MACSec

A Security Solution that Protects LANs from Internal Threats

P/N 915-0910-01 Rev A July, 2008

Contents

Using MACSec to Guard Against Behind-the-Firewall Attacks and Complement External Security

Until recently, most network security concerns focused on external threats. Solutions such as IPSec and TLS (SSL), which provide protection against most external threats and intrusions, are typically placed between gateways (for IPSEC) and between hosts and servers (for TLS and SSL) in an end-to-end client-server topology. However, this topology limits the deployment of in-line security servers that enable IT departments to inspect traffic with such tools as intrusion detection systems. Security systems that encrypt traffic also inhibit the ability to perform load balancing and traffic management. As a result, IT departments usually terminate end-to-end secure connections at gateways and firewalls and allows LAN data to travel "in the clear," without encryption. This is an inherently risky technique, since it does not secure a LAN from internal threats such as man–in-the-middle, masquerading, passive wiretapping, playback, and other denial of service (DoS) attacks.

Standardized in 2006, media access control security (MACSec – IEEE802.1AE) specifies how encryption may be used to secure links behind external firewalls. MACSec provides source authentication, data integrity check, and encryption on each hop to help secure the network from the inside. Devices at each hop can be used as IT insertion points since the traffic within those devices is not encrypted. As a result, IT and security devices can now monitor and inspect internal LAN traffic.

In addition, Ethernet-based WAN networks such as EPONs (Ethernet Packet Optical Network) can use MACSec to provide link security over short-, medium-, and long-haul connections. Since MACSec is transparent to layer 3 and higher layer protocols, and is not limited to IP traffic only, it may be more applicable than IPSec. MACSec works with any type of traffic carried over Ethernet links.

MACSec provides secure, encrypted communication at layer 2 that is capable of identifying and preventing threats from denial of service and intrusion attacks, as well as man-in-the-middle, masquerading, passive wiretapping, and playback attacks launched from behind the firewall. MACSec provides point-to-point integrity, which complements existing end-to-end security solutions such as IPSec. It also provides security for situations where many protocols such as spanning tree, link aggregation, DHCP and ARP are not securable via layer 3.

MACSec Overview

MACSec (IEEE802.1ae), along with KeySec (IEEE802.1af) define LinkSec as the layer 2 link security standard as shown in Figure 1. MACSec defines the layer 2 security protocols that provide origin authentication, data integrity checking, and data confidentiality. It defines a frame format that includes data encapsulation, encryption, and authentication. KeySec defines the key management protocol for MACSec. MACSec supports point-to-point connections in a hop-by-hop architecture. There are certain advantages to this architecture, including:

- Low processing overhead for the receiver, since only a single far-end connection and its keys need to be managed.
- IT insertion points for IDS, anti-virus protection, load balancing and traffic management are easier to deploy since encryption/decryption is local.

