

使用Cisco AnyConnect和ISE的MACsec交换机主机加密配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图和流量流程](#)

[配置](#)

[ISE](#)

[交换机](#)

[AnyConnect NAM](#)

[验证](#)

[故障排除](#)

[工作场景的调试](#)

[失败场景的调试](#)

[数据包捕获](#)

[MACsec和802.1x模式](#)

[相关信息](#)

简介

本文档提供802.1x请求方（Cisco AnyConnect移动安全）和身份验证器（交换机）之间介质访问控制安全(MACsec)加密的配置示例。思科身份服务引擎(ISE)用作身份验证和策略服务器。

MACsec在802.1AE中进行标准化，并在Cisco 3750X、3560X和4500 SUP7E交换机上受支持。802.1AE定义使用带外密钥的有线网络上的链路加密。这些加密密钥与MACsec密钥协议(MKA)协议协商，MKA协议在802.1x身份验证成功后使用。MKA在IEEE 802.1X-2010中进行标准化。

数据包仅在PC和交换机之间的链路上加密（点对点加密）。交换机收到的数据包将解密并通过未加密的上行链路发送。为了加密交换机之间的传输，建议使用交换机 — 交换机加密。对于该加密，安全关联协议(SAP)用于协商和重新生成密钥。SAP是思科开发的一种准标准密钥协议。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1x配置的基本知识
- Catalyst交换机CLI配置的基本知识
- ISE配置体验

使用的组件

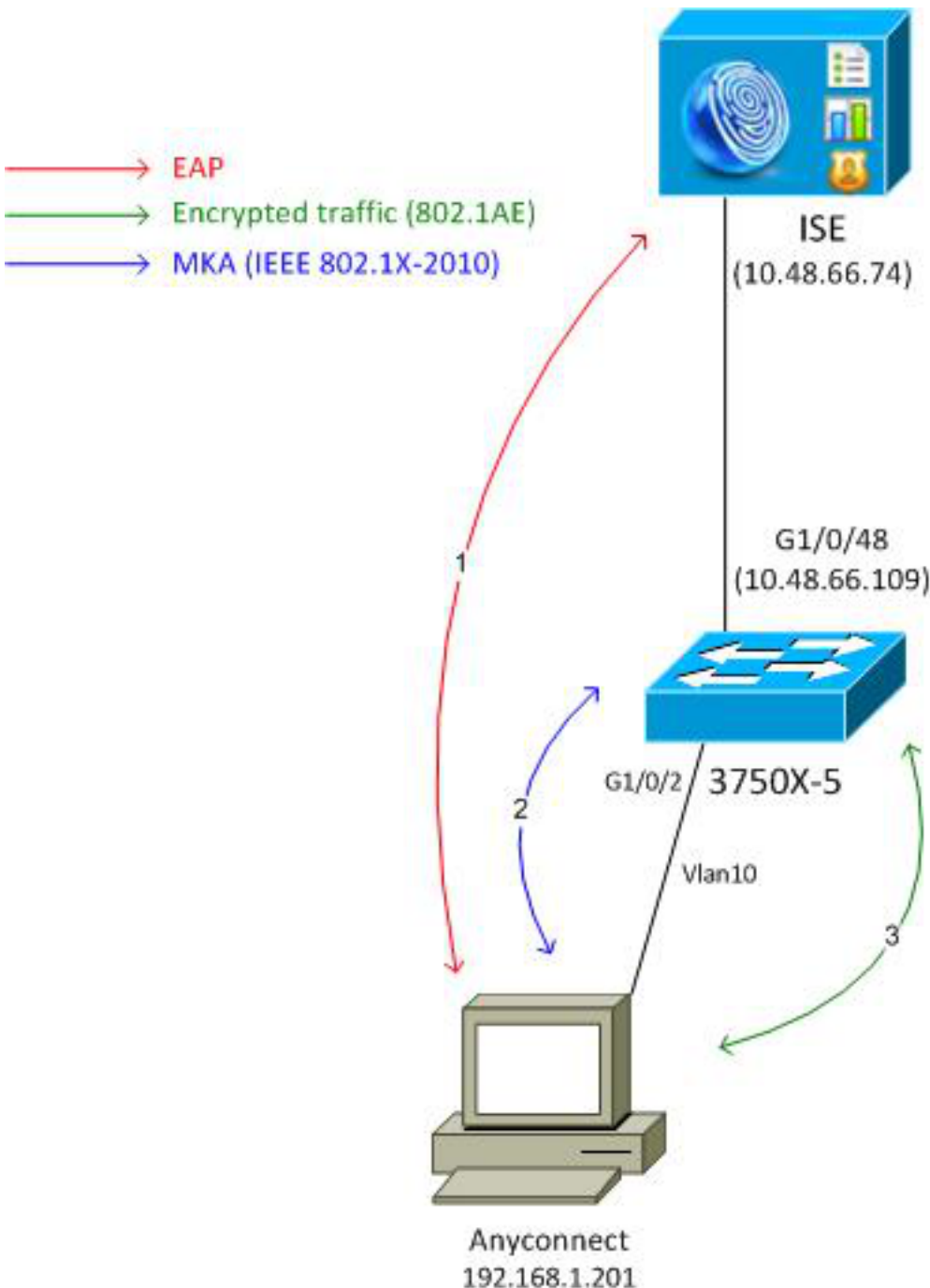
本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7和Microsoft Windows XP操作系统
- Cisco 3750X软件15.0版及更高版本
- 思科ISE软件版本1.1.4及更高版本
- 带网络接入管理器(NAM)的Cisco AnyConnect移动安全3.1版及更高版本

