



Configuring MACsec Encryption

This chapter describes how to configure Media Access Control Security (MACsec) encryption on the Catalyst 4500 series switch.

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. The Catalyst 4500 series switch supports 802.1AE encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the switch and host devices. The switch also supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).



Note

MACsec is supported on the Catalyst 4500 series switch universal k9 image. It is not supported with the NPE license or with a LAN Base service image.

All downlink ports on a switch can run Cisco TrustSec MACsec link layer switch-to-switch security.

Table 1 *MACsec Support on Switch Ports*

Interface	Connections	MACsec support
User-facing downlink ports	Switch-to-host	MKA MACsec encryption
Switchports connected to other switches	Switch-to-switch	Cisco TrustSec NDAC MACsec

Cisco TrustSec and Cisco SAP are meant only for switch-to-switch links and are not supported on switch ports connected to end hosts, such as PCs or IP phones. MKA is meant for switch-to-host facing links and is not supported on switch-to-switch links. Host-facing links typically use flexible authentication ordering for handling heterogeneous devices with or without IEEE 802.1X, and can optionally use MKA encryption. Cisco NDAC and SAP are mutually exclusive with Network Edge Access Topology (NEAT), which is used for compact switches to extend security outside the wiring closet.

- [Understanding Media Access Control Security and MACsec Key Agreement, page 45-2](#)
- [Configuring MACsec and MACsec Key Agreement, page 45-6](#)
- [Understanding Cisco TrustSec MACsec, page 45-8](#)
- [Configuring Cisco TrustSec MACsec, page 45-10](#)

For more information on TrustSec, refer to the following URL:

<http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html>

Understanding Media Access Control Security and MACsec Key Agreement

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1X Extensible Authentication Protocol (EAP) framework. Only host facing links (links between network access devices and endpoint devices such as a PC or IP phone) can be secured using MACsec.

A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the client. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the client, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a client) using the current session key.

The MKA Protocol manages the encryption keys used by the underlying MACsec protocol. The basic requirements of MKA are defined in 802.1X-2010. The MKA Protocol extends 802.1X to allow peer discovery with confirmation of mutual authentication and sharing of MACsec secret keys to protect data exchanged by the peers.

The EAP framework implements MKA as a newly defined EAP-over-LAN (EAPOL) packet. EAP authentication produces a master session key (MSK) shared by both partners in the data exchange. Entering the EAP session ID generates a secure connectivity association key name (CKN). Because the switch is the authenticator, it is also the key server, generating a random 128-bit secure association key (SAK), which it sends it to the client partner. The client is never a key server and can only interact with a single MKA entity, the key server. After key derivation and generation, the switch sends periodic transports to the partner at a default interval of 2 seconds.

The packet body in an EAPOL Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). MKA sessions and participants are deleted when the MKA lifetime (6 seconds) passes with no MKPDU received from a participant. For example, if a client disconnects, the participant on the switch continues to operate MKA until 6 seconds have elapsed after the last MKPDU is received from the client.

These sections provide more details:

- [MKA Policies, page 45-2](#)
- [Virtual Ports, page 45-3](#)
- [MACsec, page 45-3](#)
- [MACsec, MKA, and 802.1X Host Modes, page 45-3](#)
- [MKA Statistics, page 45-4](#)

MKA Policies

You apply a defined MKA policy to an interface to enable MKA on the interface. Removing the MKA policy disables MKA on that interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.

- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface.
- Replay protection. You can configure MACsec window size, as defined by the number of out-of-order frames that are accepted. This value is used while installing the security associations in the MACsec. A value of 0 means that frames are accepted only in the correct order.

**Note**

MKA is not supported in the Virtual Switching System (VSS) mode.

Virtual Ports

You use virtual ports for multiple secured connectivity associations on a single physical port. Each connectivity association (pair) represents a virtual port, with a maximum of two virtual ports per physical port. Only one of the two virtual ports can be part of a data VLAN; the other must externally tag its packets for the voice VLAN. You cannot simultaneously host secured and unsecured sessions in the same VLAN on the same port. Because of this limitation, 802.1X multiple authentication mode is not supported.

The exception to this limitation is in multiple-host mode when the first MACsec supplicant is successfully authenticated and connected to a hub that is connected to the switch. A non-MACsec host connected to the hub can send traffic without authentication because it is in multiple-host mode. We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients.

