Hewlett Packard Enterprise

HPE FlexNetwork 5510 HI Switch Series

MACsec Command Reference

Part number: 5200-1246
Software version: Release 1118P02
Document version: 6W100-20160328

Acknowledgments

Contents

MACsec commands

confidentiality-offset

Use **confidentiality-offset** to set the MACsec confidentiality offset in an MKA policy.

Use **undo confidentiality-offset** to restore the default.

Syntax

confidentiality-offset *offset-value*

undo confidentiality-offset

Default

The MACsec confidentiality offset is 0. The entire frame is encrypted.

Views

MKA policy view

Predefined user roles

network-admin

Parameters

offset-value: Sets the confidentiality offset in bytes. The value can be 0, 30 or 50.

Usage guidelines

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.

When an MKA policy is applied to a port, the MACsec confidentiality offset in the policy overwrites the confidentiality offset previously configured on the port. However, MACsec uses the confidentiality offset propagated by the key server.

Examples

Set the MACsec confidentiality offset to 30 bytes in MKA policy **abcd**.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] confidentiality-offset 30
```

Related commands

- **macsec confidentiality-offset**
- **mka apply policy**

display macsec

Use **display macsec** to display MACsec information on ports.

Syntax

display macsec [**interface** *interface-type interface-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MACsec information on all ports.

verbose: Displays detailed MACsec information. If you do not specify this keyword, the command displays brief MACsec information.

Examples

Display brief MACsec information on GigabitEthernet 1/0/1.

```
<Sysname> display macsec interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Active MKA policy      : PL01
  Replay protection      : Enabled
  Replay window size     : 0 frames
  Confidentiality offset : 0 bytes
  Validation mode        : Strict
```

Display detailed MACsec information on GigabitEthernet 1/0/1.

```
<Sysname> display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Active MKA policy      : PL01
  Replay protection      : Enabled
  Replay window size     : 0 frames
  Confidentiality offset : 0 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 000C29F6A4380004
      Elapsed time: 00h:02m:19s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 000C29258D430124
      Elapsed time: 00h:02m:17s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

Table 1 Command output

Field	Description
Protect frames	Status of MACsec desire on the port: • **Yes**. • **No**. If the port does not have an MKA principal actor, this field displays **N/A**. NOTE: MKA instance refers to the operation entity of the MKA protocol on a port. A port might have multiple MKA instances. The principal actor is the MKA instance in active state.
Active MKA policy	MKA policy applied to the port. This field displays **N/A** if the port is not enabled with MACsec desire. This field is not available if the port is enabled with MACsec desire but is not applied an MKA policy.
Replay protection	Status of replay protection on the port: • **Enabled**. • **Disabled**. If the port is not enabled with MACsec desire, this field displays **N/A**.

Field	Description
Replay window size	Replay protection window size in number of frames. This field displays **N/A** in the following situations: • The port is not enabled with MACsec desire. • The port is not enabled with replay protection.
Confidentiality offset	Confidentiality offset in bytes. If the port is not enabled with MACsec desire, this field displays **N/A**.
Validation mode	Validation mode. In the current software version, only the **Strict** mode is supported. If the port is not enabled with MACsec desire, this field displays **N/A**.
Included SCI	Whether the frame includes SCI tag: • **Yes**. • **No**. If the port is not enabled with MACsec desire, this field displays **N/A**.
SCI conflict	Whether the SCI in the received MKA packets is the same as the local SCI: • **Yes**—The SCI in the received MKA packets is the same as the local SCI. • **No**—No MKA packet is received, or the SCI in the received MKA packets is different from the local SCI.
Cipher suite	If the port is not enabled with MACsec desire, this field displays **N/A**.
Transmit secure channel	Information about the secure channel for outbound traffic. This field is not available if the port is not enabled with MACsec desire.
Receive secure channel	Information about the secure channel for inbound traffic. This field is not available if the port is not enabled with MACsec desire.
Elapsed time	Lifetime of the secure channel.
SCI	A hexadecimal string that contains the MAC address and port ID.
Current SA	Current SA used by the secure channel. If no current SA is available, each of the AN, PN, and LPN fields for the current SA displays **N/A**.
Previous SA	Previous SA used by the secure channel. If no previous SA is available, each of the AN and LPN fields for the previous SA displays **N/A**.
PN	Packet number for outbound traffic.
AN	SA number.
LPN	The minimum received packet number allowed by SAK.

Related commands

mka apply policy

display mka policy

Use **display mka policy** to display MKA policy information.

