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 ensure 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.

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 — by 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

Keysight's MACsec Test Solution

Keysight now offers the industry's first MACsec test solution for high-speed Ethernet. It enables MACsec validation from hardware design, software stack implementation, to system integration with full coverage of various MACsec functions. Customer can now benchmark MACsec performance under a realistic traffic mix of cloud and data center workloads, guarantee service continuity during key rotation, and ensure stability under various negative conditions.

In addition, Keysight also provides a software based MACsec solution with essential capability to help MACsec validation for lower Ethernet speed in other industries, including 5G, Automotive, and Industrial.

Highlights

- Line-rate 100G/200G/400G 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

Key Features

Hardware based MACsec at 100GE

- Line rate MACsec traffic encryption and decryption at 100GE PAM4
- Line rate MACsec traffic encryption and decryption at 100G NRZ with active electrical cable (AEC) technology 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 Pre-shared Keys (PSK) mode 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
- Timer based roll over of PSK (key chain functionality).
- VLAN in clear text (before secTAG) or in encrypted payload (after secTAG)
- Confidentiality Offset 0/30/50
- 'Delay Protect' with MKA
- Negative test with bad ICV, unused SA, mal-configured TCI flags, out of window PN
- RFC2544 benchmark for MACsec encrypted traffic
- Full automation support with Python, REST, TCL, and HLAPI for continuous validation
- LAG with MACsec, LACPDUs are encrypted or in clear text.

Hardware based MACsec at 400/200GE

- Line rate MACsec traffic encryption and decryption at 400GE/200GE
- GCM-XPN128 and GCM-AES128 ciphers
- Static SAK provisioning
- Zero Confidentiality Offset
- VLAN in encrypted payload
- Traffic and MACsec stats
- Single MACsec session per port
- RFC2544 performance benchmarking
- L47 Applib traffic
- Negative test capabilities (bad ICV, out of window PN, unused SA, mal-configured secTAG)
- Wireshark capture and low-level APIs

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 by 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 Extended Packet Number (XPN) 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
- Timer based roll over of PSK (key chain functionality).
- VLAN in clear text or in encrypted payload
- Confidentiality Offset 0/30/50 (non-zero offset is supported only for stateless traffic)
- MACsec frame decryption and ICV validation in Wireshark capture
- Negative test with mal-configured TCI flags, bad ICV, erroneous SL, out of window PN
- Full automation support with Python, REST, TCL, and HLAPI for continuous validation

