PRELIMINARY
DATA SHEET

IxNetwork MACsec Test Solution

The Industry's First MACsec Test Solution for High-Speed Ethernet

Data Security with MACsec

With increasing demand of data privacy and protection of critical business assets, security has become an important part of every network, including cloud, data center, 5G, and automotive.

While there are different encryption technologies available for data protection, media access control security (MACsec) brings line-rate encryption throughput for high-speed Ethernet, which is critical for cloud and data center operation. It secures network components, ensuring confidentiality, and defending against potential threats.

MACsec has become an important encryption technology that is shipped with next-generation chips, routers, and switches. Thorough validation of MACsec encryption functions, throughput, and key exchange and rotation is critical to ensuring robust implementation and smooth deployment.

Keysight now offers the industry's first MACsec test solution for high-speed Ethernet to help with early validation in MACsec design and implementation.

Highlights

- Line-rate 400G/200G/100G MACsec traffic encryption and decryption to stress decryption engine
- Dynamic MKA key negotiation or static SAK provision
- Vary frame sizes with fixed, increment, random and IMIX pattern from 64 bytes to 16K bytes
- Control plane protocol messages in either encryption or clear text
- VLAN in clear text for provider bridged network
- Dynamic rekey to validate no packet drop during rekey
- Mode of operation: "Integrity (ICV) only" or "integrity + encryption"
- Full automation support with Python, REST, and other APIs for continuous validation

MACsec Overview

MACsec 802.1AE is an industry-standard security technology that secures a point-to-point link between directly connected nodes. It operates at the link layer and protects layer 2 and above content. MACsec provides line-rate encryption regardless of packet size, and scales linearly compared to IPsec.

MACsec offers the following key services that can protect against most security threats, including denial of service, intrusion, man-in-the-middle, playback attacks, and passive wiretapping:

- Data confidentiality – cipher-based encryption of user data
- Data integrity – through the ICV
- Replay protection – using packet number and window mechanism

With its line-rate encryption throughput, strong encryption protection, lower overhead, and transparency to higher-layer applications, MACsec has become an ideal encryption technology suitable for data center and cloud services that have adopted high-speed Ethernet to meet increased bandwidth demand.

KEYSIGHT TECHNOLOGIES

Keysight's MACsec Test Solution

Keysight now offers its MACsec test solution with a phased approach. Our phase 1 software based MACsec solution provides a *fast*-to-market solution with essential capability. It enables our customers to start testing as early as possible in their design and development cycle. As we follow with an upcoming hardware-based MACsec test solution, customers can fully test their MACsec design, implementation, and interop to ensure quality and performance for massive deployment in the future.

