Secured Edge Node Technical Compliance Register: Huawei CloudEngine S6730-H 10GE Switch MACsec Encryption Processing

SECURITY POSITIONING

The Huawei CloudEngine S6730-H series represents a purpose-built response to the escalating threat landscape confronting enterprise campus aggregation and small-scale core deployments. Within this architecture, MACsec encryption processing is not an auxiliary feature but a foundational security primitive integrated at the hardware forwarding plane. The S6730-H-V2 variants equipped with the "Z" designation—specifically the S6730-H28X6CZ-V2 and S6730-H48X6CZ-V2—incorporate line-rate IEEE 802.1AE MACsec capability directly into the switching ASIC, ensuring that confidentiality and integrity verification for 10GE uplinks are delivered without compromising forwarding throughput or introducing measurable latency penalties. This positioning addresses the critical gap between perimeter defense and internal lateral movement, enabling operators to treat the access-to-aggregation link as a zero-trust conduit rather than an implicit trust boundary.



LINE-RATE ENCRYPTION CAPABILITIES

The MACsec implementation on the S6730-H-V2 platform operates at the hardware layer, processing encryption and integrity check value (ICV) generation for every frame traversing secured interfaces. Unlike software-based cryptographic overlays that introduce jitter and throughput degradation, this ASIC-integrated approach maintains deterministic forwarding performance. The switch supports the GCM-AES-XPN-128 and GCM-AES-XPN-256 cipher suites, with configuration flexibility across three operational modes: normal (encryption and integrity), integrity-only (no payload encryption but full tamper detection), and none (pass-through for interoperability staging). The MACsec key agreement (MKA) protocol operates with configurable session lifetimes, and the key server priority mechanism ensures deterministic election of the transmitting entity in point-to-point topologies. Notably, MACsec functionality

requires no additional license activation; the feature package is available as a software download, lowering the barrier to deployment for security-conscious operators.

PHYSICAL TAMPER-RESISTANCE

While MACsec secures data in transit against passive interception and active modification, the S6730-H chassis contributes a complementary physical security posture. The 1RU metal enclosure provides a rigid mounting foundation, and the redundant power architecture—supporting 1+1 AC or DC pluggable modules with mixed AC/DC operation permitted within the same chassis — reduces the attack surface associated with single points of power failure. Airflow design follows a front-to-rear path for the S6730-H24X6C and similar variants, facilitating deployment in controlled datacenter or telecommunications closet environments where thermal and physical access are already governed by procedural controls. The integration of secure boot and signed firmware images, while not explicitly documented in the MACsec configuration guides, represents standard Huawei practice for CloudEngine platforms and reinforces the chain of trust from hardware root to encrypted link.

DETAILED PARAMETERS

The following parameters reflect the S6730-H-V2 series (specifically the Z-designated variants supporting MACsec) and the broader S6730-H hardware family where applicable. Values are drawn from Huawei official specification repositories.

Parameter	**Specification**
Form Factor	1RU metal chassis; dimensions 43.6 mm × 442.0 mm × 420.0 mm (H × W × D, basic)
MACsec-Supported Models	S6730-H28X6CZ-V2, S6730-H48X6CZ-V2 (Z-designated V2 variants only)
MACsec Interfaces (S6730-H48X6CZ-V2)	10GE ports 1–48; 40GE/100GE ports 5–6
MACsec Interfaces (S6730-H28X6CZ-V2)	10GE ports 1–28; 40GE/100GE ports 5–6
Cipher Suites	GCM-AES-XPN-128, GCM-AES-XPN-256
Encryption Modes	Normal (encrypt + integrity), Integrity-only, None (pass-through)
License Requirement	No license required; MACsec feature

	package available as software download
Switching Capacity (S6730-H48X6C-V2 class)	2.4 Tbps
Forwarding Performance	490 Mpps
Power Supply	1+1 redundant pluggable AC or DC; mixed AC/DC permitted in same chassis
Typical Power Consumption	149 W (S6730-H24X6C reference)
MTBF	62.27 years (S6730-H24X6C reference)
Operating Temperature	-5 °C to +45 °C (0–1800 m altitude); derating above 1800 m
MACsec Standard	IEEE 802.1AE

REGULATORY CERTIFICATIONS

The CloudEngine S6730-H series carries EMC, safety, and production certifications appropriate for enterprise and carrier-adjacent deployments. While MACsec itself is a protocol-level capability governed by IEEE 802.1AE, the supporting hardware platform has been validated for operational stability across extended temperature ranges. The switch operates within a long-term

ambient range of -5°C to +45°C at altitudes up to 1800 meters, with derating above that elevation at a rate of 1°C per 220 meters. Storage tolerance extends from -40°C to +70°C. These environmental qualifications, combined with the MTBF rating exceeding 62 years for the S6730-H24X6C variant, substantiate the reliability claims necessary for deploying cryptographic processing in production aggregation roles.

PERIMETER DEPLOYMENT

In a representative campus architecture, the S6730-H48X6CZ-V2 serves as the aggregation node for a building or floor, terminating 10GE SFP+ links from access switches while providing 40GE or 100GE QSFP28 uplinks toward the core. MACsec is applied to the 10GE interfaces facing downstream access layers, where cable runs may traverse semi-public spaces (riser closets, shared conduits) susceptible to tapping. The 48 10GE ports on the S6730-H48X6CZ-V2 all support MACsec binding; on the S6730-H28X6CZ-V2, the first 28 10GE interfaces are eligible. For uplinks toward the core, MACsec may also be applied if the peer device supports compatible cipher suites, though in practice operators often terminate encryption at the aggregation boundary to avoid cipher negotiation complexity with legacy core infrastructure. The QSFP28 interfaces (ports 5-6 on both models) additionally support MACsec, enabling secured high-capacity transport where the core peer is similarly equipped. This

deployment model preserves the investment in existing access switching while extending cryptographic protection to the most vulnerable segment of the campus transport fabric.

