使用Cisco AnyConnect和ISE的MACsec交換機 — 主機加密配置示例

目錄

簡介

本檔案將提供802.1x請求方（Cisco AnyConnect行動安全）和驗證器（交換器）之間的媒體存取控制安全(MACsec)加密組態範例。 思科身份服務引擎(ISE)用作身份驗證和策略伺服器。

MACsec在802.1AE中實現了標準化，並在Cisco 3750X、3560X和4500 SUP7E交換機上受支援。802.1AE定義使用帶外金鑰的有線網路上的鏈路加密。這些加密金鑰與MACsec金鑰協定(MKA)協定協商，該協定在802.1x身份驗證成功後使用。MKA在IEEE 802.1X-2010中被標準化。

封包只會在PC和交換器之間的連結上加密（點對點加密）。 交換器接收的封包會進行解密，並透過未加密的上行鏈路傳送。為了加密交換器之間的傳輸，建議使用交換器 — 交換器加密。對於該加密，安全關聯協定(SAP)用於協商和重新生成金鑰。SAP是由思科開發的一種預標準金鑰協定協定。

必要條件

需求

思科建議您瞭解以下主題：

- 802.1x配置基礎知識
- Catalyst交換機CLI配置基礎知識

- ISE配置體驗

採用元件

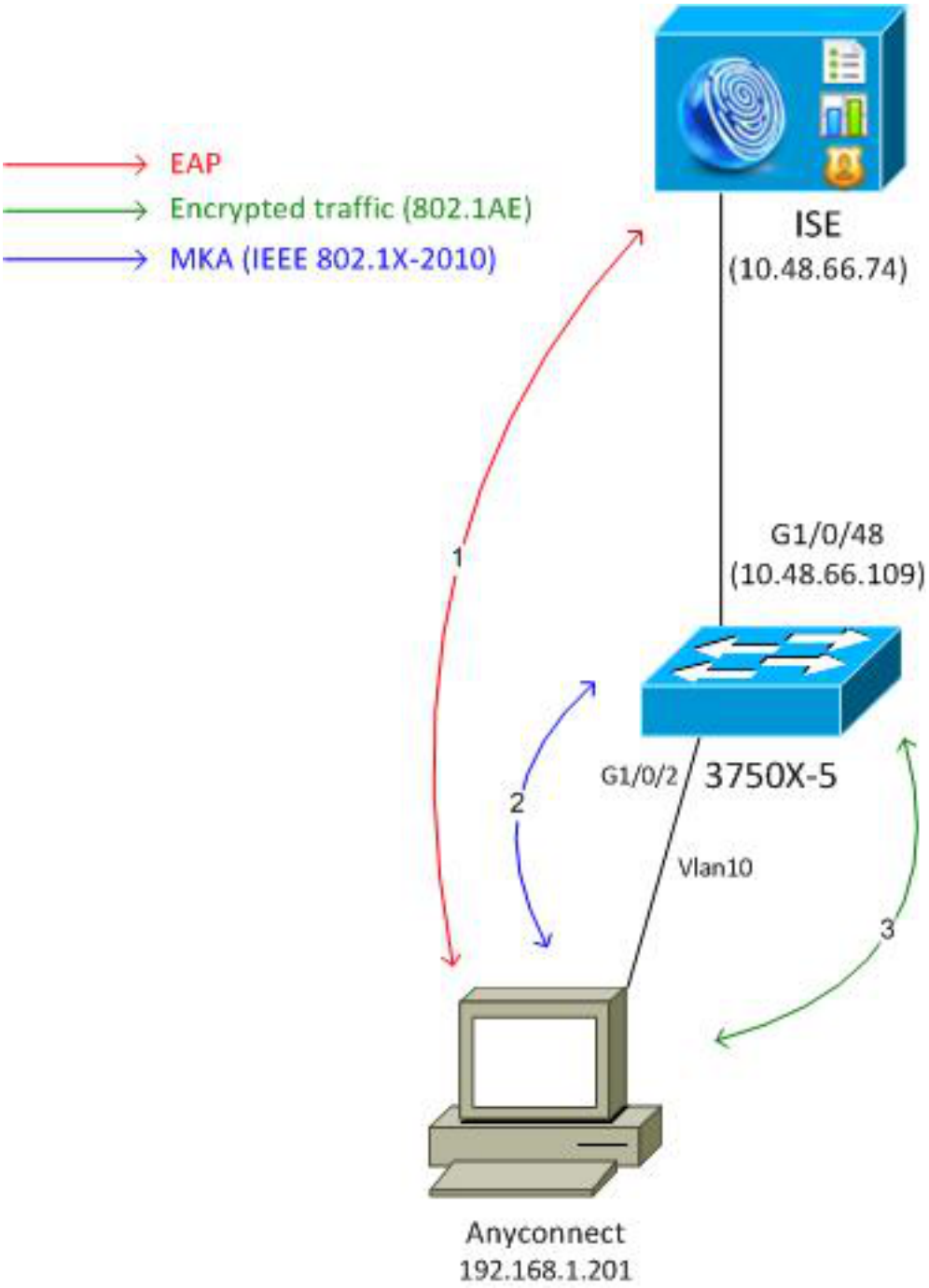
本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7和Microsoft Windows XP作業系統
- Cisco 3750X軟體15.0版及更新版本
- Cisco ISE軟體1.1.4版及更高版本
- Cisco AnyConnect Mobile Security with Network Access Manager(NAM)，版本3.1及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表和流量傳輸



