MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example

Contents

Introduction

This document provides a configuration example for Media Access Control Security (MACsec) encryption between an 802.1x supplicant (Cisco AnyConnect Mobile Security) and an authenticator (switch). Cisco Identity Services Engines (ISE) is used as authentication and policy server.

MACsec is standardized in 802.1AE and supported on Cisco 3750X, 3560X, and 4500 SUP7E switches. 802.1AE defines link encryption over wired networks that use out-of-band keys. Those encryption keys are negotiated with the MACsec Key Agreement (MKA) protocol which is utilized after successful 802.1x authentication. MKA is standardized in IEEE 802.1X-2010.

A packet is encrypted only on the link between the PC and the switch (point-to-point encryption). The packet received by the switch is decrypted and sent via uplinks unencrypted. In order to encrypt transmission between the switches, switch-switch encryption is recommended. For that encryption, Security Association Protocol (SAP) is used to negotiate and regenerate keys. SAP is a prestandard key agreement protocol developed by Cisco.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of 802.1x configuration
- Basic knowledge of CLI configuration of Catalyst switches
- Experience with ISE configuration

Components Used

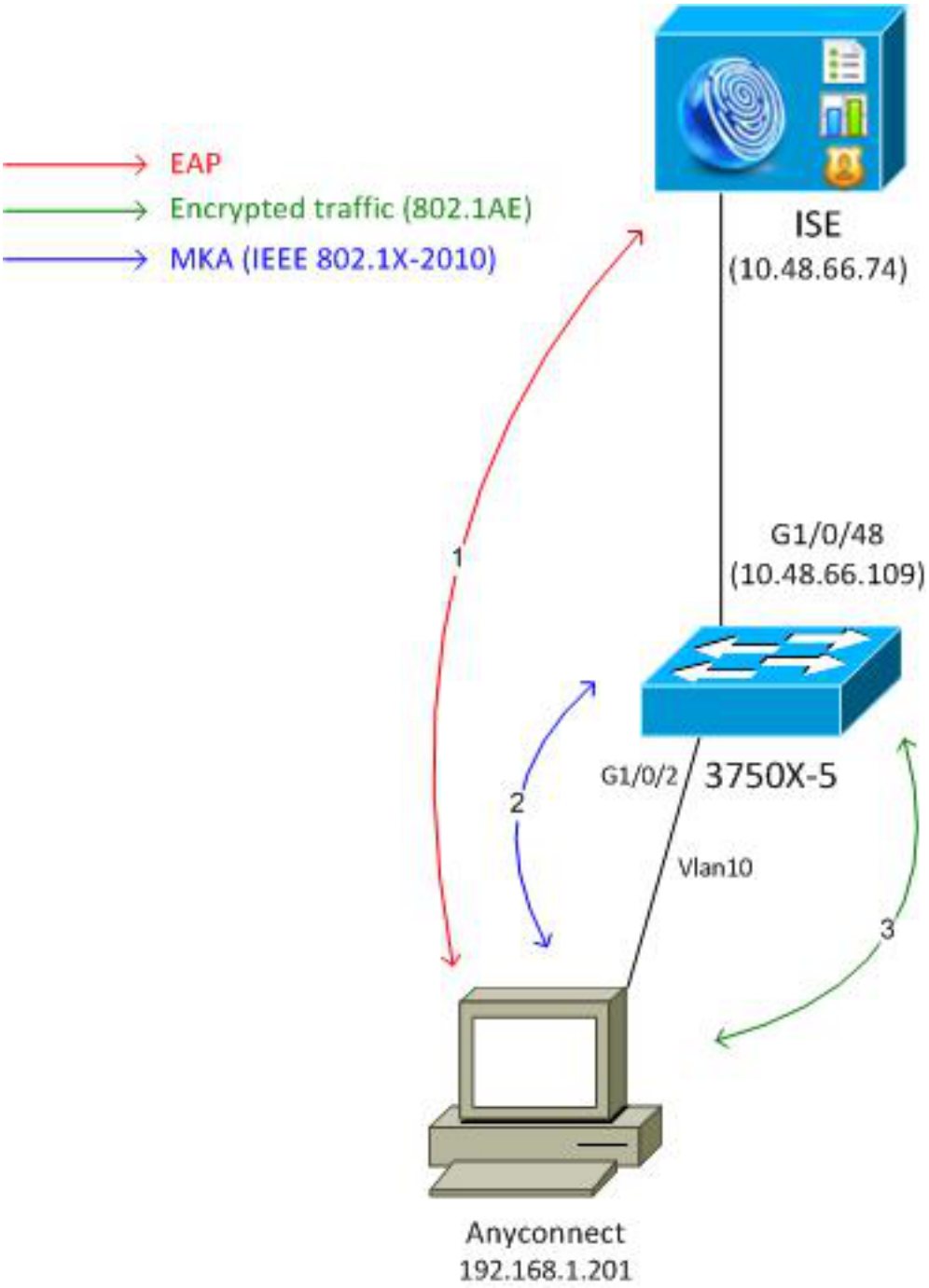
The information in this document is based on these software and hardware versions:

