OPEN POSSIBILITIES.

MACsec - Securing data in motion without performance penalty

OCP
GLOBAL
SUMMIT

NOVEMBER 9-10, 2021

[Security]

MACsec - Securing data in motion without performance penalty

Yuanwen (Daisy) Sun
Principal Technical Product Manager
Keysight

OPEN POSSIBILITIES.

OPEN COMMUNITY®

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Agenda

SECURITY

- MACsec market and technology overview
- Why MACsec is now mission-critical?
- The state of the industry and the key use cases for hyperscalers
- The challenges of realizing the promises of MACsec
- Testing must evolve to ensure proper validation
- Introduce Keysight/Juniper Joint 100/400GE MACsec demo

Encryption Market Overview

SECURITY

Cloud/Data Center

- Data Center Interconnect
  - 100G, 400G
- Direct connect service for enterprise
  - 10G, 100G

5G/Open RAN

- Secure Open RAN network
- RU, DU, Transport device
- Speed - 10G, 25G, 100G

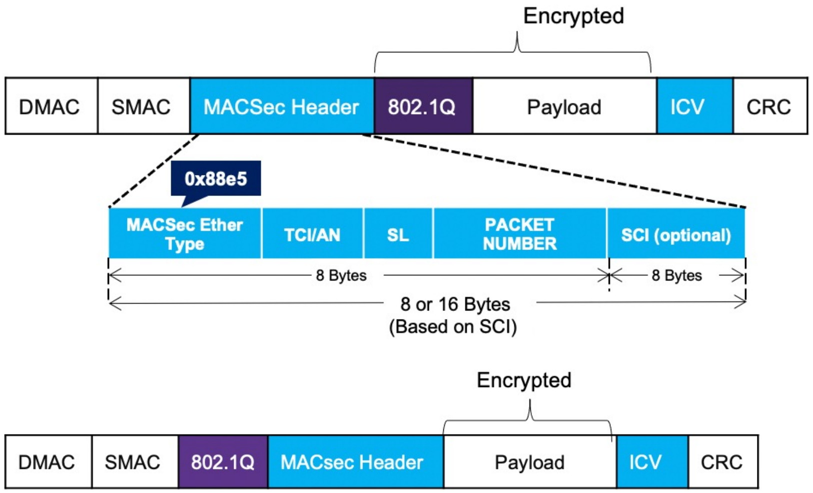
Industrial/Automotive

- Automotive
- Access Point and Modem
- Speed - 10G, 5/2.5G, 1G

MACsec Technology Overview

SECURITY

- Secure LAN/WAN and encrypt data for L2 and above
- Services: Integrity, Confidentiality, Replay Protection
- Key features:
  - GCM-AES-128/256 and GCM-AES-XPN-128/256 Cipher
  - Clear 802.1Q tag
  - Confidentiality Offset 0/30/50
- Key provision modes
  - Pre-shared Keys (PSK) - Static CAK mode
  - Master Session Key (802.1X/EAP) – Dynamic CAK mode
  - Static SAK mode
- MACsec Key Agreement (MKA) protocol for



Why MACsec is now mission-critical?

SECURITY

- Cloud and data center drives higher Ethernet link speed with increased bandwidth demand
- Bandwidth application requirements outpacing IP encryption capabilities

- MACsec secure data in motion without performance penalty
  - Suitable for both LAN and WAN
  - Line rate encryption throughput for high-speed Ethernet
  - Secure Layer 2 and above, transparent to higher layer applications
  - Strong encryption protection and lower overhead

Encryption at Different Layer

SECURITY

- Enterprise IT infrastructure and mission-critical apps moving to Cloud
- Cloud Services MUST provide very high security
- Every part of a network is vulnerable and requires protection
- Encryption at different layers provides comprehensive protection

