Hewlett Packard Enterprise

HPE FlexNetwork 5510 HI Switch Series

MACsec Configuration Guide

Part number: 5200-1247
Software version: Release 1118P02
Document version: 6W100-20160328

Acknowledgments

Contents

Configuring MACsec

Overview

Media Access Control Security (MACsec) secures data communication on IEEE 802 LANs. MACsec provides services such as data encryption, frame integrity check, and data origin validation for frames on the MAC sublayer of the Data Link Layer.

Basic concepts

CA

Connectivity association (CA) is a group of participants that use the same key and key algorithm. The encryption key used by the CA participants is called a connectivity association key (CAK). The following types of CAKs are available:

- **Pairwise CAK**—Used by CAs that have two participants.
- **Group CAK**—Used by CAs that have more than two participants.

The pairwise CAK is used most often because MACsec is typically applied to point-to-point networks.

A CAK can be an encryption key generated during 802.1X authentication or a user-configured preshared key. The user-configured preshared key takes precedence over the 802.1X-generated key.

SA

Secure association (SA) is an agreement negotiated by CA participants. The agreement includes a cipher suite and keys for integrity check.

A secure channel can contain more than one SA. Each SA uses a unique secure association key (SAK). The SAK is generated from the CAK, and MACsec uses the SAK to encrypt data transmitted along the secure channel.

MACsec Key Agreement (MKA) limits the number of packets that can be encrypted by an SAK. When the limit is exceeded, the SAK will be refreshed. For example, when packets with the minimum size are sent on a 10-Gbps link, an SAK rekey occurs about every 300 seconds.

MACsec services

MACsec provides the following services:

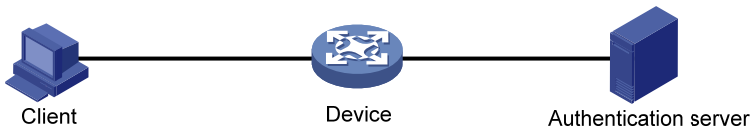
- **Data encryption**—Enables a port to encrypt outbound frames and decrypt MACsec-encrypted inbound frames.
- **Integrity check**—Performs integrity check when the device receives a MACsec-encrypted frame. The integrity check uses the following process:
  a. Uses a key negotiated by MKA to calculate an integrity check value (ICV) for the frame.
  b. Compares the calculated ICV with the ICV in the frame trailer.
    - If the ICVs are the same, the device verifies the frame as legal.
    - If the ICVs are different, the device determines whether to drop the frame based on the validation mode.
- **MACsec replay protection**—When MACsec frames are transmitted over the network, frame disorder might occur. MACsec replay protection allows the device to accept the out-of-order packets within the replay protection window size and drop other out-of-order packets.

MACsec applications

MACsec supports the following application modes:

- **Client-oriented mode**—Secures data transmission between the client and the access device. In this mode, the authentication server generates and distributes the CAK to the client and the access device. In this mode, MACsec must operate with 802.1X authentication.

  Figure 1 Client-oriented mode

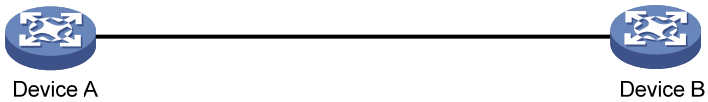
  

  NOTE:

  In client-oriented mode, an MKA-enabled port on the access device must perform port-based 802.1X access control. The authentication method must be EAP relay.

- **Device-oriented mode**—Secures data transmission between devices. In this mode, the devices do not perform identity authentication, and the same preshared key must be configured on the MACsec ports that connect the devices. The devices use the configured preshared key as the CAK.

