW upgrade) and PIM-SM

Security (User, Network and Management)

- User security
  - Authentication (802.1X, MAC, PWA+ and CEP), MAC (Static and Dynamic) port locking
  - Multi-user authentication/policies
- Network security
  - Access Control Lists (ACL) – basic and extended
  - Policy-based security services (examples: spoofing, unsupported protocol access, intrusion prevention, DoS attacks limits)
- Management Security
  - Secure access to the K-Series via SSH, SNMP v3

Management, Control and Analysis – provide streamlined tools for maintaining network availability and health

- Configuration
  - Industry-standard CLI and web management support
  - Multiple firmware images with editable configuration files
- Network Analysis
  - SNMP v1/v2c/v3, RMON (9 groups) and SMON (RFC2613) VLAN and Stats
  - Port/VLAN mirroring (one-to-one, one-to-many, many-to-many)
  - Unsampled NetFlow on every port with no impact on system switching and routing performance
- Automated set-up and reconfiguration
  - Replacement I/O module will automatically inherit previous modules configuration

Examples of additional functionality and features that are supported by the Enterasys K-Series:

- NetFlow–Provides real-time visibility, application profiling and capacity planning
- LLDP-MED–Link Layer Discovery Protocol for Media Endpoint Devices enhances VoIP deployments
- Flow Setup Throttling–(FST) effectively preempts and defends against DoS attacks
- Node & Alias Location–Automatically tracks user and device location and enhances network management productivity and fault isolation
- Port Protection Suite–Maintain network availability by ensuring good protocol and end station behavior
- Flex-Edge Technology–Provides advanced bandwidth management and allocation for demanding access/edge devices

Flow Setup Throttling (FST) is a proactive feature designed to mitigate zero-day threats and Denial of Service (DoS) attacks before they can affect the network. FST directly combats the effects of zero-day and DoS attacks by limiting the number of new or established flows that can be programmed on any individual switch port. This is achieved by monitoring the new flow arrival rate and/or controlling the maximum number of allowable flows.

In network operations, it is very time consuming to locate a device or find exactly where a user is connected. This is especially important when reacting to security breaches. Enterasys K-Series modules automatically track the network's user/device location information by listening to network traffic as it passes through the switch. This information is then used to populate the Node/Alias table with information such as an end-station's MAC address and Layer 3 alias information (IP address, IPX address, etc.). This information can then be utilized by Enterasys NMS Suite management tools to quickly determine the switch and port number for any IP address and take action against that device in the event of a security breach. This node and alias functionality is unique to Enterasys and reduces the time to pinpoint the exact location of a problem from hours to minutes.

For organizations looking to deploy Unified Communications, the Enterasys K-Series combines policy-based automation with support for multiple standards-based discovery methods, including LLDP-MED, SIP and H.323, to automatically identify and provision UC services for IP phones from all major vendors. K-Series switches also provide dynamic mobility for IP clients; when an IP phone moves and plugs in elsewhere in the enterprise network, its VoIP service provisioning, security and traffic priority settings move with it, with none of the typical manual administration required for moves, adds and changes.

The K-Series also supports a comprehensive portfolio of port protection capabilities, such as SPANguard and MACLock, which provide the ability to detect unauthorized bridges in the network and restrict a MAC address to a specific port. Other port protection features include Link Flap, Broadcast Suppression and Spanning Tree Loop protection which protects against mis-configuration and protocol failure.

Enterasys K-Series Flex-Edge technology provides line rate traffic classification for all access ports with guaranteed priority delivery for control plane traffic and high-priority traffic as defined by the Enterasys policy overlay. In addition to allocating resources for important network traffic, prioritized bandwidth can be assigned on a per port or per authenticated user basis. Flex-Edge technology is ideal for deployment in wiring closets and distribution points that can often suffer from spikes in utilization that cause network congestion. With Flex-Edge technologies, organizations no longer have to fear a momentary network congestion event that would result in topology changes and random packet discards.

