Lantech™
Pioneering Industrial and IP Networks

White Paper

MACsec

Introduction and Benefits

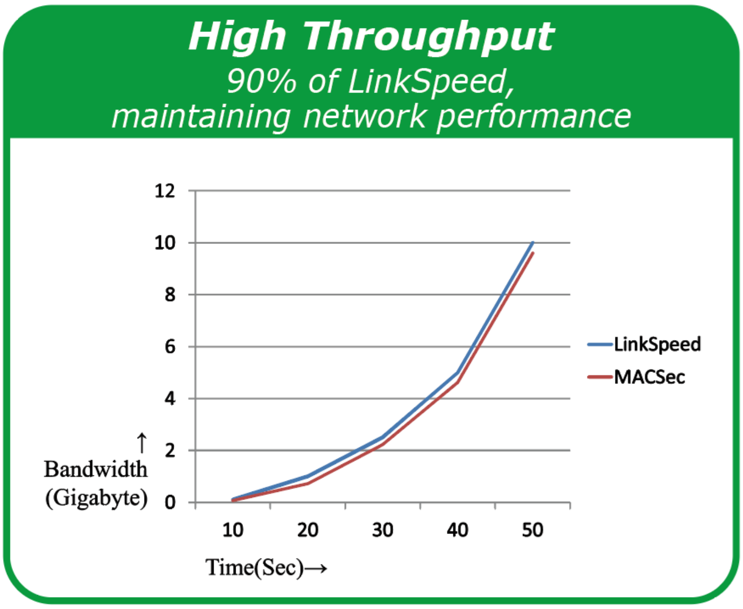
Version1.2
Nov 12, 2024

Introduction

The current landscape of cryptographic network protocols is rather narrow. By default, TCP/IP doesn't offer any security guarantee. Internet Protocol Security (IPsec) is a most used secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two hosts ove., but most other protocols in use today are proprietary.

IPsec functions at Layer 3, providing security by using end-to-end tunnels. These are encrypted only at the ends of each tunnel. A major drawback to IPsec is its complexity. Not only does it typically entail a dedicated encryption engine, but IPsec significantly enlarges the size of the Ethernet header. This compounds network inefficiencies and adds to overall solution cost.

In contrast, MACsec is a relatively simple protocol, which only minimally expands the header. Because MACsec is usually PHY port-based, it supports easy upgrades and high-speed connectivity up to 100G at low power and low cost. Unlike IPsec, it's possible to implement MACsec as a simple line-card upgrade and without a dedicated security processor.



High Throughput

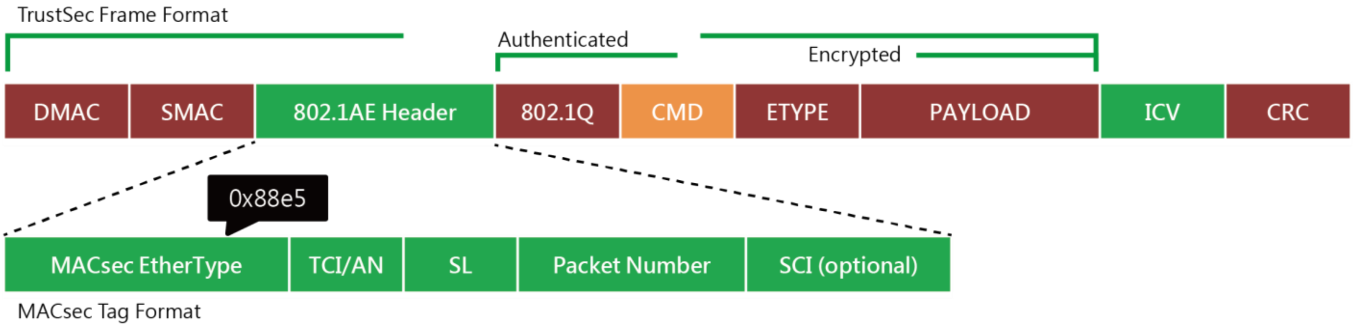
90% of LinkSpeed,
maintaining network performance

How MACsec works?