Syntax

display mka { **default-policy** | **policy** [**name** *policy-name*] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

default-policy: Specifies the default MKA policy.

policy [**name** *policy-name*]: Specifies an MKA policy or all MKA policies. The *policy-name* argument represents the MKA policy name, a case-sensitive string of 1 to 16 characters. If you do not specify the **name** *policy-name* option, this command displays information about all MKA policies.

Examples

Display information about all MKA policies.

```
<Sysname> display mka policy
PolicyName          ReplayProtection   WindowSize    ConfOffset    Validation
default-policy      Yes                0             0             Strict
policy1             Yes                0             30            Strict
policy2             Yes                100           0             Strict
policy3             No                 0             0             Strict
policy4             Yes                200           50            Strict
policy5             Yes                0             0             Strict
```

Table 2 Command output

Field	Description
PolicyName	Name of the MKA policy.
ReplayProtection	Whether the replay protection function is enabled.
WindowSize	Replay protection window size in number of frames.
ConfOffset	Confidentiality offset in bytes.
Validation	Validation mode. In the current software version, only the **Strict** mode is supported.

Related commands

- **mka policy**
- **mka apply policy**

display mka session

Use **display mka session** to display MKA session information.

Syntax

display mka session [**interface** *interface-type interface-number* | **local-sci** *sci-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MKA session information on all ports.

local-sci *sci-id*: Specifies a local SCI, a case-insensitive hexadecimal string of 16 characters.

verbose: Displays detailed MKA session information. If you do not specify this keyword, the command displays brief MKA session information.

Examples

Display brief MKA session information on GigabitEthernet 1/0/1.

```
<Sysname> display mka session interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
Tx-SCI    : 000C29F6A4380004
Priority  : 0
Capability: 3
  CKN for participant: ABCD
    Key server            : Yes
    MI (MN)               : D7B00EDA353242704CC6B0DB (7)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 30 bytes
```

Display detailed MKA session information on GigabitEthernet 1/0/1.

```
<Sysname> display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 000C29F6A4380004
Priority  : 0
Capability: 3
  CKN for participant: ABCD
    Key server            : Yes
    MI (MN)               : D7B00EDA353242704CC6B0DB (7)
    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)   : 4273791304C1C26259C94C3400000001 (1)
    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
    EA58DC3F8715953DBC6593F0  840        100       3           00E0020000000106

    Potential peer list:
    MI                      MN         Priority  Capability  Rx-SCI
    DA58DC3Q4573543DBC6699F0  3          200       3           00E0021200000107
```

Table 3 Command output

Field	Description
Tx-SCI	SCI for outbound traffic, in hexadecimal notation.
Priority	Key server priority, in the range of 0 to 255.
Capability	MACsec capability: • **0**—The port is MACsec incapable. • **1**—The port supports integrity check only. • **2**—The port supports integrity check and packet encryption. The confidentiality offset must be 0.

Field	Description
	• **3**—The port supports integrity check and packet encryption. The confidentiality offset can be 0, 30, or 50.
CKN for participant	CAK name of the MKA instance.
Key server	Whether the local end is the key server.
MI	Member identifier in hexadecimal notation.
MN	Message number.
Live peers	Numbers of peers that have already been learned.
Potential peers	Numbers of peers that are being negotiated.
Principal actor	Whether the MKA instance is the principal actor.
MKA session status	MKA session status: • **Unknown**. • **Pending**. • **Unauthenticated**—The port has not been authenticated. • **Authenticated**—The port has passed the 802.1X authentication. • **Secured**—The session will be secured. If the MKA instance is not the principal actor, this field displays **N/A**.
Confidentiality offset	Confidentiality offset issued by the key server. This field displays **N/A** in the following situations: • The packet is transmitted in plain text. • The MKA instance is not the principal actor.
Current SAK status	Status of the current SAK: • **Tx**—The SAK is used to send packets. • **Rx**—The SAK is used to receive packets. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Current SAK AN	SA number of the current SAK in use. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Current SAK KI	Key identifier of the current SAK in use, a string of hexadecimal digits that contains the key server's 12-byte MI and KN. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
KN	SAK number. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Previous SAK status	Status of the previous SAK: • **Tx**—The SAK is used to send packets. • **Rx**—The SAK is used to receive packets. This field displays **N/A** in the following situations:

Field	Description
	• The MKA instance is not the principal actor. • The SAK does not exist.
Previous SAK AN	SA number of the previous SAK. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Previous SAK KI	Key identifier of the previous SAK, a string of hexadecimal digits that contains the key server's 12-byte MI and KN. This field displays **N/A** in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Live peer list	List of peers that have participated in the MKA session. This field is not available if no live peer exists.
Potential peer list	List of peers that are being negotiated. This field is not available if no potential peer exists.
Rx-SCI	SCI for inbound traffic, in hexadecimal notation.