All K-Series 10 Gigabit Ethernet SFP+ ports are dual speed and will also accept standard Gigabit SFP transceivers. This capability enables a smooth migration path from Gigabit Ethernet for connecting devices to 10 Gigabit Ethernet in the future. Customers can use Gigabit Ethernet optical uplinks today and migrate to 10 Gigabit at their own pace. In addition,all Gigabit SFP ports will accept Fast Ethernet 100BASE-FX/TX SFPs to enable connection of legacy devices.

Features/Standards and Protocols

Switching/VLAN Services

- Generic VLAN Registration Protocol (GVRP)
- 802.1ab LLDP-MED
- 802.1ad Provider Bridges
- 802.1ag Connectivity Fault Management (CFM)
- 802.1ak Multiple VLAN Registration Protocol (MVRP)
- 802.1aq (SPB) Shortest Path Bridging (Ready)
- 802.1ax-2008 / 802.3ad Link Aggregation
  - up to 36 groups with up to 8 ports in a group
- 802.1d MAC Bridges
- 802.1q VLANs
- 802.1s Multiple Spanning Tree
- 802.1t Path Cost Amendment to 802.1D
- 802.1w Rapid re-convergence of Spanning Tree
- 802.3-2008 Clause 57 (Ethernet OAM – Link Layer OAM)
- 802.3ab Gigabit Ethernet (copper)
- 802.3ae 10 Gigabit Ethernet (fiber)
- 802.3an 10GBASE-T (copper)
- 802.3u Fast Ethernet
- 802.3x Flow Control
- 802.3z Gigabit Ethernet (fiber)
- IP Multicast (IGMPv1,v2,v 3)
- IGMP v1/v2/v3 Snooping and Querier
- Jumbo Packet with MTU Discovery Support for Gigabit (9216 bytes)
- Link Flap Detection
- Dynamic Egress (Automated VLAN Port Configuration)
- Data Center Bridging
  - 802.1Qaz
  - ETS (Enhanced Transmission Selection)
  - DCBx (Data Center Bridge Exchange Protocol)
- MLD IPv6 Snooping and Querier
- Virtual Switch Bonding (VSB) (Ready)
- Anti-Spoofing Suite
  - DHCP Snooping
  - Dynamic Arp Inspection (DAI)
  - IP Source Guard

