SUMMIT48si

Extreme Networks® Summit®48si sets the new standard for Layer 3 switching at the edge by maximizing 10/100 port density and architecting unparalleled levels of reliability while maintaining leadership in Layer 3 software features and performance. 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 (TCO) than ever before.

At one rack unit (1.75") in height, the Summit48si packs 48 10/100 Ethernet ports and 2 Gigabit Ethernet ports with non-blocking 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 one rack unit Layer 3 switch. And the Summit48si reliability 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, ExtremeWare®, combined with the new one rack unit and dual hot swappable power supply form factor makes the Summit48si an unbeatable solution at the edge of the network. Featuring the same "i" series chipset that powers Extreme Networks' award-winning Alpine® and BlackDiamond® modular switches, the Summit48si supports the most comprehensive set of Layer 3 switched services in the industry including OSPF, RIP, BGP4, prioritization and bandwidth management Quality of Service (QoS), Access Control Lists (ACLs), Denial of Service (DoS) protection, Ethernet Automatic Protection Switching (EAPS) and many more features.

This unique combination of high performance, reliability and extensive Layer 3 switched services enables the Summit48si to support redeployment of Layer 3 edge services right to the edge of the network–saving the customer money and improving overall network functionality and performance.

CUSTOMER BENEFITS AT A GLANCE

- **Maximum Performance**
- **Application Flexibility**
- **Leadership in Network Availability**
- **Highest Security for Control and Data**
- **Maximum Scalability**
- **True End-to-End Manageability**

extreme networks

MAXIMUN PERFORMANCE

- **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.
- **Bi-directional 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.
- **8 hardware queues** provide granularity for multiple applications, and guarantee low latency/low jitter for time sensitive applications (Voice & Multimedia) **with support for advanced scheduling algorithms.**

APPLICATION FLEXIBILITY

- **128K routing table** size for maximum forwarding control at the edge with 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. Protocol based VLANs are most useful where network segments contain hosts running multiple protocols, and thus are ideal for small cores to aggregation.
- **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 Quality of Service (QoS)** with eight queues per port, bi-directional rate shaping and bandwidth management provides ability to prioritize mission-critical applications and traffic to deliver maximum productivity; deliver delay-sensitive applications such as voice and video.

LEADERSHIP IN NETWORK AVAILABILITY

- **Redundant hot-swappable power supplies, and fiber gigabit uplinks** enable 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.
- Enterprise customers can now rely on an unmatched failover time traditionally reserved for carriers (50ms) in their LAN network. The Summit48si delivers connectivity and productivity with advanced high availability features, such as **Ethernet Automatic Protection Switching (EAPS, RFC *3619)*** with multidomain support to deliver sub-second (less than 50 msec recovery) protection switching to interconnected switches in an Ethernet ring topology. EAPS is similar to the 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.
- **Extreme Standby Routing Protocol™ (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. It can be used as a STP substitute and can be scaled to protect thousands of VLANs. In fact, multiple instances of ESRP in the same VLAN allow direct host attachment to standby switches.
- **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 **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.

HIGHEST SECURITY FOR CONTROL AND DATA

- 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:** 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 reboot 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 remotely without any risk of packet snooping or man in the middle attack. **SSHv2, denial of service (DoS) protection, TACACS+ and RADIUS** bring reliable secure configuration traffic (encryption) and authentication.
- Scanning of malicious users or virus-infected 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. Thus it is possible for two client stations to be connected to the same port, with one being authenticated and the other not.
- **Wire speed Layer 2-Layer 4 Access Control Lists (ACLs)** on every port for maximum security while maintaining maximum throughput.

MAXIMUM SCALABILITY

- Higher port density in 1 RU footprint allows for maximum use of rack space.
- Maximum 10/100 connectivity per inch
- Dual Gigabit Ethernet uplinks

TRUE END-TO-END MANAGEABILITY

- True end-to-end management resulting in lower operational costs, less training, while maximizing network uptime.
- **sFlow** offers advanced detection and response to unusual network traffic.
- Automatic ACL and QoS classification with **EPICenter Policy Manager.**

HARDWARE FEATURES

- 48 10/100 auto-negotiating Ethernet ports in a 1 RU footprint allow more network connections per inch of rack space
- 2 mini-GBIC Gigabit Ethernet ports provide duplicate active uplinks for greater throughput and redundant paths
- Redundant hot-swappable power supplies to maximize uptime and network availability

EXTREMEWARE SOFTWARE FEATURES

- Security features, including Network Login, 802.1x, SSH2, ACLs, RADIUS, TACACS+, VLANs, thorough DoS protection, Network Address Translation (NAT), multiple supplicants, MAC Address security (lockdowns and limiting) provide a secure armor
- SmartRedundancy™, Ethernet Automatic Protection Switching (EAPS), Extreme Standby Router Protocol (ESRP), Virtual Redundant Routing Protocol (VRRP), Spanning Tree (STP), Rapid Spanning Tree (RSTP) and Extreme Networks STP extensions for enhanced network availability
- OSPF for large scalable meshed fault-tolerant networks
- Full-featured BGP4 for Internet peering