步驟1.請求方(AnyConnect NAM)啟動802.1x會話。交換機是身份驗證器，ISE是身份驗證伺服器。LAN上的可擴充驗證通訊協定(EAPOL)通訊協定是請求者和交換器之間進行EAP的傳輸。RADIUS用作交換機和ISE之間EAP的傳輸協定。無法使用MAC身份驗證繞行(MAB)，因為EAPOL金鑰需要從ISE返回並用於MACsec金鑰協定(MKA)會話。

步驟2. 802.1x作業階段完成後，交換器會啟動MKA作業階段，並將EAPOL作為傳輸通訊協定。如果請求方配置正確，則對稱128位AES-GCM（伽羅瓦/計數器模式）加密的金鑰匹配。

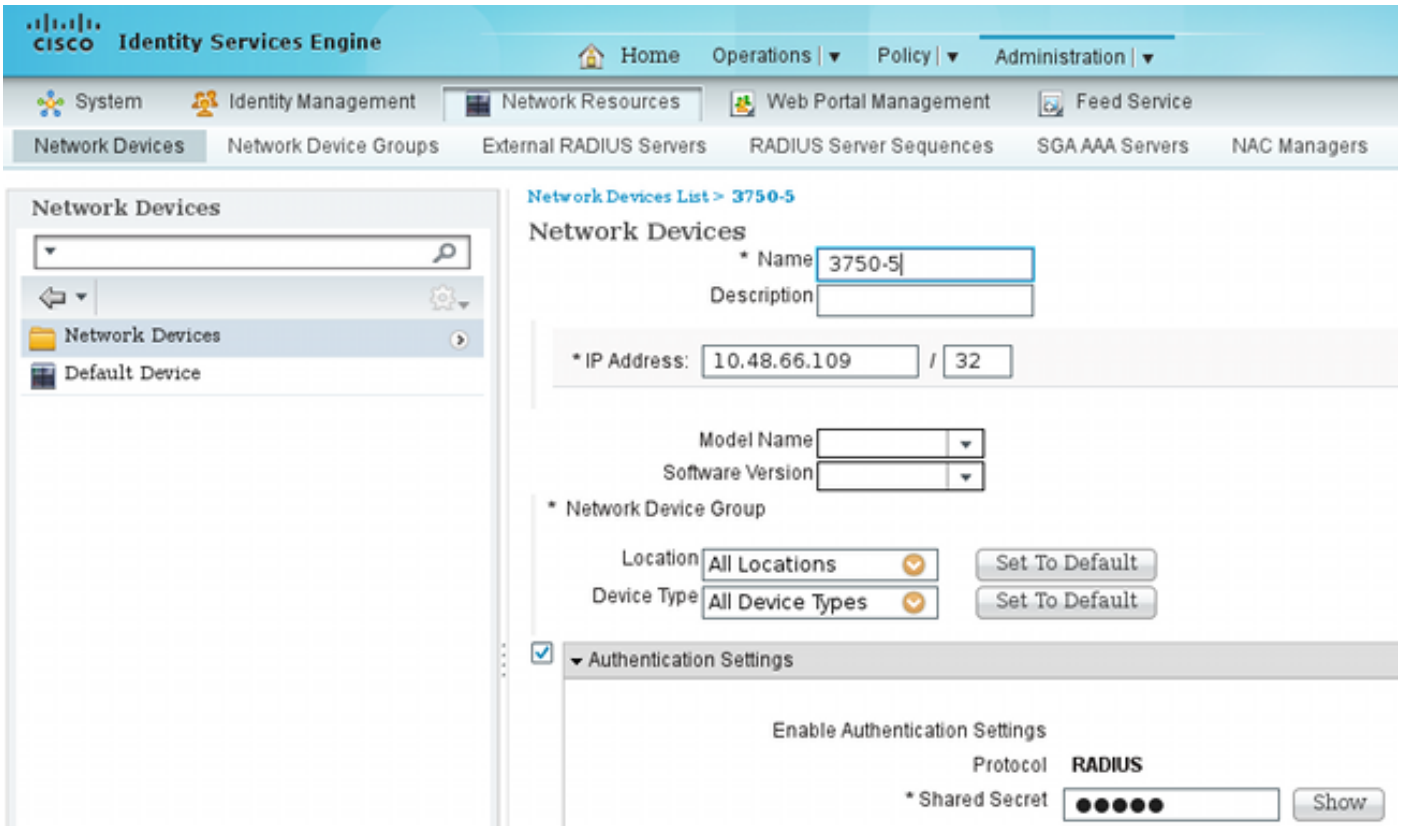
步驟3.對請求方和交換機之間的所有後續資料包進行加密（802.1AE封裝）。

組態

ISE

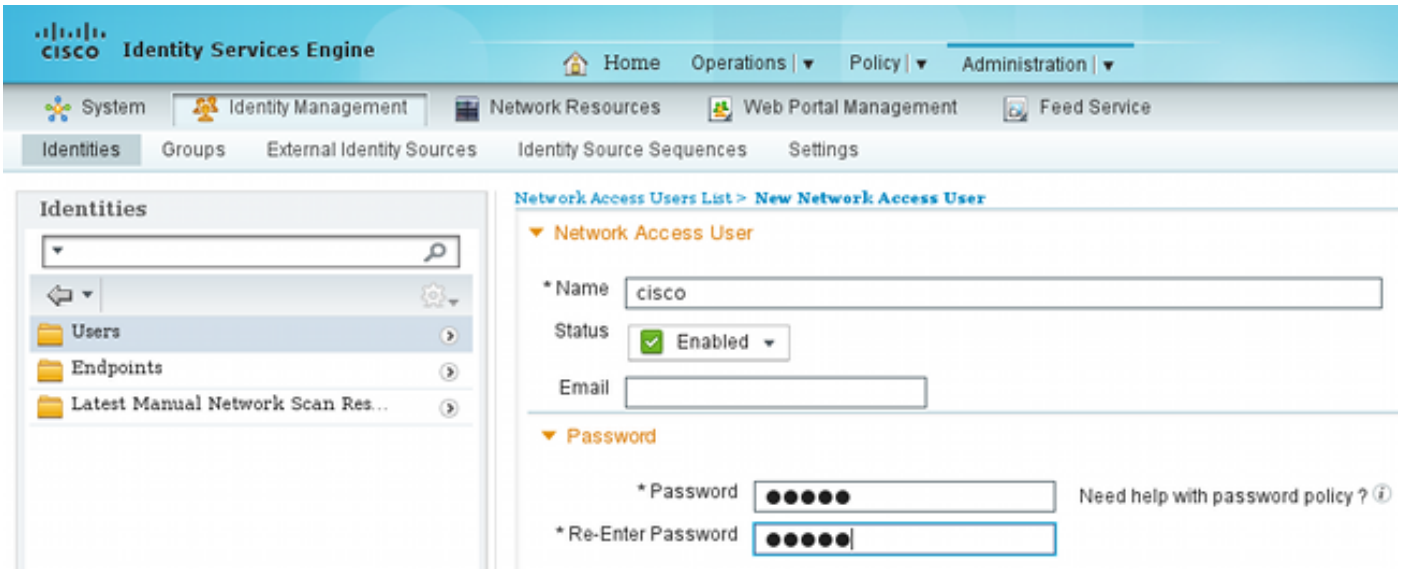
ISE配置涉及典型的802.1x方案，但授權配置檔案例外，該授權配置檔案可能包括加密策略。

選擇**Administration > Network Resources > Network Devices**，將交換機新增為網路裝置。輸入RADIUS預共用金鑰（共用金鑰）。