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

网络图和流量流程



步骤1.请求方(AnyConnect NAM)启动802.1x会话。交换机是身份验证器，ISE是身份验证服务器。LAN上的可扩展身份验证协议(EAPOL)协议用作请求方和交换机之间EAP的传输。RADIUS用作交换机和ISE之间EAP的传输协议。无法使用MAC身份验证绕行(MAB)，因为EAPOL密钥需要从ISE返回并用于MACsec密钥协议(MKA)会话。

步骤2.在802.1x会话完成后，交换机会以EAPOL作为传输协议启动MKA会话。如果请求方配置正确，则对称128位AES-GCM(Galois/Counter Mode)加密的密钥匹配。

步骤3.请求方和交换机之间的所有后续数据包都经过加密(802.1AE封装)。

配置

ISE

ISE配置涉及典型的802.1x方案，但授权配置文件例外，可能包括加密策略。

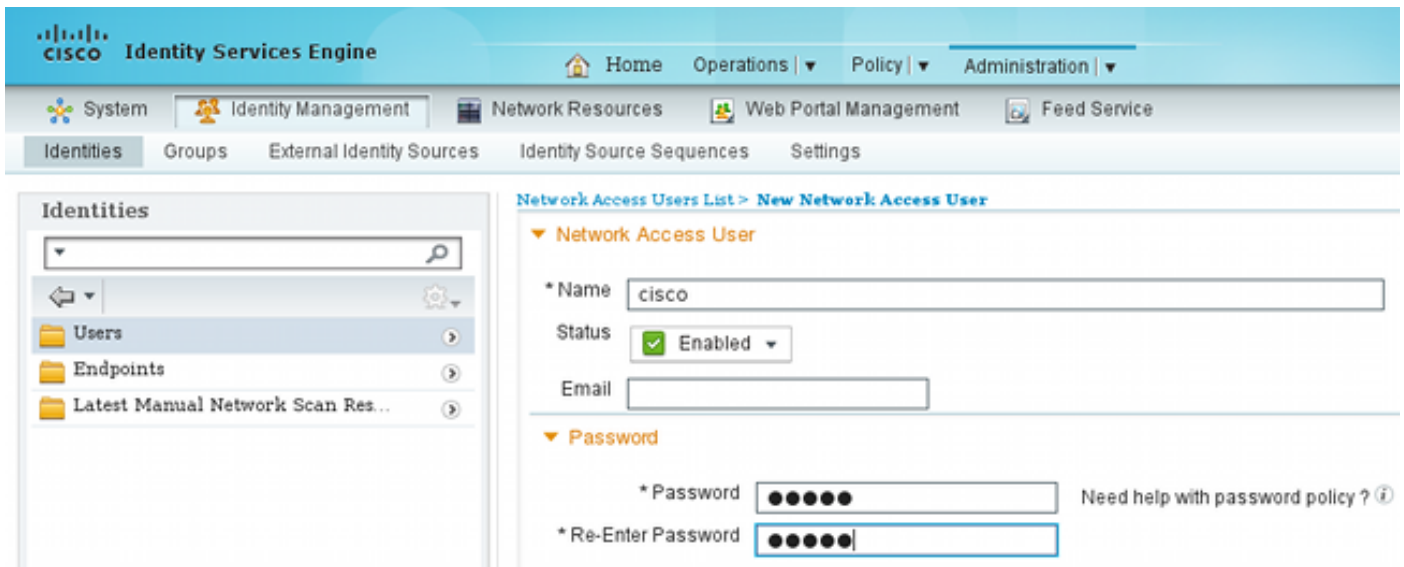
选择**Administration > Network Resources > Network Devices**以将交换机添加为网络设备。输入RADIUS预共享密钥(共享密钥)。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Network Device. The breadcrumb navigation is **Administration > Network Resources > Network Devices**. The page title is **Network Devices List > 3750-5**. The main configuration area is titled **Network Devices** and contains the following fields:

