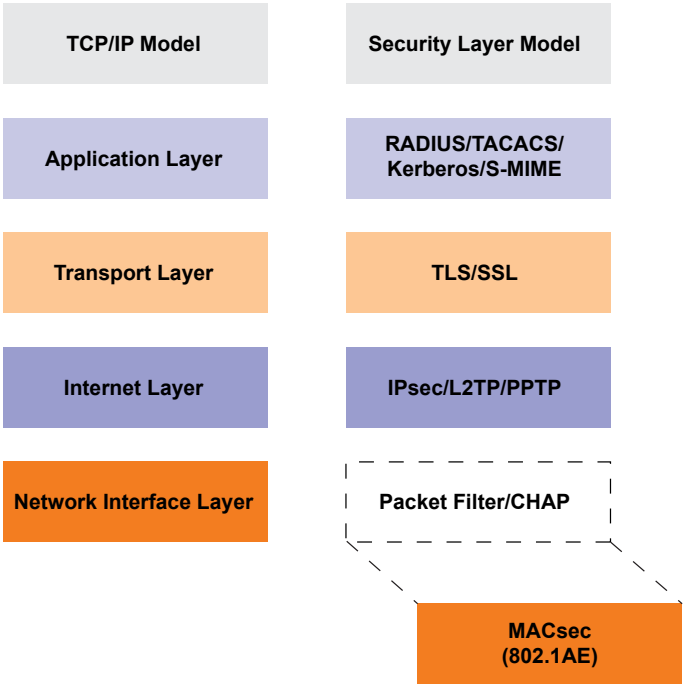
ipinfusion™

# Technical Brief
## MACsec

### Securing Data Link layer with MACsec

The OSI model defines that each layer can only communicate with the layer above and the layer below, hence each layer must implement security independent of other layers. Compromised security at any layer puts all of the layers above it at risk. For example, the network layer will be ignorant of an attack if the data link layer is compromised. It is necessary to deploy security mechanism at each OSI layer to achieve complete network security.

The picture below shows some of the security mechanisms used at each network layer, including MACsec at the Data link layer.




The data link layer differs from other protocol layers because it is often lumped in with the physical layer and often neglected from a security perspective. Access to other layers above the data link layer can be controlled using filtering, access control lists, authentication, and application controls. However, the data link was designed primarily to transport data frames and not security so this layer lacks fine-grain controls to prevent attacks.

MAC security (802.1AE) (1) defines a security infrastructure to provide data confidentiality, data integrity and data origin authentication. By using these techniques, MAC sec can prevent attacks on Layer 2 protocols.

A few possible security attacks at Layer 2 are listed below.

#### *MAC flood / address table exhaustion attacks*

A switch forwards Ethernet frames based on MAC addresses. An address table (frequently implemented in a Content Addressable Memory or CAM) contains a list of MAC addresses and VLANs with their physical ports. Using this table, a switch delivers the frames to intended ports only. This offers considerable security over a simple hub. On any given switch, the address table size is limited. A successful attacker can fill the table with new MAC addresses which, in essence, convert the switch to a hub. Hence it starts flooding Ethernet frames to ensure successful delivery. Now an intruder can see the traffic flowing through the switch.

This attack can be mitigated using port security (authenticate the user using 802.1X[2]) and by limiting the number of MAC address that can be learned per port. Static MAC address entry can also be enforced but is not scalable.

#### *ARP Spoofing attacks*

The Address Resolution Protocol (ARP) translates an IP address to a MAC address. Upon receiving a gratuitous ARP message, an IP station updates its ARP table with a new IP address to MAC address mapping. An ARP attack occurs when an intruder broadcasts a gratuitous ARP for any of its neighbor's IP address with his own MAC address. All the stations in the local network will start delivering traffic to the intruder instead of the intended recipient. With this, the intruder successfully performs a Man-In-The-Middle attack. When the client under attack realizes it is not receiving any traffic, it offers a gratuitous ARP to the network. The intruder then triggers a counter gratuitous ARP. This tug-of-war consumes the network bandwidth resulting in Denial-Of-Service to the clients on network.

ARP attacks can be mitigated by employing Dynamic ARP Inspection, static entries in cache, port security, arpwatch, DHCP Snooping, and ArpON.