Virtual ports represent an arbitrary identifier for a connectivity association and have no meaning outside the MKA Protocol. A virtual port corresponds to a separate logical port ID. Valid port IDs for a virtual port are 0x0002 to 0xFFFF. Each virtual port receives a unique secure channel identifier (SCI) based on the MAC address of the physical interface concatenated with a 16-bit port ID.

MACsec

A Catalyst 4500 series switch running MACsec maintains the configuration files that show which ports on a member switch support MACsec. The stack master performs these functions:

- Processes secure channel and secure association creation and deletion.
- Sends secure association service requests to the stack members.
- Processes packet number and replay-window information from local or remote ports and notifies the key management protocol.
- Sends MACsec initialization requests with the globally configured options to new switches that are added to the stack.
- Sends any per-port configuration to the member switches.

A member switch performs these functions:

- Processes MACsec initialization requests from the stack master.
- Processes MACsec service requests sent by the stack master.
- Sends information about local ports to the stack master.

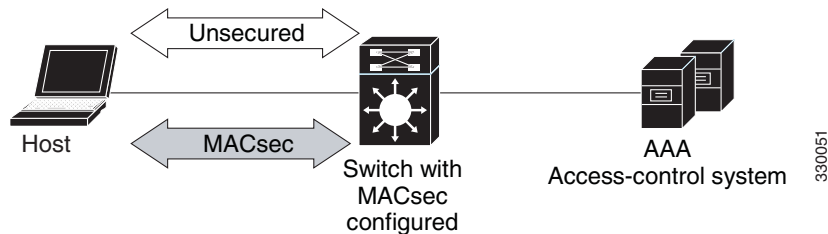
MACsec, MKA, and 802.1X Host Modes

You can use MACsec and the MKA Protocol with 802.1X single-host mode, multiple-host mode, or Multi Domain Authentication (MDA) mode. Multiple authentication mode is not supported.

Single-Host Mode

Figure 45-1 shows how a single EAP authenticated session is secured by MACsec using MKA.

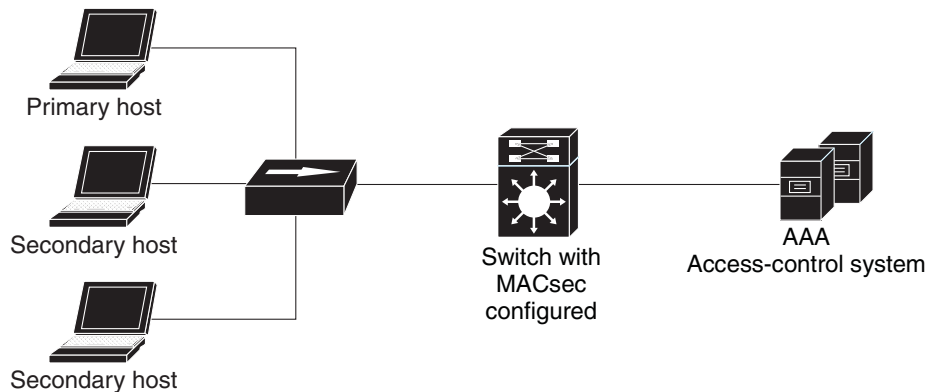
Figure 45-1 *MACsec in Single-Host Mode with a Secured Data Session*



Multiple-Host Mode

In standard (not 802.1X-2010) 802. multiple-host mode, a port is open or closed based on a single authentication. If one user, the primary secured client services client host, is authenticated, the same level of network access is provided to any host connected to the same port. If a secondary host is a MACsec supplicant, it cannot be authenticated and traffic would no flow. A secondary host that is a non-MACsec host can send traffic to the network without authentication because it is in multiple-host mode. See Figure 45-2.

Figure 45-2 *MACsec in Standard Multiple-Host Mode - Unsecured*



We do not recommend using multi-host mode because after the first successful client, authentication is not required for other clients, which is not secure.