When MACsec is enabled on a point-to-point Ethernet link, the link is secured after matching security keys are exchanged and verified between the interfaces at each end of the link. The key can be configured manually, or can be generated dynamically, depending on the security mode used to enable MACsec.

MACsec uses a combination of data integrity checks and encryption to secure traffic traversing the link:

Data integrity—MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured link. The header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. If the data integrity check detects anything irregular about the traffic, the traffic is dropped.



Encryption—Encryption ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable. You can enable MACsec to ensure the data integrity checks are performed while still sending unencrypted data "in the clear" over the MACsec-secured link, if desired.

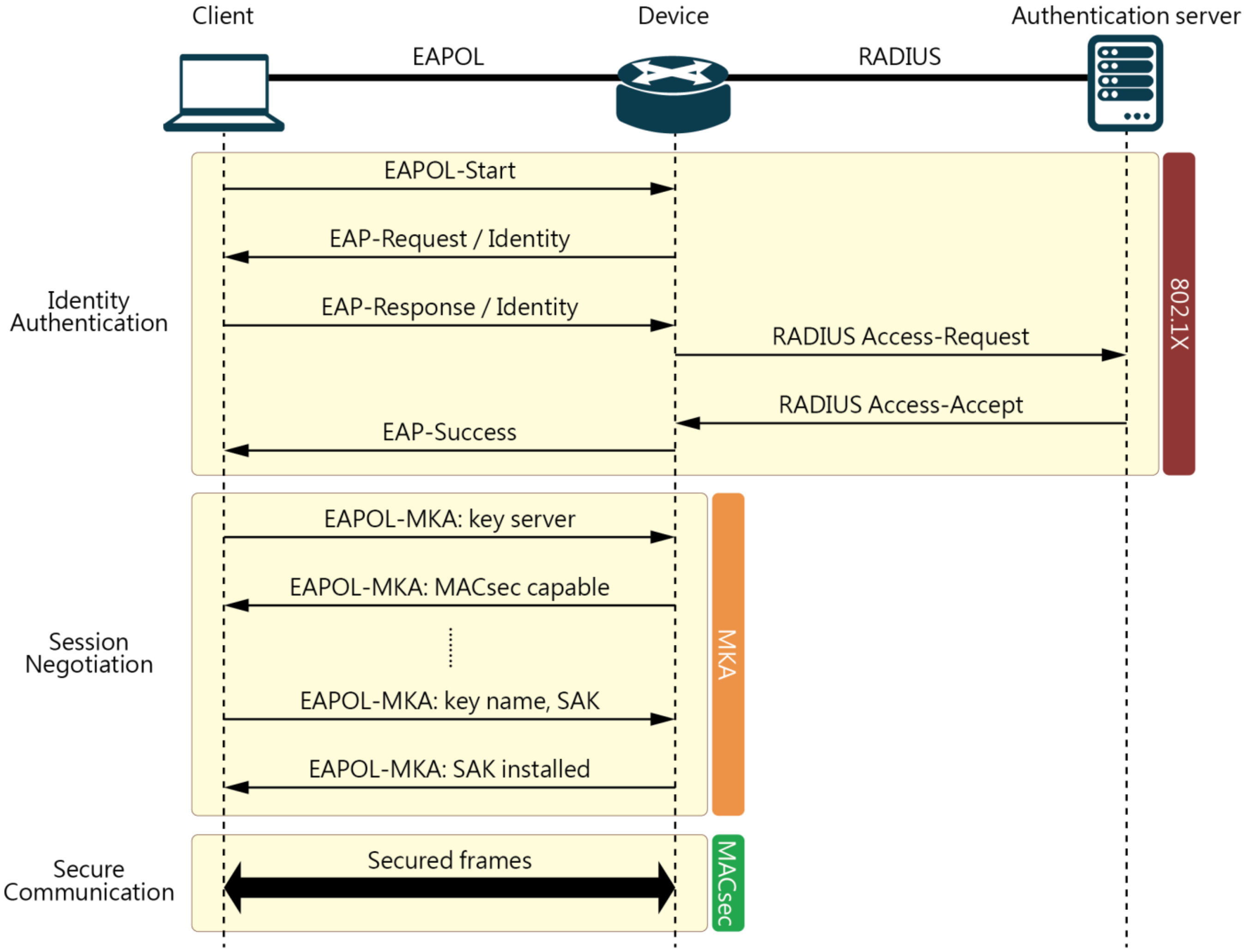
MACsec key agreement

MACsec Key Agreement (MKA) protocol installed on a device relies on an IEEE 802.1X Extensible Authentication Protocol (EAP) framework to establish communication.

