
# MACsec Between AOS OmniSwitch

A Step-by-Step Configuration Guide for Alcatel-Lucent Enterprise OmniSwitch

Alcatel·Lucent

# 1. Introduction

As enterprise networks carry increasingly sensitive data, securing Layer 2 links is no longer optional. MACsec (IEEE 802.1AE) provides hardware-accelerated, hop-by-hop encryption and authentication directly on Ethernet segments — protecting traffic before it leaves the wire. This guide walks through enabling MACsec between two Alcatel-Lucent Enterprise (ALE) OmniSwitch devices running AOS, using the Dynamic SA mode powered by the MACsec Key Agreement (MKA) protocol.

MACsec is an IEEE 802.1AE standard that provides encryption and packet authentication to IEEE 802.1 frames. MACsec provides point-to-point security on Ethernet links between directly connected nodes. Using MACsec prevents DoS/M-in-M/playback attacks, intrusion, wire-tapping, masquerading, etc. MACsec can be used to secure most of the traffic on Ethernet links – LLDP frames, LACP frames, DHCP/ARP packets, etc.

MACsec (IEEE 802.1AE) provides:

- Layer 2 encryption
- Data integrity
- Replay protection

Before starting, ensure:

- Both devices support MACsec
- A valid MACsec license is installed and active
- Devices are running a supported AOS version

The default crypto suite used in MACsec is “128-bit AES-GCM” and the Session key is called a “Secure Association Key (SAK)”. Each endpoint in a MACsec-protected network has at least one TX Secure Channel (SCI-TX) and multiple RX Secure Channels (SCI-RX). Between a MACsec secure link, each endpoint is configured with a matching SCI-TX and SCI-RX pair in both directions. Each Secure Channel (SC) is associated with Secure Associations (SAs) which in turn hold the Secure Association Keys (SAK) along with a Packet Number (PN).

Based on how the Secure Association Key (SAK) is exchanged, there are two modes for MACsec SA:

1. **Static SA Mode** [Use case: Switch-to-Switch links]
    - Admin configures SC/SA/keys manually

2. **Dynamic SA Mode** [Use case: Switch-to-Switch or Switch-to-Host links]
    - MKA (MACsec Key Agreement protocol)
    - Discovery of other MACsec nodes
    - Setup of SC/SA
    - Key generation and distribution
    - Synchronization of packet numbers (PN)

**Dynamic Secure Association (SA) mode is recommended, and this document provides the configuration details for this mode.**

This document covers Dynamic SA Mode configuration. Static SA mode configuration (manual SC/SA/key setup) is covered separately in the ALE MACsec Static SA guide.

## 2. Scope & Supported Platforms

This guide applies to the following ALE OmniSwitch platforms and AOS software releases:

| Platform | AOS Version | Notes |
|---|---|---|
| OmniSwitch 6900 | AOS 8.6R2 and later | MKA / Dynamic SA supported |
| OmniSwitch 9900 | AOS 8.7R1 and later | MKA / Dynamic SA supported |
| OmniSwitch 6860/6865 | AOS 8.6R2 and later | Check platform datasheet |

Additional prerequisites:

- The inter-switch link must be a direct Ethernet connection (MACsec is hop-by-hop and does not traverse Layer 3 boundaries)
- Clock synchronization via NTP is recommended to avoid key-expiry issues

## 3. Sample Topology

The diagram below shows the reference topology used in this guide: two ALE OmniSwitch devices (DIST-5 and DIST-6) connected via a direct link on port 1/1/1. MACsec is enabled on this inter-switch link, encrypting all Ethernet frames traversing the segment. DIST-5 acts as the MKA Key Server in the configuration examples that follow.

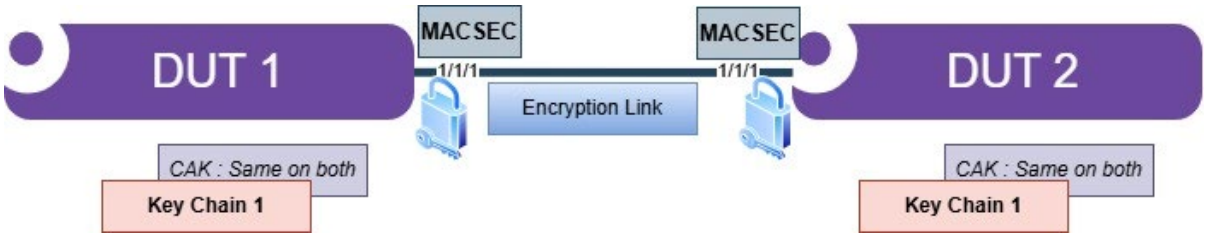


*Figure 1: MACsec-protected direct link between two AOS OmniSwitch devices*

## 4. MACsec License Installation

A MACsec feature license must be applied and active on both switches before configuring MACsec. The steps below must be repeated on each device.