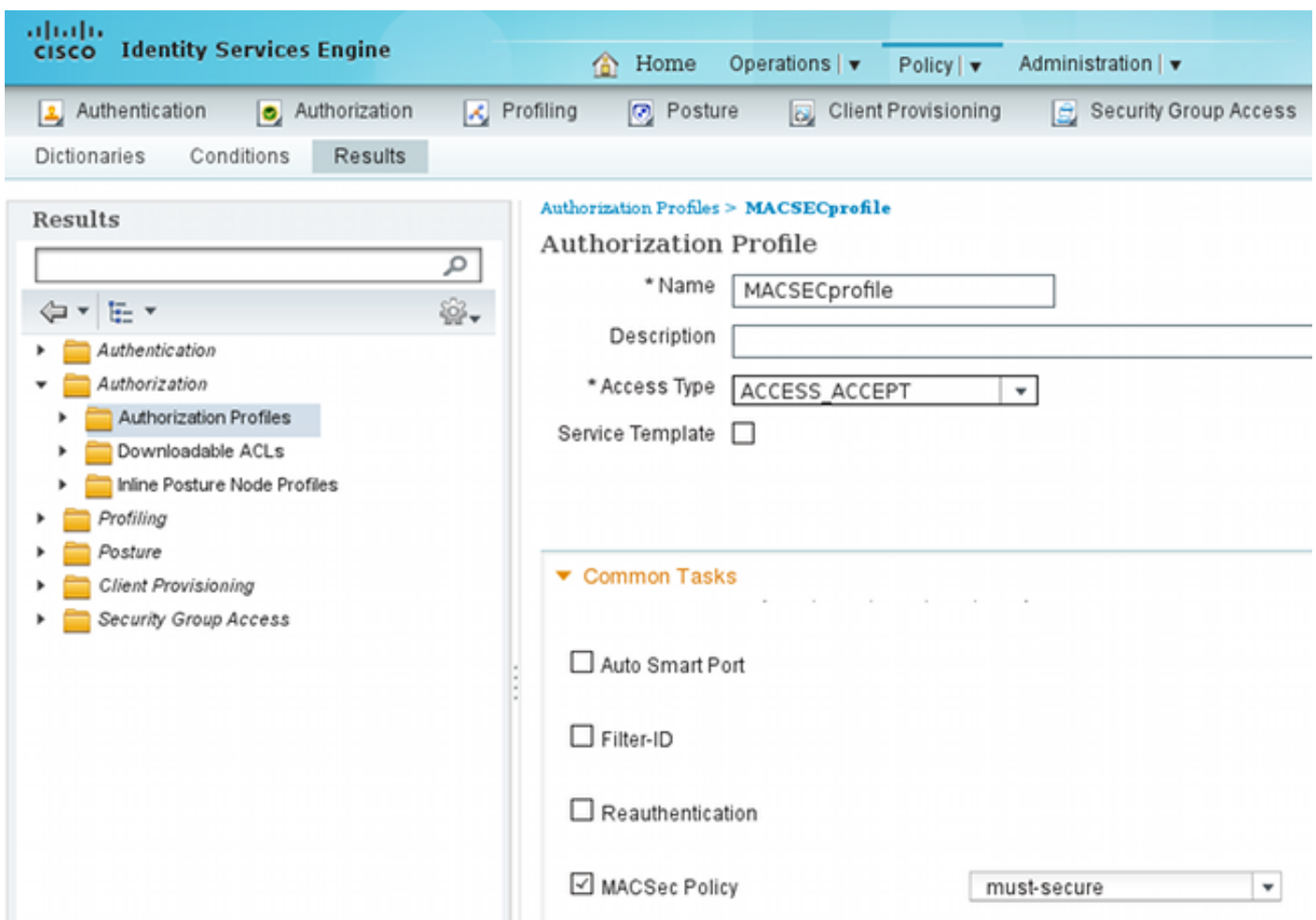
- Name:** 3750-5
- Description:** (empty)
- IP Address:** 10.48.66.109 / 32
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- Network Device Group:** (dropdown menu)
- Location:** All Locations (dropdown menu) with a **Set To Default** button.
- Device Type:** All Device Types (dropdown menu) with a **Set To Default** button.
- Authentication Settings:** (checked checkbox) with a dropdown arrow.
- Enable Authentication Settings:** (checkbox)
- Protocol:** RADIUS
- Shared Secret:** (masked field with 6 dots) and a **Show** button.

