Cisco TrustSec™ 3.0 How-To Guide: Introduction to MACSec and NDAC
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>MACsec</td>
<td>4</td>
</tr>
<tr>
<td>Downlink MACsec</td>
<td>4</td>
</tr>
<tr>
<td>ISE Configuration</td>
<td>7</td>
</tr>
<tr>
<td>Uplink MACsec</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Uplink MACsec</td>
<td>8</td>
</tr>
<tr>
<td>Network Device Admission Control</td>
<td>11</td>
</tr>
<tr>
<td>Creating an NDAC Domain</td>
<td>12</td>
</tr>
<tr>
<td>Configuring Seed Devices</td>
<td>15</td>
</tr>
<tr>
<td>Adding Non-Seed Switches</td>
<td>17</td>
</tr>
<tr>
<td>Configuring the Switch Interfaces for Both Seed and Non-Seed Devices</td>
<td>19</td>
</tr>
<tr>
<td>MACsec Sequence in an NDAC Domain</td>
<td>20</td>
</tr>
</tbody>
</table>

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
Introduction

When Wi-Fi was first introduced into the consumer and corporate space, security concerns were raised around sensitive data being transmitted through the air, without any level of confidentiality. The initial solution was Wired Equivalency Protection (WEP). While not very secure, WEP provided an extra level of protection designed to bring wireless connections to the same security level as wired networks.

Wireless networks quickly became more secure than wired networks, with solutions like 802.1X authentication and enhancements to encryption and keying mechanisms, such as Wi-Fi Protected Access (WPA/WPA2) using AES encryption. This gave wireless networks full encryption mechanisms to provide the confidentiality and integrity of data traversing the Layer 2 hop from the endpoint to the network infrastructure, in addition to the strong identity capabilities of 802.1X.

Next, "wireless equivalency" was needed for wired networks so that they could provide equivalent confidentiality and integrity. One approach that was considered was using end-to-end IPSec, encrypting entire communications from end to end. However, QoS cannot be provided when a packet’s contents are not visible: It wasn’t possible to ensure security while encrypting both good and bad traffic across the network.

The way to provide wireless equivalency - and a viable alternative to end-to-end IPSec - was to layer on the confidentiality and integrity using IEEE 802.1AE (MACsec). MACsec provides Layer 2 encryption on the LAN between endpoints and the switch as well as between the switches themselves (Figure 1).

---

Figure 1. MACsec Layer-2 Hop-by-Hop Encryption

---
MACsec

MACsec provides Layer 2 encryption on the LAN. It also encapsulates and protects the metadata field that carries the Security Group TAG (SGT), as described in the Cisco TrustSec® How-To Guide.

Currently, two keying mechanisms are available: Security Association Protocol (SAP) and MAC Security Key Agreement (MKA). SAP is a proprietary Cisco® keying protocol used between Cisco switches. MKA will be the industry standard, and is currently used between endpoints and Cisco switches. Both use 128-bit AES-GCM (Galois/Counter Mode) symmetric encryption, which is capable of line-rate encryption and decryption for both 1 GB and 10 GB Ethernet interfaces, and provides replay attack protection of every frame.

Downlink MACsec

“Downlink MACsec” is the term used to describe the encrypted link between an endpoint and the switch. The encryption between the endpoint and the switch is handled by the MKA keying protocol. This requires a MACsec-capable switch (such as a Cisco Catalyst® 3750-X Series switch) and a MACsec-capable supplicant on the endpoint (such as the Cisco AnyConnect® Network Access Manager). The encryption on the endpoint may be handled in hardware (if the endpoint possesses the correct hardware) or in software using the main CPU for the encryption and decryption.

The Cisco switch has the ability to force encryption, make encryption optional, or force non-encryption; this setting may be configured manually per port (not very common) or dynamically as an authorization result from the Cisco Identity Services Engine (ISE) (much more common). If ISE returns an encryption policy with the authorization result, the policy issued by ISE overrides anything set using the switch CLI.

Figure 2 shows the MACsec policy within an authorization profile on ISE. Under Attributes Details, you can see that the attribute sent to the switch is cisco-av-pair=subscriber:linksec-policy, followed by the policy itself. The choices are “Must-Secure,” “Should-Secure,” and “Must-Not-Secure.” Example 1 shows these options on the switch CLI, and Table 1 displays the resulting policy based on the Supplicant Policy and Switch Policy.

Figure 2. Authorization Profile
Example 1  MACsec Policy Switch CLI

```bash
C3750X(config-if)#authentication linksec policy?
must-not-secure  Never secure sessions
must-secure Always secure sessions
should-secure OPTIONALLY secure sessions
```

Table 1. Resulting MACsec Policies

<table>
<thead>
<tr>
<th>Supplicant Policy</th>
<th>Switch Policy</th>
<th>Resulting Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Supplicant Not Capable of MACsec</td>
<td>Not MACsec-Capable</td>
<td>Not Secured</td>
</tr>
<tr>
<td></td>
<td>Must-Not-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Must-Secure</td>
<td>Blocked or Fallback</td>
</tr>
<tr>
<td>Client Supplicant Configured as “Must-Not-Secure”</td>
<td>Not MACsec-Capable</td>
<td>Not Secured</td>
</tr>
<tr>
<td></td>
<td>Must-Not-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Must-Secure</td>
<td>Blocked or Fallback</td>
</tr>
<tr>
<td>Client Supplicant Configured as “Should-Secure”</td>
<td>Not MACsec-Capable</td>
<td>Not Secured</td>
</tr>
<tr>
<td></td>
<td>Must-Not-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should-Secure</td>
<td>Secured</td>
</tr>
<tr>
<td></td>
<td>Must-Secure</td>
<td></td>
</tr>
<tr>
<td>Client Supplicant Configured as “Must-Secure”</td>
<td>Not MACsec-Capable</td>
<td>Blocked</td>
</tr>
<tr>
<td></td>
<td>Must-Not-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should-Secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Must-Secure</td>
<td>Secured</td>
</tr>
</tbody>
</table>

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 of “Should-Secure.”

Switch Configuration Modes

Some of the configurations on the switch interface have implications for a MACsec deployment; an example is the authentication host mode. The host mode determines the number of endpoints that may be connected to a single switch interface.

- **Single-Host Mode**: MACsec is fully supported in single-host mode. In this 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, a security violation will be triggered on the port.
Multi-Domain Authentication (MDA) Mode: In this mode, one endpoint may be on the data domain and another endpoint may be on the voice domain. MACsec is fully supported in MDA mode. 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-Authentication Mode: In this mode, a virtually unlimited number of endpoints may be authenticated to a single switch port. MACsec is not supported in this mode.

Multi-Host Mode: While MACsec usage in this mode is technically possible, it is not recommended. In Multi-Host Mode, the first endpoint on the port authenticates, and then any additional endpoints will be permitted onto the network via the first authorization. MACsec would work with the first connected host, but no other endpoint’s traffic would actually pass, since it would not be encrypted traffic.

Example 2 shows a switch interface configuration for MACsec-enabled endpoints. The example is using the default MACsec policy of “Should-Secure”; therefore, the default setting is displayed.

Example 2  
Switch Interface Configuration for MACsec

```plaintext
interface X
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 2274
authentication event server alive action reinitialize
authentication event linksec fail action next-method
authentication host-mode multi-domain
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
macsec
mka default-policy
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
end
```
ISE Configuration
Downlink MACsec is configured as an attribute within the Authorization Profile (the result of an authorization).

Procedure 1  Add This Result to an Authorization Profile (see Figure 3)
Step 1. Navigate to Policy → Policy Elements → Results.
Step 2. Choose Authorization Profiles.
Step 3. Edit an Authorization Profile that you would like to add MACsec to (PCI was used in our example).
Step 4. Under Common Tasks, scroll down to MACsec Policy.
Step 5. Select must-secure, should-secure, or must-not-secure.
Step 6. Click Submit or Save to save the change.

Figure 3. Adding MACsec to an Authorization Profile

Uplink MACsec
“Uplink MACsec” is the term used to describe encrypting the link between the switches with 802.1AE. At the time this guide was written, the switch-to-switch encryption uses Cisco’s proprietary SAP instead of MKA, which is used with the downlink MACsec. The encryption is still the same AES-GCM-128 encryption used with both uplink and downlink MACsec.

Uplink MACsec may be achieved manually or dynamically. Dynamic MACsec requires 802.1X between the switches; this is covered in the Network Device Admission Control (NDAC) section. Here, we are focusing on manual mode.
Configuring Uplink MACsec

Procedure 1  Manually Configuring Uplink MACsec

This method of MACsec is perfect to layer on top of the manual SGTs configured as part of the Cisco TrustSec How-To Guide. Manual configuration will encrypt the interswitch links without requiring the entire domain of trust, the way that NDAC does. It also removes the dependency on ISE for the link keying, similar to how an IPSec tunnel may be built using pre-shared keys.

Let’s start by re-examining the configuration of our uplink interface as we had it configured at the end of the Cisco TrustSec How-To Guide.

Example 3  Uplink Configuration from the Cisco TrustSec How-To Guide

```
C3750X# show run int Ten 1/1/1
Building configuration...

Current configuration : 286 bytes
!
interface TenGigabitEthernet1/1/1
  description Cat6K Ten1/5
  no switchport
  ip address 10.1.48.2 255.255.255.252
  ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 EIGRP
  load-interval 60
  cts manual
  policy static sgt 2 trusted
  no macro auto processing
end
```

With the configuration shown in Example 3, our uplink between the Cisco Catalyst 3750-X and the Cisco Catalyst 6500-Sup2T is set up to use manual keying without any encryption, but to apply SGTs to the frames. Now we will layer encryption on top of this to provide confidentiality and integrity of the SGTs and the data. Figure 4 depicts the relevant infrastructure configuration used for this example.

Figure 4.  Adding MACsec to the Uplink
Step 7. From interface configuration mode, enter **cts manual**.

Step 8. Enable encryption with the **sap pmk pairwise-master-key mode-list gcm-encrypt** command.

The Pairwise Master Key (PMK) should be a hexadecimal value configured to be the same on both sides of the link. This master key can be compared to a RADIUS shared-secret between a NAD and ISE, or even the pre-shared key used with IPSec encryption.

**Note:** There is a difference in how the PMK is padded between Nexus® and Catalyst platforms if the key is less than 64 hex digits. On a Catalyst switch, the PMK is padded with leading 0’s. On a Nexus switch, the PMK is padded with trailing zeros. To resolve this, on the Nexus add “left zero padded” to the command (e.g., “sap pmk 26 left-zero-padded mode-list gcm-encrypt”).

**Note:** The PMK is just one of the components used to derive the session keys that are used to encrypt traffic. Therefore it is important to keep in mind that static configuration of the PMK, as shown above, does not mean that session keys are not dynamically derived.

Step 9. Add the **sap pmk pairwise-master-key mode-list gcm-encrypt** command to the other side of the link.

Step 10. Done.

Example 4 displays the example configuration steps, and Example 5 shows the final configuration for the uplink port on the Cisco Catalyst 3750-X.

### Example 4 Adding Encryption to the Uplink Interface

```
C3750X#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C3750X(config)#int Ten1/1/1
C3750X(config-if)#cts manual
C3750X(config-if-cts-manual)#sap pmk 26 mode-list gcm-encrypt
C3750X(config-if-cts-manual)#end

C3750X#
```

### Example 5 Final Configuration for Uplink Interface

```
C3750X#sho run int ten1/1/1
Building configuration...

Current configuration : 386 bytes
!
interface TenGigabitEthernet1/1/1
description Cat6K Ten1/5
no switchport
ip address 10.1.48.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP
load-interval 60
cts manual
    policy static sgt 2 trusted
```

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
Procedure 2  Verifying the Manual Configuration

We can validate that the manual encryption on the uplink was successful with the show cts interface command, as shown in Example 6. SAP status is the status of the encryption, and we can see in the example that SAP succeeded, the pairwise cypher is using gcm-encrypt, and replay protection is enabled.

Example 6  Output of show cts interface Command

```
sap pmk 0000000000000000000000000000000000000000000000000000000000000026 mode-list gcm-encrypt
no macro auto processing
end
```

C3750X#show cts interface TenGigabitEthernet 1/1/1
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/1/1:
  CTS is enabled, mode: MANUAL
  IFC state: OPEN
  Authentication Status: NOT APPLICABLE
  Peer identity: "unknown"
  Peer's advertised capabilities: "sap"
  Authorization Status: SUCCEEDED
  Peer SGT: 2
  Peer SGT assignment: Trusted
  SAP Status: SUCCEEDED
  Version: 2
  Configured pairwise ciphers:
    gcm-encrypt

  Replay protection: enabled
  Replay protection mode: STRICT

  Selected cipher: gcm-encrypt

  Propagate SGT: Enabled
  Cache Info:
    Cache applied to link : NONE

  Statistics:
    authc success: 0
    authc reject: 0
    authc failure: 0
    authc no response: 0
    authc logoff: 0
    sap success: 2
    sap fail: 0
As you can see from this section, little configuration is needed to use manual uplink MACsec, assuming you are using MACsec-capable hardware. However, there is still this concept of a “domain of trust” with the secure access solution, where we can authenticate and authorize any network devices before allowing them to participate in our infrastructure. To examine that domain of trust further, we will now discuss Network Device Admission Control (NDAC).

Network Device Admission Control

The Cisco Secure Unified Access architecture builds secure networks by establishing domains of trusted network devices, preventing, for example, a rogue off-the-shelf switch from connecting to your enterprise network infrastructure and possibly wreaking havoc.

In order for a network device to be part of the network infrastructure and pass traffic, its peer(s) must first authenticate it. We authenticate the switch via 802.1X, much like we are authenticate the endpoints and users. However, once the device is allowed to join the network infrastructure, the communication on the links between devices is secured with MACsec. This process is known as Network Device Admission Control (NDAC).

There are three main roles within NDAC:

- **Supplicant**: The role of an unauthenticated switch that is connected to a peer within the trusted domain and is attempting to join that domain.
- **Authentication server**: The server that validates the identity of the supplicant, issues the policies to allow the device onto the network, and is responsible for the encryption keys. This is the Cisco ISE server.
- **Authenticator**: An authenticated device that is already part of the trusted domain and can authenticate new peer supplicants on behalf of the authentication server.
There is another role, known as a "seed device": a device that has knowledge of at least one ISE Policy Service Node. That seed device begins or creates the NDAC trusted domain (Figure 5). When a new switch is added to the network, a switch that is already a member of the NDAC domain authenticates it. There must be at least one seed device.

**Figure 5. NDAC Seed Device**

Creating an NDAC Domain

An NDAC domain is created when the first switch (the seed device) is authenticated and authorized by ISE.

**Note:** Since the seed device begins the trusted domain, a non-seed device should be configured to perform CTS dot1x between itself and a neighbour device, not ISE.

**Procedure 1 Configuring ISE Network Device Group (see Figure 6)**

Prepare ISE for NDAC and Cisco TrustSec. From the ISE GUI:

- Step 1. Navigate to Administration → Network Resources → Network Device Groups.
- Step 2. Add a new Top-Level Device Group.
- Step 3. Name the Group and the Type "TRUSTSEC".
- Step 4. Create a new NDG named “TRUSTSEC-Device”; the type should be TRUSTSEC.
- Step 5. Create a new NDG named “Non-TRUSTSEC-Device”; type should be TRUSTSEC.
The next step is to add the switch to ISE as a NAD. This may have been completed during the Cisco TrustSec How-To Guide; however, you should go through the screens in ISE and ensure the configuration is correct.

**Procedure 2  Add the NAD to ISE**

From the ISE GUI:

Step 1. Navigate to Administration → Network Resources → Network Devices.

Step 2. If the switch is already in the device list, edit it. If not, add a new device.

Step 3. Ensure the RADIUS shared secret is configured.

Step 4. Set the Network Device Groups. Specifically, assign the NAD to the TRUSTSEC-Device NDG.

Step 5. Enable the “Advanced TrustSec Settings” section of the NAD definition (see Figure 7).

Step 6. You may use the device-id for TRUSTSEC Identification, or you may configure a new name here.  

**Note:** This name must match what you configure on the switch in later steps.

Step 7. The device configuration deployment section is to allow ISE to push SGT-to-IP mappings to the switch. This is optional, but if you want that functionality you should add the exec and enable passwords.

Step 8. Click Save.

Step 9. Repeat Steps 1 through 8 for all network devices that will participate in the NDAC trusted domain.

**Figure 7.** Advanced TrustSec Settings

Once you submit a network device with the Advanced TrustSec Settings configured, the device name and password are added to a special internal identity store, known as “Internal CTS Devices.” This identity store is what will be used for the NDAC authentications.
Procedure 3   Add the Cisco TrustSec AAA Servers

The big difference between seed and non-seed devices is whether a device is configured with the list of AAA servers for NDAC. A new device gets the list of AAA servers from the seed device. To build the list of AAA servers to be sent to non-seed devices, add it to the SGA AAA Servers list within ISE (Figure 8).

Step 1.  Navigate to Administration → Network Resources → SGA AAA Servers

Step 2.  Click Add

Step 3.  Enter the PSN name

Step 4.  Enter the PSN IP Address

Step 5.  Click Submit

Step 6.  Repeat Steps 2 through 5 for all PSNs that will be involved with NDAC

Figure 8.  SGA AAA Servers

Procedure 4   Create the Network Authorization Policy

We need to create a network authorization policy for the switches to be assigned an SGT and permitted to join the NDAC trusted domain (Figure 9). The switches get assigned a SGT so that packets originating from the device are also tagged. Switch-originated traffic can also be subject to SG-ACL filtering.


Step 2.  Insert a rule above the default rule.

Step 3.  Name the rule “TRUSTSEC Devices”.

Step 4.  Set the condition to be TRUSTSEC equals TRUSTSEC-Device. This is using the network device group we created earlier in this guide.

Step 5.  Set the resulting Security Group to be the “NADs” group created in the Cisco TrustSec How-To Guide (SGT = 2).

Step 6.  Click Done.

Step 7.  Click Save.
Configuring Seed Devices

Now that ISE is prepared, it is time to configure the first switch of the NDAC trusted domain (the seed device). For this example, we will use the Nexus core switch as the seed device, as was shown in Figure 5. All switches may be configured as seed devices.

Procedure 1 Configure a Seed Device

From the switch CLI:

Step 1. Enter `show dot1x` to see if the feature is enabled from the “Introduction to Cisco TrustSec” guide. If it is not, then type `feature dot1x` from global configuration mode.

Step 2. Enter `show cts` and validate that the feature is enabled from the “Introduction to Cisco TrustSec” Guide. If not, then type `feature cts` from global configuration mode.

Step 3. Set the CTS device-id at global configuration mode using the `cts device-id` `device-id password password` command.

**Note:** This device-id and password must match exactly what was configured in the Network Device definition within ISE.

Step 4. Add ISE to the configuration with the `radius-server host ip-address key shared-secret pac`.

**Note:** The pac keyword is used to configure the Nexus switch to download a Protected Access Credential (PAC) that will be used to secure the RADIUS transactions.

Step 5. Repeat Step 4 for all applicable RADIUS servers.

Step 6. Create a RADIUS server group with the `aaa group server radius group-name` command.

Step 7. Add the servers to the group with the `server ip-address` command.

Step 8. Repeat Step 7 for all applicable servers.

Step 9. Configure the RADIUS server group to use the correct VRF with the `use-vrf vrf-name` command.

Step 10. Configure AAA authentication for 802.1x with the `aaa authentication dot1x default group radius-group-name` command.

Step 11. Configure AAA accounting for 802.1x with the `aaa accounting dot1x default group radius-group-name` command.

Step 12. Configure CTS authorization for 802.1x with the `aaa authorization cts default group radius-group-name` command.
Step 13. Reenter the `cts device-id device-id password password` command to trigger an immediate download of the PAC file.

**Note:** Below are examples of seed device configuration for NX-OS and IOS switches. Please note the syntax differences.

Example 7 shows an example configuration on the Nexus 7000 Series core switch.

**Example 7 Configuring the Nexus 7000 Seed Device**

```
NX7K-CORE(config)# cts device-id NX7K-CORE password Cisco123
NX7K-CORE(config)# radius-server host 10.1.103.4 key Cisco123 pac
NX7K-CORE(config)# aaa group server radius ise
NX7K-CORE(config-radius)# server 10.1.103.4
NX7K-CORE(config-radius)# use-vrf default
NX7K-CORE(config)# cts device-id NX7K-CORE password Cisco123
NX7K-CORE(config)# show cts pac
PAC Info :

==============================
PAC Type            : Trustsec
AID                 : 01ecb966907841dd6af9cdfc810c3d4e
I-ID                : NX7K-CORE
AID Info            : Identity Services Engine
Credential Lifetime : Wed Mar 27 14:51:01 2013
PAC Opaque          : 000200b8000300010004001001ecb966907841dd6af9cdfc810c3d4e
                          0006009c00030100eb281fae6759891966c609335bb71930000001350d502f300093a805f1acdc863015e76decdb96e98d628146738491ef414d34d5c4685d09fded04dbfbb46eebe17174e4b75403a10e29014032189c3c1eba408261f5862dabae1e9c275b2c264267bdc1333beaa370aa7e49f97e0c353b620badb4ca00a185af6fb1b7e0c5a12407c7ecfd2284f2aa50e168640040eeefe8ca9c47d
NX7K-CORE(config)#
NX7K-CORE(config)# show cts environment-data
CTS Environment Data

==============================
Current State            : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
Last Status              : CTS_ENV_SUCCESS
Local Device SGT         : 0x0002
Transport Type           : CTS_ENV_TRANSPORT_DIRECT
Data loaded from cache   : FALSE
```

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
Example 8 shows an example configuration on the Catalyst 6500 Series Sup2T Distribution Switch.

**Example 8  Configuration of a Catalyst 6500 Seed Device**

```plaintext
C6K-DIST# cts credentials id C6K-DIST password Cisco123
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.

C6K-DIST(config)# cts authorization list default
C6K-DIST(config)# radius-server host 10.1.103.3 auth-port 1812 acct-port 1813 test
username radius-test pac key Cisco123
Request successfully sent to PAC Provisioning driver.

C6K-DIST(config)# radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 test
username radius-test pac key Cisco123
Request successfully sent to PAC Provisioning driver.

Note: the pac keyword in the radius-server configuration is essential, to ensure the RADIUS communication between the switch and ISE is secured for NDAC.

C6K-DIST(config)# radius-server vsa send authentication !(this will most likely be configured already)
C6K-DIST(config)# dot1x system-auth-control !(this will most likely be configured already)
```

**Adding Non-Seed Switches**

A non-seed device does not have a configuration to locate the AAA servers to use with NDAC. Instead, the list is downloaded from the seed device. However, the device still needs to be added to ISE as a network device, which we did in an earlier procedure within this guide.

Using non-seed devices is not required, but it is a viable option and therefore will be covered in this guide. For these examples, we will configure the Cisco Catalyst 3750X as a non-seed device; all other switches are configured as seed devices. (See Figure 10)
Figure 10. NDAC Trusted Domain

Procedure 1 Configure a Non-Seed Device

The majority of the configuration required for a non-seed device is accomplished when bootstrapping the device to work with ISE in the Bootstrap How-To Guide.

Step 1. The CTS credentials will need to be entered into the device, just as with the seed device.

Example 9 Cisco Catalyst 3750-X Non-Seed Device Configuration

```
C3750X#cts credentials id C3750X password Cisco123
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.
```

Step 2. The next set of commands should already be configured in the switch from the Bootstrap How-To Guide.

```
C3750X(config)#aaa new-model
C3750X(config)#aaa authentication dot1x default group radius
C3750X(config)#aaa authorization network default group radius
C3750X(config)#aaa accounting dot1x default start-stop group radius
C3750X(config)#radius-server vsa send authentication
C3750X(config)#dot1x system-auth-control
```
Configuring the Switch Interfaces for Both Seed and Non-Seed Devices

Now that the global configuration is taken care of, we can enter the commands to be part of NDAC.

Procedure 1  Enable NDAC on the Interface

Enter the `cts dot1x` command on the switch interfaces that are to be trusted in NDAC.

Example 10  Enabling NDAC on the Interface

```
C3750X(config)#int Ten1/1/1
C3750X(config-if)#cts dot1x
C3750X(config-if-cts-dot1x)#
```

To verify the interface activities, use the `show cts interface interface-name` command.

```
C6K-DIST#sho cts interface
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/5:
   CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Authentication Status:   SUCCEDED
   Peer identity:       "C3750X"
   Peer's advertised capabilities: "sap"
   802.1X role:    Authenticator
   Reauth period configured:     86400 (default)
   Reauth period per policy:      86400 (server configured)
   Reauth period applied to link:  86400 (server configured)
   Reauth starts in approx. 0:14:11:09 (dd:hr:mm:sec)
   Authorization Status:         SUCCEDED
   Peer SGT:            2:NADs
   Peer SGT assignment: Trusted
   SAP Status:              SUCCEDED
   Version:             2
   Configured pairwise ciphers:
      gcm-encrypt
      null

   Replay protection: enabled
   Replay protection mode: STRICT

   Selected cipher:       gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
      Cache applied to link : NONE
```
MACsec Sequence in an NDAC Domain

When the link between a supplicant and an authenticator first comes up, the following sequence of events typically occurs:

1. **Authentication:** Using NDAC, ISE authenticates a device using EAP-FAST before allowing it to join the network. During the EAP-FAST exchange, ISE creates and sends a unique PAC to the supplicant switch (the switch attempting to join the NDAC domain). That PAC contains a shared key and an encrypted token to be used for future secure communications with the authentication server.

2. **Authorization:** Based on the identity information of the supplicant switch, ISE provides authorization policies to each of the linked peers. The authentication server provides the identity of each peer to the other, and each peer then applies the appropriate policy for the link.

3. **Security Association Protocol (SAP) negotiation:** When both sides of a link support encryption, the supplicant and the authenticator negotiate the necessary parameters to establish a security association (SA), and encrypt the traffic.

When all three steps are complete, the authenticator changes the state of the link from the unauthorized (blocking) state to the authorized state, and the supplicant switch becomes a member of the NDAC trusted domain.