#### *DHCP Starvation attacks*

When a new client enters a network, it may contact a DHCP server for an IP address. The DHCP server will respond with an address and a lease period for that address. This handshake is usually not encrypted. An attacker can take advantage of this and flood the network with DHCP requests for address. This attack consumes all the leasable IP address served by DHCP server. In this condition, the DHCP server cannot offer addresses to any future clients that join the network. To make matters worse, an attacker can setup a rogue DHCP server and start responding to new DHCP requests. This allows the rogue DHCP server to assign IP addresses and open the possibility to Man-In-The-Middle monitoring of all traffic.

DHCP starvation attacks can be mitigated by limiting the number of MAC addresses on a switch port. DHCP Rogue attacks can be mitigated by using DHCP Snooping. DHCP snooping identifies the untrusted edge ports and blocks the sending of DHCP discover messages to those untrusted ports.

### *VLAN hopping attacks*

One way an attacker configures his workstation is to generate Dynamic Trunking Protocol (DTP) messages. The default configuration of a switch needs only one side of a connection to announce themselves as a trunk. The switch automatically trunks all available VLANs over the switch port which results in hearing all the traffic across all VLANS. A second way is an attacker can hop the VLANs by using double tagging. This works only when the attacker is connected to an interface which belongs to the native VLAN of the trunk port. An attacker changes the original frame by adding an outer tag, which is of his own VLAN and an inner hidden tag of victim's VLAN.

These attacks can be mitigated by disabling auto-trunking and not using VLAN 1 as the switch management VLAN.

### *STP attacks*

This attack involves an attacker spoofing the root bridge in the topology. The attacker attaches to a port on the switch either directly or via another switch. Injects BPDU frames whose bridge priority in BID are lower than the existing root bridge. As a result, the root bridge status is obtained for attackers connected port which helps to see various frames.

These attacks can be mitigated by disabling spanning tree functions on all user interfaces and enable root guard (or) BPDU guard on user ports.

### *Multicast Brute Force attack*

An attacker sends a large number of multicast frames to a known VLAN in a rapid succession to overload the switch. This causes the frames to broadcast into other VLANs instead of containing it on the original VLAN. This might cause a denial of service situation.

This attack can be mitigated by a well-equipped switch which can prevent the frames leaking into other VLANS.

The attacks summarized in this section establish the fact that existing mitigations are not efficient and shows that there is a need for a stronger Data Link Layer security mechanism to prevent these vulnerabilities. IEEE published a standard to address this requirement, known as IEEE 802.1AE, the MACsec protocol.

## MACsec Protocol (IEEE 802.1AE)

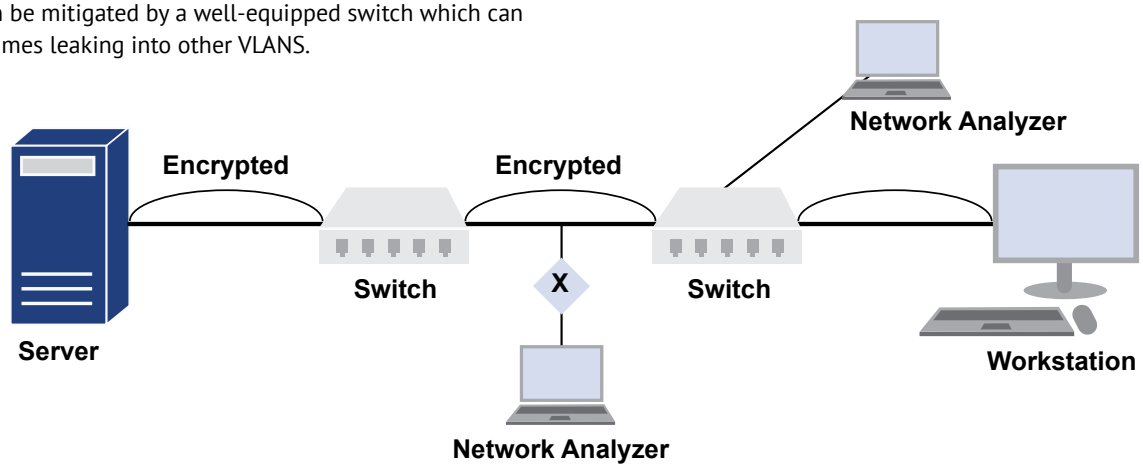
MACsec is an industry standard to provide secure communication for all traffic on Ethernet links. The services provided by MACsec are Confidentiality, Integrity, and Source Authentication. This is used to secure LANs from the attacks of passive wiretapping, impersonation, man-in-the-middle and replay attacks. MACsec allows for securing an Ethernet link including LLDP, LACP, DHCP, ARP, and other protocols frames that are not typically secured. This can be used in combination with IP Security (IPsec) and Secure Socket Layer (SSL) to provide end-to-end network security.