MKA Statistics

Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

This is an example of the **show mka statistics** command output:

```

Switch# show mka statistics
MKA Global Statistics
=====
MKA Session Totals
  Secured..... 32
  Reauthentication Attempts.. 31

  Deleted (Secured)..... 1
  Keepalive Timeouts..... 0

CA Statistics
  Pairwise CAKs Derived..... 32
  Pairwise CAK Rekeys..... 31
  Group CAKs Generated..... 0
  Group CAKs Received..... 0

SA Statistics
  SAKs Generated..... 32
  SAKs Rekeyed..... 31
  SAKs Received..... 0
  SAK Responses Received..... 32

MKPDU Statistics
  MKPDUs Validated & Rx..... 580
    "Distributed SAK"..... 0
    "Distributed CAK"..... 0
  MKPDUs Transmitted..... 597
    "Distributed SAK"..... 32
    "Distributed CAK"..... 0

MKA Error Counter Totals
=====
Bring-up Failures..... 0
Reauthentication Failures..... 0

SAK Failures
  SAK Generation..... 0
  Hash Key Generation..... 0
  SAK Encryption/Wrap..... 0
  SAK Decryption/Unwrap..... 0

CA Failures
  Group CAK Generation..... 0
  Group CAK Encryption/Wrap..... 0
  Group CAK Decryption/Unwrap..... 0
  Pairwise CAK Derivation..... 0
  CKN Derivation..... 0
  ICK Derivation..... 0
  KEK Derivation..... 0
  Invalid Peer MACsec Capability.. 2

MACsec Failures
  Rx SC Creation..... 0
  Tx SC Creation..... 0
  Rx SA Installation..... 0
  Tx SA Installation..... 0

MKPDU Failures
  MKPDU Tx..... 0
  MKPDU Rx Validation..... 0
  MKPDU Rx Bad Peer MN..... 0
  MKPDU Rx Non-recent Peerlist MN.. 0

```

For description of the output fields, see the command reference for this release.

Configuring MACsec and MACsec Key Agreement

- [Default MACsec MACsec Key Agreement Configuration, page 45-6](#)
- [Configuring an MKA Policy, page 45-6](#)
- [Configuring MACsec on an Interface, page 45-7](#)

Default MACsec MACsec Key Agreement Configuration

MACsec is disabled. No MACsec Key Agreement (MKA) policies are configured.

Configuring an MKA Policy

To create an MKA Protocol policy, perform this task. Note that MKA also requires that you enable 802.1X.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>mka policy <i>policy-name</i></code>	Identifies an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters.
Step 3	<code>replay-protection window-size <i>frames</i></code>	Enables replay protection, and configure the window size in number of frames. The range is from 0 to 4294967295. The default window size is 0. Entering a window size of 0 is not the same as entering the no replay-protection command. Configuring a window size of 0 uses replay protection with a strict ordering of frames. Entering no replay-protection turns off MACsec replay-protection.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show mka policy</code>	Verifies your entries.
Step 6	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

This example configures the MKA policy *relay-policy*:

```
Switch(config)# mka policy relay-policy
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

Let's say that we configure an MKA policy as follows:

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mka policy pol1
Switch(config-mka-policy)# replay-protection window-size 1000
Switch(config-mka-policy)# confidentiality-offset 50
Switch(config-mka-policy)# end
```

We observe the following:

- The payload starting from the SA (source MAC address) + 50 bytes offset is encrypted.
- Replay protect is YES with a window size of 1000. If the frame received has a packet number (PN) of 1020, for example, all frames with a PN of 20 to 1020 can come out of order (i.e, frame with PN 900 can come first and frame with PN 800 can come later). However, if a frame with a PN of 1021 is received first, followed by a frame with a PN of 20, the frame with PN of 20 is dropped. In this scenario, the expected PN is 1022 and the window size is 1000, so the acceptable PN number is anything greater than or equal to (expected PN - window size) = 22. So, any frame with PN < 22 is dropped.

To apply the MKA protocol default policy on an interface, use the **mka default-policy** interface configuration command. This command also enables MKA on the interface if no MKAs were applied.

When we configure the MKA default policy, all the values in the policy (such as confidentiality, offset, and replay protection) take the default values. For example,

- Confidentiality offset is 0—Encrypts the payload that is immediately after the SA (source MAC address).
- Replay protect is YES with window size 0—Frames cannot come out of order.