  Figure 2 Device-oriented mode

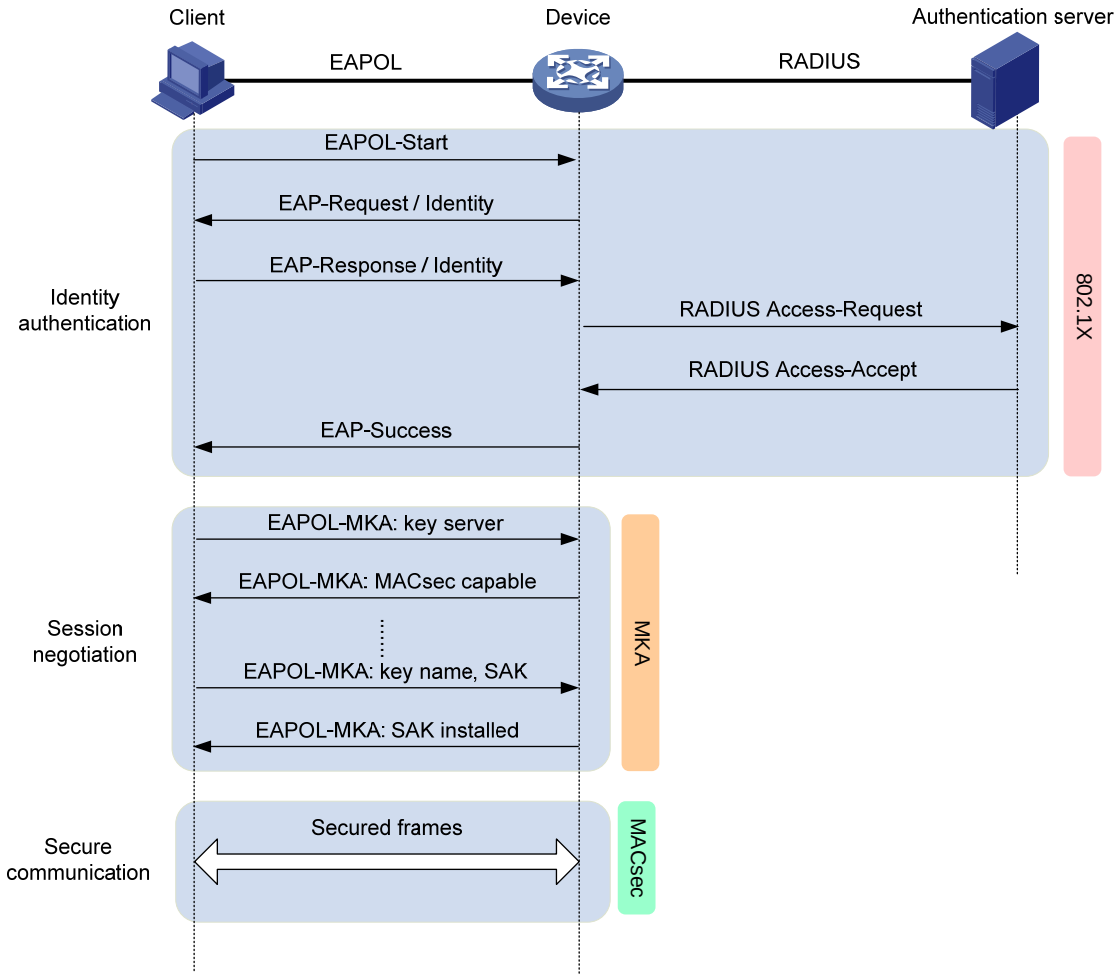
  

MACsec operating mechanism

Operating mechanism for client-oriented mode

Figure 3 illustrates how MACsec operates in client-oriented mode.

Figure 3 MACsec interactive process in client-oriented mode



The following shows the MACsec process:

1. After the client passes 802.1X authentication, the RADIUS server distributes the generated CAK to the client and the access device.
2. After receiving the CAK, the client and the access device exchange EAPOL-MKA packets.

   The client and the access device exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire.

   During the negotiation process, the access device automatically becomes the key server. The key server generates an SAK from the CAK for packet encryption, and it distributes the SAK to the client.
3. The client and the access device use the SAK to encrypt packets, and they send and receive the encrypted packets in secure channels.
4. When the access device receives a logoff request from the client, it immediately removes the associated secure session from the port. The remove operation prevents an unauthorized client from using the secure session established by the previous authorized client to access the network.