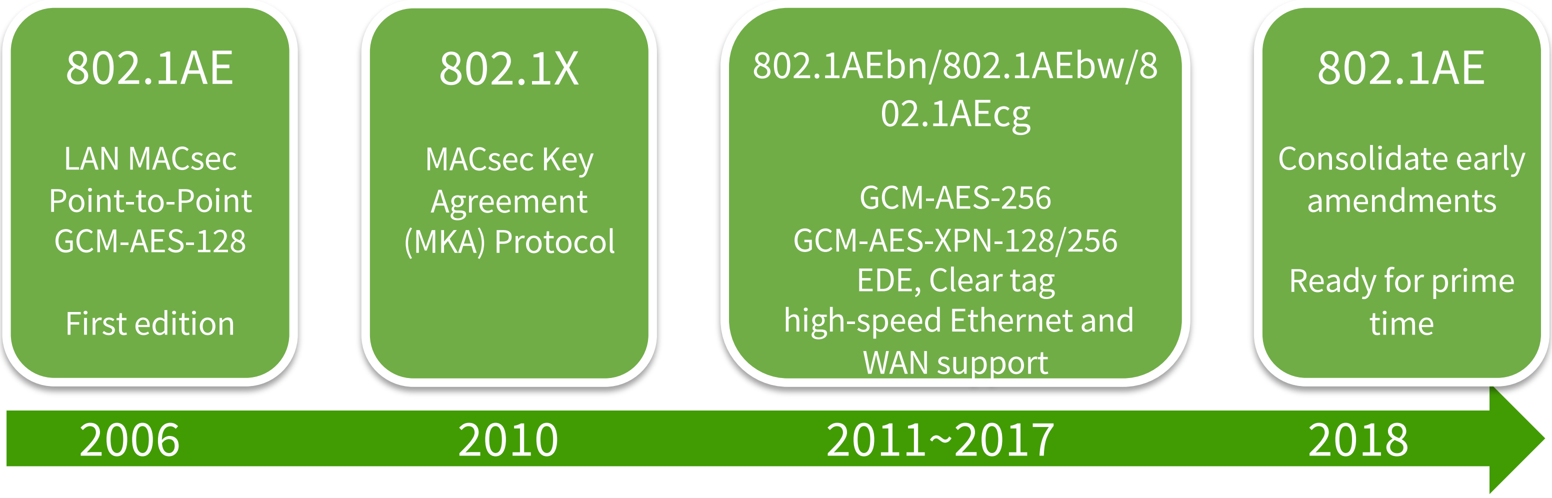
Application Layer Encryption	IPSec L3 Encryption	MACsec L2 Encryption	L1 Encryption
• End-to-end encryption • Operationally complex • High latency and overhead • bandwidth inefficient	• IETF standards-based • Support IP only • High latency and overhead • bandwidth inefficient	• IETF standards-based • High efficiency and low latency • Requested by hyperscalers	• 100% throughput • High efficiency • Protocol agnostic

Best fit for securing network infrastructure

MACsec Technology Evolution

SECURITY

- Standards:
  - IEEE 802.1AE-2018 - Media Access Control (MAC) Security
  - IEEE 802.1X-2020. Port-Based Network Access Control



802.1AE

LAN MACsec Point-to-Point GCM-AES-128

First edition

2006

802.1X

MACsec Key Agreement (MKA) Protocol

2010

802.1AEbn/802.1AEbw/802.1AEcg

GCM-AES-256
GCM-AES-XPN-128/256
EDE, Clear tag
high-speed Ethernet and WAN support