Features/Standards and Protocols

IP/Routing Features

- Static Routes
- Standard ACLs
- OSPF with Multipath Support
- OSPF Passive Interfaces
- IPv6 Routing Protocol
- Extended ACLs
- Policy-based Routing
- VRF Virtual Routing and Forwarding (IPv6 and IPv4)
- PIM Source Specific Multicast - PIM SSM
- RFC 147 Definition of a socket
- RFC 768 UDP
- RFC 781 Specification of (IP) timestamp option
- RFC 783 TFTP
- RFC 791 Internet Protocol
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 894 Transmission of IP over Ethernet Networks
- RFC 919 Broadcasting Internet Datagrams
- RFC 922Broadcasting IP datagrams over subnets
- RFC 925 Multi-LAN Address Resolution
- RFC 950 Internet Standard Subnetting Procedue
- RFC 951 BOOTP
- RFC 959 File Transfer Protocol
- RFC 1027 Proxy ARP
- RFC 1034 Domain Names - Concepts and Facilities
- RFC 1035 Domain Names - Implementation and Specification
- RFC 1071 Computing the Internet checksum
- RFC 1112 Host extensions for IP multicasting
- RFC 1122 Requirements for IP Hosts - Comm Layers
- RFC 1123 Requirements for IP Hosts - Application and Support
- RFC 1157 Simple Network Management Protocol
- RFC 1191 Path MTU discovery
- RFC 1195 Use of OSI IS-IS for Routing in TCP/IP
- RFC 1245 OSPF Protocol Analysis
- RFC 1246 Experience with the OSPF Protocol
- RFC 1323 TCP Extensions for High Performance
- RFC 1349 Type of Service in the Internet Protocol Suite
- RFC 1350 TFTP
- RFC 1387 RIPv2 Protocol Analysis
- RFC 1388 RIPv2 Carrying Additional Information
- RFC 1492 TACAS+
- RFC 1517 Implementation of CIDR
- RFC 1518 CIDR Architecture
- RFC 1519 Classless Inter-Domain Routing (CIDR)
- RFC 1542 BootP: Clarifications and Extensions
- RFC 1624 IP Checksum via Incremental Update
- RFC 1721 RIPv2 Protocol Analysis
- RFC 1722 RIPv2 Protocol Applicability Statement
- RFC 1723 RIPv2 with Equal Cost Multipath Load Balancing
- RFC 1812 General Routing/RIP Requirements
- RFC 1853 IP in IP Tunneling
- RFC 1886 DNS Extensions to support IP version 6
- RFC 1924 A Compact Representation of IPv6 Addresses
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2001 TCP Slow Start
- RFC 2003 IP Encapsulation within IP
- RFC 2018 TCP Selective Acknowledgment Options
- RFC 2030 SNTP
- RFC 2080 RIPng (IPv6 extensions)
- RFC 2082 RIP-II MD5 Authentication
- RFC 2104 HMAC
- RFC 2113 IP Router Alert Option
- RFC 2117 PIM -SM Protocol Specification
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 2132 DHCP Options and BOOTP Vendor Extensions
- RFC 2138 RADIUS Authentication
- RFC 2236 Internet Group Management Protocol, Version 2
- RFC 2276 Architectural Principles of Uniform Resource Name Resolution
- RFC 2328 OSPFv2
- RFC 2329 OSPF Standardization Report
- RFC 2338 VRRP
- RFC 2362 PIM-SM Protocol Specification
- RFC 2370 The OSPF Opaque LSA Option
- RFC 2373 Address notation compression
- RFC 2374 IPv6 Aggregatable Global Unicast Address Format
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2428 FTP Extensions for IPv6 and NATs
- RFC 2450 Proposed TLA and NLA Assignment Rule
- RFC 2453 RIPv2
- RFC 2460 IPv6 Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2463 ICMPv6
- RFC 2464 Transmission of IPv6 over Ethernet
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of DS Field in the IPv4/v6 Headers
- RFC 2475 An Architecture for Differentiated Service
- RFC 2553 BasiCSocket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2581 TCP Congestion Control
- RFC 2597 Assured Forwarding PHB Group
- RFC 2685 Virtual Private Networks Identifier
- RFC 2697 A Single Rate Three Color Marker
- RFC 2710 IPv6 Router Alert Option
- RFC 2711 Multicast Listener Discovery (MLD) for IPv6
- RFC 2715 Interoperability Rules for Multicast Routing Protocols
- RFC 2740 OSPF for IPv6
- RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 2784 Generic Routing Encapsulation Ready