MACsec was primarily designed to be used in conjunction with IEEE802.1x-2010. IEEE 802.1AE can be treated as a data plane protocol and IEEE 802.1X-2010 (MKA) as a control plane protocol.

As shown in the above picture, IEEE 802.1AE encrypts frames between network devices (Hop-by-Hop). The frames are decrypted in the switches, processed and re-encrypted back to send to the next device. Network traffic can't be monitored on the wire (shown as X), however a network monitor attached to a switch span port can monitor traffic.

**MAC Security takes care of:**

- Nurtures correct network connectivity and services
- Confinement of denial of service attacks
- The construction of public networks, offering service to unrelated customers, using shared LAN infrastructures
- Secure communication between organizations
- Incremental and non-disruptive deployment



A combination of 802.1AE and 802.1X can handle numerous security requirements, such as:

- **Authentication, Authorization, and Accounting (AAA):** Achieved using 802.1X and a RADIUS authentication server
- **Data Integrity:** MACsec Integrity Check Value (ICV) safeguards against data tampering
- **Data Confidentiality:** MACsec AES encryption ensures that only intended device can read secure data

Key agreement protocols (802.1X) establish and maintain a secure Connectivity Association (CA). A secure CA is created for connectivity between stations. Each CA supports a unidirectional Secure Channel. Each instance of MACsec operates within a single CA. MACsec Key Agreement (MKA) takes responsibility for discovering, authenticating, and authorizing the potential participants in the CA. The MAC Security Entity (SecY) within each station transmits frames with secure MAC service request on a Secure Channel (SC). Each SC comprises a succession of Secure Associations (SAs), each with a different Secure Association Keys (SAKs). MKA also takes responsibility for creating and distributing SAKs to each of SecYs in a CA. MACsec provides a secure MAC service using cryptographic methods with in MKA security relationship.

