TrustSec Cloud with 802.1x MACsec on Catalyst 3750X Series Switch Configuration Example

Contents

Introduction

This article describes the steps required in order to configure a Cisco TrustSec (CTS) cloud with link encryption between two Catalyst 3750X Series switches (3750X).

This article explains the switch-to-switch Media Access Control Security (MACsec) encryption process that uses Security Association Protocol (SAP). This process uses the IEEE 802.1x mode instead of manual mode.

Here is a list of the steps involved:

- Protected Access Credential (PAC) provisioning for seed and non-seed devices
- Network Device Admission Control (NDAC) authentication and MACsec negotiation with SAP for key management
- Environment and policy refresh
- Port authentication for clients

- Traffic tagging with the Security Group Tag (SGT)
- Policy enforcement with the Security Group ACL (SGACL)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of CTS components
- Basic knowledge of CLI configuration of Catalyst switches
- Experience with Identity Services Engine (ISE) configuration

Components Used

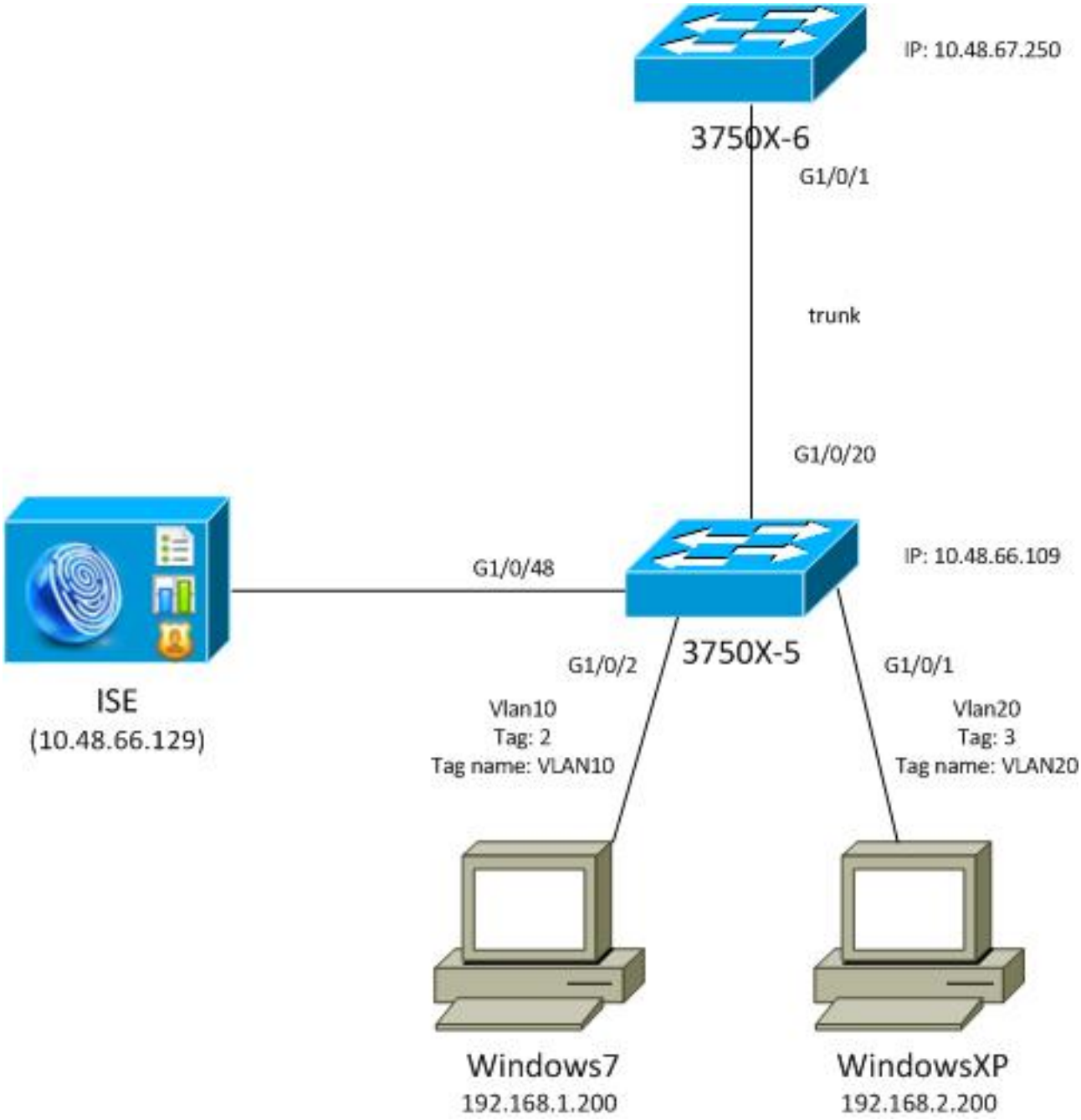
The information in this document is based on these software and hardware versions:

- Microsoft (MS) Windows 7 and MS Windows XP
- 3750X Software, Versions 15.0 and Later
- ISE Software, Versions 1.1.4 and Later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



In this network topology diagram, the 3750X-5 switch is the seed device that knows the IP address of the ISE, and it automatically downloads the PAC that is used for subsequent authentication in the CTS cloud. The seed device acts as an 802.1x authenticator for non-seed devices. The Cisco Catalyst 3750X-6 Series switch (3750X-6) is the non-seed device. It acts as an 802.1x supplicant to the seed device. After the non-seed device authenticates to the ISE through the seed device, it is permitted access to the CTS cloud. After a successful authentication, the 802.1x port status on the 3750X-5 switch is changed to **authenticated**, and MACsec encryption is negotiated. Traffic between the switches is then tagged with SGT and encrypted.

This list summarizes the expected traffic flow:

- The seed 3750X-5 connects to the ISE and downloads the PAC, which is later used for an environment and policy refresh.
- The non-seed 3750X-6 performs 802.1x authentication with the supplicant role in order to authenticate/authorize and download the PAC from the ISE.
- The 3750X-6 performs a second 802.1x Extensible Authentication Protocol-Flexible Authentication via Secure Protocol (EAP-FAST) session in order to authenticate with the

protected tunnel based on the PAC.
- The 3750X-5 downloads SGA policies for itself and on behalf of 3750X-6.
- An SAP session occurs between the 3750X-5 and 3750X-6, MACsec ciphers are negotiated, and the policy is exchanged.
- Traffic between the switches is tagged and encrypted.

Configure Seed and Non-Seed Switches

The seed device (3750X-5) is configured in order to use the ISE as a RADIUS server for CTS:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

cts authorization list ise

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

Role-Based Access Control List (RBACL) and Security Group Based Access Control List (SGACL) enforcement are enabled (they are used later):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

The non-seed device (3750X-6) is configured only for Authentication, Authorization, and Accounting (AAA) without the need for RADIUS or CTS authorization:

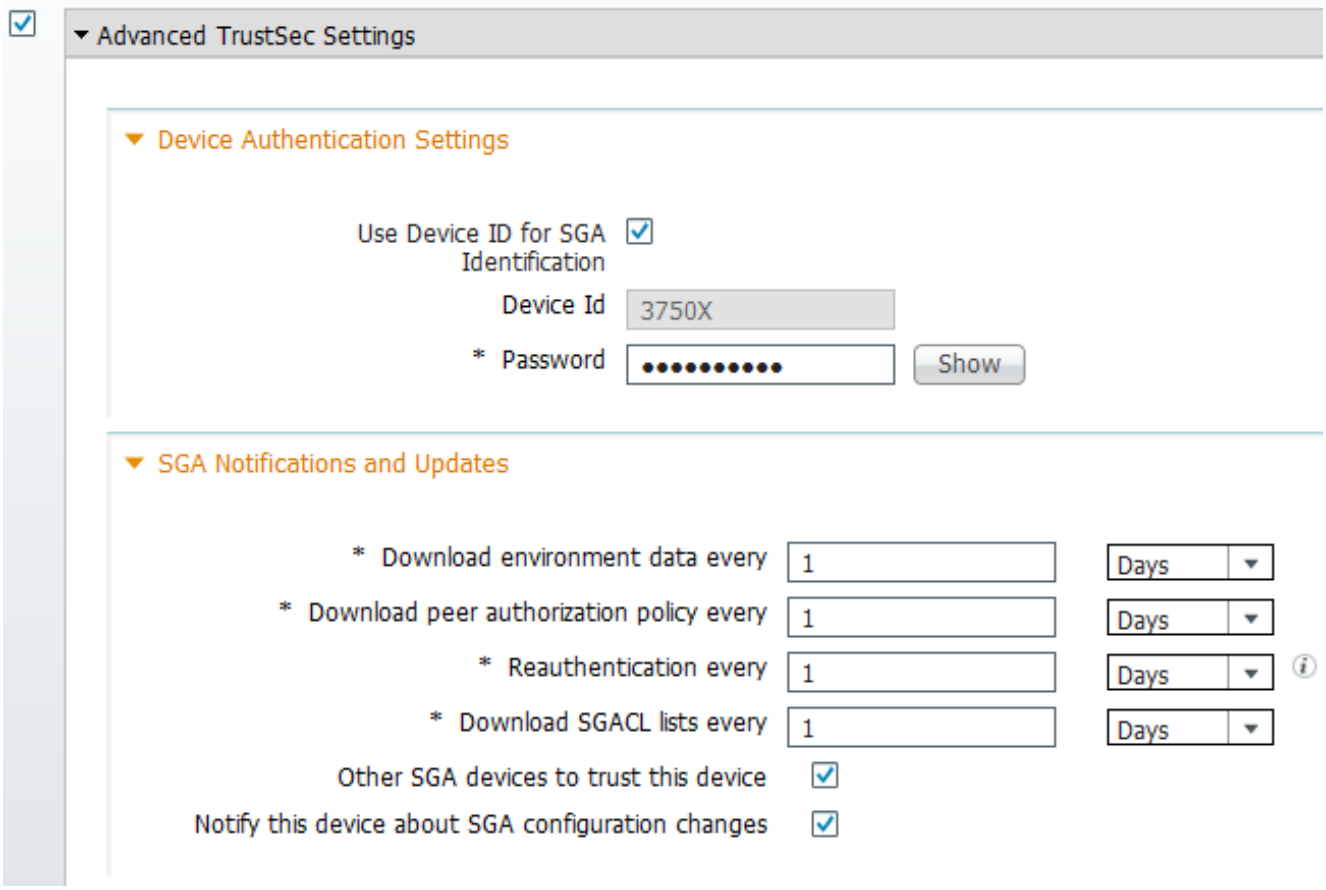
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Before you enable 802.1x on the interface, it is necessary to configure the ISE.

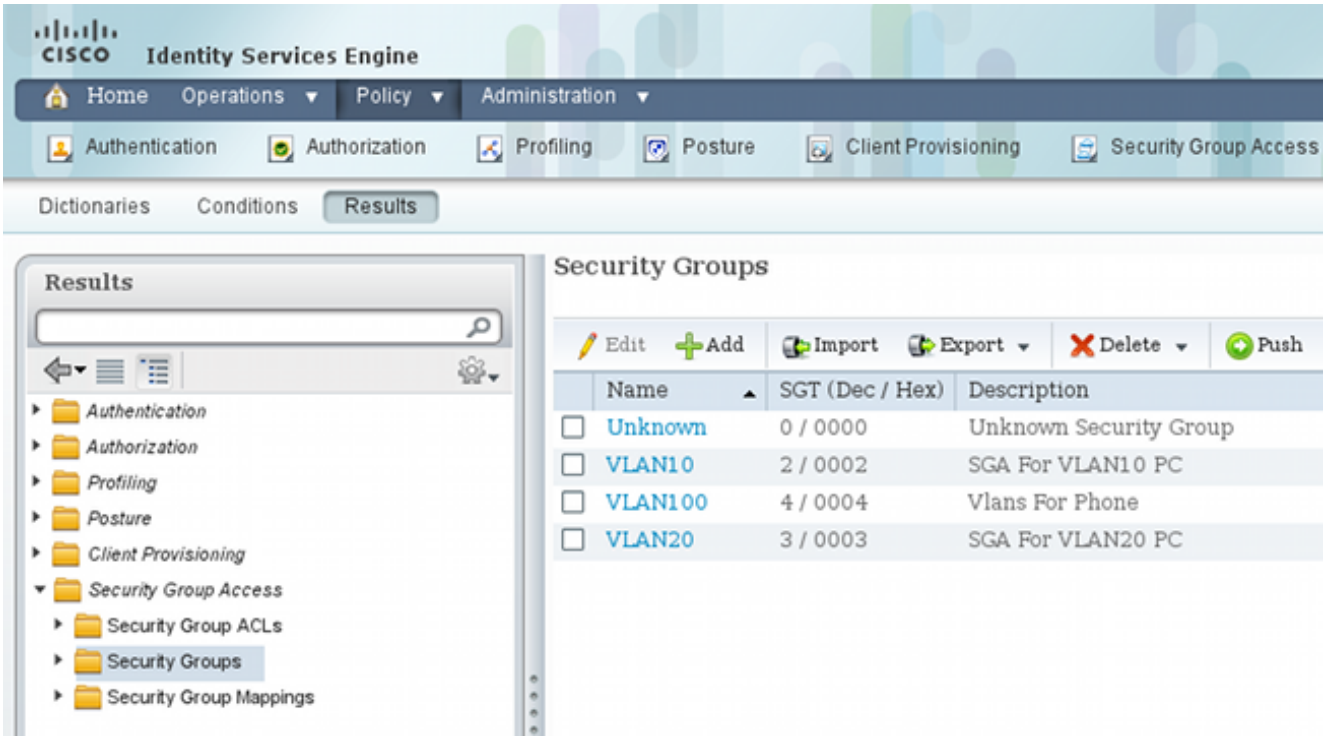
Configure the ISE

Complete these steps in order to configure the ISE:

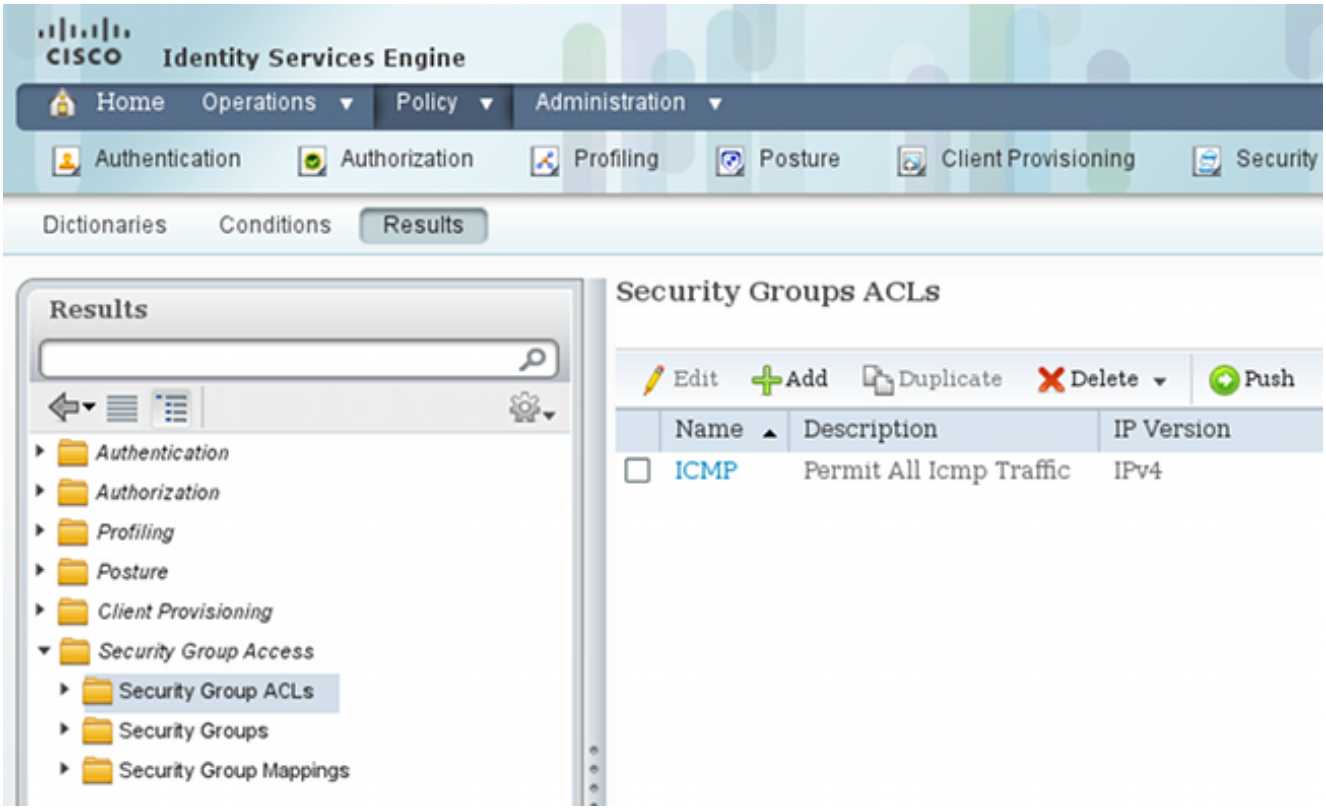
1. Navigate to **Administration > Network Resources > Network Devices**, and add both switches as Network Access Devices (NADs). Under **Advanced TrustSec Settings**, configure a CTS password for later use on the switch CLI.



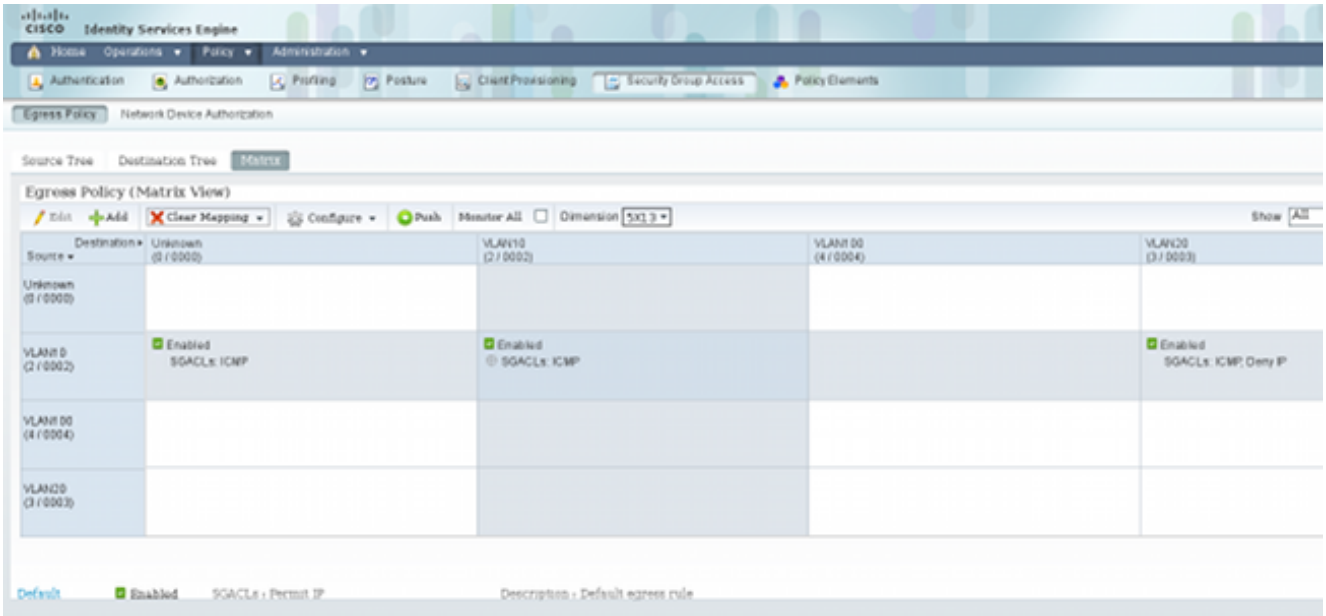
2. Navigate to **Policy > Policy Elements > Results > Security Group Access > Security Groups**, and add the appropriate SGTs. These tags are downloaded when switches request an environment refresh.



3. Navigate to **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**, and configure a SGACL.



4. Navigate to **Policy > Security Group Access**, and define a policy with the matrix.



Note: You must configure the authorization policy for the MS Windows supplicant, so that it receives the correct tag. Refer to [ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide] for a detailed configuration for this.

PAC Provisioning for the 3750X-5

PAC is needed for authentication in the CTS domain (as phase1 for EAP-FAST), and it is also used in order to obtain environment and policy data from the ISE. Without the correct PAC, it is not possible to obtain that data from the ISE.

After you provide the correct credentials on the 3750X-5, it downloads the PAC:

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

The PAC is downloaded via EAP-FAST with Microsoft's Challenge Handshake Authentication Protocol (MSCHAPv2), with the credentials provided in CLI and the same credentials configured on the ISE.

The PAC is used for the environment and policy refresh. For those switches, use RADIUS requests with **cisco av-pair cts-pac-opaque**, which is derived from the PAC key and can be decrypted on the ISE.

PAC Provisioning for the 3750X-6 and NDAC Authentication

In order for a new device to be able to connect to the CTS domain, it is necessary to enable 802.1x on the corresponding ports.

SAP protocol is used for key management and cipher suite negotiation. Galois Message Authentication Code (GMAC) is used for authentication and Galois/Counter Mode (GCM) for encryption.

On the seed switch:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

On the non-seed switch:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

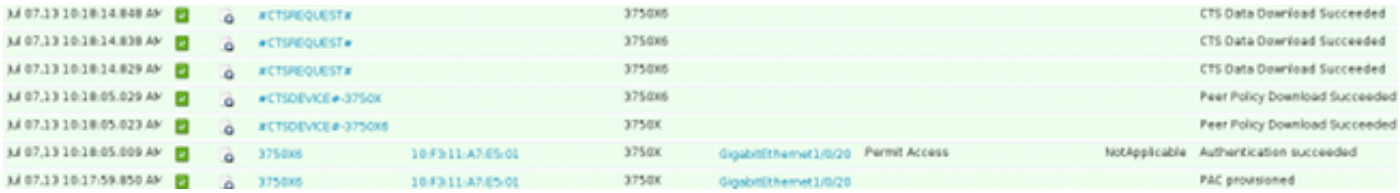
This is supported only on trunk ports (switch-switch MACsec). For switch-host MACsec, which uses MACsec Key Agreement (MKA) protocol instead SAP, refer to Configurig MACsec Encryption.

Immediately after you enable 802.1x on ports, the non-seed switch acts as a supplicant to the seed switch, which is the authenticator.

This process is called NDAC, and its aim is to connect a new device to the CTS domain. Authentication is bidirectional; the new device has credentials that are verified on the authentication server ISE. After PAC provisioning, the device is also sure that it connects to the CTS domain.

> **Note**: PAC is used in order to build a Transport Layer Security (TLS) tunnel for EAP-FAST. The 3750X-6 trusts the PAC credentials that are provided by the server similar to the way a client trusts the certificate provided by the server for the TLS tunnel for EAP-TLS method.

Multiple RADIUS messages are exchanged:



The first session from the 3750X (seed switch) is used for PAC provisioning. EAP-FAST is used without PAC (an anonymous tunnel for MSCHAPv2 authentication is built).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

The MSCHAPv2 username and password configured via the **cts credentials** command is used. Also, a RADIUS Access-Reject is returned at the end, because after PAC has already provisioned, no further authentication is needed.

The second entry in the log refers to 802.1x authentication. EAP-FAST is used with the PAC that was provisioned earlier.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

This time, the tunnel is not anonymous, but protected by PAC. Again, the same credentials for the MSCHAPv2 session are used. Then, it is verified against the authentication and authorization rules on the ISE, and a RADIUS Access-Accept is returned. Then, the authenticator switch applies the returned attributes, and the 802.1x session for that port moves to an authorized state.

What does the process for the first two 802.1x sessions look like from the seed switch?

Here are the most important debugs from the seed. The seed detects that the port is up, and tries to determine which role should be used for 802.1x - the supplicant or the authenticator:

```
debug cts all
```

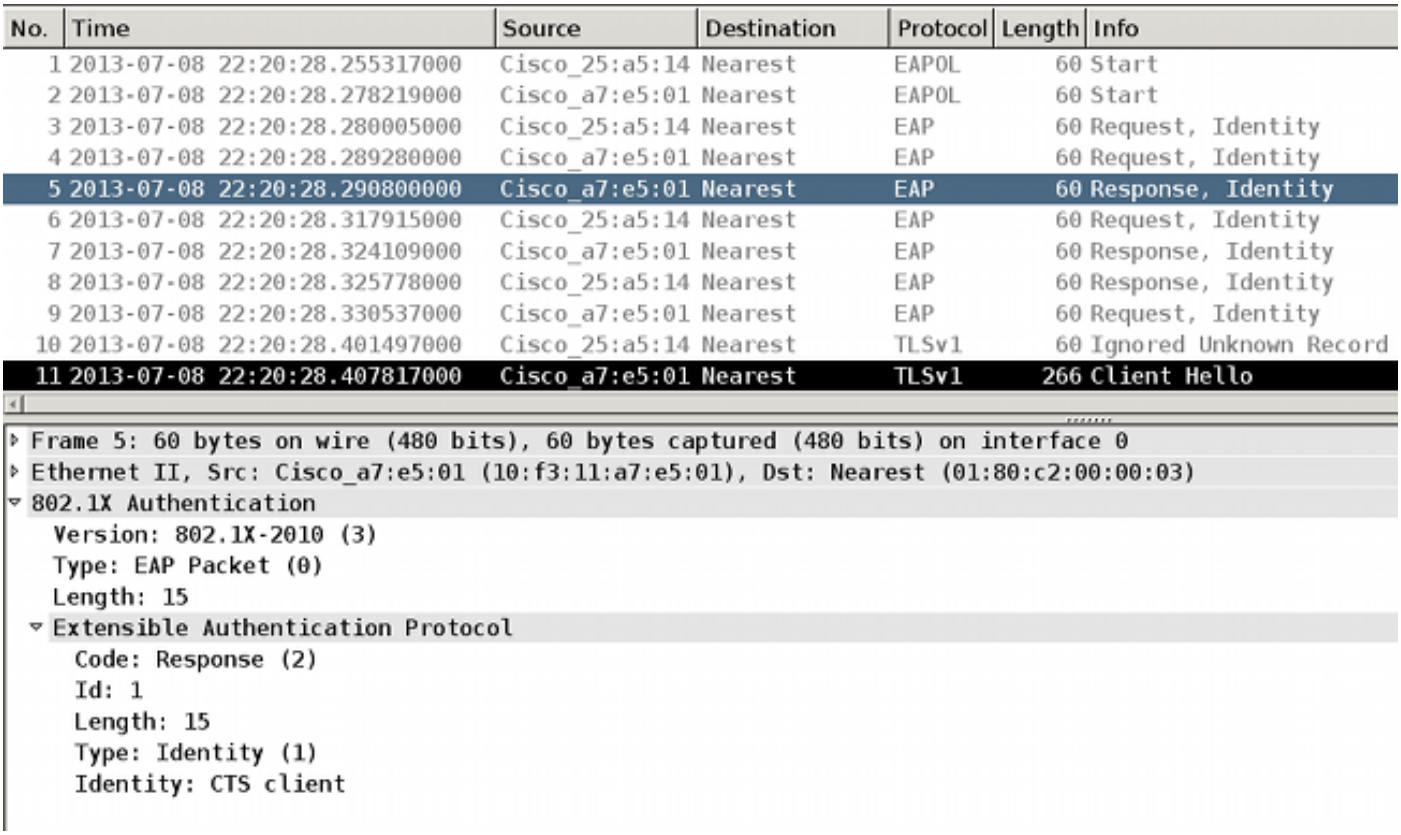
```
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Finally, the authenticator role is used, because the switch has access to the ISE. On the 3750X-6, the supplicant role is chosen.

Details on 802.1x Role Selection

> **Note**: After the supplicant switch obtains the PAC and is 802.1x-authenticated, it downloads the environment data (described later), and learns the IP address of the AAA server. In this example, both switches have a dedicated (backbone) connection for the ISE. Later, the roles can be different; the first switch that receives a response from the AAA server becomes the authenticator, and the second one becomes the supplicant.

This is possible because both switches with the AAA server marked as ALIVE send an Extensible Authentication Protocol (EAP) Request Identity. The one that first receives the EAP Identity Response becomes the authenticator, and drops subsequent Identity Requests.



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

After the 802.1x role is selected (in this scenario, the 3750X-6 is the supplicant, because it has no access to the AAA server yet), the next packets involve the EAP-FAST exchange for PAC provisioning. The username **CTS client** is used for the RADIUS Request Username and as the EAP identity:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

After the anonymus EAP-FAST tunnel is built, a MSCHAPv2 session occurs for the username **3750X6** (**cts credentials**). It is not possible to see that on the switch, because it is a TLS tunnel (encrypted), but detailed logs on the ISE for PAC provisioning proves it. You can see **CTS Client** for the RADIUS Username and as the EAP identity response. However, for the inner method (MSCHAP), the **3750X6** username is used:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

The second EAP-FAST authentication occurs. This time, it uses the PAC that was provisioned earlier. Again, the **CTS client** is used as the RADIUS username and outer identity, but **3750X6** is used for the inner identity (MSCHAP). Authentication succeeds:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

However, this time, the ISE returns several attributes in the RADIUS Accept packet:

Authentication Result

```
User-Name=3750X6
State=ReauthSession:C0A800010000053A33FD79AF
Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
Session-Timeout=86400
Termination-Action=RADIUS-Request
EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
cisco-av-pair=cts:security-group-tag=0000-01
cisco-av-pair=cts:supplicant-cts-capabilities=sap
MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

Here, the authenticator switch changes the port to the authorized state:

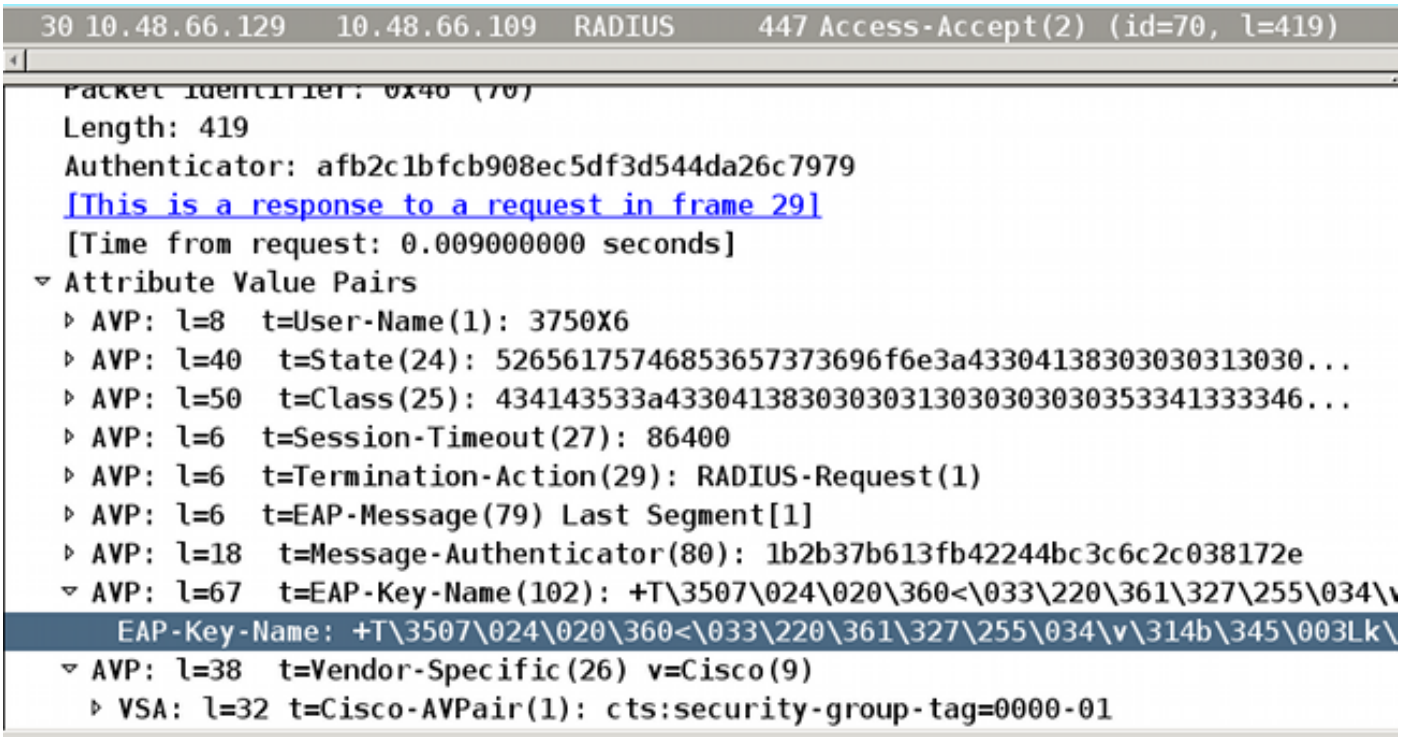
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

How does the authenticator switch learn that the User-Name is **3750X6**? For the RADIUS username and the outer EAP identity, **CTS client** is used, and the inner identity is encrypted and

not visible for the authenticator. The username is learned by the ISE. The last RADIUS packet (Access-Accept) contains **username=3750X6**, while all the others contained **username = Cts client**. This is why the supplicant switch recognizes the real username. This behavior is RFC-compliant. From RFC3579 section 3.0:

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

In the last packet of the 802.1x authentication session, the ISE returns a RADIUS Accept message **cisco-av-pair** with the **EAP-Key-Name**:

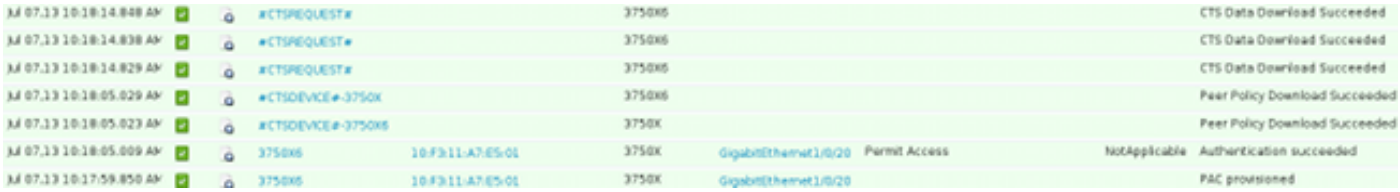


This is used as a keying material for SAP negotiation.

Also, the SGT is passed. This means that the authenticator switch tags traffic from the supplicant with a **default value = 0**. You can configure a specific value on the ISE to return any other value. This applies only for untagged traffic; tagged traffic is not rewritten because, by default, the authenticator switch trusts the traffic from the authenticated supplicant (but this can also be changed on the ISE).

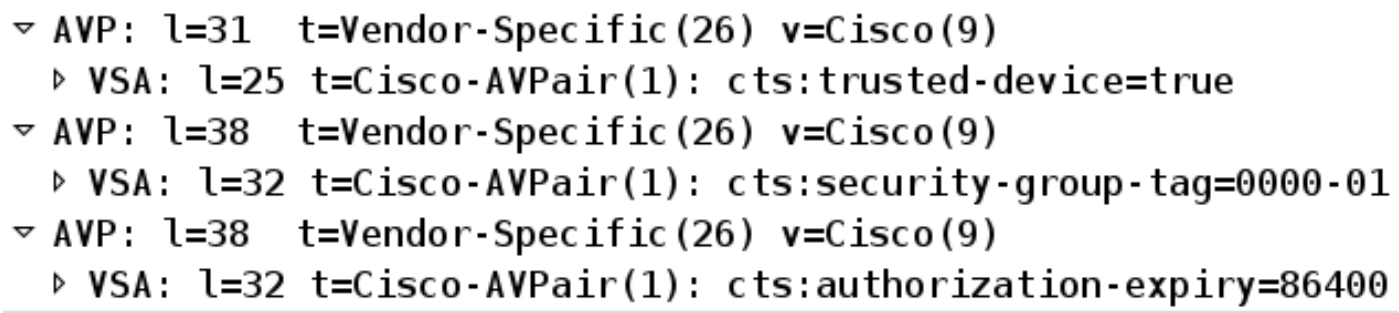
SGA Policy Download

There are additional RADIUS exchanges (without EAP) other than the first two 802.1x EAP-FAST sessions (the first for PAC provisioning, and the second for authentication). Here are the ISE logs again:



The third log (**Peer Policy Download**) indicates a simple RADIUS exchange: RADIUS Request

and RADIUS Accept for the **3760X6** user. This is needed in order to download policies for traffic from the supplicant. The two most important attributes are:



Because of this, the authenticator switch trusts traffic that is SGT-tagged by the supplicant (**cts:trusted-device=true**), and also tags untagged traffic with **tag=0**.

The fourth log indicates the same RADIUS exchange. However, this time, it is for the **3750X5** user (authenticator). This is because both peers must have a policy for each other. It is interesting to note that the supplicant still does not know the IP address of the AAA server. This is why the authenticator switch downloads the policy on behalf of the supplicant. This information passes later to the supplicant (along with the ISE IP address) in SAP negotiation.

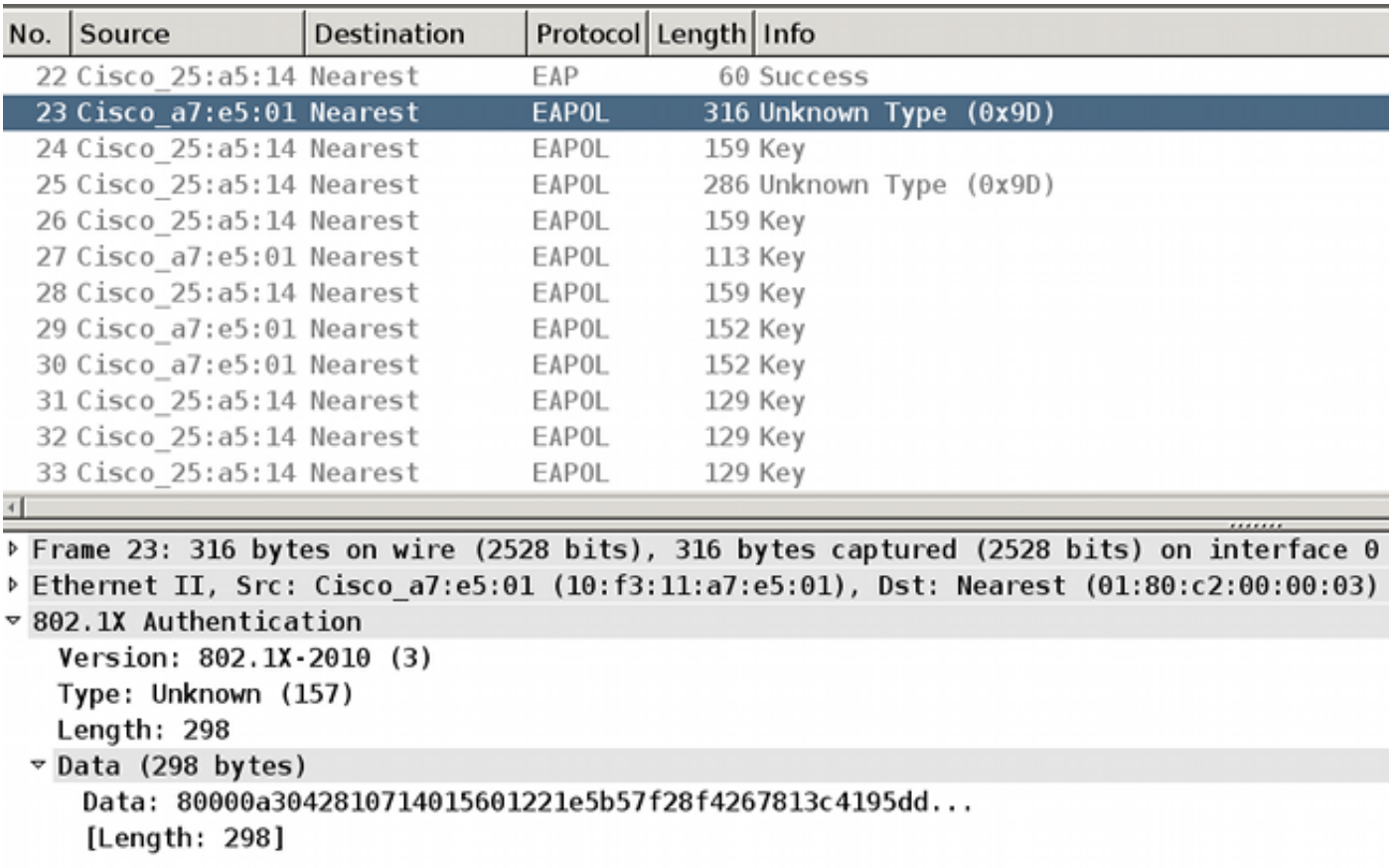
SAP Negotiation

Immediately after the 802.1x authentication session finishes, SAP negotiation occurs. This negotiation is required in order to:

- Negotiate encryption levels (with the **sap mode-list gcm-encrypt** command) and cipher suites
- Derive session keys for data traffic
- Undergo the rekeying process
- Perform additional security checks and make sure that the previous steps are secured

SAP is protocol designed by Cisco Systems based on a draft version of 802.11i/D6.0. For details, request access on the Cisco TrustSec Security Association Protocol - protocol supporting Cisco Trusted Security for the Cisco Nexus 7000 page.

SAP exchange is 802.1AE-compliant. An Extensible Authentication Protocol over LAN (EAPOL) key exchange occurs between the supplicant and the authenticator in order to negotiate a cipher suite, exchange security parameters, and manage keys. Unfortunately, Wireshark does not have decoder for all the required EAP types:



Successful completion of these tasks results in the establishment of a security association (SA).

On the supplicant switch:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       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:              12
```

```
       authc reject:              1556
       authc failure:             0
       authc no response:         0
       authc logoff:              0
       sap success:               12
       sap fail:                  0
       authz success:             12
       authz fail:                0
       port auth fail:            0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
```

On the authenticator:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       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. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
       Peer ID               : unknown
```

```
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

   Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Here, the ports use the mode **gcm-encrypt**, which means that traffic is both authenticated and encrypted, as well as correctly SGT-tagged. Neither device uses any specific network device authorization policy on the ISE, which means that all traffic initiated from the device uses the default tag of **0**. Also both switches trust SGTs received from the peer (because of RADIUS attributes from the peer policy download phase).

Environment and Policy Refresh

After both devices are connected to the CTS cloud, an environment and policy refresh is initiated. The environment refresh is needed in order to obtain the SGTs and names, and a policy refresh is needed in order to download the SGACL defined on the ISE.

At this stage, the supplicant already knows the IP address of the AAA server, so it can do it for itself.

Refer to ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide for details about the environment and policy refresh.

The supplicant switch remembers the RADIUS server IP address, even when there is no RADIUS server configured and when the CTS link goes down (towards the authenticator switch). However, it is possible to force the switch to forget it:

```
bsns-3750-6#show run | i radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius
```

```
radius-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

In order to verify the environment and policy on the supplicant switch, enter these commands:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

bsns-3750-6#show cts role-based permissions
```

Why do no policies display? No policies display, because you must enable **cts enforcement** in

order to apply them:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
        ICMP-20
```

Why does the supplicant have only one policy to **group Unknown** while the authenticator has more?

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Port Authentication for Clients

The MS Windows client is connected and authenticated to the **g1/0/1** port of the 3750-5 switch:

```
bsns-3750-5#show authentication sessions int g1/0/1
       Interface:  GigabitEthernet1/0/1
         MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Policy:  20
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                  SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


Runnable methods list:
      Method   State
      dot1x    Authc Success
      mab      Not run
```

Here, the switch 3750-5 knows that traffic from that host should be tagged with **SGT=3** when sent to the CTS cloud.

Traffic Tagging with the SGT

How do you sniff and verify traffic?

This is difficult because:

- Embedded Packet Capture is supported only for IP traffic (and this is a modified Ethernet frame with SGTs and MACsec payload).
- Switched Port Analyzer (SPAN) port with the **replication** keyword - this might work, but the problem is that any PC with Wireshark connected to the destination port of a monitoring session drops the frames because of the lack of support of 802.1ae, which can happen at the hardware level.
- SPAN port without the **replication** keyword removes the **cts** header before it puts on a destination port.

Policy Enforcement with the SGACL

Policy enforcement in the CTS cloud is always done at the destination port. This is because only the last device knows the destination SGT of the endpoint device that is connected directly to that switch. The packet carries only the source SGT. Both the source and destination SGT are required in order to make a decision.

This is why devices do not need to download all the policies from the ISE. Instead, they only need the part of the policy that is related to the SGT for which the device has directly-connected devices.

Here is the 3750-6, which is the supplicant switch:

```
bsns-3750-6#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
```

There are two policies here. The first is the default for untagged traffic (to/from). The second is from **SGT=2** to the untagged SGT, which is **0**. This policy exists because the device itself uses the SGA policy from the ISE, and belongs to **SGT=0**. Also, **SGT=0** is a default tag. Therefore, you must download all the policies that have the rules for traffic **to/from SGT=0**. If you look at the matrix, you see only one such policy: **from 2 to 0**.

Here is the 3750-5, which is the authenticator switch:

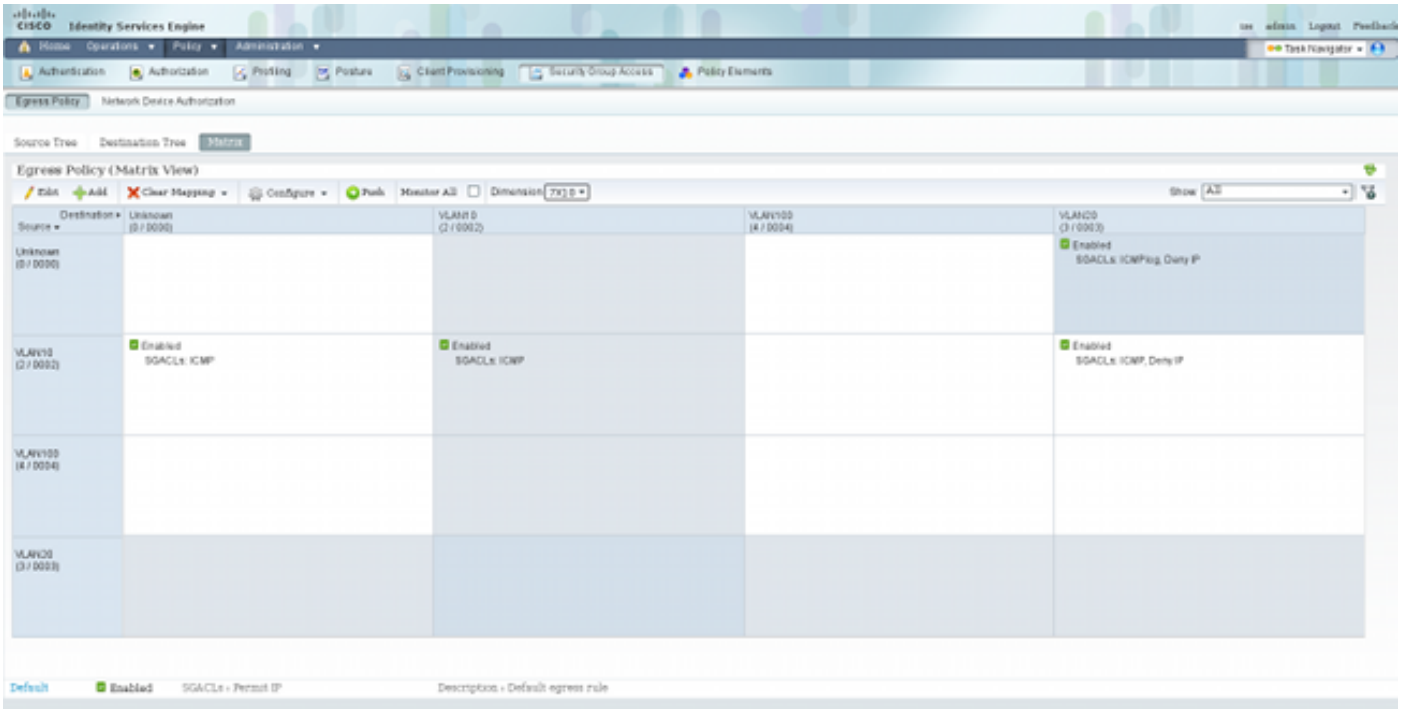
```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

There is one more policy here: **from 2 to 3**. This is because the 802.1x client (MS Windows) is connected to **g1/0/1** and tagged with **SGT=3**. This is why you must download all the policies **to SGT=3**.

Try to ping from 3750X-6 (**SGT=0**) to MS Windows XP (**SGT=3**). The 3750X-5 is the enforcing

device.

Before this, you must configure a policy on the ISE for traffic from **SGT=0 to SGT=3**. This example created a SGACL Internet Control Message Protocol (ICMP) log with only the line, **permit icmp log**, and used it in the matrix for traffic from **SGT=0 to SGT=3**:



Here is a refresh of the policy on the enforcing switch, and a verification of the new policy:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress

bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

In order to verify that the Access Control List (ACL) is downloaded from the ISE, enter this commmand:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
   10 permit icmp log
```

In order to verify that the ACL is applied (hardware support), enter this command:

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
 refcnt = 2
```

```
 flag   = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale  = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Here are the counters before ICMP:

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Here is a ping from **SGT=0** (3750-6 switch) to MS Windows XP (**SGT=3**) and the counters:

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Here are the ACL counters:

```
bsns-3750-5#show ip access-lists ICMPlog-10
Role-based IP access list ICMPlog-10 (downloaded)
    10 permit icmp log (5 matches)
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco TrustSec Configuration Guide for 3750**
- **Cisco TrustSec Configuration Guide for ASA 9.1**
- **Cisco TrustSec Deployment and RoadMap**
- **Technical Support & Documentation - Cisco Systems**