Features/Standards and Protocols

- RFC 2827 Network Ingress Filtering
- RFC 2865 RADIUS Authentication
- RFC 2865 RADIUS Accounting
- RFC 2890 Key and Sequence Number Extensions to GRE
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2894 Router Renumbering
- RFC 2966 Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 2991 Multipath Issues in Ucast & Mcast Next-Hop
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3162 RADIUS and IPv6
- RFC 3315 DHCPv6
- RFC 3359 TLV Codepoints in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3376 IGMPv3
- RFC 3411 SNMP Architecture for Management Frameworks
- RFC 3412 Message Processing and Dispatching for SNMP
- RFC 3413 SNMP Applications
- RFC 3446 Anycast RP mechanism using PIM and MSDP
- RFC 3484 Default Address Selection for IPv6
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3509 Alternative Implementations of OSPF ABRs
- RFC 3513 IPv6 Addressing Architecture
- RFC 3542 Advanced Sockets API for IPv6
- RFC 3567 IS-IS Cryptographic Authentication
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3590 MLD Multicast Listener Discovery
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 3596 DNS Extensions to Support IP Version 6
- RFC 3623 Graceful OSPF Restart
- RFC 3678 Socket Interface Ext for Mcast Source Filters
- RFC 3704 Network Ingress Filtering
- RFC 3719 Recommendations for Interop Networks using IS-IS
- RFC 3766 Determining Strengths For Public Keys Used For Exchanging Symmetric Keys
- RFC 3768 VRRP
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3787 Recommendations for Interop IS-IS IP Networks
- RFC 3810 MLDv2 for IPv6
- RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm
- RFC 3847 Restart signaling for IS-IS
- RFC 3879 Deprecating Site Local Addresses
- RFC 3956 Embedding the RP Address in IPv6 MCAST Address
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4109 Algorithms for IKEv1
- RFC 4167 Graceful OSPF Restart Implementation Report
- RFC 4191 Default Router Preferences and More-Specific Routes
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4213 Basic Transition Mechanisms for IPv6
- RFC 4222 Prioritized Treatment of OSPFv2 Packets
- RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers
- RFC 4251 The Secure Shell (SSH) Protocol Architecture
- RFC 4252 The Secure Shell (SSH) Authentication Protocol
- RFC 4253 The Secure Shell (SSH) Transport Layer Protocol (no support diffie-hellman-group14-sha1)
- RFC 4254 The Secure Shell (SSH) Connection Protocol
- RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4294 IPv6 Node Requirements
- RFC 4301 Security Architecture for IP
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Crypto Algorithm Requirements for ESP and AH
- RFC 4306 Internet Key Exchange (IKEv2) Protocol
- RFC 4307 Cryptographic Algorithms for Use in IKEv2
- RFC 4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol (no support diffie-hellman-group-exchange-sha256)
- RFC 4443 ICMPv6 for IPv6
- RFC 4541 IGMP Snooping
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM-SM
- RFC 4602 PIM-SM IETF Proposed Std Req Analysis
- RFC 4604 IGMPv3 & MLDv2 & Source-Specific Multicast
- RFC 4607 Source-Specific Multicast for IP
- RFC 4608 PIM–SSM in 232/8
- RFC 4610 Anycast-RP Using PIM
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4716 The Secure Shell (SSH) Public Key File Format
- RFC 4835 CryptoAlgorithm Requirements for ESP and AH
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 4878 OAM Functions on Ethernet-Like Interfaces
- RFC 4884 Extended ICMP Multi-Part Messages
- RFC 4940 IANA Considerations for OSPF
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5186 IGMPv3/MLDv2/MCAST Routing Protocol Interaction
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5250 The OSPF Opaque LSA Option
- RFC 5294 Host Threats to PIM
- RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
- RFC 5302 Domain-wide Prefix Distribution with IS-IS
- RFC 5303 3Way Handshake for IS-IS P2P Adjacencies
- RFC 5304 IS-IS

Features/Standards and Protocols

Cryptographic Authentication
- RFC 5306 Restart Signaling for IS-IS
- RFC 5308 Routing IPv6 with IS-IS
- RFC 5309 P2P operation over LAN in link-state routing
- RFC 5310 IS-IS Generic Cryptographic Authentication
- RFC 5340 OSPF for IPv6
- RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3
- RFC 6104 Rogue IPv6 RA Problem Statement
- RFC 6105 IPv6 Router Advertisement Guard
- RFC 6106 IPv6 RA Options for DNS Configuration
- RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links
- RFC 6549 OSPFv2 Multi-Instance Extensions