MACsec peers on the same LAN belong to a unique connectivity association. Members of the same connectivity association identify themselves with a shared Connectivity Association Key (CAK) and Connectivity Association Key Name (CKN). The CAK is a static key that is preconfigured on each MACsec-enabled interface. MACsec authentication is based on mutual possession and acknowledgment of the preconfigured CAK and Connectivity Association Key Name (CKN).

Each peer device establishes a single unidirectional secure channel for transmitting MACsec frames (Ethernet frames with MACsec headers that usually carry encrypted data) to its peers within the connectivity association. A connectivity association consists of two secure channels, one for inbound traffic, and one for outbound traffic. All peers within the connectivity association use the same cipher suite, either Galois/Counter Mode Advanced Encryption Standard 128 or 256 (GCM-AES-128 or GCM-AES-256), for MACsec-authenticated security functions.

MACsec Key Agreement (MKA) protocol uses the Connectivity Association Key to derive transient session keys called Secure Association Keys (SAKs). SAKs and other MKA parameters are required to sustain communication over the secure channel and to perform encryption and other MACsec security functions. SAKs, along with other essential control information, are distributed in MKA protocol control packets, also referred to as MKPDUs.



Benefit of MACsec

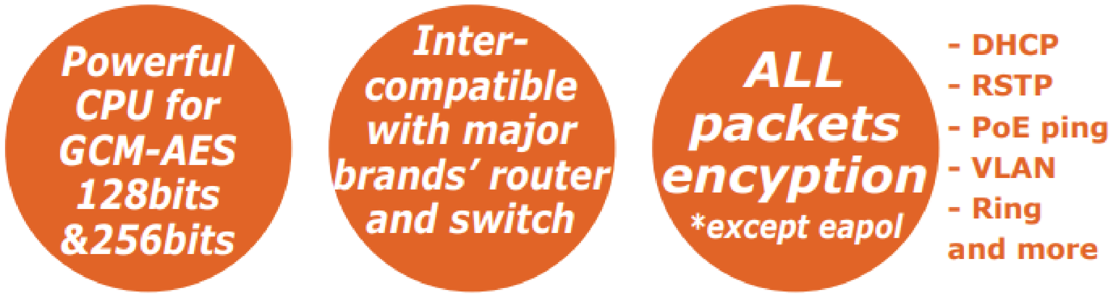
- **Point-to-Point Security:** Protects Ethernet links from threats such as Denial of Service, intrusion, and wiretapping.
- **High Performance:** Encryption and decryption are handled by hardware, maintaining network performance.
- **Vendor Interoperability:** Works across different vendor devices, enhancing network flexibility.

MACsec is an IEEE-standard security technology that provides secure communication for all traffic on Ethernet links. Users can use the devices with MACsec from different vendors to extend current application. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks.

The AES-256 encryption makes packets unable to be tampered with, even the packets are captured by hacker. Encryption and decryption are processed by hardware. Therefore, the hop-to-hop architecture reduces the loading of network switch, so the network system can work with the same performance as usual.

The format of MACsec frames is the same as standard Ethernet, so even network devices without MACsec receives a MACsec packet, and can forward the packet to the destination MAC address.

Advantages of Lantech’s MACsec Solution (OS5)



