CLI Command Line Interface SSHv2 Management - Official Technical Overview & Hardware Datasheet

EXECUTIVE SUMMARY

The global telecommunications infrastructure landscape demands secure, cryptographically verified out-of-band management interfaces for carrier-grade routing, switching, and transport equipment. The CLI Command Line Interface SSHv2 Management framework represents a hardened, FIPS 140-2/3-compliant secure shell access methodology, purpose-built for network engineers and automated orchestration systems requiring authenticated, encrypted, and integrity-checked device administration. This datasheet defines the hardware-accelerated SSHv2 management plane implemented across our portfolio of edge routers, core switches, and optical transport platforms.

ARCHITECTURE & CHASSIS DESIGN

The SSHv2 management subsystem is architected as a logically isolated control-plane module with dedicated cryptographic acceleration co-processors. Key architectural components include:

- DEDICATED MANAGEMENT ETHERNET PORT: 10/100/1000BASE-T out-of-band channel, electrically isolated from the forwarding data plane
- CRYPTOGRAPHIC ACCELERATOR: Hardware Security Module (HSM) supporting RSA (2048/4096-bit), ECDSA (P-256, P-384), and Ed25519 public-key algorithms
- SECURE KEY STORAGE: Tamper-resistant NVRAM with zeroization capability, storing up to 32 host key pairs and 2048 user public keys
- SESSION MANAGEMENT: Concurrent support for up to 64 active SSHv2 sessions, with per-session memory isolation and strict traffic policing

The physical management port is located on the front panel of the 1RU/2RU chassis, adjacent to console and USB ports, color-coded in blue for immediate identification. LED indicators provide real-time status: Solid Green indicates active SSH daemon, Blinking Amber signifies authentication failures, and Solid Blue denotes a session established with perfect forward secrecy (PFS).

HARDWARE FEATURES

- DEDICATED SSH DAEMON PROCESSOR: ARM Cortex-A72 quad-core at 1.5 GHz, exclusively assigned to management plane functions
- SECURE BOOT CHAIN: U-Boot verified boot with RSA-2048 signature validation on SSHv2 firmware binaries
- ALGORITHM SUITE: AES-128/256-CBC, AES-128/256-CTR, AES-128/256-GCM, ChaCha20-Poly1305, 3DES-CBC (legacy mode disableable)
- KEY EXCHANGE: curve25519-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group-exchange-sha256
- MESSAGE AUTHENTICATION CODES (MACs): hmac-sha2-256, hmac-sha2-512, hmac-sha1 (disabled by default)
- USER AUTHENTICATION: publickey, password, keyboard-interactive, and hostbased methods; support for TACACS+ and RADIUS proxy
- ACCESS CONTROL: IPv4/IPv6 ACLs applied at the management ACL table, prefix-based restrictions, and role-based CLI views
- AUDIT LOGGING: Session recording to internal syslog buffer (64 MB) and external rsyslog servers; timestamped with millisecond precision

COMPLIANCE & STANDARDS

- IETF RFC 4251-4256 (SSH Protocol Architecture, Transport Layer,

Authentication, Connection)

- FIPS 140-2 Level 2 (certificate #XXXX) awaiting FIPS 140-3 validation

- Common Criteria EAL4+ (certificate #YYYY)

- NIST SP 800-131A (transitioning cryptographic algorithms)

- PCI DSS v3.2.1 (requirement 2.2.3, 3.4, 8.2.1)

- ISO/IEC 27001:2022 (Annex A.14.2.1)

TECHNICAL SPECIFICATIONS

Parameter	**Specification**
Form Factor	1RU (front-to-back cooling) or 2RU (side-to-side) chassis options
Management Ports	1x RJ45 10/100/1000BASE-T (OOB) + 1x USB 3.0 Console + 1x RJ45 RS-232 Console
Concurrent SSHv2 Sessions	64 (standard), 128 (enhanced SKU)
Host Key Storage Capacity	32 key pairs (RSA/ECDSA/Ed25519)
User Public Key Capacity	2048 entries
Cryptographic Accelerator Throughput	25,000 handshakes per second (RSA-2048)
Session Log Buffer	64 MB internal, external syslog up to 1 TB

Operating Temperature	-5 °C to +55 °C (standard), -40 °C to +70°C (hardened)
Power Consumption (Management Plane)	15W (max), 8W typical
Mean Time Between Failures (MTBF)	285,000 hours (Telcordia SR-332)

ORDERING OPTIONS

The SSHv2 management capability is included as standard firmware on all current-generation routing and switching platforms. No separate license is required for base functionality. Enhanced features require specific SKUs:

- SSH-SC-01: Advanced session recording and playback module (includes 512 GB internal storage)
- SSH-HSM-02: External USB HSM for enhanced key storage (RSA-4096, ECDSA-P521)
- SSH-FIPS-03: FIPS 140-2 validated mode firmware module (restricts algorithms to approved set)
- SSH-BULK-10: Volume licensing for 10,000+ managed devices (includes centralized key management server integration)

All hardware platforms ship with default SSHv2 disabled. Initial configuration must be performed via physical console port or USB serial adapter. Factory default settings enforce:

- Protocol version: SSHv2 only (SSHv1 explicitly disabled)
- Root login: prohibited
- Password authentication: enabled with minimum 15-character complexity
- Idle timeout: 600 seconds
- Maximum authentication attempts: 3

For hardware-specific Management Interface Modules (MIMs) and line card compatibility, refer to the platform-specific Ordering Guide document. All cryptographic components are export-controlled under ECCN 5D002 and require end-user certification for international shipments.