Network Security and Policy Management

- 802.1X Port-based Authentication
- Web-based Authentication
- MAC-based Authentication
- Convergence Endpoint Discovery with Dynamic Policy Mapping (Siemens HFA, Cisco VoIP, H.323, and SIP)
- Multiple Authentication Types per Port Simultaneously
- Multiple Authenticated users per Port with unique policies per user/
- End System (VLAN association independent)
- RFC 3580 IEEE 802.1 RADIUS Usage Guidelines, with VLAN to Policy Mapping
- Worm Prevention (Flow Set-Up Throttling)
- Broadcast Suppression
- ARP Storm Prevention
- MAC-to-Port Locking
- Span Guard (Spanning Tree Protection)
- Stateful Intrusion Detection System Load Balancing
- Stateful Intrusion Prevention System and Firewall Load Balancing
- Behavioral Anomaly Detection/Flow Collector (non-sampled Netflow)
- Static Multicast Group Provisioning
- Multicast Group, Sender and Receiver Policy Control
- Enterasys Private VLANs

Class of Service

- Strict Priority Queuing
- Weighted Fair Queuing with Shaping
- Hybrid Arbitration
- 12 Transmit Queues per Port
- Up to 10,750 rate limiters Class products
- Packet Count or Bandwidth based Rate Limiters (BandwidthThresholds between 8 Kbps and 4 Gbps)
- IP ToS/DSCP Marking/Remarking
- 802.1D Priority-to-Transmit Queue Mapping

Enterasys Network Management Suite (NMS)

- NetSight Base
- NetSight
- NetSight Advanced
- Data Center Manager

Network Management

- SNMP v1/v2c/v3
- Web-based Management Interface
- Industry Common Command Line Interface
- Multiple Software Image Support with Revision Roll Back
- Multi-configuration File Support
- Editable Text-based Configuration File
- COM Port Boot Prom and Image Download via ZMODEM
- Telnet Server and Client
- Secure Shell (SSHv2) Server and Client
- Cabletron Discovery Protocol
- Cisco Discovery Protocol v1/v2
- Syslog
- FTP Client
- Simple Network Time Protocol (SNTP)
- Netflow version 5 and version 9
- RFC 2865 RADIUS
- RFC 2866 RADIUS Accounting
- TACACS+ for Management Access Control
- Management VLAN
- 4 Many to-One-port, One-to-Many Ports, VLAN Mirror Sessions
- Remote Port Mirrors

Standard MIB Support

- RFC 1156 MIB
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1659 RS-232 MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPF MIB
- RFC 2012 TCP MIB
- RFC 2013 UDP MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 2233 The Interfaces Group MIB using SMIv2
- RFC 2576 SNMP-Community MIB
- RFC 2578 SNMPv2 SMI
- RFC 2579 SNMPv2-TC
- RFC 2613 SMON MIB
- RFC 2618 RADIUS Client MIB
- RFC 2620 RADIUS Accounting MIB
- RFC 2674 802.1p/q MIB
- RFC 2787 VRRP MIB
- RFC 2819 RMON MIB (Groups 1-9)
- RFC 2863 IF MIB
- RFC 2864 IF Inverted Stack MIB
- RFC 2922 Physical Topology MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3273 HC RMON MIB
- RFC 3291 INET Address MIB
- RFC 3411 SNMP Framework MIB
- RFC 3412 SNMP-MPD MIB
- RFC 3413 SNMPv3 Applications
- RFC 3413 SNMP Notifications MIB
- RFC 3413 SNMP Proxy MIB
- RFC 3413 SNMP Target MIB
- RFC 3414 SNMP User-Based SM MIB
- RFC 3415 SNMP View Based ACM MIB
- RFC 3417 SNMPv2-TM
- RFC 3418 SNMPv2 MIB
- RFC 3433 Entity Sensor MIB
- RFC 3621 Power Ethernet MIB
- RFC 3635 EtherLike MIB
- RFC 4022 MIB for the Transmission Control Protocol (TCP)
- RFC 4087 IP Tunnel MIB
- RFC 4113 MIB for the User Datagram Protocol (UDP)
- RFC 4133 ENTITY MIB
- RFC 4188 Bridge MIB
- RFC 4268 Entity State MIB
- RFC 4268 Entity State TC MIB
- RFC 4292 IP Forwarding MIB
- RFC 4293 MIB for Internet Protocol (IP)
- RFC 4444 MIB for IS-IS
- RFC 4560 DISMAN-PING-MIB
- RFC 4560 DISMAN-TRACEROUTE-MIB
- RFC 4560 DISMAN-NSLOOKUP-MIB
- RFC 4750 OSPFv2 MIB
- RFC 4836 MAU-MIB
- RFC 4836 IANA-MAU-MIB
- RFC 4878 DOT3-OAM-MIB
- RFC 5060 PIM MIB
- RFC 5240 PIM Bootstrap Router MIB
- RFC 5519 MGMD-STD-MIB
- RFC 5643 OSPFv3 MIB
- IANA Address Family Numbers MIB
- IEEE802.1 BRIDGE MIB
- IEEE802.1 CFM MIB
- IEEE802.1 CFM V2 MIB