Key Features

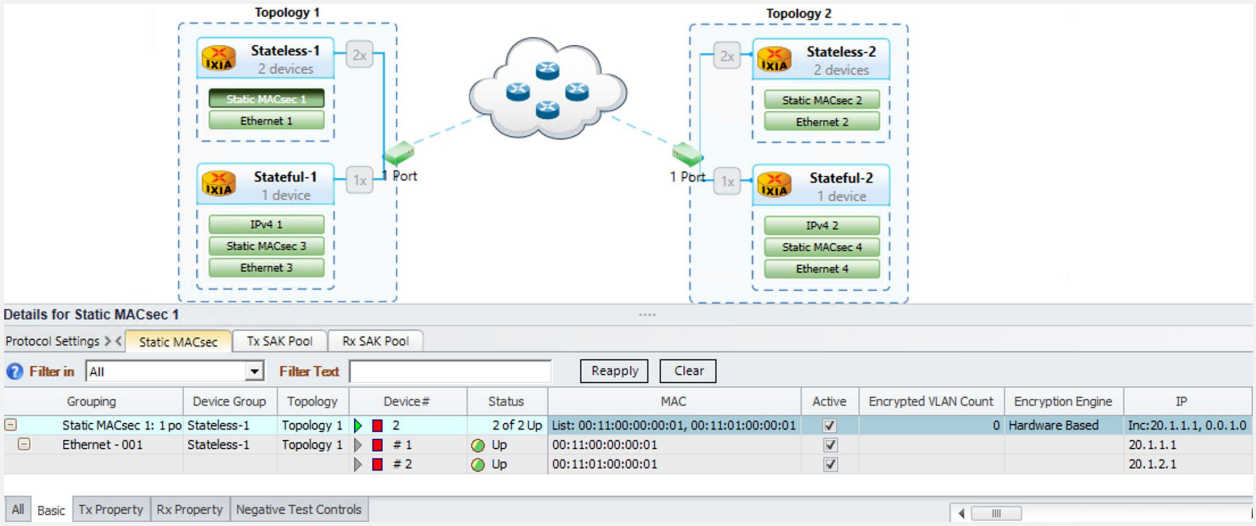
Hardware based MACsec

- Line rate MACsec traffic encryption and decryption at 400/200/100GE PAM4
- Line rate MACsec traffic encryption and decryption at 100G NRZ with active electrical cable (AEC) technology cable interconnect to covert PAM4 signaling and NRZ signaling.
- Option to include or exclude from encryption for selected control plane protocol
- Vary frame sizes from 64 bytes to 16K bytes with fixed, increment, random and IMIX traffic patterns
- Static secure association Key (SAK) provision or dynamic key negotiation with MACsec key agreement (MKA) protocol
- Integrity (ICV) only or integrity + encryption
- 128/256 bits Cipher Suites with XPN (Extended Packet Number) support
  - GCM-AES-128
  - GCM-AES-256
  - GCM-AES-XPN-128
  - GCM-AES-XPN-256
- Re-key on exhaustion of packet number or timer-based periodic re-key
- VLAN in clear text or in encrypted payload
- Confidentiality Offset 0/30/50
- Negative test with bad ICV, unused SA, mal-configured TCI flags, , out of window PN, etc.
- RFC2544 benchmark for MACsec encrypted traffic

Software based MACsec

- MACsec traffic encryption at line rate from 1GE to 400GE with fixed PN (packet number) and payload
- Static secure association Key (SAK) provision or dynamic key negotiation with MACsec key agreement (MKA) protocol
- Real-world application traffic encryption and decryption up to Gbps using Layer 4-7 AppLibrary traffic with standard-defined MACsec statistics
- Frame sizes from 64 bytes to 14K bytes, vary per stream
- Integrity (ICV) only or integrity + encryption
- 128/256 bits Cipher Suites with XPN (Extended Packet Number) support
  - GCM-AES-128

  - GCM-AES-256
  - GCM-AES-XPN-128
  - GCM-AES-XPN-256
- Timer-based periodic re-key with fixed count or continuous
- VLAN in clear text or in encrypted payload
- Confidentiality Offset 0/30/50
- MACsec frame decryption and ICV validation in Wireshark capture
- Negative test with mal-configured TCI flags, bad ICV, erroneous SL, out of window PN, etc.



IxNetwork Static MACsec Emulation

Specifications

Hardware-Based MACsec	
Standards	• IEEE - Std 802.1AE-2018 • IEEE - Std. 802.1X-2020
Cipher Suites	• GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 • GCM-AES-XPN-256
Stateless L2/3 Traffic	• Line rate encryption throughput 400G/200G/100G PAM4 and 100G NRZ • Line rate decryption at receiving port • Static SAK provision or dynamic SAK provision by MKA (PSK based). • Frame size from 64 bytes to 16K bytes, as well as short length frame