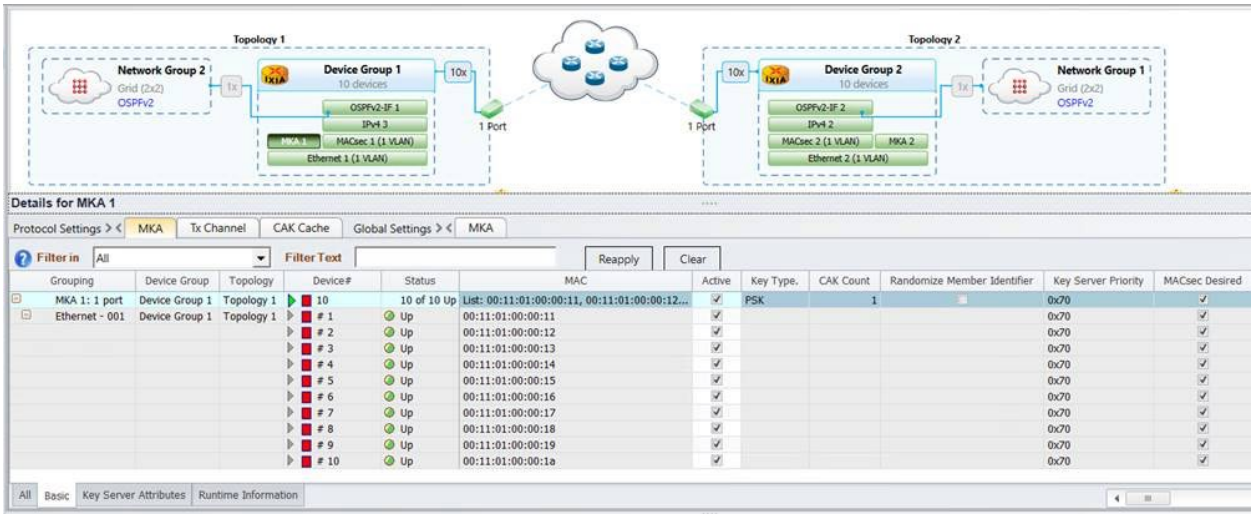

Figure 1. IxNetwork MACsec Emulation

Specifications

Hardware-Based MACsec

Standards	IEEE — Std 802.1AE-2018 IEEE — Std. 802.1X-2020 (MKA only)
Cipher Suites	GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
Stateless L2/3 Traffic	Line rate encryption and decryption throughput over 400/200/100G interface 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 Vary frame sizes with fixed, increment, random, and IMIX patterns Integrity (ICV) only or integrity + encryption 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 4 clear text and 6 encrypted VLANs) Negative test with bad ICV, unused SA, mal-configured TCI flags, encryption with incorrect key, out of window PN Up to 256 Tx/Rx SC support per port for pair-wise CA Up to 128 Tx/Rx SC support per port for group CA Ingress and egress tracking per Src/Dest MAC/IP, SCI, and VLAN RFC2544 benchmark for MACsec encrypted traffic Data traffic from/to end points configured over LAG port Data traffic distribution as well as collection across multiple physical links of LAG with MACsec encryption/decryption at line rate Data traffic failover within multiple links of a LAG port with MACsec Data traffic with encrypted VLAN over LAG with MACsec Checksum calculation support for MACsec encrypted UDP traffic Note: 400/200GE support a subset of the features mentioned above. Please refer “Key Features" section.
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 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 4 clear text and 6 encrypted VLANs)
Control Plane Protocol	Option to include selected control plane protocols (BGP, OSPF, ISIS, EVPN VXLAN) to be encrypted. Encryption of undersize control messages less than 64 bytes, for example, ARP LACP over MACsec with LACPDUs as encrypted/clear. BGP/OSPF/ISIS/EVPN VXLAN over LAG port with MACsec encryption/decryption
MKA	PSK (Pre-shared Key) based key hierarchy Timer based roll over of PSKs (Key Chain) Supports AES-CMAC-128/256 Key Derivation Function (KDF) 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 Simulate delayed MACsec packets on demand by bumping up the LLPN advertised in Hello packets, to test DUT's 'delay protect' behavior Configurable destination MAC and EAPOL ethernet type
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	Per Device: Valid Packet Rx Bad Packet Rx Invalid ICV Discarded

	Invalid ICV Accepted
Hardware-Based MACsec	
	Rx Bytes Validated Rx Bytes Decrypted Per Port: OutPktsEncrypted Protected Packet Tx Encrypted Packet Tx Protected Byte Tx Encrypted Byte Tx Non-MACsec Packet Tx Protected Packet Rx Encrypted Packet Rx Protected Byte Rx Encrypted Byte Rx Non-MACsec Packet Rx Unknown SCI/SA Accepted Unknown SCI/SA Discarded Valid Packet Rx Broadcast Bad Packet Rx Broadcast Invalid ICV Discarded Broadcast Invalid ICV Accepted Broadcast Rx Bytes Validated Broadcast Rx Bytes Decrypted Broadcast Valid Packet Rx Multicast Bad Packet Rx Multicast Invalid ICV Discarded Multicast Invalid ICV Accepted Multicast Rx Bytes Validated Multicast Rx Bytes Decrypted Multicast
Data Plane Statistics	Full L2/3 traffic statistics with throughput, loss, latency/Jitter Stateful traffic statistics
Negative Testing	Packets with bad ICV Out of window packet generation Delayed packet simulation Packets with malformed secTAG Packets with Unused SA Mix of MACsec and non-MACsec traffic

Note: See the 7019-0473-T-DS-AresONE-400GE-QSFP-DD-High-Performance data sheet for hardware specifications.