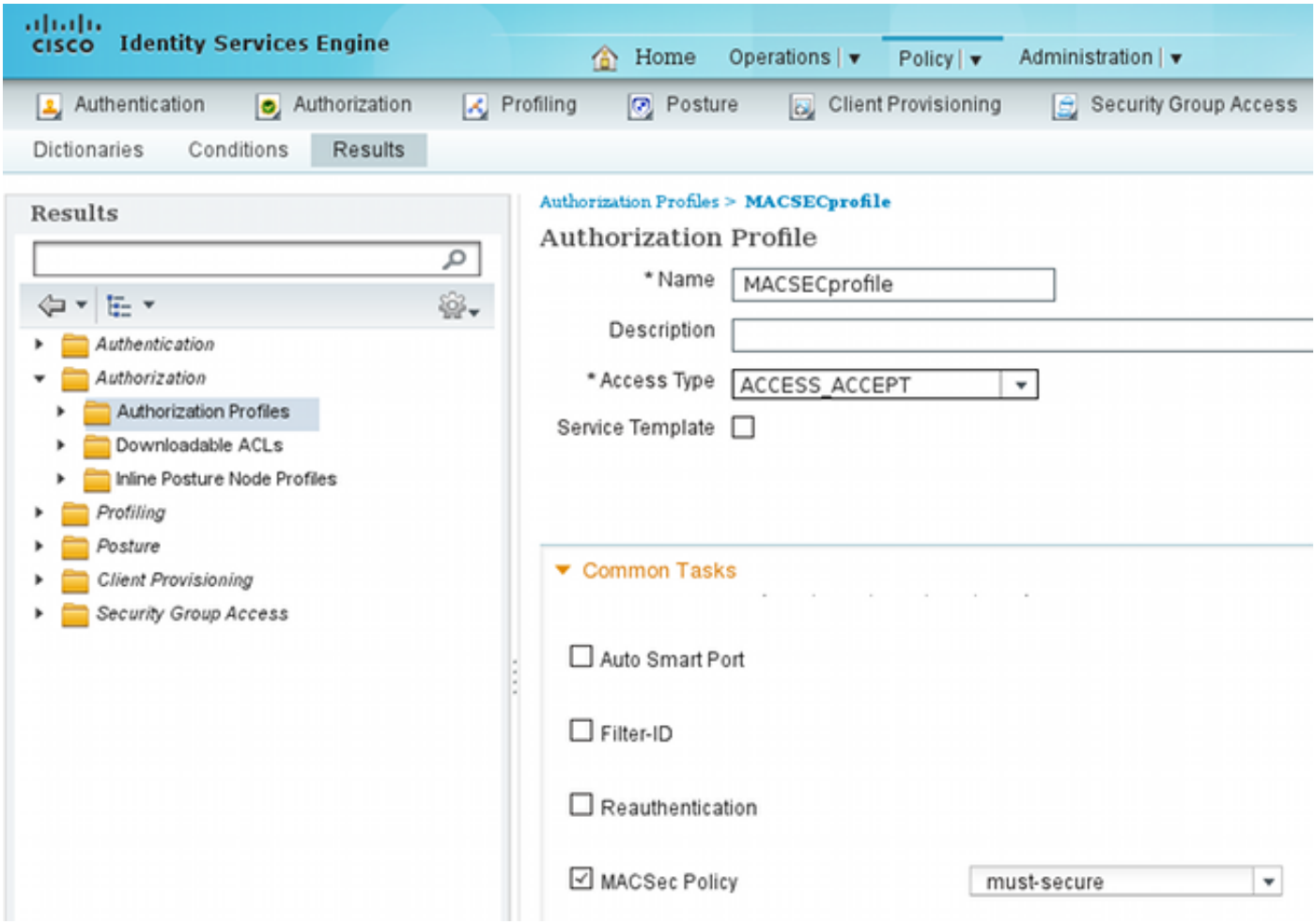


可以使用預設身份驗證規則（適用於ISE本地定義的使用者）。

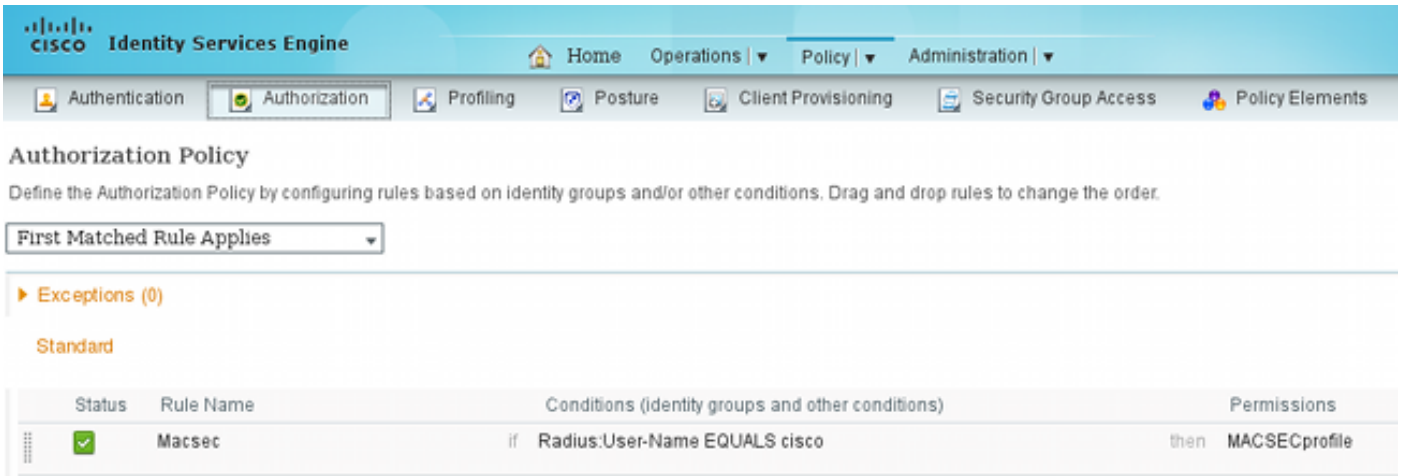
選擇**Administration > Identity Management > Users**，以在本地定義使用者「cisco」。



授權配置檔案可能包含加密策略。如以下示例所示，選擇**Policy > Results > Authorization Profiles**以檢視ISE返回交換機中鏈路加密為必需的資訊。此外，還配置了VLAN編號(10)。



選擇**Policy > Authorization**，以在授權規則中使用授權配置檔案。此範例返回使用者「cisco」的設定檔。 如果802.1x成功，ISE會將Radius-Accept返回到Cisco AVPair linksec-policy=must-secure的交換機。該屬性強制交換機啟動MKA會話。如果該會話失敗，交換機上的802.1x授權也會失敗。