Hardware-Based MACsec	
	• Vary frame sizes with fixed, increment, random, and IMIX patterns • Integrity (ICV) only or integrity + encryption • Replay Protection with packet number and window mechanism • XPN (Extended Packet Number) • Re-key on packet number exhaustion or timer-based periodic re-key • Validation of old and new SAK interleaving by the DUT after Rekey • Confidentiality offset 0/30/50 with MKA • Confidentiality offset 0~64 without MKA • With and without SCI • VLAN in clear text and/or in encrypted payload (up to 6 VLANs) • Negative test with bad ICV, unused SA, mal-configured TCI flags, encryption with incorrect key, out of window PN, etc. • Up to 256 Tx/Rx SC support per port, each SC having two concurrent SAs • Ingress and egress tracking per Src/Dest MAC, SCI, and VLAN • RFC2544 benchmark for MACsec encrypted traffic
Stateful L4/7 AppLibrary Traffic	• Encryption and decryption throughput up to Gbps with port aggregation • Encryption with incremental PN and variable payload • Frame size varies per stateful flows • Static SAK provision or dynamic SAK provision by MKA (PSK based) • Integrity (ICV) only or integrity + encryption • Replay Protection with packet number and window mechanism • XPN (Extended Packet Number) • Re-key on packet number exhaustion or timer-based periodic re-key • Confidentiality offset 0/30/50 with MKA • Confidentiality offset 0~64 without MKA • With and without SCI • VLAN in clear text and/or in encrypted payload (up to 6 VLANs) • Negative test with bad ICV, unknown SA, mal-configured TCI flags, out of window PN, etc. • Validation of old and new SAK interleaving by the DUT after Rekey
Control Plane Protocol	• Option to include/exclude selected control plane protocols from encryption • Encryption of undersize control messages less than 64 bytes, e.g. ARP
MKA	• PSK (Pre-shared Key) based key hierarchy • Act as key server or non-key server • Multiple MKA sessions each with a pair-wise CA • Multiple MKA sessions each with multiple members for a group CA • MKA members leaving/joining a CA on the fly • MKA session over VLAN with up to 6 VLAN tags • Confidentiality offset 0/30/50 • Configurable Rekey threshold PN (PendingPNExhaustion) to expedite PN-based Rekey • Configurable starting message number, key number and AN

Hardware-Based MACsec	
MKA Learned Information	• ICV Key • Key Encrypting Key • Secure Association Key • SSCI • Live Peer Member Identifier • Live Peer Message Number • Potential Peer Member Identifier • Potential Peer Message Number
MKA Statistics	• MKPDU Tx • MKPDU Rx • Live Peer Count • Potential Peer Count • Latest Key Tx Peer Count • Latest Key Rx Peer Count • Malform Rx MKPDU • ICV Mismatch
MACsec Statistics	• OutPktsProtected • OutPktsEncrypted • OutOctetsProtected • OutOctetsEncrypted • OutPktsUntagged • InPktsOK • InPktsBad • InPktsBadTag • InPktsLate • InPktsNoSAError • InPktsNotValid • InPktsNoSA • InPktsInvalid • InPktsDelayed • InOctetsValidated • InOctetsDecrypted • InPktsUnchecked • InPktsNoTag
Data Plane Statistics	• Full L2/3 traffic statistics with throughput, loss, latency/Jitter, etc. • Stateful traffic statistics
Negative Testing	• Bad ICV generation • Out of window packet generation • Malformed SecTAG • Unused SA • Mix of MACsec and non-MACsec traffic

Software-Based MACsec	
Standards	• IEEE - Std 802.1AE-2018 • IEEE – Std. 802.1X, June 2019
Cipher Suites	• GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 (in Static Key mode) • GCM-AES-XPN-256 (in Static Key mode)
Stateless Traffic	• Encryption throughput 1G to 400G • Encryption with fixed PN and payload per stream • Decryption and ICV checking with Wireshark • Frame size 64 bytes to 14K bytes, vary per stream, Tx frame can be less than 64 bytes • Static SAK provision or dynamic SAK provision by MKA (PSK based). • Egress only tracking per Rx SCI or Dest MAC • Confidentiality offset 0/30/50 • With and without SCI • Timer-based periodic Rekey • VLAN in clear text and/or in encrypted payload (up to 6 VLANs)
Stateful AppLibrary Traffic	• Encryption and decryption throughput up to Gbps with port aggregation • Encryption with incremental PN and variable payload • Static SAK provision or dynamic SAK provision by MKA (PSK based). • Frame size vary per stateful flows • Confidentiality offset 0 • With and without SCI • Timer-based periodic rekey (no rekey on PN exhaustion) • VLAN in clear text (up to 6 VLANs)
Wireshark Capture	• Decryption per configured SAK • ICV validation • Display SAK used for decryption • Display decrypted payload along with encrypted payload
Negative Testing	• Bad ICV generation • Out of Window packet generation • Malformed SecTAG • Invalid SL value • Mix of MACsec and non-MACsec traffic
MKA	• PSK (Pre-shared Key) based key hierarchy • Act as key server or non-key server • Multiple MKA sessions each with a pair-wise CA • Multiple MKA sessions each with multiple members for group CA • MKA members leaving/joining a CA on the fly

