Summit®48si
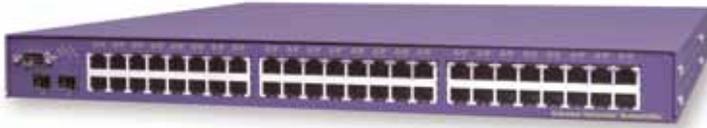
The extensive capabilities of the Summit48si fit a large span of application spaces, both within an enterprise and a metro network.

Quality of Service and Application Flexibility

- Bidirectional rate shaping
- DiffServ and 802.1p
- Virtual MANs (vMANs)
- Policy-Based Quality of Service (QoS) with 8 queues per port

High Network Availability

- Redundant hot-swappable power supplies and fiber gigabit uplinks
- Ethernet Automatic Protection Switching (EAPS, RFC 3619)
- Layer 2 and Layer 3 Extreme Standby Routing Protocol™ (ESRP) for dual-homed configuration

Comprehensive Security for Control at the Edge of the Network

- Wire-speed Layers 2 – 4 ACLs, web-based Network Login, 802.1x, SSH2, TACACS, RADIUS, DoS protection, MAC address security
- Routing features for maximum forwarding control at the edge
- Automatic Access Control List (ACL) and QoS classification with EPICenter® Policy Manager

Summit48si from Extreme Networks® sets the standard for Layer 3 switching at the edge by maximizing 10/100 port density and architecting high levels of reliability while maintaining leadership in Layer 3 software features and performance. The unsurpassed software features, capacity and performance of Summit48si enable customers to provide more Layer 3 services to more users while using less space and at a lower Total Cost of Ownership than ever before.

At one rack unit (1RU) in height, Summit48si packs 48 10/100 Ethernet ports and 2 Gigabit Ethernet ports with nonblocking capacity to support every port at full line-rate. This compact yet powerful package is capable of supporting two hot swappable load sharing power supplies—a reliability first in a 1RU Layer 3 switch. The reliability of Summit48si is enhanced even further with dual Gigabit Ethernet uplinks, both of which are active and can be aggregated for enhanced throughput and increased redundancy.

Extreme Networks' advanced Layer 3 software feature set, combined with dual hot-swappable power supplies makes Summit48si an unbeatable solution at the edge of the network.

Target Applications

- In enterprise markets—such as banking, manufacturing, education—where high-performance, reliability and security features are critical
- Metro Ethernet access rings where granular bandwidth allocation, billing, and security are critical
- Metro service providers that need high speed IP unicast and multicast services supporting carrier-class routing protocols like OSPF, BGP, and PIM-SM

The unsurpassed software features, capacity, and performance of the Summit48si enable customers to provide more Layer 3 services to more users while using less space and at a lower Total Cost of Ownership than ever before.

Summit48si Customer Benefits

Quality of Service and Application Flexibility

Maximum Performance

With industry-leading performance for the most demanding applications, Summit48si has a non-blocking architecture with 17.5 gigabits of throughput with wire-speed performance on every port.

Bidirectional rate shaping allows you to manage bandwidth on Layer 2 and Layer 3 traffic flowing both to and from the switch.

DiffServ and 802.1p deliver varied levels of service for time-sensitive, demanding applications for voice, video and data and ensure efficient bandwidth usage.

Eight hardware queues provide granularity for multiple applications, and guarantee low latency/low jitter for time sensitive applications (voice and multimedia) with support for advanced scheduling algorithms.

Application Flexibility

Summit48si features a 128K routing table size for maximum forwarding control at the edge with the same advanced feature set supported end-to-end throughout the customer's network. Protocol-based VLANs enable the network administrators to define a packet filter that the switch uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.

Virtual MANs (vMANs) feature is useful in building transparent private networks that need point-to-point or point-to-multipoint connectivity across an Ethernet infrastructure.

Policy-Based QoS with 8 queues per port, bidirectional rate shaping and bandwidth management provides the ability to prioritize mission-critical applications and traffic to deliver maximum productivity and deliver delay-sensitive applications such as voice and video.

