MACsec Configuration and Operation

Encryption is a critical element of many network designs, to ensure confidentiality and defend against potential threats such as replay attacks. Both MACsec and IPSec provide strong encryption, with different performance levels that make them suitable for different roles.

Media Access Control Security (MACsec) 802.1AE, is an industry standard security technology that provides secure communication for all application traffic on high speed Ethernet links at wirespeed. MACsec provides higher performance and scales linearly, compared to IPSec.

As IPSec operates at the IP layer it traditionally has been leveraged for end to end encryption between devices, both over the Internet and for private WAN networks. It is a practical option for any IP transport medium, scales to large numbers of simultaneous connections making it ideal for hub and spoke networks and it is transparent to the intermediate L2 and L3 devices so it can be carried over public and private networks.

As an encryption solution IPSec is capable of many simultaneous connections, but the total encryption performance of the router is limited by the embedded hardware used for the encryption. To perform encryption at high throughput IPSec is offloaded to dedicated encryption engines or ASICs. Despite the use of hardware accelerated IPSec, performance is unable to keep pace with the link speeds typically deployed for interconnecting sites at 10G to 400G.

On the other hand, MACsec is a link layer encryption for Ethernet, and is typically executed in the PHY device, and operates at the link speed of the ports - 1G to 100G. For switches and routers capable of supporting multiple terabits of throughput MACsec can provide line rate encryption for secure connections, regardless of packet size, and scales linearly as it is distributed throughout the device.

MACsec is available on a number of 7280R fixed form factor switches and 7500R Series line cards, and this paper discusses the configuration of MACsec on those systems.

MACsec Support on Arista's Modular Platforms

7500R Series 8-Port 200G Tunable Coherent DWDM Line Card

The Arista DWDM line card has built-in 100G wire-speed encryption on every port. Standards-based IEEE 802.1AE (MAC Security standard, referred to as MACsec) capabilities provide line-rate frame encryption and authentication for traffic transported across DWDM. This optional functionality removes the need for additional intermediate devices and provides encryption which ensures confidentiality as well as provides anti-replay protection and therefore confidence in the integrity of encrypted traffic.

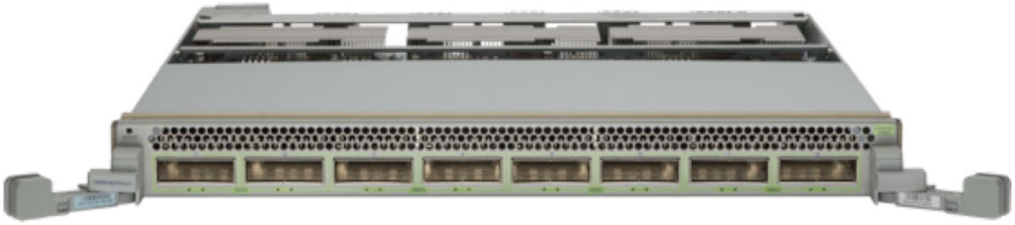

Figure 1: DCS-7500R-8CFPX-LC

7500R Series 36-Port QSFP Line Card

The Arista 100G MACsec line card delivers up to 7.2 Tbps of bandwidth with 36 ports of 100G QSFP interfaces. Full 100GbE standards support ensures interoperability and future proofing for next generation network architecture. Support for industry standard pluggable optics for both single and multi-mode fiber provide a wide choice of connection options. All QSFP ports are capable of operating independently in providing a flexible combination of speeds and operating distances using Arista pluggable optics and cables. Each port is individually configurable for MACsec allowing a flexible combination of encrypted links and standard links. There are three different product SKUs available with identical port configuration, each SKU has its advantages. Please refer to the individual product datasheet for further details.

Figure 2: DCS-7500R(2)(A)M-36CQ

MACsec Support on Arista's Fixed Platforms

The Arista 7280R and 7280R2 are part of the 7280R series of fixed systems, which are key components of the Arista 7000 Series portfolio of data center switches. The 7280R MACsec systems are high performance compact routing platforms with built-in wire speed MACsec encryption that is purpose built for the highest performance environments, and to meet the needs of large scale data centers.

