Identity-Based Networking Services: MAC Security

Deployment Guide

May, 2011

Contents

1. Introduction

The need for secure network access has never been greater. In today's diverse workplaces, consultants, contractors, and even guests require access to network resources over the same LAN connections as regular employees, who may themselves bring unmanaged devices into the workplace. As data networks become increasingly indispensable in day-to-day business operations, the possibility that unauthorized people or devices will gain access to controlled or confidential information also increases.

The best and most secure solution to vulnerability at the access edge is to use the intelligence of the network. IEEE 802.1X provides port-based access control using authentication, but authentication alone does not guarantee the confidentiality and integrity of data on the LAN. While physical security and end-user awareness can mitigate threats to data on an IEEE 802.1X–authenticated LAN, there may be situations or locations (such as remote offices or publicly accessible areas) in which the LAN needs additional protection. When additional protection is needed, Cisco IOS® Software enables data confidentiality and integrity on the LAN by using MAC Security (MACsec). Defined by the IEEE 802.1AE standard, MACsec secures communication for authorized endpoints on the LAN.

This document focuses on deployment consideration specific to MACsec in the campus access layer.

2. About MACsec

2.1 Benefits and Limitations

MACsec offers the following benefits on wired networks:

- **Confidentiality:** MACsec helps ensure data confidentiality by providing strong encryption at Layer 2.
- **Integrity:** MACsec provides integrity checking to help ensure that data cannot be modified in transit.
- **Flexibility:** You can selectively enable MACsec using a centralized policy, thereby helping ensure that MACsec is enforced where required while allowing non-MACsec-capable components to access the network.
- **Network intelligence:** Unlike end-to-end, Layer 3 encryption techniques that hide the contents of packets from the network devices they cross, MACsec encrypts packets on a hop-by-hop basis at Layer 2, allowing the network to inspect, monitor, mark, and forward traffic according to your existing policies.

Although MACsec offers outstanding data security, it has limitations that must be addressed by your design:

- **Endpoint support:** Not all endpoints support MACsec.
- **Hardware support:** Line-rate encryption typically requires updated hardware on the access switch.
- **Technology integration:** Enabling MACsec may affect the functions of other technologies that also connect at the access edge, such as IP telephony. Understanding and accommodating these technologies is essential to a successful deployment.

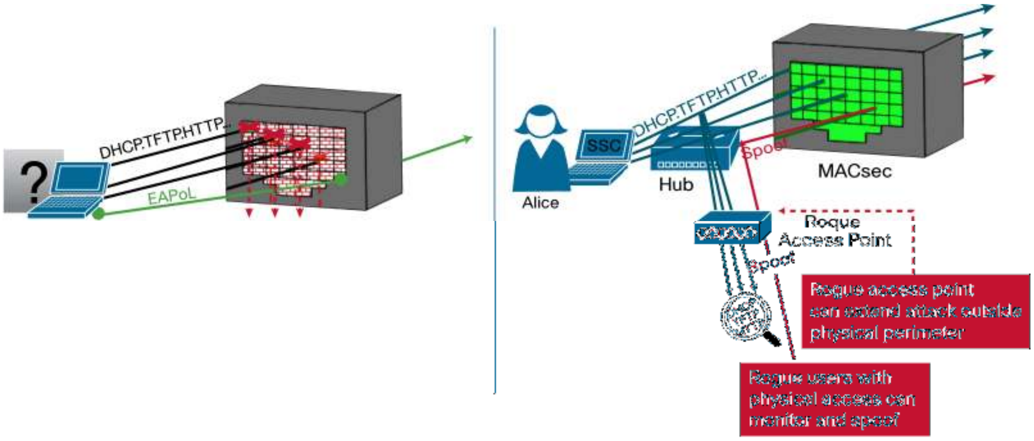
2.2 Functional Overview

2.2.1 What Is MACsec?

MACsec provides secure communication on wired LANs. When MACsec is used to secure the communication between endpoints on a LAN, each packet on the wire is encrypted using symmetric key cryptography so that communication cannot be monitored or altered on the wire.

MACsec was primarily designed to be used in conjunction with IEEE 802.1X-2010. IEEE 802.1X provides port-based access control using authentication. An IEEE 802.1X–enabled port can be dynamically enabled or disabled based on the identity of the user or device that connects to it. Figure 1 illustrates the default behavior of an IEEE 802.1X–enabled port.

Figure 1. Default Network Access Without MACsec



Prior to authentication, the endpoint's identity is unknown and all traffic is blocked. After authentication, the endpoint's identity is known and all traffic from that endpoint is allowed. The switch performs source MAC address filtering and port state monitoring to help ensure that only the authenticated endpoint is allowed to send traffic.

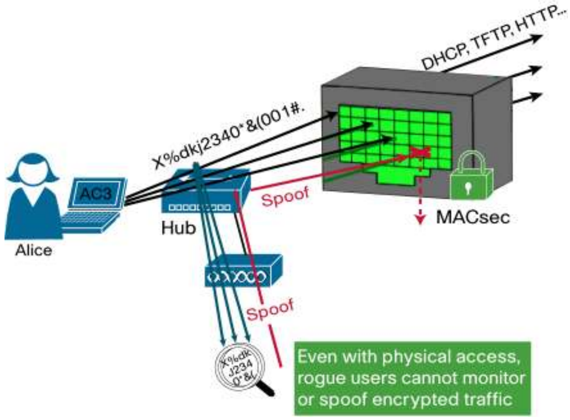
Before the 2010 revision of IEEE 802.1X, there was no mechanism to help ensure the confidentiality or integrity of the traffic sent after authentication. Because traffic was sent in the clear with no integrity checks, rogue users with physical access to the authenticated port could monitor, modify, and send traffic. In addition, source MAC address filtering could be circumvented by MAC address spoofing.

IEEE 802.1X Exploits Before MACsec

For a discussion of potential exploits of pre–IEEE 802.1X-2010 deployments, see http://technet.microsoft.com/en-us/library/cc512611.aspx. Note that these exploits require physical access to the authenticated port because the attacker needs to insert a hub to snoop and spoof traffic from the authorized endpoint. If a rogue access point is attached to the hub, the attacker can perform attacks remotely. However, even without MACsec, these IEEE 802.1X exploits can be mitigated by good physical security (to prevent insertion of a hub), good wireless LAN (WLAN) security (to detect unauthorized access points), and user education (to recognize and remove unauthorized hubs). However, there are situations in which these commonsense mechanisms are not sufficient. Publicly accessible areas, remote offices, and after-hours access represent potential attack vectors that need to be protected with MACsec.

IEEE 802.1X-2010 defines the way that MACsec can be used in conjunction with authentication to provide secure port-based access control using authentication. IEEE 802.1X authenticates the endpoint and transmits the necessary cryptographic keying material to both sides. Using the master keys derived from the IEEE 802.1X authentication, MACsec can establish an encrypted link on the LAN, thereby helping ensure the security of the authenticated session. Figure 2 illustrates the behavior of a MACsec-enabled port.

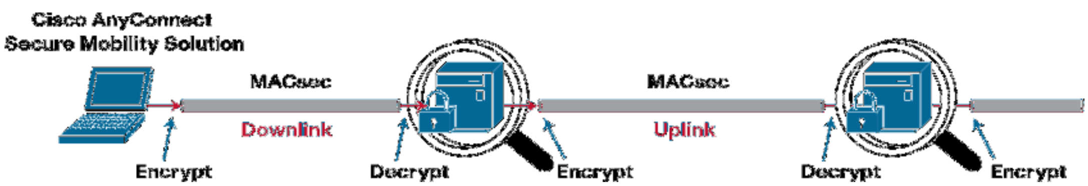
Figure 2. Securing the LAN with MACsec



MACsec was designed for incremental deployment to enable to you to protect your most vulnerable assets first. Because MACsec can involve significant investments in new hardware, you should evaluate the threats to your LANs before deciding where and when to deploy MACsec. For example, MACsec is often most useful in the access layer, where end users have direct access to switch ports. This type of deployment is sometimes called user-facing or downlink MACsec. The uplink between the access and distribution layers can also be secured by MACsec. However, the physical connection between access and distribution switches typically occurs inside a secure wiring closet, and the uplink is protected by additional physical security. Therefore, MACsec can be enabled on the downlink ports as a first step in the process of enabling MACsec pervasively throughout the infrastructure. After further risk assessment, remaining threats can be addressed with uplink encryption in subsequent phases of deployment.

When MACsec is applied on both the uplink and the downlink, the MACsec sessions are completely independent. Moreover, while all traffic is encrypted on the wire, the traffic is in the clear inside each switch. This feature allows the switch to apply all the network policies (quality of service [QoS], deep packet inspection, NetFlow, etc.) to each packet without compromising the security of the packet on the wire. With hop-by-hop encryption, MACsec secures communication while maintaining network intelligence (Figure 3).

