Port Isolation in Industrial Ethernet Switching - Official Technical Overview & Hardware Datasheet

PORT ISOLATION IN INDUSTRIAL ETHERNET SWITCHING

OFFICIAL TECHNICAL OVERVIEW & HARDWARE DATASHEET

EXECUTIVE SUMMARY

The increasing density of OT (Operational Technology) networks mandates stringent traffic segmentation at the physical port level without the overhead of VLAN configuration or inter-VLAN routing. This document details the hardware-accelerated Port Isolation (Private VLAN Edge) feature set implemented across our industrial switch portfolio. Port Isolation enables network operators to enforce layer-2 traffic separation between specified downstream ports while maintaining uplink connectivity to a common gateway or server farm. Unlike traditional VLANs that consume 802.1Q tags and require IP routing for inter-VLAN blocking, hardware-based Port Isolation operates within the switching silicon’ s forwarding database (FDB), achieving line-rate blocking with zero latency penalty. This datasheet provides system architects with the precise forwarding engine behavior, performance metrics, and deployment topologies for secure, high-density edge aggregation.



HARDWARE ARCHITECTURE & SILICON

PROPRIETARY FORWARDING ENGINE IMPLEMENTATION

Port Isolation is implemented directly within the switch ' s ASIC (Application-Specific Integrated Circuit) forwarding pipeline, specifically within the egress access control list (ACL) lookup stage. Each physical port is assigned a private "isolation group" identifier (1-4094) via hardware registers. The ASIC compares source and destination port group IDs before performing a layer-2 lookup. If both ports belong to the same isolation group and neither is designated as a "promiscuous" (uplink) port, the frame is dropped inside the switching fabric without consuming packet buffer memory. This hardware-native design achieves wire-speed filtering for all frame sizes (64 to 9216 bytes).

INTERNAL PACKET FLOW FOR ISOLATED PORTS

1. Frame arrives on an ingress port.

2. ASIC extracts ingress port ID and maps to its isolation group (stored in TCAM).

3. Parallel lookup: Destination MAC is resolved to egress port ID.

4. Comparison logic: IF (ingress_group == egress_group AND both_ports_are_isolated) THEN drop_flag = TRUE.

5. If drop_flag = FALSE, forward frame to switching fabric.

KEY FEATURES & ROUTING LOGIC

- Hardware-Based Port Isolation: Blocking is performed in the ASIC pipeline, not via software ACLs or CPU intervention. Achieves 148.8 Mpps (million packets per second) for 64-byte frames on Gigabit ports, with zero performance degradation when all 28 ports are isolated.

- Promiscuous (Uplink) Port Designation: Any port can be configured as a promiscuous port (community port in Private VLAN terminology). Promiscuous ports communicate freely with all isolated ports, but isolated ports cannot communicate directly with each other.

- Overlapping Isolation Groups: A single physical port may belong to multiple

isolation groups, enabling complex segmentation (e.g., Isolated Group A: Ports 1-8, Isolated Group B: Ports 5-12, with Ports 5-8 mutually blocked but individually visible to different uplinks).

- Preservation of 802.1Q VLANs: Port Isolation operates orthogonally to VLANs. Isolated ports can reside in the same broadcast domain (same VLAN) yet remain unable to forward unicast, broadcast, or multicast frames to each other. VLAN tags are unmodified, preserving end-to-end QoS markings.

- IGMP Snooping Override: For IP multicast applications (e.g., IP cameras or industrial controllers), the ASIC can optionally allow specific multicast streams to bypass isolation rules when the destination multicast group is known to be required on multiple isolated ports.

- Port Isolation + Storm Control: Hardware-level storm control (broadcast, unknown-unicast, multicast) applies priority over isolation rules, dropping excess frames before isolation check to conserve fabric bandwidth.

COMPLIANCE & STANDARDS

- IEEE 802.1Q (VLAN Tagging) – Interoperable with industry-standard Private VLAN Edge implementations from Cisco, Arista, and Juniper.

- IEC 61850-3 (Substation Automation) – Port Isolation qualified for GOOSE/SMV traffic isolation without introducing latency variance.

- EN 50121-4 (Railway EMC) – Switching noise immunity for wayside

applications requiring port-to-port electrical isolation.

- IEEE 1588v2 (PTP) – Hardware timestamps are unaffected by isolation rules; one-step transparent clock continues to correct residence time.

- NERC CIP-005 (Cyber Security) – Supports compliance for BES cyber system electronic access points by enforcing port-based separation.

TECHNICAL SPECIFICATIONS

Parameter	**Specification**
Form Factor	1RU Industrial / IP30 Metal Chassis (12, 28, or 52-port variants)
Switching Capacity	68 Gbps (non-blocking for 28-port model), 128 Gbps (52-port model)
Port Isolation Groups	16 (default), expandable to 256 with ISW-LIC-ISO-256
Forwarding Rate	148.8 Mpps (Gigabit ports, all frame sizes)
Latency (Isolation On)	≤ 5.6 microseconds (64-byte frame, store-and-forward)
Power Supply	Dual 24-60 VDC redundant inputs (Hot-swappable option)
Operating Temperature	-40°C to +75°C (fanless operation up

	to +60°C)
MTBF	> 850,000 hours (Telcordia SR-332, Issue 4, GB)
Packet Buffer Memory	12 MB shared (dynamic per port)
MAC Address Table	16K entries (shared between FDB and isolation group TCAM)

ORDERING SKU INFORMATION

ISW-28P-IE: 28-Port Industrial Managed Switch (24x 10/100/1000BASE-T + 4x 1G SFP slots). Includes hardware port isolation engine.

ISW-28P-IE-P: Same as ISW-28P-IE with PoE+ (IEEE 802.3at, 30W per port) and per-port isolation power budget management.

ISW-12M-IE: 12-Port modular industrial switch (8x combo ports + 4x 10G SFP+). Supports isolation groups across chassis backplane.

ISW-LIC-ISO-256: Software license to expand isolation groups from default 16 to 256 groups. Required for large-scale multi-tenant deployments.