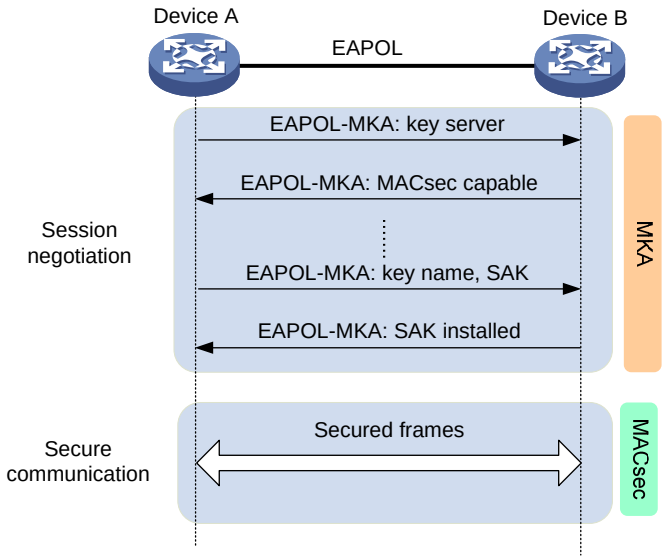
The MKA protocol also defines a session keepalive timer. If one participant does not receive any MKA packets from the peer after the timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.

Operating mechanism for device-oriented mode

As shown in Figure 4, the devices use the configured preshared keys to start the session negotiation.

In this mode, the session negotiation, secure communication, and session termination processes are the same as the processes in client-oriented mode. However, MACsec performs a key server selection in this mode. The port with higher MKA key server priority becomes the key server, which is responsible for the generation and distribution of SAKs.

Figure 4 MACsec interactive process in device-oriented mode



Protocols and standards

- IEEE 802.1X-2010, *Port-Based Network Access Control*
- IEEE 802.1X-2006, *Media Access Control (MAC) Security*

Feature and hardware compatibility

IMPORTANT:

MKA cannot be enabled on MACsec-incapable interfaces. In this switch series, the following interfaces are MACsec-capable:

- The leftmost eight interfaces (GigabitEthernet x/0/1 through GigabitEthernet x/0/8) on each switch.
- The interfaces on LSWM2XGT2PM(JH156A) and LSWM2SP2PM(JH157A) interface modules installed on switch models except HPE 5510 24G SFP 4SFP+ HI 1-slot Switch (JH149A). The interface modules do not support hot swapping if MKA is enabled on such interfaces.

MACsec configuration task list

In device-oriented mode, the MACsec configuration takes effect on Layer 2 and Layer 3 Ethernet ports. In client-oriented mode, the MACsec configuration takes effect only on 802.1X-enabled ports.

To configure MACsec, perform the following tasks:

Tasks at a glance	Remarks
(Required.) Enabling MKA	N/A

Tasks at a glance	Remarks
(Optional.) Enabling MACsec desire	N/A
(Optional.) Configuring a preshared key	This task is required in device-oriented mode.
(Optional.) Configuring the MKA key server priority	N/A

(Optional.) Use one of the following methods to configure MACsec protection parameters:
• Configuring MACsec protection parameters in interface view:
  ◦ Configuring the MACsec confidentiality offset
  ◦ Configuring MACsec replay protection
  ◦ Configuring the MACsec validation mode
• Configuring MACsec protection parameters by MKA policy:
  ◦ Configuring an MKA policy
  ◦ Applying an MKA policy
	N/A

Enabling MKA

MKA establishes and manages MACsec secure channels on a port. It also negotiates keys used by MACsec.

You cannot enable MKA on a MACsec-incapable port.

To enable MKA:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MKA.	**mka enable**	By default, MKA is disabled on the port.

Enabling MACsec desire

The MACsec desire feature expects MACsec protection for outbound frames. The key server determines whether MACsec protects the outbound frames.