默认身份验证规则可用于(用于ISE上本地定义的用户)。

选择**Administration > Identity Management > Users**以在本地定义用户“cisco”。



授权配置文件可能包括加密策略。如本示例所示，选择**Policy > Results > Authorization Profiles**以查看ISE返回给交换机的链路加密是必需的信息。此外，还配置了VLAN编号(10)。



选择**Policy > Authorization**以在授权规则中使用授权配置文件。此示例返回用户“cisco”的配置文件。如果802.1x成功，ISE将Radius-Accept返回到具有Cisco AVPair linksec-policy=must-secure的交换机。该属性强制交换机启动MKA会话。如果该会话失败，交换机上的802.1x授权也会失败。

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Macsec	if Radius:User-Name EQUALS cisco	then MACSECprofile

交换机

典型的802.1x端口设置包括 (显示顶部) :

```

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

```

本地MKA策略已创建并应用于接口。此外，接口上启用了MACsec。

```

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

```

```

interface GigabitEthernet1/0/2

```

```

macsec
mka policy mka-policy

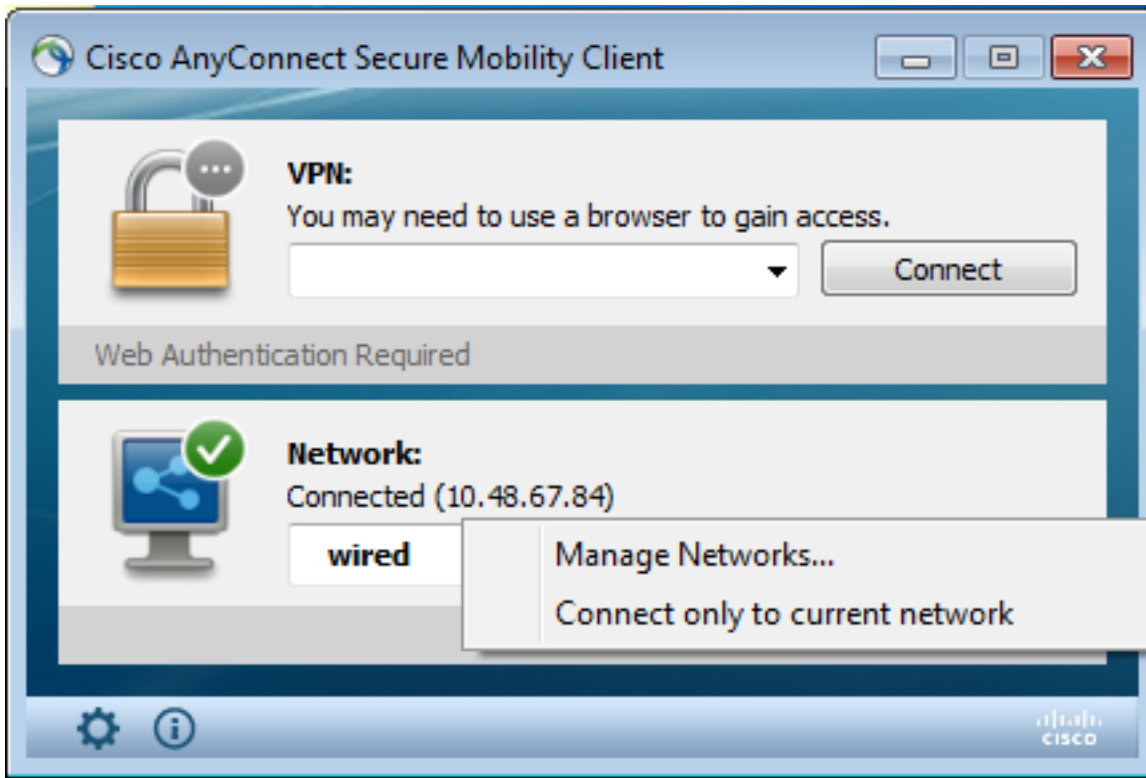
```