2011~2017

802.1AE

Consolidate early amendments

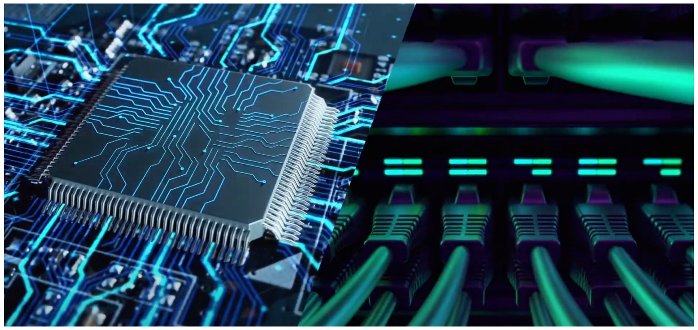
Ready for prime time

2018

The State of the Industry

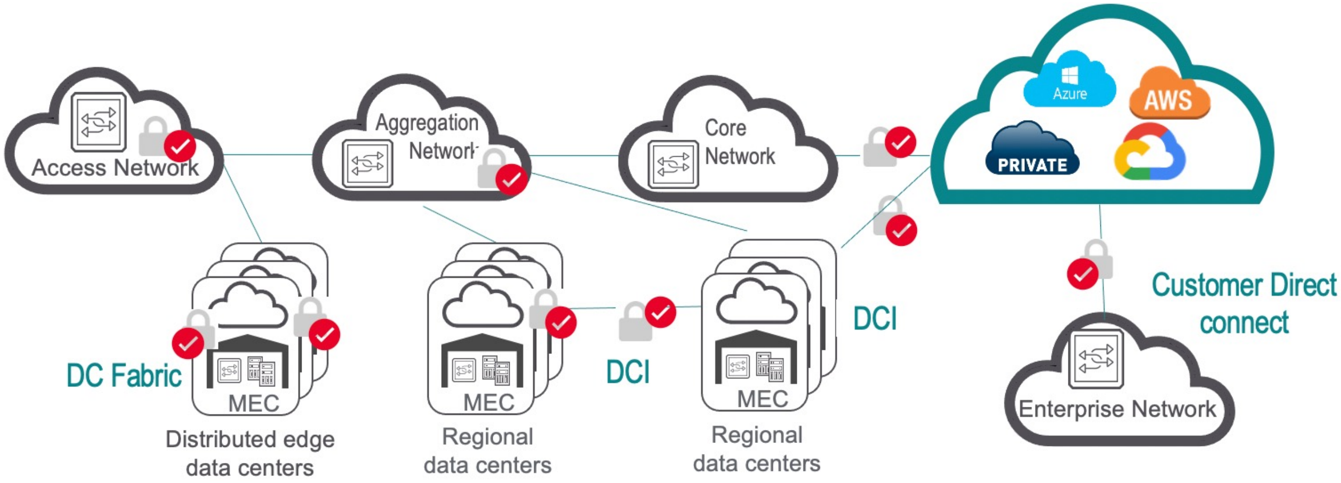
SECURITY

- MACSEC is now built into the silicon (PHY + FABRIC)
- MACsec is now shipped with next-generation routers and switches
- OCP whitebox switch with MACsec support is emerging
- Linux add MACsec support back in 2016
- SONiC SAI WG created API extension to cover MACsec and external Phys



Key Use Cases for Hyperscalers

SECURITY



Data Center Interconnect

- Secure any link outside of physical control
- No performance penalty
- Protect against outage and incident

Direct Customer Connect

- Provided by all major hyperscalers
- Extends customer on-premises network into Cloud
- From 10 Gbps to 100 Gbps circuit sizes
- Enterprise-grade SLA

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Challenges of Realizing the Promises of MACsec

SECURITY

- Achieve line rate throughput at high-Ethernet speed
- Support smaller to Jumbo frame size without loss and impact on throughput
- Minimize the latency impact with encryption
- Multiplex services over a physical link
- Ensure service continuity during key rotation
- Optimize control and data plane interaction
- Guarantee robustness under various network conditions