Configuring MACsec on an Interface

To configure MACsec on an interface with one MACsec session for voice and one for data, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.
Step 3	<code>switchport access vlan vlan-id</code>	Configures the access VLAN for the port.
Step 4	<code>switchport mode access</code>	Configures the interface as an access port.
Step 5	<code>macsec</code>	Enables 802.1ae MACsec on the interface.
Step 6	<code>authentication event linksec fail action authorize vlan vlan-id</code>	(Optional) Specifies that the switch processes authentication link-security failures resulting from unrecognized user credentials by authorizing a restricted VLAN on the port after a failed authentication attempt.
Step 7	<code>authentication host-mode multi-domain</code>	Configures authentication manager mode on the port to allow both a host and a voice device to be authenticated on the 802.1X-authorized port. If not configured, the default host mode is single.
Step 8	<code>authentication linksec policy must-secure</code>	Sets the LinkSec security policy to secure the session with MACsec if the peer is available. If not set, the default is <i>should secure</i> .
Step 9	<code>authentication port-control auto</code>	Enables 802.1X authentication on the port. The port changes to the authorized or unauthorized state based on the authentication exchange between the switch and the client
Step 10	<code>mka policy policy-name</code>	Applies an existing MKA protocol policy to the interface, and enable MKA on the interface. If no MKA policy was configured (by entering the mka policy global configuration command), you must apply the MKA default policy to the interface by entering the mka default-policy interface configuration command.
Step 11	<code>dot1x pae authenticator</code>	Configures the port as an 802.1X port access entity (PAE) authenticator.

	Command	Purpose
Step 12	<code>spanning-tree portfast</code>	Enables spanning tree Port Fast on the interface in all its associated VLANs. When Port Fast feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.
Step 13	<code>end</code>	Returns to privileged EXEC mode.
Step 14	<code>show authentication session interface interface-id</code>	Verifies the authorized session security status.
Step 15	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

This is an example of configuring and verifying MACsec on an interface:

```
Switch(config)# interface GigabitEthernet1/0/25
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
Switch(config-if)# authentication port-control auto
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch# show authentication sessions interface gigabitethernet1/0/25
Interface: GigabitEthernet1/0/25
MAC Address: 001b.2140.ec3c
IP Address: 1.1.1.103
User-Name: ms1
Status: Authz Success
Domain: DATA
Security Policy: Must Secure β--- New
Security Status: Secured β--- New
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 10
Session timeout: 3600s (server), Remaining: 3567s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A05783B0000001700448BA8
Acct Session ID: 0x00000019
Handle: 0x06000017
Runnable methods list:
Method State
dot1x Authc Success
```

Understanding Cisco TrustSec MACsec



Note

MACsec is supported on the Catalyst 4500 series switch universal k9 image. It is not supported with the NPE license or with a LAN Base service image.

Table 45-2 summarizes the Cisco TrustSec features supported on the switch. For more detailed explanations, see the *Cisco TrustSec Switch Configuration Guide*:

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html#wp1054561

Table 45-2 Cisco TrustSec Features

Cisco TrustSec Feature	Description
802.1AE Encryption (MACsec)	<p>Protocol for 802.1AE-based wire-rate hop-to-hop Layer 2 encryption.</p> <p>Between MACsec-capable devices, packets are encrypted on egress from the sending device, decrypted on ingress to the receiving device, and in the clear within the devices.</p> <p>This feature is only available between 802.1AE-capable devices.</p>
Network Device Admission Control (NDAC)	<p>NDAC is an authentication process by which each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC uses an authentication framework based on IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol Flexible Authentication via Secure Tunnel (EAP-FAST) as its EAP method. Authentication and authorization by NDAC results in Security Association Protocol negotiation for 802.1AE encryption.</p>
Security Association Protocol (SAP)	<p>SAP is a Cisco proprietary key exchange protocol between switches. After NDAC switch-to-switch authentication, SAP automatically negotiates keys and the cipher suite for subsequent switch-to-switch MACsec encryption between TrustSec peers. The protocol description is available under a nondisclosure agreement.</p>
Security Group Tag (SGT) Note SGT is not supported in this release.	<p>An SGT is a 16-bit single label showing the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.</p>
SGT Exchange Protocol (SXP), including SXPv2	<p>With SXP, devices that are not TrustSec-hardware capable can receive SGT attributes for authenticated users or devices from the Cisco Access Control System (ACS). The devices then forward the source IP-to-SGT binding to a TrustSec-hardware capable device for tagging and security group ACL (SGACL) enforcement.</p>

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Cisco TrustSec uses AES-128 GCM and GMAC and is compliant with the 802.1AE standard. GCM is not supported on switches running the NPE or the LAN Base image.

Cisco TrustSec NDAC SAP is supported on trunk ports because it is intended only for network device to network device links, that is, switch-to-switch links. It is not supported on:

- Host facing access ports (these ports support MKA MACsec)
- Switch virtual interfaces (SVIs)
- SPAN destination ports

The switch also does not support security group ACLs.