交換器

典型的802.1x埠設定包括（顯示的頂部）：

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

aaa group server radius ISE
```

```
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

建立本地MKA策略並將其應用到介面。此外，MACsec在介面上啟用。

```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

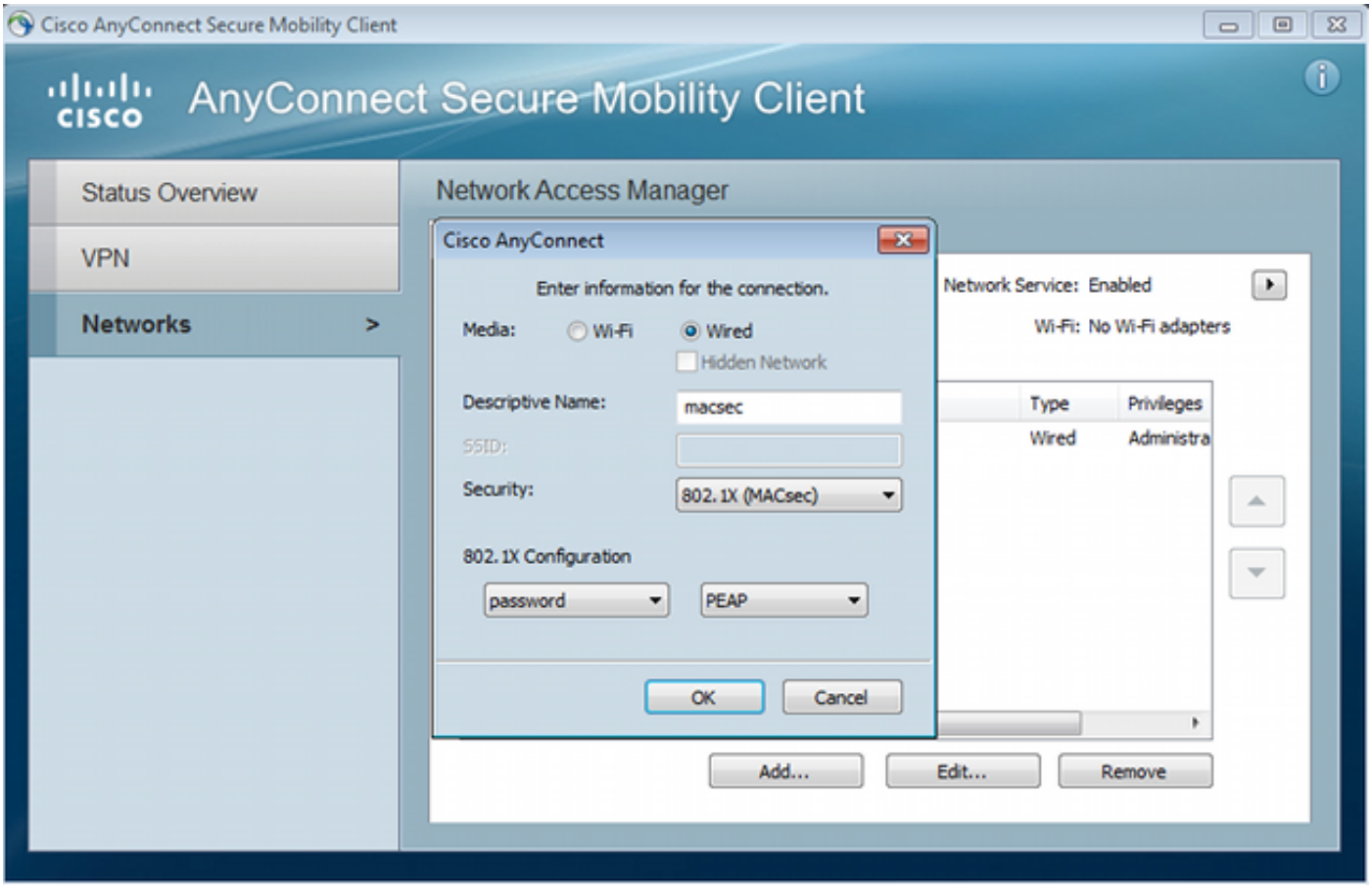
本地MKA策略允許您配置無法從ISE推送的詳細設定。本地MKA策略是可選的。

