

MACsec

Media Access Control Security



SOLUTION TRACK

Key Features

- IEEE 802.1AE-2018 MACsec support
- Supports both Point-to-point and group Connectivity Associations (CAs)
- Traffic type can be L2 (Ethernet, VLAN) and L3 (IPv4, IPv6) and a mix of MACsec and non-MACsec.
- 128 Secure Channels per port, up to 4 SAKs
- PN exhaust or configurable packet number based rekeying
- Suitable for Z100qx Loki 4-port traffic generators: 4 x 25G or 4 x 10G
- Requires Xena Release 106 (or later) and XM3

MACsec delivers strong, hardware-based security at the Link Layer, protecting data on the local network segment with integrity, confidentiality, and defense against on-link attacks. This offers a key advantage over Layer 3 security protocols, which cannot stop threats that originate within the same Layer 2 domain.

In addition to the standard Ethernet testing options offered by XM3, the MACsec Solution Track adds IEEE 802.1AE functionality for testing of MACsec on 10G and 25G ports when using Z100qx Loki traffic generators.

Available for use with the four-port Z100qx Loki traffic generators, the **MACsec Solution Track** offers the ability to generate MACsec-encrypted frames at wire speed, control rekeying behaviour, and log throughput and key performance metrics, thereby providing comprehensive validation of MACsec implementations.

This Solution Track is primarily intended for:

- Developers of devices that support MACsec and need to verify performance under realistic traffic loads.
- Operators of secure networks who must validate performance before deployment and troubleshoot issues during operation.

It enables verification and performance testing of a device's reception, forwarding and transmission of MACsec encrypted frames.

Testing can be performed with various traffic loads up to wire speed 100Gbps.

All these extra features are made available via the XenaManager3 software.

ABOUT SOLUTION TRACKS

Solution Tracks add advanced features and functionalities for specialized test scenarios to the already extensive list of core features available on Xena systems. Solution Tracks do not require any hardware update to the module they are installed on, and one module can support multiple Solution Tracks. Solution Tracks are dynamic, with new features and enhancements being added over time as demand and technology evolves. These features and enhancements are included in the general software updates and will be available as long as the module is covered by a valid warranty.

General tests

- L2 and L3 forwarding efficiency
- Non-zero confidentiality offset
- Decryption of traffic with SCI
- Performance during rekeying
- Validating MACsec/Non-MACsec gateway functionality
- Max of MACsec and non-MACsec traffic

Point-to-point tests

- Performance with large number of CAs

Group CA tests

- Performance with large number of piers within one group CA



MACsec Solution Track

MACsec features	
Cipher suites	<ul style="list-style-type: none">• GCM-AES-128 (Clause 14.5)• GCM-AES-256 (Clause 14.6)• GCM-AES-XPB-128 (Clause 14.7)• GCM-AES-XPB-256 (Clause 14.8)
Traffic types	<ul style="list-style-type: none">• L2 (Ethernet, VLAN)• L3 (IPv4, IPv6)• Mix of MACsec and non-MACsec.
Confidentiality	<ul style="list-style-type: none">• Confidentiality (authentication + encryption)• Authentication-only• Offset: 0, 30, 50 (Clause 10.7.25)
SCI	<ul style="list-style-type: none">• With SCI (Clause 9.5, 9.9)• End Station (Clause 9.5, 9.9)• Auto-generated, or manual input SCI
SAK distribution	<ul style="list-style-type: none">• Static SAK
Number of SCs per port	<ul style="list-style-type: none">• Up to 128
Number of MACsec SCs Per Port	<ul style="list-style-type: none">• 4 SAKs per SC (GCM-AES-128 and GCM-AES-XPB-128)• 2 SAKs per SC (GCM-AES-256 and GCM-AES-XPB-256)
Traffic scenarios	<ul style="list-style-type: none">• MACsec to MACsec• MACsec to non-MACsec
Frame size	<ul style="list-style-type: none">• Mixed, Fixed, Increment, Random
Rekey modes	<ul style="list-style-type: none">• PN Exhaustion (default)• Configurable packet count based

Statistics counters	
TX statistics	<ul style="list-style-type: none">• Protected byte count• Encrypted byte count• Total packet count• Total byte count
Rx statistics	<ul style="list-style-type: none">• Delayed packet count• Late packet count (out of window)• Not valid packet count• Total packet count• Latency & jitter• Packet loss