7280R with MACsec and DWDM Fixed Platform

The Arista 7280SRM-40CX2 is a high performance, compact, 1RU 7280R Series switch router with built-in wire speed MACsec encryption and DWDM interfaces. The 7280SRM-40CX2 has built-in 100G wire-speed encryption on the 2 CFP2-DCO ports, eliminating the need for external encryption devices and provides security against intrusion, passive wire tapping and other playback attacks. Standards-based IEEE 802.1AE capabilities provide line-rate frame encryption and authentication for traffic transported across DWDM. The switch delivers 1.6Tbps of wire speed performance along with 4GB of packet buffer.

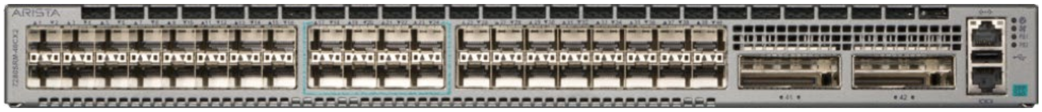

Figure 3: DCS-7280SRM-40CX2

7280R High Density MACsec Fixed Platform

The 7280CR2M-30 delivers large packet buffers, scale and high availability with built-in wire-speed MACsec encryption on all 30 x 100GE ports in a high density compact 1RU form factor. The 7280CR2M-30 can support upto 30x100GbE ports all with MACsec. MACSec is supported only at 100G port speeds but other speeds are supported without MACsec. The switch delivers 6Tbps of wire speed performance with 12GB of packet buffer.

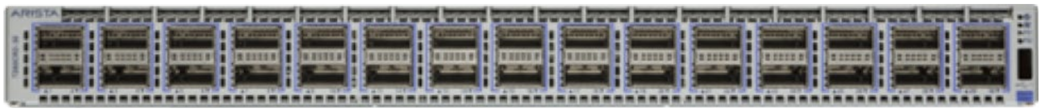

Figure 4: DCS-7280CR2M-30

7280R ToR MACsec Fixed Platform

7280SRAM-48C6 switch supports 48 port SFP+ and 6 ports QSFP100. The 6, 100G QSFP ports support built-in wire-speed MACsec encryption on all 6 x 100GE ports. MACsec is supported only at 100G port speed. The switch delivers 2.16Tbps of wire speed performance with 4GB of buffer.

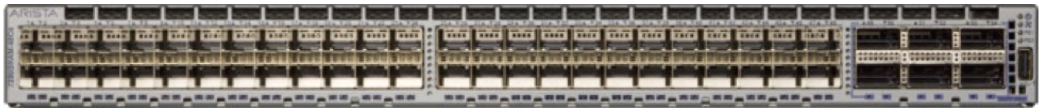

Figure 5: DCS-7280SRAM-48C6

Encryption Feature Licensing

As MACsec is a strong encryption technology that has restrictions on it's use, it is controlled by an EOS license, and requires a license key is installed to enable the encryption. A valid Mac Security license must be configured on a switch before it can be configured.

The following command is used to configure a Mac Security license:

```
Arista(config)#mac security

Arista(config-mac-security)#license <licensee> <license-code>
```

The <license-code> is tied to the switch serial number and the <licensee> which means you'll need one license-code for each switch that'll be configured for MACsec.

Get in touch with your local Arista Account team to obtain the license keys if required.

Deployment of MACsec

When MACsec is enabled on an interface, the interface moves into an "unauthorized" mode (Identical to Dot1x) dropping all frames and accepting only MACsec packets (which in turn are EAPOL packets called MKPDUs). In this state, the interface is not considered to be a part of any topology and the interface continues this way until the Macsec Key Agreement (MKA) procedures are complete. Once an MKA handshake is concluded, the interface enters an "authorized" mode permitting all packets which pass the integrity and encryption check on that interface.

Key MACsec Terminology

MACsec Key Agreement Protocol (MKA): Key agreement protocol for discovering MACsec peers and negotiating keys between MACsec peers (IEEE 802.1X-REV).

Connectivity Associations (CA): A security relationship between MACsec-capable devices. Endpoints that share CAK are part of same Secure Connectivity Association (CA). There can be more than two endpoints in a Secure Connectivity Association. Arista implementation is limited to 2 endpoints.

Connectivity Association Key (CAK): Endpoints that share CAK are part of same Secure Connectivity Association (CA). This key can either be a static pre-shared key or dynamically derived when 801.1x authentication is used. The CAK is a long-lived master key used to generate all other keys used for MACsec.

Connectivity Association Key Name (CKN): Identifies the CAK.

Primary Key: Ideally this should be the CAK for the MKA session in progress.