- Microsoft Windows 7 and Microsoft Windows XP operating systems
- Cisco 3750X Software, Version 15.0 and later
- Cisco ISE Software, Version 1.1.4 and later
- Cisco AnyConnect Mobile Security with Network Access Manager (NAM), Version 3.1 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 and Traffic Flow



Step 1. The supplicant (AnyConnect NAM) starts the 802.1x session. The switch is the authenticator and the ISE is the authentication server. Extensible Authentication Protocol over LAN (EAPOL) protocol is used as a transport for EAP between the supplicant and the switch. RADIUS is used as a transport protocol for EAP between the switch and the ISE. MAC Authentication Bypass (MAB) cannot be used, because EAPOL keys need to be returned from ISE and used for the MACsec Key Agreement (MKA) session.

Step 2. After the 802.1x session is complete, the switch initiates an MKA session with EAPOL as a transport protocol. If the supplicant is configured correctly, the keys for symmetric 128-bit AES-GCM (Galois/Counter Mode) encryption match.

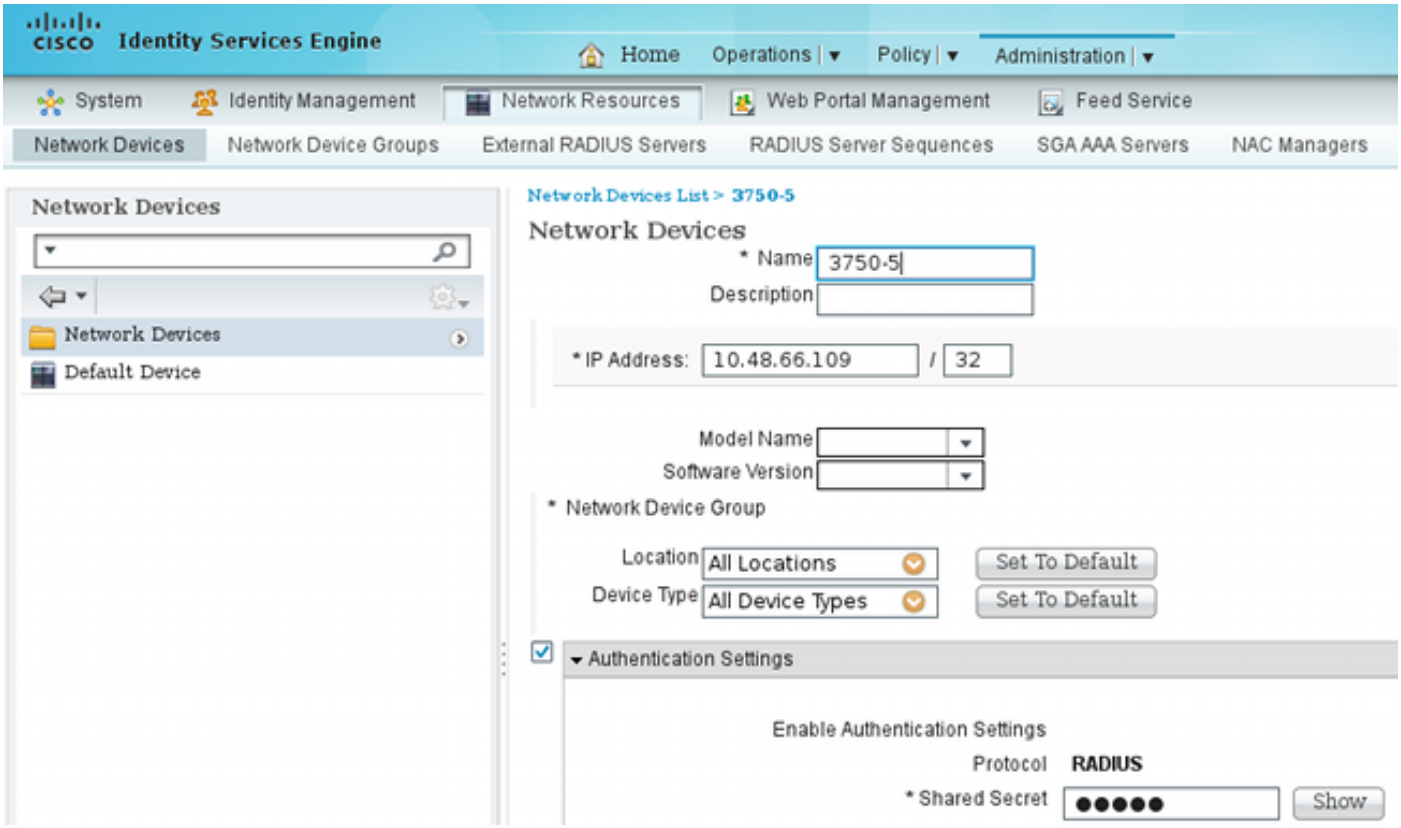
Step 3. All subsequent packets between the supplicant and the switch are encrypted (802.1AE encapsulation).

Configurations

ISE

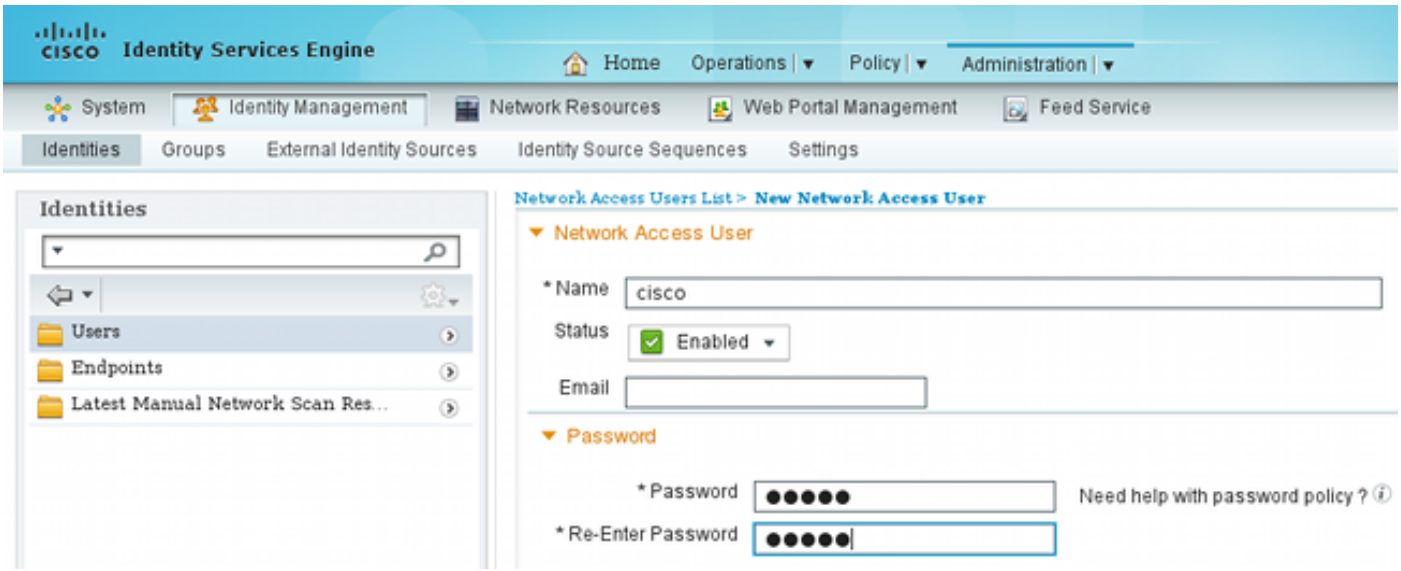
The ISE configuration involves a typical 802.1x scenario with an exception to the Authorization Profile which might include encryption policies.