MACsec protects the outbound frames of a port when the following requirements are met:

- The key server is MACsec capable.
- Both the local participant and its peer are MACsec capable.
- A minimum of one participant is enabled with MACsec desire.

To enable MACsec desire:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MACsec desire.	**macsec desire**	By default, the port does not expect MACsec protection for outbound frames.

Configuring a preshared key

In device-oriented mode, configure a preshared key as the CAK to be used during MKA negotiation. To successfully establish an MKA session between two devices, make sure the connected MACsec ports are configured with the same preshared key.

A user-configured preshared key has higher priority than the 802.1X-generated CAK. To ensure a successful MKA session establishment, do not configure a preshared key in client-oriented mode.

To configure a preshared key:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set a preshared key.	**mka psk ckn** *name* **cak simple** *string*	By default, no MKA preshared key exists. The MACsec cipher suite supported by the device requires that the CKN and CAK each must be 32 characters long. If the configured CKN or CAK is not 32 characters long, the system performs the following operations when it runs the cipher suite: • Automatically increases the length of the CKN or CAK by zero padding if the CKN or CAK contains less than 32 characters. • Uses only the first 32 characters if the CKN or CAK contains more than 32 characters.

Configuring the MKA key server priority

Configure an MKA key server priority for key server selection. The lower the priority value, the higher the priority.

In client-oriented mode, the access device port automatically becomes the key server. You do not have to configure the MKA key server priority.

In device-oriented mode, the port that has higher priority becomes the key server. If a port and its peers have the same priority, MACsec compares the secure channel identifier (SCI) values on the

ports. The port with the lowest SCI value (a combination of MAC address and port ID) becomes the key server.

A port with priority 255 cannot become the key server. For a successful key server selection, make sure a minimum of one participant's key server priority is not 255.

To configure the MKA key server priority:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the MKA key server priority.	**mka priority** *priority-value*	The default setting is 0.

Configuring MACsec protection parameters in interface view

If you configure a parameter in interface view after applying an MKA policy, the configuration in interface view overwrites the configuration of the parameter in the MKA policy. Your configuration also removes the MKA policy application from the port. However, other parameter settings of the MKA policy are effective on the port.

If the parameter value in interface view is the same as the value in the MKA policy, your configuration does not take effect. The policy remains active on the port.

Configuring the MACsec confidentiality offset

The MACsec confidentiality offset specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame.

MACsec uses the confidentiality offset propagated by the key server.

To configure the MACsec confidentiality offset:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the MACsec confidentiality offset.	**macsec confidentiality-offset** *offset-value*	The default setting is 0, and the entire frame needs to be encrypted. The offset value can be 0, 30, or 50.

Configuring MACsec replay protection

The MACsec replay protection feature allows a MACsec port to accept a number of out-of-order or repeated inbound frames. The configured replay protection window size is effective only when MACsec replay protection is enabled.

To configure MACsec replay protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MACsec replay protection.	**macsec replay-protection enable**	By default, MACsec replay protection is enabled on the port.
4. Set the MACsec replay protection window size.	**macsec replay-protection window-size** *size-value*	The default setting is 0, and frames are accepted only in the correct order.

Configuring the MACsec validation mode

The MACsec validation allows a port to perform integrity check based on the following validation modes:

- **check**—Performs validation only, and does not drop illegal frames.
- **disabled**—Does not perform validation.
- **strict**—Performs validation, and drops illegal frames.

In the current software version, only the **strict** mode is supported.

To configure the MACsec validation mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set a MACsec validation mode.	**macsec validation mode** { **check** | **disabled** | **strict** }	In the current software version, only the **strict** mode is supported.

Configuring MACsec protection parameters by MKA policy

Configuring an MKA policy

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an MKA policy and enter its view.	**mka policy** *policy-name*	By default, a system-defined MKA policy exists. The policy name is default-policy. The settings for parameters in the default policy are the same as the default settings for the parameters on a port. You cannot delete or modify the default MKA policy.