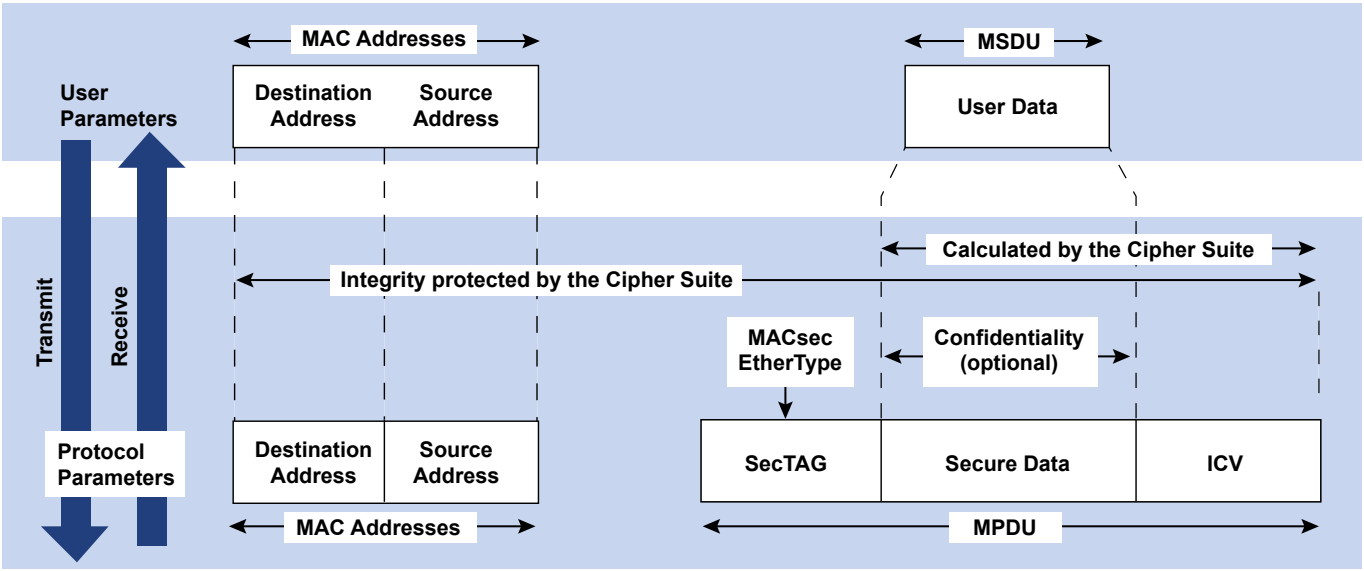
**MACsec incorporates**

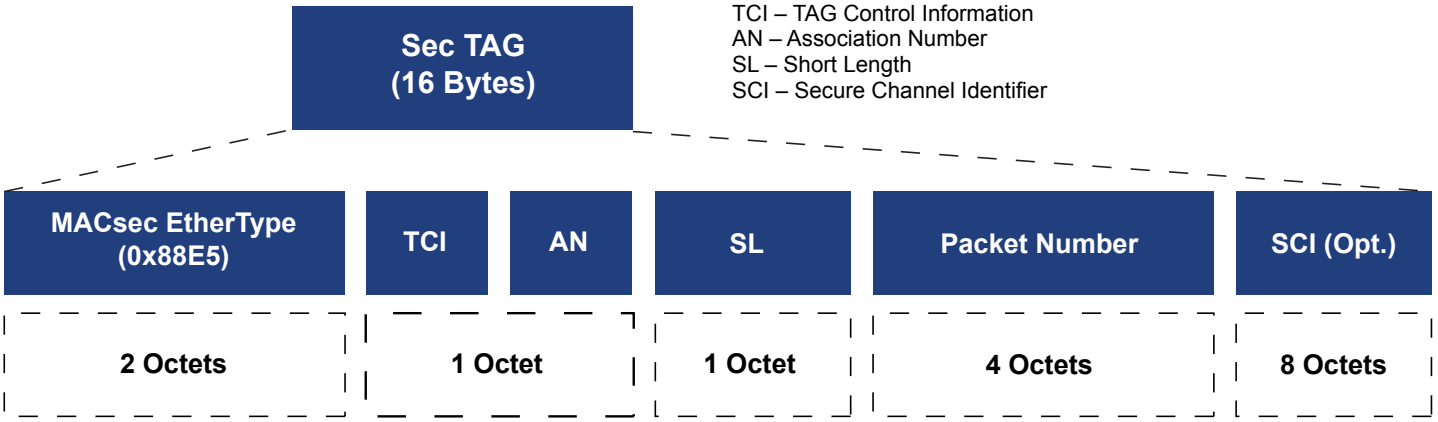
- Modifications to the MAC Service Data Unit (MSDU) conveyed by each frame transmitted by a user of the protocol
- MAC Security TAG (SecTAG) that conveys parameters that identify the protocol, identify the key to be used to validate the received frame, and provide replay protection
- Secure Data field that conveys the User Data, encrypted if confidentiality is provided
- Integrity Check Value (ICV) that ensures the integrity of the MAC Destination Address, MAC Source Address, SecTAG, and User Data

MACsec does not transmit additional frames, such as keep alive or key exchange. Upon transmission, each frame is assigned to an SA and identified by its Association Number (AN). The AN is used to identify the SAK and the next Packet Number (PN) and all of these are encoded into a SecTAG. Upon receipt of a MACsec frame, the AN, PN and Short Length (SL) field are extracted from the SecTAG and used to assign the frame to an SA to identify the SAK. Cipher Suite returns VALID upon successful integrity check of the frame and decoding of user data. Replay protection is applied for a valid received frame. MACsec Protocol Data Units (MPDUs) are exchanged between MAC Security Entities (SecYs).