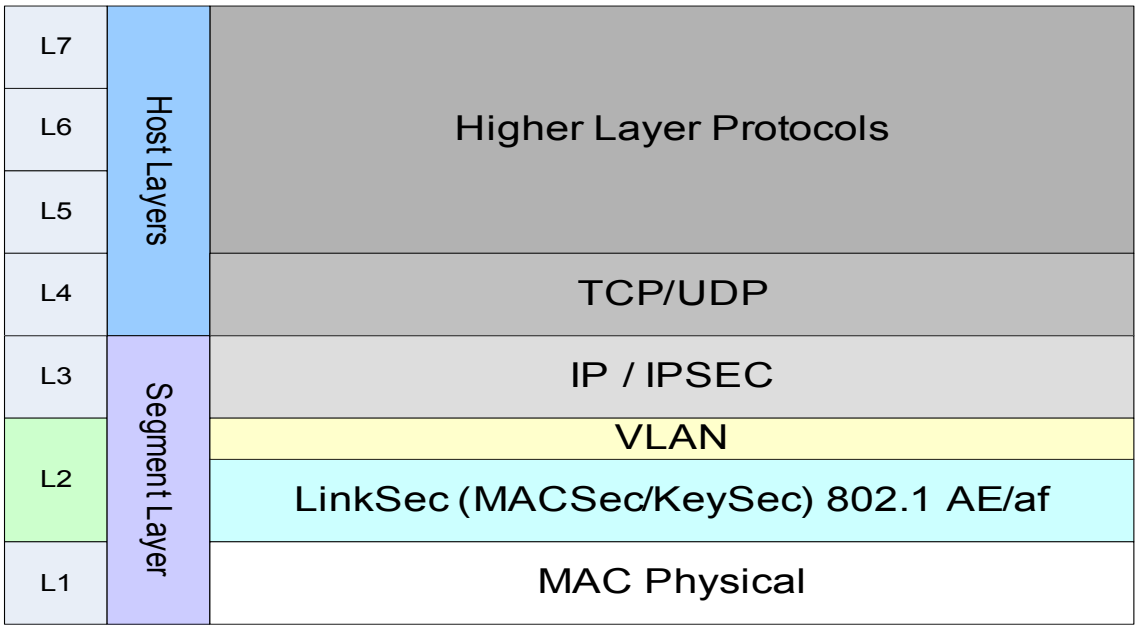

Figure 1. LinkSec's Position in the Network Stack

How MACSec Works

HOW IT WORKS: 802.1AE

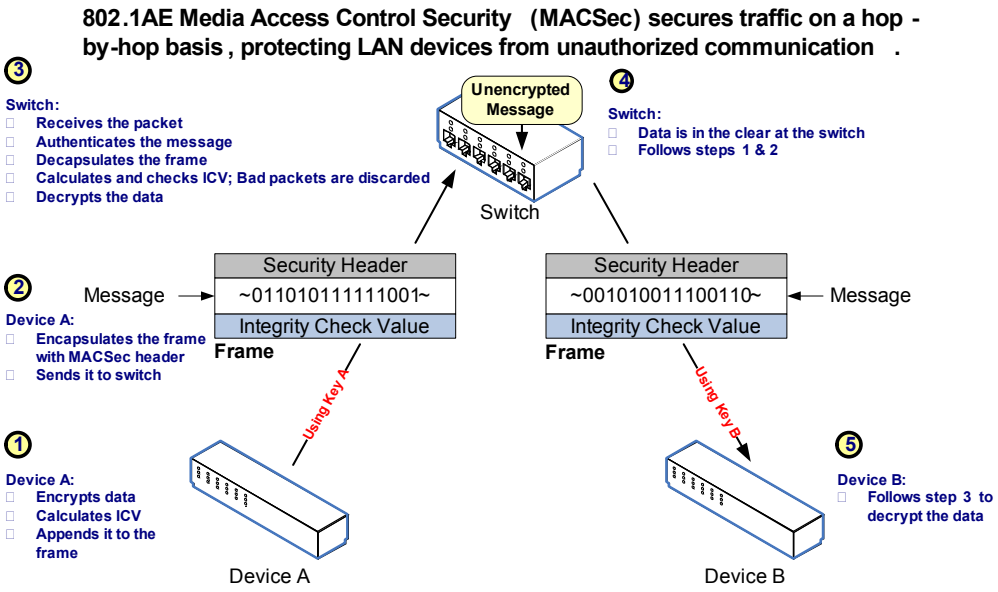

Figure 2. A Simple Example of MACSec Operation, courtesy NetworkWorld

A simple example of MACSec operation is illustrated in Figure 2. There are two secure connections, one between device A and a switch, and the other between device B and a switch.

In Figure 3, there are four devices attached to a LAN. Connectivity between the devices is insecure.

