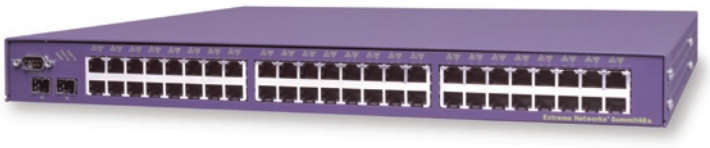
Summit®48si



The Summit48si—an unbeatable solution at the edge of the network

Features

- Non-blocking performance with Quality of Service (QoS) and application flexibility
- High network availability
- High security and ease of management for control at the edge of the network

Target Applications

- Enterprise markets—such as banking, manufacturing, and education—where high-performance, reliability, security features are critical
- Metro Ethernet access rings for high-speed IP unicast and multicast services supporting carrier-class routing protocols like OSPF, BGP, and PIM-SM
- Metro Service Providers—such as ILECs—where granular bandwidth allocation, billing, and security are critical

Extreme Networks® Summit48si 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.

At one rack unit (1RU)—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 1RU Layer 3 switch. 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 1RU and dual hot-swappable power supply form factor makes the Summit48si an unbeatable solution at the edge of the network.

Non-Blocking Performance with QoS and Application Flexibility

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. The Summit48si has eight

hardware queues that provide granularity for multiple applications, and guarantee low latency/low jitter for time sensitive applications (voice and multimedia) with support for advanced scheduling algorithms. Policy-Based QoS with eight queues per port, bidirectional 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.

The virtual MANs (vMANs) feature supported on the Summit48si is useful in building transparent private networks that need point-to-point or point-to-multipoint connectivity across an Ethernet infrastructure.

High Network Availability

Redundant hot-swappable power supplies and fiber gigabit uplinks enable true high availability as Summit48si is able to failover immediately 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 multi-domain support to deliver sub-second (less than 50ms 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. The Summit48si supports software redundant port, a feature that enables a specified primary port to be backed up by another port. Should the link go down on the primary port, the redundant port will establish a link and become active. Thus, multi-homed redundancy can be easily designed without the complexity of a protocol.

High Security and Ease of Management

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 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 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.

Wire-speed Layer 2-Layer 4 Access Control Lists (ACLs) are on every port for maximum security while maintaining maximum throughput, providing 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 is supported with EPICenter® Policy Manager.

www.extremenetworks.com **email: info@extremenetworks.com**

Corporate Headquarters 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