### *MACsec Frame structure*

MACsec adds an additional 8 or 16 bytes (SCI is optional) of Security TAG and 8 to 16 bytes (depends on Cipher Suite) of ICV. MPDU structure is shown in below figure.






Each MPDU comprises a Security TAG (SecTAG), Secure Data and Integrity Check Value (ICV).

**Security TAG:** conveys parameters that identify the protocol and key to be used to validate the received frames. Also, pledges replay protection.

**Secure Data:** comprises of all the user data octets that follow the MACsec TAG and precede the ICV.

**ICV:** This ensures the integrity of destination MAC address, source MAC address, SecTAG and user data. Length of ICV depends on Cipher Suite between 8 octets to 16 octets.

The latest MACsec standard uses AES 256-bit encryption, this is an enormous number and cannot be decrypted using brute force. Fields such as MPLS labels and 802.1Q tags are also encrypted and they cannot be used when Ethernet frame traverses the underlying transport between encrypted switches.

### *MACsec Advantages*

- MACsec design allows security to be introduced into a network one LAN segment at a time
- SecY allows the deployment of MACsec capable systems one by one on a LAN, prior to enabling security
- MACsec design allows coexistence with other protocols on the same insecure LAN
- MACsec supports usage of shared media to provide independent services
- MACsec detects unauthorized attempts by integrity and replay protection
- MACsec discards frames sent by systems that are not authenticated and authorized members of the CA, thus localizing the traffic sent by those stations to a single LAN

### *MACsec Limitations*

- MACsec will not protect against ARP spoofing
- An asymmetric MAC service can cause these side effects:
  - STP could create loops in the network
  - The operation of OSPF routing protocol will be inefficient
- A point-to-multipoint LAN does not provide the MAC Service
- MAC Service does not guarantee the origin or authenticity of service requests
- MACsec does not support Non-repudiation or protection against Traffic Analysis
- MACsec does not protect against brute force denial of service attacks

### *Hop-by-hop Vs End-to-End*

- Hop-by-Hop (Link Encryption) also known as “bump in the wire” model, packets are decrypted on the receive (ingress) port and encrypted on the transmit (egress) port. This encrypts all of the data including headers, addresses and routing information.
- End-to-end encryption does not include header, address, routing and trailer information. The packets need not be decrypted and encrypted at each hop.

In a LAN environment, hop-by-hop encryption is preferable, whereas in a MAN / WAN environment end-to-end encryption is more efficient and flexible.

### *Hardware Implementation Choice*

The MACsec control plane (802.1X-2010) runs on a control processor whereas Ethernet MAC is the natural place for MACsec data plane (802.1AE). But the respin of switch ASIC to include MACsec is very expensive cycle so it may be preferable to implement MACsec outside the switch ASIC.

Two choices can be made

- Integrate with PHY device
- Separate device (FPGA) placed in between ASIC and PHY device

## Conclusion

When compared to IPsec, MACsec offers improved network efficiency and latency, lower incremental cost and power (MACsec standard is an extension of standard Ethernet), and is less complex to manage than at the IP layer. MACsec was initially designed for LAN environment with a hop-by-hop encryption. With the popularity of WAN services using Metro Ethernet it makes more sense to extend MACsec capabilities to support the end-to-end encryption. Some equipment manufacturers and merchant silicon vendors are already providing proprietary MACsec end-to-end encryption solutions. Using these solutions MACsec can be deployed in a Metro Ethernet WAN and support E-Line, E-LAN and multipoint-to-multipoint services.

Another upcoming wave of Internet of Things (IoT) makes it inevitable to extend MACsec towards IoT network. MACsec over VxLAN can encrypt the tenant's data and doesn't have to rely on a hypervisor's security mechanism.

*References*

[1] 802.1AE – 2006 IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Security.

[2] 802.1X – 2004 IEEE Standard for Local and Metropolitan area networks: Port-Based Network Access Control.

[3] http://muniwireless.com/2010/06/02/smart-grid-security-ground-zero-for-cyber-security/



Contact Us
**Phone:** +1-877-699-3267

**Email:** ipisales@ipinfusion.com