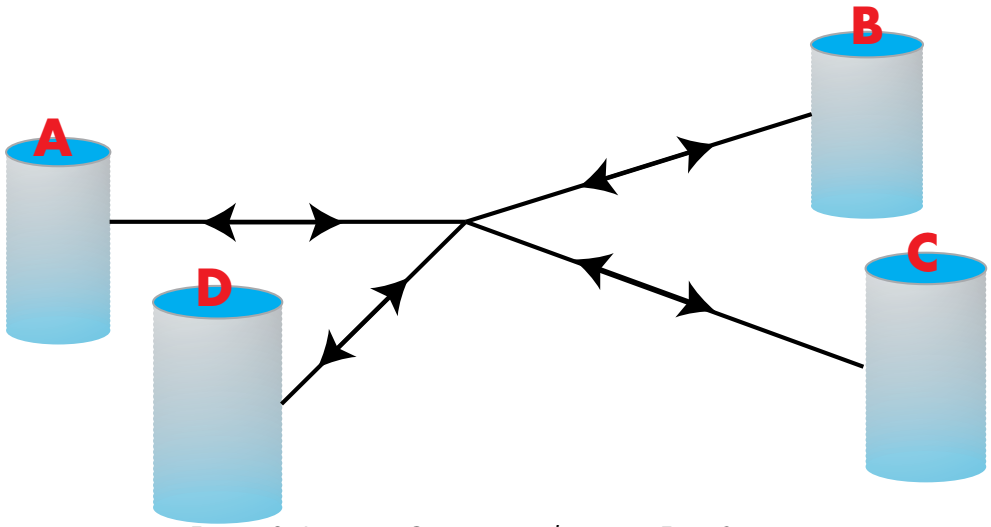

Figure 3. Insecure Connectivity between Four Stations

In Figure 4, devices A, B, and C have been included in a connectivity association (CAABC). KeySec creates the CA using MACSec key agreement entity (Kay) of each member device. MACSec provides the secure entity (SecY) for each member device (A, B, and C). In this example, only devices A, B, and C are members of CA and can securely communicate with each other. Device D can still communicate with devices A, B, and C in an insecure fashion.

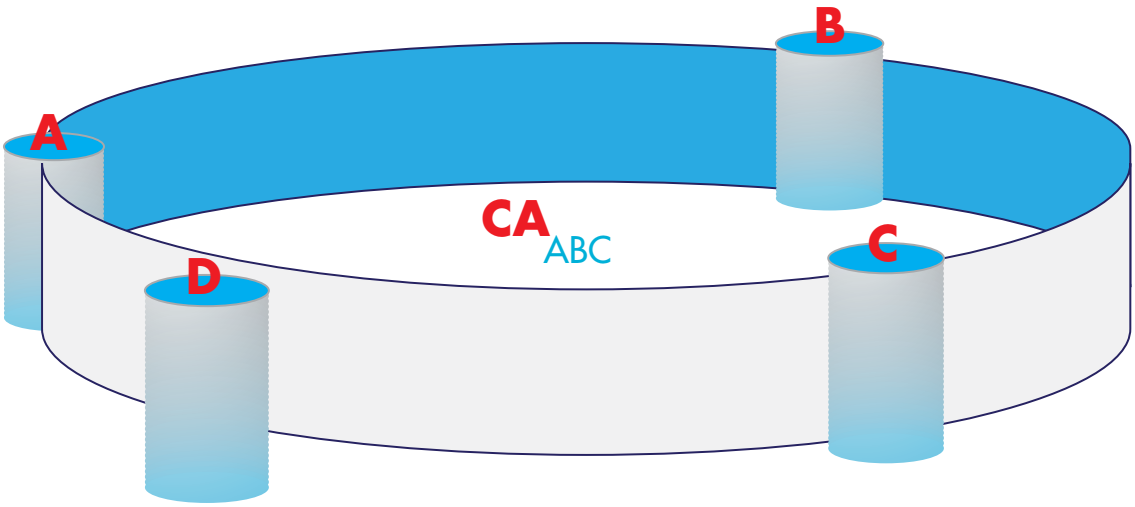

Figure 4. Secure Connection between Devices A, B, and C

KeySec defines a secure channel (SC) between the SecY of each CA member device. Each SC is unidirectional; for full bidirectional, secure communication between two devices, two SCs must be defined, as shown in Figure 5. Each SC has secure association keys (SAKs) negotiated by KeySec. SCs use the SAKs for authentication and encryption. MACSec defines the frame format for data encapsulation, encryption and authentication.