AnyConnect NAM

802.1x請求方的配置檔案可以手動配置或通過思科ASA推送。接下來的步驟是手動配置。

要管理NAM配置檔案：

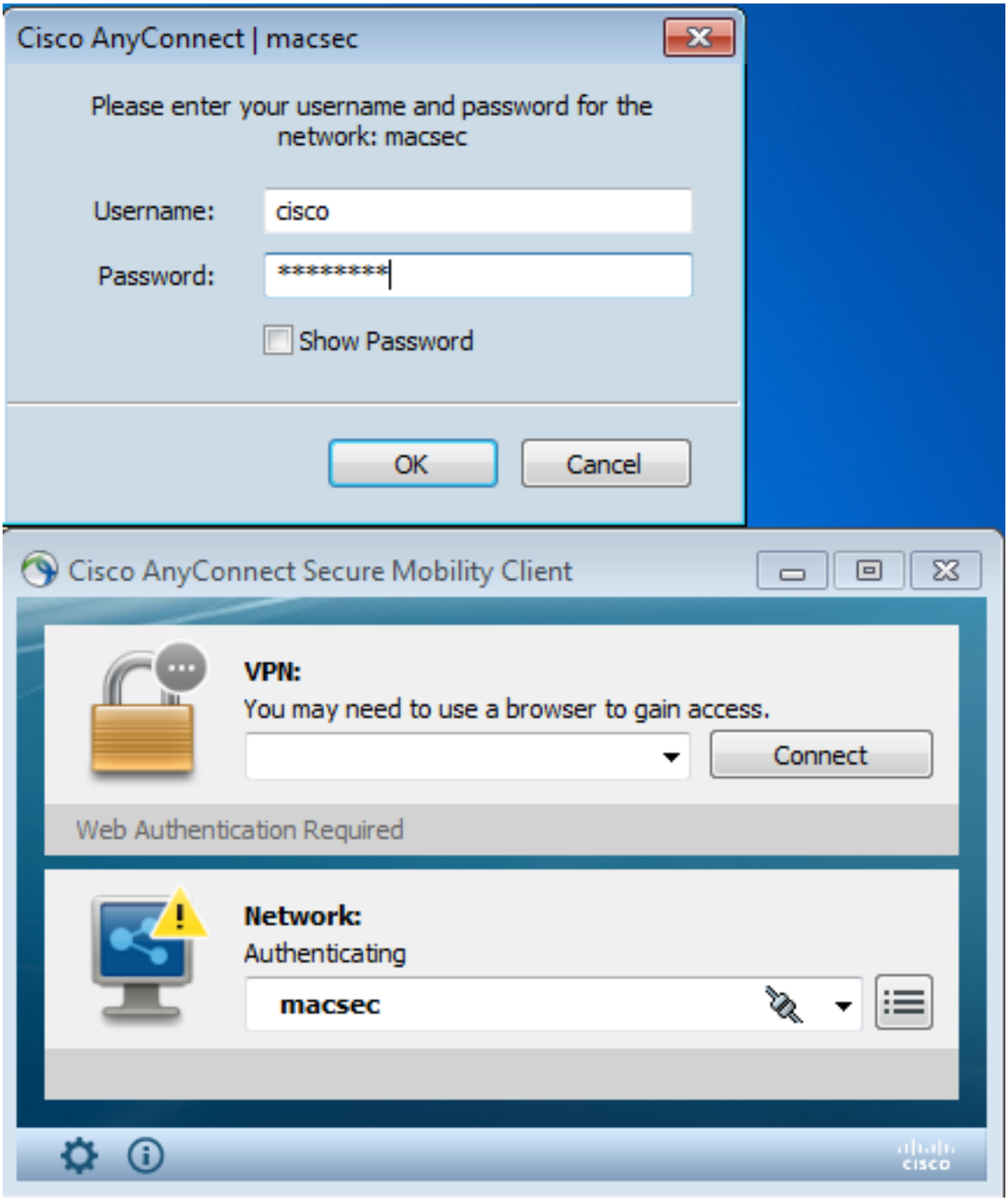
新增新的802.1x配置檔案和MACsec。對於802.1x，使用受保護的可擴展身份驗證協定(PEAP)（在ISE上配置使用者「cisco」）：



驗證

使用本節內容，確認您的組態是否正常運作。

為EAP-PEAP配置的AnyConnect NAM需要正確的憑據。



交換器上的作業階段應經過驗證和授權。安全狀態應為「安全」：

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D56FD55B3BF
```