Step	Command	Remarks
		You can create multiple MKA policies.
3. (Optional.) Set the MACsec confidentiality offset.	**macsec confidentiality-offset** *offset-value*	The default setting is 0. MACsec uses the confidentiality offset propagated by the key server.
4. (Optional.) Configure MACsec replay protection.	**a** Enable MACsec replay protection: **replay-protection enable** **b** Set the replay protection window size: **replay-protection window-size** *size-value*	By default, MACsec replay protection is enabled. The default replay protection window size is 0. Frames are accepted only in the correct order.
5. Set a MACsec validation mode.	**macsec validation mode** { **check** | **disabled** | **strict** }	In the current software version, only the **strict** mode is supported

Applying an MKA policy

MKA policy provides a centralized method to configure MACsec confidentiality offset, replay protection, and validation mode. An MKA policy can be applied to a port or multiple ports. When you apply an MKA policy to a port, follow these restrictions and guidelines:

- The MACsec parameter settings configured in the MKA policy overwrite the MACsec parameters previously configured on the port.
- Any modifications to the MKA policy take effect immediately.
- When you remove an MKA policy application from the port, the MACsec parameter settings on the port restore to the default.
- When you apply a nonexistent MKA policy to the port, the port automatically uses the default MKA policy. If you create the policy, the policy will be automatically applied to the port.

To apply an MKA policy to a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Apply an MKA policy.	**mka apply policy** *policy-name*	By default, no MKA policy is applied to the port.

Displaying and maintaining MACsec

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display MACsec information on ports.	**display macsec** [**interface** *interface-type interface-number*] [**verbose**]
Display MKA session information.	**display mka session** [**interface** *interface-type interface-number* | **local-sci** *sci-id*] [**verbose**]

Task	Command
Display MKA policy information.	**display mka** { **default-policy** | **policy** [**name** *policy-name*] }
Display MKA statistics on ports.	**display mka statistics** [**interface** *interface-type interface-number*]
Reset MKA sessions on ports.	**reset mka session** [**interface** *interface-type interface-number*]
Clear MKA statistics on ports.	**reset mka statistics** [**interface** *interface-type interface-number*]

MACsec configuration examples

Client-oriented MACsec configuration example

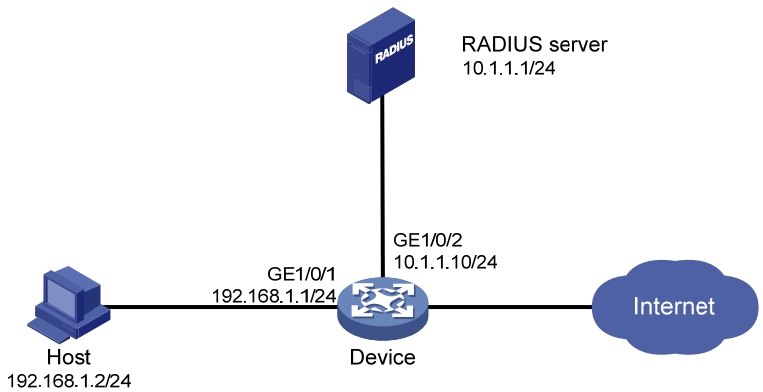
Network requirements

As shown in Figure 5, the host accesses the network through GigabitEthernet 1/0/1. The device performs RADIUS-based 802.1X authentication for the host to control user access to the Internet.

To ensure secure communication between the host and device, perform the following tasks on the device:

- Enable MACsec desire, and configure MKA to negotiate SAKs for packet encryption.
- Set the MACsec confidentiality offset to 30 bytes.
- Enable MACsec replay protection, and set the replay protection window size to 100.
- Set the MACsec validation mode to **strict**.

Figure 5 Network diagram



Configuration procedure

1. Configure the RADIUS server to provide authentication, authorization, and accounting services. Add a user account for the host. (Details not shown.)
2. Configure IP addresses for the Ethernet ports. (Details not shown.)
3. Configure AAA:

   # Enter system view.

   ```
   <Device> system-view
   ```

   # Configure the RADIUS scheme **radius1**.

   ```
   [Device] radius scheme radius1
   ```

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
[Device-radius-radius1] key authentication simple name
[Device-radius-radius1] key accounting simple money
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

Configure the authentication domain **bbb** for 802.1X users.