Choose **Administration > Network Resources > Network Devices** in order to add the switch as a network device. Enter a RADIUS preshared key (Shared Secret).



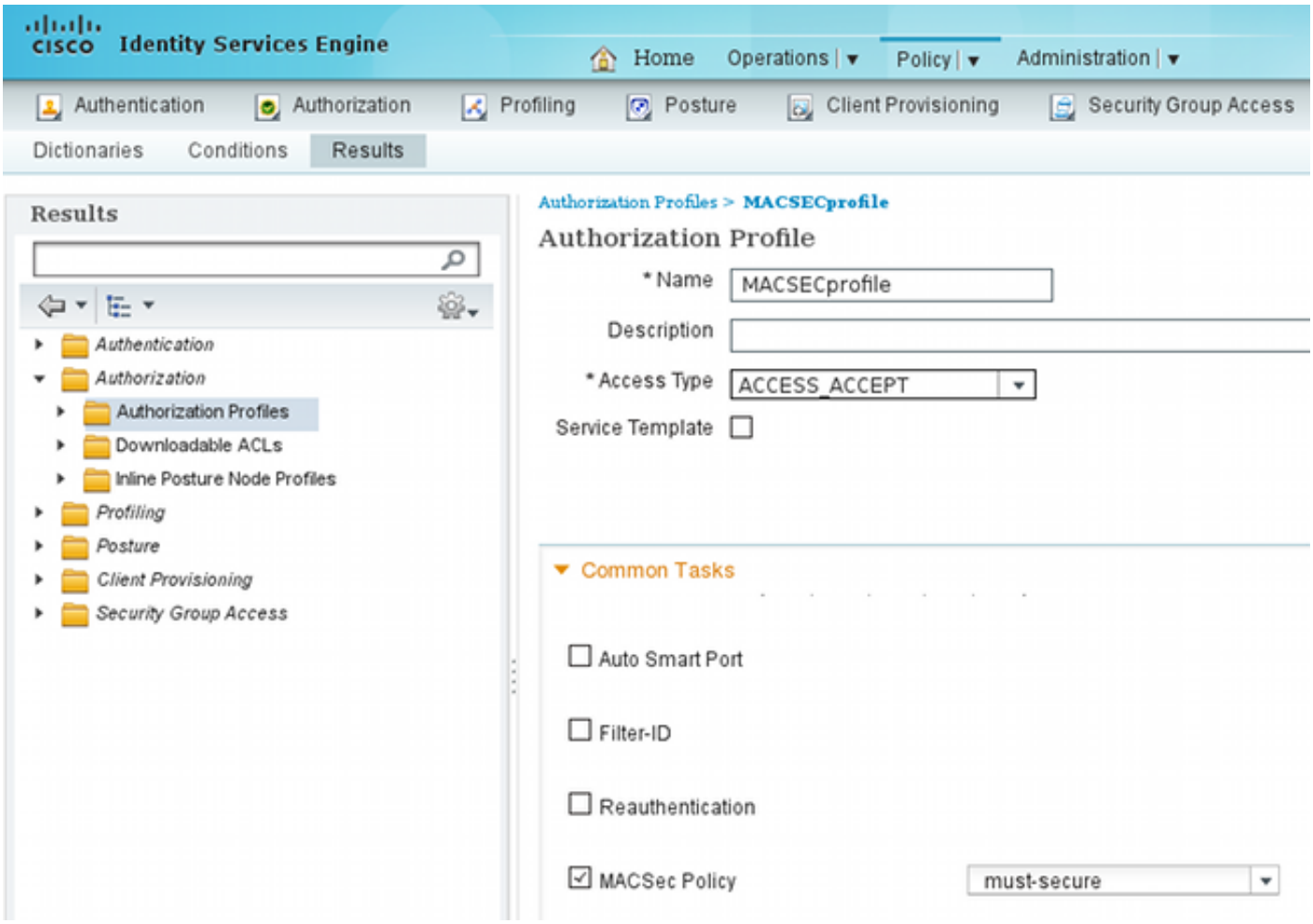
The default authentication rule can be used (for users defined locally on ISE).