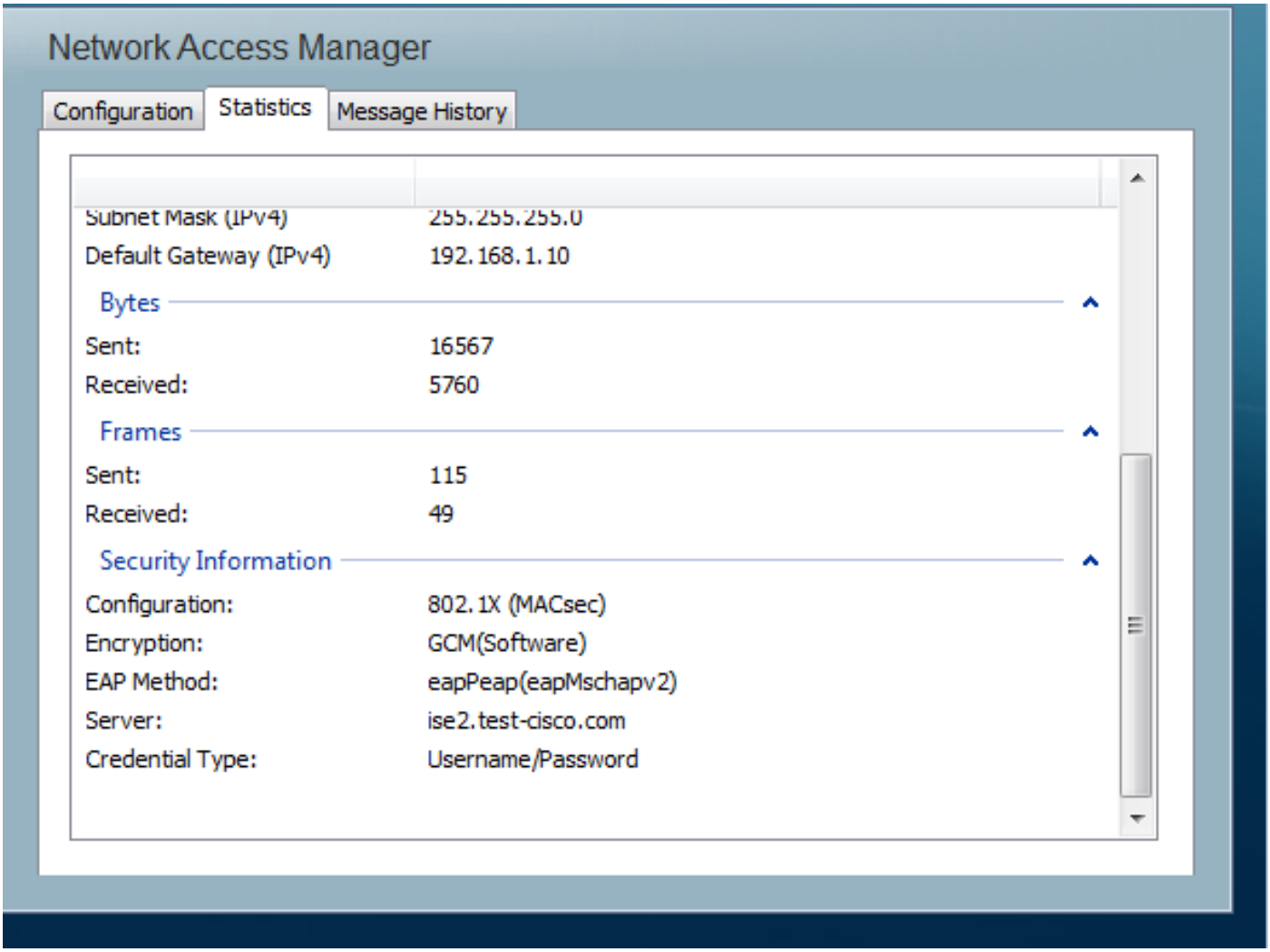
```
     Acct Session ID:  0x00011CB4
              Handle:  0x97000D57

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

交換機上的MACsec統計資訊提供有關本地策略設定、接收/傳送流量的安全通道識別符號(SCI)以及埠統計資訊和錯誤的詳細資訊。