Powerful CPU for GCM-AES 128bits &256bits

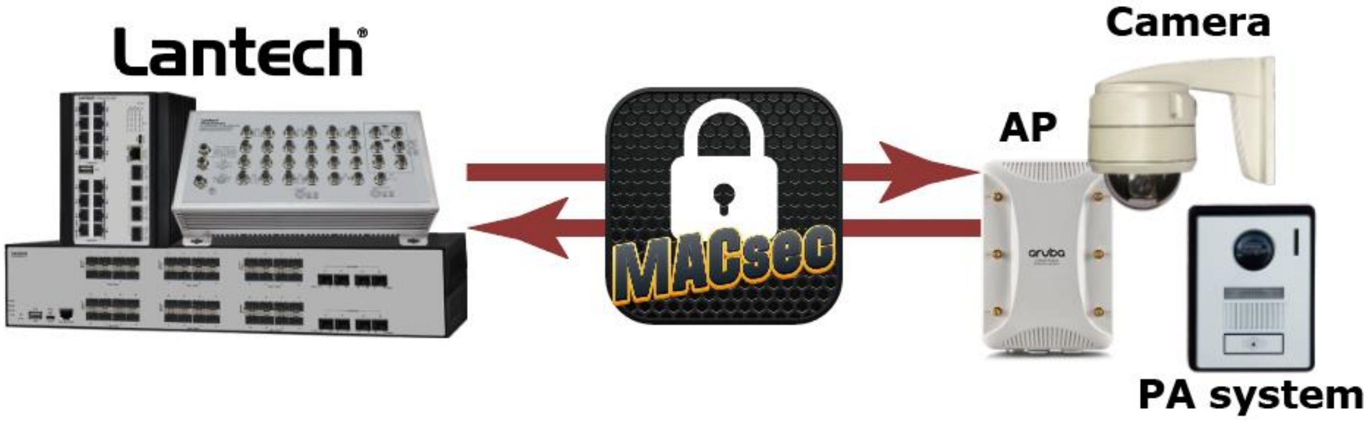
Inter-compatible with major brands’ router and switch

ALL packets encyption *except eapol

- DHCP
- RSTP
- PoE ping
- VLAN
- Ring

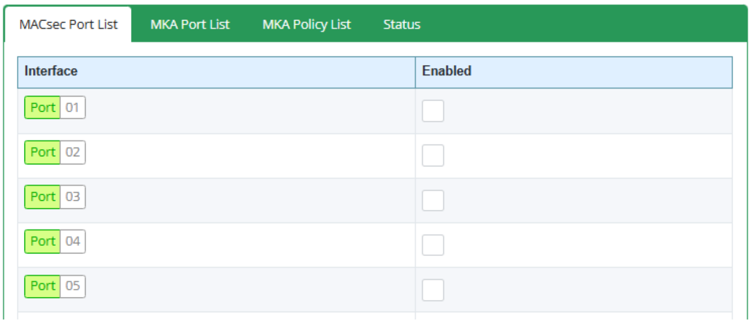
and more

“Secure the integrity of data that transferred between Lantech switches and MACsec-enabled devices”



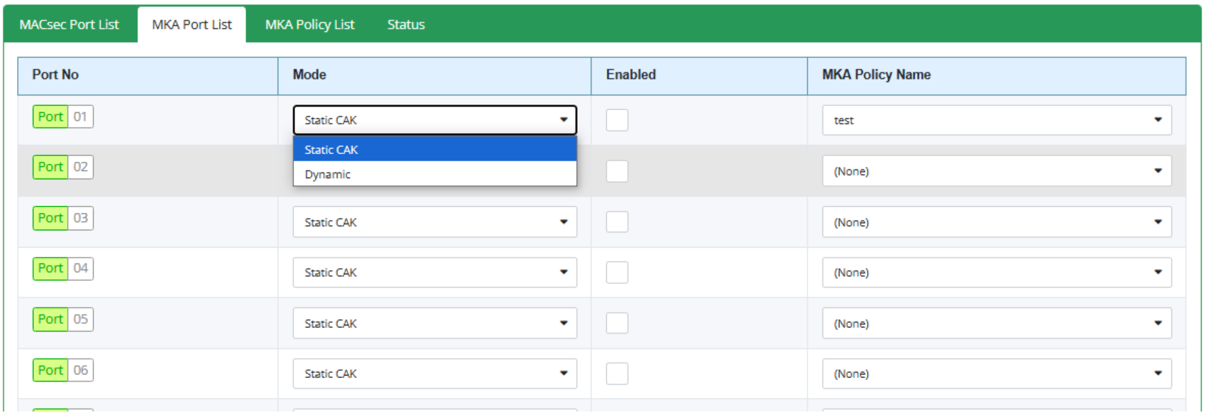
Screenshots of Lantech's MACsec Solution (OS5)

