Switch MAC Address Table Exhaustion Countermeasures and Port Security Profiles - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

The Switch MAC Address Table Exhaustion Countermeasures and Port Security Profiles feature set represents a comprehensive Layer 2 security framework designed to protect enterprise and carrier-grade switching platforms against MAC flooding attacks, table overflow conditions, and unauthorized network access. This document provides detailed technical specifications for the hardware-assisted countermeasures and configurable port security profiles integrated into our switching silicon architecture.

The exponential growth of endpoint devices in modern campus and datacenter environments has introduced critical vulnerabilities at the access layer. Malicious actors and misconfigured endpoints can overwhelm Content Addressable Memory (CAM) tables by flooding the switch with thousands of spoofed source MAC addresses. When the MAC address table reaches capacity, the switching fabric fails open, causing unknown unicast frames to be flooded across all ports in the VLAN, resulting in severe performance degradation and potential data interception.

Our hardware platform addresses these threats through a multi-layered

defense architecture. The system implements dynamic MAC address table threshold monitoring, per-port MAC address limits, sticky MAC configurations, and violation actions that include port shutdown, restrict mode, and protect mode. All countermeasures operate at line rate, ensuring that security enforcement introduces zero forwarding performance penalties.

The port security subsystem supports three operational profiles: Static, Dynamic, and Sticky. Static profiles require manual MAC address provisioning for maximum control. Dynamic profiles learn addresses automatically with configurable aging timers. Sticky profiles combine the flexibility of dynamic learning with the persistence of static entries, ensuring that learned addresses survive link flaps and device reboots.

This datasheet covers the complete hardware specification, silicon-level architecture, configuration parameters, compliance certifications, and ordering information for our switching platforms equipped with MAC Address Table Exhaustion Countermeasures and Port Security Profiles.



HARDWARE ARCHITECTURE & SILICON

The switching ASIC implements a dedicated Layer 2 security engine that operates independently from the main forwarding pipeline. This separation ensures that MAC table security enforcement occurs in parallel with normal packet processing, maintaining wire-speed throughput even during active attack conditions.

The CAM table architecture supports 128K entries in standard configuration, expandable to 256K entries with optional memory modules. Each entry contains the MAC address, VLAN identifier, port index, entry type flags, and hardware timestamp for aging operations. The table supports hash-based lookup with a load factor threshold of 80 percent, triggering automatic hash table resizing to maintain lookup performance.

Key silicon-level countermeasures include:

MAC Address Learning Rate Limiting: The ASIC enforces a configurable threshold on the number of new MAC addresses learned per second per port. When exceeded, the system generates a violation event and applies the configured violation action. Default threshold is 1000 addresses per second with a burst allowance of 2000.

Table Threshold Monitoring: The hardware continuously monitors overall CAM utilization. When utilization exceeds configurable thresholds (default 70 percent and 90 percent), the system generates SNMP traps and syslog messages, enabling proactive network management before table exhaustion occurs.

Automatic Aging Acceleration: When the CAM table exceeds 90 percent capacity, the hardware automatically reduces the aging timer from the default 300 seconds to 60 seconds, accelerating the removal of stale entries and creating headroom for legitimate traffic.

Per-Port Entry Limits: Each physical port can be configured with a maximum MAC address count ranging from 1 to 1024 entries. When a port reaches its

configured limit, additional addresses are not learned, and the configured violation action is triggered.

The security engine supports hardware-based sticky MAC persistence through dedicated non-volatile memory. Sticky entries are automatically saved to flash storage and restored upon device reboot, eliminating the need for external authentication servers in environments requiring persistent port security.

All security events are logged to an on-chip event buffer with 16K entry capacity. The buffer supports configurable overflow actions including wraparound, halt, and remote syslog forwarding. Hardware timestamps with 100-nanosecond resolution ensure precise event correlation for forensic analysis.

KEY FEATURES & ROUTING LOGIC

PORT SECURITY PROFILES

- Static Profile: Requires manual provisioning of permitted MAC addresses. Provides maximum security for critical infrastructure ports. Supports up to 1024 static entries per port with VLAN-aware matching.
- Dynamic Profile: Automatically learns MAC addresses up to the configured

maximum. Implements configurable aging timers from 10 to 1000000 seconds. Violation actions include Protect, Restrict, and Shutdown.

- Sticky Profile: Combines dynamic learning with persistent storage. Learned addresses are written to non-volatile memory and survive reboot cycles. Supports manual clear commands for address removal.

VIOLATION ACTIONS

- Protect Mode: Drops frames with unauthorized source MAC addresses silently. No SNMP trap or syslog message is generated. Suitable for high-density access ports where logging noise is a concern.

- Restrict Mode: Drops frames with unauthorized source MAC addresses and generates SNMP traps and syslog messages. Includes violation counters for performance monitoring.

- Shutdown Mode: Administratively disables the port upon violation. Supports automatic recovery via errdisable timeout or manual intervention. Generates critical-level syslog alerts.

HARDWARE-ASSISTED COUNTERMEASURES

- MAC Flooding Detection: Silicon-level counters track MAC learning rate per port. When the configured threshold is exceeded, the system automatically

applies rate limiting to new address learning while preserving existing entries.