Related commands

reset mka session

display mka statistics

Use **display mka statistics** to display MKA statistics on ports.

Syntax

display mka statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MKA statistics on all ports.

Examples

Display MKA statistics on GigabitEthernet 1/0/1.

```
<Sysname> display mka statistics interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1 statistics
MKPDUs with invalid CKN : 0
MKPDUs with invalid ICV : 0
MKPDUs with Rx error    : 0
CKN for participant     : ABCD
  Tx MKPDUs             : 2379
  Rx MKPDUs             : 2375
  MKPDUs with invalid MN: 0
  MKPDUs with Tx error  : 0
  SAKs distributed      : 0
  SAKs received         : 5
```

Table 4 Command output

Field	Description
MKPDUs with invalid CKN	Number of received MKA packets with invalid CKNs.
MKPDUs with invalid ICV	Number of MKA packets that failed ICV check.
MKPDUs with Rx error	Number of received error MKA packets.
CKN for participant	CAK name of the MKA instance.
Tx MKPDUs	Number of the MKA packets sent by the MKA instance.
Rx MKPDUs	Number of the MKA packets received by the MKA instance.
MKPDUs with invalid MN	Number of MKA packets with illegal MNs received by the MKA instance.
MKPDUs with Tx error	Number of error MKA packets sent by the MKA instance.
SAKs distributed	Number of SAKs distributed by the MKA instance.
SAKs received	Number of SAKs received by the MKA instance.

Related commands

reset mka statistics

macsec confidentiality-offset

Use **macsec confidentiality-offset** to set the MACsec confidentiality offset on a port.

Use **undo macsec confidentiality-offset** to restore the default.

Syntax

macsec confidentiality-offset *offset-value*

undo macsec confidentiality-offset

Default

The MACsec confidentiality offset on the port is 0. The entire frame is encrypted.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

offset-value: Sets the confidentiality offset in bytes. The value can be 0, 30 or 50.

Usage guidelines

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.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the confidentiality offset in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except the confidentiality offset) of the MKA policy are effective on the port.

MACsec uses the MACsec confidentiality offset propagated by the key server.

Examples

Set the MACsec confidentiality offset to 30 bytes on GigabitEthernet 1/0/1.
```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

Related commands

- **confidentiality-offset**
- **display macsec**
- **display mka session**
- **mka apply policy**

macsec desire

Use **macsec desire** to enable MACsec desire. The port expects MACsec protection for outbound frames.

Use **undo macsec desire** to restore the default.

Syntax

macsec desire

undo macsec desire

Default

MACsec desire is disabled. A port does not expect MACsec protection for outbound frames.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command allows a MACsec port to expect MACsec protection for outbound frames. The key server determines whether MACsec protects the outbound frames.

MACsec protects the outbound frames of the 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 the MACsec desire feature.

Examples

Enable MACsec desire on GigabitEthernet 1/0/1.
```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec desire
```

macsec replay-protection enable

Use **macsec replay-protection enable** to enable MACsec replay protection on a port.

Use **undo macsec replay-protection enable** to disable MACsec replay protection on a port.

Syntax

macsec replay-protection enable

undo macsec replay-protection enable

Default

MACsec replay protection is enabled on the port.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This function allows a MACsec port to accept a number of out-of-order or repeated inbound frames.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the MACsec replay protection configuration in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except MACsec replay protection) of the MKA policy are effective on the port.

Examples

Enable MACsec replay protection on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec replay-protection enable
```

Related commands

- **display macsec**
- **macsec replay-protection window-size**
- **mka apply policy**
- **replay-protection enable**

macsec replay-protection window-size

Use **macsec replay-protection window-size** to set the MACsec replay protection window size on a port.

Use **undo macsec replay-protection window-size** to restore the default.

Syntax

macsec replay-protection window-size *size-value*

undo macsec replay-protection window-size

Default

The MACsec replay protection window size is 0 on a port. Frames are accepted only in the correct order.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

size-value: Sets the replay protection window size, in the range of 0 to 4294967295 frames.

Usage guidelines

To allow a MACsec port to accept a number of out-of-order frames, enable replay protection and specify a replay protection window size on the port.

For example, the replay protection window size is **a** on a port. After the port receives a packet with packet number (PN) **x**, it can accept only packets whose PN is greater than or equal to **x-a**.

The replay protection window size takes effect only when the replay protection function is enabled on the port.