MACsec Port List



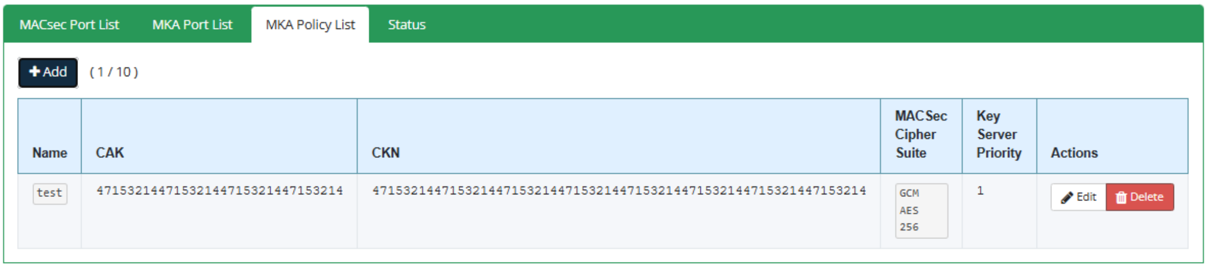
Interface	Enabled
Port 01	□
Port 02	□
Port 03	□
Port 04	□
Port 05	□

MKA Port List



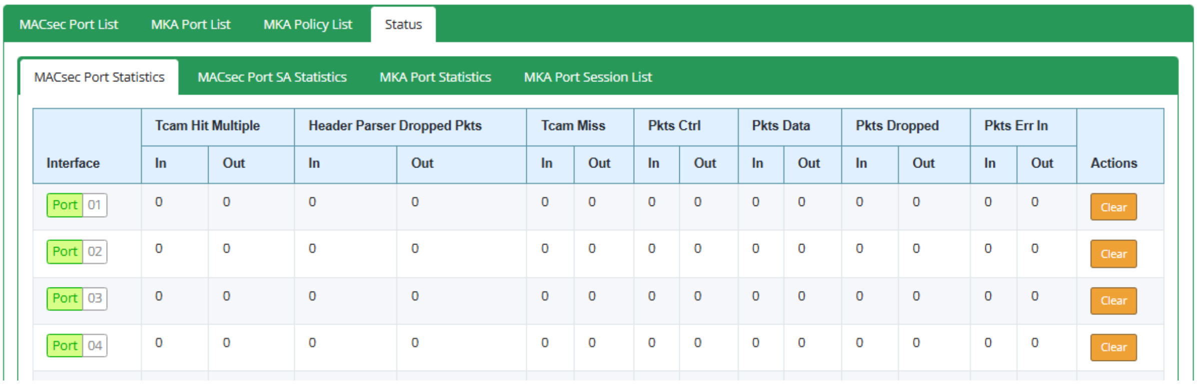
Port No	Mode	Enabled	MKA Policy Name
Port 01	Static CAK	□	test
Port 02		□	(None)
Port 03	Static CAK	□	(None)
Port 04	Static CAK	□	(None)
Port 05	Static CAK	□	(None)
Port 06	Static CAK	□	(None)

MKA Policy List



Name	CAK	CKN	MACSec Cipher Suite	Key Server Priority	Actions
test	47153214471532144715321447153214	4715321447153214471532144715321447153214471532144715321447153214	GCM AES 256	1	Edit Delete

Status



Interface	Tcam Hit Multiple		Header Parser Dropped Pkts		Tcam Miss		Pkts Ctrl		Pkts Data		Pkts Dropped		Pkts Err In		Actions
	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	In	Out	
Port 01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
Port 02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
Port 03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear
Port 04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear

About Lantech

Lantech Communications Global, Inc. is an IRIS & ITxPT certified manufacturer of Ethernet products focused on the transportation markets, bus, train, trackside, ITS, smart city and many more applications. Our range of onboard EN50155 & E-Marked Ethernet switches & wireless/ LTE routers offer cutting edge design and functionality. We continue to work with our key customers in creating further enhancements & developments in on board passenger information, video security, trackside data communications by providing rugged 10GbE, PoE managed Ethernet switches, LTE/Wi-Fi routers in line with ITxPT and E-Marked certifications for various applications and critical solutions.