本地MKA策略允许您配置无法从ISE推送的详细设置。本地MKA策略是可选的。

AnyConnect NAM

802.1x请求方的配置文件可以手动配置或通过Cisco ASA推送。后续步骤提供手动配置。

要管理NAM配置文件，请执行以下操作：



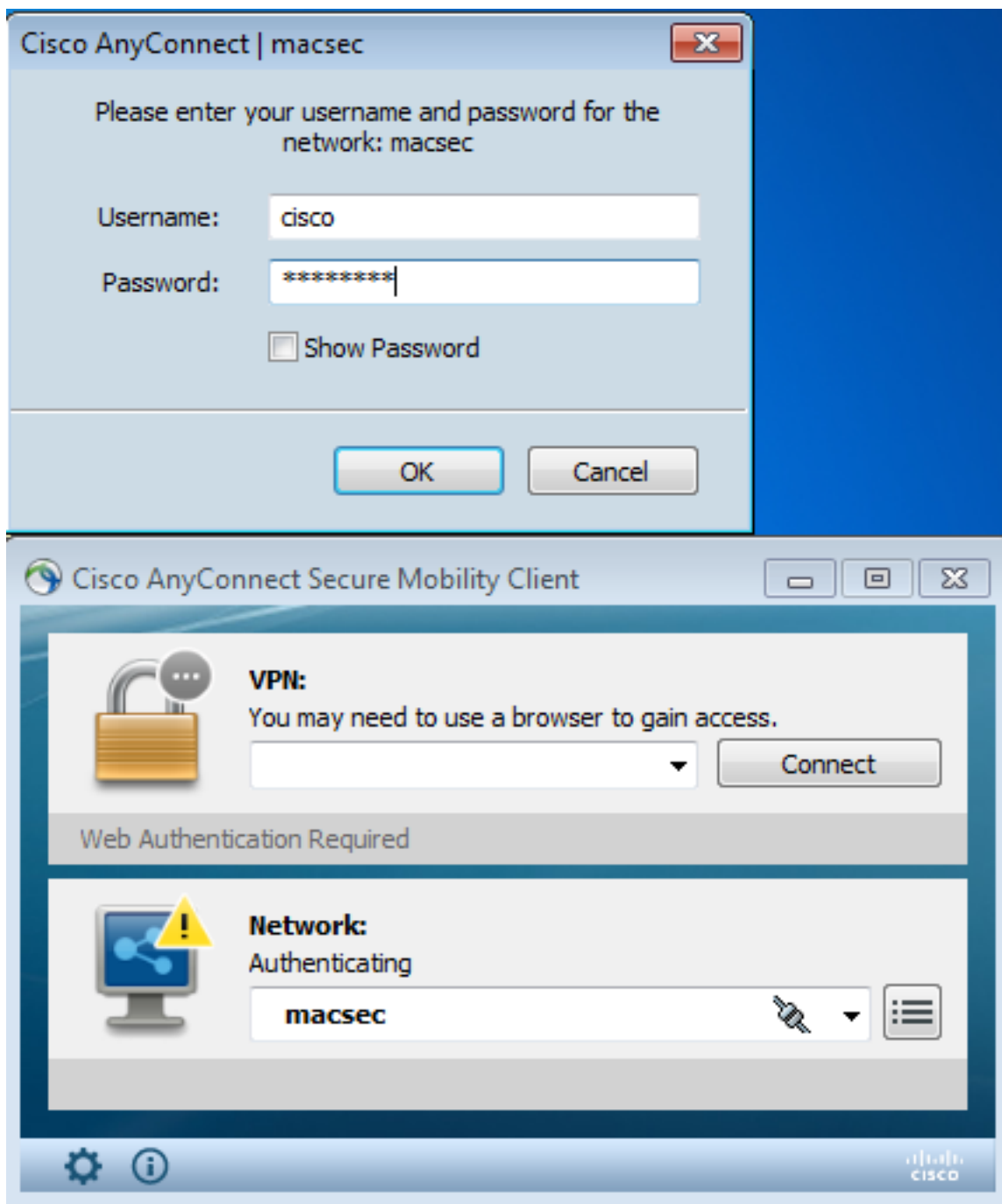
添加带MACsec的新802.1x配置文件。对于802.1x，使用受保护的可扩展身份验证协议(PEAP)（在ISE上配置的用户“cisco”）：