Set a replay protection window size based on the forwarding path of frames. If the frames might be forwarded multiple times, set a large replay protection window size.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the replay protection window size in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except the replay protection window size) of the MKA policy are effective on the port.

Examples

Set the MACsec replay protection window size to 100 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

Related commands

- **display macsec**
- **macsec replay-protection enable**
- **mka apply policy**
- **replay-protection window-size**

macsec validation mode

Use **macsec validation mode** to configure the MACsec validation mode on a port.

Use **undo macsec validation mode** to restore the default.

Syntax

macsec validation mode { **check** | **disabled** | **strict** }

undo macsec validation mode

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

check: Performs validation only and does not drop illegal frames.

disabled: Does not perform validation.

strict: Performs validation and drops illegal frames.

Usage guidelines

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

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the validation mode in the MKA policy. The MKA policy application is removed from the

port. However, other settings (settings for parameters except the validation mode) of the MKA policy are effective on the port.

Examples

Set the MACsec validation mode to **strict** on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec validation mode strict
```

Related commands

- **display macsec**
- **mka apply policy**
- **validation mode**

mka apply policy

Use **mka apply policy** to apply an MKA policy to a port.

Use **undo mka apply policy** to remove the MKA policy from a port.

Syntax

mka apply policy *policy-name*

undo mka apply policy

Default

No MKA policy is applied to the port.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an MKA policy, a case-sensitive string of 1 to 16 characters.

Usage guidelines

An MKA policy defines MACsec parameters, including confidentiality offset, validation mode, replay protection, and replay protection window size.

When you apply an MKA policy to a port, the MACsec parameter settings in the policy overwrite the MACsec parameters previously configured on the port. Any modifications to the MKA policy take effect immediately.

When you remove the MKA policy from a port, the MACsec parameter settings on the port restore to the default.

When you delete an MKA policy, ports that use the policy automatically use the default MKA policy named **default-policy**.

When you apply a nonexistent MKA policy to a port, the port automatically uses the default MKA policy. After you create the specified policy, the policy will be automatically applied to the port.

Examples

Apply MKA policy **abcd** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka apply policy abcd
```

Related commands

- **confidentiality-offset**
- **display mka policy**
- **replay-protection enable**
- **replay-protection window-size**
- **validation mode**

mka enable

Use **mka enable** to enable MKA on a port.

Use **undo mka enable** to disable MKA on a port.

Syntax

mka enable

undo mka enable

Default

MKA is disabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

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

The enabling of MKA on a port triggers MKA negotiation. After MKA negotiation succeeds, an MKA session is successfully established.

Examples

Enable MKA on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka enable
```

Related commands

display mka session

mka policy

Use **mka policy** to create an MKA policy, and enter MKA policy view. If the MKA policy already exists, the command enters MKA policy view directly.

Use **undo mka policy** to delete an MKA policy.

Syntax

mka policy *policy-name*

undo mka policy *policy-name*

Default

The default MKA policy **default-policy** exists.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an MKA policy, a case-sensitive string of 1 to 16 characters.

Usage guidelines

MKA policy provides a centralized method for configuring MACsec confidentiality offset, validation mode, replay protection, and replay protection window size. An MKA policy can be applied to multiple ports.

You cannot delete or modify the default MKA policy.

Examples

Create an MKA policy named **abcd**, and enter MKA policy view.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd]
```

Related commands

- **confidentiality-offset**
- **display mka policy**
- **mka apply policy**
- **replay-protection enable**
- **replay-protection window-size**
- **validation mode**

mka priority

Use **mka priority** to configure the MKA key server priority.

Use **undo mka priority** to restore the default.

Syntax

mka priority *priority-value*

undo mka priority

Default

The MKA key server priority is 0.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Sets the priority value, in the range of 0 to 255. The priority is inversely related to its value.

Usage guidelines

If you use 802.1 X-generated CAK, the access device port automatically becomes the key server.

If you use a preshared key as the CAK, the port that has higher priority (lower priority value) becomes the key server. If the port and its peers have the same priority, MACsec compares the SCI values on the ports. The port with the lowest SCI value 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.