Fallback Key: In case the primary configured key does not establish its connection, we fall back on the fallback key, so as to ensure no loss of traffic

Secure Association Key (SAK): Derived from the CAK and is the key used by the network device ports to encrypt traffic for a given session.

Key Server: One of the MACsec peers in the CA becomes the Key Server. Main role of the Key Server is creation and distribution of Secure Association Keys (SAKs), which are used in actual data encryption.

Frame Overhead

MACsec adds 24 bytes (sectag + ICV) to every encrypted frame. The ethtype for MACsec encrypted frames is 0x88e5.

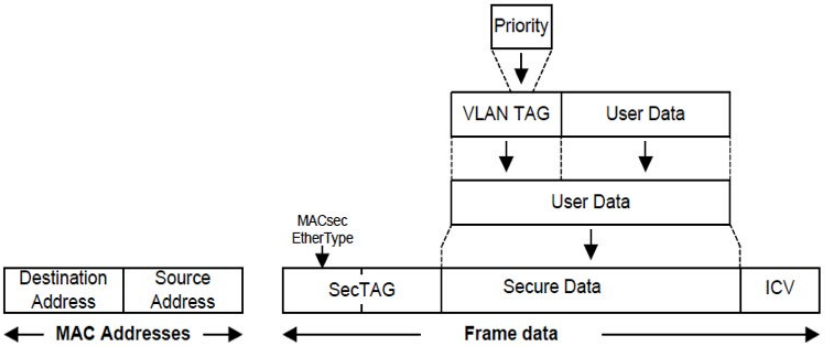

Figure 6: Frame Overhead

Configuration Options

MKA with static keys

There are 2 main methods of configuring MACsec

- MACsec with Static Keys
- MACsec with Dynamic security Keys

For the purpose of this document we will focus on MACsec with Static Keys

Static Keys (Pre-configured Keys)

First step create a profile

```
Arista(config-mac-security)#profile <profile-name>
```

Next is to configure Connection Association Key (CAK) and Connection Association Key Name (CKN). CAK/CKN needs to pre-configured on both ends. On Arista switches, both the CKN and the CAK are entered in hex octets. When a CAK is configured into a profile as described below, it is considered to be the primary key to be used to derive all subsequent encryption keys. In order for a MAC Security profile to be active, a primary key MUST be configured in it. On Arista switches, the CAK is configured into a profile using the “key” command. For Example:

```
Arista(config-mac-security-profile-sampleProfile)#
```

- “key” is the command used to configure the CAK.
- “0abcd1” is the CKN
- “0” indicates that an un-encrypted CAK is about to follow
- “1234abcd” is the CAK

Optionally a fallback CAK can also be configured on a profile. This CAK is picked up by MAC Security to negotiate keys when the primary CAK fails for some reason. A CAK can be configured as a backup key using the "fallback" keyword with the "key" command. Here is an example:

```
Arista(config-mac-security-profile-sampleProfile)#
```

The fallback key kicks in under following conditions:

- When the switch boots with a corrupted or mismatched keys, OR
- After an interface flap, primary keys do not match for the very first macsec negotiation, OR
- Primary key change on one switch via "same CKN + same/different CAK".

Fallback key does not kick in when macsec is already established and primary key configuration is changed on one switch such that primary key configuration do not match anymore. The older primary key continue to remain operational in this case.

There is an option to configure a key-server between the MACsec peers by configuring a priority value. By default the priority is 16, lower value indicates higher priority.

Key Server

- One of the MACsec peers in the CA becomes the Key Server
- Main role of the Key Server is creation and distribution of Secure Association Keys (SAKs), which are used in actual data encryption
- In MKA with static keys, one end should be configured with a greater key server priority than the other - this end will be the Key Server
- If both ends have the same key server priority configured, then the end with lower mac address will become the Key Server
- SAKs are generated by the Key Server, wrapped through AES-key wrap and sent over to the peers, in MKPDUs

On Arista switches, default priority is 16 when no key-server priority is configured on the CLI. A lower value indicates higher priority. In case Mac Security peers have identical priority, the peer with the lower MAC address is elected as the key server. The default key server priority can be edited as shown below:

```
Arista(config-mac-security-profile-sampleProfile)#
```

The switch acting as Key Server can be identified with the following show command:

On the Key Server:

```
Arista#
Interface: Ethernet5/3/1
    CKN: 0abc1234
      Message ID: 6a2bf40a95be4a1595fda30e
      Success: True
      Principal: True
      Default: False
```