PERFORMANCE FEATURES

- Extreme Networks' award-winning "i" series chipset based performance
- Full line rate bandwidth on every port
- 17.5 Gbps non-blocking switch fabric
- 4,096 VLANs and 128,000 MAC or Layer 3 addresses
- Policy-Based QoS, with 8 hardware queues per port, and bidirectional rate shaping delivering bandwidth-by-the-slice
- 802.1p priority marking, DiffServ
- Protocol based VLANs
- Layer 2-4 ACLs for optimal security and diverse traffic classification
- Jumbo frame support for special high-throughput applications

MANAGEMENT FEATURES

- Extensive management through HTTP, SNMP, RMON and command line interface
- sFlow for advanced detection and response
- Serial management port on the front panel for ease of installation

PROTOCOLS AND STANDARDS

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 802.1Q - 1998 Virtual Bridged Local Area Networks
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol
- PVST+, Per VLAN STP (802.1Q interoperable)
- Extreme Standby Router Protocol (ESRP)
- Static Unicast Routes
- 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
- Bi-directional Rate Shaping
- 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

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 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2)
- 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 2737 Entity MIB v2
- RFC 2233 Interface MIB
- RFC 1354 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
- 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
- 999 Local Messages (criticals stored across reboots)
- 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. http://www.extremenetworks.com/services/documentation

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 2138 RADIUS Authentication
- RFC 2139 RADIUS Accounting
- RADIUS Per-command Authentication
- 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)
- MAC Address Security - Lockdown and Limit
- 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 Access Control Lists (ACLs)

Denial of Service Protection

- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs

- Wire-speed ACLs
- Rate Limiting / 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 ratelimiting to management CPU / Enhanced DoS Protect
- Uni-directional 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

PHYSICAL AND ENVIRONMENTAL

Dimensions:

(H) 1.75 in x (W) 17.25 in x (D) 18.25 in
(H) 4.45 cm x (W) 43.87 cm x (D) 46.41 cm

- Weight: 14 lbs (6.35 Kg) (1 PSU)
- PSU Weight: 2 lbs (0.9 Kg)
- Operating Temperature: -40° C to 40° C (-40° F to 104° F)
- Storage Temperature: -40° C to 70° C (-40° F to 158° F)
- Humidity: 10% to 95% non-condensing
- AC Power: 100-240 VAC, 50-60 Hz, 1.5-3.0 A max.
- DC Power: -36 to -75 VDC, 5% max p-p ripple, 4.2 Amps maximum at -48 VDC
- Heat Dissipation: 631 BTU/hr (185 watts)

REGULATORY

Safety

- UL 1950 3rd Edition, Listed
- EN60950:1992/A1-4:1997 plus ZB/ZC Deviations
- IEC 950CB
- Low Voltage Directive (LVD)
- CSA 22.2#950-95
- AS/NZS 3260
- EN60825-1
- FCC CFR 21

EMI/EMC

- FCC Part 15 Class A
- ICES-0003 A/C108.8-M1983 Class A
- VCCI Class A
- AS/NZS 3548
- EN55022 Class A
- CISPR 22 Class A
- EN50082 -1:1997 include ENV 50204
- EN55024:1998 includes IEC 61000-4-2, 3, 4, 5, 6, 8, 11
- EN 61000-3-2, 3
- CNS 13438 Class A

Environmental

- EN60068 to Extreme IEC68 schedule

ORDERING INFORMATION

Part Number	Part Name	Description
15601	Summit48si AC	Summit48si AC with 48 10/100BASE-TX Ethernet ports, two unpopulated mini-GBIC 1000BaseX ports. Basic Layer 3 switching, single hot swappable AC power supply. Includes power cord for US and Japan.
15602	Summit48si DC	Summit48si DC with 48 10/100BASE-TX Ethernet ports, two unpopulated mini-GBIC 1000BaseX ports. Basic Layer 3 switching, single hot swappable DC power supply. Includes power cord for US and Japan.
15603	S48si PSU, AC	Summit48si Power Supply Unit, Hot Swappable, AC, Spares
15604	S48si PSU, DC	Summit48si Power Supply Unit, Hot Swappable, DC, Spares
15605	Voucher, S48si, Full L3	Full L3 License upgrade, Summit48si

ACCESSORIES

Part Number	Part Name	Description
10051	SX mini-GBIC	Mini-GBIC, SFP, 1000BaseSX
10052	LX mini-GBIC	Mini-GBIC, SFP, 1000BaseLX

3585 Monroe Street Santa Clara, CA 95051-1450 Phone +1 408 579 2800 Fax +1 408 579 3000
Email info@extremenetworks.com Web www.extremenetworks.com