- CAM Table Watermarks: Configurable high and low watermarks trigger proactive aging and alerting. High watermark default is 90 percent, low watermark is 70 percent.

- Hash Collision Management: Hardware implements perfect hash algorithms with collision chain depth of 8 entries. Automatic rehashing occurs when collision chains exceed 6 entries.

- VLAN-Aware Enforcement: Port security profiles operate independently per VLAN, preventing cross-VLAN MAC address spoofing and ensuring tenant isolation in multi-tenant environments.

COMPLIANCE & STANDARDS

The Switch MAC Address Table Exhaustion Countermeasures and Port Security Profiles feature set complies with the following industry standards and regulatory requirements:

IEEE 802.1X-2020: Port-Based Network Access Control

IEEE 802.1AE-2018: MAC Security (MACsec)

IEEE 802.1Q-2018: Virtual Bridged Local Area Networks

IEEE 802.1D-2004: Media Access Control (MAC) Bridges

IETF RFC 2863: The Interfaces Group MIB

IETF RFC 3635: Definitions of Managed Objects for Ethernet-like Interface Types

IETF RFC 4188: Definitions of Managed Objects for Bridges

IETF RFC 4663: Transfer of MIB Module for IEEE 802.1X

IETF RFC 6614: Encapsulating MPLS in IP or GRE

NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems

ISO 27001:2013: Information Security Management Systems

Common Criteria EAL2+ Certification

FIPS 140-2 Level 1 Cryptographic Module Validation

TECHNICAL SPECIFICATIONS

Parameter	**Specification**
Form Factor	1RU Standard Rack Mount / Modular Chassis Options Available
Switching Capacity	1.2 Tbps Full-Duplex, Non-Blocking Architecture
MAC Address Table Size	128K Entries Standard, Expandable to 256K
Port Security Profiles	Static, Dynamic, Sticky (Per-Port and Per-VLAN Configurable)
Maximum MAC Addresses Per Port	1 to 1024 Configurable
Violation Actions	Protect, Restrict, Shutdown

	(Configurable per Port)
MAC Learning Rate Limit	1000 Addresses/Second Default, Burst 2000
Aging Timer	10 to 1,000,000 Seconds Configurable, Default 300 Seconds
CAM Watermark Thresholds	High 90%, Low 70%, Configurable
Event Buffer Capacity	16K Entries with 100ns Timestamp Resolution
Sticky MAC Persistence	Non-Volatile Flash Storage, Auto-Restore on Reboot
802.1X Integration	Supports RADIUS, TACACS+, and CoA
MACsec Support	IEEE 802.1AE-2018, 128-bit and 256-bit Encryption
Power Supply	Dual Hot-Swappable Redundant AC/DC, 100-240V AC, 48V DC
Power Consumption	120W Typical, 180W Maximum
Operating Temperature	0°C to 45°C (32°F to 113°F), Extended Range Optional
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Relative Humidity	5% to 95% Non-Condensing
MTBF	>300,000 Hours Telcordia SR-332 Issue 4

Dimensions (H x W x D)	1.72 x 17.4 x 16.2 Inches (43.7 x 442 x 411 mm)
Weight	12.5 lbs (5.7 kg) with Dual Power Supplies
Regulatory Compliance	FCC Part 15 Class A, CE, VCCI, CISPR 22 Class A, UL 60950-1, IEC 60950-1, RoHS 6/6

ORDERING SKU INFORMATION

Base Platform SKUs:

SW-MAC-SEC-48P: 48-Port 10/100/1000BASE-T with MAC Security and Port Security Profiles, 4x 10G SFP+ Uplinks, Dual Redundant Power Supplies

SW-MAC-SEC-24P: 24-Port 10/100/1000BASE-T with MAC Security and Port Security Profiles, 2x 10G SFP+ Uplinks, Single Power Supply

SW-MAC-SEC-48F: 48-Port 1000BASE-X SFP with MAC Security and Port Security Profiles, 6x 10G SFP+ Uplinks, Dual Redundant Power Supplies

SW-MAC-SEC-32Q: 32-Port 40G QSFP+ with MAC Security and Port Security Profiles, 8x 100G QSFP28 Uplinks, Dual Redundant Power Supplies

SW-MAC-SEC-64P: 64-Port 10GBASE-T with MAC Security and Port Security Profiles, 8x 100G QSFP28 Uplinks, Dual Redundant Power Supplies

Software License SKUs:

LIC-MAC-SEC-ADV: Advanced MAC Security License including Sticky MAC, Per-VLAN Enforcement, and Hardware Event Buffer

LIC-MAC-SEC-ENT: Enterprise MAC Security License including all Advanced features plus 802.1X Integration and RADIUS Change of Authorization

LIC-MAC-SEC-CAR: Carrier MAC Security License including all Enterprise features plus MEF-compliant Service OAM and Y.1731 Performance Monitoring

Accessory SKUs:

ACC-MAC-SEC-FAN: Replacement Fan Tray Module for 1RU Platforms

ACC-MAC-SEC-PSU: Replacement Power Supply Unit, AC or DC Input

ACC-MAC-SEC-RMK: Rack Mount Kit, 19-inch EIA Standard

ACC-MAC-SEC-CBL: Console Cable, RJ45 to DB9, 6-foot Length