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme radius1
[Device-isp-bbb] authorization lan-access radius-scheme radius1
[Device-isp-bbb] accounting lan-access radius-scheme radius1
[Device-isp-bbb] quit
```

4. Configure 802.1X:

Enable 802.1X on GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

Implement port-based access control on GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] dot1x port-method portbased
```

Specify **bbb** as the mandatory authentication domain for 802.1X users on GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally, and sets the device to relay EAP packets.

```
[Device] dot1x
[Device] dot1x authentication-method eap
```

5. Configure MACsec:

Create an MKA policy named **pls**.

```
[Device] mka policy pls
```

Set the MACsec confidentiality offset to 30 bytes.

```
[Device-mka-policy-pls] confidentiality-offset 30
```

Enable MACsec replay protection.

```
[Device-mka-policy-pls] replay-protection enable
```

Set the MACsec replay protection window size to 100.

```
[Device-mka-policy-pls] replay-protection window-size 100
```

Set the MACsec validation mode to **strict**.

```
[Device-mka-policy-pls] validation mode strict
[Device-mka-policy-pls] quit
```

Apply the MKA policy to GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mka apply policy pls
```

Configure MACsec desire and enable MKA on GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] macsec desire
[Device-GigabitEthernet1/0/1] mka enable
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display MACsec information on GigabitEthernet 1/0/1.

```
[Device] display macsec interface gigabitethernet 1/0/1 verbose
```

```
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Active MKA policy      : pls
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:02m:07s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 00E0020000000106
      Elapsed time: 00h:02m:03s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

Display MKA session information on GigabitEthernet 1/0/1 after a user logs in.

```
[Device] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E00100000A0006
Priority  : 0
Capability: 3
  CKN for participant: 1234
    Key server            : Yes
    MI (MN)               : A1E0D2897596817209CD2307 (2509)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 30 bytes
    Current SAK status    : Rx & Tx
    Current SAK AN        : 0
    Current SAK KI (KN)   : A1E0D2897596817209CD230700000002 (2)
    Previous SAK status   : N/A
    Previous SAK AN       : N/A
    Previous SAK KI (KN)  : N/A
    Live peer list:
    MI                        MN         Priority  Capability  Rx-SCI
    B2CAF896C9BFE2ABFB135E63  2512       0         3           00E0020000000106
```

Device-oriented MACsec configuration example

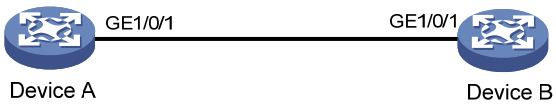
Network requirements

As shown in Figure 6, Device A is the MACsec key server.

To secure data transmission between the two devices by MACsec, perform the following tasks on Device A and Device B, respectively:

- Set the MACsec confidentiality offset to 30 bytes.
- Enable MACsec replay protection, and set the replay protection window size to 100.
- Set the MACsec validation mode to **strict**.
- Configure the CAK name (CKN) and the CAK as **E9AC** and **09DB3EF1**, respectively.

Figure 6 Network diagram



Configuration procedure

1. Configure Device A:

Enter system view.

```
<DeviceA> system-view
```

Enter GigabitEthernet 1/0/1 interface view.

```
[DeviceA] interface gigabitethernet 1/0/1
```

Enable MACsec desire on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] macsec desire
```

Set the MKA key server priority to 5.

```
[DeviceA-GigabitEthernet1/0/1] mka priority 5
```

Configure the CKN as **E9AC** and the CAK as **09DB3EF1** in plain text.

```
[DeviceA-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1
```

Set the MACsec confidentiality offset to 30 bytes.