Software-Based MACsec	
	• MKA session over VLAN with up to 6 VLAN tags • Confidentiality offset 0/30/50 • Configurable Rekey threshold PN (PendingPNExhaustion) to expedite PN-based Rekey • Configurable starting message number, starting key number and AN number
MKA Learned Information	• ICV Key • Key Encrypting Key • Secure Association Key • SSCI • Live Peer Member Identifier • Live Peer Message Number • Potential Peer Member Identifier • Potential Peer Message Number
MKA Statistics	• MKPDU Tx • MKPDU Rx • Live Peer Count • Potential Peer Count • Latest Key Tx Peer Count • Latest Key Rx Peer Count • Malform Rx MKPDU • ICV Mismatch
MACsec Statistics	• Protected Packet Tx • Encrypted Packet Tx • Valid Packet Rx • Bad Packet Rx • Bad Tag/ICV Discarded • Out of Window Discarded • Unknow SCI Discarded • Unused SA Discarded • Invalid ICV Discarded • Unknown SCI Rx • Unused SA Rx • Invalid ICV Rx • Tx Bytes Protected • Tx Bytes Encrypted • Rx Bytes Validated • Rx Bytes Decrypted • Non-MACsec Packet Rx
Data Plane Statistics	• Full L2/3 traffic statistics with throughput, loss, etc. • Stateful traffic statistics

Supported Hardware Platforms

Visit keysight.com for More Information on IxNetwork Platform Options	
Hardware-Based MACsec	• AresONE-400G High Performance QSFP-DD 400/200/100/50GE
Software-Based MACsec	• AresONE-400G QSFP-DD 400/200/100/50GE • AresONE-400G OSFP 400/200/100/50GE • Novus ONE PLUS 10GE/5GE/2.5GE/1GE/100M • Novus High Density QSPF28 100/50/40/25/10GE • Novus 10GE/1GE/100M • Novus 10GE/5GE/2.5GE/1GE/100M

Ordering Information

MACsec Part Numbers

Part Number	Description
905-1061	**IXIA, MACsec Enablement FACTORY INSTALLED Option (905-1061);** REQUIRED ON NEW PURCHASES of AresONE T400GP-4P-QDD 400GE high performance fixed chassis models (944-1178); One option is required for each fixed chassis system to enable MACsec capability for 400GE/200GE/100GE ports; REQUIRES: 930-2207 IxNetwork Encryption Test package for AresONE
905-1062	**IXIA, MACsec Enablement FIELD UPGRADE Option (905-1062);** REQUIRED ON FIELD UPGRADE PURCHASES for AresONE T400GP-4P-QDD 400GE high performance fixed chassis models (944-1178); One option is required for each fixed chassis system to enable MACsec option for 400GE/200GE/100GE ports; REQUIRES: 930-2207 IxNetwork Encryption Test package for AresONE
930-2207 (AresONE)	**IXIA IxNetwork, Encryption Test package for AresONE**; INCLUDES: MACsec Emulation; REQUIRES: 930-2201 IxNetwork Basic package for AresONE; Recommend with: 930-3461 IxNetwork AppLibrary Slot Bundle, Optional Software, Layer 4-7 Performance Test Application for additional encryption/decryption capability in Static MACsec emulation
930-2135 (Chassis based)	**IXIA IxNetwork, Optional Software, MACsec Emulation**; Enable MACsec traffic encryption; REQUIRES: pre-existing 930-1999 IxNetwork Base license OR new purchase of either IxNetwork Base PLUS (930-2056) or IxNetwork Base PREMIUM (930-2076); Recommend with: 930-3461 IxNetwork AppLibrary Slot Bundle, Optional Software, Layer 4-7 Performance Test Application for additional encryption/decryption capability
930-2222 (Novus ONE PLUS)	**IXIA IxNetwork, Encryption Test package for Novus ONE PLUS**; INCLUDES: MACsec Emulation; REQUIRES: 930-2221 IxNetwork Basic package for Novus ONE PLUS; Recommend with: 930-3461 IxNetwork AppLibrary Slot Bundle, Optional Software, Layer 4-7 Performance Test Application for additional encryption/decryption capability in Static MACsec emulation