Features/Standards and Protocols

- IEEE802.1 MSTP MIB
- IEEE802.1 Q BRIDGE MIB
- IEEE802.1 SPANNING TREE-MIB
- IEEE802.3 DOT3 LLDP EXT V2 MIB Partial
- IEEE802.1PAE MIB
- IEEE802.3 LAG MIB
- LLDP MIB
- LLDP EXT MED MIB
- LLDP EXT DOT1 MIB
- LLDP EXT DOT3 MIB
- LLDP EXT DOT3 V2 MIB (IEEE 802.3-2009) ETS Admin table read only
- Draft-ietf-isis-experimental-tlv (Partial Support)
- Draft-ietf-isis-ipv6-te (Partial Support)
- Draft-ietf-ospf-ospfv3-mib
- Draft-ietf-ospf-te-node-addr
- Draft-ietf-idmr-dvmrp-v3-11
- Draft-ietf-vrrp-unified-spec-03.txt

Private MIB Support

- CT Broadcast MIB
- CTIF EXT MIB
- CTRON Alias MIB
- CTRON-Bridge-MIB
- CTRON CDP MIB
- CTRON Chassis MIB
- CTRON Environmental MIB
- CTRON MIB Names
- CTRON OIDS
- CTRON Q Bridge MIB EXT MIB
- Cisco TC MIB
- Cisco CDP MIB
- Cisco NETFLOW MIB
- DVMRP-MIB
- Enterasys Flow Limiting MIB
- Enterasys 802.1X Extensions MIB
- Enterasys AAA Policy MIB
- Enterasys Anti-Spoof MIB
- Enterasys Auto Tracking MIB
- Enterasys Class of Service MIB
- Enterasys Configuration Change MIB
- Enterasys Configuration Management MIB
- Enterasys Convergence Endpoint MIB
- Enterasys Diagnostic Message MIB
- Enterasys DNS Resolver MIB
- Enterasys DVMRP EXT MIB
- Enterasys Entity Sensor MIB Ext MIB
- Enterasys IEEE8023 LAG MIB EXT MIB
- Enterasys IETF Bridge MIB EXT MIB
- Enterasys ETF P Bridge MIB EXT MIB
- Enterasys ETH OAM EXT MIB
- Enterasys IF MIB EXT MIB
- Enterasys IEEE802.1 Bridge MIB EXT MIB
  Enterasys IEEE802.1 Q-Bridge MIB EXT MIB
- Enterasys IEEE802.1 Spanning Tree MIB EXT MIB
- Enterasys Jumbo Ethernet Frame MIB
- Enterasys License Key MIB
- Enterasys License Key OIDS MIB
- Enterasys Link Flap MIB
- Enterasys MAC Authentication MIB
- Enterasys MAC Locking MIB
- Enterasys MAU MIB EXT MIB
- Enterasys MGMT Auth Notification MIB
- Enterasys MGMT MIB
- Enterasys MIB Names Definitions
- Enterasys Mirror Config
- Enterasys MSTP MIB
- Enterasys MULTI Auth MIB
- Enterasys MULTI Topology Routing MIB
- Enterasys MULTI User 8021X MIB
- Enterasys NETFLOW MIB (v5 & v9)
- Enterasys OIDS MIB Definitions
- Enterasys OSPFEXT MIB
- Enterasys PIM EXT MIB
- Enterasys PFC MIB EXT MIB
- Enterasys Policy Profile MIB
- Enterasys Power Ethernet EXT MIB
- Enterasys PTOPO MIB EXT MIB
- Enterasys PWA MIB
- Enterasys RADIUS ACCT Client EXTMIB
- Enterasys RADIUS AUTH Client MIB
- Enterasys Resource Utilization MIB
- Enterasys RIPv2 EXT MIB
- Enterasys RMON EXT MIB
- Enterasys SNTP Client MIB
- Enterasys Spanning Tee Diagnostics MIB
- Enterasys SYSLOG Client MIB
- Enterasys TACACS Client MIB
- Enterasys UPN-TC-MIB
- Enterasys VLAN Authorization MIB
- Enterasys VLAN Interface MIB
- Enterasys VRRP EXT MIB Definitions
- RSTP MIB
- U Bridge MIB
- USM Target Tag MIB
- SNMP REARCH MIB