```
[DeviceA-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

Enable MACsec replay protection.

```
[DeviceA-GigabitEthernet1/0/1] macsec replay-protection enable
```

Set the MACsec replay protection window size to 100.

```
[DeviceA-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

Set the MACsec validation mode to **strict**.

```
[DeviceA-GigabitEthernet1/0/1] macsec validation mode strict
```

Enable MKA on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] mka enable
[DeviceA-GigabitEthernet1/0/1] quit
```

2. Configure Device B:

Enter system view.

```
<DeviceB> system-view
```

Enter GigabitEthernet 1/0/1 interface view.

```
[DeviceB] interface gigabitethernet 1/0/1
```

Enable MACsec desire on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] macsec desire
```

Set the MKA key server priority to 10.

```
[DeviceB-GigabitEthernet1/0/1] mka priority 10
```

Configure the CKN as **E9AC** and the CAK as **09DB3EF1** in plain text.

```
[DeviceB-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1
```

Set the MACsec confidentiality offset to 30 bytes.

```
[DeviceB-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

Enable MACsec replay protection.

```
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection enable
```

Set the MACsec replay protection window size to 100.

```
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

Set the MACsec validation mode to **strict**.

```
[DeviceB-GigabitEthernet1/0/1] macsec validation mode strict
```

Enable MKA on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] mka enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display MACsec information on GigabitEthernet 1/0/1 of Device A.

```
[DeviceA] display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:05m:00s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 00E0020000000106
      Elapsed time: 00h:03m:18s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

Display MKA session information on GigabitEthernet 1/0/1 of Device A.

```
[DeviceA] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E00100000A0006
Priority  : 5
Capability: 3
  CKN for participant: E9AC
    Key server            : Yes
    MI (MN)               : 85E004AF49934720AC5131D3 (182)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 30 bytes
    Current SAK status    : Rx & Tx
```

```
    Current SAK AN        : 0
    Current SAK KI (KN)   : 85E004AF49934720AC5131D300000003 (3)
    Previous SAK status   : N/A
    Previous SAK AN       : N/A
    Previous SAK KI (KN)  : N/A
    Live peer list:
    MI                       MN         Priority  Capability  Rx-SCI
12A1677D59DD211AE86A0128  182        10        3           00E0020000000106
```

Display MACsec information on GigabitEthernet 1/0/1 of Device B.

```
[DeviceB] display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 00E0020000000106
      Elapsed time: 00h:05m:36s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:03m:21s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

Display MKA session information on GigabitEthernet 1/0/1 of Device B.

```
[DeviceB] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E0020000000106
Priority  : 10
Capability: 3
  CKN for participant: E9AC
    Key server            : No
    MI (MN)               : 12A1677D59DD211AE86A0128 (1219)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 30 bytes
    Current SAK status    : Rx & Tx
    Current SAK AN        : 0
    Current SAK KI (KN)   : 85E004AF49934720AC5131D300000003 (3)
    Previous SAK status   : N/A
    Previous SAK AN       : N/A
    Previous SAK KI (KN)  : N/A
```

```
Live peer list:
MI                          MN         Priority  Capability  Rx-SCI
85E004AF49934720AC5131D3  1216       5         3           00E00100000A0006
```

Troubleshooting MACsec

Cannot establish MKA sessions between MACsec devices

Symptom

The devices cannot establish MKA sessions when the following conditions exist:

- The link connecting the devices is up.
- The ports at the ends of the link are MACsec capable.

Analysis

The symptom might occur for the following reasons:

- The ports at the link are not enabled with MKA.
- A port at the link is not configured with a preshared key or configured with a preshared key different from the peer.

Solution

To resolve the problem:

1. Enter interface view.
2. Use the **display this** command to check the MACsec configuration:
   - If MKA is not enabled on the port, execute the **mka enable** command.
   - If a preshared key is not configured or the preshared key is different from the peer, use the **mka psk** command to configure a preshared key. Make sure the preshared key is the same as the preshared key on the peer.
3. If the problem persists, contact Hewlett Packard Enterprise support.

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.

Convention	Description
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

T

V