IEEE 802.1X Port-Based Authentication - Official Technical Overview & Hardware Datasheet

IEEE 802.1X PORT-BASED AUTHENTICATION

OFFICIAL TECHNICAL OVERVIEW & HARDWARE DATASHEET

EXECUTIVE SUMMARY

The IEEE 802.1X standard defines a port-based network access control (PNAC) mechanism that provides an authentication framework for devices wishing to attach to a LAN or WLAN. This document serves as the definitive technical reference for our hardware implementation of 802.1X, covering authenticator, supplicant, and authentication server roles embedded within our enterprise switching and routing platforms. Our implementation ensures that only authorized devices gain access to protected network ports, preventing unauthorized endpoint connectivity at the physical or virtual port level.



HARDWARE ARCHITECTURE & SILICON

The 802.1X processing pipeline is implemented directly within the programmable forwarding ASIC, enabling line-rate Extensible Authentication Protocol over LAN (EAPoL) frame inspection and state machine processing without CPU intervention for non-blocked flows. Key hardware elements include:

- DEDICATED EAPoL PARSER: Deep packet inspection engine identifying EtherType 0x888E frames at wire speed.
- PORT STATE MACHINE: Per-port silicon-level finite state machine tracking Unauthorized, Authorized, and Held states.
- INTEGRATED RADIUS CLIENT: Hardware-accelerated RADIUS request/response handling for authentication, authorization, and accounting

(AAA).

- SECURE CREDENTIAL STORAGE: 64KB on-chip trusted memory for MAC Authentication Bypass (MAB) whitelists and Guest VLAN parameters.

KEY FEATURES & ROUTING LOGIC

- MULTI-DOMAIN AUTHENTICATION: Differentiate authentication for voice and data devices on the same physical port, applying distinct VLAN and QoS profiles.
- MAC AUTHENTICATION BYPASS (MAB): Support for legacy devices lacking 802.1X supplicant capability; MAC addresses are silently learned and authenticated via RADIUS.
- GUEST VLAN: Automatic assignment of unauthenticated devices to a restricted Guest VLAN with limited network access, allowing captive portal workflows.
- CRITICAL VLAN: Ports automatically transition to a Critical VLAN when RADIUS servers become unreachable, ensuring business continuity.
- EAP METHOD SUPPORT: EAP-MD5, EAP-TLS, EAP-TTLS, PEAPv0/MSCHAPv2, EAP-FAST – all terminated on the authenticator or passed through to backend servers.
- DYNAMIVE VLAN ASSIGNMENT: RADIUS server returns VLAN identifiers (RFC 3580) upon successful authentication; the switch dynamically reconfigures the

port's VLAN membership.

- SUPPLEMENTANT AUTO-DETECTION: hardware logic detects EAPoL-Start packets; ports without supplicants can automatically fall back to MAB or Guest VLAN.

- RE-AUTHENTICATION TIMERS: Programmable hardware timers (60 to 86400 seconds) force periodic re-authentication to maintain session validity.

COMPLIANCE & STANDARDS

- IEEE 802.1X-2020 (Port-Based Network Access Control)

- IEEE 802.1AE (MACsec) – Optional link-layer encryption for authenticated ports

- IEEE 802.1Q (VLAN assignment extension)

- RFC 2865 (RADIUS Authentication)

- RFC 2866 (RADIUS Accounting)

- RFC 3576 (RADIUS Dynamic Authorization / CoA)

- RFC 3580 (RADIUS attributes for 802.1X)

- RFC 5176 (RADIUS Disconnect and Change of Authorization)

TECHNICAL SPECIFICATIONS

Maximum Concurrent Authenticated Sessions: 32,000 (per system)

EAPoL Frame Processing Rate: 14.88 Mpps (at wire speed for Gigabit ports)

Authentication State Machine Clock Resolution: 1 ms

Configurable Quiet Period: 0 – 65,535 seconds

Configurable Tx Period (EAP-Request/Identity retry): 1 – 60 seconds

Configurable Supplicant Timeout: 1 – 300 seconds

Max EAPoL Start Retries: 3 (default, configurable 1-10)

MAB Learning Timeout: 30 seconds (default)

RADIUS Server Failover Detection: Sub-3 second keep-alive with 3 retries

Port Modes Supported: Single-host, Multi-host, Multi-domain

Parameter	**Specification**
Authenticator Capacity (Concurrent Ports)	Up to 512 ports per chassis / 48 ports per 1RU fixed switch
Max Authentication Sessions	32,000 (system-wide)
EAPoL Frame Processing	Line-rate, full wire speed, no performance penalty
RADIUS Server Support	Up to 12 servers (primary + 11 backup), round-robin or priority-based
Supported EAP Methods	MD5, TLS, TTLS, PEAPv0/MSCHAPv2, FAST
Power Supply Requirement	Dual hot-swappable redundant AC/DC

	(100-240V AC / -48V DC)
Operating Temperature	0° C to +50° C (32° F to 122° F)
MTBF (Telcordia SR-332)	285,000 hours (authenticator function as integrated component)

ORDERING SKU INFORMATION

Hardware platforms supporting 802.1X authenticator function (standard on all enterprise switching SKUs). Optional software license for advanced features:

- LIC-8021X-ADV: Enables per-user ACLs, downloadable user roles, and RADIUS CoA for session tear-down
- LIC-MACSEC-1G/10G/25G/100G: Adds IEEE 802.1AE encryption for authenticated ports (requires transceivers with MACsec capability)

Our 802.1X implementation does not require any hardware license for base authenticator, MAB, Guest VLAN, or Critical VLAN functions across all Enterprise Switching Series (ESS-2000, ESS-5000, ESS-9000) and Campus Core Series (CCS-7000).