High Network Availability

Redundant hot-swappable power supplies, and fiber gigabit uplinks provide true high availability as Summit48si immediately is able to failover to the redundant port and the

user's application is unaffected. The user stays connected to the network and remains productive.

Summit48si delivers connectivity and productivity with advanced high availability features, such as EAPS (RFC 3619) with multidomain support to deliver subsecond (less than 50ms recovery) protection switching to interconnected switches in an Ethernet ring topology. EAPS is similar to Spanning Tree Protocol (STP), but offers the advantage of converging in significantly less time than STP or even Rapid Spanning Tree (802.1w) when a link breaks in the ring.

ESRP can be implemented at both Layers 2 and 3 and extends the Virtual Redundant Redundancy Protocol's (VRRP) capabilities, adding Layer 2 resiliency and loop prevention and Layer 3 default router redundancy.

Equal Cost Multipath (ECMP) allows the networks to be even more resilient as multiple equal-cost routes can be used concurrently to an end destination.

With the software redundant port feature, a specified primary port can be backed up by another port. Should the link go down on the primary port, the redundant port will establish link and become active. Thus multihomed redundancy can be easily designed without the complexity of a protocol.

Comprehensive Security for Control at the Edge of the Network

With IEEE 802.1x Login, network managers can always control who is connected to the network and prevent unauthorized clients from gaining access to the network.

Web-based Network Login does not require any specific client software and can work with any HTTP-compliant web browser and thus is independent of platform. Every user on every port can be authenticated so the network is protected at the most sensitive point of attack.

MAC address security allows identifying port abuse such as rogue wireless access points or hubs/switches on edge ports. It includes two features: lockdown on a per port basis and limiting the number of MAC addresses learned by a port. Lockdown

and saving learned MAC addresses between reboots can be used to protect dedicated ports for VoIP phones or printers from abuse. Limiting the number of MAC addresses learned on a port also allows enforcement of service level agreements in tenant or service provider environments.

SSHv2 allows network managers to securely configure the box remotelywithout any risk of packet snooping or man-in-the-middle attack. SSHv2, DoS protection, TACACS+ and RADIUS bring reliable secure configuration traffic (encryption) and authentication.

Scanning of malicious users or virusinfected end-clients can cause the Forwarding Database (FDB) table to fill up very quickly and FDB replacements to happen at higher rate. The attacks can hurt the quality of internal traffic significantly, if all Layer 3 forwarding is made by host lookup. The IPDA SUBNET lookup feature forces the attack traffic to use the IPFDB SUBNET forwarding table instead of the host-forwarding table. This feature is intended to decrease frequency of FDB collision and replacement and accelerate packet forwarding for Summit48si.

Multiple Supplicant (client) enables multiple clients to be individually authenticated on the same port.

Summit48si has wire-speed Layers 2 – 4 ACLs on every port for maximum security while maintaining maximum throughput.

Ease of Management

Extreme Networks has developed tools that save you time and resources in managing your network. EPICenter® provides all fault configuration, accounting, performance, and security functions to manage Extreme Networks' multi-layer switching equipment in a converged network. EPICenter Policy Manager provides layer-independent policy enforcement for Layers 1 – 4. Extreme Networks' software application, ServiceWatch®, delivers powerful, Layers 4 – 7 monitoring and management for mission-critical network services.

Technical Specifications

ExtremeWare 7.7 Supported Protocols

General Routing and Switching
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2338 VRRP
- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- IEEE 802.1D – 1998 Spanning Tree Protocol (STP)
- IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP
- IEEE 802.1s – 2004 Multiple Instances of STP, MSTP
- Extreme Multiple Instances of Spanning Tree Protocol (EMISTP)
- PVST+, Per VLAN STP (802.1Q interoperable)
- Extreme Standby Router Protocol (ESRP)
- IEEE 802.1Q – 2003 Virtual Bridged Local Area Networks
- Extreme Discovery Protocol (EDP)
- Static Unicast Routes
- Extreme Loop Recovery Protocol (ELRP)
- Software Redundant Ports
- IPX RIP/SAP Router specification

