DATA SHEET

C-Series C5

Gigabit Ethernet Stackable L2/L3/L4 Switch

BENEFITS

BUSINESS ALIGNMENT

- Aligns network resource utilization with business goals and priorities
- Reliable network operation for mission-critical applications

OPERATIONAL EFFICIENCY

- Management automation capabilities reduce network operational expenses
- Automatic discovery and deployment of VoIP services

SECURITY

- Ability to audit network for adherence to compliance regulations, such as PCI or HIPAA
- Network resources securely allocated according to user roles
- Network security maintained concurrently with user mobility

SUPPORT AND SERVICE

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training
- Comprehensive lifetime warranty, including feature upgrades and more

- Future-proofed with 802.3at high-power PoE and IPv6 routing support
- Automatic discovery and deployment of VoIP services
- High-availability stacking assures reliable network operations
- Automated management features reduce operational costs
- Investment protection via comprehensive lifetime warranty
- 2.11Tbps capacity and 809.5Mpps

Product Overview

The Extreme Networks C5 is a scalable, high-performance Gigabit Ethernet switch that provides support for the bandwidth-intensive and latency-sensitive requirements of today's demanding business applications. The C5 is an excellent choice for environments that require complete multi-layer switching capabilities and support for high density 10/100/1000 Ethernet ports and 10GE uplinks. The C5 also includes dynamic IPv4 and IPv6 routing and switching built into the hardware and policy-based automation capabilities for advanced edge deployments.

The C5 incorporates the new 802.3at high-power PoE on all ports, which translates into increased power provisioning for power-hungry devices such as Pan/Tilt/Zoom (PTZ) IP surveillance cameras, IP videophones, third party 802.11n access points and virtual desktops. Built-in high-power PoE support is a cost effective alternative for customers in place of purchasing separate PoE midspans, which can take away valuable rack space, add cost and contribute more cabling to the wiring closet.

The C5 provides high port density in a 1U footprint and is environmentally friendly by design. The C5's overall energy efficiency is further enhanced by a low current draw and an extreme tolerance for high environmental temperatures. A highly-scalable architecture and a comprehensive lifetime warranty ensure that a C5 network investment will sustain a secure, feature-rich and cost-effective network well into the future.

The C5's highly customizable Layer 2/3/4 packet classification capabilities work together with the 8 hardware-based priority queues associated with each Ethernet port to support a suite of differentiated services with as many as 8 distinct priority levels to provide guaranteed Quality of Service (QoS) for critical voice and video network traffic. In conjunction with its non-blocking L2 switching and L3 routing architecture, the C5's intelligent queuing mechanisms ensure that mission-critical applications receive prioritized access to network resources.

Reliability and Availability

The C5 design incorporates redundancy and failure protection mechanisms complete with automatic failover and recovery capabilities to provide a reliable network. An integral power supply is the primary source of power for the C5 and complete power redundancy is provided by an optional external power supply. The C5 redundant power supply provides load sharing, backup, or additive PoE power to a C5 stackable switch. With the power supply connected, the power requirement for the switch is equally shared by the two power supplies thereby stressing the power supplies less and increasing the lifetime and reliability of the power supplies.

A virtual switch can be created by interconnecting as many as eight C5s in a single stack, which can be managed via a single IP address with redundant management connections. The C5's closed-loop stacking capability utilizes bi-directional switch interconnects to maintain connectivity within the virtual switch despite any physical failures, which includes switches, cables and connections. Flexible Link Aggregation Groups (6 groups of 8, 12 groups of 4 or 24 groups of 2) are supported which allow multiple Ethernet ports (8, 4 or 2) to be grouped together to create a LAG. A LAG's Ethernet ports can be co-located on a single C5 or they can be distributed across multiple C5s within a stack to prevent a switch-level failure from disrupting data communications. The C5 also supports equal cost multipath protocol (ECMP) and virtual router redundancy protocol (VRRP) to strengthen its ability to quickly recover from a network failure. The C5 also includes Host CPU Protection support to help prevent Denial of Service (DoS) and BPDU attacks.

Advanced Quality of Service

Robust Quality of Service features enable strong support for integrated multimedia networks, as well as all types of data-intensive applications. The C5 is a standards-based solution optimized for multimedia applications, including VoIP, videoconferencing and real-time collaboration. The C5 uses multiple standards-based discovery methods with Extreme Networks policy capabilities to automatically identify and provision VoIP services for IP phones from all major vendors. C5 switches provide dynamic mobility for VoIP clients and reduce operating costs; 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 no manual administration required.

Advanced packet buffering on the C5 means less jitter on the network and a greater level of QoS for time-sensitive applications, such as VoIP and IP video, resulting in better network performance.

Security

The C5 enables strong network security by utilizing its authentication and security features, which can be applied at the port level or at the user level. Making use of the Extreme Network Management Suite's Policy Manager or a standard CLI, the Extreme Networks role-based architecture enables a network administrator to define distinct roles or profiles that represent operational groups within a business (e.g., employee, executive, guest, etc). Multiple users/devices per port can be authenticated via IEEE 802.1X, MAC address, or web authentication, and then assigned a pre-defined operational role. The C5 now supports increased password security via increased complexity, history tracking and aging. Passwords can now be encrypted using a FIPS 1402 approved algorithm.

Administrators can easily transition from RFC 3580 and complex access control list (ACL) deployments to the Extreme Networks role-based policy framework in a seamless fashion, without the need to make changes to their RADIUS infrastructure (e.g., adding filter-ID). In addition, the C5 also supports ACLs for supplementary network security. Network operations can be easily tailored to meet business-oriented requirements by providing each role with individualized access to network services and applications (e.g., a guest should have different network access privileges than an employee). Utilizing Extreme Networks role-based policy, administrators are able to manipulate DSCP and 802.1p rewrite for classification and prioritization of network traffic.

The C5 allows administrators even more network visibility, with the ability to audit their network for adherence to compliance regulations, such as PCI or HIPAA. The C5 is able to segment roles down to specific business functions, such as marketing, finance, HR or corporate, tailoring employee access to sensitive information.

The C5 switching line has also successfully completed the Department of Defense's Unified Capabilities (UC) Certification testing at the U.S. Army Technology Integration Center (TIC) in accordance with the Joint Interoperability Test Command (JITC) and is listed on the Unified Capabilities Approved Products List (UC APL). This important milestone means Extreme Networks' premier policy-enabled modular and stackable switches are now available for use in DoD critical infrastructure applications.

Investment Protection

The C5 is a cost-effective, feature-rich, stackable switch that provides a broad set of features today and will continue to deliver benefits well into the future. All C-Series products include a lifetime warranty that includes warranty and support services for which many competitors charge additional fees – adding up to 10% of initial deployment costs on an annual basis. Included benefits, such as advanced hardware return, firmware feature upgrades (which most vendors cover at most for 90 days) and telephone support (which most don't include or severely limit) combine to significantly decrease operational costs for customers over the life of their network. For more information regarding warranty terms and conditions please go to: http://www.extremenetworks.com/support/warranty.aspx.

Performance & Scalability

The C5, with support for 32,000 MAC addresses, provides scalable, wire-rate performance in support of the bandwidth-intensive and delay-sensitive requirements of today's demanding applications. Along with a switch capacity of 264 Gbps, the C5 provides up to 48 10/100/1000 Ethernet ports as well as 2 SFP+ ports, with the ability to support both 1GE and 10GE uplinks on the same port. Leveraging the C5's stacking capability, as many as 8 C5s (both 24-port and 48-port combinations) can be interconnected in a single stack to create a virtual switch that provides 2.11 Tbps of capacity and up to 384 10/100/1000 Ethernet ports as well as 16 10GE uplink ports.

Features / Standards and Protocols

MAC ADDRESS TABLE SIZE

32,000

VLANS

4,094 VLAN IDs
1,024 VLAN Entries per Stack

SWITCHING SERVICES PROTOCOLS

IEEE 802.1AB – LLDP
ANSI/TIA-1057 – LLDP-MED
IEEE 802.1D – MAC Bridges
IEEE 802.1s – Multiple Spanning Trees
IEEE 802.1t – 802.1D Maintenance
IEEE 802.1w – Rapid Spanning Tree Reconvergence
IEEE 802.3 – Ethernet
IEEE 802.3ab – GE over Twisted Pair
IEEE 802.3ad – Link Aggregation
IEEE 802.3ae – 10 Gigabit Ethernet (fiber)
IEEE 802.3af – PoE
IEEE 802.3at – High Power PoE (up to 30W per port)
IEEE 802.3i – 10Base-T
IEEE 802.3u – 100Base-T, 100Base-FX
IEEE 802.3z – GE over Fiber
Full/half duplex auto-sense support on all ports
IGMP Snooping v1/v2/v3
Jumbo Frame support (9,216 bytes)
Loop Protection
One-to-One and Many-to-One Port Mirroring
Port Description
Protected Ports
Selectable LAG Configuration (6 x 8, 12 x 4, 24 x 2)
Host CPU Protection – Broadcast/ Multicast/
Unknown Unicast Suppression
Spanning Tree Backup Root
STP Pass Thru

VLAN SUPPORT

Generic Attribute Registration Protocol (GARP)
Generic VLAN Registration Protocol (GVRP)
IEEE 802.1p – Traffic classification
IEEE 802.1Q – VLAN Tagging
Protocol-based VLANs with Extreme Networks Policy
IEEE 802.3ac – VLAN Tagging Extensions
Port-based VLAN (private port/private VLAN)
Tagged-based VLAN
VLAN Marking of Mirror Traffic
Standalone VLAN Association application for subnet, protocol and MAC based VLAN classification

SECURITY

ARP Spoof Protection
DHCP Spoof Protection
IEEE 802.1X Port Authentication
MAC-based Port Authentication
RADIUS Accounting for network access
RADIUS Client
IPsec for RADIUS transactions
RFC 3580 – IEEE 802.1X RADIUS Usage Guidelines
Multi-user Authentication
Pre-login banner
Password Protection (encrypted using a FIPS 1402 approved algorithm)
Secure Networks Policy
Secured Shell (SSHv2)
Secured Socket Layer (SSL)
User and IP Phone Authentication
Web-based Port Authentication
Auto Console Disconnect
Security Log
Secure Directory

IPV4 ROUTING

Standard Access Control List (ACLs)
Extended ACLs

VLAN-based ACLs
Service ACLs
MAC-based ACLs - not simultaneously supported with policy
ARP & ARP Redirect
DVMRP
IP Helper Address
OSPF Passive Interface
VRRP master-icmp-reply
RFC 826 – Ethernet ARP
RFC 1058 – RIP v1
RFC 1256 – ICMP Router Discovery Messages
RFC 1519 Classless Inter-Domain Routing
RFC 1724 – RIPv2 MIB Extension
RFC 2236 – IGMPv2
RFC 2328 – OSPF version 2
RFC 2338 – IP Redundancy VRRP
RFC 2362 – PIM-SM
RFC 2453 – RIP v2
RFC 3046 – DHCP/BootP Relay
RFC 3376 – IGMPv3
RFC 3768 – Virtual Router Redundancy Protocol Static Routes

IPV6 ROUTING

IPv6 ACLs - not simultaneously supported with policy
RFC 1981 – Path MTU for IPv6
RFC 2373 – IPv6 Addressing
RFC 2460 – IPv6 Protocol Specification
RFC 2461 – Neighbor Discovery
RFC 2462 – Stateless Autoconfiguration
RFC 2463 – ICMPv6
RFC 2464 – IPv6 over Ethernet
RFC 2473 – Generic Packet Tunneling in IPv6
RFC 2271 – SNMP Framework MIB
RFC 2711 – IPv6 Router Alert
RFC 2740 – OSPFv3
RFC 2893 – Transition Mechanisms for
IPv6 Hosts and Routers (6 over 4 configured)
RFC 3315 – DHCPv6 (stateless + relay)
RFC 3484 – Default Address Selection for IPv6
RFC 3493 – Basic Socket Interface for IPv6
RFC 3513 – Addressing Architecture for IPv6
RFC 3542 – Advanced Sockets API for
RFC 3587 – IPv6 Global Unicast Address Format
RFC 3736 – Stateless DHCPv6
Dual IPv4/IPv6 TCP/IP Stack
RFC 4007 - IPv6 Scoped Address Architecture
RFC 4291 - IPv6 Addressing Architecture

MIB SUPPORT

Extreme Networks Entity MIB
Extreme Networks Policy MIB
Extreme Networks VLAN Authorization MIB
Extreme Networks Spanning Tree Diagnostic MIB
ANSI/TIA-1057 – LLDP-MED MIB
IEEE 802.1AB – LLDP MIB
IEEE 802.1X MIB – Port Access
IEEE 802.3ad MIB – LAG MIB
RFC 826 – ARP and ARP Redirect
RFC 951, RFC 1542 – DHCP/
BOOTP Relay
RFC 1213 – MIB/MIB II
RFC 1493 – BRIDGE-MIB
RFC 1643 – Ethernet-like MIB
RFC 1724 – RIPv2 MIB Extension
RFC 1850 – OSPF MIB
RFC 2096 – IP Forwarding Table MIB
RFC 2131, RFC 3046 – DHCPClient/Relay
RFC 2233 – IF-MIB
RFC 2465 – IPv6 MIB
RFC 2466 – ICMPv6 MIB
RFC 2571 – SNMP Framework MIB
RFC 2618 – RADIUS Authentication Client MIB
RFC 2620 – RADIUS Accounting Client MIB
RFC 2668 – Managed Object Definitions for 802.3 MAUs
RFC 2674 – P-BRIDGE-MIB
RFC 2674 – QBRIDGE-MIB VLAN Bridge MIB
RFC 2737 – Entity MIB (physical branch only)
RFC 2787 – VRRP-MIB
RFC 2819 – RMON-MIB
RFC 2933 – IGMP MIB
RFC 2934 – PIM MIB for IPv4
RFC 3413 – SNMP v3 Applications MIB
RFC 3414 – SNMP v3 User-based
Security Module (USM) MIB
RFC 3584 – SNMP Community MIB
RFC 3621 – Power over Ethernet MIB

QUALITY OF SERVICE

8 Priority Queues per Port
802.3x Flow Control
Class of Service (CoS)
Ingress Rate Limiting
IP ToS/DSCP Marking/Remarking
IP Precedence
IP Protocol
Layer 2/3/4 Classification
Multi-layer Packet Processing
Mixed Queuing Control – Strict and Weighted
Round Robin
Source/Destination IP Address
Source/Destination MAC Address
Dynamic and Static MAC Locking
EAP Pass-Thru
RFC 2474 Definition of Differentiated Services Field

MANAGEMENT

Alias Port Naming
Command Line Interface (CLI)
Configuration Upload/Download
Dual IPv4/IPv6 Management Support
Editable Text-based Configuration File
TFTP Client
Command Logging
Multi-configuration File Support
NMS Automated Security Manager
NMS Console
NMS Inventory Manager
NMS Policy Manager
Node/Alias Table
RFC 768 – UDP
RFC 783 – TFTP
RFC 791 – IP
RFC 792 – ICMP
RFC 793 – TCP
RFC 826 – ARP
RFC 854 – Telnet
RFC 951 – BootP
RFC 1157 – SNMP
RFC 1321 – The MD5 Message-Digest Algorithm
RFC 1901 – Community-based SNMPv2
RFC 2030 Simple Network Time Protocol (SNTP)
RFC 2933 – IGMP MIB
RFC 3176 – sFlow
RFC 3413 – SNMPV3 Applications
RFC 3414 –User-based Security Module (USM) for SNMPv3
RFC 3415 – View-based Access Control Model for SNMP
RFC 3826 – Advanced Encryption
Standard (AES) for SNMP
RMON (Stats, History, Alarms, Events, Filters, Packet Capture)
Secure Copy (SCP)
Secure FTP (SFTP)
Simple Network Management Protocol
(SNMP) v1/v2c/v3
SSHv2
RFC 3164 – The BSD Syslog Protocol
TACACS+ support
Authentication, Authorization and Auditing
Web-based Management
Webview via SSL Interface

Switch Model Specifications

	C5G124-24	C5G124-24P2	C5G124-48	C5G124-48P2
PERFORMANCE				
Throughput Capacity wire-speed Mpps (switch / stack)	35.7 Mpps / 285.7 Mpps	35.7 Mpps / 285.7 Mpps	71.4 Mpps / 571.4 Mpps	71.4 Mpps / 571.4 Mpps
Switching Capacity (switch / stack)	48 Gbps (35.7 Mpps) / 384 Gbps (285.7 Mpps)	48 Gbps (35.7 Mpps) / 384 Gbps (285.7 Mpps)	96 Gbps (71.4 Mpps) / 768 Gbps (571.4 Mpps)	96 Gbps (71.4 Mpps) / 768 Gbps (571.4 Mpps)
Stacking Capacity (switch / stack)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)
Aggregate Throughput Capacity (switch / stack)	176 Gbps (130.9 Mpps) / 1,408 Gbps (1,047.5 Mpps)	176 Gbps (130.9 Mpps) / 1,408 Gbps (1,047.5 Mpps)	224 Gbps (166.6 Mpps) / 1,792 Gbps (1,333.2 Mpps)	224 Gbps (166.6 Mpps) / 1,792 Gbps (1,333.2 Mpps)
POE SPECIFICATIONS				
802.3af Interoperable	N/A	Yes	N/A	Yes
802.3at Interoperable	N/A	Yes	N/A	Yes
System Power	N/A	850 watts per switch with up to 30 watts per port Per-port switch power monitor: • Enable/disable • Priority safety • Overload & short circuit protection	N/A	850 watts per switch with up to 30 watts per port Per-port switch power monitor: • Enable/disable • Priority safety • Overload & short circuit protection
PHYSICAL SPECIFICATIONS				
Dimensions (H x W x D)	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")
Net Weight	5.03 kg (11.10 lb)	6.21 kg (13.70 lb)	5.42 kg (11.95 lb)	6.60 kg (14.55 lb)
MTBF	395,557 hours	289,425 hours	311,897 hours	229,532 hours
Physical Ports	• (24) 10/100/1000 auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (4) Combo SFP ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port	• (24) 10/100/1000 PoE (.af+.at) auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (4) Combo SFP ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port	• (48) 10/100/1000 auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (4) Combo SFP ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port	• (48) 10/100/1000 PoE (.af+.at) auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (4) Combo SFP ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port
POWER REQUIREMENTS				
Normal Input Voltage	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC
Input Frequency	50 – 60 Hz	50 – 60 Hz	50 – 60 Hz	50 – 60 Hz
Input Current	2 A Max	12 A Max	2 A Max	12 A Max
Power Consumption	65 watts	125 watts	101 watts	150 watts

Switch Model Specifications (cont.)

	C5G124-24	C5G124-24P2	C5G124-48	C5G124-48P2
TEMPERATURE				
IEC 6-2-1 Standard Operating Temperature	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)
IEC 6-2-14 Non-Operating Temperature	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)
Heat Dissipation	222 BTUs/Hr	428 BTUs/Hr	345 BTUs/Hr	513 BTUs/Hr
HUMIDITY				
Operating Humidity	5% - 95% non-condensing	5% - 95% non-condensing	5% - 95% non-condensing	5% - 95% non-condensing
VIBRATION				
	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36
SHOCK				
	IEC 68-2-29	IEC 68-2-29	IEC 68-2-29	IEC 68-2-29
DROP				
	IEC 68-2-32	IEC 68-2-32	IEC 68-2-32	IEC 68-2-32
ACOUSTICS				
Front of switch (normal operation)	44 dB	45.5 dB	46 dB	45.5 dB
ALTITUDE				
Operating	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)
Non-operating	15,000 ft (4,572 m)	15,000 ft (4,572 m)	15,000 ft (4,572 m)	15,000 ft (4,572 m)
AGENCY AND REGULATORY STANDARD SPECIFICATIONS				
Safety	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1
EMC	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3
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)	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)

Switch Model Specifications (cont.)

	C5K125-24	C5K125-24P2	C5K125-48	C5K125-48P2	C5K175-24
PERFORMANCE					
Throughput Capacity wire-speed Mpps (switch / stack)	65.5 Mpps / 523.8 Mpps	65.5 Mpps / 523.8 Mpps	101.2 Mpps / 809.5 Mpps	101.2 Mpps / 809.5 Mpps	65.5 Mpps / 523.8 Mpps
Switching Capacity (switch / stack)	88 Gbps (65.5 Mpps) / 704 Gbps (523.8 Mpps)	88 Gbps (65.5 Mpps) / 704 Gbps (523.8 Mpps)	136 Gbps (101.2 Mpps) / 1,088 Gbps (809.5 Mpps)	136 Gbps (101.2 Mpps) / 1,088 Gbps (809.5 Mpps)	88 Gbps (65.5 Mpps) / 704 Gbps (523.8 Mpps)
Stacking Capacity (switch / stack)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)	128 Gbps (95.2 Mpps) / 1,024 Gbps (761.8 Mpps)
Aggregate Throughput Capacity (switch / stack)	216 Gbps (160.7 Mpps) / 1,728 Gbps (1,285.6 Mpps)	216 Gbps (160.7 Mpps) / 1,728 Gbps (1,285.6 Mpps)	264 Gbps (196.4 Mpps) / 2,112 Gbps (1,571.3 Mpps)	264 Gbps (196.4 Mpps) / 2,112 Gbps (1,571.3 Mpps)	216 Gbps (160.7 Mpps) / 1,728 Gbps (1,285.6 Mpps)
POE SPECIFICATIONS					
802.3af Interoperable	N/A	Yes	N/A	Yes	N/A
802.3at Interoperable	N/A	Yes	N/A	Yes	N/A
System Power	N/A	850 watts per switch with up to 30 watts per port Per-port switch power monitor: • Enable/disable • Priority safety • Overload & short circuit protection	N/A	850 watts per switch with up to 30 watts per port Per-port switch power monitor: • Enable/disable • Priority safety • Overload & short circuit protection	N/A
PHYSICAL SPECIFICATIONS					
Dimensions (H x W x D)	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")	H: 4.4 cm (1.73") W: 44.1 cm (17.36") D: 36.85 cm (14.51")
Net Weight	4.92 kg (10.85 lb)	6.10 kg (13.45 lb)	5.31 kg (11.70 lb)	6.49 kg (14.30 lb)	4.97 kg (10.95 lb)
MTBF	365,615 hours	273,083 hours	284,345 hours	213,965 hours	395,839 hours
Physical Ports	• (24) 10/100/1000 auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (2) Combo SFP ports • (2) SFP+ ports • (2) dedicated stacking ports • DB9 console port • (1) RPS port	• (24) 10/100/1000 PoE (.af + .at) auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (2) Combo SFP ports • (2) SFP+ ports • (2) dedicated stacking ports • DB9 console port • (1) RPS port	• (48) 10/100/1000 auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (2) Combo SFP ports • (2) SFP+ ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port	• (48) 10/100/1000 PoE (.af + .at) auto-sensing, auto-negotiating MDI/MDI-X RJ45 ports • (2) Combo SFP ports • (2) SFP+ ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port	• (24) SFP • (2) SFP+ ports • (2) dedicated stacking ports • (1) DB9 console port • (1) RPS port
POWER REQUIREMENTS					
Normal Input Voltage	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC	100 - 240 VAC
Input Frequency	50 – 60 Hz	50 – 60 Hz	50 – 60 Hz	50 – 60 Hz	50 – 60 Hz
Input Current	2 A Max	12 A Max	2 A Max	12 A Max	2 A Max
Power Consumption	74 watts	130 watts	120 watts	165 watts	69 watts
TEMPERATURE					
IEC 6-2-1 Standard Operating Temperature	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)	0° to 50° C (32° to 122° F)
IEC 6-2-14 Non-Operating Temperature	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)	-40° to 70° C (-40° to 158° F)
Heat Dissipation	253 BTUs/Hr	445 BTUs/Hr	408 BTUs/Hr	565 BTUs/Hr	234 BTUs/Hr
HUMIDITY					
Operating Humidity	5% - 95% non-condensing	5% - 95% non-condensing	5% - 95% non-condensing	5% - 95% non-condensing	5% - 95% non-condensing
VIBRATION					
	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36	IEC 68-2-6, IEC68-2-36
SHOCK					
	IEC 68-2-29	IEC 68-2-29	IEC 68-2-29	IEC 68-2-29	IEC 68-2-29
DROP					
	IEC 68-2-32	IEC 68-2-32	IEC 68-2-32	IEC 68-2-32	IEC 68-2-32

Switch Model Specifications (cont.)