验证

使用本部分可确认配置能否正常运行。

为EAP-PEAP配置的AnyConnect NAM需要正确的凭证。



交换机上的会话应经过身份验证和授权。安全状态应为“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

交换机上的MACsec统计信息提供有关本地策略设置、接收/发送流量的安全通道标识符(SCI)以及端口统计和错误的详细信息。

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

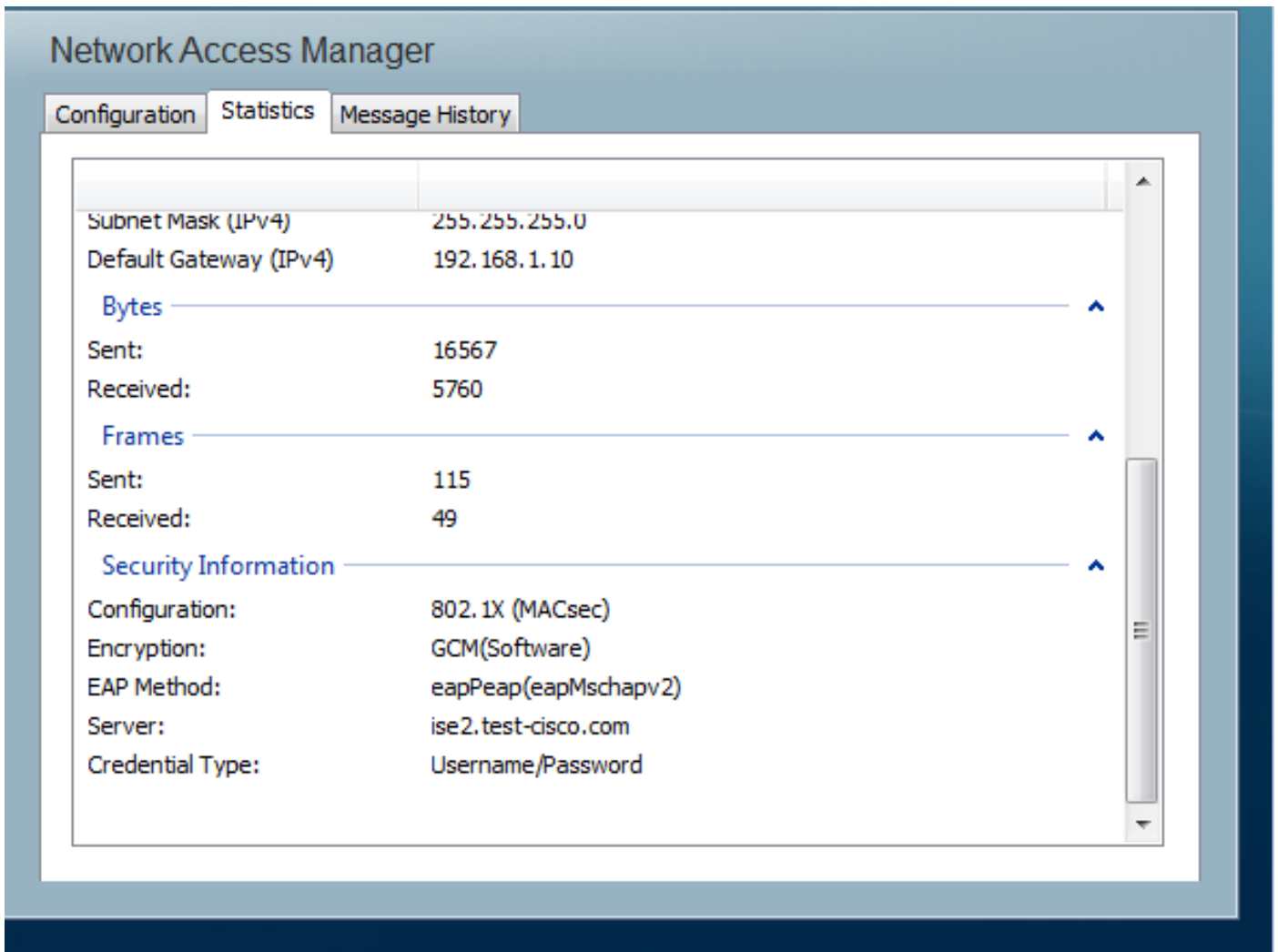
Ingress badtag pkts 0 Ingress unknownSCI pkts 0