Software-Based MACsec

Standards	IEEE — Std 802.1AE-2018 IEEE — Std. 802.1X-2020 (MKA only)
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 Destination 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 sizes 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 Timer based roll over of PSKs (Key Chain) 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 MKA session over VLAN with up to 6 VLAN tags Confidentiality offset 0/30/50

Software-Based MACsec	
	Configurable Rekey threshold PN (‘pendingPNExhaustion’) to expedite PN-based Rekey Configurable starting message number, starting key number and AN number Configurable destination MAC and EAPOL ethernet type
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 Stateful traffic statistics

Supported Hardware Platforms

Visit www.keysight.com for More Information on IxNetwork Platform Options

Hardware-Based MACsec	AresONE 400G High Performance QSFP-DD 100GE
Software-Based MACsec	AresONE 800G QSFP-DD 800/400/200/100GE
	AresONE 800G OSFP 800/400/200/100GE
	AresONE 400G High Performance QSFP-DD 400/200/100/50GE
	AresONE-S 400G QSFP-DD 400/200/100/50GE
	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 High Density SFP28/QSPF28 100/50/25/10GE
	Novus 10GE/1GE/100M
	Novus 10GE/5GE/2.5GE/1GE/100M

Ordering Information

MACsec part numbers

Part number	Description
905-1061	IXIA, **MACsec Enablement** for AresONE T400GP-4P-QDD 400GE high performance fixed chassis system (944-1178) with **FACTORY INSTALLED Option (905-1061)**; One option is required for each fixed chassis system to enable MACsec capability for 100GE ports; REQUIRES: 905-1044 AresONE T400GD/GDR/GP 2x200GE, 4x100GE, 8x50GE FAN-OUT FACTORY INSTALLED option; REQUIRES: 930-2207 IxNetwork Encryption Test package for AresONE
905-1062	IXIA, **MACsec Enablement** for AresONE T400GP-4P-QDD 400GE high performance fixed chassis system (944-1178) with **FIELD UPGRADE Option (905-1062)**; One option is required for each fixed chassis system to enable MACsec option for 100GE ports; REQUIRES: 905-1044 AresONE T400GD/GDR/GP 2x200GE, 4x100GE, 8x50GE FAN-OUT FACTORY INSTALLED option OR 905-1045 AresONE T400GD/GDR/GP 2x200GE, 4x100GE, 8x50GE FAN-OUT FIELD UPGRADE option; 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

MACsec bundle part numbers

Part number	Description
947-4063	**IXIA MACsec 16-Port 100GE Bundle**, enable MACsec testing over 100GE Ethernet Interface of AresONE high performance 400G fixed chassis (947-4063); Include AresONE T400GP-4P-QDD 400GE high performance fixed chassis model with native QSFP-DD 400GE physical interfaces and L1-3 support (944-1178), and AresONE T400GD/GDR/GP 2x200GE, 4x100GE, 8x50GE FAN-OUT FACTORY INSTALLED option (905-1044), and MACsec ENABLEMENT FACTORY INSTALLED option (905-1061), and IxNetwork Basic package for AresONE (930-2201), and IxNetwork Encryption Test package for AresONE (930-2207)

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).
944-1179	**IXIA AresONE T400GP-2P-QDD, 2-port enablement** on AresONE T400GP-4P-QDD high performance fixed chassis model (944-1178), with native QSFP-DD 400GE physical interfaces, L1-3 support (944-1179)
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.
944-1164	**IXIA NOVUS-S 10/25GE8SFP28, 8-port, SFP28 10GE/25GE load module,** 1-slot with 8-ports adaptor based SFP28 physical interface
944-1165	**IXIA NOVUS100GE4Q28+FAN, 4-port enablement on the NOVUS100GE8Q28+FAN load module** (944-1140), 1-slot with 4-ports, L2-3 load module with complete protocol coverage, and full scale and performance
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.

Part number	Description
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.

More information:

https://www.keysight.com/in/en/products/network-test/protocol-load-test/ixnetwork.html