	C5K125-24	C5K125-24P2	C5K125-48	C5K125-48P2	C5K175-24
ACOUSTICS					
Front of switch (normal operation)	45 dB	45.5 dB	47 dB	46 dB	46 dB
ALTITUDE					
Operating	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)
Non-operating	15,000 ft (4,572 m)	15,000 ft (4,572 m)	15,000 ft (4,572 m)	15,000 ft (4,572 m)	15,000 ft (4,572 m)
AGENCY AND REGULATORY STANDARD SPECIFICATIONS					
Safety	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1	UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1
EMC	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3	FCC Part 15 (Class A), ICES-003 (Class A), BSMI, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, and EN 61000-3-3
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)	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)	2002/95/EC (RoHS Directive), 2002/96/EC (WEEE Directive), Ministry of Information Order #39 (China RoHS)

Redundant Power Supply Equipment Specifications

STK-RPS-1005CH3 POWER SHELF

Power Supply Slots: 3

Dimensions (H x W x D)*

5.5 cm (2.2") x 44.0 cm (17.3") x 35.1 cm (13.8")

Weight

0.95 kg (2.09 lbs)

STK-RPS-150CH2 POWER SHELF

Power Supply Slots: 2

Dimensions (H x W x D)*

5.5 cm (2.2") x 44.0 cm (17.3") x 18.0 cm (7.0")

Weight

5.27 kg (11.6 lbs)

STK-RPS-150CH8 POWER SHELF

Power Supply Slots: 8

Dimensions (H x W x D)*

22.26 cm (8.77") x 44.0 cm (17.3") x 26.4 cm (10.4")

Weight

5.27 kg (11.6 lbs)

*Note: dimensions include integrated rack mount ears

STK-RPS-150PS POWER SUPPLY

Dimensions (H x W x D)

19.6 cm (7.7") x 5.2 cm (2.04") x 25.7 cm (10.1")

Net Weight (Unit Only)

1.75 kg (3.85 lbs)

Gross Weight (Packaged Unit)

3.20 kg (7.04 lbs)

MTBF

300,000 hours

Operating Temperature

0° C to 50° C (32° F to 122° F)

Storage Temperature

-30° C to 73° C (-22° F to 164° F)

Operating Relative Humidity

5% to 95%

AC Input Frequency Range

50 – 60 Hz

AC Input Voltage Range

100 – 240 VAC

Maximum Output Power

156 W continuous

STK-RPS-1005PS POWER SUPPLY

Dimensions (H x W x D)*
4.3 cm (1.7”) x 15.4 cm (6.06”) x 34.0 cm (13.39”)

Net Weight (Unit Only)
2.1 kg (4.63 lb)

Gross Weight (Packaged Unit)
3.53 kg (7.77 lb)

MTBF
800,000 hours

Operating Temperature
0° C to 50° C (32° F to 122° F)

Storage Temperature
-40° C to 70° C (-40° F to 158° F)

Operating Relative Humidity
5% to 95%

AC Input Frequency Range
50-60 Hz

AC Input Voltage Range
100 - 240 VAC

Maximum Output Power
1005 W continuous

Ordering Information

PART NUMBER	DESCRIPTION
C5 SWITCHES	
C5G124-24	(24) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
C5G124-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports
C5G124-48	(48) 10/100/1000 RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
C5G124-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (4) combo SFP ports, (2) dedicated high-speed dedicated stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports
C5K125-24	(24) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K125-24P2	(24) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K125-48	(48) 10/100/1000 RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K125-48P2	(48) 10/100/1000 PoE (.at + .af) RJ45 ports, (2) combo SFP ports, (2) SFP+, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (48) Gigabit ports + (2) 1GE or 10GE SFP+ ports
C5K175-24	(24) SFP, (2) SFP+ ports, (2) dedicated high-speed stacking ports and external RPS connector. Total active ports per switch: (24) SFP, (2) 1GE or 10GE SFP+ ports
OPTIONAL SOFTWARE LICENSES	
C5L3-LIC	C5 advanced IPv4 (OSPF, PIM-SM, DVMRP and VRRP) and IPv6 routing licensing (OSPF) (per switch)
CABLES	
STK-RPS-1005CH3	3-slot modular power supply chassis (power supply STK-RPS-1005PS sold separately)
STK-RPS-1005PS	1005W 802.3at PoE redundant power supply with load-balancing support
STK-RPS-150CH2	2-slot modular power supply shelf (power supply STK-RPS-150PS sold separately)
STK-RPS-150CH8	8-slot modular power supply shelf (power supply STK-RPS-150PS sold separately)
STK-RPS-150PS	150W non-PoE redundant power supply

Transceivers

Extreme Networks transceivers provide connectivity options for Ethernet over twisted pair copper and fiber optic cables with transmission speeds from 100 Megabits per second to 10 Gigabits per second. The Extreme Networks C5 includes SFP+ transceivers that can support both 10GE and 1GE transceivers. All Extreme Networks 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.extremenetworks.com/products/transceivers-ds.pdf.

Warranty

As a customer-centric company, Extreme Networks 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. C-Series switches come with the Extreme Networks lifetime warranty against manufacturing defects. For full warranty terms and conditions please go to: www.extremenetworks.com/support/warranty.aspx.

Service and Support

Extreme 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 Extreme Networks account executive for more information about Extreme Networks Service and Support.

Extreme networks

http://www.ExtremeNetworks.com/contact / Phone +1-408-579-2800

DATA SHEET

Extreme S-Series®

Terabit-class, Convergence-ready, Modular Switch for Edge-to-Core and Data Deployments

Extreme Networks S-Series Highlights

Terabit-class performance with granular traffic visibility and control

Automated network provisioning for virtualized, cloud, and converged voice/video/data environments

High availability redundancy features including self-healing, maximizes business continuity for critical applications

Versatile high density solution with highly flexible connectivity and power options reduces cost of ownership

Built-in hardware support for 40Gb and 100 Gbps Ethernet, emerging protocols (IPv6) and large scale deployment protocols (MPLS)

Greater than 9.5 Tbps backplane capacity with 2.56 Tbps switching capacity and 1920 Mpps throughput

Product Overview

The Extreme Networks S-Series family of flow-based switches brings high performance distributed switching to the network access layer, distribution layer, enterprise/campus core, and data center. The S-Series family consists of the 8-slot S8, 6-slot S6, 4-slot S4, 3-slot S3, 1-slot S1A chassis and the fixed configuration S-Series Stand Alone (SSA). The S-Series delivers some of the highest switching port densities per rack unit available in the market and is future-proofed and scalable to provide overall system capacities of up to nine and a half Terabits. All chassis support 802.3af and 802.3at (high power) standards-based PoE via an integrated or field installable power system. There are a variety of I/O modules designed and optimized for deployment at the network access layer, distribution layer, network core and data center that provide a broad array of connectivity options for copper and fiber cabling infrastructures.

The S-Series provides a highly resilient distributed switching and routing architecture withmanagement and control functions embedded in each module, delivering unsurpassed reliability, scalability, and fault tolerance. Organizations can cost-effectively add connectivity as needed while scaling performance capacity with each new module. The highly available architecture 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 datacenter and campus 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 S-Series implements our custom packet processor technology, CoreFlow2, which provides 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 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.

S-Series policy rules combined with deep packet inspection can intelligently identify and automatically respond to security threats while improving reliability and quality of the user experience.

A significant differentiator for the S-Series is the ability to collect NetFlow data at wire-speed on every port, providing total visibility into network resource consumption for users and applications. The S-Series is the only enterprise switch to support multi-user, multi-method 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. When quality of service, device and application prioritization and security matters, there is no better choice than the Extreme Networks S-Series.

FORWARDING PARADIGM

The Extreme Networks S-Series chassis utilize both fabric-based point-to-point and fabric-less meshed forwarding architectures. The S1A, S4, S6, and S8 chassis use a fabric-based forwarding architecture that provides multiple high bandwidth data paths between I/O modules, while the S3 chassis provides a high performance, fabric-less meshed forwarding architecture ideally suited for highly available network edge wiring closet deployments. All chassis are optimized for redundant high performance switching and routing as well as providing flexible connectivity and the ability to add features and scale performance as required and as new technologies become available.

I/O fabric modules provide scalable, high performance data paths as well as a full complement of front panel interfaces with flexible modular interface options. A single I/O fabric may be used in either an S1A, S4, S6, or an S8 chassis, however, the use of two I/O fabrics creates a load sharing fabric pair that provides up to 2560 Gbps switching capacity and adds high-availability features. The S8 and S6 chassis augments the load sharing fabric pair by allowing the addition of a third I/O fabric module, increasing the system reliability and performance in the unlikely event of an I/O fabric failure. An S8 or S6 system with two I/O fabrics installed will gracefully reduce the fabric switching capacity by 50 percent, in the event of an I/O fabric failure, however, when a third I/O fabric is installed, the system will maintain a full 2560 Gbps of switching performance. The load sharing fabric architecture ensures the highest availability and performance for the most demanding and mission-critical networks.

Performance and Port Density Specification

	SSA130	SSA150	SSA180	S1	S3	S4	S6	S8
CHASSIS SLOTS				1	3	4	6	8
System Switching Capacity	40 Gbps	120 Gbps	120 Gbps	320 Gbps	360 Gbps	1.28 Tbps	1. 92 Tbps	2.56 Tbps
System Switching Throughput	30 Mpps	90 Mpps	90 Mpps	240 Mpps	360 Mpps	960 Mpps	1440 Mpps	1920 Mpps
Total Backplane Capacity				320 Gbps	525 Gbps	3 Tbps	7 Tbps	9.5 Tbps
Maximum 10/100/1000 Base-TX Class 3 PoE or 1000Base-X SFP (MGBIC) ports per system	48	48	48 (No PoE)	72	216	288	432	576
Maximum 10GBase-X SFP+ ports per system	4	4	4	24	96	112	168	232
Maximum 40GBase-X QSFP+ ports per system				6		24	36	48

I/O Module Specification

	S130 CLASS MODULES		S140 I/O MODULES				S180 I/O MODULES		
	WIRING CLOSET, DISTRIBUTION LAYER, SMALL NETWORK CORE		WIRING CLOSET, DISTRIBUTION LAYER, SMALL NETWORK CORE				DISTRIBUTION LAYER, SERVER AGGREGATION,		
Part Number	ST4106-0248	SG4101-0248	ST2206-0848	SG2201-0848	SK2008-0832	SK2009-0824	SK8008-1224	SK8009-1224	SL8013-1206
Used in	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S3/S4/S6/S8 Chassis	S4/S6/S8 Chassis	S4/S6/S8 Chassis	S4/S6/S8 Chassis
Port Type	RJ45	SFP	RJ45	SFP	SFP+	10GBase-T	SFP+	10GBase-T	QFSP+
Port Quantity	48	48	48	48	32	24	24	24	6
Port Speed	10/100/1000 Gbps	1000 Gbps	10/100/1000 Gbps	1000 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps	40 Gbps
PoE Support	802.3af, 802.3at		802.3af, 802.3at						
Option Module Slots	1, (Type 1)	1, (Type 1)	2, (Type 2)	2, (Type 2)					
Module I/O Throughput	30 Mpps	30 Mpps	120 Mpps	120 Mpps	120 Mpps	120 Mpps	240 Mpps	240 Mpps	240 Mpps
I/O Switching Capacity	40 Gbps	40 Gbps	160 Gbps	160 Gbps	160 Gbps	160 Gbps	320 Gbps	320 Gbps	320 Gbps

Distributed, Flow-Based Architecture

In order to ensure granular visibility and manage traffic without sacrificing performance, the Extreme Networks S-Series implements our CoreFlow2 distributed, flow-based 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 I/O modules and I/O fabric modules. 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 CoreFlow2 ASICs without any further processing. In this way the Extreme Networks S-Series is able to apply a very granular level of control to each flow at full line rate.

I/O Module Specification

	S130 CLASS FABRIC MODULES	S180 CLASS I/O FABRIC MODULES					
	WIRING CLOSET, DISTRIBUTION LAYER, SMALL NETWORK CORE	DISTRIBUTION LAYER, SERVER AGGREGATION, DATA CENTER CORE, ENTERPRISE					
Part Number	ST4106-0348-F6	ST8206-0848-F8	SG8201-0848-F8	SK8008-1224-F8	SK8208-0808-F8	SK8009-1224-F8	SL8013-1206-F8
Used in	S1A/S4/S6/S8 Chassis	S1A/S4/ S6/S8 Chassis	S1A/S4/ S6/S8 Chassis	S1A/S4/ S6/S8 Chassis	S1A/S4/ S6/S8 Chassis	S1A/S4/ S6/S8 Chassis	S1A/S4/ S6/S8 Chassis
Port Type	RJ45	RJ45	SFP	SFP+	SFP+	10GBase-T	QSFP+
Port Quantity	48	48	48	24	8	24	6
Port Speed	10/100/1000 Gbps	10/100/1000 Gbps	1000 Gbps	10 Gbps	10 Gbps	10 Gbps	40 Gbps
PoE Support	802.3af, 802.3at	802.3af, 802.3at					
Option Module Slots	1, (Type 2)	2, (Type 2)	2, (Type 2)		2, (Type2)		
Module I/O Throughput	45 Mpps	120 Mpps	120 Mpps	240 Mpps	120 Mpps	240 Mpps	240 Mpps
I/O Switching Capacity	60 Gbps	160 Gbps	160 Gbps	320 Gbps	160 Gbps	320 Gbps	320 Gbps
Fabric Throughput (Each)	480 Mpps	960 Mpps	960 Mpps	960 Mpps	960 Mpps	960 Mpps	960 Mpps
Fabric Throughput (Load Sharing Pair)	960 Mpps	1920 Mpps	1920 Mpps	1920 Mpps	1920 Mpps	1920 Mpps	1920 Mpps

SYSTEM SUMMARY

Extreme Networks S-Series I/O modules are high performance, fully-featured switch routers that deliver a fully distributed switching system as well as management and route processing capabilities, where each module is individually driven and managed by on-board processors. Extreme Networks CoreFlow2 ASICs, together with firmware microprocessors, create a traffic control solution that delivers high performance and flexibility. This distributed ASIC-based architecture increases processing power as modules are added for a higher level of scalability and flexibility.

I/O fabrics and I/O modules are available with a wide array of interface types and port densities (10/100/1000BASE-TX, 1000BASE SFP, 10GBASE SFP+, 10GBASE-T and 40GBASE QSFP+) to address varied network requirements. All triple speed copper I/O modules are PoE-enabled. A number of I/O modules also include either one or two option-module slots; an option-module slot provides additional media and port speed connectivity via triple speed copper, Gigabit SFP, 10 Gigabit SFP+ or a combination of gigabit and SFP+ Ethernet ports. This further simplifies network design and reduces the cost of network deployments. All S-Series I/O Fabrics and I/O Modules include deep packet buffers per port to avoid dropped packets in the event of network congestion.

All S-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.

S180 CLASS I/O AND I/O FABRIC MODULES

The S180 class is designed to support the most demanding areas of the network where sustained high volumes of traffic are most common. Both 10 Gigabit and 40 Gigabit Ethernet modules incorporate advanced traffic management mechanisms and large packet buffers to ensure optimal network performance, predictability and reliability. The S180 Class is optimized for 10Gb and 40Gb Ethernet aggregation and the rigorous requirements of enterprise network core and data center. These modules support the full range of Extreme Networks OneFabric, CoreFlow2 features and advanced switching and routing without the need for additional licensing. The S180 class includes support for Virtual Switch Bonding via dedicated VSB SFP+ ports, which simplifies network virtualization functionality for the S-Series product lines. Dedicated VSB ports and support for Data Center Bridging protocols enable scalable virtual services in a data center environment.

S140 CLASS I/O MODULES

The S140 class delivers a high performance, mid-tier switching solution that provides increased density and a lower-cost alternative in 10G aggregation scenarios. These modules offer the option for a high density, fabric-less aggregation solution by deploying gigabit and 10 Gigabit aggregation in the S3 chassis. The S140 class also provides high performance SFP and triple-speed with media flexibility and support for IEEE 802.3af PoE and IEEE 802.3at high power PoE standards. The S140 modules provide the gigabit aggregation connectivity for the S180 class chassis configurations. Dedicated VSB ports via Option Module and support for Data Center Bridging protocols enable scalable virtual services in a data center environment.

S130 CLASS I/O MODULES

S130 class I/O modules are optimized for use in wiring closets for user connectivity, in the distribution layer to aggregate edge switches and in small and medium network cores. These modules provide high density with media flexibility and support for IEEE 802.3af PoE and IEEE 802.3at high power PoE standards. S130 class I/O modules deliver scalable triple speed performance and flexibility to ensure compatibility with today's high performance workstations, as well as legacy devices, while providing the highest levels of QoS, security, and bandwidth control via flow-based switching.

S130 class I/O modules include a unique feature that enables full line rate forwarding for bandwidth hungry workstations or when downstream switches are connected. Flex-Edge technology provides line rate forwarding through the switch even when the systems uplinks are in an oversubscribed state. This ensures that critical and time sensitive data passes through the switch to its destination at line rate, unlike inefficient methods used by other solutions on the market.

S130 class I/O modules support up to 512 users with up to eight authenticated users per port in contrast to S140/S180 class modules which support up to 1,024 users/devices per module with no restriction to the number of users per port. In cases where an S130 class I/O module needs to support more than 8 authenticated users per port, a software upgrade license may be purchased and applied to the module that enables this capability. The S-EOS-PPC license is required for each S130 class I/O module that requires 8 users per port restriction removed. Only one S-EOS-PPC license is required for the S130 class SSA switch.

Performance/Capacity

Switching Fabric Bandwidth

2560 Gbps Load Sharing Fabric Pair

Switching Throughput

1920 Mpps

(Measured in 64-byte packets)

IPv4/IPv6 Routing Throughput

1920 Mpps

(Measured in 64-byte packets) (Capacities above are for an S8 System)

Address Table Size

128K MAC Addresses

VLANs Supported

4094

Transmit Queues

12 for S130, SSA130/SSA150

16 for S180/S140, SSA180

Classification Rules

57K per chassis

Main Memory

S130, SSA130:

1 GB Per Module

S140/S180, SSA180/SSA150A:

2 GB Per Module

Flash Memory: 1 GB Per Module

Packet Buffering

Chassis Buffer Size (Max.)

S1	3 GB
S3	6 GB
S4	12 GB
S6	18 GB
S8	24 GB
SSA130 Class	1.0 GB
SSA150/180 Class	1.5 GB

(Actual chassis buffering capacity is dependent on the modules classes installed)

HIGH AVAILABILITY HW FEATURES

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

High Availability Summary:

- Passive chassis backplanes S1A, S3, S4, S6, S8 chassis
- Meshed backplane architecture in the S3 chassis
- Hot swappable fan trays with multiple cooling fans
- Separate system and PoE power supplies
- Hot swappable power supplies
- Multiple AC input connections for power circuit redundancy
- Load sharing/redundant I/O fabrics S4, S6, and S8 chassis
- N+1 fabric redundancy in the S8 and S6 chassis
- Hot swappable I/O fabrics and I/O modules
- Multiple host CPU for N+X redundancy
- Virtual Switch Bonding

FEATURE-RICH FUNCTIONALITY

Examples of additional functionality and features that are supported in the Extreme S-Series.

Features Summary:

- Multi-user, Multi-method Authentication and Policy per port
- Line Rate, non-sampled Netflow (v5/v9)
- Server Load Balancing (LSNAT)
- Network Address Translation (NAT)
- Generic Route Encapsulation (GRE)
- Flow Setup Throttling (FST)
- Flex-Edge Technology
- High Availability Firmware Upgrades (HAU)
- Anti-Spoofing Protection and User tracking
- Virtual Private Port Service (GRE with Layer 2)
- Fabric Routing with IP Host Mobility
- Application Policy Controls (Bonjour, uPNP)
- Remote Port and Flow Mirrors
- Policy driven mirrors
- Layer 2 MAC Access Control Lists
- RADIUS Server Load Balancing
- DHCP Server (IPv4/IPv6)
- IPSLA

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 64 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)
  - 802.1Qbb PFC (Priority Flow Control)
  - 802.1Qau Congestion Notification
- MLD IPv6 Snooping and Querier
- Virtual Switch Bonding (VSB)
- Anti-Spoofing Suite
  - DHCP Snooping
  - Dynamic Arp Inspection (DAI)
  - IP Source Guard

IP/ROUTING FEATURES

- Static Routes
- Standard ACLs
- OSPF with Multipath Support
- OSPF Passive Interfaces
- IPv6 Routing Protocol
- Extended ACLs
- Policy-based Routing
- NAT Network Address Translation
- TWCB Transparent Web Cache Redirect
- VRF Virtual Routing and Forwarding (IPv6 and IPv4)
- Border Gateway Routing Protocol - BGPv4
- 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 922 Broadcasting IP datagrams over subnets
- RFC 925 Multi-LAN Address Resolution
- RFC 950 Internet Standard Subnetting Procedure
- 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 a nd Support
- RFC 1157 Simple Network Management Protocol

Features/Standards and Protocols (cont.)

- 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 1265 BGP Protocol Analysis
- RFC 1266 Experience with the BGP 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 1657 Managed Objects for BGP-4 using SMIv2
- RFC 1721 RIPv2 Protocol Analysis
- RFC 1722 RIPv2 Protocol Applicability Statement
- RFC 1723 RIPv2 with Equal Cost Multipath Load Balancing
- RFC 1771 A Border Gateway Protocol 4 (BGP-4)
- RFC 1772 Application of BGP in the Internet
- RFC 1773 Experience with the BGP-4 protocol
- RFC 1774 BGP-4 Protocol Analysis
- 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 1930 Guidelines for creation, selection, and registration of an
- Autonomous System (AS)
- RFC 1966 BGP Route Reflection
- RFC 1981 Path MTU Discovery for IPv6
- RFC 1997 BGP Communities Attribute
- RFC 1998 BGP Community Attribute in Multi-home Routing
- 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 2260 Support for Multi-homed Multi-prov
- RFC 2270 Dedicated AS for Sites Homed to one Provider
- 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 2385 BGP TCP MD5 Signature Option
- RFC 2391 Load Sharing Using Network Address Translation(LSNAT)
- 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

Features/Standards and Protocols (cont.)

- 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 2519 A Framework for Inter-Domain Route Aggregation
- RFC 2545 BGP Multiprotocol Extensions for IPv6
- RFC 2547 BGP/MPLS VPNs
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2577 FTP Security Considerations
- RFC 2581 TCP Congestion Control
- RFC 2597 Assured Forwarding PHB Group
- RFC 2663 NAT & PAT (NAPT)
- 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
- RFC 2796 BGP Route Reflection
- RFC 2827 Network Ingress Filtering
- RFC 2858 Multiprotocol Extensions for BGP-4
- 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 2918 Route Refresh Capability for BGP
- 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 3022 Traditional NAT
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederations for BGP
- RFC 3069 VLAN Aggregation for Efficient IP Address Allocation
- RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3162 RADIUS and IPv6
- RFC 3315 DHCPv6
- RFC 3345 BGP Persistent Route Oscillation
- RFC 3359 TLV Code points in IS-IS
- RFC 3373 Three-Way Handshake for IS-IS
- RFC 3376 IGMPv3
- RFC 3392 Capabilities Advertisement with BGP-4
- 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 3562 Key Mgt Considerations for TCP MD5 Signature Opt
- 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 3618 Multicast Source Discovery Protocol (MSDP)
- 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

Features/Standards and Protocols (cont.)

- 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 4023 Encapsulating MPLS in IP
- RFC 4026 Provider Provisioned VPN Terminology
- 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 4264 BGP Wedgies
- RFC 4265 Definition of Textual Conventions for (VPN) Management
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4273 Managed Objects for BGP-4 using SMIv2
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4275 BGP-4 MIB Implementation Survey
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 protocol
- 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 4308 Cryptographic Suites for IPSec
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP VPNs
- RFC 4365 Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4384 BGP Communities for Data Collection
- 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 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4541 IGMP Snooping
- RFC 4541 MLD Snooping
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4577 OSPF as PE/CE Protocol for BGP L3 VPNs
- 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 4611 Multicast Source Discovery Protocol (MSDP) Deployment Scenarios
- RFC 4632 Classless Inter-Domain Routing (CIDR)
- RFC 4659 BGP-MPLS (VPN) Extension for IPv6 VPN
- RFC 4716 – The Secure Shell (SSH) Public Key File Format
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- 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 4893 BGP Support for Four-octet AS Number Space
- RFC 4940 IANA Considerations for OSPF
- RFC 5059 Bootstrap Router (BSR) Mechanism for (PIM)

Features/Standards and Protocols (cont.)

- RFC 5065 Autonomous System Confederations for BGP
- 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 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Outbound Route Filter for BGP-4
- 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 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 5396 Textual Representation AS Numbers
- RFC 5398 AS Number Reservation for Documentation Use
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5668 4-Octet AS Specific BGP Extended Community
- 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 6296 IPv6-to-IPv6 Network Prefix Translation
- RFC 6549 OSPFv2 Multi-Instance Extensions
- RFC 4577 OSPF as PE/CE Protocol for BGP L3 VPNs
- RFC 6565 OSPFv3 as PE/CE Protocol for BGP L3 VPNs

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 Networks Private VLANs

CLASS OF SERVICE

- Strict Priority Queuing
- Weighted Fair Queuing with Shaping
- Hybrid Arbitration
- 16/12 Transmit Queues per Port
- Up to 3,072 rate limiters for S130 Class products
- Up to 12,288 rate limiters for S180 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

EXTREME NETWORKS NETWORK MANAGEMENT SUITE (NMS)

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

Features/Standards and Protocols (cont.)

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
- 15 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 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB
- RFC 4444 MIB for IS-IS

Features/Standards and Protocols (cont.)

- RFC 4560 DISMAN-PING-MIB
- RFC 4560 DISMAN-TRACEROUTE-MIB
- RFC 4560 DISMAN-NSLOOKUP-MIB
- RFC 4624 MSDP 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
- 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-idr-bgp4-mibv2 (Partial Support)
- Draft-ietf-idr-bgp-identifier
- Draft-ietf-idr-as-pathlimit
- Draft-ietf-idr-mrai-dep (Partial Support)
- 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

Features/Standards and Protocols (cont.)

- Enterasys License Key MIB
- Enterasys License Key OIDS MIB
- Enterasys Link Flap MIB
- Enterasys LSNAT-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
- EnterasysMULTI User 8021X MIB
- Enterasys NAT 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 TWCB 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

PHYSICAL SPECIFICATIONS		
MODEL NUMBER	DIMENSIONS (H X W X D)	RACK UNITS
S8-Chassis	63.96 cm x 44.70 cm x 47.32 cm (25.19" x 17.60" x 18.63")	14.5U
S8-Chassis-POE4	72.87 cm x 44.70 cm x 47.32 cm (28.69" x 17.60" x 18.63")	16.5U
S8-Chassis-POE8	77.31 cm x 44.70 cm x 47.32 cm (30.44" x 17.60" x 18.63")	17.5U
S6-Chassis	88.70 cm x 44.70 cm x 47.35 cm (34.92" x 17.59" x 18.64")	20U
S6-Chassis-POE4	97.50 cm x 44.70 cm x 47.35 cm (38.39" x 17.59" x 18.64")	22U
S4-Chassis	40.00 cm x 44.70 cm x 47.32 cm (15.75" x 17.60" x 18.63")	9U
S4-Chassis-POE4	48.90 cm x 44.70 cm x 47.32 cm (19.25" x 17.60" x 18.63")	11U
S3-Chassis-A	31.11 cm x 44.70 cm x 47.32 cm (12.25" x 17.60" x 18.63")	7U
S3-Chassis-POEA	37.46 cm x 44.70 cm x 47.32 cm (14.75" x 17.60" x 18.63")	9U
S1-Chassis-A	8.69 cm x 44.88 cm x 60.27 cm (3.42" x 17.67" x 23.73")	2U
SSA S130 and S150A (S-Series Stand Alone)	4.44 cm x 44.70 cm x 59.43 cm (1.75" x 17.60" x 23.40")	1U
SSA S180 (S-Series Stand Alone)	4.37cm x 44.73 cm x 57.30 cm (1.72" x 17.61" x 22.55")	1U

POWER SUPPLIES					
MODEL NUMBER	CURRENT RATING	INPUT VOLTAGE	INPUT FREQUENCY	POWER OUTPUT	
				(100-120V)	(208-240v)
S-AC-PS	20A	100 - 240 VAC	50 - 60 Hz	1,200W	1,600W
S-AC-PS-15A	15A	100 - 240 VAC	50 - 60 Hz	930W	1,600W
S-DC-PS		48-60 V DC		1200W	
SSA-FB-AC-PS-A (I/O Exhaust)	15A	100 - 240 VAC	50 - 60 Hz	480W	
SSA-FB-AC-PS-B (I/O Intake)	15A	100 - 240 VAC	50 - 60 Hz	480W	
SSA-PS-625	15A	100 - 240 VAC	50 - 60 Hz	625W	625W
SSA-PS-1000W	15A	100 - 240 VAC	50 - 60 Hz	1,000W	1,200W
POE Power (802.3af, 802.3at)					
S-POE-PS	20A	100 - 240 VAC	50 - 60 Hz	1,200W	2,000W
4 Bay POE Power				4,800W (max)	8,000W (max)
8 Bay POE Power				9,600W (max)	16,000W (max)
Environmental					
Operating Temperature	5° to 40° C (41° to 104° F)				
Storage Temperature	-30° to 73° C (-22° to 164° F)				
Operating Relative Humidity	5% to 95% (non-condensing)				
Agency 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)				
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)				
Environmental	2002/95/EC (RoHS Directive), 2002/96/EC (WEEE Directive), Ministry of Information Order #39 (China RoHS)				

Chassis Model Number Information

Part Number	Description
S8 Chassis	
S8-Chassis	S-Series S8 Chassis and fan trays (Power supplies ordered separately)
S8-Chassis-POE4	S-Series S8 Chassis and fan trays with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S8-Chassis-POE8	S-Series S8 Chassis and fan trays with 8 bay PoE subsystem (System and PoE Power supplies ordered separately)
S8-POE-8BAY-UGK	S-Series 8 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)
S8-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S8 (PoE Power supplies ordered separately)
S8-Midmount-Kit	S-Series S8 Chassis 19" midmount installation rack kit can be used with all S8 chassis types
S6 Chassis	
S6-Chassis	S-Series S6 Chassis and fan trays. Front to back cooling. (Power supplies ordered separately)
S6-Chassis-POE4	S-Series S6 Chassis and fan tray with 4 bay POE subsystem. Front to back cooling. (System and POE power supplies ordered separately)
S6-Midmount-Kit	S-Series S6 Chassis 19" midmount installation rack kit, can be used with all S6 Chassis types
S6-FAN	S-Series Fan Tray (For use w/ S6)
S4 Chassis	
S4-Chassis	S-Series S4 Chassis and fan tray (Power supplies added separately)
S4-Chassis-POE4	S-Series S4 Chassis and fan tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S4-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S4 (PoE Power supplies ordered separately)
S4-Midmount-Kit	S-Series S4 Chassis 19" midmount installation rack kit, can be used with all S4 Chassis types
S3 Chassis	
S3-Chassis-A	S-Series S3 Chassis and fan tray (Power supplies ordered separately)
S3-Chassis-POEA	S-Series S3 Chassis and Fan Tray with 4 bay PoE subsystem (System and PoE Power supplies ordered separately)
S3-POE-4BAY-UGK	S-Series 4 bay PoE upgrade kit for the S3 (PoE Power supplies ordered separately)
S3-Midmount-Kit	S-Series S3 Chassis 19" midmount installation rack kit, can be used with all S3 Chassis types
S1-Chassis	
S1-Chassis-A	S-Series S1 Chassis and fan tray. Compatible with Fabric Modules only. (SSA 1000W Power supplies ordered separately)
S1-Mount-Kit	S-Series S1 Chassis 19" accessory mounting kit. Supports midmount and rail kit installation options for 2 and 4 post racks, can be used with the S1 chassis.
S1-FAN-A	S1 Chassis fan tray, Spare (For use w/S1)
Power Supplies and Fans	
S-AC-PS	S-Series AC power supply, 20A 100-240 VAC input (1200W/1600W) (For use w/S3/S4/S6/S8)
S-AC-PS-15A	S-Series AC power supply, 15A, 100-240 VAC input, (930W/1600W) (For use w/S3/S4/S6/S8)
S-POE-PS	S-Series POE power supply, 20A, 100-240 VAC input, (1200/2000 W) (For Use in 4/8 Bay PoE power subsystems)
S-DC-PS	S-Series 48-60v DC Power Supply (For Use w/ S3/S4/S6/S8) (1200W)
S-FAN	S-Series Fan Tray (For use w/ S3/S4/S8)

I/O and I/O Fabric Model Number Information

PART NUMBER	DESCRIPTION
S130 I/O Fabric Modules	
ST4106-0348-F6	S-Series S130 Class I/O - Fabric Class Module, 1280Gpbs Load Sharing - 48Ports 10/100/1000Base-TX via RJ45 with PoE (802.3at) and one Type2 option slot (Used in S1A/S4/S6/S8)
S130 I/O Modules	
ST4106-0248	S-Series S130 Class I/O Module - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and one Type1 option slot (Used in S3/S4/S6/S8)
SG4101-0248	S-Series S130 Class I/O Module - 48 Ports 1000BASE-X ports via SFP and one Type1 option slot (Used in S3/S4/S6/S8)
S140 I/O Modules	
ST2206-0848	S-Series S140 Class I/O Module - 48 Ports 10/100/1000BASE-TX via RJ45 with PoE (802.3at) and two Type2 option slot (Used in S3/S4/S6/S8)
SG2201-0848	S-Series S140 Class I/O Module - 48 Ports 1000BASE-X ports via SFP and two Type2 option slot (Used in S3/S4/S6/S8)
SK2008-0832	S-Series S140 Class I/O Module - 32 Ports 10GBASE-X via SFP+ (Used in S3/S4/S6/S8)
SK2009-0824	S-Series S140 Class I/O Module -24 Ports 10GBASE-T via RJ45 (Used in S3/S4/S6/S8)
S180 I/O Fabric Modules	
SL8013-1206-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 6 Ports 40GBASE-X Ethernet via QSFP, 4 ports VSB via SFP+ (Used in S1A/S4/S6/S8)
SK8008-1224-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 24 Ports 10GBASE-X via SFP+, 4 ports VSB via SFP+ (Used in S1A/S4/S6/S8)
SK8208-0808-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 8 Ports 10GBASE-X via SFP+ and two Type2 option slots (Used in S1A/S4/S6/S8)
SK8009-1224-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 24 Ports 10GBASE-T via RJ45, 4 ports VSB via SFP+ (Used in S1A/S4/S6/S8)
ST8206-0848-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and two Type2 option slots (Used in S1A/S4/S6/S8)
SG8201-0848-F8	S-Series S180 Class I/O - Fabric Module, Load Sharing - 48 Ports 1000BASE-X via SFP and two Type2 options slots (Used in S1A/S4/S6/S8)
S180 I/O Modules	
SL8013-1206	S-Series S180 Class I/O Module - 6 Ports 40GBASE-X Ethernet via QSFP, VSB expansion slot (Used in S4/S6/S8)
SK8008-1224	S-Series S180 Class I/O Module - 24 Ports 10GBASE-X via SFP+, VSB expansion slot (Used in S4/S6/S8)
SK8009-1224	S-Series S180 Class I/O Module - 24 Ports 10GBASE-T via RJ45, VSB expansion slot (Used in S4/S6/S8)
Option Modules	
SOK2208-0102	S-Series Option Module (Type1) - 2 Ports 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1 & Type2 option slots)
SOK2208-0104	S-Series Option Module (Type1) - 4 Ports 10GBASE-X Ethernet ports via SFP+ (Compatible with Type1 & Type2 option slots)
SOK2208-0204	S-Series Option Module (Type2) - 4 10GBASE-X Ethernet ports via SFP+ (Compatible with Type2 option slots)
SOG2201-0112	S-Series Option Module (Type1) - 12 1000BASE-X ports via SFP (Compatible with Type1 & Type2 option slots)
SOT2206-0112	S-Series Option Module (Type1) - 12 Ports 10/100/1000BASE-TX via RJ45 with PoE (802.3at) (Compatible with Type1 & Type2 option slots)
SOTK2268-0212	S-Series Option Module (Type2) - 10 Ports 10/100/1000BASE-T via RJ45 with PoE and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)
SOGK2218-0212	S-Series Option Module (Type2) - 10 Ports 1000BASE-X via SFP and 2 ports 10GBASE-X via SFP+ (Compatible with Type2 option slots)
SOV3208-0202	S-Series Option Module (Type2) - 2 Port VSB Option Module (Compatible with Type2 option slots on S140/S180 modules only)
Expansion Modul**e**	
SOV3008-0404	S-Series VSB Expansion Module - 4 Port VSB Module (Compatible with S180 Class 10Gb/40Gb I/O modules only)

SSA and License Model Number Information

PART NUMBER	DESCRIPTION
SSA S130/S150A (S-Series Stand Alone)	
SSA-T4068-0252	S-Series S130 Class Stand Alone (SSA) - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and 4 10GBASE-X Ethernet ports via SFP+ (Power supplies not included - Please order separately)
SSA-T1068-0652A	S-Series S150 Class Stand Alone (SSA) - S150 Class - 48 Ports 10/100/1000BASE-T via RJ45 with PoE (802.3at) and 4 10GBASE-X Ethernet ports via SFP+ (Power supplies not included - Please order separately)
SSA-AC-PS-625W	S-Series Standalone (SSA S130 and S150 Class) - AC power supply, 15A, 100-240VAC input, (625W)
SSA-AC-PS-1000W	S-Series Standalone (SSA S130 and S150 Class) and S1-Chassis - AC and POE power supply, 15A, 110-240VAC input, (1000/1200W)
SSA-FAN-KIT	S-Series Stand Alone (SSA S130 and S150 Class) - Replacement fan assembly (Single Fan)
SSA S180 (S-Series Stand Alone)	
SSA-T8028-0652	S-Series S180 Class Standalone (SSA) - 48 Ports 10/100/1000BASE-T via RJ45 and 4 ports 10GBASE-X via SFP+, Front to Back cooling (Power supplies not included - Please order separately)
SSA-G8018-0652	S-Series S180 Class Standalone (SSA) - 48 Ports 1000BASE-X via SFP and 4 ports 10GBASE-X via SFP+, Front to Back cooling (Power supplies not included - Please order separately)
SSA-FB-MOUNTKIT	Optional Rack Mount Kit for the SSA 'Front to Back' models.
SSA-FB-AC-PS-A	S-Series Standalone (SSA Front to Back) - AC power supply, 15A, 100-240VAC input, I/O side exhaust
SSA-FB-AC-PS-B	S-Series Standalone (SSA Front to Back) - AC power supply, 15A, 100-240VAC input, I/O side intake
SSA-FB-FAN	S-Series Standalone (SSA Front to Back) - Spare fan tray assembly
Optional Licenses	
S-EOS-L3-S130	S-Series Advanced Routing License (For use on S130 Class Modules) (Enables VRF, BGP, Tunneling)
S-EOS-PPC	S-Series Per Port User Capacity License Upgrade (For use on S130 Class Modules)
S-EOS-VSB	S-Series Multi-slot Virtual Switch Bonding License Upgrade (For use on S130/S140/S150 Class Modules)
SSA-EOS-VSB	S-Series SSA Virtual Switch Bonding License Upgrade (For use on SSA Only)
SSA-EOS-2XUSER	SSA180/SSA150 double user capacity license
S1-EOS-VSB	S-Series S1 Chassis Virtual Switch Bonding License Upgrade (For use on S1-Chassis-A /S1-Chassis Only)

TRANSCEIVERS

Extreme Networks transceivers provide flexible connectivity options for Ethernet. All Extreme Networks 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.Extreme Networks.com/products/transceivers-ds.pdf.

WARRANTY

The Extreme Networks S-Series comes with a one year hardware warranty. For full warranty terms and conditions please go to http://www.Extreme Networks.com/support/warranty.aspx

SERVICE AND SUPPORT

Extreme 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 Extreme Networks account executive for more information about Extreme Networks Service and Support.

ADDITIONAL DETAILS

For additional information on the Extreme Networks S-Series please visit http://www.Extreme Networks.com/products/switching/

http://www.ExtremeNetworks.com/contact / Phone +1 408 579 2800

nGenius InfiniStream Appliance

Why Consider nGenius InfiniStream Appliance for Intelligent Deep Packet Capture and Analysis?

nGenius® InfiniStream® appliance is an intelligent deep packet capture and analysis appliance that delivers dedicated, always on, monitoring and continuous capture capabilities for real-time and back-in-time analysis. The appliance can be used with the nGeniusONE™ Unified Performance Management platform, as a foundation of nGenius Service Assurance Solution, or standalone with Sniffer® Analysis to analyze all packets traversing the network for rapid problem isolation and service delivery assurance.

The nGenius InfiniStream appliance hosts Adaptive Session Intelligence™ (ASI) technology, a high-performance deep packet inspection engine that analyzes network traffic in real-time and generates highly scalable metadata that enables a comprehensive view of service, network, application, and server performance across complex multi-tier, multi-domain service delivery environments.

The appliance performs local real-time granular Layer 4-7 data mining as traffic crosses the wire, eliminating the need for middleware and extensive backend processing while reducing management traffic loads. In addition, the appliance captures, indexes and stores packets crossing the wire for comprehensive deep-dive forensic analysis activities.

What Challenges Does the nGenius InfiniStream Appliance Help Solve?

The nGenius InfiniStream appliance succeeds in delivering complete visibility into monitored traffic flows and packet data. The combination of two critical functions – real-time packet flow-based data monitoring integrated with back-in-time analysis accelerates problem resolution and helps protect overall service delivery quality and availability.

To be effective in meeting service levels and delivering high quality user experience, IT teams need to understand all the complexities involved in the service delivery environment with full visibility into all elements making up the service to truly understand how applications are performing. Resolving sevice performance problems often require cross-domain expertise as performance issues can stem from any number of root causes.

The nGenius InfiniStream appliance passively and non-intrusively captures all network traffic and generates metrics to provide rich and detailed operational understanding of application and network performance in live production environments. It captures every transaction and session that makes up an application service in real-time and simultaneously extracts intelligence from Layer 2 through Layer 7. This information is used by the nGeniusONE platform to provide critical context so IT teams across network, application, telecom, server and security domains can work collaboratively. The correlated data is used to spot network and application issues, understand the impact of enabling services on applications, distinguish application and network brownouts, identify server issues and security breaches, provides insights for infrastructure optimization and planning, and identify other significant service delivery problems.

Since most networks generate large amounts of traffic, the appliance delivers the performance capabilities and provides the scale needed to analyze network traffic generated by thousands of users using hundreds of applications with millions to billions of transactions.

The nGenius InfiniStream appliance features multi-CPU, multi-threaded architecture for delivering high performance DPI capabilities; multiple 10G Ethernet interfaces to capture huge amounts of data streams generated by large, high capacity networks; massive storage space with support of up to 96TB of disk capacity to store the performance metrics and packet data for long-term use.

While organizations benefit from end-to-end visibility for the entire enterprise, the challenge is to find a right-sized appliance that meets the needs of the traffic volume at a

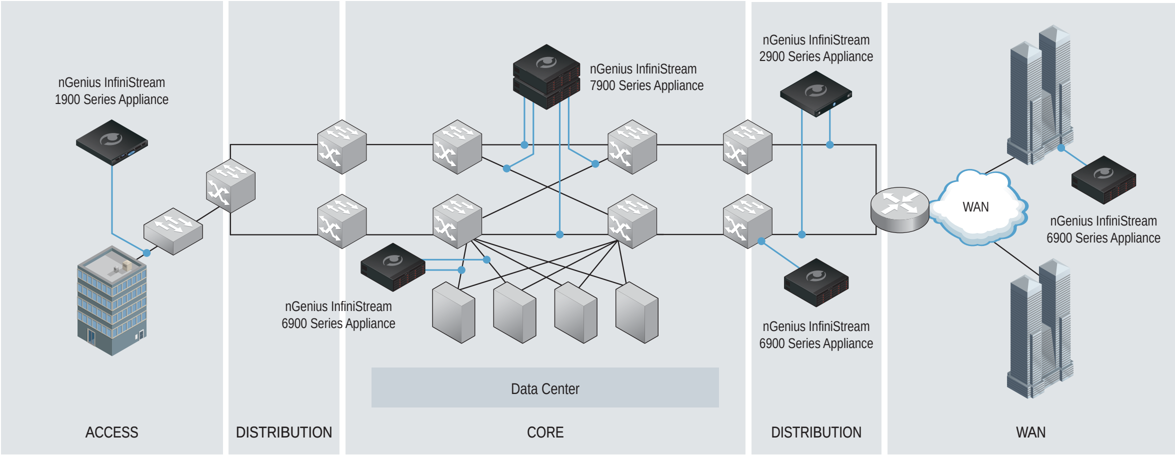


Figure 1: nGenius InfiniStream appliances strategically deployed in an enterprise network.

particular location in the network. nGenius InfiniStream appliances are available in different capacities and configurations suitable for deploying in multiple topologies to enable pervasible visibility supporting monitoring needs for different size installations from small offices to large enterprise data centers. As networks grow, achieving scale becomes a critical enterprise requirement. To solve monitoring needs of very large environments, multiple appliances can be deployed to provide virtually unlimited scalability. Finally, to reduce management complexity in large networks, all appliances are centrally managed through the nGeniusONE platform.

nGenius InfiniStream Appliance

nGenius InfiniStream appliance, running on a customized Linux® operating system, is purpose-built for enabling pervasive visibility across enterprise networks and provides a foundation for extracting application and network performance metrics for the nGeniusONE platform. With support for 10/100/1000 Mbps and 10GbE interfaces and up to 96TB of disk storage space, this appliance provides configuration flexibility and an integrated approach to eliminating performance problems by delivering end-to-end visibility to accomplishing application, network, unified communications performance management and CyberSecurity monitoring and incident response.

The flexible, high-performance appliance features a robust deep packet inspection and analysis engine that has the ability to dynamically recognize different applications and protocols behind each IP session and delivers detailed performance metrics in real-time to the nGeniusONE platform.

Some of the unique capabilities of the nGenius InfiniStream appliance include:

- High resolution visibility into packet data with deep packet analysis identifies thousands of protocols and applications associated with every network flow
- Generates real-time performance, traffic, and error metrics as well as session event records
- Packet recording capacity from 1TB and up to 96TB
- Interface speeds from 10 Mbps to 10 Gbps with RJ-45 copper or pluggable fiber/copper transceiver support
- Time synchronization based on either IETF NTP or IEEE 1588 (PTP v1/v2) with optional time synchronization adapter to leverage Global Positioning System (GPS) to connect to highly precise time source
- Extensible software architecture enables support for new protocols and analysis metrics through software-based ASI adaptors
- Appliances with different levels of storage protection, up to RAID 6, and power supply redundancy
- Role-based access security for controlling access to sensitive data
- Intelligent packet recording with granular selection of protocols and packet recording slice size
- Highly secured platform built on a customized and hardened Linux operating system
- Certified for international Common Criteria EAL3+ and U.S. NIAP CCEVS

All nGenius InfiniStream appliances share a common foundation of proven technology including continuous packet-flow data capture, simultaneous deep packet inspection and analysis, metadata creation and storage to disk. Customers who deploy the single nGenius InfiniStream appliance in their networks can take advantage of the highly specialized deep-dive packet analysis application included with every appliance. This application provides a direct-connect interface to an nGenius InfiniStream appliance to perform unrestricted packet analysis activities for locally stored packets.

The family consists of 1900 series, 2900 series, 6900 series and 7900 series to achieve enterprise deployment flexibility covering data centers, headquarters, branch offices and small sites.

What are the Benefits of the nGenius InfiniStream Appliance?

- Single appliance used with nGeniusONE platform, nGenius Service Assurance Solution, or standalone with Sniffer Analysis
- Passive and non-intrusive appliance does not impact production networks
- Provides two critical functions – 1) Real-Time packet flow-based data monitoring; 2) Packet storage for forensics
- Powerful ASI technology for high-performance, deep packet inspection and analysis
- Plug and play deployment recognizes over 5000 common protocols and over 500 applications
- Flexible range of appliances support from 10 Mbps to 10 Gbps Ethernet monitoring interfaces with copper, SFP and XFP transceivers
- Scalable architecture enables enterprises to scale for any size deployment
- Built for high security environments with a hardened Linux operating system, role-based access controls, and data encryption

nGenius InfiniStream 1900 Series Appliance	nGenius InfiniStream 2900 Series Appliance	nGenius InfiniStream 6900 Series Appliance	nGenius InfiniStream 7900 Series Appliance
• Height: 1 RU • Storage Capacity: 1TB • Packet Capture: 2 x 1GbE ports	• Height: 1 RU • Storage Capacity: 2TB • Packet Capture: 4 x 1GbE ports	• Height: 3 RU • Storage Capacity: 16TB • Packet Capture: 8 x 1GbE ports, 4 x 10GbE ports	• Height: 3 RU • Storage Capacity: 32TB (expandable to 96TB) • Packet Capture: 4 x 10GbE or 2 x 10GbE & 4 x 1GbE

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

nGenius Virtual Agent

Enabling Packet Flow Visibility into Virtual Server Environments and Private Clouds

Highlights

- Real-time granular visibility into virtualized server environments
- Monitors traffic inside and across virtualized servers
- Metrics and capabilities consistent with hardware-based nGenius® Intelligent Data Sources
- Delivers intelligent anomaly detection, CDM-based metrics and Key Performance Indicators (KPIs)
- Supports short-term on-demand packet capture from within the virtual environment
- Self-contained virtual appliance installs easily
- Virtual Tap mode mirrors virtual traffic to an nGenius InfiniStream® appliance for long-term packet capture and deeper analysis capabilities
- Supports VMware®-based virtualized server environments
- Supports Cisco® Nexus® 1000V Series Switches, VMware ESX/ESXi 3.5 vSwitch, VMware vSwitch Standard Switch, and VMware vNetwork Distributed Switch (vDS) implementations

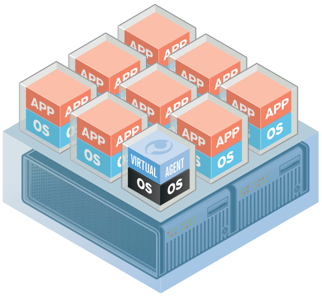
As IT organizations are increasingly leveraging application and server virtualization technologies to improve efficiency, reduce costs and ease the environmental impact of compute resources, they lose vital visibility into the behavior and performance of virtualized applications. Although tools exist for managing the virtual computing platform, IT organizations need to consistently manage, optimize and troubleshoot virtualized applications in context with end-to-end service delivery and the user experience. IT staff needs a unified view into inter-application transactions and performance levels for virtualized applications that is consistent with how traditional physical server-based application deployments have been measured, to understand how a virtualized application is being delivered and consumed by users.

nGenius Virtual Agent

nGenius Virtual Agent software extends unified visibility into applications and services contained within a virtual computing environment. The nGenius Virtual Agent is a virtualized implementation of the widely deployed nGenius Probe technology. It seamlessly extends high-performance deep-packet analysis capabilities deeper into the data center and private clouds - enabling the IT organization to achieve true end-to-end visibility of application traffic from within virtual servers.

Enabling IT organizations to achieve a pervasive visibility strategy, the nGenius Virtual Agent complements traditional hardware-based nGenius instrumentation by enabling real-time, always-on visibility into mission-critical virtual computing environments to provide granular visibility into virtualized application performance and behavior. This allows the IT organization to more effectively manage end-to-end service levels in context with how applications perform where they are hosted. The nGenius Virtual Agent:

- Extends proven nGenius Probe technology to virtualized server environments to deliver real-time visibility of virtualized application traffic
- Provides scalable, granular and cost-effective visibility into virtualized applications and services to reveal multi-tier application performance and interactions
- Supports on-demand and triggered packet captures, enabling IT managers to collect and analyze live packets from within the virtual environment



Optimized for the virtual environment, the nGenius Virtual Agent is a plug-and-play virtual appliance containing an operating system and virtualized nGenius Probe software. Deployed within a dedicated virtual machine, the nGenius Virtual Agent is self-contained and consumes modest platform resources and requires little administrative actions.

Once deployed, nGenius Virtual Agent software provides real-time visibility into the virtual computing environment by monitoring all application traversing the hypervisor. This includes all interactions between virtualized applications contained in a single server, traffic in and out of the physical virtual server, and traffic associated with another virtual server platform. The nGenius Virtual Agent supports the native VMware vSwitch standard switch and VMware vNetwork Distributed Switch (vDS) for extended environments. In addition, nGenius Virtual Agent supports the Cisco Nexus 1000V series switch, providing a high degree of seamless deployment flexibility. Server administrators can control access to traffic visibility through virtual LAN (vLAN) mapping to ensure data privacy and security. The virtualized nGenius Probe software discovers all applications and their interdependencies, within and external to the virtual server.

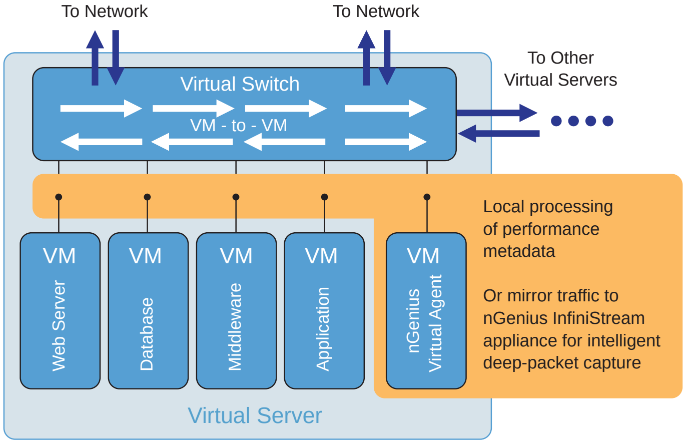


Figure 1: Real-time visibility into all interactions between virtualized applications contained in a single server, traffic in and out of the physical virtual server, and traffic associated with another virtual server platform.

Rich Application Performance Metrics

nGenius Virtual Agent is an nGenius Intelligent Data Source for the nGenius Solution, providing rich granular application performance metrics. The nGenius Solution leverages these metrics to analyze and report on virtualized application transactions in the identical manner and context as non-virtualized server transactions. This enables the IT organization to achieve seamless visibility into virtualized application performance, enabling a unified end-to-end view of all tiers of service delivery. This allows the IT organization to understand how application interdependencies and relationships may impact overall application performance and the downstream effect on user experience.

Since metrics are correlated across an end-to-end deployment, IT staff benefit from a unified view of the virtual application traffic in context with the end-to-end service delivery environment. This dramatically simplifies the management of complex virtual application deployments and enables the IT organization to more efficiently optimize service delivery, predict and prevent performance issues, and speed problem resolution in context with the overall service delivery environment and the user experience.

With this server visibility, nGenius Virtual Agent software allows IT organizations to gain a complete understanding of end-to-end service performance:

- Granular visibility into virtualized application performance extends industry leading technology, including Key Performance Indicator (KPI) monitoring and automated behavioral analytics
- Unified views of service performance across physical and virtual infrastructure for unified end-to-end visibility across the service delivery environment
- Provides unique insight into the interactions of application tiers within the virtual server
- Enables virtual infrastructure optimization to improve application performance and service levels
- Better assure the user experience by understanding application performance within the virtual server environment
- Dramatically reduce the time to resolve performance issues, minimizing the impact of application and service performance degradation

Virtual Probe or Tap Modes Supports Flexible Deployments

nGenius Virtual Agent supports two operational modes for a high degree of deployment flexibility. It can be deployed as a full-function virtualized probe, providing the same functionality as a traditional hardware-based nGenius Probe. When deployed in Probe Mode, nGenius Virtual Agent performs the deep-packet inspection to analyze network traffic locally in real time and provides rich metrics, KPIs and intelligent anomaly detection to the nGenius Solution.

In the event the IT organization needs long-term continuous packet capture or have more granular metrics, nGenius Virtual Agent can be deployed in TAP Mode. In TAP Mode, all traffic flowing across the virtual switch is exported to an external nGenius InfiniStream appliance for external capture, analysis and forensics, functioning exactly like a traditional TAP would on a physical network link. System users can quickly switch between Probe and TAP modes for flexible extended analysis capabilities based upon specific events or needs.

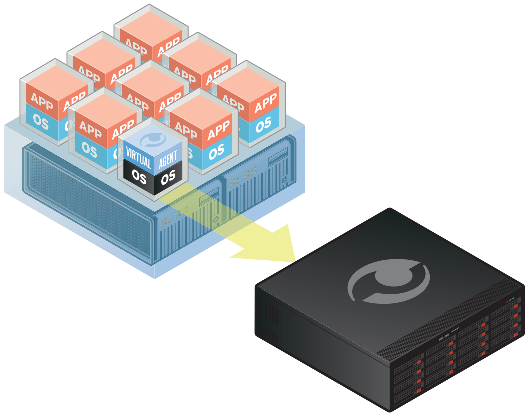


Figure 2: nGenius Virtual Agent can stream packet flow to an nGenius InfiniStream appliance for long-term packet capture and deeper analysis capabilities.

Visibility into Moving Applications

In a virtualized deployment, applications can move from one virtual server to another, increasing the network management team's challenge of anticipating and managing network traffic. Since virtual servers can be located in different parts of the data center or around the world, an application's movement can cause significant and unexpected impact to network operations - resulting in performance degradations and undesired user impact. While the application or server team may know about the application's movement, the network staff can be caught by surprise from moving application traffic. With nGenius Virtual Agent deployed, the nGenius Solution will identify application movement between servers from a network perspective.

nGenius Virtual Agent automatically discovers new or moved applications within a virtual server, enabling network staff to instantaneously know which applications have moved and enabling them to predict and address sudden changes in network traffic patterns. This knowledge will also help IT staff correlate and better understand the performance of virtualized services across multiple servers and network elements, validate the implementation of moved services, and aid in the optimization of application use of compute and network resources.

Take Me to the Cloud™

IT organizations can leverage nGenius Virtual Agent to provide visibility into cloud-based hosting environments. By adding an nGenius Virtual Agent instance to a virtual machine within the same server as an externally hosted virtual application, the IT organization can gain valuable insight into the performance of hosted applications residing outside the corporate data center. In this deployment model, nGenius Virtual Agent will require its own dedicated virtual server and necessary resources. Once deployed, the IT organization can leverage granular visibility and metrics into application transactions occurring within the hosted cloud environment. Leveraged by the nGenius Solution, cloud metrics can be viewed alongside metrics from within the traditional enterprise service delivery environment, enabling unprecedented visibility into hybrid cloud and blended service deployments.

Key Features

The nGenius Virtual Agent is deployed within a virtual server to provide visibility into all application and service traffic flowing across a server's virtual switch. When deployed in Probe Mode, key capabilities of the nGenius Virtual Agent include:

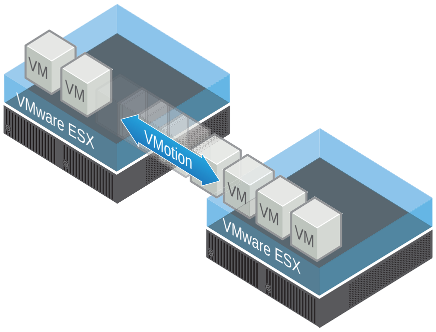
Application Recognition and Monitoring

Support for a variety of application types, including:

- Well-known and children of well-known applications
- User-defined and custom-developed applications
- Peer-to-peer applications
- Web-based applications and URLs

Packet Analysis-Based Troubleshooting

- Supports on-demand, short-term packet capture for analysis by nGenius Solution or Sniffer® Analysis software
- Manual or automatic data capture to start by matching a pattern of packets, alarms or error conditions
- Pre-capture filtering



Response-Time Analysis/KPIs

- Response-time metrics for virtually all application types
- Passive application responsiveness measurements
- One-minute granularity: average response time, number of active sessions, number of successful transactions, and number of server error types
- Fifteen-minute granularity: maximum and average response time per client/server pair, total number of transactions, number of successful transactions, TCP connect time, number of active sessions, total packet loss, response-time distribution, number of timeouts, number of retries, and application payload
- KPI measurements, including packet loss, inter-packet delay, client and server errors, and timeouts

Network-based Metrics

- TCP, HTTP and server-specific performance and error conditions
- Percent utilization and packet/byte counts for link, host, host group, applications and conversations

Alarming and Event Identification

- Define alarms for link utilization, application utilization, application response time, application availability
- “Burst alarms” at millisecond resolution
- “Power alarms” highlight root cause by gathering top users and applications automatically at violation time for segments exceeding utilization, responsiveness and availability thresholds
- Supports rising, falling and time-over-threshold templates

Data Granularity

- Fifteen-second, real-time views with one-second peaks
- One-minute historically logged data for all application, hosts, and conversation flows

System Requirements	
Virtual Switches Supported	VMware ESX/ESXi 3.5 Switches VMware vSwitch Standard Switch VMware vNetwork Distributed Switch (vDS) Cisco Nexus 1000V Series Switches
Supported VMware ESX Versions	VMware ESX/ESXi 3.5 VMware ESX/ESXi 4.x VMware ESXi 5.0 VMware ESXi 5.1
Supported VMware Client Versions	VMware Virtual Infrastructure Client 2.5 VMware vSphere® Client 4.0 VMware vSphere Client 5.0 VMware vSphere Client 5.1
Supported VMware	VMware Virtual Center 2.5 Virtual Management Server VMware vCenter 4.0 U1 or higher versions
Virtual Central Processing	Requires 2.4 GHz XEON processors or better Two (2) cores of physical CPU need for installation, one (1) core of the physical CPU need for operation
Random Access Memory (RAM) Requirements	512 MB
Required Hard Drive Space	Eight (8) GB

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

nGeniusONE

Unified Performance Management Platform

Highlights

- One unified platform converges application and network performance management to capture all components contributing to the user experience
- Macro and micro-level insights into service performance enterprise-wide, or by site, user community, user, server group and more
- Visibility into complex multi-tier service delivery environments including elements such as servers, applications, users and networks
- Effectively manage the health and availability of diverse service environments
- Rich graphical real-time and historical views derived from packet-flow-based analytics
- Simple, easy to use workflows enable fast root cause analysis
- Scalable, enterprise-class architecture supports large-scale geographically distributed deployments
- Backwards compatible with nGenius Service Assurance Solution deployments for investment protection

Product Overview

The nGeniusONE™ Unified Performance Management platform unifies application and network performance management providing a top-down view into any IP-based business services, including voice, video and data. Rather than look at individual elements in isolation, nGeniusONE provides an overarching view into the performance characteristics of all infrastructure and application components associated with service delivery. This platform combines real-time situational awareness, historical analysis, and multi-layered analytics capabilities. This unified perspective enables IT organizations to more effectively manage the health and availability of diverse application environments, improving the network and application teams' ability to proactively identify and triage performance issues, assess impact and quickly identify the root cause of problems.

Traditional application performance management tools focus predominantly on web-based services, such as J2EE or .NET applications. These traditional tools take a very narrow, siloed approach to identifying and resolving related service issues, which can complicate and delay problem resolution. The nGeniusONE platform complements this compartmentalized model, providing a simple end-to-end view into overall application and network performance management by delivering valuable macro-level insights and understanding of the complexities and interdependencies of a service delivery environment.

nGeniusONE delivers extensive operational intelligence supporting many different performance management use cases within a single unified platform. Common use cases include intelligent early warning, incident response, real-time and historical performance analysis, planning & optimization, session analysis, forensics and reporting. These use cases can be leveraged across IT organizations, benefiting Network, Application, Server and Unified Communications teams, as well as CyberSecurity owners.

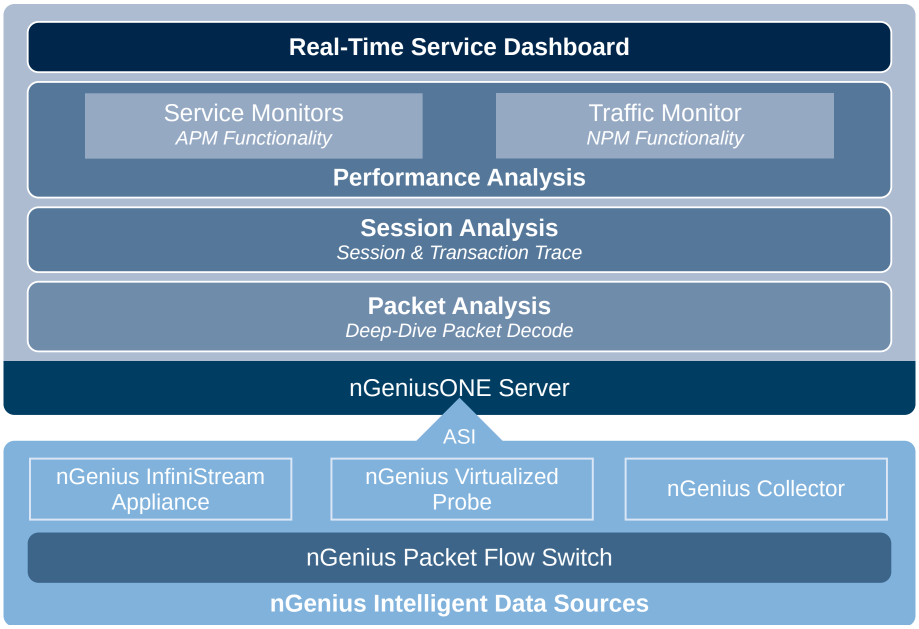


Figure 1: nGeniusONE unifies application performance management and network performance management in a single platform to deliver correlated metrics and simplified workflows that dramatically streamline service delivery management activities.

Product Capabilities

- Service Dashboard provides real-time views with logical visualization of key services in business-relevant hierarchies
- Service-oriented performance analysis based on network or application-oriented workflows
- Real-time and historical network, application and server visualization with contextual drilldown from rich service views to comprehensive session and packet level deep-dive analysis
- Hop-by-hop session trace combining application and network performance details
- Robust service definition enables monitoring and recognition of all applications or services, out of the box or user-defined, including Web-based applications
- Meaningful visibility into service interdependencies provided by user and server communities, site, qos, vlan, and vrf location details correlated with application metrics
- Service-focused reporting based on rich application and network metadata

Service-Focused Approach To Performance Management

nGeniusONE platform supports diverse voice, video and data environments with a service-focused approach to performance management. This enables IT teams to manage diverse services including web-based applications, remote desktop application such as Citrix, public and private cloud environments, Unified Communications services such as Voice over IP and specialized environments such as payment processing or financial trading with one unified tool. Custom application definitions and logical groupings of user, server, application, and network data enable IT teams to create meaningful analysis views.

Logical user or server groupings, or communities, are an important element of this approach, allowing nGeniusONE to aggregate traffic destined to the group of users as a whole, presenting views that are more meaningful and relevant to business needs. Groups of client addresses can be configured to be viewed as a single entity, while important IP addresses within the block can still be separated out for individual visibility.

Extending beyond the concept of server or user communities, nGeniusONE also incorporates a feature called My Network. This feature is enabled by default, and ensures that data pertaining to internal network, server and application performance is collected at the highest level of granularity. My Network includes all RFC 1918 space by default, and can be configured to include private address ranges or important partner or Software as a Service connections. Connections outside of My Network are monitored at lesser granularity, to reduce noise from non-business applications or services.

Along with these user and server communities, nGeniusONE further enables the logical organization of traffic with the configuration of location keys. Traditional network performance Management tools will group data by source and destination IP address, or perhaps the monitored interface the traffic was collected from. Location keys allow users to define vlans, sites, qos levels, or MPLS VRF groups as a location, thus allowing more granular data mining and analysis of the observed network traffic.

To allow IT teams to better visualize the state of the enterprise IT architecture, nGeniusONE leverages these location keys in the creation of flexible, user-defined service domains. These service domains enable IT teams to create views that dynamically align with how services are delivered across physical and virtual

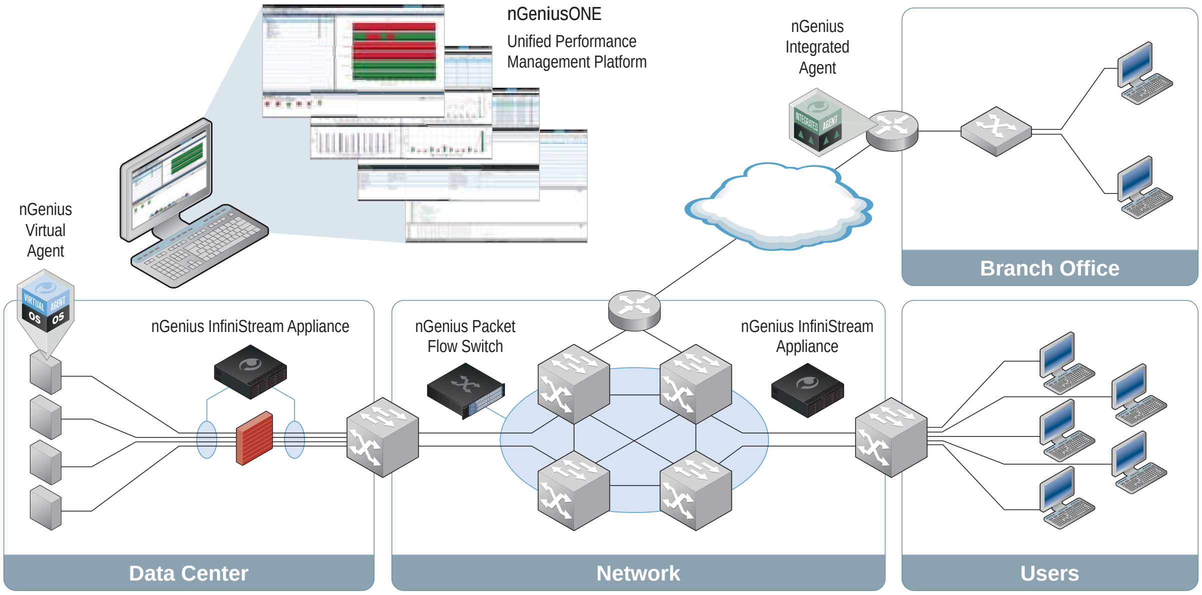

nGeniusONE
Unified Performance Management Platform
nGenius Integrated Agent
INTEGRATED AGENT
Branch Office
nGenius Virtual Agent
VIRTUAL AGENT
OS
OS
nGenius InfiniStream Appliance
nGenius Packet Flow Switch
nGenius InfiniStream Appliance
Data Center
Network
Users

Figure 2: The nGeniusONE platform can monitor thousands of critical applications and services supporting tens of thousands of users across large multi-location Enterprise environments.

infrastructure. Domains are constructed based upon physical and logical attributes such as a specific application or service, physical sites, logical workgroups, geographic regions or even business units. This allows for a customized view into end-to-end service delivery that streamlines performance management activities and improves operational consistency that encourages better communication across the different functional IT groups. This service-focused approach provides a more holistic view into service health revealing interactions and dependencies between the infrastructure and application tiers across complex and distributed environments, solving problems that host and agent-based APM approaches cannot.

Unification of Application and Network Performance Management

Representing a completely new architecture, the nGeniusONE platform unites the traditional approaches of application and network performance management in a single unified tool. For application performance management needs, this platform provides specific insights into key performance indicators such as application responsiveness, new and active client-server session metrics, service requests and application error codes. For network performance management needs, the nGeniusONE platform provides hop-by-hop transaction latency measurements, details about traffic volume and link utilization, information about quality of service (QoS) levels, and information about application usage across the network. By bringing this information together in a series of multi-dimensional views, the nGeniusONE platform is able to provide deep insights which enable IT users to proactively identify problems faster and manage the health and availability of the service delivery environment.

Top-Down, Service-Oriented Workflows

The nGeniusONE platform provides a top-down, service-focused approach to application and network performance management. Through the use of performance analysis layers, IT users can start with a high level view of the overall enterprise environment and then drill down proactively to potential problem spots for rapid investigation and resolution.

nGeniusONE workflows are simplified to make problem identification and resolution fast and easy. The start of the workflow is the Service Dashboard, which provides real-time visibility into the overall service delivery environment. The hierarchical view from this dashboard presents alerts in a business-relevant context, allowing IT users to quickly and proactively respond to potentially user-impacting issues. In addition, high-level summaries and topology maps show the status of a service at all times.

For detailed application performance analysis, Service Monitors deliver comprehensive, multi-dimensional views that facilitate investigating service performance characteristics, with all elements of the service displayed comparatively in context. Several specialized Service Monitors come pre-defined, such as call signaling, DNS, or DHCP, with streamlined workflows for simplifying the troubleshooting of these services. This platform also includes a general purpose Service Monitor called Application Delivery Monitor, which can be customized to analyze any application or service. These Service Monitors show key metrics relating to client-server communications, application errors, and other indicators of service health.

Traffic Monitor complements Service Monitors by providing an application-aware view into network performance metrics, including details such as top N applications, traffic volumes and utilization filtered by physical link, class of service, VLAN, or other logical attributes. Graphical displays show link utilization in terms of volume or percent utilization for each application on a link, as well as a pie chart depicting the location breakdown of observed application traffic in the network. For more application-centric metrics, Traffic Monitor supports a contextual drilldown into Application Delivery Monitor.

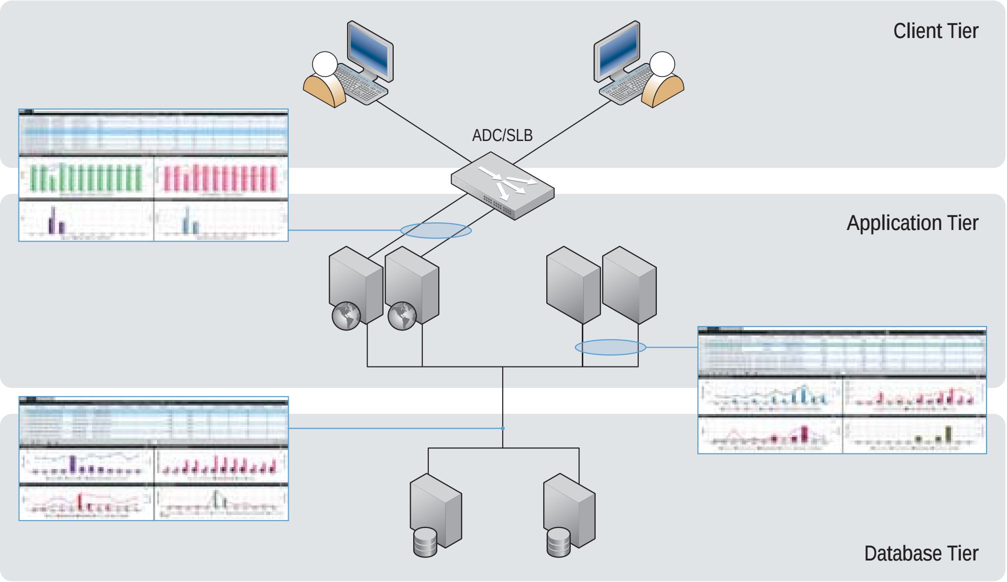


Figure 3: Visibility into multiple tiers of a service helps separate causes from symptoms and zoom in on problem spots quickly and easily.

For in-depth troubleshooting of service issues, administrators can progress to Session Analysis from within a Service Monitor to see a contextual, transaction-level view of the impacted user sessions. nGeniusONE Session Analysis intelligently correlates and displays all transactions from each user session observed across multiple network segments, even across NAT/PAT boundaries, providing an end-to-end view that accelerates the analysis process. Graphical representations are shown in the form of a ladder diagram illustrating the multi-hop transactions, including latency time stamps. A table above the ladder diagram includes sortable, searchable information fields including location, server name, client IP or community, application errors, retries, and timeouts.

Should Deep-Dive protocol-level analysis be needed, administrators can contextually perform packet analysis for efficient, deep-dive analysis or to collect forensic evidence. nGeniusONE Packet Analysis creates a predefined filter of the packets viewed in Session Analysis, ensuring only the relevant details for the specific transaction under investigation are decoded. Alternatively, new filters can be created from scratch, leveraging regular expressions with Boolean logic to filter for multiple strings based on text, hex, host, application, pattern, and more. The decoding of packets actually take place in the nGenius InfiniStream® appliance which collected the packets, then the decoded results are sent back to the nGeniusONE console for display, speeding analysis time and eliminating unnecessary network loads.

Intelligent Early Warning

With increasing requirements for high availability and increasing complexity of business services, IT organizations need to adopt predictive service management approaches to minimize or avoid downtime whenever possible. The continued growth in applications, users, and traffic poses a challenge to establishing stringent alarm thresholds, for realizing the benefits of early warning, due to the frequent need for threshold adjustments under such scenarios. The nGeniusONE Service Dashboard addresses these challenges with an intelligent early warning capability powered by an advanced analytics engine that automatically establishes performance baselines and generates alerts on significant deviations from these baselines. The engine also automatically adjusts the baselines over time to adapt to gradual changes in service utilization while delivering timely alerts on performance anomalies.

Performance baselines can be set for Key Traffic Indicators (KTI) and Key Performance Indicators (KPI) including rising and falling link utilization, application transaction failure rates and responsiveness. Time-based exclusions can be defined to ensure baselines only measure performance during business hours. Early warnings generated by the analytics engine can be viewed in the Service Dashboard as well as forwarded to up to four SNMP trap listeners. Using this intelligent early warning capability, IT organizations can obtain visibility into emerging service performance issues, contextually analyze alert evidence and underlying causes using the Service Monitors and Traffic Monitor, and predictively take action to avoid future impact on end users.

Powered by Adaptive Session Intelligence

The nGeniusONE platform is powered by the patent pending Adaptive Session Intelligence™ (ASI) 2.0 technology. This powerful deep packet inspection data mining engine runs on nGenius Intelligent Data Sources, generating metadata based upon actual session traffic in real-time as the packets cross the wire. This metadata is then used by the nGeniusONE platform to visualize application and network performance characteristics, enabling IT teams to quickly identify and resolve application and server performance problems. Common performance analysis use cases include understanding the root cause of application performance issues, server performance issues, and understanding or mitigating end-user impact from service degradations.

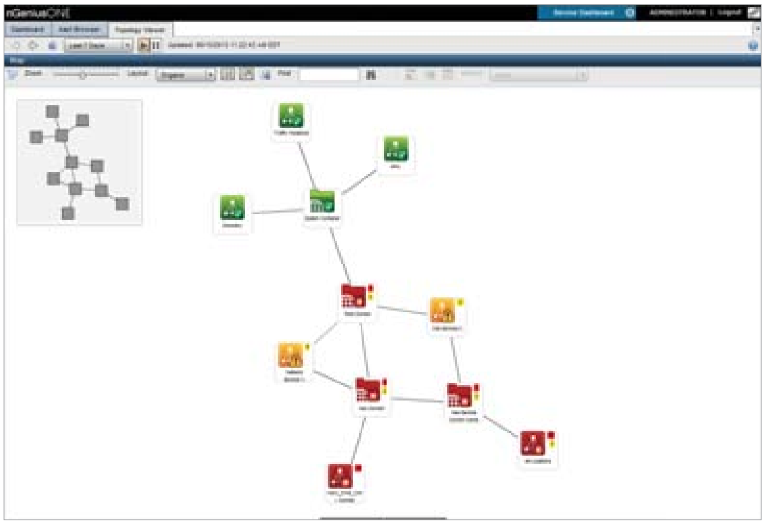


Figure 4: The nGeniusONE Service Dashboard topology map feature illustrates server and application interrelationships within a service domain.

A quick glance at the analysis views provided by nGeniusONE allow IT teams to view business-relevant details such as most active application traffic, traffic distribution among different tiers of a multi-tier application, or application specific errors at each service tier. Additional benefits of the ASI metrics include verifying that servers are properly load balanced, comparing performance among different application tiers, or visualizing interdependencies of services with other services or enabling protocols. ASI metadata is organized into three categories – Adaptive Common Data Model (A-CDM), Adaptive Session Records (ASR), and Adaptive Session Trace (AST). The highest level of metadata, A-CDM, is collected from nGenius InfiniStream appliances and stored on the nGeniusONE Server at set intervals throughout the day. ASR and AST metadata is collected and stored on nGenius InfiniStream appliances and leveraged by the nGeniusONE Session Analysis and Packet Analysis applications on-demand.

A-CDM metadata contains a full-spectrum of unique metadata intended to provide a comprehensive view of service, network, application and server performance that includes KPIs, KTIs, Key Server Indicators (KSIs) and Key Error Indicators (KEIs). This data generated by the ASI engine includes important metrics such as application traffic volumes, application server response times, server throughputs, aggregate error counts, error codes specific to application servers and domain, as well as other data related to network and application performance. These metrics are measured across multiple dimensions called location keys and used by the nGeniusONE platform to support network and application performance management workflows. These keys include information such as vlans, sites/physical location, Quality of Service (QoS) tags, and VRFs.

ASRs contain session and transaction-level metadata. This metadata contains data relating to events that occurred during the session transaction, errors observed during the session and any supplemental information extracted from the session such as requested URL, DNS query, etc. The localized processing power of the nGenius InfiniStream appliances provide a platform where millions of sessions and transactions are concurrently collected and recorded while allowing the IT user to drill down to any particular session using nGeniusONE Session Analysis. Additionally, the nGenius InfiniStream appliances provide a scalable architecture for nGeniusONE as these appliances process ASR data records in parallel across different appliances. This enables the solution to correlate transactions from across the enterprise network, providing end-to-end visibility into user sessions.

ASTs, contain a record of the actual physical packets seen traversing the network. These intelligently sliced packets take up a smaller footprint on the nGenius InfiniStream appliance thanks to optimized formatting, while still preserving the packet headers. ASTs take up less room on the disk than native packets, enable faster data mining, and can still be read by any protocol analyzer to be used for deep dive packet level decode and troubleshooting workflows.

Broad Application Support

nGeniusONE recognizes more than five hundred well-known applications out-of-the-box. Thousands of new applications and services can be created with user-defined criteria such as port ranges, source IP addresses or ranges and other filters. Flexible configuration options allow the definition of dynamic or static applications such as Web-based or custom applications. For web-based applications in particular, URL grouping is supported to allow users to logically organize their traffic. In cases where services are inter-dependent on multiple different applications, such as in multi-tier services or applications that cross data center environments, these application tiers can be aggregated in a single application group. Applications are shown in context to better expose the impact of inter-relationships and protocol dependencies on overall service delivery.

Once an application has been defined, a wealth of information regarding application responsiveness, user new/existing application sessions, application success

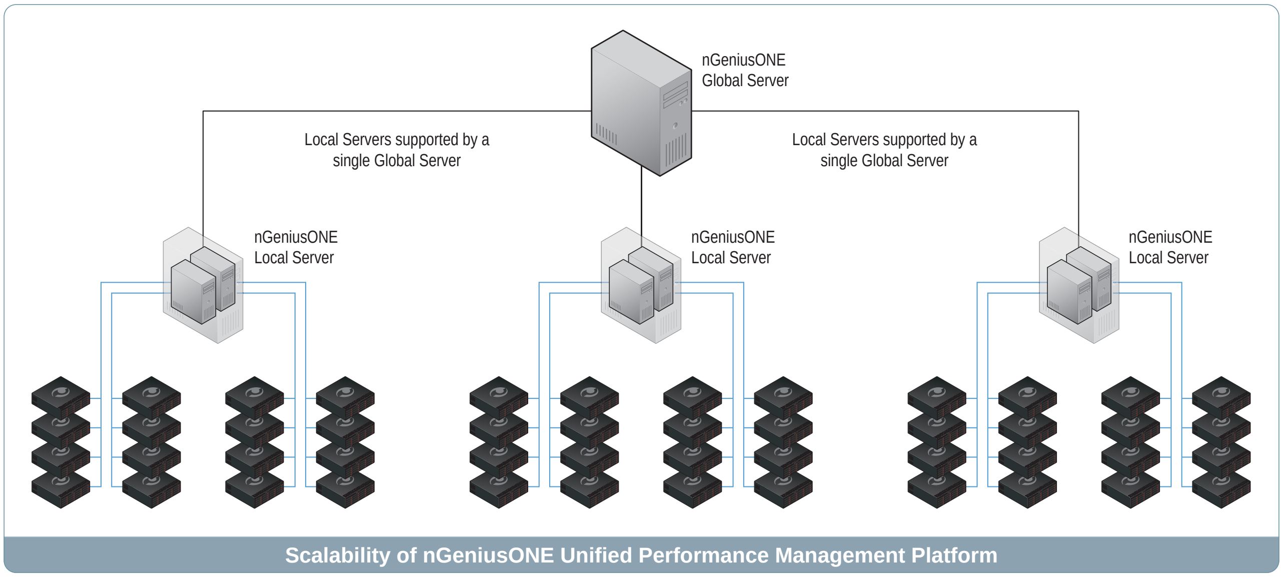

nGeniusONE
Global Server
Local Servers supported by a single Global Server
Local Servers supported by a single Global Server
nGeniusONE
Local Server
nGeniusONE
Local Server
nGeniusONE
Local Server
Scalability of nGeniusONE Unified Performance Management Platform

Figure 5: nGeniusONE has a distributed, scalable system architecture which enables unified visibility across large, geographically distributed enterprise environments.

and failures, and more can be extracted and leveraged by nGeniusONE in detailed service views.

Service-Focused Reporting

nGeniusONE includes extensive reporting capabilities to accelerate problem identification and facilitating communication and collaboration between IT teams to speed problem resolution. IT users can create scheduled template-based reports for such tasks as service performance analysis or capacity planning which are generated on a daily, weekly, or monthly basis. Reports can also be generated on-demand from nGeniusONE Service Dashboard, Service Monitors, or Traffic Monitor to support any view that IT users need for their daily monitoring activities. These reports are used to achieve objectives such as tuning traffic to optimize existing infrastructure, scoping differences between current and historic use, validating current site or application performance, or communicating service levels to business-level users.

On-demand reports are generated as a PDF, CSV or RTF file, which can then be emailed to interested users. Scheduled reports can be delivered via e-mail as either a direct URL or as a PDF, CSV or RTF attachment, or alternately displayed within the My Reports view from the Report Administrator application. Scheduled reports contain contextual drilldown links to the appropriate traffic or service monitor, making them an integral part of the simplified workflows powering the nGeniusONE platform. Robust access controls allow users to control on a per-user or role basis who has access to specified reports. Activity logging provides information to nGeniusONE administrators on the number of reports being run and who is viewing them.

Distributed Architecture for Maximum Scalability

nGeniusONE provides highly scalable coverage for complex distributed service delivery environments. Each nGeniusONE license enables monitoring of up to fifty physical interfaces, with up to two licenses supported per nGeniusONE local server. For large, geographically dispersed environments, the separately licensed nGeniusONE Global Server provides integrated access to data from multiple instances of nGeniusONE to unify and scale broad IT operations management. In a large-scale deployment, all instances of nGeniusONE are centrally managed by the nGeniusONE Global Server, presenting the appearance of a single application regardless of the actual number of nGeniusONE servers or licenses deployed. All configurations and settings are configured once on the nGneiusONE Global Server, then automatically propagated out to all nGeniusONE local servers, creating a scalable, efficient and centralized system management of the enterprise deployment. By using this distributed, scalable architecture, local processing of analytics and metadata takes place on the individual nGeniusONE local servers, speeding analysis and reducing network overhead while still providing centralized management and a single unified view into all network and application performance data from.

Resilient Operation

For additional resiliency, IT managers can deploy a separate instance of nGeniusONE to act as a hot standby server. Scripts running on both servers ensure the standby server database is kept accurate and current. If the active server fails, services can be switched over to the standby server to rapidly restore functionality with minimal effort. A standby instance of nGeniusONE requires a separately licensed nGeniusONE Standby Server.

Investment Protection

nGeniusONE platform licensing provides a scalable “pay as you grow” model. As the monitoring footprint expands, additional licenses can be added, enabling the IT organization to only pay for the coverage required.

For current users of the nGenius Service Assurance Solution, each nGeniusONE deployment also includes licenses for nGenius Performance Manager and nGenius Service Delivery Manager. This allows customers using the legacy analysis modules today to seamlessly migrate to nGeniusONE while still having access to familiar workflows and historical data.

This solution takes advantage of the same nGenius Intelligent Data Sources already deployed across a number of enterprise organizations. Many of these data sources can provide data to both the nGeniusONE platform and the previous generation nGenius Service Assurance Solution Analysis modules, preserving customer's long term investments in existing monitoring appliances.

Secure System Management with Role-Based User Management

nGeniusONE includes a streamlined graphical management interface to provide a consistent workflow across all management tasks, which improves productivity and minimizes time needed to configure and manage the platform. The central database containing all collected metadata and element settings is managed from this interface, along with server management settings, system backup configuration, message logging, software updates and user role and access permissions.

nGeniusONE securely manages the configuration of user roles and access to information. Granular permissions are defined on a per-user, per-role and per-group basis to allow each user to have only the access they need, with a searchable audit trail documenting user activity in the system. User authentication is supported through mechanisms including TACACS+, LDAP, Radius, Active Directory, and others. The system comes with six default user roles, providing a blend of read-only and administrator level functions. These user roles can be customized or new user roles can be defined. Users can be assigned multiple roles on either an individual or group basis, or access to monitored elements can be restricted, to ensure each user has precisely the right level of access needed to perform their tasks.

The configuration and settings for all nGenius Intelligent Data Sources are centrally managed from within the nGeniusONE platform. These settings include data such as application and service definitions, site groups, user communities. These settings can then be pushed globally out to all data sources, instead of requiring separate configuration of each box. From the Device Configuration view, IT users can view firmware version, decode pack versions and device health, update firmware, configure logical monitored element groupings of physical or virtual interfaces, or even remotely log into connected data sources.

Support for System Health Validation

nGeniusONE performs a number of integrity checking and reporting activities to ensure healthy operation of the platform. These capabilities include system logging and system health alarms for the nGeniusONE servers and nGenius Intelligent Data Sources, as well as more advanced usage metrics contained within the nGenius Deployment Database. System logs can be viewed on the system, or forwarded dynamically to a listening syslog server. System health alarms notify IT Administrators of issues with raid array or hardware failure, free disk space, high memory utilization, excessive processing time, and process restart within the nGeniusONE server or nGenius InfiniStream appliances. These alarms are managed in the same way as all other alarms in the system. They appear in the Service Dashboard alert browser, and can be forwarded to third party SNMP trap listeners.

The nGenius Deployment Database collects and stores information about the nGeniusONE platform deployment, including data such as installed software versions of the different nGeniusONE local servers, license summary of all installed nGeniusONE servers, server time zone, server operating system, nGenius Intelligent Data Source device types, and more. The information provided enables IT administrators to manage hardware resource allocation and software versions. The user activity log can also be accessed from this view.

Third Party Integration

nGeniusONE supports out-of-the-box integration with third-party Enterprise Management Systems (EMS) such as EMC Smarts, HP Network Node Manager and IBM Tivoli. The integration supports two-way communication flow between the EMS platform and nGeniusONE. Performance alerts generated by nGeniusONE are passed to these EMS platforms with contextual drilldown links embedded. This integration allows the nGenius Solution to become an integral part of any IT organization's troubleshooting workflow.

Product Features*

Service Dashboard	• Real-time and historical visibility into custom analytics and alarm views • Hierarchical organization of critical applications and services • Custom service definition • High level real-time service summary views
Service Monitors	• Real-time and historical visibility into service traffic • Comparative views include graphical overlays to illustrate key performance indicators • Specialized Service Monitors – Voice - Call Signalling (SCCP, SIP, H.323), Call Quality (RTP) – Service Enablers - DNS, DHCP, LDAP, Radius – Financial Services –Card transaction processing (ISO 8583), Stock trading (FIX, STAMP, OUCH) • Customizable general purpose service monitor for all other services • Drilldown into Session Analysis
Traffic Monitor	• Real-time and historical visibility into network traffic • Key volume and utilization metrics • Sort and chart traffic by location attributes • Top N applications per interface • 15 sec granularity traffic view • Drilldown into Application Delivery Monitor for service-centric view
Session Analysis	• Contextual, transaction level view of user sessions • Ladder diagram maps out transactions within a session • Contextual drilldown to Packet Analysis
Packet Analysis	• Regular-expression based custom filters on text, hex, host, application, pattern, or other string matches • Bounce charts to illustrate traffic behavior • TCP Session/Follow Stream support • Remote packet decode support • HTTPS decryption support* • Extended duration analysis from trace file merging • Save, share, import and export capture files in standard formats (cap and pcap) *requires private SSL keys or integration with hardware security module
Application classification	• Well-known protocols • Custom-defined proprietary applications • Web-based applications • Peer to peer protocols • Financial protocols and market data feeds • Voice signaling and multimedia protocols
Virtual and logical traffic elements	• Up to 50 Type 1 (physical) interfaces monitored, depending on license type • Customizable logical groupings of traffic – Site (custom subnet groupings) – VLAN – QoS groups based on DSCP tagging – MPLS VRF – User Community – Logically named group of client IP addresses – Server Community – Logically named group of client and server IP addresses – Monitored Elements – Logical groupings of physical interfaces and / or traffic matching specified location keys – Application – Logical grouping of like applications to aggregate similar types of traffic – My Network

Data Storage	• Up to one year of metadata retained on server • Configurable data granularity stored for daily, weekly, monthly intervals
Alarming	• KTI and KPI baseline and threshold-based alerts on ingress/egress bitrate, application failure rate, and application responsiveness • Time exclusions supported for baseline alerts • User notifications by visual indications in the GUI and alert notification export to up to four vendor agnostic SNMP trap listeners • Contextual drilldown into either Service Monitor or Traffic Monitor
Reporting	• Selection of pre-built reports available out-of-the-box • Customizable reports • New reports can be created on-demand or scheduled • Schedule reports for delivery at daily, weekly or monthly intervals • One-click on-demand reports from service dashboard, service monitor and traffic monitor applications • PDF, RTF and CSV format supported • Configurable user access permissions can be set on a per-report basis • Report accessed from – Email – URL – My Report view • Reporting analytics track number of reports generated, how often reports are accessed and by which users
System Management	• Up to two nGeniusONE licenses supported on a single server • Scheduled or on-demand remote firmware upgrade supported • Database backup supported – Full or incremental – Scheduled or ad hoc • User management – Granular access permissions restricted by role, group, or allowed monitored elements – Granular filters to control user access to different nGeniusONE servers in a multi-server deployment – Custom role or group definitions support – Radius, TACACS+, LDAP, Active Directory, or local authentication supported • System health monitoring – Measurement of system CPU and memory – System health alarms generated – Server log entries exportable via syslog • Device health monitoring – Measurement of device CPU and memory – Device health alarms generated – Device log entries exportable via syslog • Deployment database analytics – User statistics – User activity log – nGeniusONE system deployment details such as: – Server type summary – License summary – Firmware version summary – User account summary – Data Source summary, including device type counts and firmware versions

Supported Data Sources	• ASI 2.0 views require nGenius InfiniStream appliances running version 5.1 or later • ASI 1.0 views support the following: – All nGenius Intelligent Data Sources running version 4.12 or later – SNMPv2 and SNMPv3-capable devices
Third Party Integration	• HP Network Node Manager (NNMI) • IBM Tivoli® NetView, Netcool/OMNIbus • EMC® Smarts® • HP Arcsight

*Note: All features described are based upon nGeniusONE Release 5.1.1.

Minimum Hardware Recommendations

Component	Specification
Operating system	Red Hat® Enterprise Linux® v6.x 64-bit (English only) Windows® 2008 R2 x64 - Standard and Enterprise
Processors	Dual 2.4Ghz Quad-Core processors with multithreading support
Available Operating System Memory	24 GB RAM with swap space equal to twice the capacity of physical memory
File system (Windows platforms)	• Minimum 30 GB for the OS partition (if installing nGeniusONE on a second partition) • Virtual memory page file set for System Managed Size • NTFS-formatted hard disk is required
File system (Linux platforms)	• Minimum 100 MB for the boot partition • Minimum 10 GB for the OS or / (root) partition
RAID Configuration	RAID 5; Ultra 320 SCSI, SATA, or SAS
Hard Drive Configuration	3 TB
Media Device	DVD-ROM drive
Network Adapter	One 100/1000 Ethernet adapter
Power Supply Configuration	Dual, redundant power supplies
IP Address	Static IP address

Ordering Information

Part Number	Description
9600L-DGM	nGeniusONE Global Server (Linux) Dedicated Global Manager for distributed server environments. Does not support local device management.
9600L-ENT1	nGeniusONE (Linux) Permanent license for use up to 50 Type 1 interfaces and 10,000 Type 2 interfaces.
9600L-STB1	nGeniusONE Standby Server (Linux) Permanent license for use up to 50 Type 1 interfaces and 10,000 Type 2 interfaces
9600L-INC1	nGeniusONE – Incremental License (Linux) The Incremental license extends an existing nGeniusONE License by up to an additional 50 Type 1 interfaces and 10,000 Type 2 interfaces.
9600L-WG1	nGeniusONE (Linux) Permanent license for up to 10 Type 1 interfaces and 2,000 Type 2 interfaces.
9600W-DGM	nGeniusONE Global Server (Windows) Dedicated Global Manager for distributed server environments. Does not support local device management.
9600W-ENT1	nGeniusONE (Windows) Permanent license for use up to 50 Type 1 interfaces and 10,000 Type 2 interfaces.
9600W-STB1	nGeniusONE Standby Server (Windows) Permanent license for use up to 50 Type 1 interfaces and 10,000 Type 2 interfaces.
9600W-INC1	nGeniusONE – Incremental License (Windows) The Incremental license extends an existing nGeniusONE License by up to an additional 50 Type 1 interfaces and 10,000 Type 2 interfaces.
9600W-WG1	nGeniusONE (Windows) Permanent license for up to 10 Type 1 interfaces and 2,000 Type 2 interfaces.

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

nGenius Integrated Agent for Cisco Integrated Services Router

An nGenius Intelligent Data Source enabling cost-effective visibility into network and application performance in branch office environments

Highlights

- Simplifies and consolidates deployment of service assurance capabilities in the branch office
- Tracks user experience and application and network performance
- Real-time application performance and response time metrics help predict and prevent service delivery degradations
- Accelerates problem resolution to minimize the impact of branch office network and application degradations
- Easily integrates with Cisco® Integrated Services Router to lower the cost of service assurance in the branch office

nGenius Integrated Agent

The nGenius® Integrated Agent software is self-contained virtualized probe software that is integrated and deployed within a third-party network device to provide high-definition, packet-flow visibility at logical network boundaries. With the identical functionality of a hardware-base nGenius Probe, the nGenius Integrated Agent provides scalable packet-based monitoring and analysis of traffic traversing the network to feed valuable service delivery metrics to the nGenius Solution. Optimized for deployment in the branch office and at the network edge, nGenius Integrated Agent provides always-on, granular visibility into LAN and WAN environments, generating rich metadata on key performance metrics such as traffic, application and service utilization, conversations, error conditions, resource utilization, response time, and many others.

Deployed as part of a pervasive instrumentation strategy, the nGenius Integrated Agent removes the barriers to achieving visibility in more places by cost-effectively extending this visibility closer to the user. Each nGenius Integrated Agent instance appears to the nGenius Performance Manager as any other probe device would, enabling the IT organization to track service delivery from the data center to the desktop over the WAN to the branch office. The nGenius Solution combines metrics from the nGenius Integrated Agent with other distributed nGenius hardware and software-based intelligent data sources, enabling the IT organization to achieve an unmatched global perspective of their service delivery network to enable the user experience, greater business value, and simplify the end-to-end management.

The nGenius Integrated Agent delivers:

- **Network visibility** - Key network metrics, such as traffic, application and service utilization, conversations, error conditions, resource utilization, and response time on physical and virtual links
- **Application recognition and monitoring** - Tracks voice, Web, custom and well known applications and services in order to provide an all-encompassing view of the landscape, including all branches
- **Key Performance Indicators** - Real-time visibility into the health of applications and services from a user experience perspective using advanced metrics, such as response times, errors, and packet loss/jitter
- **Convergence management** - View voice, video, and data metrics together to achieve an end-to-end view of the service delivery network's performance
- **Alarming and event notification** - Provides real-time notifications for threshold violations, as well as, power alarms with millisecond resolution to quickly detect and begin investigating the root cause of complex service delivery issues
- **On-demand packet capture** - Supports local packet capture enabling deep packet analysis to identify the root cause of difficult performance issues more easily

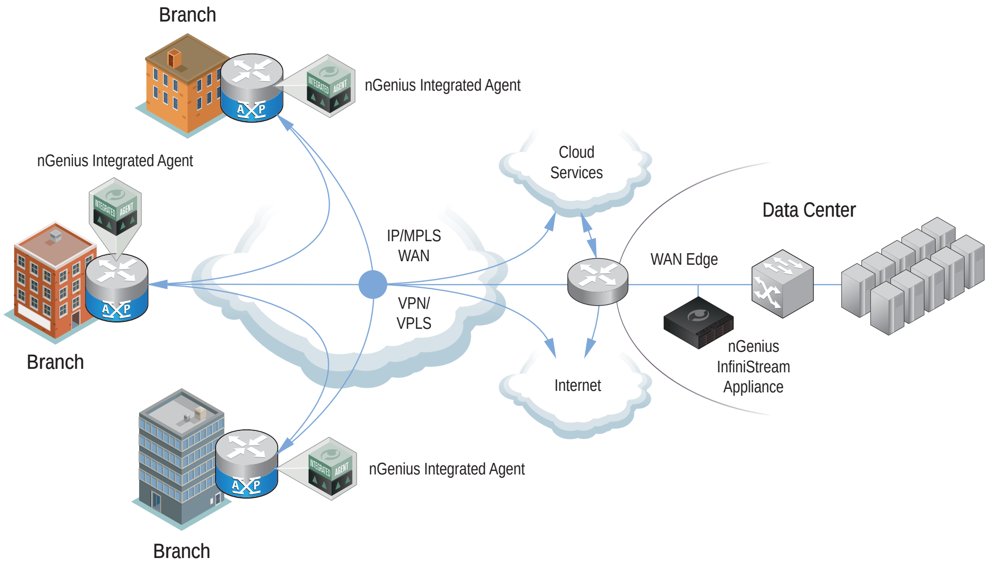


Figure 1: Instrumenting nGenius Integrated Agent at branch locations facilitates monitoring end-to-end as well as site-to-site.

nGenius Integrated Agent for Cisco Integrated Service Routers

The nGenius Integrated Agent for Cisco Integrated Services Router (ISR) cost-effectively brings always-on, end-to-end service assurance to the branch office. With nGenius Integrated Agent, IT organizations gain real-time visibility and comprehensive reporting for branch office traffic to reveal how remote network resources are being utilized, how applications and services are behaving, and how remote users are experiencing the services being delivered. As a result, IT staff has consistent and unified insight into the branch office environment in the same manner, and with the same granularity, as the data center and campus network. The combined Cisco and NetScout solution makes managing today's borderless enterprise easier by enabling a truly unified view of the global service delivery environment to assure all users have a consistent experience regardless of location.

Leveraging the powerful services virtualization capabilities of the Cisco Application Extension Platform (AXP), organizations gain the benefits of unified service delivery management without increasing the hardware footprint and complexity in the branch. This reduces the cost of operations by freeing up valuable rack space, reducing management complexities, simplifying remote location asset management, and reducing power consumption. Consequently, this enables IT staff to architect a comprehensive unified service delivery management strategy that can scale to cope with current and future demands from a widening array of services and applications while further extending their view of network and application performance.

Key benefits of integration into Cisco ISR platforms include:

- Real-time operational status with intelligent early warning of emerging performance issues in the branch office
- Consistent and unified end-to-end visibility from the data center to the branch office to assure business service continuity
- Granular, always-on view into service consumption, network and application performance, and remote user experience helps to optimize the WAN and branch office network for peak performance and efficiency
- Local visibility simplifies and speeds remote troubleshooting minimizing need for technician dispatch and dramatically reducing problem resolution time
- Enables improved operational efficiency and reduced management complexity and cost of branch office service assurance

Integration with Cisco Integrated Services Routers

The nGenius Integrated Agent software is seamlessly deployed within Cisco 2800 and 3800 Series ISR and the Cisco 2900 and 3900 Series ISR Generation 2 using the Cisco AXP and a Cisco Service Module. Cisco AXP provides a standards-based Linux® environment that hosts and integrates the nGenius Integrated Agent software within the Cisco ISR platform. The Cisco AXP hosting environment provides dedicated infrastructure to securely install, host and manage the nGenius Integrated Agent software. The Cisco Service Module provides dedicated processing and interface capabilities into network traffic independently of the host router resources. This independence helps ensure maximum concurrent routing and application performance while reducing physical footprint, lowering power consumption, and consolidating management. Depending on the chosen service module and Cisco ISR, the nGenius Integrated Agent software can be installed locally or remotely, enabling a high degree of flexibility to allow the IT organization to quickly deploy extended monitoring to virtually any branch office location.

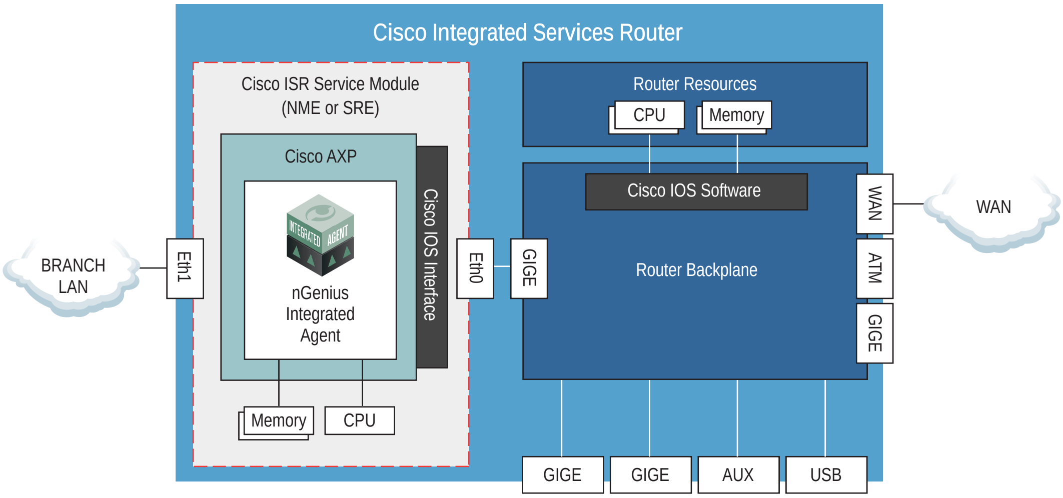


Figure 2: The router backplane interface (Eth0) is used to continuously monitor traffic destined for the WAN while the external Ethernet interface (Eth1) is used to continuously monitor traffic of the branch LAN.

The nGenius Integrated Agent runs in a virtual application instance on the AXP module within the Cisco ISR and leverages the Cisco packet API to collect and process network traffic on both the router backplane and an external Gigabit Ethernet interface. Typically the router backplane interface is used to continuously monitor the traffic to and from the WAN while the external Gigabit interface is typically used for local LAN based traffic monitoring and troubleshooting activities, see Figure 2. The metadata derived from these packet-flows is leveraged by the nGenius Solution for real-time analysis and reporting.

Key Capabilities

Automatic Recognition and Monitoring of Applications

Support for a variety of application types, including:

- Well-known and derivatives of well-known applications
- User-defined and custom-developed applications
- Peer-to-peer applications
- Web-based applications and URLs

On-Demand Packet Analysis

- Short-term packet capture (up to 1 GB of data)
- Packet capture may be triggered manually or based upon a specific event or alarm

Response Time Analysis and Key Performance Indicators

- Based upon packet loss, inter-packet delay, client and server errors, and timeouts
- Passive application responsiveness measurements for virtually all application and service types
- One-minute granularity for average response time, number of active sessions, number of successful transactions, and number of server error types
- 15-minute granularity for maximum and average response time per client/server pair, total number of transactions, number of successful transactions, TCP connect time, number of active sessions, total packet loss, responses time distribution, number of timeouts, number of retries, and application payload

Convergence Management Metrics

- Volume, utilization, host, and conversation details for RTP Voice and Video protocols
- Application-layer details for call set-up protocols, such as SIP, H.323, Q.931, and MGCP, plus Cisco's SCCP and Avaya's H.323 extensions
- VoIP quality metrics: jitter, call set-up time, packet loss, incomplete and failed calls
- IP addresses, phone extensions, and connect times
- Packet-level visibility and decode of voice protocols
- Voice configuration data including Codec, dialing plan, and QoS assignments

Network Management Metrics

- TCP, HTTP and server-specific performance, and error conditions
- Percent Utilization and Packet/Byte Counts for: link, host, host group, applications, conversations

Alarming and Event Identification

- Define alarms for link utilization, application utilization, application response time, application availability
- Burst Alarms at millisecond resolution
- “Power Alarms” highlight root cause by gathering top users and applications automatically at violation time for segments exceeding utilization, responsiveness, and availability thresholds
- Supports rising, falling, and time-over-threshold templates

Data Granularity

- 15-second real-time views with 1-second peaks
- 1-minute historically logged data for all application, hosts, and conversation flows

Requirements

- nGenius Performance Manager v4.11 MR1 or higher
- Other analysis modules supported by nGenius Performance Manager v4.11 or higher are supported
- Cisco IOS® Software version
- Cisco IOS software release 12.4(24)T2, 15.0(1)M or higher

Cisco IOS Software version

- Cisco IOS® software release 12.4(24)T2, 15.0(1)M or higher

Cisco AXP Software

- AXP software version 1.5.3 or higher

Cisco Integrated Services Router Requirements

The nGenius Integrated Agent is supported on the Cisco Integrated Services Router and the Cisco Integrated Services Router Generation 2 series. The agent software is deployed on a Cisco enhanced network module (NME) or Services Ready Engine (SRE) Service Module in conjunction with the Cisco AXP software.

	Cisco ISR Models									
AXP Model Number	2811	2821	2851	3825	3845	2911	2921	2951	3925	3945
NME-APPRE-502-K9	●	●	●	●	●					
NME-APPRE-522-K9				●	●					
SM-SRE-700-K9						●	●	●	●	●
SM-SRE-900-K9						●	●	●	●	●

Figure 3: Supported AXP models for Cisco ISR models.

Notes:

- Performance levels will vary depending host network equipment environment and performance characteristics
- For complete compatibility and system requirements, refer to related Cisco documentation

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
Suite 101
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
Room 105, 17F/B, No. 167
TunHwa N. Road
Taipei, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square 29th floor
Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

nGenius Collector 3300 Series

Scalable, high capacity appliance for collection of Cisco NetFlow and other Flow data

Highlights

- Measure service responsiveness across the network with up to five hundred Cisco IP SLA synthetic transaction tests
- Scalable collection of up to two million Cisco® NetFlow, Juniper® J-Flow, Huawei NetStream and sFlow flows per minute
- Captures and stores Flow datagrams for historical deep-dive analysis
- Collects Flow data from up to five thousand flow-enabled router or switch interfaces per appliance
- Supports both IPv4 and IPv6 environments

Product Overview

The nGenius® Collector 3300 series is a high capacity appliance that collects Flow data, such as Cisco® NetFlow, Juniper® J-Flow, sFlow and NetStream, from Flow-enabled routers and switches for analysis by nGenius Performance Manager for Flows. The appliance analyzes Flow datagrams, generates key metadata and maps this information into NetScout's Adaptive Session Intelligence™(ASI) A-CDM tables in real-time. In addition, the appliance dynamically discovers Cisco routers and switches which have been configured to run Cisco IP SLA tests, then polls those devices for the results at fixed intervals. The nGenius Collector converts Flow records that include conversation information, such as source and destination IP addresses, type of service bytes (ToS or DSCP), application port numbers and Autonomous System numbers (ASN) into a common data model that is usable by nGenius NetFlow Analytics Modules in the solution. IT Administrators are able to capitalize on their existing investment and minimize total cost of ownership by using this appliance to incorporate access to Flow and IP SLA data into a comprehensive monitoring strategy.

nGenius Collector is a hardened Linux®-based appliance containing a one terabyte TB hard drive and dual power supplies. The operating system is optimized for a secure, fast, and efficient data collection. The kernel receives in depth security scans for different security issues to identify and remediate vulnerabilities in support of a highly secure operating environment. The hard drive enables the continuous capture and storage of actual Flow datagrams (Native Flow Records), enabling deep dive analysis and troubleshooting capabilities.

Product Capabilities

- Monitors up to 5000 switch or router interfaces per appliance across the enterprise
- Collects up to two million NetFlow, J-Flow, sFlow and NetStream flows per minute
- Detects and collects the results of up to 500 IP SLA tests
- Continuously captures and stores Cisco NetFlow datagrams for decode and analysis
- Supports both IPv4 and IPv6 environments

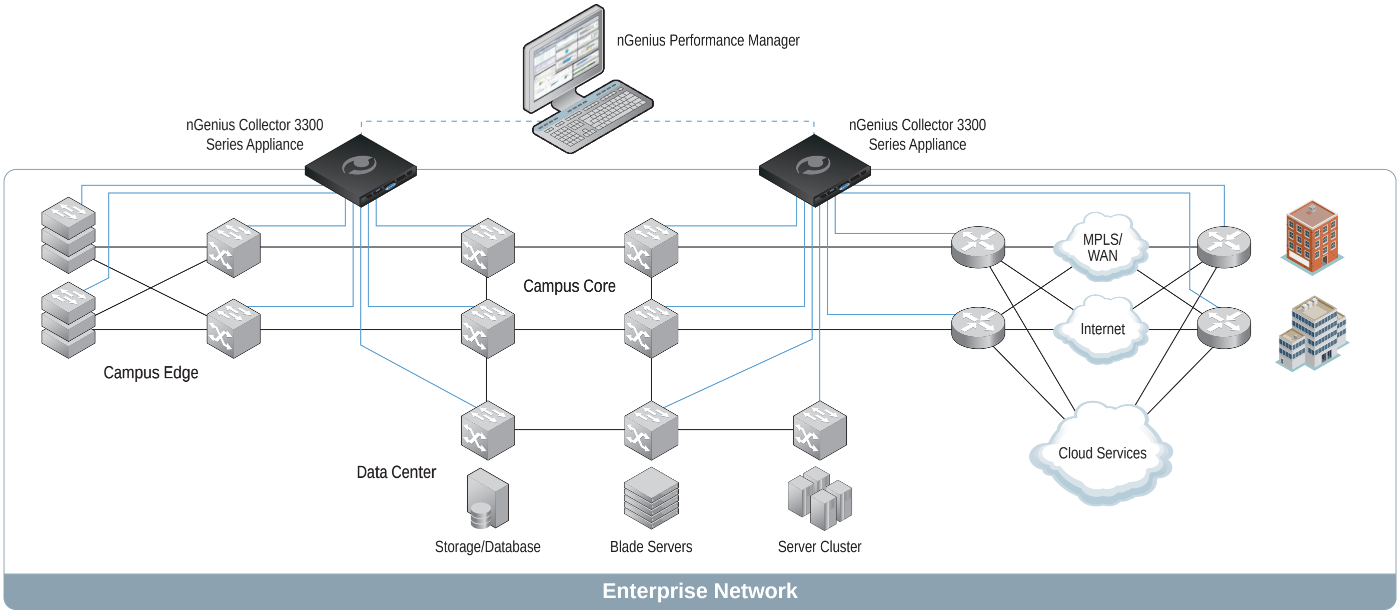


Figure 1: nGenius Collector supports large-scale, high capacity Flow collection from across the enterprise.

Leverage Existing Infrastructure Investments

nGenius Collector appliances are commonly deployed in data centers or other core locations, and configured to receive data from Flow-enabled routers or switches located anywhere in the network. The appliance does not need to be physically deployed in the same location as a targeted switch or router. This flexibility enables Flow coverage for very large or distributed environments with just a few strategically placed appliances to collect data from thousands of remote router and switch interfaces.

Troubleshoot NetFlow Deployments With Continuous Datagram Capture

Built-in capture mechanisms in the nGenius Collector enable the appliance to continuously capture and store NetFlow datagrams. nGenius Performance Manager for Flows decodes and analyzes captured datagrams. Decodes are supported for NetFlow versions 5 and 9. This decode support is most commonly used by IT operators to troubleshoot NetFlow deployments to validate that the configurations on their routers and switches are set to export the correct information and level of detail.

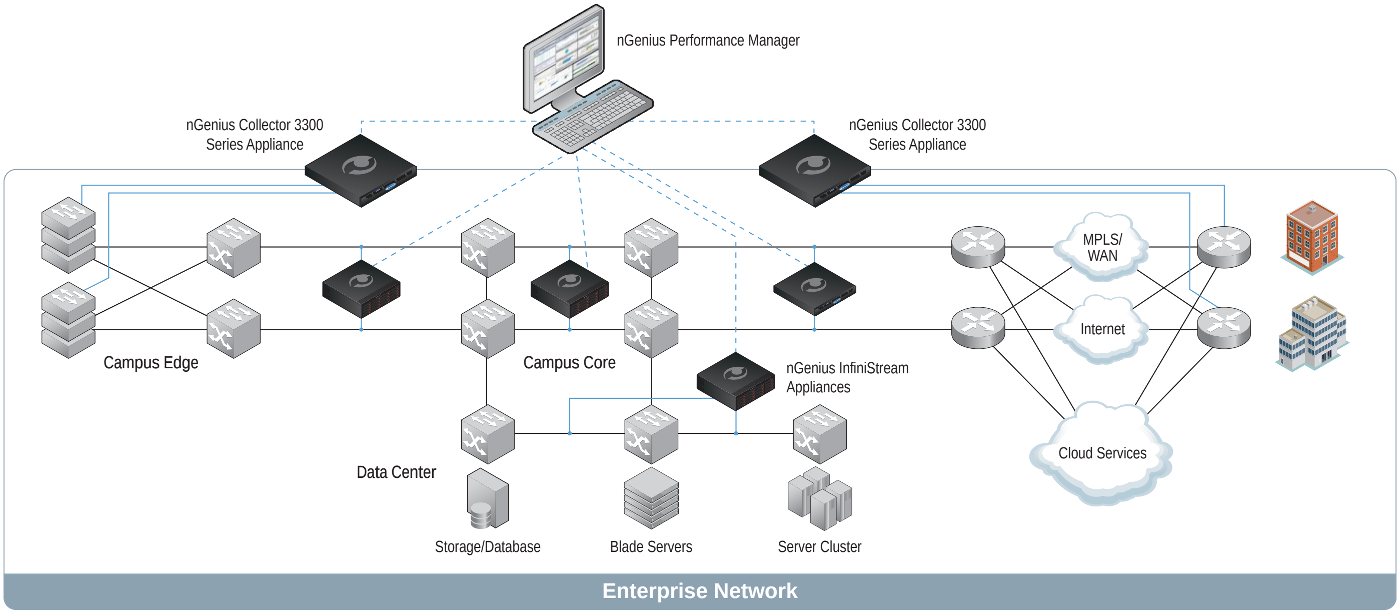
Measure Responsiveness of Network Services With IP SLA

nGenius Collector dynamically discovers IP SLA tests configured on the Cisco routers or switches and then polls those devices for the test results. IP SLA provides embedded Cisco IOS® functionality allowing the router or switch to measure application responsiveness using synthetic transactions. These tests are used to measure network performance and availability across the network, enabling IT personnel to detect problems before they affect actual user experience.

Comprehensive Flow-Based Support

The nGenius Collector is a high-capacity appliance supporting large volume traffic requirements. It allows IT Administrators to incorporate Cisco IP SLA, Cisco NetFlow, Juniper J-Flow, sFlow and NetStream metrics into a global monitoring strategy. The appliance collects the data used by nGenius NetFlow Analysis Solution to compile high level metrics – such as top hosts, top talkers, application utilization and QoS usage – across the entire organization in a cost effective manner.

Using information collected from all nGenius Collector appliances, the nGenius NetFlow Analysis Solution obtains a comprehensive view to provide advanced alarming, trending and analysis, capacity planning, troubleshooting and QoS validation in unified views.


nGenius Performance Manager
nGenius Collector 3300 Series Appliance
nGenius Collector 3300 Series Appliance
MPLS/ WAN
Internet
Cloud Services
Campus Edge
Campus Core
nGenius InfiniStream Appliances
Data Center
Storage/Database
Blade Servers
Server Cluster
Enterprise Network

Monitoring Features

Flow Types Supported	• Cisco NetFlow version 5 and 9 • Juniper J-Flow version 9 (based on NetFlow version 9) • sFlow versions 2, 3, 4 and 5 • Huawei NetStream (based on NetFlow versions 5 or 9)
Flow fields supported	• IPv4 and IPv6 Source IP address • IPv4 and IPV6 Destination IP address • Source port number (TCP or UDP) • Destination port number (TCP or UDP) • Layer 3 protocol type (IP, ICMP) • Type of Service (ToS) byte (DSCP) • Autonomous System Number
Cisco IP SLA tests supported	• DHCP – Measures the round-trip time taken to discover a DHCP Server and obtain a lease • DNS – Difference in the time from when the client sends a DNS request to when it receives a reply • ICMP Echo – Measures round trip time for how long it takes the target device to respond to an ICMP echo • UDP Jitter (VoIP) – Measures round-trip delay; include average jitter, or both jitter and MOS, as well as packet loss • TCP Socket Connect – Difference in the time from when the client sends the initial SYN to when the client sends the final ACK in the connect sequence • Web Page Retrieval – Measures time to retrieve the specified web page. Also measures the TCP connect time
Data Collection	• Measure up to 500 IP SLA tests • Monitor up to 5000 monitored interfaces in interface mode • Collect up to two million flows per minute
Flow Record Packet Capture and Decode	• Continuous capture mechanism captures datagrams from Flow-enabled devices • Decodes supported for NetFlow version 5 and 9 • Analyze datagrams via packet capture
Data Granularity	• 1 minute granularity for Flow data* • 15 minute granularity for IP SLA test results • Database supports historically logged data for applications, hosts and conversation flows *data granularity depends on router configuration
Supported Authentication Methods via nGenius Server	• TACACS • LDAP • Active Directory • Password

Hardware Specifications

Capacity	
LAN Ports	1 x 10/100/1000Base-T (RJ45)
Operating System Storage	One 32 GB Solid State Drive (SSD) Dedicated to operating system
Datagram Capture Storage Type	SATA drive, 7200 RPM
Data Storage Capacity (TB)	1
Data Storage Redundancy	Raid 0
Console Port	1xEIA/TIA-232 (DE-9)
Management Port	1 x 10/100/1000Base-T (RJ45)
Power Supply Type	Internal, hot swappable
Power Supply Redundancy	1+1
Air Flow	Front to back
Physical, Environmental, and Power	
Height (RU)	1
Rackmount Rail	Included
Dimensions	17.09" W x 1.69" H x 24" D (in) 43.4 W x 4.29 H x 60.96 D (cm)
Weight	33.02 lb 15 kg
Operating Temperature	50° to 95°F 10° to 35°C
Storage Temperature	–40° to 149°F –40° to 65°C
Operating Relative Humidity	8% to 85%, non-condensing
Storage Relative Humidity	5% to 95% , non-condensing
Max. AC Power Consumption (W)	183W @ 100 – 240 VAC, 50/60Hz
Max. Thermal Output for AC (Btu/h)	624 BTU/Hr
Altitude (Operating)	–50 to 10,000 ft (–16 to 3,048 m)
Altitude (Storage)	–50 to 35,000 ft (–16 to 10,600 m)
Regulatory and Agency Approvals	Regulatory Model Number: E07S FCC Class A, CE Mark (EN 55022 Class A, EN 55024, EN 6100-3-2, EN 61000-3-2), VCCI(Japan) Class A, UL 60950-1 CAN/CSA C22.2 No. 60950, EN 60950, CB Report UL-GS (DEMK0)

Solution Requirements

nGenius Performance Manager for Flows	Version 5.0 or later

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NetScout offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NetScout at 800-309-4804 or +1 978-614-4000

DATA SHEET

IdentiFi™ AP3710i/e

High Performance, Enterprise-Grade for High-Density Deployments

BENEFITS

BUSINESS ALIGNMENT

- Support for demanding voice/video/data applications to enhance mobile worker productivity and convenience
- Role-based grouping of users, devices, and applications to deliver priority, QoS, and security in accordiance with business needs
- Seamless roaming across an entire multi-subnet campus without the need for cumbersome client software.
- Integrated management, security, and QoS features reduce operating cost and ensure a consistent user experience regardless of location.

OPERATIONAL EFFICIENCY

- Centralized visibility and control from Extreme Networks Wireless Management Suite and Extreme Networks NMS accelerate problem resolution, optimize network utilization, and automate management
- Adaptive architecture reduces complexity and optimizes information flow for each application
- Dynamic Radio Management ensures optimal AP coverage and maximizes the availability and quality of wireless service across the enterprise
- Flexible Client Access optimizes throughput for 802.11n clients in today's mixed a/b/g and n client environments

SECURITY

- Authentication and authorization functions include role-based access control (using 802.1X, MAC, and captive portal) and authentication at the AP
- Wireless Intrusion Prevention (WIPS) functions provide continuous scanning, threat classification, rogue AP detection, and countermeasures against possible attacks
- Integration of security policies (NAC, IPS) across the wired/wireless networks enables quick diagnosing and resolution of security threats
- Integration of Policy Manager across the wired/ wireless networks dynamically oversees user access at the wireless network point of entry

SUPPORT AND SERVICE

- Industry-leading customer satisfaction and first call resolution rates
- Lifetime warranty for indoor access points
- Personalized services, including site surveys, network design, installation, and training

Overview

The AP3710 is a high-performance 802.11abgn indoor access point purposed built for high-density deployments. This access point is designed to operate in heavy-user environments such as universities, schools, hotel lobbies, conference centers, and stadiums. The high-performance AP is equally adept at serving high-bandwidth video applications as well as low-latency voice applications. The AP3710i comes with an integrated six antenna array for ease of installation. The AP3710e requires professional installation and includes six RP-SMA antenna connectors supporting both 2.4G and 5G band antennas. The access points can be powered via 802.3af power or an optional external power adpater.

The AP3710 comes packed with the latest in WiFi technology including dynamic radio management, spectrum analysis with interference classification, beamforming, self-forming and self-healing meshing, security, role-based authentication, authorization, and access control. The 3x3:3 platform is capable of delivering 900Mbps over-the-air-performance and up to 75,000 packets per second on the wire port. Multiple antenna offerings (e.g., omni, sector, panel) ensure that the AP3710e deployment can be optimized to meet any coverage or capacity need.

Technical Specifications

PRODUCT FEATURES	AP3710I/E
GENERAL	
High performance enterprise class AP	√
Number of radios	2
MIMO implementation for high performance 11n throughputs	3x3
Number of spatial streams	3
Maximum Throughput Per Radio / Total	450Mbps / 900Mbps
Wired performance in packets per second (pps)	75,000 pps
Number of SSIDs supported per radio / total	8 / 16
Simultaneous users per radio / total	127 / 254
Mode of operation	Semi-autonomous
Plug and play operation/Zero touch deployment	√
AP and the controller run the same firmware versions	√
Security and Standards	WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, X509 DER / PKCS #12
MULTIPLE OPERATING MODES	
Clients serving access points	√
Intelligent thin AP	Encryption, Security, QoS and RF management done on AP
Bridging data traffic at AP and/or at controller simultaneously	√
Simultaneous RF monitoring and client services	√
Integrated in-channel WIDS	√
Integrated in-channel WIPS	√
Integrated remote access point	√
Integrated RF spectrum analysis and fingerprinting	√
Integrated self-forming and self-healing meshing	√
HYBRID OPERATION	
Perform security scanning and serve clients on same radio	√
Perform security scanning and spectrum analysis on same radio	√
Perform spectrum analysis and serve clients on same radio	√
RADIO CHARACTERISTICS	
Max transmit power	
Radio 1 (5GHz)	23 dBm
Radio 2 (2.4GHz)	23 dBm
Max antenna gain (integrated antenna)	
Radio 1 (5GHz)	3 dBi (AP3710i)
Radio 2 (2.4GHz)	3 dBi (AP3710i)
ADAPTIVE RADIO MANAGEMENT	
Dynamic Channel Control	
Efficient use of the spectrum with a multi-channel architecture	802.11h: DFS & TPC support (ETSI)
Automatic transmit power and channel control	√
Self-healing with coverage gap detection	√
Band steering with multiple steering modes	√
Spectrum load balancing of clients	√
Airtime fairness	√
Performance protection in congested RF environments	√
Mitigates co-channel interference with coordinated access	√
Mitigates adjacent channel interference with optimized receive sensitivity	√
Efficient reuse of channels at shorter intervals	√

Mitigates non 802.11 inference without dedicated radios	√
QOS FOR APPLICATIONS	
Quality of Service (WMM, 802.11e)	√
Call Admission Control (TSPEC)	√
Power Save (U-APSD)	√
Fast secure roaming and handover between APs	√
Pre-Authentication (Pre-Auth)	√
Opportunistic Key Caching (OKC)	
Multicast Rate Control	√
Support voice, video and data using the same SSID	
Prioritize voice over data for both tagged and untagged traffic	√
Rate limiting (rule and user-based)	
Rule and role based QoS processing	√
WIRELESS SERVICES	
Media Access Protocol	CSMA/CA with ACK
Data Rates	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11b: 1, 2, 5.5, 11 Mbps 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps 802.11n: See 802.11n Performance table below
Frequency Bands	**802.11a/n:** • 5.15 to 5.25 GHz (FCC / IC / ETSI) • 5.25 to 5.35 GHz (FCC / IC / ETSI) • 5.47 to 5.725 GHz (FCC / IC / ETSI) • 5.725 to 5.850 GHz (FCC / IC) **802.11b/g/n:** • 2.400 to 2.4835 GHz (FCC / IC / ETSI)
Wireless Modulation	802.11a: OFDM 802.11b: DSSS 802.11g: DSSS and OFDM 802.11n: BPSK, QPSK, 16QAM, 64QAM with OFDM 802.11n High-throughput (HT) support: HT 20/40 802.11n Packet aggregation: A-MPDU, A-MSDU 802.11n Advanced Features: LDCP, STBC and TxBF
INTERFACES	
# 10/100/1000 Base T Ethernet autosensing link	1
Console port for the ease of installation and management	√
MOUNTING	
Wall mounting bracket	√
Drop-ceiling mounting bracket	Optional
Environmental	**Plenum rated Operating:** Temperature 0º C to +50º C (+32º F to +122º F) Humidity 0% 95% (noncondensing) **Storage:** Temperature 5º C to +50º C (+23º F to +122º F) **Transportation:** Temperature 40º C to +70º C (40º F to +158º F)

Compliance	• FCC CFR 47 Part 15, Class B • ICES-003 Class B • FCC Subpart C 15.247 • FCC Subpart E 15.407 • RSS-210 • EN 301 893 • EN 300 328 • EN 301 489 1 & 17 • EN / UL 60601-1-2 • EN 50385 • EN 55011 (CISPR 11) Class B Group 1 ISM • EN 55022 (CISPR 22) • AS/NZS3548 (CISPR22) **International (including China)** • IEC 60950-1 • IEC 60825 **Europe** • EN 60950-1 • EN 60825 **USA / Canada / Mexico (NAFTA)** • UL 60950-1 • CSA 22.2 No.60950-1-03 **Australia** • AS/NZS 60950.1
MECHANICAL	
Dimensions (W x H x L)	(7.39" x 1.50" x 7.89") – AP3710i (9.44" x 1.50" x 7.89") – AP3710e
Weight	810g – AP3710i 910g – AP3710e
Max power consumption	12.8W
Warranty	Lifetime

Ordering Information

PART NUMBER	DESCRIPTION
ACCESS POINTS	
WS-AP3710i	Dual Radio 802.11a/b/g/n, 3x3:3, indoor access point with six internal antenna array
WS-AP3710e	Dual Radio 802.11a/b/g/n, 3x3:3, indoor access point with six reverse polarity SMA connectors for external antennas
ACCESSORIES	
WS-MB3700-01	Drop ceiling mounting bracket for the 3710/25 Series
Antennas	
WS-AI- ...	
WS-AI-DT05120	Dual-band, dual-feed, sector, 5 degree, 20dBi antenna (Direct connect)
WS-AI-DX05360	Dual-band, six-feed, omni, 5dBi antenna (Direct connect)
WS-AI-...	
CABLES	
WS-CAB-PT20P	20 inch pigtail with reverse polarity type-N plug to connect AP to lightning protector or directly to antenna
WS-CAB-PT20J	20 inch pigtail with reverse polarity type-N jack; used to connect AP to the LMR cables
WS-CAB-LPM	Dual-band lightning protector with reverse polarity type-N jack on both ends
WS-CAB-L200C20	20 foot LMR200 cable with reverse polarity type-N plugs on both ends
WS-CAB-L400C06	6 foot LMR400 cable with reverse polarity type-N plugs on both ends
WS-CAB-L400C50	50 foot LMR400 cable with reverse polarity type-N plugs on both ends
WS-CAB-L400C75	75 foot LMR400 cable with reverse polarity type-N plugs on both ends
WS-CAB-L600C25	25 foot LMR600 cable with reverse polarity type-N plugs on both ends
WS-CAB-L600C50	50 foot LMR600 cable with reverse polarity type-N plugs on both ends

802.11n Performance Data Rates (Mbps)

2.4GHZ/5GHZ					
	SPATIAL STREAMS	HT20 NORMAL GI	HT20 SHORT GI	HT40 NORMAL GI	HT40 SHORT GI
MCS0	1	6.5	NA	13.5	15
MCS1	1	13	NA	27	30
MCS2	1	19.5	NA	40.5	45
MCS3	1	26	NA	54	60
MCS4	1	39	NA	81	90
MCS5	1	52	NA	108	120
MCS6	1	58.5	NA	121.5	135
MCS7	1	65	72.2	135	150
MCS8	2	13	NA	27	30
MCS9	2	26	NA	54	60
MCS10	2	39	NA	81	120
MCS11	2	52	NA	108	150
MCS12	2	78	NA	162	180
MCS13	2	104	NA	216	240
MCS14	2	117	NA	243	270
MCS15	2	130	144.4	270	300
MCS16	3	19.5	NA	40.5	45
MCS17	3	39	NA	81	90
MCS18	3	58.5	NA	121.5	135
MCS19	3	78	NA	162	180
MCS20	3	117	NA	243	270
MCS21	3	156	173.3	324	360
MCS22	3	175.5	195	364.5	405
MCS23	3	195	216.7	405	450

Warranty

As a customer-centric company, Extreme Networks 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.

Extreme Networks indoor Wireless Access Points come with a lifetime warranty. All Extreme Networks Wireless Access Points come with a one year warranty against manufacturing defects. For full warranty terms and conditions please go to:

www.extremenetworks.com/support/warranty.aspx.

Service & Support

Extreme Networks 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 Extreme Networks account executive for more information about Extreme Networks Service and Support.

http://www.ExtremeNetworks.com/contact / Phone +1-408-579-2800

DATA SHEET

Wireless Appliance

High-performance, Enterprise-class WLAN Appliance

BENEFITS

BUSINESS ALIGNMENT

- Support for demanding voice/video/data applications to enhance mobile worker productivity and convenience
- Role-based grouping of users, devices, and applications to deliver priority, QoS, and security in accordance with business needs
- Integrated management, security, and QoS features reduce operating cost and ensure a consistent user experience regardless of location
- Key element of mobility solutions that enable VoWLAN and dual-mode devices

OPERATIONAL EFFICIENCY

- Centralized visibility and control to simplify management, accelerate problem resolution, optimize network utilization, and automate response to wireless threats
- Integrated wired and wireless management, and role-based access control greatly reduce administration time and effort
- Adaptive architecture reduces complexity and optimizes information flow for each application

Scalable to over 1000 Access Points per wireless controller with unified management of 802.11n and 802.11a/b/g Access Points

Seamless roaming with centralized and distributed data forwarding

Virtualized management and control planes for cloud deployments

High-availability architecture for real-time voice/video/data applications

Lifetime warranty (select controllers) to minimize the total cost of ownership

Product Overview

The award-winning Extreme Networks Wireless Controller family provides a scalable range of solutions that are ideal for managed WLAN deployments supporting demanding voice/video/data applications. Our Wireless Appliance are simple to deploy and manage, yet provide advanced functionality to allow organizations to define how wireless voice/video/data traffic is processed without architectural constraints and in accordance with the business needs. Select wireless controllers come with a lifetime warranty and phone support as well as free software maintenance releases for 1 year to protect your wireless networking investment and minimize the total cost of ownership.

The Extreme Networks Wireless Controller portfolio includes:

- The **C25** supporting up to 96 Access Points (APs)
- The **V2110** supporting up to 496 APs
- The **C4110** supporting up to 500 APs
- The **C5110** supporting up to 1050 APs

The V2110 is available as a VMware appliance for easy deployment in cloud environments. Scalable up to 496 APs, the V2110 extends all the cost savings, hardware independence, and resiliency benefits of data center virtualization to the wireless infrastructure.

Extreme Networks Wireless Appliance provide role-based management for users, devices, and applications with individualized services including Quality of Service (QoS), call admission control, secure access policies, network access control (NAC), captive portals, rate limiting, multicast, filtering, and traffic forwarding. These

SECURITY

- Authentication and authorization functions include role-based access control using 802.1X, MAC authentication, and captive portal
- Standards-based encryption (WEP, TKIP, WPA, WPA2, WPA-PSK, WPA2-PSK, and AES)
- External captive portal allows full customization for guest access
- Integrated wired and wireless intrusion prevention
- Denial of Service (DoS) protection for management, control, and data traffic

SUPPORT AND SERVICES

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training

services are enabled by the unique and flexible Extreme Networks Wireless Virtual Network Service (VNS) architecture and easily provisioned and managed by an intuitive web interface.

Each controller supports mixed mode deployments of 802.11n and 802.11a/b/g APs along with the ability to seamlessly roam between wireless controllers and access points, providing scalability and ease of deployment. For large deployments, Extreme Networks Wireless further simplifies the management of thousands of APs by creating mobility zones that extend the VNS properties across multiple wireless controllers. Mobility zones maintain the VNS definitions and the individual policies throughout the entire mobility zone, ensuring that policies follow the user regardless of physical location.

Extreme Networks Wireless provides an easy, low cost way to deploy 802.11n solutions, delivering cost-effective pricing, wired/wireless integration, and low TCO while openly supporting a broad range of mobile voice, video, and location-based applications to drive enterprise productivity and reduce the overall cost of mobility. With the ability to deliver both centralized and distributed traffic forwarding by application, Extreme Networks Wireless Appliance enable a flexible, cost-effective path to deploying 802.11n for the enterprise. Backed by industry-leading global support and services, Extreme Networks Wireless solutions enable customers to leverage existing investments and avoid forklift upgrades.

Virtual Network Service (VNS) - An Adaptive WLAN Architecture

Most WLAN solutions force network administrators to choose between a centralized or distributed architecture. A significant advantage of Extreme Networks Wireless Appliance is that they can support both deployment models simultaneously, offering significant flexibility benefits over other solutions. Network administrators can select how traffic will be handled on a per-SSID basis, without any restrictions, so that the wireless LAN infrastructure can adapt to business requirements and applications.

A centralized architecture requires all traffic to be backhauled to a centralized controller. With the higher data rates of 802.11n APs, traffic loads on the wired network can be much greater than those created by legacy 802.11a/b/g APs. Depending on the size of the WLAN deployment and how much data is forwarded to the centralized controller, significant congestion may result.

A fully distributed deployment eliminates backhauling traffic to a wireless controller but increases the processing complexity for real-time mobile applications that require seamless cross-subnet roaming (e.g. VoWLAN). This can force IT managers to either create a large broadcast domain or apply many VLANs.

Extreme Networks Wireless Virtual Network Services control traffic flow by allowing traffic to be backhauled to a wireless controller or switched locally at the AP on a per SSID basis. With local switching, the AP is still managed centrally by the wireless controller, but data is not backhauled to the wireless controller.

This improves responsiveness and ensures that traffic does not unnecessarily traverse costly WANs or contribute to bottlenecks at aggregating switches. A VNS also provides role-based policies providing security, NAC, mobility, and QoS priority that can be implemented on a per user and per application basis. The table below highlights this capability:

SSID	USER TYPE	SECURITY ROLE	TOPOLOGY (DATA PATH)
Single	Multiple	Multiple	Single
Single	Multiple	Single	Multiple
Single	Multiple	Multiple	Multiple
Multiple	Multiple	Multiple	Single
Multiple	Multiple	Single	Multiple
Multiple	Multiple	Multiple	Multiple

Integrated Management and Control Across Wireless and Wired Networks

WEB-BASED CENTRALIZED MANAGEMENT VIA WIRELESS ASSISTANT

The Wireless Assistant provides network administrators with a centralized web-based interface designed to easily manage both infrastructure and services. Hosted on the wireless controller, this interface allows network administrators to separately configure, enable, or disable each AP or group of APs. The wireless controller consolidates data received from across the network to provide meaningful statistics in easy-to-read reports. Additionally, a number of standards-based management tools are available to facilitate integration of the WLAN infrastructure with enterprise management applications. For large networks with multiple wireless controllers the optional Extreme Networks Wireless Management Suite (WMS) can be used to collect and manage data for a centralized view of the entire WLAN.

MULTI-CONTROLLER MANAGEMENT

Extreme Networks Wireless Management Suite provides centralized management for the Extreme Networks Wireless portfolio, consolidating management information from across the entire WLAN for a global network perspective. The solution is enhanced by the addition of the WMS Intrusion Prevention System (WIPS) option which provides sophisticated wireless intrusion prevention and location assessment capabilities. Wired and wireless network integration is further enhanced by the visibility of all the wireless elements through the Extreme Networks Management Suite (NMS). Integration between NMS and the Extreme Networks Wireless portfolio provides end-to-end visibility of wireless Access Points, Appliance, and wireless clients from the NMS Console. The integration delivers improved network management efficiency and wired/wireless infrastructure topology mapping and visibility for network administrators. Further integration with NMS Inventory Manager effectively centralizes distribution of software and tracking of configuration changes.

INTEGRATED SECURITY

Wireless Management Suite WIPS enhances security with embedded wireless intrusion prevention and location-based services. When deployed in conjunction with the Extreme Networks Intrusion Prevention System (IPS), full packet inspection, adaptive signature pattern matching, protocol analysis, and behavioral anomaly detection are delivered for both wired and wireless users. Further, Extreme Networks Network Access Control (NAC) identity-based policy privileges are unified across the wired and wireless infrastructure to deliver role-based access control – regardless of connectivity method.

The NAC policies ensure only the right users have access to the right information, from the right place, at the right time. Third party authentication systems can also be integrated with the use of the External Captive Portal interface.

High Performance & High Availability

Enterasys Wireless delivers the perfect combination of high-performance and high-availability demanded by today's wireless applications. By combining unique voice optimization features and the latest in industry standards, Enterasys Wireless provides enterprise grade reliability for all users.

HIGH SCALABILITY

The Extreme Networks Wireless portfolio supports from a single AP to 1,000+ APs per wireless controller, providing linear scalability from small to large wireless deployments. In addition, wireless controllers can be networked to scale beyond the limits of a single controller or availability pair to offer a multi-wireless controller mobility zone. Mobility zones enable seamless roaming across a large number of wireless controllers while still delivering real-time session-availability services without requiring the purchase of additional AP licenses for redundancy.

Extreme Networks Wireless provides true end-to-end Quality of Service (QoS) with each controller and AP supporting native IP prioritization (DiffServ, TOS, Precedence), Ethernet 802.1p, as well as 802.11e's WMM and TSPEC wireless QoS standards. Extreme Networks Wireless devices support distinct queues on all interfaces, whether wired or wireless.

When voice and data traffic are running on the same AP, voice traffic can be prioritized to ensure minimal delay and jitter for optimal voice quality. The wireless controllers are able to translate WMM prioritized traffic to existing QoS prioritization schemes on the wired network (TOS, DSCP, etc.).

FAST AND SECURE ROAMING FOR SEAMLESS VOICE AND DATA MOBILITY

Extreme Networks Wireless Appliance manage sessions centrally to ensure fast, secure, and seamless roaming as users and devices move throughout the radio coverage range of each AP.

Seamless roaming greatly improves productivity by providing true mobility across the enterprise, all transparent to the user.

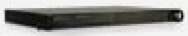
The Wireless Appliance use industry standards to deliver fast and secure roaming. 802.11i pre-authentication (Pre-Auth) ensures that the user is authenticated to adjacent APs before entering their coverage range, preserving voice calls as users move throughout the enterprise. Opportunistic Key Caching (OKC) is also a supported mechanism which greatly improves device roaming times.

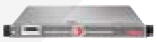
HIGH AVAILABILITY AND SELF-HEALING

Redundant Extreme Networks Wireless Appliance can be deployed across the network and operate in failover or load sharing mode. Access points can be configured for fast-failover mode to allow configuration and service restoration (in tunnel mode) in less than two seconds, thus enabling user sessions to continue uninterrupted. When switching traffic locally, APs continue to provide service even when the link to the wireless controller is severed and can be configured to resume service should a power outage force them to restart.

Extreme Networks Wireless APs also feature Dynamic Radio Management, which enables the network to automatically adapt to changes in the RF environment or failure of any individual APs, ensuring availability and performance to users. Each wireless AP continuously monitors channel use, signal to noise ratio (SNR) for interference, and the receive power of neighboring APs (Extreme Networks or third party) to adjust their channel and transmit power.

Extreme Networks Wireless Appliance





SUPPORTED FEATURES	V2110	C25	C4110	C5110
CAPACITY				
Total APs supported per controller	496	96	500	1050
Total APs supported in standard mode	248	48	250	525
Additional APs supported in high-availability mode	248	48	250	525
Simultaneous users per controller	4096	1024	4096	8192
MANAGEABILITY				
Pre-standard (CAPWAP)	✓	✓	✓	✓
Integrated VLAN-VNS	✓	✓	✓	✓
Auto-discovery of new APs	✓	✓	✓	✓
CDR/RADIUS accounting	✓	✓	✓	✓
Visibility through Extreme Networks NetSight	✓	✓	✓	✓
Extreme Networks Wireless Management Suite integration	✓	✓	✓	✓
Integration with Extreme Networks NAC	✓	✓	✓	✓
Integration with Extreme Networks IPS and SIEM	✓	✓	✓	✓
PERFORMANCE AND AVAILABILITY				
High availability with automatic failover to a backup controller (license included)	✓	✓	✓	✓
Client mobility with fast failover and session availability	✓	✓	✓	✓
Dynamic Radio Management (DRM), Flexible Client Access (airtime fairness), Load Balancing & Band-steering	✓	✓	✓	✓
Support for hybrid traffic forwarding: local switching at AP or controller-based switching (based upon user, application or segment)	✓	✓	✓	✓
Dual, hot swappable power supplies	-	-	✓	✓
SECURITY				
Robust standards-based security: 802.11i, WEP, WPA, WPA2, TKIP, AES	✓	✓	✓	✓
802.1x Authentication: EAP-TLS, EAP-SIM, EAP-TTLS, PEAP, EAP-MD5, EAP-FAST	✓	✓	✓	✓
RADIUS Authentication and Accounting	✓	✓	✓	✓
Encryption Algorithms: AES (CCMP), RC4-40, 104, 128-bit (TKIP, WEP)	✓	✓	✓	✓
Guest Services (captive portal, URL redirect, NAC) and Walled Garden (unauthorized access to URL)	✓	✓	✓	✓
Advanced filtering and integration with NetSight Policy Manager	✓	✓	✓	✓
VOICE				
Voice-over-WLAN Optimization: 802.11e/WMM, U-APSD, TSPEC, CAC, QBSS	✓	✓	✓	✓
Wired-Wireless (DSCP/TOS-to-WMM) QoS Mapping	✓	✓	✓	✓
Roaming between IP subnets	✓	✓	✓	✓
Roaming between multiple controllers	✓	✓	✓	✓
NETWORKING				
SNMPv2c/v3	✓	✓	✓	✓
Routing – OSPF v2	✓	✓	✓	✓
CSMA/CD	✓	✓	✓	✓
802.11-802.3 bridging	✓	✓	✓	✓
IEEE 802.1D-compliant bridging	✓	✓	✓	✓
IEEE 802.1Q VLAN tagging and trunking	✓	✓	✓	✓
Proxy ARP	✓	✓	✓	✓
Link Aggregation (Static LAGs)	NA	✓	✓	✓

Extreme Networks Wireless Appliance (cont.)

TECHNICAL SPECIFICATIONS	C25	C4110	C5110
DIMENSIONS			
Length	24.9 cm (9.8 in)	66.04 cm (26 in)	77.2 cm (30.4 in)
Width	43.6 cm (17.2 in)	42.63 cm (16.78 in)	42.6 cm (16.7 in)
Height	4.3 cm (1.7 in)	4.26 cm (1.67 in) – 1U	4.26 cm (1.67 in) – 1U
Weight	4.5 kg (10 lbs.)	13.45 kg (29.66 lbs.)	17.7 kg (35.8 lbs.)
ENVIRONMENTAL			
Operating Temperature	0° C to 40° C (32° F to 104° F)	10° C to 35° C (50° F to 95° F)	10° C to 35° C (50° F to 95° F)
Storage Temperature	-40° C to 70° C (-40° F to 158° F)	-40° C to 65° C (-40° F to 149° F)	-40° C to 65° C (-40° F to 149° F)
Humidity	8% to 90%, non-condensing	20% to 80%, non-condensing	5% to 95%, non-condensing
MOUNTING			
19” Rack Mountable	1U configuration to fit standard 19” rack (mounting kit included)	1U configuration to fit standard 19” rack (mounting kit included)	1U configuration to fit standard 19” rack (mounting kit included)
Front and Rear Mount	I/O cabling at back of unit; power cabling and power switch at the rear	I/O cabling and power cabling at back of unit; power switch at the front	I/O cabling and power cabling at back of unit; power switch at the front
PORTS			
Data Ports	2 x 10/100/1000 Base-T	4 x 10/100/1000 Base-T	• 2 x 10Gb Short Range Fiber Optic with LC Connectors • 1 x 10/100/1000 Base-T
Management Ports	• 1 x 10/100/1000 Base-T • 2 x USB Port • Console Port DB9	• 1 x 10/100/1000 Base-T • 1 x USB Port • Console Port DB9	• 1 x 10/100/1000 Base-T • 4 x USB Ports available. Use one. • Console Port DB9
ELECTRICAL			
Power Rating	• Voltage: 100-240 VAC • Frequency: 50-60 Hz • Power (max): 200W	• Voltage: 110/240 VAC • Frequency: 50-60 Hz • Power (max): 400 W	• Voltage: 110/220 VAC • Frequency: 48-62 Hz • Power (max): 670 W
STANDARDS COMPLIANCE			
Regulatory/Safety	• UL 60950-1 • CSA 22.1 60950	• UL 60950-1 • CSA 22.1 60950 • EN 60950-1 • IEC 60950-1	• UL 60950-1 • CSA 22.1 60950 • EN 60950-1 • IEC 60950-1
Emissions/Immunity	• FCC Part 15 (Class A) • ICES-003 (Class A) • AS/NZS CISPR 22 (Class A) • EN 55022 (Class A) • EN 55024 • EN 61000-3-2 • EN 61000-3-3	• FCC Part 15 (Class A) • ICES-003 (Class A) • AS/NZS CISPR 22 (Class A) • EN 55022 (Class A) • EN 55024 • EN 61000-3-2 • EN 61000-3-3	• FCC Part 15 (Class A) • ICES-003 (Class A) • BSMI • VCCI V-3 • AS/NZS CISPR 22 (Class A) • EN 55022 (Class A) • EN 55024 • EN 61000-3-2 • EN 61000-3-3

VIRTUAL WIRELESS SERVICES ENGINE (WISE) V2110	
DESCRIPTION	
Virtual Platform	VMWare ESX / ESXi4.1
Virtual Machine CPUs	4 cores or higher
Virtual Machine Memory	2G or higher
Virtual Machine Storage	25G or higher
Virtual Network Interfaces	Two data ports and one management

Ordering Information

PART NUMBER	DESCRIPTION
APPLIANCE	
WS-C25	C25 WLAN controller. Manages 16 Access Points, expandable to 48 in 16 AP increments with 16 AP capacity upgrade (WS-C20XCAPUP16). Requires Reg Domain Key.
WS-C4110	C4110 WLAN controller. Manages 50 Access Points, expandable to 250 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). Requires Reg Domain Key.
WS-C4110-CN	C4110 WLAN controller. Manages 50 Access Points, expandable to 250 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). China Only.
WS-C5110-2-SR	C5110 WLAN controller. Manages 150 Access Points, expandable to 525 in 25 AP increments with 25 AP capacity upgrade (WS-CTLCAPUP25). Requires Reg Domain Key.
VIRTUAL WIRELESS SERVICES ENGINE	
WS-V2110-8-IL	V2110 Virtual Wireless Services Engine for Israel. Base of 8 APs, expandable to 248 APs in 16 AP increments (WS-C20XCAPUP16).
WS-V2110-8-JP	V2110 Virtual Wireless Services Engine for Japan. Base of 8 APs, expandable to 248 APs in 16 AP increments (WS-C20XCAPUP16).
WS-V2110-8-NAM	V2110 Virtual Wireless Services Engine for NAM (FCC) Regulatory Domain. Base of 8 APs, expandable to 248 APs in 16 AP increments (WS-C20XCAPUP16).
WS-V2110-8-ROW	V2110 Virtual Wireless Services Engine for Rest-of-World (verify country availability before ordering). Base of 8 APs, expandable to 248 APs in 16 AP increments (WS-C20XCAPUP16).
CAPACITY UPGRADES	
WS-C20XCAPUP16	WLAN controller capacity upgrade for C20, C20N, C25, and V2110. Increases capacity of WLAN controller by 16 access points.
WS-CTLCAPUP25	WLAN controller capacity upgrade for C4110 and C5110. Increases capacity of WLAN controller by 25 access points.
ACTIVATION KEYS	
WS-CTLREG8P-IL	V8 Regulatory Domain Key for Israel. Enables WLAN controller and access points with appropriate radio settings for Israel.
WS-CTLREG8P-JP	V8 Regulatory Domain Key for Japan. Enables WLAN controller and access points with appropriate radio settings for Japan.
WS-CTLREG8P-NAM	V8 Regulatory Domain Key for FCC Domain. Enables WLAN controller and access points with appropriate radio settings for this region.
WS-CTLREG8P-ROW	V8 Regulatory Domain Key for Rest-of-World (verify country availability before ordering). Enables WLAN controller and access points with appropriate radio settings for this region.

Warranty

As a customer-centric company, Extreme Networks 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.

Select Extreme Networks Wireless Appliance come with a lifetime warranty. For full warranty terms and conditions please go to: www.ExtremeNetwork.com/support/warranty.aspx.

Service & Support

Extreme 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 Extreme Networks account executive for more information about Extreme Networks Service and Support.

Extreme® networks

http://www.ExtremeNetworks.com/contact / Phone +1-408-579-2800