Ingress noSCI pkts 0 Unused pkts 0

Notusing pkts 0 **Decrypt bytes 176153**

Ingress miss pkts 2437

在AnyConnect上，统计信息指示加密使用情况和数据包统计信息。



故障排除

本部分提供的信息可用于对配置进行故障排除。

工作场景的调试

在交换机上启用调试（为清楚起见，省略了某些输出）。

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

在建立802.1x会话后，多个EAP数据包通过EAPOL交换。Radius-Accept内部携带的ISE（EAP成功）的最后成功响应也包含多个Radius属性。

```
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用于MKA会话。链路安全策略强制交换机使用MACsec (如果未完成, 授权将失败)。这些属性也可以在数据包捕获中进行验证。

```
18 10.48.66.74          10.48.66.109          RADIUS          418 Access-Accept(2) (id=40, l=376)
.....
> AVP: l=7  t=User-Name(1): cisco
> AVP: l=40  t=State(24): 52656175746853657373696f6e3a43304138303030313030...
> AVP: l=51  t=Class(25): 434143533a43304138303030313030303030443536464435...
> AVP: l=6   t=Tunnel-Type(64) Tag=0x01: VLAN(13)
> AVP: l=6   t=Tunnel-Medium-Type(65) Tag=0x01: IEEE-802(6)
> AVP: l=6   t=EAP-Message(79) Last Segment[1]
> AVP: l=18  t=Message-Authenticator(80): 05fc3f0450d6b4f80564404551992972
> AVP: l=5   t=Tunnel-Private-Group-Id(81) Tag=0x01: 10
< AVP: l=67  t=EAP-Key-Name(102): \031R\315g\206\334\236\254\344:\333`jH\355(\353\343\
  [Length: 65]
  EAP-Key-Name: \031R\315g\206\334\236\254\344:\333`jH\355(\353\343\255\004\362H\376\
< AVP: l=34  t=Vendor-Specific(26) v=ciscoSystems(9)
  > VSA: l=28 t=Cisco-AVPair(1): linksec-policy=must-secure
> AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
> AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
```

身份验证成功。

```
%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
交换机应用属性 ( 这些属性包括也已发送的可选VLAN编号 )。
```

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

然后, 交换机在发送和接收EAPOL数据包时启动MKA会话。

```
%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个数据包交换安全标识符与接收(RX)安全关联一起创建。

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A502002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
会话完成, 并添加传输(TX)安全关联。
```