Relevant Hardware Part Numbers

Part Number	Description
944-1178	**IXIA AresONE T400GP-4P-QDD, 4-port**, 400GE high performance fixed chassis model with native QSFP-DD 400GE physical interfaces, and L1-3 support (944-1178).
905-1044	**IXIA AresONE T400GD/T400GDR/T400GP Fan-out option**: 2x200GE, 4x100GE, 8x50GE FACTORY INSTALLED option for the QSFP-DD and OSFP T400GD/T400GDR/T400GP 8-port and 4-port, high performance, full and reduced performance, fixed chassis systems.
905-1045	**IXIA AresONE T400GD/T400GDR/T400GP Fan-out option**: 2x200GE, 4x100GE, 8x50GE fan-out FIELD UPGRADE option for the QSFP-DD and OSFP T400GD/T400GDR/T400GP 8-port and 4-port, high performance, full and reduced performance, fixed chassis systems.
QSFPDD-4XQ28-AEC-CBL	**IXIA QSFP-DD-to-4xQSFP28 400GBASE-R Active Electrical fan-out Cable (AEC)**, for 400GE to 4x100GE fan-out, 3-meter length (942-0139).
944-1140	**IXIA NOVUS100GE8Q28+FAN, 8-port, QSFP28 100GE full scale and performance, load module**, 1-slot with 8-ports with the native QSFP28 physical interface, L2-3 support with complete protocol coverage, and full scale and performance protocol emulation for routing, switching and access protocols.
944-1141	**IXIA NOVUS10/1GE32S,** 32-port, SFP+ 10GE/1GE/100M load module, 1-slot with 32-ports with SFP+ physical interface, L2-3 support.
944-1142	**IXIA NOVUS10/1GE16DP,** 16-port, SFP+/10GBASE-T Dual-PHY 10GE/1GE/100M load module, 1-slot Dual-PHY with 16-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces, L2-7 support.
944-1146	**IXIA NOVUS1GE16DP,** 16-port 1GE/100M SFP+/1000BASE-T Dual-PHY load module. 1-slot Dual-PHY with 16- ports each of the SFP+ and 1000BASE-T RJ45 physical interfaces, L2-7 support.
944-1148	**IXIA NOVUS10/5/2.5/1/100M16DP, 5-speed**, 16-port, SFP+/10GBASE-T Dual-PHY 10G/5G/2.5G/1G/100M full scale and performance, load module, 1-slot Dual-PHY with 16-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces, L2-7 support with complete protocol coverage, and full scale and performance protocol emulation for routing, switching and access protocols.
944-1162	**IXIA NOVUS-NP10/1GE16DP**, 16-port, SFP+/10GBASE-T Dual-PHY 10GE/1GE/100M Application Network Processor load module, 1-slot Dual-PHY with 16-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces, L2-7 support.
941-0063	**IXIA Novus ONE PLUS 10/1GE16DP Fixed Chassis**, 16-port, SFP+/10GBASE-T Dual-PHY 10GE/1GE/100M, 1-slot Dual-PHY with 16-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.
941-0064	**IXIA Novus ONE PLUS 10/1GE8DP Fixed Chassis**, 8-port, SFP+/10GBASE-T Dual-PHY 10GE/1GE/100M, 1-slot Dual-PHY with 8-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.
941-0065	**IXIA Novus ONE PLUS 10/1GE4DP Fixed Chassis**, 4-port, SFP+/10GBASE-T Dual-PHY 10GE/1GE/100M, 1-slot Dual-PHY with 4-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.
941-0066	**IXIA Novus ONE PLUS 10/5/2.5/1GE16DP Fixed Chassis,** 16-port, SFP+/10GBASE-T Dual-PHY 10/5/2.5/1GE/100M, 1-slot Dual-PHY with 16-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.
941-0067	**IXIA Novus ONE PLUS 10/5/2.5/1GE8DP Fixed Chassis**, 8-port, SFP+/10GBASE-T Dual-PHY 10/5/2.5/1GE/100M, 1-slot Dual-PHY with 8-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.
941-0068	**IXIA Novus ONE PLUS 10/5/2.5/1GE4DP Fixed Chassis,** 4-port, SFP+/10GBASE-T Dual-PHY 10/5/2.5/1GE/100M, 1-slot Dual-PHY with 4-ports each of the SFP+ and 10GBASE-T RJ45 physical interfaces. L2-7 support. Includes installation of the latest production released version of the IxOS software.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus