Catalyst 3750X系列交换机上具有802.1x MACsec的TrustSec云配置示例

目录

简介

本文描述在两台Catalyst 3750X系列交换机(3750X)之间使用链路加密配置Cisco TrustSec(CTS)云所需的步骤。

本文解释使用安全关联协议(SAP)的交换机到交换机介质访问控制安全(MACsec)加密过程。此过程使用IEEE 802.1x模式而不是手动模式。

以下是相关步骤的列表：

- 种子和非种子设备的保护访问凭证(PAC)调配
- 网络设备准入控制(NDAC)身份验证和与SAP的MACsec协商，用于密钥管理
- 环境和策略更新
- 客户端的端口身份验证
- 使用安全组标记(SGT)标记流量
- 使用安全组ACL(SGACL)实施策略

先决条件

要求

Cisco 建议您了解以下主题：

- CTS组件的基础知识
- Catalyst交换机的CLI配置基础知识
- 使用身份服务引擎(ISE)配置的体验

使用的组件

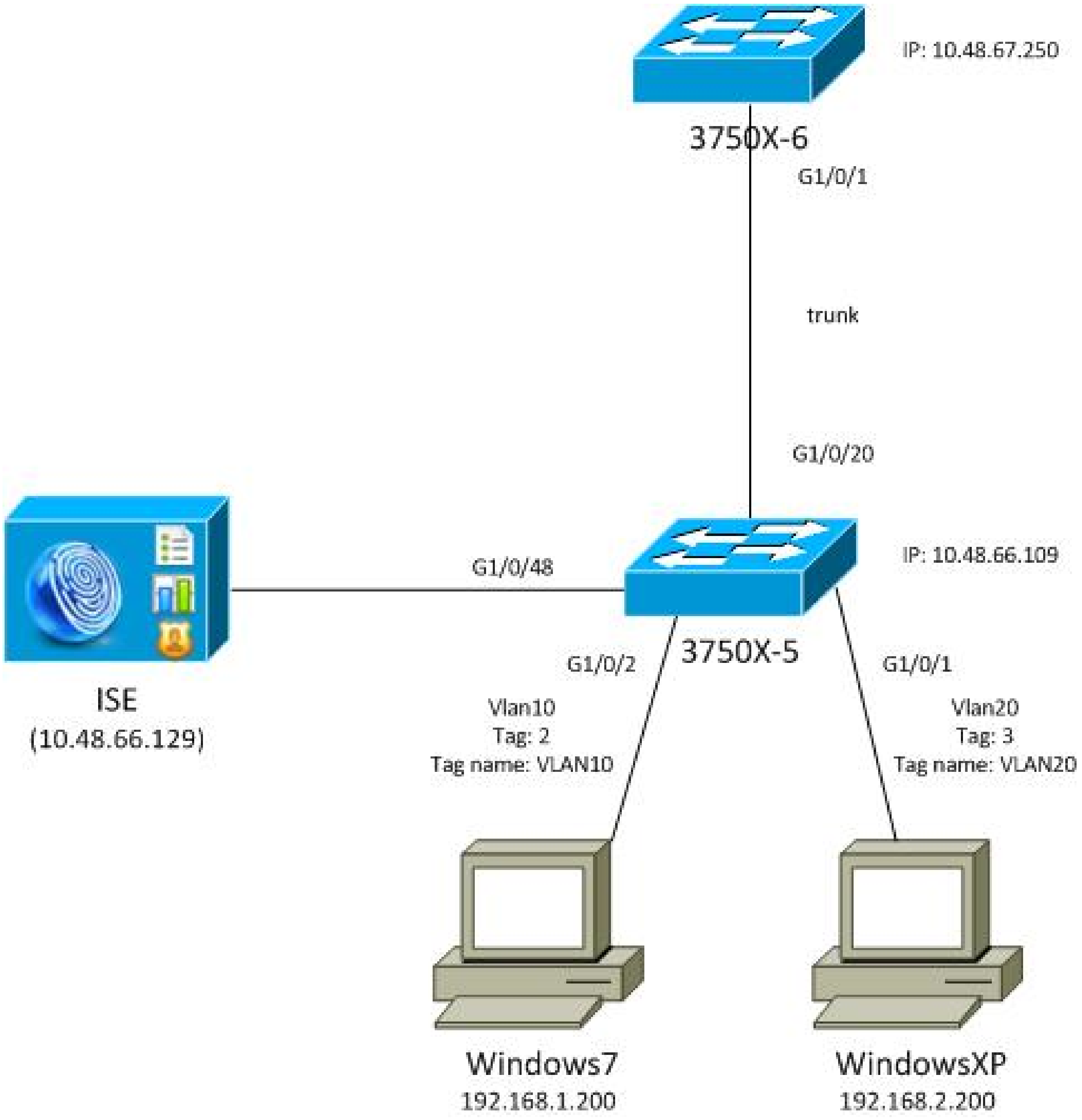
本文档中的信息基于以下软件和硬件版本：

- Microsoft(MS)Windows 7和MS Windows XP
- 3750X软件，版本15.0及更高版本
- ISE软件，版本1.1.4及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



在此网络拓扑图中，3750X-5交换机是知道ISE的IP地址的种子设备，它会自动下载PAC，用于在CTS云中进行后续身份验证。种子设备充当非种子设备的802.1x身份验证器。Cisco Catalyst 3750X-6系列交换机(3750X-6)是非种子设备。它充当种子设备的802.1x请求方。非种子设备通过种子设备向ISE进行身份验证后，将允许其访问CTS云。身份验证成功后，3750X-5交换机上的802.1x端口状态更改为**authenticated**，并协商MACsec加密。然后，交换机之间的流量将使用SGT标记并加密。

此列表汇总了预期流量：

- 种子3750X-5连接到ISE并下载PAC，后者稍后用于环境和策略更新。
- 非种子3750X-6使用请求方角色执行802.1x身份验证，以便从ISE验证/授权和下载PAC。
- 3750X-6执行第二个802.1x可扩展身份验证协议 — 通过安全协议的灵活身份验证(EAP-FAST)会话，以便根据PAC使用受保护的隧道进行身份验证。
- 3750X-5为自己和代表3750X-6下载SGA策略。
- 在3750X-5和3750X-6之间发生SAP会话，协商MACsec密码，并交换策略。
- 交换机之间的流量已标记并加密。

配置种子交换机和非种子交换机

种子设备(3750X-5)配置为使用ISE作为CTS的RADIUS服务器：

```
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
```

启用基于角色的访问控制列表(RBACL)和基于安全组的访问控制列表(SGACL)实施（稍后使用）：

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

非种子设备(3750X-6)仅配置用于身份验证、授权和记帐(AAA)，而不需要RADIUS或CTS授权：

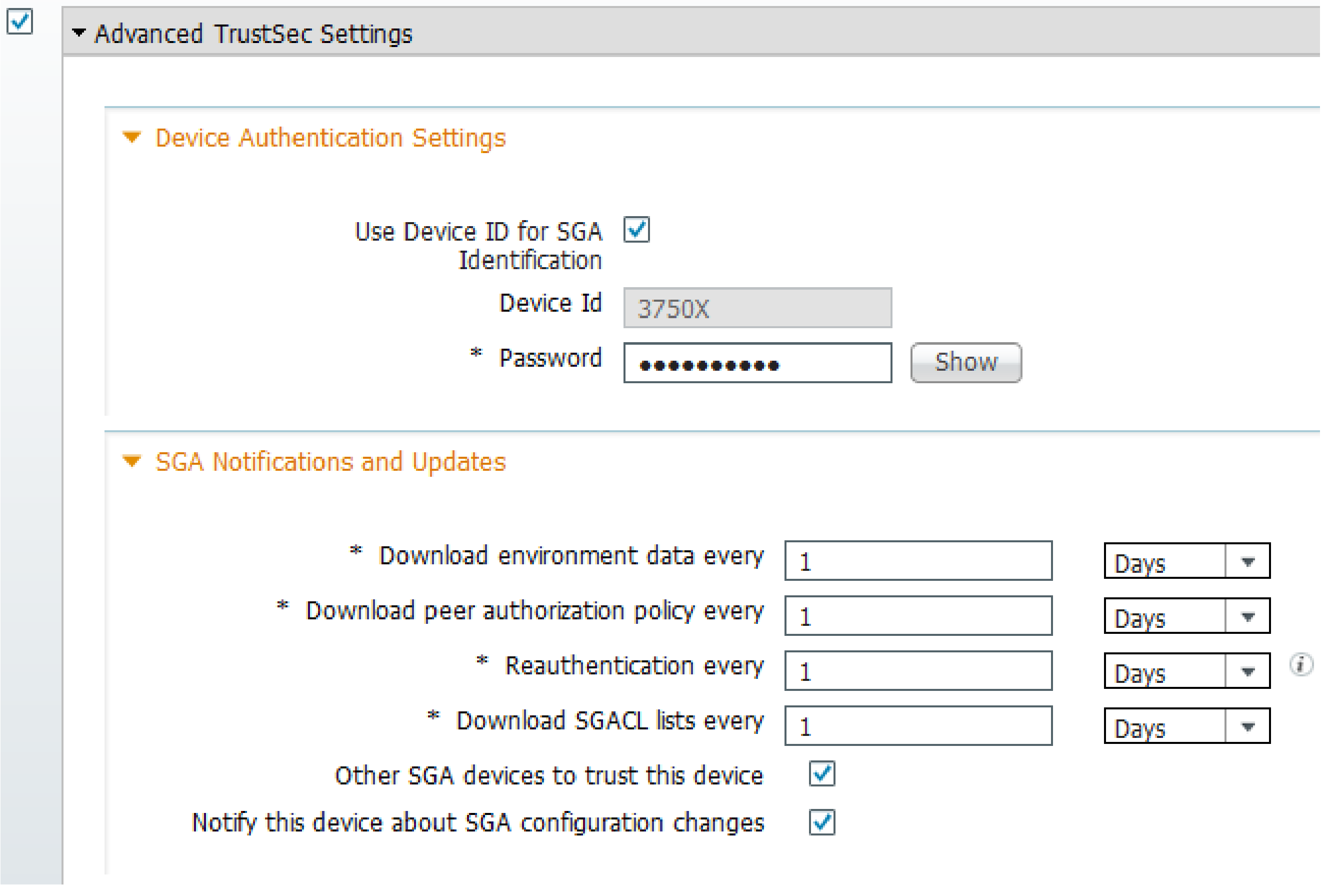
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

在接口上启用802.1x之前，需要配置ISE。

配置ISE

完成以下步骤以配置ISE:

1. 导航到**Administration > Network Resources > Network Devices**，并将两台交换机添加为网络接入设备(NAD)。在**Advanced TrustSec Settings**下，配置一个CTS密码，供以后在交换机CLI上使用。



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for SGA Identification ☑

Device Id: 3750X

* Password: ●●●●●●●●●● Show

SGA Notifications and Updates

* Download environment data every 1 Days

* Download peer authorization policy every 1 Days

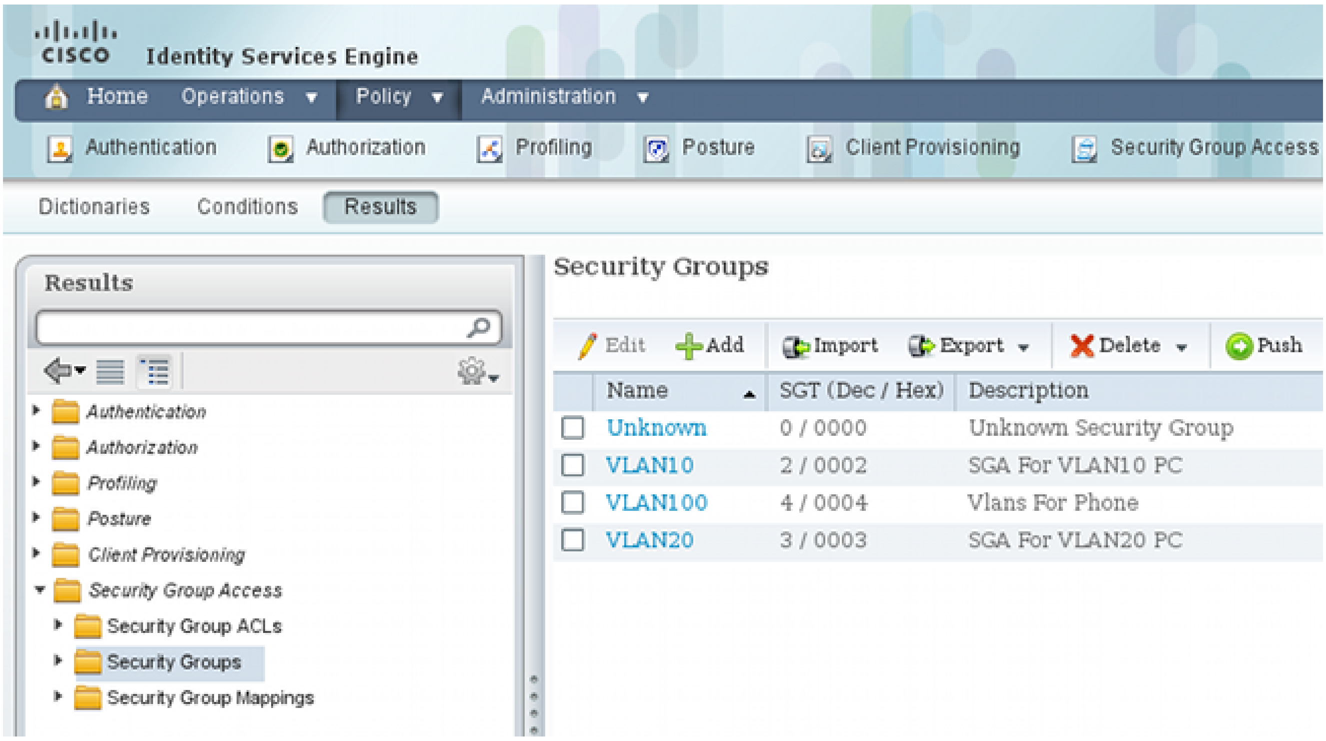
* Reauthentication every 1 Days

* Download SGACL lists every 1 Days

Other SGA devices to trust this device ☑

Notify this device about SGA configuration changes ☑

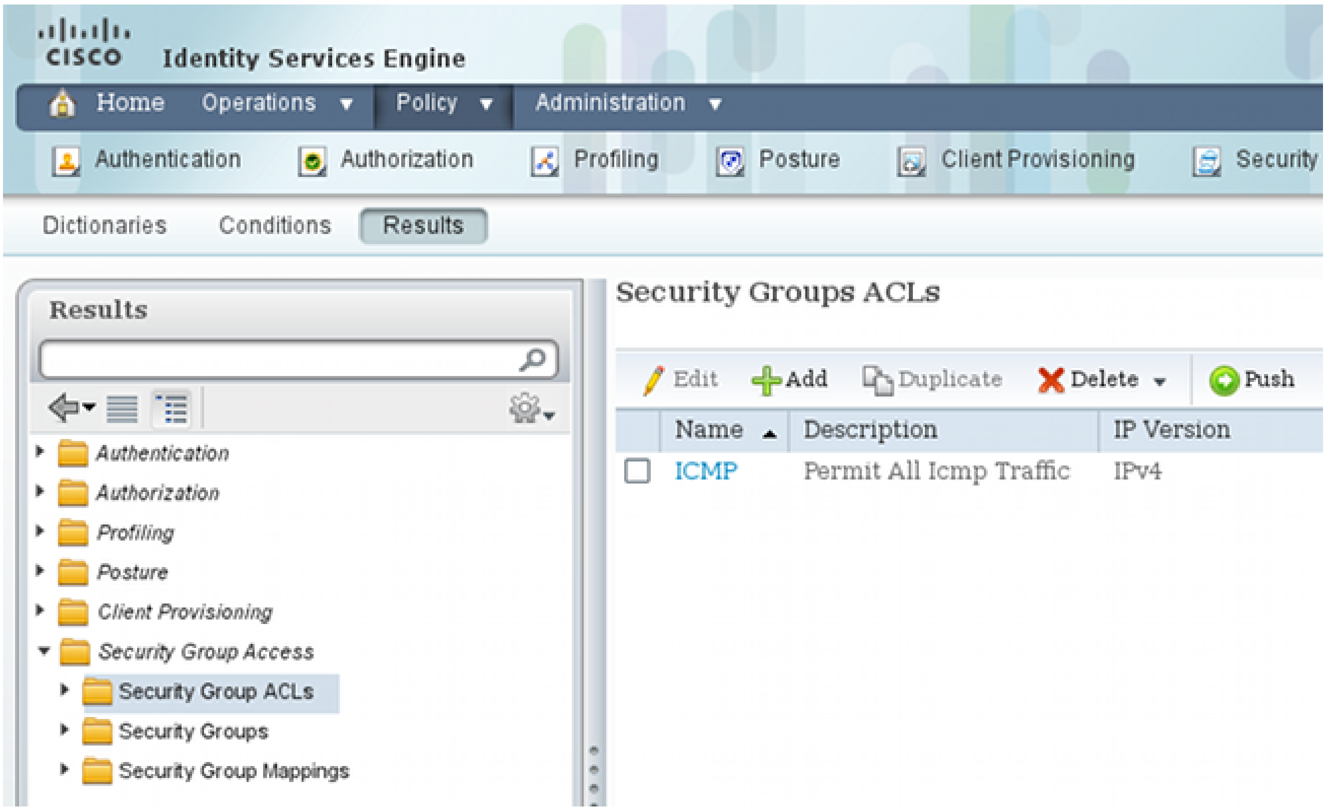
2. 导航到**Policy > Policy Elements > Results > Security Group Access > Security Groups**，然后添加适当的SGT。当交换机请求环境更新时，会下载这些标记。



Security Groups

	Name	SGT (Dec / Hex)	Description
□	Unknown	0 / 0000	Unknown Security Group
□	VLAN10	2 / 0002	SGA For VLAN10 PC
□	VLAN100	4 / 0004	Vlans For Phone
□	VLAN20	3 / 0003	SGA For VLAN20 PC

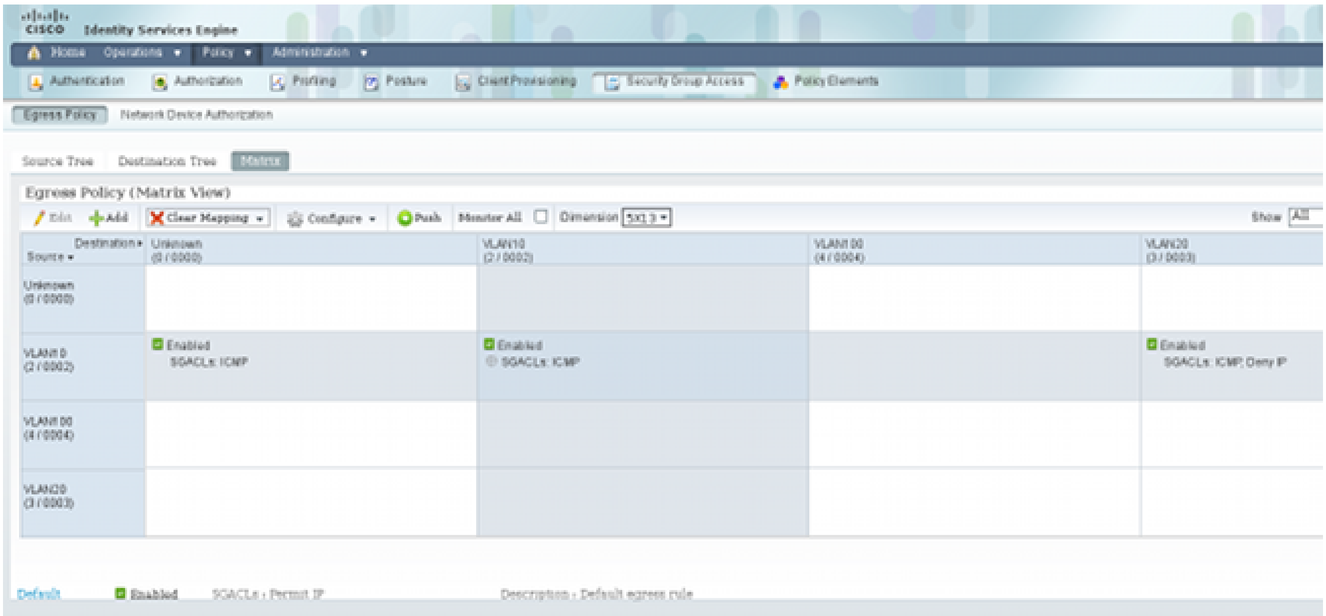
3. 导航到**Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**，然后配置SGACL。



Security Groups ACLs

	Name	Description	IP Version
□	ICMP	Permit All Icmp Traffic	IPv4

4. 导航到**Policy > Security Group Access**，然后使用矩阵定义策略。



Egress Policy (Matrix View)

Destination ▸ Source ▾	Unknown (0 / 0000)	VLAN10 (2 / 0002)	VLAN100 (4 / 0004)	VLAN20 (3 / 0003)
Unknown (0 / 0000)				
VLAN10 (2 / 0002)	Enabled SGACLs: ICMP	Enabled SGACLs: ICMP		Enabled SGACLs: ICMP, Deny IP
VLAN100 (4 / 0004)				
VLAN20 (3 / 0003)				

Default Enabled SGACLs : Permit IP Description : Default egress rule

注意：您必须为MS Windows请求方配置授权策略，使其接收正确的标记。有关此配置的详细信息，请参阅ASA和Catalyst 3750X系列交换机TrustSec配置示例和故障排除指南。

3750X-5的PAC调配

在CTS域中身份验证需要PAC（对于EAP-FAST为phase1），它还用于从ISE获取环境和策略数据。如果没有正确的PAC，则无法从ISE获取该数据。

在3750X-5上提供正确的凭证后，它会下载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: 000200B00003000100040010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

PAC通过EAP-FAST下载，使用Microsoft质询握手身份验证协议(MSCHAPv2),CLI中提供的凭证和ISE上配置的相同凭证。

PAC用于环境和策略刷新。对于这些交换机，请将RADIUS请求与**cisco av-pair cts-pac-opaque**配合使用，该请求源自PAC密钥并可在ISE上解密。

3750X-6和NDAC身份验证的PAC调配

为了使新设备能够连接到CTS域，必须在相应端口上启用802.1x。

SAP协议用于密钥管理和密码套件协商。Galois Message Authentication Code(GMAC)用于身份验证，Galois/Counter Mode(GCM)用于加密。

在种子交换机上：

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

在非种子交换机上：

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

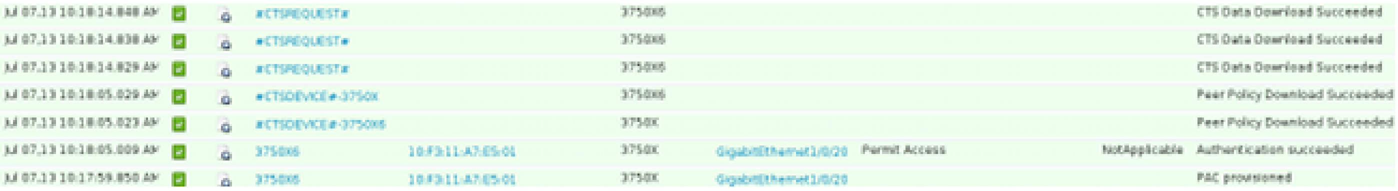
仅在中继端口（交换机 — 交换机MACsec）上支持此功能。对于使用MACsec密钥协议(MKA)协议代替SAP的交换机主机MACsec，请参阅配置MACsec加密。

在端口上启用802.1x后，非种子交换机立即充当种子交换机（即身份验证器）的请求方。

此过程称为NDAC，其目的是将新设备连接到CTS域。身份验证是双向的；新设备具有在身份验证服务器ISE上验证的凭证。在PAC调配后，设备也确信它连接到CTS域。

注意：使用PAC为EAP-FAST构建传输层安全(TLS)隧道。3750X-6信任由服务器提供的PAC凭证，类似于客户端信任由服务器为EAP-TLS方法的TLS隧道提供的证书的方式。

交换多个RADIUS消息：



Jul 07,13 10:18:14.848 AM	✓	🔍	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
Jul 07,13 10:18:14.838 AM	✓	🔍	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
Jul 07,13 10:18:14.829 AM	✓	🔍	#CTSREQUEST#		3750X6				CTS Data Download Succeeded
Jul 07,13 10:18:05.029 AM	✓	🔍	#CTSDEVICE#-3750X		3750X6				Peer Policy Download Succeeded
Jul 07,13 10:18:05.023 AM	✓	🔍	#CTSDEVICE#-3750X6		3750X				Peer Policy Download Succeeded
Jul 07,13 10:18:05.009 AM	✓	🔍	3750X6	10:F3:11:A7:E5:01	3750X	GigabitEthernet1/0/20	Permit Access	NotApplicable	Authentication succeeded
Jul 07,13 10:17:59.850 AM	✓	🔍	3750X6	10:F3:11:A7:E5:01	3750X	GigabitEthernet1/0/20			PAC provisioned

3750X（种子交换机）的第一个会话用于PAC调配。EAP-FAST不使用PAC（为MSCHAPv2身份验证构建匿名隧道）。

```
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
```

使用通过**cts credentials**命令配置的MSCHAPv2用户名和密码。此外，RADIUS Access-Reject会在结束时返回，因为在PAC已调配后，不需要进一步身份验证。

日志中的第二个条目是指802.1x身份验证。EAP-FAST用于之前调配的PAC。

```
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
```

这次，隧道不是匿名的，而是受PAC保护。再次使用MSCHAPv2会话的相同凭证。然后，根据ISE上的身份验证和授权规则进行验证，并返回RADIUS Access-Accept。然后，身份验证器交换机应用返回的属性，该端口的802.1x会话将变为授权状态。

种子交换机上前两个802.1x会话的进程是什么样的？

以下是种子中最重要的调试。种子检测到端口已启动，并尝试确定哪个角色应该用于802.1x — 请求方或身份验证器：

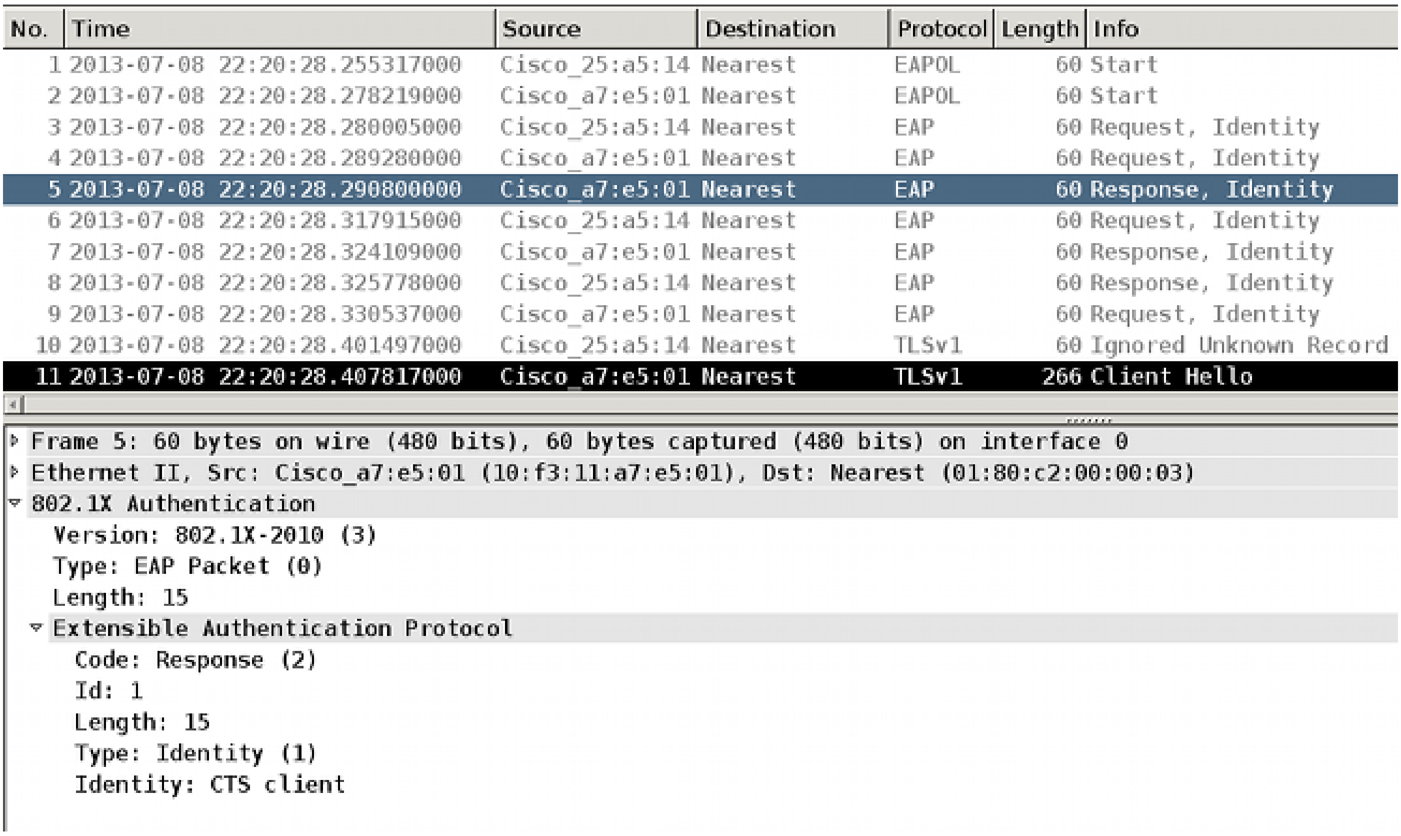
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

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
```

最后，使用身份验证器角色，因为交换机有权访问ISE。在3750X-6上，选择请求方角色。

有关802.1x角色选择的详细信息

> **注意**：请求方交换机获取PAC并经过802.1x身份验证后，它将下载环境数据（稍后说明），并获取AAA服务器的IP地址。在本示例中，两台交换机都有一个专用的（主干）连接，用于ISE。之后，角色可以不同；从AAA服务器收到响应的第一台交换机成为身份验证器，而第二台交换机成为请求方。

这是有可能的，因为AAA服务器标记为ALIVE的两台交换机都发送可扩展身份验证协议(EAP)请求身份。首先收到EAP身份响应的身份验证器成为身份验证器，并丢弃后续身份请求。

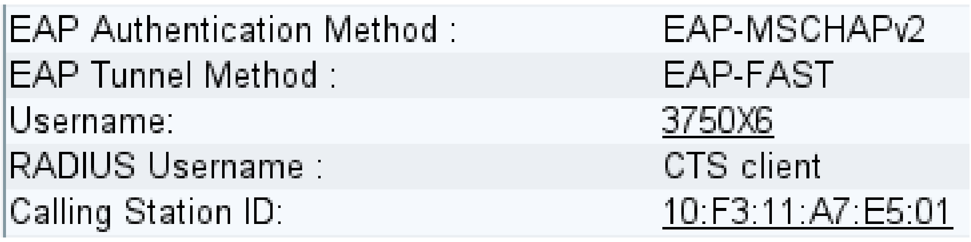


```
No. Time                           Source            Destination Protocol Length Info
  1 2013-07-08 22:20:28.255317000  Cisco_25:a5:14    Nearest     EAPOL        60 Start
  2 2013-07-08 22:20:28.278219000  Cisco_a7:e5:01    Nearest     EAPOL        60 Start
  3 2013-07-08 22:20:28.280005000  Cisco_25:a5:14    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

▸ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:e5:01 (10:f3:11:a7:e5:01), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 15
  ▾ Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 15
      Type: Identity (1)
      Identity: CTS client
```

选择802.1x角色后（在本场景中，3750X-6是请求方，因为它尚未访问AAA服务器），下一个数据包涉及用于PAC调配的EAP-FAST交换。用户名**CTS client**用于RADIUS请求用户名并作为EAP身份：

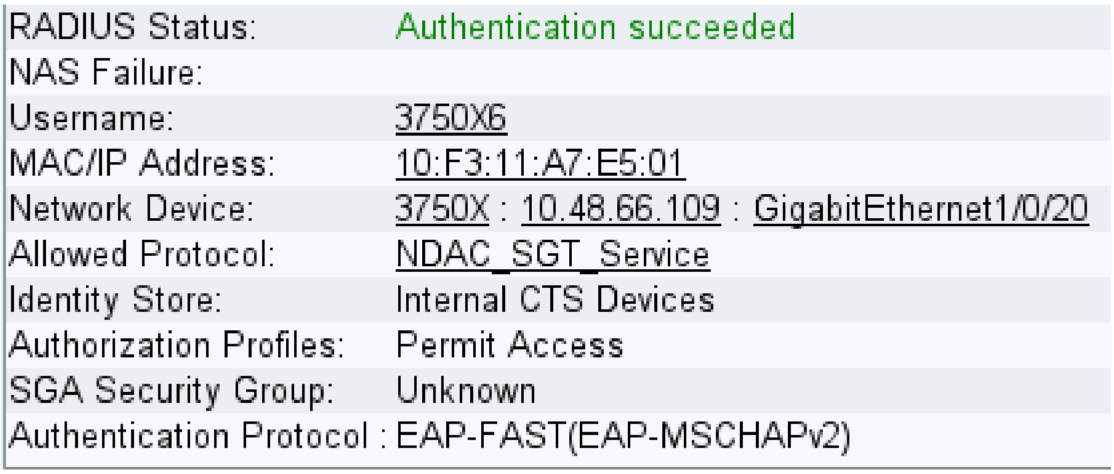
```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

在构建匿名EAP-FAST隧道后，对用户名3750X6(cts凭**证)进行**MSCHAPv**2会**话。在交换机上看不到这一点，因为它是TLS隧道（加密），但PAC调配的ISE上的详细日志可以证明这一点。您可以看到**CTS Client**作为RADIUS用户名和EAP身份响应。但是，对于内部方法(MSCHAP)，使用**3750X6**用户名：



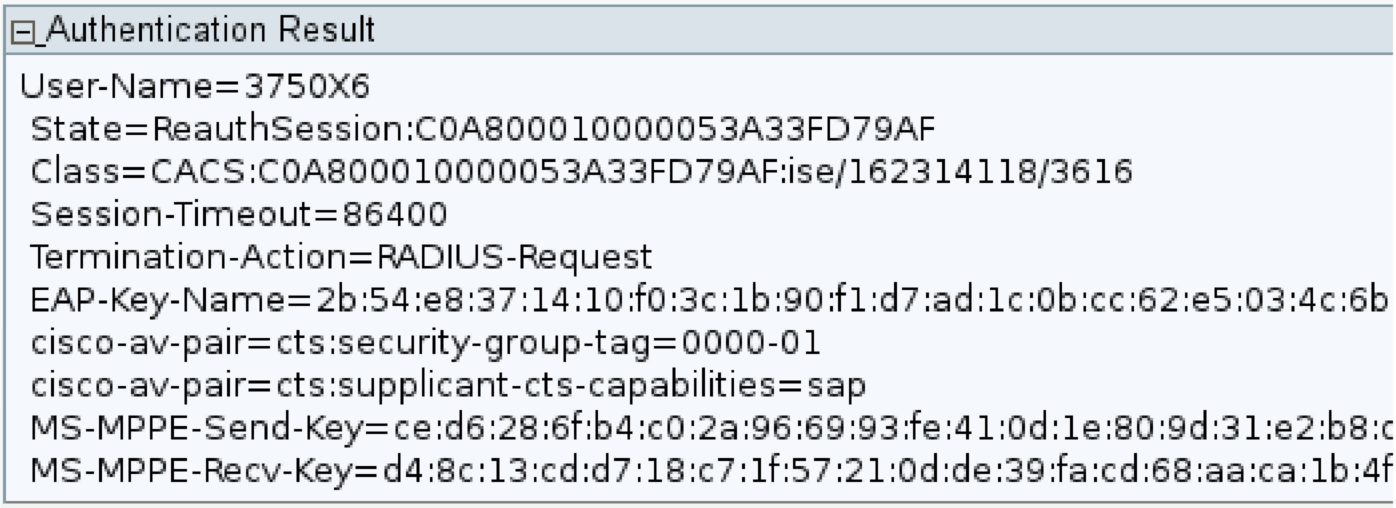
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

进行第二个EAP-FAST身份验证。这次，它使用之前调配的PAC。同样，**CTS client**用作RADIUS用户名和外部身份，而**3750X6**用于内部身份(MSCHAP)。身份验证成功：



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)

但是，这次，ISE返回RADIUS Accept数据包中的多个属性：



⊟ 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
```

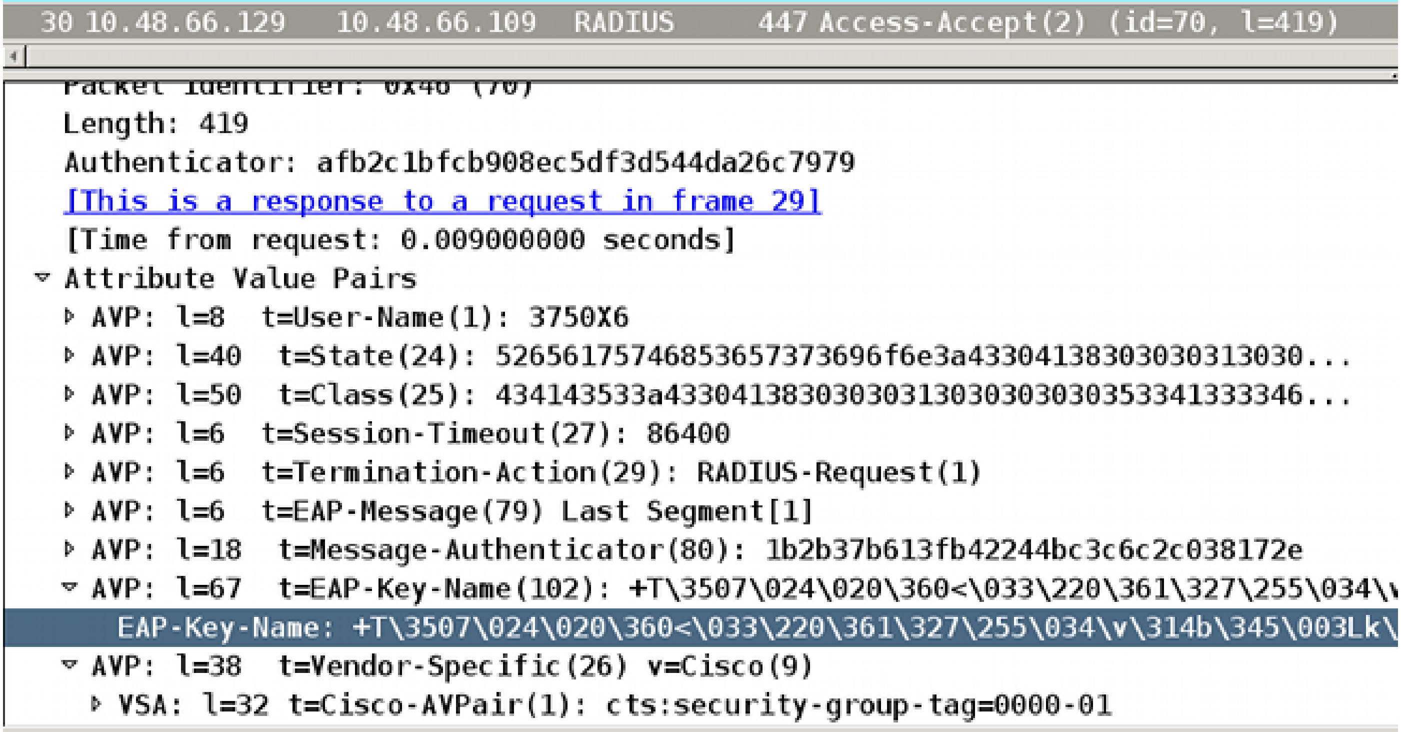
在这里，身份验证器交换机将端口更改为授权状态：

```
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
```

身份验证器交换机如何获知用户名是**3750X6**?对于RADIUS用户名和外部EAP身份，使用**CTS client**，内部身份被加密且对身份验证器不可见。用户名由ISE获取。最后一个RADIUS数据包(Access-Accept)包含**username=3750X6**，而其他所有数据包都包含**username = Cts client**。这就是请求方交换机识别实际用户名的原因。此行为符合RFC。从RFC3579第3.0节：

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

在802.1x身份验证会话的最后一个数据包中，ISE返回带有**EAP-Key-Name**的RADIUS接受消息**cisco-av-pair**:



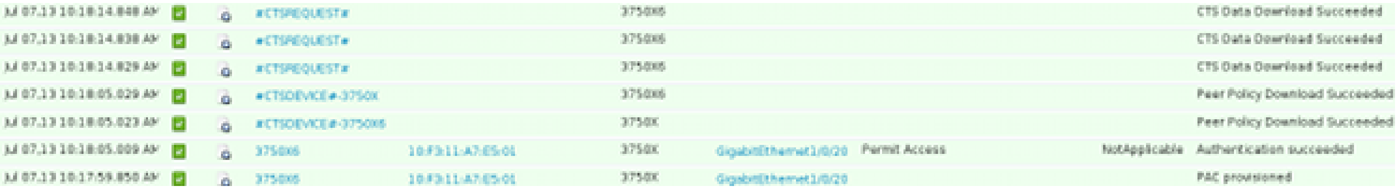
```
 30 10.48.66.129    10.48.66.109   RADIUS      447 Access-Accept(2)  (id=70, l=419)
    Packet identifier: 0x46 (70)
    Length: 419
    Authenticator: afb2c1bfcb908ec5df3d544da26c7979
    [This is a response to a request in frame 29]
    [Time from request: 0.009000000 seconds]
  ▽ Attribute Value Pairs
    ▷ AVP: l=8   t=User-Name(1): 3750X6
    ▷ AVP: l=40   t=State(24): 5265617574685365737369 6f6e3a43304138303030313030...
    ▷ AVP: l=50   t=Class(25): 434143533a43304138303030313030303030353341333346...
    ▷ AVP: l=6   t=Session-Timeout(27): 86400
    ▷ AVP: l=6   t=Termination-Action(29): RADIUS-Request(1)
    ▷ AVP: l=6   t=EAP-Message(79) Last Segment[1]
    ▷ AVP: l=18   t=Message-Authenticator(80): 1b2b37b613fb42244bc3c6c2c038172e
    ▽ AVP: l=67   t=EAP-Key-Name(102): +T\3507\024\020\360<\033\220\361\327\255\034\v
        EAP-Key-Name: +T\3507\024\020\360<\033\220\361\327\255\034\v\314b\345\003Lk\
    ▽ AVP: l=38   t=Vendor-Specific(26) v=Cisco(9)
      ▷ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
```

它用作SAP协商的密钥材料。

此外，SGT会通过。这意味着身份验证器交换机使用默认值= 0标记**来自请求方的流量**。您可以在ISE上配置特定值以返回任何其他值。这仅适用于无标记流量；标记流量不会重写，因为默认情况下，身份验证器交换机信任来自经过身份验证的请求方的流量（但这也可以在ISE上更改）。

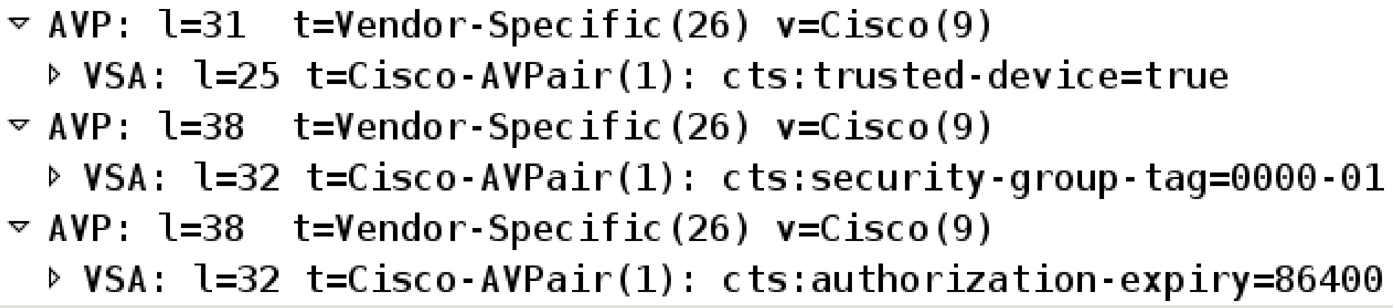
SGA策略下载

除了前两个802.1x EAP-FAST会话（第一个用于PAC调配，第二个用于身份验证）之外，还有其他RADIUS交换（无EAP）。以下是ISE日志：



```
Jul 07,13 10:18:14.848 AM  ✓  #CTSREQUEST#                           3750X6                                          CTS Data Download Succeeded
Jul 07,13 10:18:14.838 AM  ✓  #CTSREQUEST#                           3750X6                                          CTS Data Download Succeeded
Jul 07,13 10:18:14.829 AM  ✓  #CTSREQUEST#                           3750X6                                          CTS Data Download Succeeded
Jul 07,13 10:18:05.029 AM  ✓  #CTSDEVICE#-3750X                      3750X6                                          Peer Policy Download Succeeded
Jul 07,13 10:18:05.023 AM  ✓  #CTSDEVICE#-3750X6                     3750X                                           Peer Policy Download Succeeded
Jul 07,13 10:18:05.009 AM  ✓  3750X6   10:F3:11:A7:E5:01  3750X  GigabitEthernet1/0/20  Permit Access  NotApplicable  Authentication succeeded
Jul 07,13 10:17:59.850 AM  ✓  3750X6   10:F3:11:A7:E5:01  3750X  GigabitEthernet1/0/20                               PAC provisioned
```

第三个日志(**对等策略下载**)表示简单的RADIUS交换：3760X6用户的RADIUS请**求和RADIUS**接受。为从请求方下载流量的策略，需要此步骤。最重要的两个属性是：



```
▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▽ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▷ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

因此，身份验证器交换机信任由请求方进行SGT标记的流量(**cts:trusted-device=true**)，并使用**tag=0标记未标记流量**。

第四个日志指示相同的RADIUS交换。但是，这次适用于**3750X5**用户（身份验证器）。这是因为两个对等体必须拥有彼此的策略。值得注意的是，请求方仍然不知道AAA服务器的IP地址。这就是身份验证器交换机代表请求方下载策略的原因。此信息随后在SAP协商中传送给请求方（以及ISE IP地址）。

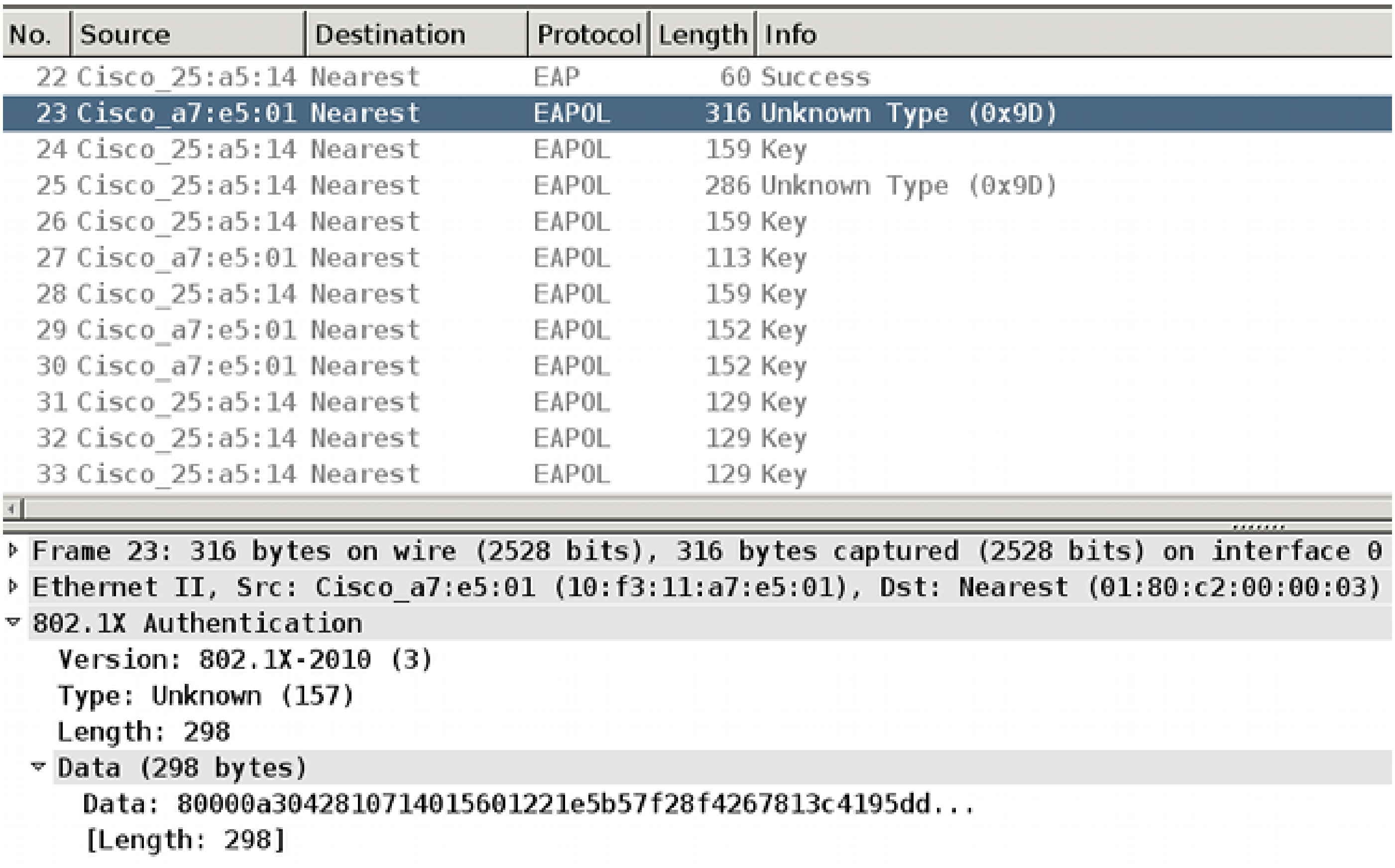
SAP协商

802.1x身份验证会话完成后，将立即进行SAP协商。此协商是必需的，以便：

- 协商加密级别(使用**sap mode-list gcm-encrypt**命令)和密码套件
- 派生数据流量的会话密钥
- 执行重新生成密钥的过程
- 执行其他安全检查并确保前面步骤的安全

SAP是由Cisco Systems基于802.11i/D6.0的草案版本设计的协议。有关详细信息，请在Cisco Nexus 7000页面请求访问Cisco TrustSec安全关联协议 — 支持Cisco Trusted Security的协议。

SAP Exchange符合802.1AE标准。LAN上的可扩展身份验证协议(EAPOL)密钥交换发生在请求方和身份验证方之间，以便协商密码套件、交换安全参数和管理密钥。遗憾的是，Wireshark没有所有必需的EAP类型的解码器：



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

```
▸ Frame 23: 316 bytes on wire (2528 bits), 316 bytes captured (2528 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:e5:01 (10:f3:11:a7:e5:01), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: Unknown (157)
    Length: 298
  ▾ Data (298 bytes)
      Data: 80000a304281071401560122 1e5b57f28f4267813c4195dd...
      [Length: 298]
```

成功完成这些任务后，将建立安全关联(SA)。

在Supplicant客户端交换机上：

```
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
```

在身份验证器上：

```
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
```

此处，端口使用**gcm-encrypt**模式，这意味着流量经过身份验证和加密，并且已正确标记SGT。两台设备都不会在ISE上使用任何特定网络设备授权策略，这意味着从设备发起的所有流量使用默认标记0。此外，两台交换机都信任从对等体收到的SGT（因为对等体策略下载阶段的RADIUS属性）。

环境和策略更新

当两台设备都连接到CTS云后，将启动环境和策略更新。要获取SGT和名称，需要进行环境刷新；要下载ISE上定义的SGACL，则需要策略刷新。

在此阶段，请求方已知道AAA服务器的IP地址，因此可以自行执行此操作。

有关环境和策略更新的详细信息，请参阅ASA和Catalyst 3750X系列交换机TrustSec配置示例和故障排除指南。

请求方交换机记住RADIUS服务器IP地址，即使没有配置RADIUS服务器以及CTS链路断开时（指向身份验证器交换机）。但是，可以强制交换机忘记它：

```
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
```

要验证请求方交换机上的环境和策略，请输入以下命令：

```
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
```

为何不显示策略？不显示策略，因为必须启用cts enforcement才能应用策略：

```
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
```

为什么请求方只有一个策略来组Unknown，而身份验证器有更多？

```
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
```

客户端的端口身份验证

MS Windows客户端已连接到3750-5交换机的**g1/0/1**端口并对其进行身份验证：

```
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
```

此处，交换机3750-5知道来自该主机的流量在发送到CTS云时应标记为**SGT=3**。

使用SGT标记流量

如何嗅探和验证流量？

这是困难的，因为：

- 只有IP流量支持嵌入式数据包捕获（这是带SGT和MACsec负载的修改后的以太网帧）。
- 带有**replication**关键字的交换端口分析器(SPAN)端口 — 这可以正常工作，但问题在于任何Wireshark连接到监控会话的目标端口的PC都会丢弃帧，因为不支持802.1ae（这可能发生在硬

件级别）。
- 不带**replication**关键字的SPAN端口在将**cts**报头置于目标端口之前将其删除。

使用SGACL实施策略

CTS云中的策略实施始终在目标端口完成。这是因为只有最后一个设备知道直接连接到该交换机的终端设备的目的SGT。数据包仅传输源SGT。做出决策需要源和目标SGT。

这就是为什么设备不需要从ISE下载所有策略。相反，他们只需要策略中与设备直接连接设备的SGT相关的部分。

以下是请求方交换机3750-6:

```
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
```

这里有两个策略。第一个是无标记流量（至/自）的默认值。第二个是从**SGT=2**到无标记的SGT，即**0**。存在此策略是因为设备本身使用来自ISE的SGA策略，并且属**于SGT=0**。此外，**SGT=0**是默认标记。因此，您必须下载所有具有流量传入/传出**SGT=0规则的策略**。如果查看矩阵，您只能看到一个此类策略：**从2到0**。

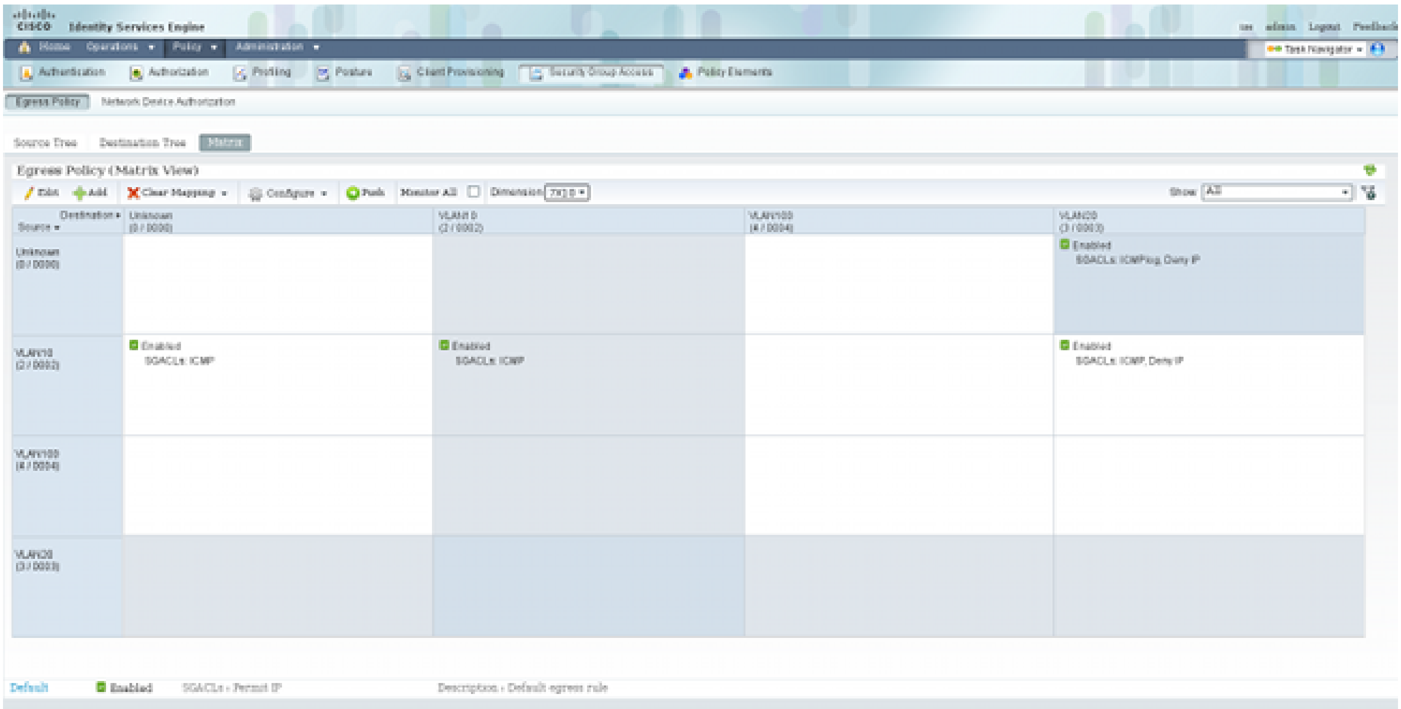
以下是身份验证器交换机3750-5:

```
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
```

此处还有一个策略：**从2到3**。这是因为802.1x客户端(MS Windows)连接到**g1/0/1，并**标记为**SGT=3**。这就是为什么您必须将所有策略**下载到SGT=3**。

尝试从3750X-6(**SGT=0)**ping MS Windows XP(**SGT=3**)。3750X-5是实施设备。

在此之前，您必须在ISE上为从**SGT=0到SGT=3的流量配置策略**。此示例创建了一个仅包含**permit icmp log**行的SGACL互联网控制消息协议(ICMP)日志，并在表中将其用于从**SGT=0到SGT=3的流量**:



Egress Policy (Matrix View)

Destination ▸ Source ▾	Unknown (0 / 0000)	VLAN10 (2 / 0002)	VLAN100 (4 / 0004)	VLAN20 (3 / 0003)
Unknown (0 / 0000)				🟩 Enabled SGACLs: ICMPlog, Deny IP
VLAN10 (2 / 0002)	🟩 Enabled SGACLs: ICMP	🟩 Enabled SGACLs: ICMP		🟩 Enabled SGACLs: ICMP, Deny IP
VLAN100 (4 / 0004)				
VLAN20 (3 / 0003)				

Default 🟩 Enabled SGACLs : Permit IP Description : Default egress rule

以下是实施交换机上的策略更新以及新策略的验证：

```
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
```

要验证访问控制列表(ACL)是否从ISE下载，请输入以下命令：

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

要验证是否已应用ACL（硬件支持），请输入以下命令：

```
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
```

以下是ICMP之前的计数器：

```
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
```

以下是从**SGT=0(**3750-6交换机)到MS Windows XP(**SGT=3)和计**数器的ping:

```
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
```

下面是ACL计数器：

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

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 适用于3750的Cisco TrustSec配置指南
- 适用于ASA 9.1的思科TrustSec配置指南
- Cisco TrustSec部署和路线图
- 技术支持和文档 - Cisco Systems

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。