```
%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“必须安全”匹配，授权成功。

%AUTHMGR-5-SUCCESS: **Authorization succeeded** for client (0050.5699.36ce) on
Interface Gil/0/2 AuditSessionID C0A8000100000D56FD55B3BF

每2秒交换一次MKA Hello数据包，以确保所有参与者都处于活动状态。

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

失败场景的调试

如果请求方未配置MKA，并且ISE在成功进行802.1x身份验证后请求加密：

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 Gil/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: **Authentication result 'success' from 'dot1x'** for client
(0050.5699.36ce) on Interface Gil/0/2 AuditSessionID C0A8000100000D55FD4D7529
当交换机发送5个EAPOL数据包时，会尝试发起MKA会话。

%MKA-5-SESSION_START: (Gil/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D55FD4D7529, AuthMgr-Handle A4000D56
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gil/0/2): Sending out EAPOL packet
EAPOL pak dump Tx

最后超时并失败授权。

%MKA-4-KEEPALIVE_TIMEOUT: (Gil/0/2 : 2) **Peer has stopped sending MKPDUs** for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gil/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 Gil/0/2 AuditSessionID C0A8000100000D55FD4D7529
802.1x会话报告身份验证成功，但授权失败。

```
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: COA8000100000D55FD4D7529
Acct Session ID: 0x00011CA0
Handle: 0xA4000D56

```

Runnable methods list:

```

Method State
dot1x Authc Success

```

数据流量将被阻止。

数据包捕获

当在请求方站点4上捕获流量时，会发送和接收互联网控制消息协议(ICMP)回应请求/应答，将有：

- 4个发送到交换机的加密ICMP回应请求（88e5保留用于802.1AE）
- 收到4个解密的ICMP应答

这是因为AnyConnect如何挂接Windows API（在发送数据包时在libpcap之前，在接收数据包时在libpcap之前）：

No.	Source	Destination	Protocol	Length	Info
3	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
4	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=255
5	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
6	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=255
7	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
8	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=255
9	Vmware_99:36:ce	Cisco_25:a5:43	0x88e5	106	Ethernet II
10	192.168.1.10	192.168.1.201	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=255


```

Frame 3: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: Vmware_99:36:ce (00:50:56:99:36:ce), Dst: Cisco_25:a5:43 (bc:16:65:25:a5:43)
Data (92 bytes)
Data: 2c00000013c0050569936ce0000565d05c5dfa65d7345d3...
[Length: 92]

```

注意：不支持使用交换端口分析器(SPAN)或嵌入式数据包捕获(EPC)等功能嗅探交换机上的MKA或802.1AE流量。

MACsec和802.1x模式

并非所有802.1x模式都支持MACsec。

《Cisco TrustSec 3.0操作指南：MACsec和NDAC简介指出：

- **单主机模式:**单主机模式完全支持MACsec。在此模式下，只有单个MAC或IP地址可以通过MACsec进行身份验证和保护。如果终端经过身份验证后在端口上检测到不同的MAC地址，则端口上将触发安全违规。
- **多域身份验证(MDA)模式:**在此模式下，一个终端可能在数据域上，而另一个终端可能在语音域上。MDA模式下完全支持MACsec。如果两个终端都支持MACsec，则每个终端都将由其独立

的MACsec会话来保护。如果只有一个终端支持MACsec，则该终端可以受到保护，而另一个终端以明文方式发送流量。

- **多身份验证模式:**在此模式下，可以向单个交换机端口验证几乎无限数量的终端。**此模式不支持MACsec。**
- **多主机模式:**虽然在此模式下使用MACsec在技术上是可能的，**但不建议使用**。在多主机模式下，端口上的第一个终端会进行身份验证，然后通过第一个授权允许任何其他终端进入网络。MACsec可与第一台连接的主机配合使用，但其他终端的流量实际上不会通过，因为它不是加密流量。

相关信息

- [适用于3750的思科TrustSec配置指南](#)
- [适用于ASA 9.1的思科TrustSec配置指南](#)
- [基于身份的网络服务：MAC安全](#)
- [在Catalyst 3750X系列交换机上具有802.1x MACsec的TrustSec云配置示例](#)
- [ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南](#)
- [Cisco TrustSec部署和路线图](#)
- [技术支持和文档 - Cisco Systems](#)