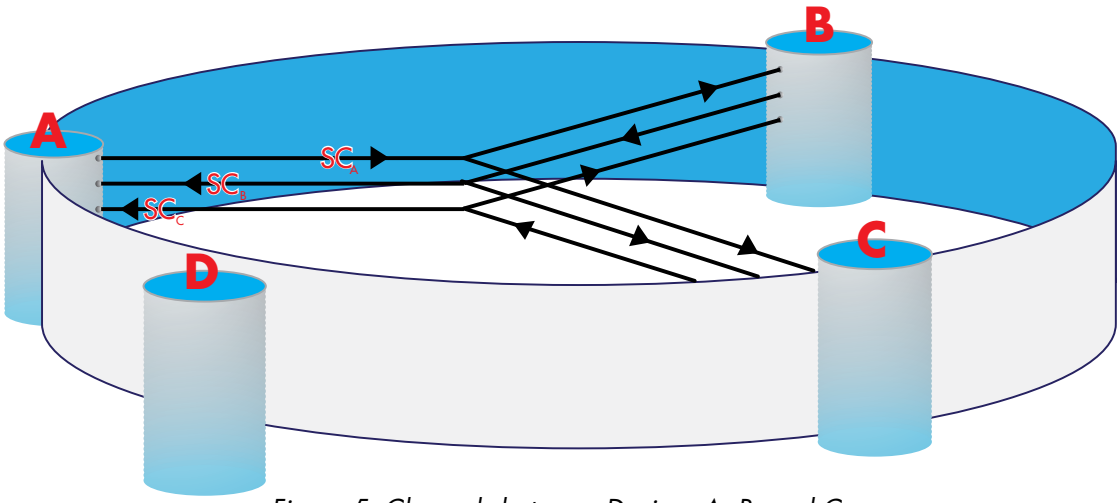

Figure 5. Channels between Devices A, B, and C.

The MACSec Protocol

MACSec defines the frame format for data encapsulation, encryption, and authentication. The format of the packet is defined below and shown in Figure 6.

MACSec frame format

- Ethernet header
  - DA, SA
- SecTAG
  - MACSec EtherType (0x88E5)
  - TAG control information (TCI)
  - Association number (AN) within the channel
  - Short length (SL)
  - Packet number (PN)
  - Optionally encoded secure channel identifier
- Data
  - Encrypted or raw format
    - Default cipher suite is GCM-AES-128
  - Destination address, source address, and SecTAG fields are not encrypted
- Integrity check value (ICV)
  - ICV calculated with destination address, source address, SecTAG, and user data (after encryption, if applicable)
- CRC