Specifications

	K6	K10
Performance/Capacity		
Switching Fabric Bandwidth	280 Gbps	440 Gbps
Switching Throughput	190 Mpps (Measured in 64-byte packets)	299 Mpps (Measured in 64-byte packets)
Routing Throughput	190 Mpps (Measured in 64-byte packets)	299 Mpps (Measured in 64-byte packets)
Address Table Size	32,000 MAC Addresses	32,000 MAC Addresses
VLANs Supported	4,096	4,096
Transmit Queues	11	11
Classification Rules	8,196/chassis	8,196/chassis
Packet Buffering	3.0GB	4.5GB
Physical Specifications		
Chassis Dimensions (H x W x D)	H: 22.15 cm (8.719") W: 44.70 cm (17.60") D: 35.546 cm (14") 5U	H: 31.02 cm cm (12.219") W: 44.70 cm (17.60"") D: 35.546 cm (14") 7U
Host Memory and Flash	2GB DRAM 32MB flash memory	2GB DRAM 32MB flash memory
Environmental Specifications		
Operating Temperature	5 °C to +40 °C (41 °F to 104 °F)	5 °C to +40 °C (41 °F to 104 °F)
Storage Temperature	30 °C to +73 °C (-22 °F to 164 °F)	30 °C to +73 °C (-22 °F to 164 °F)
Operating Humidity	5% to 90% relative humidity, non-condensing	5% to 90% relative humidity, non-condensing
Power Requirements	100 to 125 VAC, 12 A or 200 to 250 VAC, 7.6 A; 50 to 60 Hz (Max per power supply)	100 to 125 VAC, 12 A or 200 to 250 VAC, 7.6 A; 50 to 60 Hz (Max per power supply)
Power over Ethernet Specifications		
System Power	• Automated or manual PoE power distribution • Per-port enable/disable, power level, priority safety, overload, and short-circuit protection • System power monitor • PoE Power: 400W per power supply (100 to 125 VAC) 2400W Max. 800W per power supply at (200 to 250 VAC) 4800W Max.	• Automated or manual PoE power distribution • Per-port enable/disable, power level, priority safety, overload, and short-circuit protection • System power monitor • PoE Power: 400W per power supply (100 to 125 VAC) 2400W Max. 800W per power supply at (200 to 250 VAC) 4800W Max.
Standards Compliance	• IEEE 802.3af • IEEE 802.3at	• IEEE 802.3af • IEEE 802.3at
Agency and Standard Specifications		
Safety	UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSA C22.2 No.60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Low Voltage Directive)	UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSA C22.2 No.60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Low Voltage Directive)
Electromagnetic Compatibility	FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (Class A). VCCI V-3. CNS 13438 (BSMI), 2004/108/EC (EMC Directive)	FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (Class A). VCCI V-3. CNS 13438 (BSMI), 2004/108/EC (EMC Directive)
Environmental	2002/95/EC (RoHS Directive), 2002/96/EC (WEEE Directive), Ministry of Information Order #39 (China RoHS)	2002/95/EC (RoHS Directive), 2002/96/EC (WEEE Directive), Ministry of Information Order #39 (China RoHS)