You must set the Cisco TrustSec credentials to create the Cisco TrustSec network.

You can configure Cisco TrustSec link layer security in 802.1X mode or manual mode.

Configuring Cisco TrustSec MACsec



Note

MACsec is supported on the Catalyst 4500 series switch universal k9 image. It is not supported with the NPE license or with a LAN Base service image.

Following topics are discussed:

- [Configuring Cisco TrustSec Credentials on the Switch, page 45-10](#)
- [Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1X Mode, page 45-11](#)
- [Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode, page 45-12](#)
- [Cisco TrustSec Switch-to-Switch Link Security Configuration Example, page 45-14](#)



Note

The sample configuration in the last section shows the AAA and the RADIUS configuration. Use this example to configure RADIUS and AAA before configuring switch-to-switch security.

Configuring Cisco TrustSec Credentials on the Switch

To enable Cisco TrustSec features, you must create Cisco TrustSec credentials on the switch to use in other TrustSec configurations.

To configure Cisco TrustSec credentials, perform this task:

	Command	Purpose
Step 1	<code>cts credentials id device-id password</code> <i>cts-password</i>	Specifies the Cisco TrustSec credentials for this switch to use when authenticating with other Cisco TrustSec devices with EAP-FAST. <ul style="list-style-type: none"> • id device-id—Specifies a Cisco TrustSec device ID for the switch. The device-id argument has a maximum length of 32 characters and is case sensitive. • password cts-password—Specifies the Cisco TrustSec password for the device.
Step 2	<code>show cts credentials</code>	(Optional) Displays Cisco TrustSec credentials configured on the switch.
Step 3	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

To delete the Cisco TrustSec credentials, enter the **clear cts credentials** privileged EXEC command.

This example shows how to create Cisco TrustSec credentials:

```
Switch# cts credentials id trustsec password mypassword
CTS device ID and password have been inserted in the local keystore. Please make
sure that the same ID and password are configured in the server database.

Switch# show cts credentials
CTS password is defined in keystore, device-id = trustsecchange-password Initiate
password change with AAA server
```



Note

Before you configure Cisco TrustSec MACsec authentication, you should configure Cisco TrustSec seed and non-seed devices. For 802.1X mode, you must configure at least one seed device, that device closest to the access control system (ACS). See this section in the *Cisco TrustSec Switch Configuration Guide*:

<http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html>

Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1X Mode

You enable Cisco TrustSec link layer switch-to-switch security on an interface that connects to another Cisco TrustSec device. When configuring Cisco TrustSec in 802.1X mode on an interface, follow these guidelines:

- To use 802.1X mode, you must globally enable 802.1X on each device.
- If you select GCM as the SAP operating mode, you must have a MACsec encryption software license from Cisco.




Note

MACsec is supported on the Catalyst 4500 series switch universal k9 image. It is not supported with the NPE license or with a LAN Base service image.

If you select GCM without the required license, the interface is forced to a link-down state.

To configure Cisco TrustSec switch-to-switch link layer security with 802.1X, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Enters interface configuration mode.
Step 3	<code>cts dot1x</code>	Configures the interface to perform NDAC authentication.

	Command	Purpose
Step 4	<code>sap mode-list mode1 [mode2 [mode3 [mode4]]]</code>	<p>(Optional) Configures the SAP operation mode on the interface. The interface negotiates with the peer for a mutually acceptable mode. Enter the acceptable modes in your order of preference.</p> <p>Choices for <i>mode</i> are:</p> <ul style="list-style-type: none"> • gcm-encrypt—Authentication and encryption <p>Note Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</p> <ul style="list-style-type: none"> • gmac—Authentication, no encryption • no-encap—No encapsulation • null—Encapsulation, no authentication or encryption <p>Note If the interface is not capable of data link encryption, no-encap is the default and the only available SAP operating mode. SGT is not supported.</p>
		
	Note	Although visible in the CLI help, the timer reauthentication and propagate sgt keywords are not supported. However, the no propagate sgt keyword is supported (refer to Step 5 in the next section).
Step 5	<code>exit</code>	Exits Cisco TrustSec 802.1X interface configuration mode.
Step 6	<code>end</code>	Returns to privileged EXEC mode.
Step 7	<code>show cts interface [interface-id / brief / summary]</code>	(Optional) Verifies the configuration by displaying TrustSec-related interface characteristics.
Step 8	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

This example shows how to enable Cisco TrustSec authentication in 802.1X mode on an interface using GCM as the preferred SAP mode:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode

If your switch does not have access to an authentication server or if 802.1X authentication is not needed, you can manually configure Cisco TrustSec on an interface. You must manually configure the interface on each end of the connection.