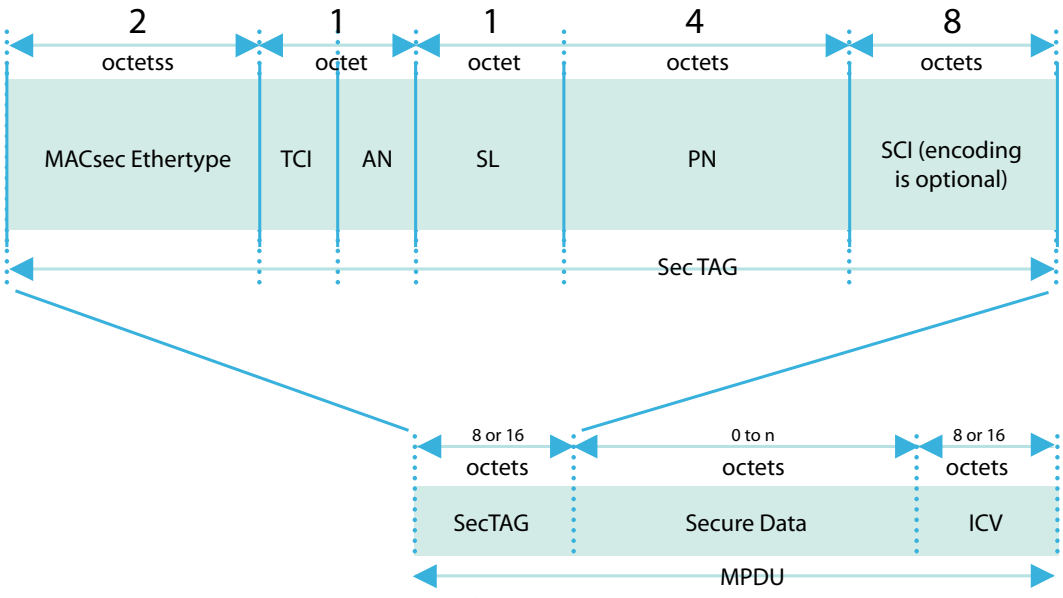

Figure 6. MACSec Frame Format

The MAC security tag (SecTAG) follows the MAC DA/SA, followed by secure data, ICV, and CRC. Figure 7 shows the composition of the secure channel identifier (SCI) and secure association identifier (SAI). A secure channel identifier is made up of a MAC SA and a port ID (PI). A secure association identifier (SAI) is made up of the SCI and the association number (AN). The association number identifies which of four possible keys the SC is using.

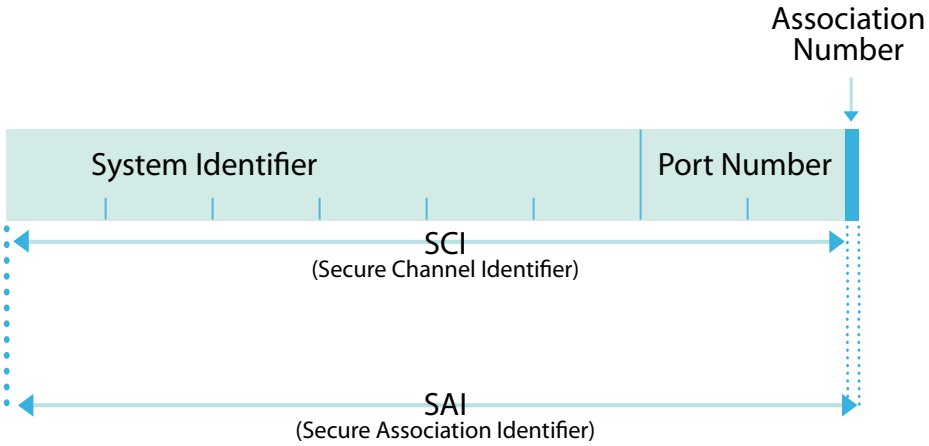

Figure 7. Secure Channel Identifier

Conclusion

MACSec helps secure the network from the inside by securing data exchange on a hop-by-hop basis. It also allows each hop to act as an IT insertion point for security purposes. This enables IT departments, through their security devices, to monitor and inspect internal "in the clear" LAN traffic. MACSec provides secure and encrypted communication at layer 2 that is capable of identifying and preventing most intrusion threats launched from behind the firewall. It provides point-to-point integrity and complements existing end-to-end security solutions such as IPSec and TLS (SSL) to prevent both external and internal network attacks. MACSec also provides transparent link layer security for Ethernet-based WAN networks such as EPONs (Ethernet Packet Optical Network) where any type of traffic, including IP, can be carried over the Ethernet link whereas IPSec will allow IP traffic only.

Ixia Worldwide Headquarters

26601 Agoura Rd.
Calabasas, CA 91302
(Toll Free North America)
1.877.367.4942
(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Other Ixia Contacts

Info: info@ixiacom.com
Investors: ir@ixiacom.com
Public Relations: pr@ixiacom.com
Renewals: renewals@ixiacom.com
Sales: sales@ixiacom.com
Support: support@ixiacom.com
Training: training@ixiacom.com