VLANs
- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Static configuration and dynamic (LACP) for server attached
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- MAC-based VLANs
- Protocol-based VLANs
- Multiple STP domains per VLAN
- RFC-3069 VLAN Aggregation for Efficient IP Address Allocation
- Virtual MANs (vMANs)
- VLAN Translation

Quality of Service and Policies
- IEEE 802.1D – 1998 (802.1p) Packet Priority
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2475 DiffServ Core and Edge Router Functions
- RED as described in "Random Early Detection Gateways for Congestion Avoidance, Sally Floyd and Van Jacobson"
- RED as recommended in RFC 2309
- Bidirectional Rate Shaping
- Ingress Rate Limiting
- Layer 1-4, Layer 7 (user name) Policy-Based Mapping
- Policy-Based Mapping/Overwriting of DiffServ code points, .1p priority
- Network Login/802.1x and DLCS (Dynamic Link Context System, WINS snooping) based integration with EPICenter Policy Manager for dynamic user/device based policies

RIP
- RFC 1058 RIP v1
- RFC 2453 RIP v2

OSPF
- RFC 2328 OSPF v2 (including MD5 authentication)
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option
Note: OSPF Edge License includes 2 active interfaces, router priority 0

IS-IS
- RFC 1142 (ISO 10589), IS-IS protocol
- RFC 1195, Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 2104, HMAC: Keyed-Hashing for Message Authentication, IS-IS HMAC-MD5 Authentication
- RFC 2763 (Dynamic Host Name Exchange for IS-IS)

BGP4
- RFC 1771 Border Gateway Protocol 4
- RFC 1965 Autonomous System Confederations for BGP
- RFC 2796 BGP Route Reflection (supersedes RFC 1966)
- RFC 1997 BGP Communities Attribute
- RFC 1745 BGP4/IDRP for IP-OSPF Interaction
- RFC 2385 TCP MD5 Authentication for BGPv4
- RFC 2439 BGP Route Flap Damping

IP Multicast
- RFC 2362 PIM-SM
- PIM-DM Draft IETF PIM Dense Mode v2-dm-03
- PIM Snooping
- DVMRP v3 draft IETF DVMRP v3-07
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2
- IGMP Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- Static IGMP Membership
- Static Multicast Routes
- Mtrace, draft-ietf-idmr-traceroute-ipm-07
- Mrinfo

Management and Traffic Analysis
- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 1866 HTML – web-based device management and Network Login
- RFC 2068 HTTP server
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (revision 2)
- RFC 951, 1542 BootP
- RFC 2131 BOOTP/DHCP relay agent and DHCP server
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
- RFC 1573 Evolution of Interface
- RFC 1901 – 1908 SNMP Version 2c, SMIv2 and Revised MIB-II
- RFC 2570 – 2575 SNMPv3, user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2665 Ethernet-Like-MIB
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2613 SMON MIB
- RFC 2668 802.3 MAU MIB

- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2737 Entity MIB, Version 2
- RFC 2674 802.1p/802.1Q MIBs
- RFC 1354 IPv4 Forwarding Table MIB
- RFC 2233 Interface MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 1657 BGPv4 MIB
- RFC 2787 VRRP MIB
- RFC 2925 Ping/Traceroute/NSLOOKUP MIB
- RFC 2932 – IPv4 Multicast Routing MIB
- RFC 2933 – Internet Group Management Protocol MIB
- RFC 2934 – Protocol Independent Multicast MIB for IPv4
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- draft-ietf-bridge-8021x-01.txt (IEEE8021-PAE-MIB)
- IEEE 802.1x – 2001 MIB
- Extreme extensions to 802.1x-MIB
- Secure Shell (SSHv2) clients and servers
- Secure Copy (SCPv2) client and server
- Secure FTP (SFTP) server
- sFlow version 5
- NetFlow version 1 export
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- Local Messages (criticals stored across reboots)
- IEEE 802.1ab LLDP