### Step 1: Copy License File

Copy the MACsec license file to the switch:

**Transfer the license file to the switch using FTP/SCP/SFTP**

```
DIST-5-> copy <source> /flash/macsec_license.txt
```

```
DIST-5-> ls -ltr
total 18752
drwxr-xr-x 2 admin user  16384 Dec 31 2019 lost+found
drwxr-xr-x 7 10    admins  4096 Dec 31 2019 extensions
drwxr-xr-x 3 admin user   4096 Mar  5 2025 pmd
drwxr-xr-x 3 admin user   4096 Mar  5 2025 afn
drwxr-xr-x 2 admin user   4096 Mar  5 2025 network
-rw-r--r-- 1 admin user    160 Jun 13 2025 macsec_license.txt
```

**Execute the license apply file command as shown.**

### Step 2: Apply License

```
DIST-5-> license apply file /flash/macsec_license.txt order-id <xxxxxxxx>
```

### Step 3: Verify License

```
DIST-5-> show license-info
```

Example output:

**Expiration must be NA and Upgrade Status should be PERM, means permanent**

```
                Time (Days)  Upgrade  Expiration
                Remaining    Status   Date
------------------------+------------+---------+--------------
Advanced            PERM       NA      NA
MACSEC              PERM       NA      NA
```

Ensure **MACSEC = PERM** is displayed for all devices.

## 5. MACsec Configuration

Configuration must be performed on **both switches**. The Connectivity Association Key (CAK) and key-chain ID must match exactly on both devices — any mismatch will prevent the MKA session from establishing.

**AES-CMAC-256 is algorithm to generate CAK for authentication and key derivation.**

### 5.1 Configure Security Key (CAK)

```
DIST-5-> security key 1 algorithm aes-cmac-256 hex-key 0x011 keyed-name 0x011
```

**Bind CAK key to the key-chain to use in the macsec.**

### 5.2 Configure Key Chain

```
security key-chain 1 key 1
```

## 5.3 Verify Key and Key Chain

```
DIST-5-> show security key 1
```

The configured CAK must be valid, and there is no validity lifetime associated with it.

Example output:

```
id  status  algorithm    start-time  life-time  keyed-name
1   valid   aes-cmac-256 -           -          <key>
```

```
DIST-5-> show security key-chain 1
```

Example output:

```
id  name       current  associated  user
1   keychain_1 -        1           esmCmm
```

These commands enable MACsec on the interface using dynamic keying with a pre-shared key,

## 5.4 Configure MACsec on Interface

```
DIST-5-> interfaces 1/1/1 macsec mode dynamic key-chain 1 encryption
DIST-5-> interfaces port 1/1/1 macsec admin-state enable
```

# 6. Verification

The output confirms that MACsec is enabled, the interface is acting as the key server, and the secure session is up with encryption active.

## Check MACsec Status

```
DIST-5-> show interfaces macsec dynamic
```

Example output: (Switch acting as key server):

```
Chas/Slot/Port  Admin-State  Mode     Keychain    Encryption  Server  Status
1/1/1           Enabled      keychain 1           Enabled     YES     UP
```

Example output: (Peer switch):

```
Chas/Slot/Port  Admin-State  Mode     Keychain   Encryption  Server  Status
1/1/1           Enabled      keychain 1          Enabled     NO      UP
```

### Check MACsec Statistics

Use the following command to view packet encryption and decryption counters and confirm traffic is flowing:

```
DIST-5-> show interfaces macsec statistics 1/1/1
```

## 7. Troubleshooting

If the MACsec session does not come UP, use the checklist below to isolate the issue.

| Symptom | Likely Cause | Resolution |
|---|---|---|
| Status shows DOWN | CAK / key-chain mismatch between peers | Verify both switches use identical hex-key and keyed-name values |
| Status shows DOWN | MACsec license missing or expired | Run show license-info and confirm MACSEC = PERM |
| Status shows DOWN | Admin-state not enabled | Run: interfaces port 1/1/1 macsec admin-state enable on both switches |
| Session UP but no traffic | Encryption mismatch (one side encrypted, other not) | Ensure both sides use the encryption keyword — or both omit it |
| Intermittent session drops | Clock skew causing key expiry | Enable NTP on both switches and confirm time synchronization |
| Interface missing from output | AOS version does not support MACsec on this port | Check the platform release notes; uplink/front ports may differ |

For deeper diagnostics, enable MACsec debug logging:

```
DIST-5-> debug interfaces macsec enable
```

## 8. Important Notes

- Both switches must:
  - Use the **same CAK (pre-shared key)**
  - Use the **same key-chain**
- MACsec operates **hop-by-hop (Layer 2)**
- One switch will act as **Key Server (MKA role)**
- **License is per-device:** Each switch must have its own active MACsec license.
- **LACP/LLDP protection:** MACsec can encrypt LACP and LLDP frames, providing additional protection for link-aggregation and topology-discovery traffic.

## Conclusion

MACsec provides a powerful and standards-based way to secure Layer 2 links in your ALE OmniSwitch network. By leveraging the MKA protocol in Dynamic SA mode, you get automated key negotiation and rotation without manual SAK management making MACsec practical to deploy at scale across campus and data-center interconnects.

The configuration is straightforward: install the license, define a shared CAK and key-chain on both devices, apply MACsec to the interface, and verify that both sessions reach the UP state. Once active, all Ethernet frames traversing the protected link are encrypted with AES-GCM-128, giving you confidentiality, integrity, and replay protection at wire speed.

As a next step, consider extending MACsec to additional inter-switch links and review your key rotation policy to align with your organization's security standards. For Switch-to-Host scenarios or environments requiring manual key management, refer to the ALE Static SA MACsec configuration guide.

## References


ALE Network Ethernet Switches — OmniSwitch Portfolio

AOS Release 8 Network Configuration Guide (PDF)

IEEE 802.1AE-2018: MAC Security Standard