When manually configuring Cisco TrustSec on an interface, consider these usage guidelines and restrictions:

- If no SAP parameters are defined, neither encryption nor MACsec Encapsulation are performed.
- If you select GCM as the SAP operating mode, you must have a MACsec Encryption software license from Cisco. If you select GCM without the required license, the interface is forced to a link-down state.

- These protection levels are supported when you configure SAP pairwise master key (**sap pmk**):
 - SAP is not configured—no protection.
 - **sap mode-list gcm-encrypt gmac no-encap**—protection desirable but not mandatory.
 - **sap mode-list gcm-encrypt gmac**—confidentiality preferred and integrity required. The protection is selected by the supplicant according to supplicant preference.
 - **sap mode-list gmac**—integrity only.
 - **sap mode-list gcm-encrypt**—confidentiality required.
 - **sap mode-list gmac gcm-encrypt**—integrity required and preferred, confidentiality optional.

To manually configure Cisco TrustSec on an interface to another Cisco TrustSec device, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Enters interface configuration mode.
Step 3	<code>cts manual</code>	Enters Cisco TrustSec manual configuration mode.
Step 4	<code>sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]</code>	<p>(Optional) Configures the SAP pairwise master key (PMK) and operation mode. SAP is disabled by default in Cisco TrustSec manual mode.</p> <ul style="list-style-type: none"> • <i>key</i>—A hexadecimal value with an even number of characters and a maximum length of 32 characters. <p>The SAP operation <i>mode</i> options:</p> <ul style="list-style-type: none"> • gcm-encrypt—Authentication and encryption <p>Note Select this mode for MACsec authentication and encryption if your software license supports MACsec encryption.</p> <ul style="list-style-type: none"> • gmac—Authentication, no encryption • no-encap—No encapsulation • null—Encapsulation, no authentication or encryption <p>Note If the interface is not capable of data link encryption, no-encap is the default and the only available SAP operating mode. SGT is not supported.</p>
Step 5	<code>no propagate sgt</code>	<p>Prevents the interface from transmitting the SGT to the peer and is required in manual mode.</p> <p>Use the no form of this command when the peer is incapable of processing a SGT.</p>
Step 6	<code>exit</code>	Exits Cisco TrustSec 802.1X interface configuration mode.
Step 7	<code>end</code>	Returns to privileged EXEC mode.
Step 8	<code>show cts interface [interface-id brief summary]</code>	(Optional) Verifies the configuration by displaying TrustSec-related interface characteristics.
Step 9	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

This example shows how to configure Cisco TrustSec authentication in manual mode on an interface:

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

Cisco TrustSec Switch-to-Switch Link Security Configuration Example

This example shows the configuration necessary for a seed and non-seed device for Cisco TrustSec switch-to-switch security. You must configure the AAA and RADIUS for link security. In this example, *ACS-1* through *ACS-3* can be any server names and *cts-radius* is the Cisco TrustSec server.

Seed Device Configuration:

```
Switch(config)# aaa new-model
Switch(config)# radius server ACS-1 address ipv4 10.5.120.12 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# radius server ACS-2 address ipv4 10.5.120.14 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# radius server ACS-3 address ipv4 10.5.120.15 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# aaa group server radius cts-radius
Switch(config-sg-radius)# server name ACS-1
Switch(config-sg-radius)# server name ACS-2
Switch(config-sg-radius)# server name ACS-3
Switch(config-sg-radius)# exit
Switch(config)# aaa authentication login default none
Switch(config)# aaa authentication dot1x default group cts-radius
Switch(config)# aaa authentication network cts-radius group radius
Switch(config)# aaa session-id common
Switch(config)# cts authorization list cts-radius
Switch(config)# dot1x system-auth-control

Switch(config)# interface g1/1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)# exit

Switch(config)# interface g1/1/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-dot1x)# sap pmk 033445AABCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-36 password trustsec123
```

Non-Seed Device:

```
Switch(config)# aaa new-model
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control

Switch(config)# interface g11/1/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface g11/1/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
Switch(config-if-cts-dot1x)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-72 password trustsec123
```