On the Non Key Server:

```
Arista#
Interface: Ethernet10/3/1
    CKN: 0abc1234
      Message ID: ea80ba94d249a00ed241017d
      Success: True
      Principal: True
      Default: False
```

Session Association Key (SAK)

MACsec uses a Session Association Key (SAK) for encrypting data traffic. The SAK is derived from the CAK. The default session rekey-period is 0. The SAK is not refreshed periodically in the absence of the below config and can be configured as shown:

```
Arista(config-mac-security-profile-sampleProfile)#
```

You can check the SAK re-key period using the following show command.

```
Arista#
Interface: Ethernet5/3/1
    SCI: 28:99:3a:82:63:00::763
    SSCI: 00000002
    Controlled port: True
    Key server priority: 16
     Key in use: 6a2bf40a95be4a1595fda30e:66
    Latest key: None
    Old key: 6a2bf40a95be4a1595fda30e:66(RT)
```

Cipher

Cipher defines the data encryption algorithm and mode. Arista supports aes128-gcm-xpn and aes256-gcm-xpn. Default cipher (if nothing is configured) is aes128-gcm-xpn. Our recommendation will be to use aes256-gcm-xpn for stronger encryption which supports upto 64 hexadecimal characters for the key string.

```
Arista(config-mac-security-profile-macsec-test)#

  aes128-gcm-xpn  Advanced Encryption Standard (128 bit, Galois/Counter mode, Extended
Packet Numbering)

  aes256-gcm-xpn  Advanced Encryption Standard (128 bit, Galois/Counter mode, Extended
Packet Numbering)
```

Mac Security relies on a strong random number generator to generate cryptographic keys. Configuring the following command strengthens the random number generator used by Mac Security

```
Arista(config)management security

Arista(config-mgmt-security)#entropy source hardware
```

Mac Security can function adequately without hardware generated entropy. **However, it is highly recommended to use this command in conjunction with Mac Security.**

MACsec Configuration

Let's put all the above components together to see how the entire MACsec configuration would look like. You'll need the following configs to enable MACsec with static keys:

- Global MACsec license configuration
- Global MACsec profile definition
- Interface-level MACsec profile application
- (Optional) Hardware Entropy Configuration

```
mac security
   license productTest db7cf232
   !
   profile macsec-test
      key 0abc1234 7 06070E234E4D0A48544540585F507E
      key 0def5678 7 09484A0C1C0311475E5A527D7C7C70 fallback
      mka session rekey-period 30
    cipher aes256-gcm-xpn
!

interface Ethernet5/3/1
   mac security profile macsec-test
!
management security
   entropy source hardware
```

In the MACsec profile definition above:

⇨ “key” is the command used to configure the CAK.

⇨ “0abc1234” is the Connectivity Association Key Name (CKN)

⇨ “7” indicates that an encrypted CAK is about to follow

⇨ “06070E234E4D0A48544540585F507E” is the CAK for primary key

⇨ “09484A0C1C0311475E5A527D7C7C70” is the CAK for fallback key

⇨ “fallback” is the keyword required for fallback key

Both CKN and CAK are hexadecimal strings.

Note: If you have a port-channel, the MACsec profile needs to be applied under the physical interface members of the port-channel.

Reference :

Platform	Datasheet
DCS-7500R-8CFPX-LC	https://www.arista.com/assets/data/pdf/Datasheets/7500RDWDM-Datasheet.pdf
DCS-7500RM-36CQ-LC	https://www.arista.com/assets/data/pdf/Datasheets/7500RM_36CQdatasheet.pdf
DCS-7500R2M-36CQ-LC	https://www.arista.com/assets/data/pdf/Datasheets/7500RM_36CQdatasheet.pdf
DCS-7500R2AM-36CQ-LC	https://www.arista.com/assets/data/pdf/Datasheets/7500RM_36CQdatasheet.pdf
DCS-7280SRM-40CX2	https://www.arista.com/assets/data/pdf/Datasheets/7280SRAM_DWWMdatasheet.pdf
DCS-7280SRAM-48C6	https://www.arista.com/assets/data/pdf/Datasheets/7280SRAM_48C6%20datasheet.pdf
DCS-7280CR2M-30	https://www.arista.com/assets/data/pdf/Datasheets/7280SRAM_48C6%20datasheet.pdf

https://eos.arista.com/eos-4-15-4f/macsec/

https://eos.arista.com/eos-4-17-0f/macsec-eap-fast-support/

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062