Early MACsec Testing Uncovers Critical Issues

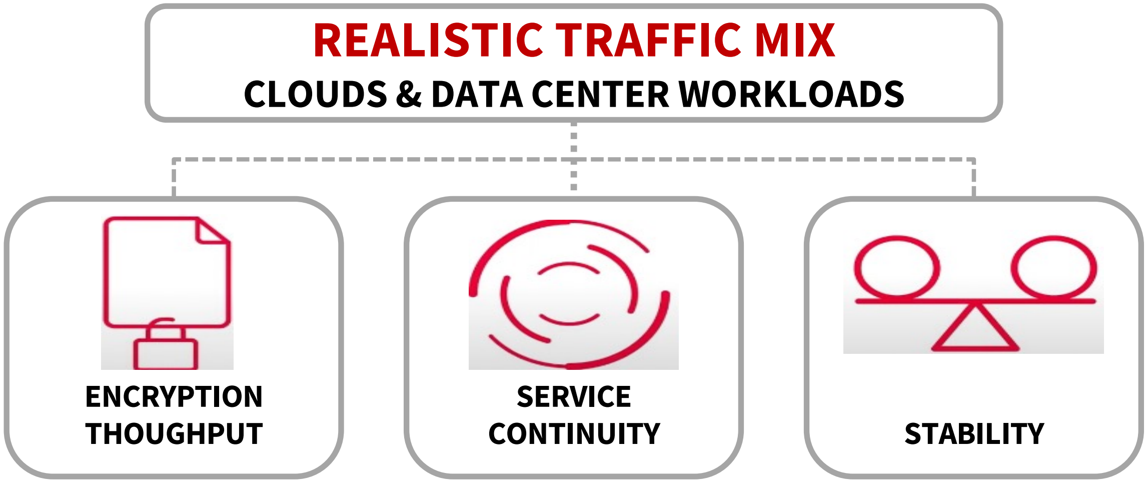
SECURITY

- Broken MACsec Key Agreement (MKA) Control Plane
  - MKA failure with XPN cipher, such as session failure, wrong SSCI, etc.
  - MKPDU failure with Clear Text VLAN
  - Stops sending MKPDU under stress (100G line rate traffic with frames < 128 bytes
- Data Plane Forwarding issue
  - Padding 64 bytes frame to 96 bytes causing packet drop
  - Failure under traffic with different frame sizes, eg. IMIX traffic, cause loss and CRC error
  - Failure understand stress, like mismatch SCI, sending to a port in different CA – Serious security concern
- Issue during key rotation
  - Wrong key server ID cause delayed switchover to the new key and a short period of loss
  - Wrongly sending unencrypted traffic during rekey
  - Failure of detecting PN exhaustion by Key server due to wrong LLPN and cause loss

Testing Must Evolve to Ensure Proper Validation

SECURITY

- No effective test tool in the market for high-speed Ethernet
- Most vendors and end customers test B2B between vendor devices
- Back-to-back test fall short and compromise quality
- Testing must evolve to deploy MACsec with confidence



REALISTIC TRAFFIC MIX

CLOUDS & DATA CENTER WORKLOADS

ENCRYPTION THOUGHPUT

SERVICE CONTINUITY

STABILITY

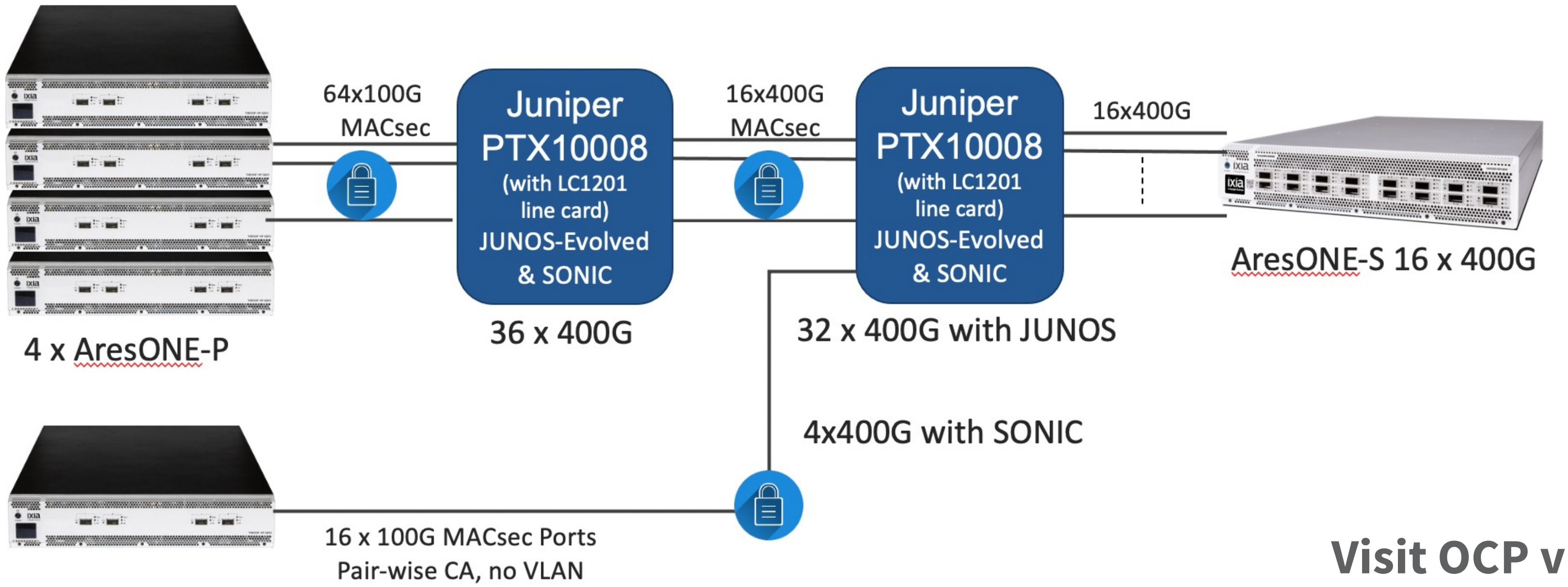
OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT

NOVEMBER 9-10, 2021

Demo MACsec Readiness for 100/400GE

SECURITY



Visit OCP virtual expo

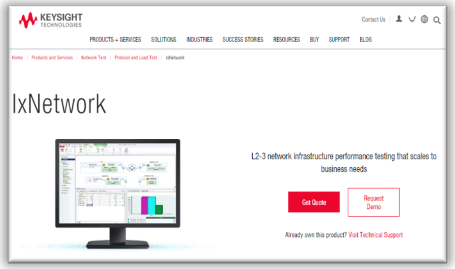
- Keysight/Juniper Joint MACsec Demo
- Demonstrate MACsec readiness with SONiC and JUNOS

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Available Resources

IxNetwork MACsec Intro Video



IxNetwork

L2-3 network infrastructure performance testing that scales to business needs

Already own this product? Visit Technical Support

IxNetwork Product page

DATA SHEET

IxNetwork MACsec Test Solution

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

Data Security with MACsec

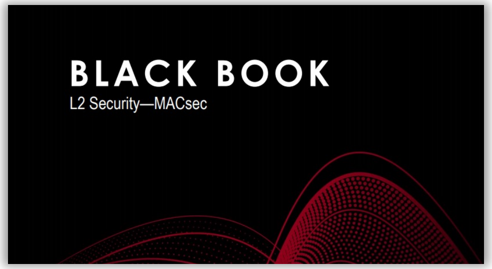
With increasing demand of data privacy and protection of critical business assets, security has become an important part of every network, including cloud, data center, 5G, and automotive.

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.

Highlights

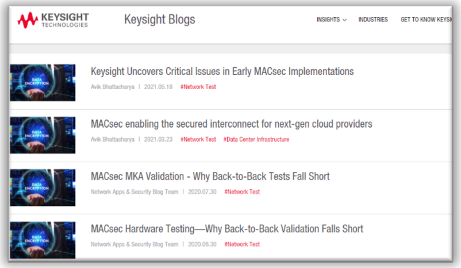
- Line-rate 100G MACsec traffic encryption and decryption to stress decryption engine
- Dynamic MKA key negotiation or static SAK provision

MACsec Data Sheet


BLACK BOOK

L2 Security—MACsec

MACsec Black Book



Keysight Uncovers Critical Issues in Early MACsec Implementations
Avik Bhattacharya | 2021.05.18 #Network Test

MACsec enabling the secured interconnect for next-gen cloud providers
Avik Bhattacharya | 2021.03.23 #Network Test #Data Center Infrastructure

MACsec MKA Validation - Why Back-to-Back Tests Fall Short
Network Apps & Security Blog Team | 2020.07.30 #Network Test

MACsec Hardware Testing—Why Back-to-Back Validation Falls Short
Network Apps & Security Blog Team | 2020.06.30 #Network Test

MACsec Blogs

Thank you!

OCP
GLOBAL
SUMMIT

NOVEMBER 9-10, 2021