Figure 3. Hop-by-Hop Encryption Allows Data Inspection

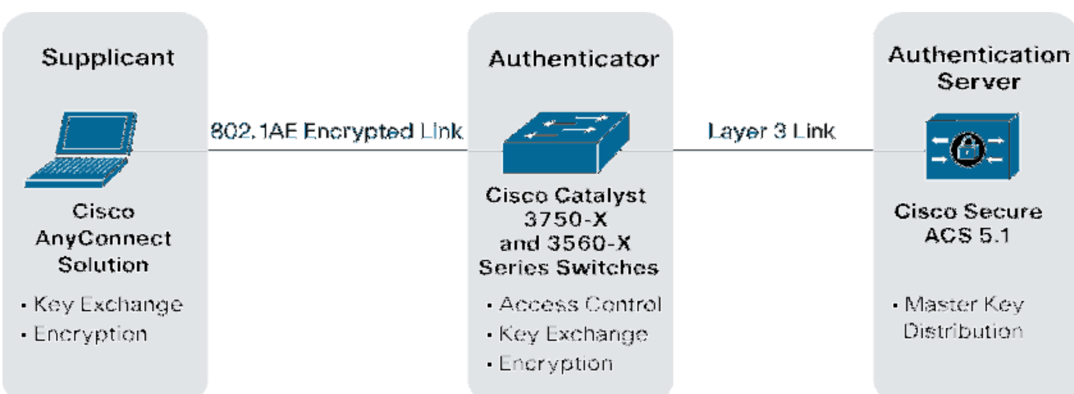


2.2.1.1 Components

In a typical access-layer environment, the simplest implementation of MACsec helps secure communication on the point-to-point link between the endpoint and the access switch port. Like IEEE 802.1X, MACsec uses three components (as shown in Figure 4):

- Supplicant: The supplicant is a client that runs on the endpoint and submits credentials for authentication. To support MACsec, the supplicant must also be able to manage MACsec key negotiation and encrypt packets.
- Authenticator: The authenticator is the network access device that facilitates the authentication process by relaying the supplicant's credentials to the authentication server. In the context of this document, the authenticator is simply the access-layer switch, and the two terms—"authenticator" and "switch"—can be considered interchangeable. The authenticator enforces the network access policy, including MACsec. Like the supplicant, the authenticator must be capable of MACsec key negotiation and packet encryption. The authenticator typically needs special hardware to support MACsec at line rate.
- Authentication server: The authentication validates the supplicant's credentials and determines what network access the supplicant should receive. The industry standard essentially is a RADIUS server, such as the Cisco® Secure Access Control Server (ACS). In this document, "RADIUS server" and "authentication server" are used interchangeably. In MACsec, the authentication server plays an important role in the distribution of master keying material to the supplicant and authenticator. In addition, the authentication server can define the MACsec policy to be applied to a particular endpoint.

Figure 4. IEEE 802.1X and MACsec Components



2.2.1.2 Protocols

MACsec uses several protocols:

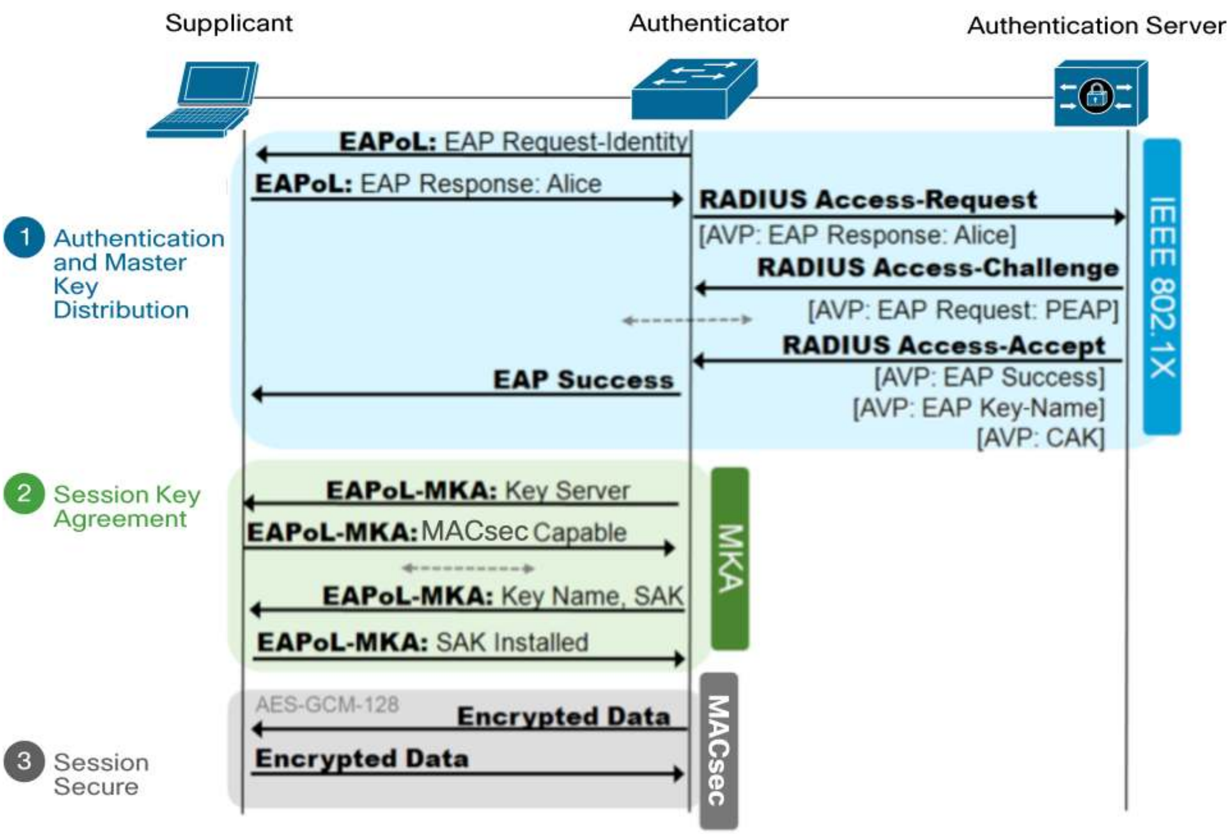
- Extensible Authentication Protocol (EAP): The message format and framework defined by RFC 4187 that provides a way for the supplicant and the authenticator to negotiate the EAP authentication method and MACsec association
- EAP method: Protocol that defines the authentication method—that is, the credential type and how it will be submitted from the supplicant to the authentication server using the EAP framework; for MACsec, the EAP method must be capable of generating keying material to export a master session key (MSK) to the supplicant and authentication server

- MACsec Key Agreement (MKA): Protocol that discovers MACsec peers and negotiates the keys used by MACsec; MKA is defined in IEEE 802.1X-2010
- Security Association Protocol (SAP): A pre-standard key agreement protocol similar to MKA
- EAP over LAN (EAPoL): An encapsulation defined by IEEE 802.1X for the transport of EAP from the supplicant to the switch over IEEE 802 wired networks; EAPoL is a Layer 2 protocol
- RADIUS: Essentially the standard for communication between the switch and the authentication server—the switch extracts the EAP payload from the Layer 2 EAPoL frame and encapsulates the payload inside a Layer 4 RADIUS packet; RADIUS is also used to deliver keying material to the authenticator

2.2.1.3 High-Level Functional Sequence

The high-level functional sequence in Figure 5 shows how the components and protocols of MACsec work together. The message exchange is divided into three stages: master key distribution, session key agreement, and session secured. A fourth stage, session termination, is not shown. Each stage is described in the sections that follow.

Figure 5. High-Level IEEE 802.1X and MACsec Sequence



2.2.2 IEEE 802.1X and Master Key Distribution

Successful IEEE 802.1X authentication is the first step in establishing a MACsec session. IEEE 802.1X provides master key material to the supplicant and switch that will subsequently be used by MACsec.

The supplicant and the switch derive the master key through different mechanisms. By using an EAP method that supports the generation of encryption keys, the supplicant and the authentication server independently derive the same MSK. The MSK passes through a key derivation function to generate a connectivity association key (CAK) on the supplicant and the authentication server. The CAK is a long-lived master key that is used to generate all other keys needed for MACsec.

The switch has no visibility into the details of the EAP session between the supplicant and the authentication server, so it cannot derive the MSK or the CAK directly. Instead, the switch receives the CAK from the authentication server in the Access-Accept message at the end of the IEEE 802.1X authentication. The CAK is delivered in the RADIUS vendor-specific attributes (VSAs) MS-MPPE-Send-Key and MS-MPPE-Recv-Key. Along with the CAK, the authentication server sends an EAP key identifier that is derived from the EAP exchange and is delivered to the authenticator in the EAP Key-Name attribute of the Access-Accept message.

> **Note:** MACsec is similar to IEEE 802.11i.
>
> If you are familiar with the wireless encryption mechanisms defined in IEEE 802.11i, you will notice similarities with MACsec. In IEEE 802.11i, the MSK derived from EAP is used to generate a pairwise master key (PMK) on the supplicant and the authentication server. The authentication server transmits the PMK to the authenticator through the Microsoft Point-to-Point Encryption (MPPE) VSAs. Thus, the PMK is the wireless analogue of the CAK. However, the use of the EAP Key-Name value is unique to MACsec.

2.2.3 Session Key Agreement

During the session-key agreement stage, the switch and the supplicant advertise their capabilities and derive all the parameters needed for MACsec. These functions are accomplished by the MKA protocol, which is transported on the wire using a new EAPoL packet type 5 (EAPoL-MKA).

If the supplicant and the switch are capable of MACsec, the switch automatically becomes the key server. The key server is responsible for selecting and advertising a cipher suite. Cisco components all support the default cipher suite Galois/Counter Mode Advanced Encryption Standard 128 (GCM-AES-128).

The key server is also responsible for generating a secure association key (the SAK) from the CAK. The SAK is the secret key that is used to encrypt traffic on the wire for a given connection. The SAK is the actual key that is used to encrypt traffic for a session. Unlike the CAK, which is a long-term master key, the SAK is a transient key that can periodically be refreshed.

To successfully encrypt traffic, the supplicant must also possess the SAK. Using MKA, the switch will send the SAK to the supplicant. To keep the SAK secure, the switch encrypts it with some additional CAK-derived keys and the AES key wrap (RFC 3394) function. Because the supplicant possesses the CAK, it can decrypt the key wrap and retrieve the SAK.

Pre-standard implementations may support SAP instead of MKA to negotiate session encryption keys. Although SAP uses different terminology and different message formats, the key exchange proceeds essentially the same way as with MKA. SAP and MKA do not interoperate, and only one protocol can be configured on a link.

MKA limits the number of frames that can be protected with a single SAK. After the number of allowed frames has been exceeded, the SAK will be refreshed. Sending minimum-sized frames at line rate on a 10-Gbps link would cause a rekey after about 5 minutes. MKA will also rekey after a device reauthenticates.

2.2.4 Session Secured

After the supplicant and the switch have installed the SAK, they begin transmitting and receiving encrypted traffic. In general, traffic that is not encrypted will be dropped. However, some exceptions are made for certain types of traffic.

See Section 2.3.16 for more information about the types of unencrypted traffic that are permitted on a secured port.

2.2.5 Session Termination

In the absence of MACsec, session termination is a particularly important part of IEEE 802.1X. To help ensure the integrity of a non-MACsec-secured session, sessions must be cleared when the authenticated endpoint disconnects from the network. Sessions that are not terminated immediately can lead to security violations and security holes. Ideally, session termination occurs as soon as the endpoint physically unplugs, but this is not always possible if the endpoint is connected indirectly (for example, through an IP phone or hub).

With the introduction of MACsec, session termination is still an important consideration. Because MACsec eliminates the possibility of MAC address spoofing, a MACsec-secured session is not vulnerable to the security hole that a dangling unsecured session represents. However, the possibility of a security violation still exists if a new device connects to a port before the previous session has been terminated. In addition, MACsec invalidates some older methods of session termination while introducing new ones.

Multiple termination mechanisms may be needed to address all use cases. Table 1 summarizes the various mechanisms and their applications.

Table 1. Typical Termination Mechanisms and Use Cases

Use Case	Typical Termination Mechanisms	
	Unsecure IEEE 802.1X Session	MACsec Session
All endpoints directly connected • Single endpoint per port • No IP phones	Link down EAPoL-Logoff	Link down
Endpoints connected through IP phone • At most two endpoints per port (one phone and one data)	Cisco Discovery Protocol enhancement for second-port disconnect (Cisco phones) Proxy EAPoL-Logoff message and inactivity timer (phones other than Cisco phones)	Cisco Discovery Protocol enhancement for second-port disconnect (Cisco phones) MKA timeout (phones other than Cisco phones)
Endpoints connected through hub • Physical hub • Bridged virtual hubs	Inactivity timer	MKA timeout

The following sections discuss in more detail the ways that an IEEE 802.1X session can be terminated.

2.2.5.1 Link Down

The most direct way to terminate an IEEE 802.1X session (MACsec secured or not) is to unplug the endpoint. When the link state of the port goes down, the switch completely clears the session. If the original endpoint (or a new endpoint) plugs in, the switch will restart authentication from the beginning.

2.2.5.2 MKA Timeout

The MKA protocol defines a keepalive packet that is sent every 2 seconds for a MACsec session. If more than three keepalives go unanswered, the switch will tear down the session. The MKA timeout is therefore 6 seconds. The MKA keepalive function is always operational on MACsec sessions, and no configuration is required.

2.2.5.3 EAPoL-Logoff and Proxy EAPoL-Logoff

The EAPoL-Logoff message was originally designed to allow the supplicant to tell the switch to terminate the existing session. However, MACsec changes the operation of the EAPoL-Logoff message.

Prior to the introduction of MACsec, the switch terminated the existing session upon receipt of an EAPoL-Logoff message. Proxy EAPoL-Logoff messages have proven to be especially useful. For example, an IP phone can transmit a proxy EAPoL-Logoff message when the phone detects that an IEEE 802.1X–authenticated endpoint has unplugged from behind the phone. The phone substitutes the data endpoint's MAC address, so the proxy EAPoL-Logoff message is indistinguishable from an actual EAPoL-Logoff message from the data endpoint itself. The switch immediately clears the session as soon as it receives the Logoff message.

While proxy EAPoL-Logoff messages are useful in IP telephony deployments, they also introduce a vector for a denial-of-service (DoS) attack. Therefore, to prevent rogue users from terminating existing sessions, a MACsec-secured session ignores all EAPoL-Logoff messages.

> **Warning: Proxy EAPoL-Logoff Cannot Be Used with MACsec**
> If a device behind a phone has been secured with MACsec, proxy EAPoL-Logoff messages sent from phones will be ignored. For IP telephony deployments, some other mechanism must be used to terminate a MACsec-secure session.

2.2.5.4 Cisco Discovery Protocol Enhancement for Second-Port Disconnect

For IP telephony deployments with Cisco IP Phones, the best way to help ensure that all IEEE 802.1X sessions, whether MACsec or not, are properly terminated is to use Cisco Discovery Protocol. Cisco IP Phones can send a Cisco Discovery Protocol message to the switch indicating that the link state for the data endpoint's port is down, allowing the switch to immediately clear the data endpoint's authenticated session.

Cisco Catalyst® Family switches process Cisco Discovery Protocol even when a MACsec session is present on the port.

> **Best Practice Recommendation: Use CDP Enhancement for Second-Port Disconnect for IP Telephony Deployments**
> This feature works for all authentication methods with and without MACsec, takes effect as soon as the endpoint disconnects, and requires no configuration. If you are using Cisco IP Phones and Cisco Catalyst switches with the appropriate code release, this method offers the simplest and most effective solution. No other method works as well to terminate authenticated sessions behind Cisco IP Phones. The MKA timeout function will terminate the session after 6 seconds, but the Cisco Discovery Protocol enhancement for second-port disconnect works more quickly.

2.2.5.5 Inactivity Timer

When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session. The inactivity timer for IEEE 802.1X can be statically configured on the switch port, or it can be dynamically assigned using the RADIUS Idle-Timeout attribute (Attribute 28).

For a MACsec session, the inactivity timer is typically not necessary because the MKA keepalive timeout will automatically terminate the session in 6 seconds. The inactivity timer will not be enforced unless its value is less than the MKA timeout value (6 seconds). However, if your network has some endpoints that are MACsec capable and some that are not, you can configure the inactivity timer so that non-MACsec sessions can be terminated by the inactivity timer.

2.2.5.6 RADIUS Change of Authorization

RADIUS change of authorization (CoA) allows a RADIUS server to dynamically instruct the switch to alter an existing session. Cisco Catalyst switches support four actions for CoA: reauthenticate, terminate, port shutdown, and port bounce. The reauthenticate and terminate actions terminate the authenticated session in the same way as the reauthentication and session timeout actions discussed in Section 2.3.7. The port down and port bounce actions clear the session immediately, since these actions result in link-down events.

2.3 Design Considerations

This section discusses a variety of design considerations that you should evaluate prior to deploying IEEE 802.1X with MACsec.

2.3.1 Choosing MACsec Policies

Deciding when and where MACsec should be enforced is a matter of policy. MACsec policy is instantiated in two places: the switch and the supplicant.

When a device connects to a MACsec-capable switch and passes IEEE 802.1X authentication, the switch has three policy choices for the session:

- Must Not Secure: The switch will not perform MKA. If the supplicant sends MKA protocol frames, they will be ignored. The switch will send and receive unencrypted traffic only.
- Should Secure: The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only. If MKA times out or fails, the switch will permit unencrypted traffic.
- Must Secure: The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only. If MKA times out or fails, the switch will treat this result as an authorization failure by terminating the IEEE 802.1X–authenticated session and retrying authentication after a quiet period. No other authentication methods will be tried, and no traffic will be allowed from that endpoint unless a specific MACsec fallback authentication or authorization technique is configured.

> **Note:** MACsec fallback policies are not the same as authentication fallback policies.
>
> The switch treats a failure to create a Must Secure MACsec session differently than a failed authentication and an authentication that times out because a supplicant is not present. Suppose you have configured your switch port to fall back to MAC Authentication Bypass (MAB) if IEEE 802.1X fails or times out. If IEEE 802.1X succeeds but the switch is unable to start a MACsec connection when the policy is Must Secure, the switch will not fall back to MAB by default. Instead you must explicitly configure a MACsec fallback policy. The MACsec fallback policy can be set to try the next authentication method (for example, MAB) or authorize into a special VLAN.

MACsec-capable supplicants can also implement a MACsec policy along the same lines as the switch:

- Must Not Secure: The supplicant will not perform MKA. If the switch sends MKA protocol frames, they will be ignored. The supplicant will send and receive unencrypted traffic only.
- Should Secure: The supplicant will attempt MKA. If MKA succeeds, the supplicant will send and receive encrypted traffic only. If MKA times out or fails, the supplicant will permit unencrypted traffic.
- Must Secure: The supplicant will attempt MKA. If MKA succeeds, the supplicant will send and receive encrypted traffic only. If MKA times out or fails, the supplicant will not allow any traffic to enter or exit the end host.

The most flexible and adaptable policy has Should Secure policy on the switch and the supplicant. With this combination, MACsec-capable endpoints can apply MACsec, and non-MACsec-capable endpoints can gain access to the network in an unencrypted session.

Other combinations may be more effective depending on your deployment scenario. See Section 2.3.20 for more information about the best MKA policies for common deployment scenarios. In any event, be sure that the policy you configure on your supplicant matches your switch policy.

Table 2 shows the type of connection that will result based on any given combination of MACsec policy and capability. Be aware that some combinations will cause all traffic to be blocked for that session, regardless of whether the endpoint authenticated successfully.

Table 2. Policies and Resulting Connections

Supplicant Policy	Switch Policy	Resulting Connection
Not MACsec capable or Must Not Secure policy	Not MACsec capable or Must Not Secure policy	Not secure
Should Secure policy	Not MACsec capable or Must Not Secure policy	Not secure
Must Secure policy	Not MACsec capable or Must Not Secure policy	Blocked
Not MACsec capable or Must Not Secure policy	Should Secure policy	Not secure
Should Secure policy	Should Secure policy	Secure
Must Secure policy	Should Secure policy	Secure
Not MACsec capable or Must Not Secure policy	Must Secure policy	Blocked if no MACsec fallback policy configured
Should Secure policy	Must Secure policy	Secure
Must Secure policy	Must Secure policy	Secure

2.3.2 Setting MACsec Policies on the Switch

For Cisco switches, the switch policy can be set in either of two places: on individual switch ports or on the authentication server. If the policy is defined on the authentication server, the authentication server returns the policy to the switch through a RADIUS attribute-value pair (Cisco-av-pair=subscriber:linksec-policy) in the RADIUS Access-Accept message at the end of the IEEE 802.1X authentication exchange. The following rules govern the interaction of command-line interface (CLI)–based policy and server-based policy:

- If the authentication server returns a policy, this policy overrides anything set using the switch CLI.
- If the authentication server does not return the appropriate attribute-value pair to set the policy, the switch uses the configured policy on the port.
- If no policy is specified in the switch configuration, the switch reverts to the default policy, which is Should Secure.

Often, your design goals can be met by relying on the default policy on the switch and applying policy exceptions through the RADIUS attributes.

Best Practice Recommendation: Use the Default Switch Policy with Server-Based Exceptions

This approach gives you centralized control over the policy that should be applied to a session without adding excessive control-plane overhead (since the authentication server has to send policy only when the default policy is not appropriate). The default policy (Should Secure) secures the sessions that can be secured while still allowing access for endpoints that cannot implement MACsec.

2.3.3 Supplicant Considerations

When choosing a supplicant, your goal should be to choose a supplicant (or supplicants) that provides the needed functions, reduces the administrative overhead, and can be easily deployed and maintained. Although many supplicants support IEEE 802.1X, only a few currently support IEEE 802.1X with MACsec.

The Cisco AnyConnect Secure Mobility Client 3.0 is the industry's first software supplicant to support MACsec with software-based encryption for endpoints that do not support MACsec in hardware. Cisco AnyConnect Secure Mobility Client 3.0 can also be used in conjunction with a MACsec-capable network interface card (NIC) that offloads the encryption to hardware. For example, the Intel 82576 family of Ethernet controllers supports hardware-based MACsec.

2.3.4 Switch Considerations

Although many switches support IEEE 802.1X, only a few support line-rate MACsec.

In the access layer, Cisco Catalyst 3750-X and 3560-X Series Switches currently offer integrated hardware support for MACsec on all user-facing (downlink) ports starting with Cisco IOS Software Release 12.2(53)SE1]] Support for switch-to-switch (uplink) encryption will be available in the future.

Although not typically deployed in the access layer, the Cisco Nexus® 7000 Series Switches also support MACsec for data center interconnect (DCI).

2.3.5 Authentication Server Considerations

MACsec requires a MACsec-capable authentication server. Although many RADIUS servers support IEEE 802.1X authentication, few support MACsec. In particular, a MACsec-capable RADIUS server must support the EAP Key-Name attribute, which is unique to IEEE 802.1X-2010.

Cisco Secure Access Control System 5.1 is the first authentication server to support MACsec in wired networks.

2.3.6 User and Machine Authentication

MACsec can be used with both machine and user authentication.

If an endpoint secures a connection using machine credentials when a user logs in, the successful completion of user authentication will cause MKA to rekey.

If user authentication fails, the switch will not tear down the machine authentication session as long as the supplicant continues sending MKA keepalives. This behavior prevents a rogue user from launching a DoS attack on a valid authenticated session. It is the responsibility of the supplicant to tear down the machine session if user authentication fails.

If authorization fails on user authentication, then the session is torn down.

2.3.7 Reauthentication

MACsec can be used with reauthentication. However, MACsec often eliminates the need for reauthentication.

In a non-MACsec environment, successful reauthentication allows the switch to confirm that the authenticated endpoint is still connected. In other words, reauthentication can essentially be used as a IEEE 802.1X keepalive mechanism. Since MACsec provides its own keepalive mechanism through MKA, reauthentication usually is not needed.

Best Practice Recommendation: Disable Periodic Reauthentication for MACsec Endpoints
Because MACsec continuously helps ensure the validity of the authenticated session, reauthentication typically does not need to be used as a keepalive mechanism.

A secondary use of reauthentication is to provide essentially a reauthorization mechanism. In the absence of explicit mechanisms to dynamically push policy updates to switches, reauthentication provides a mechanism by which the switch can pull the latest authorization policy (such as VLAN or access control list [ACL] assignment) for authenticated endpoints.

If an endpoint has secured a connection, the successful completion of reauthentication causes MKA to rekey.

If reauthentication fails, the user will still have access to the network as long as the supplicant continues sending MKA keepalives. This behavior prevents a rogue user from launching a DoS attack on a valid authenticated session. It is the responsibility of the supplicant to tear down the session if reauthentication fails.

If authorization fails (for example, because of a bad VLAN assignment) during reauthentication, then the session is torn down.

2.3.8 EAP Methods

MACsec requires an EAP method that supports the derivation of an MSK. Common EAP methods used in IEEE 802.1X that also support MSK are EAP Transport Layer Security (EAP-TLS), Protected EAP Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2), and EAP Flexible Authentication via Secure Tunneling (EAP-FAST). EAP-MD5 does not support key derivation and should not be used for MACsec.

2.3.9 Open Access

MACsec is supported with open access.

By default, IEEE 802.1X drops all traffic prior to successful IEEE 802.1X authentication. This approach is sometimes referred to as closed mode. Cisco switches can also be configured for open access, which allows all traffic while still enabling IEEE 802.1X and MAB. Open access has many applications, from increasing network visibility as part of a monitor mode deployment scenario to providing incremental access control as part of a low-impact mode deployment scenario. For more information about these deployment scenarios, see Section 2.3.20.

Regardless of whether the switch is configured for open access, the switch will not enforce the MACsec policy until after successful IEEE 802.1X authentication. Therefore, when open access is configured, endpoints that are MACsec capable may send and receive traffic in the clear until after IEEE 802.1X succeeds and MKA finishes.

2.3.10 Multiple Endpoints per Port

By default, an IEEE 802.1X–enabled port allows only a single endpoint per port. Any additional MAC addresses seen on the port will cause a security violation. Frequently, the limitation of a single endpoint per port will not meet all the requirements of real-world networks. Cisco Catalyst switches allow you to address multiple use cases by modifying the default behavior. The host mode on a port determines the number and type of endpoints allowed on a port.

The IEEE 802.1AE specification defines a method to support single endpoints and groups of endpoints on a single port, but support for different host modes on a MACsec port is hardware dependent. Table 3 summarizes host mode support for each MACsec platform.

Table 3. Support for MACsec by Host Mode and Platform

	Single- Host Mode	Multidomain Authentication Host Mode	Multi-Authentication (Multi-Auth) Host Mode	Multihost Mode
Cisco Catalyst 3750-X Series	Supported	Supported	Not supported	Supported with restrictions
Cisco Catalyst 3560-X Series	Supported	Supported	Not supported	Supported with restrictions

Each host mode is discussed in detail here.

Single-Host Mode

MACsec is fully supported in single-host mode.

In single-host mode, only a single MAC or IP address can be authenticated and secured with MACsec. If a different MAC address is detected on the port after an endpoint has authenticated, then a security violation will be triggered on the port. The only exception is if a voice VLAN is configured on the port and the second MAC address first sends an appropriate Cisco Discovery Protocol message indicating that it is a Cisco IP Phone.

This is the default behavior.

Multidomain Authentication Host Mode

MACsec is fully supported in multidomain authentication host mode.

Multidomain authentication was specifically designed to address the requirements of IP telephony in an IEEE 802.1X environment. When multidomain authentication is configured, two endpoints are allowed on the port: one in the voice VLAN and one in the data VLAN. Additional MAC addresses will trigger a security violation.

If both endpoints are MACsec capable, each will be secured by its own independent MACsec session. If only one endpoint is MACsec capable, that endpoint can be secured while the other endpoint sends traffic in the clear.

Multi-Auth Host Mode

MACsec is not supported in multi-auth host mode

If the port is configured for multi-auth host mode, then multiple endpoints can be authenticated in the data VLAN, but they cannot be secured with MACsec. If the MACsec policy is Should Secure, then authentication will succeed, and the endpoint will be allowed to send traffic in the clear. If the MACsec policy is Must Secure, the authentication will fail, and the endpoint will not be authorized for network access.

Multihost Mode

MACsec is supported in multihost mode with some restrictions.

Unlike multi-auth host mode, which authenticates every MAC address, multihost mode authenticates the first MAC address and then allows an unlimited number of other MAC addresses. However, the same MACsec session will apply to all traffic, regardless of the source MAC address. Multihost mode cannot, therefore, be used with a hub to connect multiple devices with different MAC addresses. It can, however, be used to for switch-to-switch encryption in which the downstream switch needs to forward traffic with multiple MAC addresses in a single MACsec session.

> **Note:** Switch-to-switch encryption is not currently supported.
>
> Switch-to-switch encryption is not currently supported on the Cisco Catalyst 2960, 3560, and 3750 Series Switches. Future releases will support uplink encryption.

2.3.11 IP Telephony

Multidomain Authentication

MACsec is compatible with IP telephony when multidomain authentication is used.

Multidomain authentication is the recommended method for integrating IP telephony in an IEEE 802.1X–enabled network. Since the phone and the device behind the phone are authenticated independently, each device can have its own MACsec policy. If both the phone and the PC are MACsec capable, each can establish its own independent encrypted session. If only one device is MACsec capable, that device will be secured and the other device will operate normally without encryption. See Section 2.3.10 for more information about multidomain authentication host mode.

Cisco Discovery Protocol Bypass

MACsec supports Cisco Discovery Protocol Bypass.

Some Cisco switches allow Cisco IP Phones to bypass authentication by sending Cisco Discovery Protocol packets with the appropriate information. If MACsec is configured, the phone will be exempt from MACsec after sending Cisco Discovery Protocol. In other words, the phone can send and receive traffic in the clear, even if the PC behind it has an active MACsec session. A PC or other data device connecting behind the phone will be authenticated and subject to the MACsec policy. A port configured for single-host mode and a voice VLAN will automatically perform Cisco Discovery Protocol bypass for Cisco IP Phones. See Section 2.3.10 for more information about single-host mode.

IP Telephony and Link State

When devices behind IP phones disconnect from the phones, the switch has no direct knowledge of the link state of the session. Another method must be used to terminate the session.

Cisco IP Phones and switches support a feature called Cisco Discovery Protocol second-port status type length value (TLV) that allows the phone to communicate with the switch when the device behind the phone unplugs, enabling the switch to clear the MACsec session. For phones that do not support Cisco Discovery Protocol second-port status, the only solution is to rely on the MKA keepalive timeout. For more information about terminating MACsec sessions behind phones, see Section 2.2.5.

2.3.12 Wake on LAN

MACsec has no effect on wake on the LAN (WoL) function.

WoL is an industry-standard power management feature that allows you to remotely wake up a hibernating endpoint by sending a “magic packet” over the network. Most WoL endpoints flap the link when going into hibernation or standby mode, thus clearing any existing MACsec session.

2.3.13 Non–IEEE 802.1X–Capable Endpoints

Endpoints that are not capable of IEEE 802.1X authentication cannot implement MACsec. If a non–IEEE 802.1X–capable endpoint is authorized for network access using a secondary authentication method such as MAB or Web Authentication (WebAuth) or a fallback authorization such as Guest VLAN, all traffic to and from the endpoint will be in the clear.

2.3.14 IEEE 802.1X Endpoints with Invalid Credentials

Endpoints that fail IEEE 802.1X authentication cannot implement MACsec. If a failed IEEE 802.1X endpoint is authorized for network access using a secondary authentication method such as MAB or WebAuth or a fallback authorization such as a Authentication Failure (AuthFail) VLAN, all traffic to and from the endpoint will be in the clear.

2.3.15 Inaccessible Authentication Bypass

If an endpoint cannot complete IEEE 802.1X authentication because the authentication server is inaccessible, a new MACsec session cannot be created.

If the authentication server becomes inaccessible after a MACsec session has been established, the session will continue until it is terminated by one of the mechanisms described in Section 2.2.5 or until the session is reauthenticated.

By default, reauthentication will fail when the authentication server is inaccessible. The MACsec session will be torn down, and the endpoint will lose network access.

The inaccessible authentication bypass feature can be used to change the default behavior during reauthentication. If inaccessible authentication bypass is configured, then the network access is preserved, but the MACsec session is torn down. All traffic will be sent in the clear until the authentication server recovers and the session is reinitialized.

When the authentication server returns, the switch can be configured to reinitialize the critically authorized sessions. This reinitialization will restart MACsec for the endpoints that support it.

2.3.16 MACsec Exceptions

MACsec typically encrypts all traffic on the wire for a given session, but there are a few exceptions. These exceptions enable interoperability and backward compatibility with existing functions.

The handling of unencrypted traffic depends in part on the hardware implementation of the particular platform. The rest of this section discusses special traffic handling for downlink ports on the Cisco Catalyst 3750-X and 3560-X Series Switches.

After a session has been secured, the types of unencrypted traffic that can be sent to and received from the secured endpoint are:

- Cisco Discovery Protocol
- Link Layer Discovery Protocol (LLDP)
- EAPoL-Start
- Link Aggregation Control Protocol (LACP)

For all other traffic from the secured endpoint, unencrypted traffic is dropped. Traffic from other endpoints (that is, from unique source MAC addresses) on the port is subject to the IEEE 802.1X security policy on the port. Here are some examples:

- In single-host mode, unencrypted traffic from an IP phone that has bypassed authentication using Cisco Discovery Protocol bypass will be allowed.
- In multidomain authentication host mode, unencrypted traffic from an authenticated, non-MACsec phone will be allowed.

- In single-host and multidomain authentication host modes, unencrypted traffic from an unauthenticated data endpoint will cause a security violation.

2.3.17 Accounting

MACsec does not add any information to RADIUS accounting records.

2.3.18 Simple Network Management Protocol

There is currently no MIB support for MACsec.

2.3.19 Cisco Catalyst Integrated Security Features

This section describes Cisco Catalyst integrated security features.

2.3.19.1 Port Security

In general, Cisco does not recommend enabling port security when IEEE 802.1X (and, by extension, MACsec) is also enabled. Since IEEE 802.1X enforces a single MAC address per port (or per VLAN when multidomain authentication is configured for IP telephony), port security is largely redundant and may in some cases interfere with the expected operation of IEEE 802.1X.

2.3.19.2 Dynamic Host Configuration Protocol Snooping

Dynamic Host Configuration Protocol (DHCP) snooping is fully compatible with MACsec and should be enabled as a best practice.

2.3.19.3 Dynamic Address Resolution Protocol Inspection

Dynamic Address Resolution Protocol (ARP) Inspection (DAI) is fully compatible with MACsec and should be enabled as a best practice.

2.3.19.4 IP Source Guard

IP source guard is compatible with MACsec and should be enabled as a best practice.

2.3.20 Deployment Scenarios

When deploying IEEE 802.1X, Cisco recommends a phased deployment model that gradually deploys identity-based access control to the network. The three scenarios for phased deployment are monitor mode, low-impact mode, and high-security mode. Each scenario identifies combinations of authentication and authorization techniques that work well together to achieve a particular set of use cases. By developing your IEEE 802.1X design in the context of a comprehensive deployment scenario, you can use well-understood blueprints to address common design issues.

Table 4 provides a summary of recommended MACsec settings in each deployment scenario.

Table 4. Recommended MACsec Settings for Phased-Deployment Scenarios

Deployment Scenario	Endpoint Type	Network MACsec Policy	Supplicant Policy
Monitor mode	All	–	–
Low-impact mode	General	Should Secure	Should Secure
High-security mode	General	Should Secure	Should Secure
All	Highly secure	Must Secure	Must Secure

These recommendations and the effect of MACsec on each deployment scenario are discussed in more detail in this section. For general information about scenario-based deployments, see Section 5.

2.3.20.1 Monitor Mode

MACsec is not applicable in monitor mode.

The primary goal of monitor mode is to enable authentication without imposing any form of access control. This approach allows network administrators to see who is on the network and prepare for access control in a later phase without affecting end users in any way.

Monitor mode relies on the multi-auth host mode to allow multiple devices per port. Since MACsec is not supported in multi-auth host mode, there is no point in enabling MACsec in monitor mode.

> **Best Practice Recommendation: Use Default Policy in Monitor Mode**
> To reduce the need for configuration on the switch and authentication server, use the default policy settings for MACsec in monitor mode.

2.3.20.2 Low-Impact Mode

MACsec is fully supported in low-impact mode.

Low-impact mode builds on the idea of monitor mode, gradually introducing access control in a completely configurable way. Instead of denying all access before authentication (as a traditional IEEE 802.1X deployment would require), low-impact mode allows you to use ACLs to selectively allow traffic (such as DHCP traffic) before authentication.

A major benefit of MACsec is that it provides hop-by-hop encryption. This feature means that traffic that is encrypted on the wire will be in the clear on the switch itself. Therefore, the switch can fully enforce port ACLs even on MACsec-secure connections. Therefore, you can get all the benefits of low-impact mode while creating secure connections for MACsec-capable endpoints.

Low-impact mode uses multidomain authentication host mode or single host mode instead of multi-auth host mode. MACsec is fully supported in multidomain authentication host mode and single-host mode, so there is no conflict with low-impact mode.

If you enable MACsec in low-impact mode, be aware that the switch port will be operating in open-access mode, which allows traffic before authentication (subject to the ACL configured on the port). MACsec policy will not be enforced until a successful IEEE 802.1X authentication occurs. Therefore, even endpoints that are MACsec-capable can send traffic in the clear until after IEEE 802.1X succeeds and MKA finishes.

Typically, customers who deploy low-impact mode have evaluated and accepted the security implications of permitting unencrypted and unauthenticated traffic prior to authentication. In this environment, MACsec usually is performed on a best-effort basis. MACsec-capable endpoints connecting to MACsec-capable switch ports should use MACsec. All other endpoints should be allowed access after successful authentication. To accomplish this, the policy for MACsec should be Should Secure on the switch and the supplicant.

> **Best Practice Recommendation: Set Should Secure in Low-Impact Mode**
> To help ensure that MACsec-capable connections are secured while preventing older devices from getting locked out of the network, set the MACsec policy for switch ports and supplicants to Should Secure by default.

2.3.20.3 High-Security Mode

MACsec is fully supported in high-security mode.

High-security mode is a more traditional deployment model for IEEE 802.1X, which denies all access prior to authentication. It also facilitates dynamic VLAN assignment and network virtualization.

Customers deploying high-security mode often implement fallback authentication or authorization techniques to permit devices that cannot perform or pass IEEE 802.1X authentication to get some access to the network. Examples of such techniques include MAB, Guest VLAN, and AuthFail VLAN. To take advantage of these fallback features, make sure that the supplicant can fail open if IEEE 802.1X authentication does not pass or MKA does not succeed. To enable IEEE 802.1X–capable devices that cannot implement MACsec to gain access to the network, leave the MACsec policy at the default value of Should Secure.

> **Best Practice Recommendation: Set Should Secure in High-Security Mode**
> To help ensure that MACsec-capable connections are secured while preventing older devices from getting locked out of the network, set the MACsec policy for switch ports and supplicants to Should Secure by default.

2.3.20.4 Exceptions for Highly Secure Endpoints in All Deployment Scenarios

In any deployment scenario, you may have some highly secure endpoints that must never send or receive unencrypted traffic. In that case, you should configure the MACsec policy as Must Secure and configure the supplicant to block traffic from the endpoint prior to successful authentication and MKA. Endpoints in this configuration will never send unencrypted traffic. Also note that if these endpoints connect to a switch that does not support MACsec, they will not get network access.

2.4 Deployment Summary for MACsec

Table 5 summarizes the major design decisions that need to be addressed prior to deploying MACsec.

Table 5. MACsec Deployment Reference

Design Consideration	Relevant Section
Design a MACsec policy that meets the needs of your security policy and the capabilities of your components.	2.3.1
Deploy MACsec on the most vulnerable links first.	2.2.1
Make sure that the same keying protocol is used by both devices on any given link.	2.2.3
Understand how session termination will work in your environment.	2.2.5
Use the default MACsec policy on the switch with server-based exceptions.	2.3.2
Select a supplicant that provides the required functions.	2.3.3
Make sure that your switches have the hardware support necessary for MACsec.	2.3.4
Select an authentication server that supports MACsec.	2.3.5
Disable reauthentication for MACsec endpoints.	2.3.7
Select EAP methods that support MSK key derivation.	2.3.8
Disable MACsec on multi-auth host mode ports.	2.3.10
Evaluate your MACsec policy as part of a larger deployment scenario.	2.3.20

3. Configuration Quick Reference

This section summarizes the configuration necessary to enable MACsec using Cisco AnyConnect 3.0, Cisco Catalyst 3750-X and 3560-X Series Switches, and Cisco Secure ACS 5.1. Only the MACsec-specific configurations are covered. These configuration steps assume that a working IEEE 802.1X solution is already in place.

For additional information about how to configure a basic IEEE 802.1X solution, see Section 5.

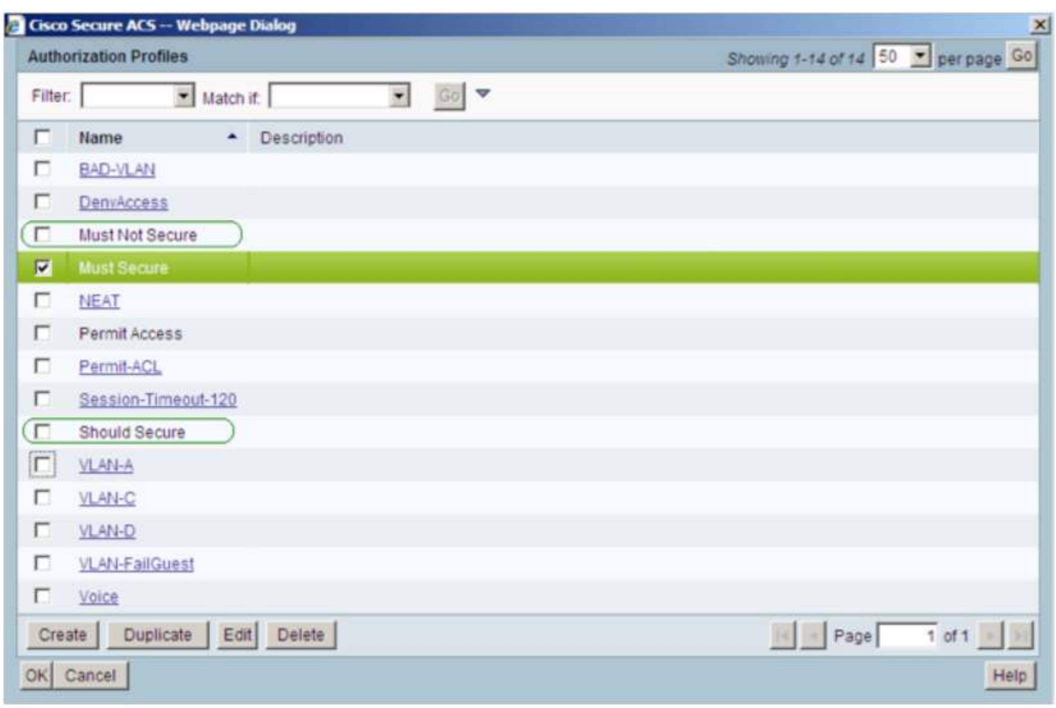
3.1 Cisco Secure ACS 5.1

Often, no additional configuration is needed to enable MACsec on Cisco Secure ACS 5.1. The keying material and EAP Key-Name attributes will be sent automatically to the switch as part of a successful authentication. The only reason to change the Cisco Secure ACS configuration would be to override the default policy on the switch. The default policy on the switch is Should Secure, which typically grants the expected access to most endpoints; endpoints that can implement MACsec will be secured, and non-MACsec endpoints can still get access.

Cisco Secure ACS comes with three preconfigured authorization profiles for MACsec: Must Not Secure, Must Secure, and Should Secure. If the default policy on the switch should be overridden for a particular session, you can explicitly set the MACsec policy in the authorization policy on Cisco Secure ACS by selecting one of these three preconfigured authorization profiles in addition to any other authorization profiles that you require.

Figure 6 shows how to select Must Secure in an authorization policy. The other two options, Should Secure and Must Not Secure, are circled.

Figure 6. Selecting Must Secure in an Authorization Policy



3.2 Cisco Catalyst 3750-X and 3560-X Series Switches

A typical port configuration for MACsec is shown here. Lines in bold are required to enable MACsec. The rest of the commands are part of a typical IEEE 802.1X port configuration. No additional global commands are needed for MACsec.

interface GigabitEthernet1/0/25
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 21
 authentication port-control auto
 macsec
 mka default-policy
 dot1x pae authenticator
 spanning-tree portfast

By default, the MACsec policy on the switch is Should Secure. Typically, the default policy will be appropriate for most deployments. However, if you need to change the default policy, use the following interface configuration command:

```
3750X1-boulder(config-if)#authentication linksec policy ?
  must-not-secure  Never secure sessions
  must-secure      Always secure sessions
  should-secure    OPTIONALLY secure sessions
```

If the MACsec policy is Must Secure, you have the option of configuring a MACsec fallback policy that will be applied to the port if IEEE 802.1X authentication passes but MACsec cannot establish a secure connection. If you do not configure a MACsec fallback policy, no access will be granted if a Must Secure session cannot be secured. In other words, the default fallback policy truly is Must Secure and will typically be appropriate for most deployments that need to enforce a strict MACsec policy. However, if you need to change the default policy, use the following interface configuration command:

```
3750X1-boulder(config-if)#authentication event linksec fail action ?
  authorize    Authorize the port
  next-method  Move to next authentication method
```

If the MACsec policy is Should Secure or Must Not Secure, the MACsec fallback policy configuration has no effect.

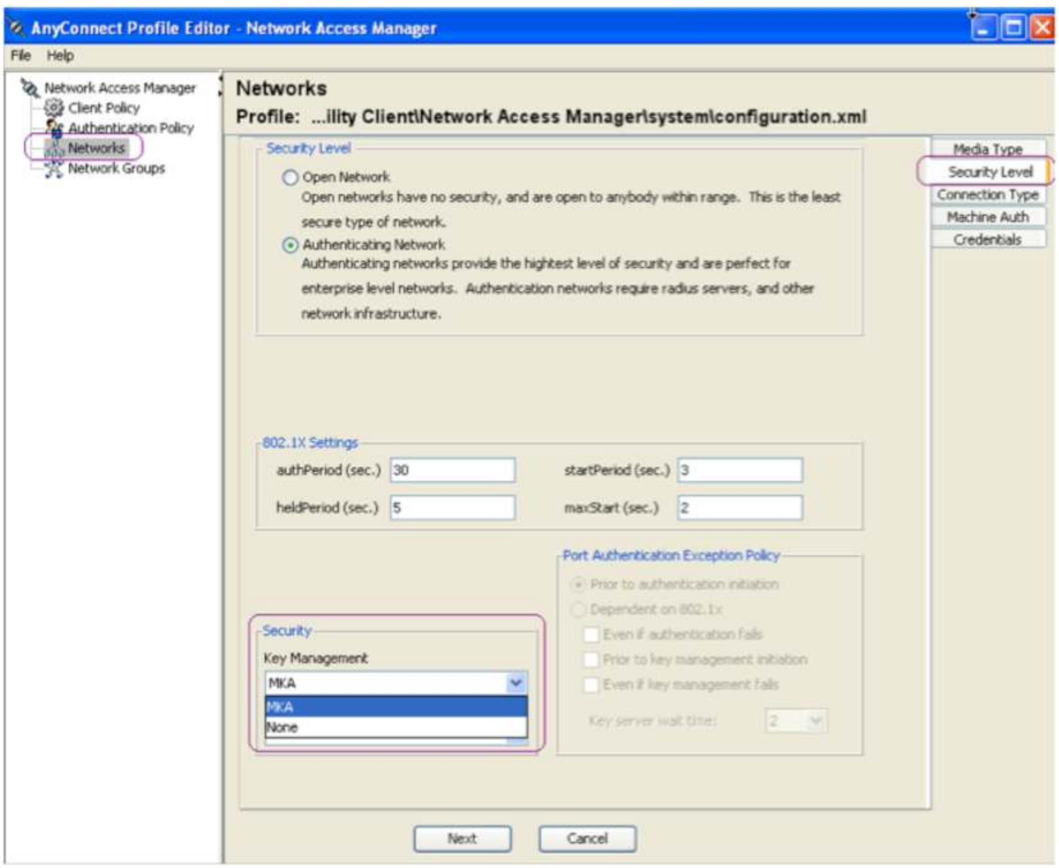
3.3 Cisco AnyConnect 3.0

A MACsec-enabled profile in a Cisco AnyConnect Secure Mobility Client requires several steps in addition to the basic IEEE 802.1X configuration: enable MKA, select an encryption suite, set the MACsec policy, and select a valid EAP method. Each of these steps is described in more detail here.

3.3.1 Enable MKA

Open the Network Access Manager Profile Editor and select the network you want to enable for MACsec. On the right side of the screen, select the Security Level tab. In the Security box at the bottom left, choose MKA from the Key Management drop-down box as shown in Figure 7.

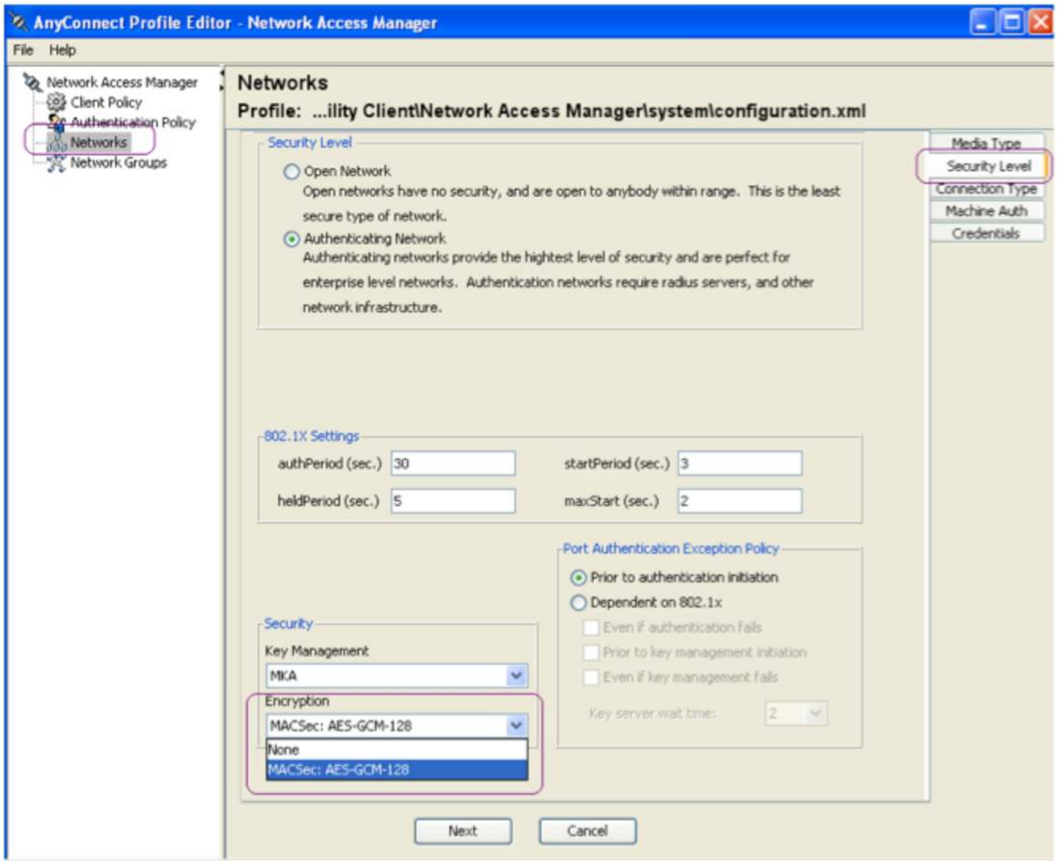
Figure 7. Selecting a MACsec Key Management Protocol



3.3.2 Select Encryption Suite

Open the Network Access Manager Profile Editor and select the network you want to enable for MACsec. On the right side of the screen, select the Security Level tab. In the Security box at the bottom left, choose MACsec: AES-GCM-128 from the Encryption drop-down box as shown in Figure 8.

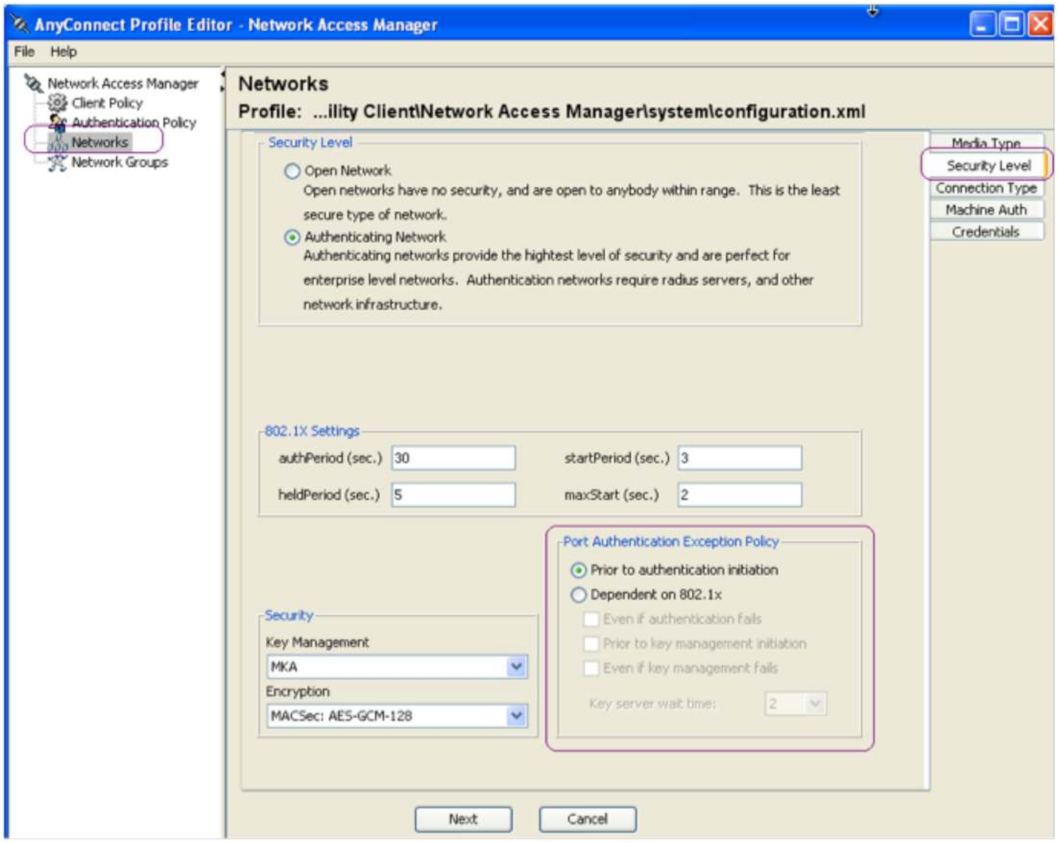
Figure 8. Selecting a MACsec Cipher Suite



3.3.3 Set MACsec Policy

Open the Network Access Manager Profile Editor and select the network you want to enable for MACsec. On the right side of the screen, select the Security Level tab. In the Port Authentication Exception Policy box at the bottom right, select the Prior to Authentication Initiation radio button for Should Secure, as shown in Figure 9. For Must Secure, select Dependent on 802.1X.

Figure 9. Selecting a MACsec Policy



3.3.4 Select an EAP Method.

Open the Network Access Manager Profile Editor and select the network you want to enable for MACsec. On the right side of the screen, select the Machine Auth or User Auth tab. In the EAP Methods box at the top, select an EAP method that supports MSK key derivation (for example, PEAP, EAP-TLS or EAP-FAST),

Figure 10. Selecting a MACsec-Compatible EAP Method

3.4 Monitoring and Troubleshooting

3.4.1 Show Commands

To see the status of a session, use the **show authentication sessions** command on the switch:

```
3750X1-boulder#show authentication sessions interface gigabitEthernet 1/0/25
            Interface:  GigabitEthernet1/0/25
          MAC Address:  000c.2904.8f2f
           IP Address:  192.168.20.202
            User-Name:  host/xp2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
                  SGT:  0000-00
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80A020000000C0604C111
      Acct Session ID:  0x00000011
               Handle:  0x7C00000C
```

The two lines that are relevant to MACsec are shown in bold. The security policy reflects the policy that the switch is following. In this case, it is the default policy, Should Secure. The security status reflects the actual state of the session. In this case, the session status is Secured, indicating that the supplicant was MACsec capable and that the session has been successfully encrypted.

To see detailed parameters and status information for MKA, use the **show mka sessions** command.

```
3750X1-boulder#show mka sessions interface g1/0/25 detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. d0d0.fd25.0119/0002
Interface MAC Address.... d0d0.fd25.0119
MKA Port Identifier...... 2
Interface Name........... GigabitEthernet1/0/25
Audit Session ID......... C0A80A020000000C0604C111
CAK Name (CKN)........... A5B597EBC360C6AB99DFD832521E3D4A
Member Identifier (MI)... FE65D2BE5840C49CE1FAA93B
Message Number (MN)...... 178
Authenticator............ YES
Key Server............... YES
```

```
Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... FE65D2BE5840C49CE1FAA93B00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Cipher Suite............. 0080020001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                         MN          Rx-SCI (Peer)
  ---------------------------------------------------------
  F1BBE9EBB3A6DB3C870C3E99  179         000c.2904.8f2f/0000

Potential Peers List:
  MI                         MN          Rx-SCI (Peer)
  ---------------------------------------------------------
```

For parameters and statistics related to the encrypted session, use the **show macsec interface** command:

```
3750X1-boulder#show macsec interface g1/0/25
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
```

```
 Ciphers supported : GCM-AES-128
Transmit Secure Channels
 SCI : D0D0FD2501190002
  Elapsed time : 00:07:55
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (145 / 0)
Receive Secure Channels
 SCI : 000C29048F2F0000
  Elapsed time : 00:07:55
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 122         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 10730
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 15390
  Ingress miss pkts 10676
```

3.4.2 Debug Commands

Most MACsec-related problems can be debugged using one of three debug commands: **debug mka, debug macsec**, and **debug authentication**. See Section 3.4.4 for specific examples.

3.4.3 Syslogs

Cisco Catalyst switches generate multiple syslogs that can be used to monitor the status of MACsec. Syslogs provide additional information about MACsec sessions. Cisco switches generate syslogs under the conditions listed here. Sample syslogs for each condition are also shown.

- Session start %MKA-5-SESSION_START: (Gi1/0/25 : 2) MKA Session started for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, AuthMgr-Handle FB00000D
- Session secure %MKA-5-SESSION_SECURED: (Gi1/0/25 : 2) MKA Session was secured for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, CKN 8420E74ED289486AAA7FD1A1B1F57DD6
- Reauth %MKA-5-SESSION_REAUTH: (Gi1/0/25 : 2) Reauthenticating for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, AuthMgr-Handle FB00000D, Old CKN 8420E74ED289486AAA7FD1A1B1F57DD6
- Reauth success %MKA-6-SESSION_REAUTH_SUCCESS: (Gi1/0/25 : 2) MKA Session reauthenticated successfully for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, New CKN 98857669040591FB3153B1236DB9BA42

- Rekey %MKA-6-SAK_REKEY: (Gi1/0/25 : 2) MKA Session is beginning a SAK Rekey (current Latest AN/KN 0/1, Old AN/KN 0/1) for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, CKN 98857669040591FB3153B1236DB9BA42
- Rekey success %MKA-6-SAK_REKEY_SUCCESS: (Gi1/0/25 : 2) MKA Session successfully completed a SAK Rekey (new Latest AN/KN 1/2, Old AN/KN 0/1) for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, CKN 98857669040591FB3153B1236DB9BA42
- MKA Timeout %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/25 : 2) Peer has stopped sending MKPDUs for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, CKN 98857669040591FB3153B1236DB9BA42
- Termination %MKA-5-SESSION_STOP: (Gi1/0/25 : 2) MKA Session stopped by MKA for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000D061156FB, CKN 98857669040591FB3153B1236DB9BA42
- Session Unsecured %MKA-4-SESSION_UNSECURED: (Gi1/0/25 : 2) MKA Session was stopped by MKA and not secured for RxSCI 000c.2904.8f2f/0000, AuditSessionID C0A80A020000000E0615AE3E, CKN E4CF9E37274E22DF42BC932D93375935
- Must Secure Failed %AUTHMGR-7-RESULT: Authentication result 'linksec fail' from 'dot1x' for client (0050.56aa.6324) on Interface Fa0/1 AuditSessionID C0A80A0200000027235313C6

Note: Depending on the circumstances, the Session Unsecured syslog may not be generated for all cases in which a session is not secured. The absence of a Session Secured syslog is a more reliable indicator that a Should Secure session failed to secure.

If your platform supports the Cisco Embedded Syslog Manager (ESM), use it to filter unwanted MACsec syslogs. The Cisco Catalyst 3750-X and 3560-X Series Switches do not currently support Cisco ESM. The only other option is to use logging severity to filter syslogs. For example, if you globally configure **logging console 4**, only the syslog messages with a severity of 4 or lower will be displayed on the console. Be aware that this configuration applies to all syslogs, not just MACsec syslogs, so be sure you are not filtering necessary syslogs from other facilities when you filter by severity.

3.4.4 Troubleshooting

Table 6 provides troubleshooting information for common problems.

Table 6. Troubleshooting Information

Symptom	Additional Information	Possible Causes	Resolution
Session is not secure	**debug mka error** contains **MKA-ERR: Interface does not have MACsec enabled while trying to create a new MKA Session.**	Interface configuration does not contain **macsec**.	Configure **macsec** on the interface.
Session is not secure	**debug mka contains MKA-LLI: No policy applied on the interface.**	Interface configuration does not contain **mka default-policy** or **mka policy**.	Configure an MKA policy on the interface.
Session is not secure	**debug authentication** contains **AUTH-EVENT LinkSec not allowed on multi-auth port.**	Port is configured for multi-auth.	Disable multi-auth on MACsec ports.
Session is not secure	**debug mka** contains **MKA-LLI: No Keys.**	EAP method does not support MSK.	Configure the supplicant and authentication server with an EAP type that supports MKA.
Session is not secure	Syslog contains **%MKA-4-SESSION_UNSECURED.**	Supplicant was not enabled for MACsec.	Enable MACsec on the supplicant.
Authentication failed	Syslog contains **%AUTHMGR-7-RESULT: Authentication result 'linksec fail'**.	Supplicant or switch did not support MACsec, and MACsec policy was Must Secure.	Change MACsec policy to Should Secure.
Switch does not apply MACsec policy from Authentication server	Local switch MACsec policy is enforced.	Switch was not configured to accept authorization instructions from the authentication server.	Add the line **aaa authorization network default group radius** to the global authentication, authorization, and accounting (AAA) configuration.

4. Conclusion

MACsec offers outstanding confidential, identity-based access control at the network edge. With the appropriate design and well-chosen components, you can meet the needs of your security policy while reducing the impact on your infrastructure and end users.

5. For More Information

IEEE 802.1X Quick Reference Guide:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_c27-574041.pdf

IEEE 802.1X Deployment Scenarios Design Guide:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html

IEEE 802.1X Deployment Scenarios Configuration Guide:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/Whitepaper_c11-532065.html

6. MACsec Terminology

Table 7 defines some common MACsec terminology.

Table 7. MACsec Terminology

MKA	MACsec key agreement	Defined in IEEE 802.1X-2010, MKA is a key agreement protocol for discovering MACsec peers and negotiating the keys used by MACsec.
SAP	Security Association Protocol	This pre-standard key agreement protocol is similar to MKA.
MSK	Master session key	Generated during the EAP exchange, the MSK is used to generate the CAK.
CAK	Connectivity association key	Derived from the MSK, the CAK is a long-lived master key that is used to generate all other keys needed for MACsec.
SAK	Secure association key	Derived from the CAK, the SAK is the encryption key used to encrypt traffic for a given session.

Printed in USA C17-663760-00 05/11