ExtremeWare vendor MIBs: Includes ACL, MAC FDB, IP FDB, MAC Address Security, Software Redundant Port, NetFlow, DoS-Protect MIB, QoS policy, Cable Diagnostics, VLAN config, vMAN, VLAN Translation and VLAN Aggregation MIBs

Security
- Routing protocol MD5 authentication (see above)
- Secure Shell (SSHv2),Secure Copy (SCPv2) and SFTP with encryption/authentication
- SNMPv3 user based security, with encryption/authentication (see above)
- RFC 1492 TACACS+
- RFC 2865 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- RFC 3579 RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 3580 802.1X RADIUS
- RADIUS Per-command Authentication
- MAC based Network Login using RADIUS
- Access Profiles on All Routing Protocols
- Access Profiles on All Management Methods
- Network Login (web-based DHCP/HTTP/RADIUS mechanism)
- RFC 2246 TLS 1.0 + SSL v2/v3 encryption for web-based Network Login
- IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login
- Multiple supplicants for Network Login (web-based and 802.1x modes)
- Guest VLAN for 802.1x
- MAC Address Security – Lockdown, limit and aging
- IP Address Security with DHCP Option 82, DHCP
- Enforce/Duplicate IP Protection via ARP Learning Disable
- Network Address Translation (NAT)
- Layer 2/3/4/7 ACLs
- Source IP Lockdown – Dynamic filtering against invalidly sourced traffic

Technical Specifications

Denial of Service Protection

- RFC 2267 Network Ingress Filtering RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting ACLs
- Rate Shaping by ACLs
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- Server Load Balancing with Layer 3, 4 Protection of Servers
- SYN attack protection
- FDB table resource protection via IPDA Subnet Lookup
- CPU DOS protection with ACL integration: Identifies packet floods to CPU and sets an ACL automatically, configurable traffic rate limiting to management CPU/Enhanced DoS Protect
- Unidirectional Session Control

Robust Against Common Network Attacks

- CERT (http://www.cert.org)
  - CA-2003-04: "SQL Slammer"
  - CA-2002-36: "SSHredder"
  - CA-2002-03: SNMP vulnerabilities
  - CA-98-13: tcp-denial-of-service
  - CA-98.01: smurf
  - CA-97.28: Teardrop_Land -Teardrop and "LAND" attack
  - CA-96.26: ping
  - CA-96.21: tcp_syn_flooding
  - CA-96.01: UDP_service_denial
  - CA-95.01: IP_Spoofing_Attacks_and_Hijacked _Terminal_Connections
  - IP Options Attack

Host Attacks

- Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, smurf, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream, Land, Octopus

Ordering Information

Part Number	Name	Description
15601	Summit48si AC	Summit48si AC with 48 10/100BASE-TX Ethernet ports, two unpopulated mini-GBIC 1000BASE-X ports. Basic Layer 3 switching, single hot-swappable AC power supply. Power cord ordered separately.
15602	Summit48si DC	Summit48si DC with 48 10/100BASE-TX Ethernet ports, two unpopulated mini-GBIC 1000BASE-X ports. Basic Layer 3 switching, single hot-swappable DC power supply. Power cord ordered separately.
15603	Summit48si PSU, AC	Summit48si Power Supply Unit, Hot-Swappable, AC, Spares
15604	Summit48si PSU, DC	Summit48si Power Supply Unit, Hot-Swappable, DC, Spares
15605	Voucher, Summit48si, Full Layer 3	Full Layer 3 License upgrade, Summit48si

Accessories

10051	SX SFP	1000BASE-SX SFP, LC connector (multimode fiber)
10052	LX SFP	1000BASE-LX SFP, LC connector (single/multimode fiber)
10053	ZX SFP	1000BASE-ZX SFP, LC connector (single mode fiber)

www.extremenetworks.com

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +852 2517 1123

Japan
Phone +81 3 5842 4011