Examples

Set the MKA key server priority to 2 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka priority 2
```

Related commands

display mka session

mka psk

Use **mka psk** to configure a preshared key as the CAK.

Use **undo mka psk** to delete the configured preshared key.

Syntax

mka psk ckn *name* **cak simple** *value*

undo mka psk

Default

No preshared key exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ckn *name*: Specifies the preshared key name, a hexadecimal string with an even number of case-insensitive characters. The name length is in the range of 2 to 64 characters.

cak: Specifies the preshared key.

simple: Specifies a plaintext preshared key.

value: Specifies the plaintext key, a hexadecimal string with an even number of case-insensitive characters. The key length is in the range of 2 to 64 characters.

Usage guidelines

The CAK can be either generated during 802.1X or manually configured at the CLI. The manually configured CAK takes precedence over the 802.1X-generated key. To ensure a successful MKA session establishment, do not configure a preshared key in client-oriented mode.

In device-oriented mode, you must execute this command to configure a preshared key on each MACsec port. Make sure the local port and peer ports are configured with the same key. If the connected ports are configured with different keys, they cannot successfully establish MKA sessions.

To delete the configured keys for MKA sessions that have been established, perform the following tasks:

1. Execute the **undo mka psk** command on the key server.
2. Execute the **undo mka psk** command on the non-key server.

The deletion operation deletes the established MKA sessions at the same time.

The MACsec cipher suite supported by HP devices requires that the configured 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.

Examples

Configure the CAK name as **AB**, and set the CAK to **1234** in plain text on Gigabit Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka psk ckn AB cak simple 1234
```

replay-protection enable

Use **replay-protection enable** to enable MACsec replay protection in an MKA policy.

Use **undo replay-protection enable** to disable MACsec replay protection.

Syntax

replay-protection enable

undo replay-protection enable

Default

MACsec replay protection is enabled.

Views

MKA policy view

Predefined user roles

network-admin

Usage guidelines

This function allows a MACsec port to accept a number of out-of-order or repeated inbound frames.

When an MKA policy is applied to a port, the replay protection configuration in the policy overwrites the replay protection function already used by the port.

Examples

Enable MACsec replay protection in MKA policy **abcd**.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] replay-protection enable
```

Related commands

- **macsec replay-protection enable**
- **mka apply policy**
- **replay-protection window-size**

replay-protection window-size

Use **replay-protection window-size** to set the MACsec replay protection window size in an MKA policy.

Use **undo replay-protection window-size** to restore the default.

Syntax

replay-protection window-size *size-value*

undo replay-protection window-size

Default

The MACsec replay protection window size in an MKA policy is 0. Frames are accepted only in the correct order.

Views

MKA policy view

Predefined user roles

network-admin

Parameters

size-value: Sets the replay protection window size, in the range of 0 to 4294967295 frames.

Usage guidelines

The MACsec replay protection window size allows a MACsec port to accept a number of out-of-order inbound frames.

For example, the replay protection window size is **a** on a port. After the port receives a packet with PN **x**, it can accept only packets whose PN is greater than or equal to **x-a**.

The replay protection window size takes effect only when the replay protection function is enabled on the port.

Set a replay protection window size based on the forwarding path of frames. If the frames might be forwarded multiple times, set a large replay protection window size.

When an MKA policy is applied to a port, the replay protection window size in the policy overwrites the window size already configured on the port.

Examples

Set the MACsec replay protection window size to 100 in MKA policy **abcd**.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] replay-protection window-size 100
```

Related commands

- **macsec replay-protection window-size**
- **macsec replay-protection enable**
- **mka apply policy**

reset mka session

Use **reset mka session** to reset MKA sessions on ports.

Syntax

reset mka session [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command resets MKA sessions on all ports.

Usage guidelines

This command first clears MKA sessions, and then immediately triggers a new session establishment negotiation.

Examples

Reset MKA sessions on GigabitEthernet 1/0/1.
```
<Sysname> reset mka session interface gigabitethernet 1/0/1
```

Related commands

display mka session

reset mka statistics

Use **reset mka statistics** to clear MKA statistics on ports.

Syntax

reset mka statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears MKA statistics on all ports.

Examples

Clear MKA statistics on GigabitEthernet 1/0/1.
```
<Sysname> reset mka statistics interface gigabitethernet 1/0/1
```

Related commands

display mka statistics

validation mode

Use **validation mode** to configure the MACsec validation mode in an MKA policy.

Use **undo validation mode** to restore the default.

Syntax

validation mode { **check** | **disabled** | **strict** }

undo validation mode

Views

MKA policy view

Predefined user roles

network-admin

Parameters

check: Performs validation only and does not drop illegal frames.

disabled: Does not perform validation.

strict: Performs validation and drops illegal frames.

Usage guidelines

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

When an MKA policy is applied to a port, the MACsec validation mode in the policy overwrites the MACsec validation mode already configured on the port.

Examples

Set the MACsec validation mode to **strict** in MKA policy **abcd**.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] validation mode strict
```

Related commands

- **macsec validation mode**
- **mka apply policy**

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.
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