Ordering Information

Part Number	Description
K6 Chassis	
K6-Chassis	K-Series 6 Slot Chassis and Fan Tray
K6-FAN	K6 Fan Tray - Spare
K6-MID-KIT	K6 Mid-Mount Kit
K10 Chassis	
K10-Chassis	K-Series 10 Slot Chassis and Fan Tray
K10-FAN	K10 Fan Tray - Spare
K10-MID-KIT	K10 Mid-Mount Kit

Ordering Information

Part Number	Description
Power Supplies and Accessories	
K-AC-PS	K-Series Power Supply, 15A, 100-240VAC input, (600W system, 400/800W POE)
K-POE-4BAY	K-Series External 4 Bay Power Shelf
K-POE-4BAY-RAIL	Mounting Kit for K-POE-4BAY
K-POE-CBL-2M	K-Series PoE Power to K Chassis Cable - 2M
I/O Fabric Modules	
KK2008-0204-F2	K10 Management/Fabric Module (4) 10GB via SFP+
KK2008-0204-F2G	K10 Management/Fabric Module (4) 10GB via SFP+ (TAA Compliant)
KK2008-0204-F1	K6 Management/Fabric Module (4) 10GB via SFP+
KK2008-0204-F1G	K6 Management/Fabric Module (4) 10GB via SFP+ (TAA Compliant)
I/O Modules	
KT2006-0224	K-Series (24) Port 10/100/1000 802.3at RJ45 PoE IOM
KT2006-0224-G	K-Series (24) Port 10/100/1000 802.3at RJ45 PoE IOM (TAA Compliant)
KT2010-0224	K-Series (24) Port 10/100/1000 802.3at Mini-RJ21 PoE IOM
KT2010-0224-G	K-Series (24) Port 10/100/1000 802.3at Mini-RJ21 PoE IOM (TAA Compliant)
KG2001-0224	K-Series (24) Port 1Gb SFP IOM
KG2001-0224-G	K-Series (24) Port 1Gb SFP IOM (TAA Compliant)
KK2008-0204	K-Series (4) Port 10Gb SFP+ IOM
KK2008-0204-G	K-Series (4) Port 10Gb SFP+ IOM (TAA Compliant)
Licenses	
K-EOS-L3	Advanced Routing License (OSPF, VRF, PIM-SM)
K-EOS-PPC	K-Series Per Port User Capacity License Upgrade

Transceivers

Enterasys transceivers provide flexible connectivity options for Ethernet. All Enterasys transceivers meet the highest quality for extended life cycle and the best possible return on investment. For detailed specifications, compatibility and ordering information please go to http://www.enterasys.com/products/transceivers-ds.pdf.

Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible. K-Series switches come with the Enterasys lifetime warranty against manufacturing defects. For full warranty terms and conditions please go to: http://www.enterasys.com/support/warranty.aspx.

Service and Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

Additional Details

For additional information on the Enterasys K-Series please visit http://www.enterasys.com/products/switching/

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

Thought Leadership
Patented Innovation

enterasys® Secure Networks™

6070-1013

Delivering on our promises. On-time. On-budget.