```
bsns-3750-5#show macsec interface g1/0/2
MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
 Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
 SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

在AnyConnect上，統計資訊指示加密使用情況和資料包統計資訊。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

工作方案的調試

在交換機上啟用調試（為清楚起見，某些輸出已被忽略）。

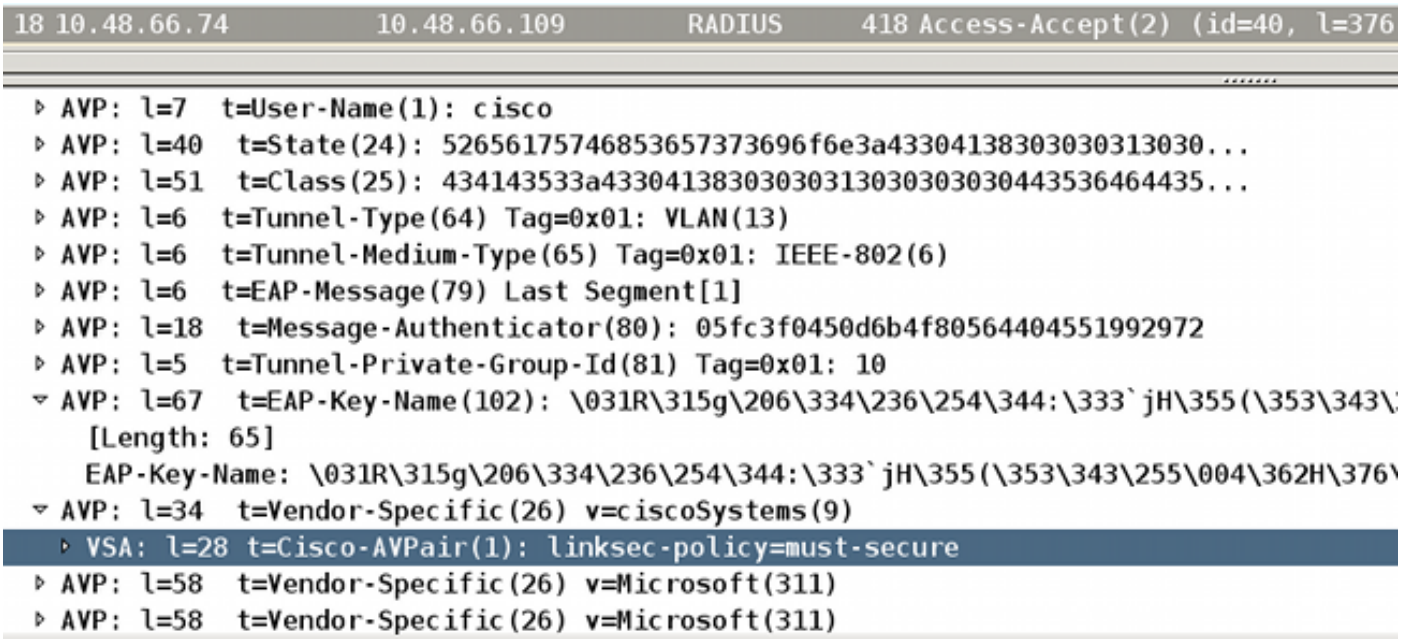
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

建立802.1x作業階段後，會透過EAPOL交換多個EAP封包。在Radius-Accept中傳送的ISE的最後成功響應（EAP成功）還包括多個Radius屬性。

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS:  EAP-Key-Name        [102] 67  *
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "linksec-policy=must-secure"
RADIUS:  Vendor, Microsoft   [26]  58
RADIUS:   MS-MPPE-Send-Key   [16]  52  *
RADIUS:  Vendor, Microsoft   [26]  58
```

```
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
```

EAP-Key-Name用於MKA會話。linksec-policy強制交換機使用MACsec（如果授權未完成，則授權失敗）。 這些屬性也可以在封包擷取中驗證。



身份驗證成功。

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

交換器會套用屬性（包括已傳送的可選VLAN編號）。

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```

交換器在傳送和接收EAPOL封包時啟動MKA作業階段。

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D56FD55B3BF, AuthMgr-Handle 97000D57
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
EAPOL pak dump rx
dot1x-packet(Gi1/0/2): Received an EAPOL frame
dot1x-packet(Gi1/0/2): Received an MKA packet
```

4個資料包交換安全識別符號與接收(RX)安全關聯一起建立。

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```

作業階段完成，且傳輸(TX)安全關聯已新增。

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
```

```
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```
策略「必須安全」已匹配，授權成功。

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```
每2秒交換一次MKA Hello資料包，以確保所有參與者都處於活動狀態。

```
dot1x-ev(Gi1/0/2): Received TX PDU (5) for the client 0x6E0001EC (0050.5699.36ce)
dot1x-packet(Gi1/0/2): MKA length: 0x0084 data&colon; ^A
dot1x-ev(Gi1/0/2): Sending EAPOL packet to group PAE address
EAPOL pak dump Tx
```

失敗方案的調試

當請求方未配置MKA且ISE在成功的802.1x身份驗證後請求加密時：

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```
交換器傳送5個EAPOL封包時嘗試啟動MKA作業階段。

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D55FD4D7529, AuthMgr-Handle A4000D56
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
```
最後，超時並且授權失敗。

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```
802.1x會話報告身份驗證成功，但授權失敗。

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Failed
```

```
               Domain:  DATA
      Security Policy:  Must Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8000100000D55FD4D7529
      Acct Session ID:  0x00011CA0
               Handle:  0xA4000D56

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

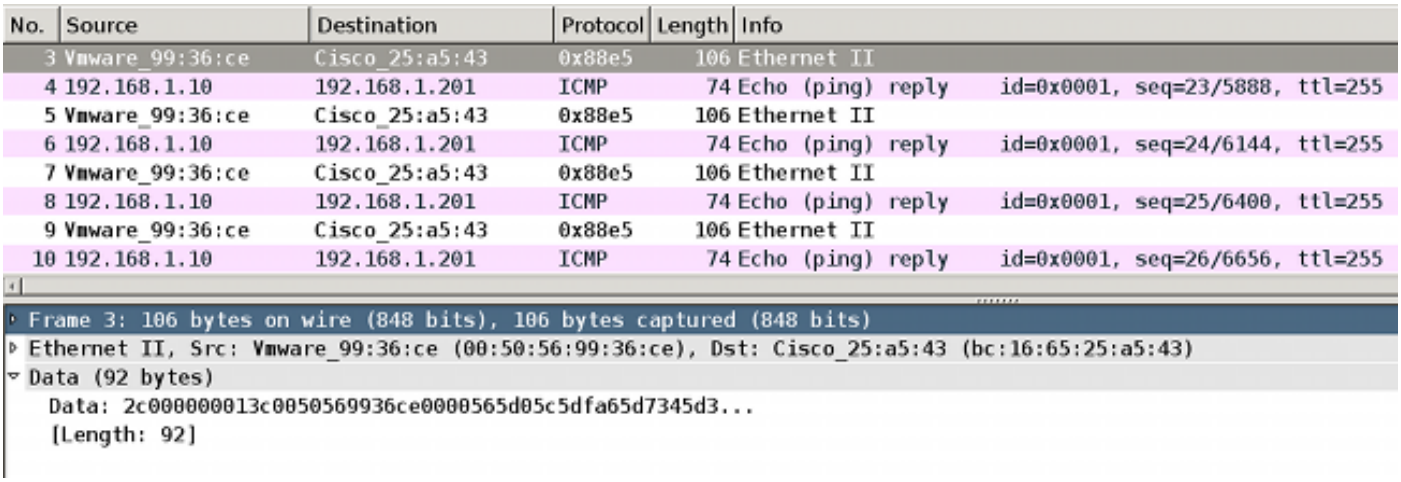
資料流量將被阻止。

封包擷取

在請求方站點上捕獲流量時，傳送和接收網際網路控制消息協定(ICMP)回應請求/應答時，將發生以下情況：

- 向交換機傳送4個加密的ICMP回應請求（88e5保留用於802.1AE）
- 收到4個解密的ICMP回應應答

這是因為在Windows API上AnyConnect掛接的方式（傳送資料包時在libpcap之前，接收資料包時在libpcap之前）：



> **附註**：不支援使用交換式連線埠分析器(SPAN)或嵌入式封包擷取(EPC)等功能在交換器上偵測MKA或802.1AE流量。

MACsec和802.1x模式

MACsec不支援所有802.1x模式。

*Cisco TrustSec 3.0操作指南：MACsec和NDAC簡介*指出：

- **單主機模式**:**在單主機模**式下完全支援MACsec。在此模式下，只有一個MAC或IP地址可以通過MACsec進行身份驗證和保護。如果終端通過身份驗證後在埠上檢測到不同的MAC地址，則會在埠上觸發安全違規。
- **多網域驗證(MDA)模式**:在此模式中，一個端點可能位於資料域上，而另一個端點可能位於語音

域上。**MDA模式完全支援MACsec**。如果兩個終端都支援MACsec，則每個終端都將由其自己的獨立MACsec會話進行保護。如果只有一個端點支援MACsec，則可以在另一個端點以明文形式傳送流量時保護該端點。

- **多重驗證模式**:在此模式中，實際上無限數量的端點可被認證到單個交換機埠。**在此模式下不支援MACsec。**
- **多主機模式**:雖然在此模式下使用MACsec在技術上可行，但**不建議這樣做**。在多主機模式下，埠上的第一個端點進行身份驗證，然後通過第一個授權允許任何其他端點訪問網路。MACsec可與第一個連線的主機一起使用，但其他端點的流量不會實際通過，因為它不是加密流量。

相關資訊

- Cisco TrustSec 3750配置指南
- 適用於ASA 9.1的Cisco TrustSec配置指南
- 基於身份的網路服務：MAC安全
- 在Catalyst 3750X系列交換機上使用802.1x MACsec的TrustSec雲配置示例
- ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南
- Cisco TrustSec部署和路線圖
- 技術支援與文件 - Cisco Systems