Choose **Administration > Identity Management > Users** in order to define the user "cisco" locally.

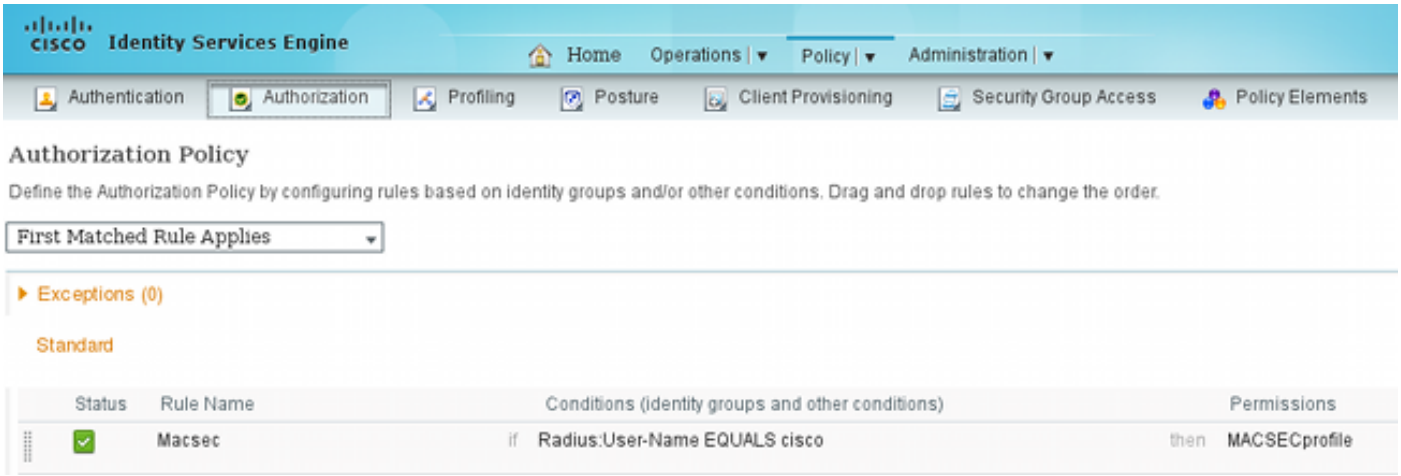


The Authorization profile might include encryption policies. As shown in this example, choose **Policy > Results > Authorization Profiles** in order to view the information ISE returns to the

switch that link encryption is mandatory. Also, the VLAN number (10) has been configured.



Choose **Policy > Authorization** in order to use the authorization profile in the authorization rule. This example returns the configured profile for user "cisco". If 802.1x is successful, ISE returns Radius-Accept to the switch with Cisco AVPair linksec-policy=must-secure. That attribute forces the switch to initiate an MKA session. If that session fails, 802.1x authorization on the switch also fails.



Switch

Typical 802.1x port settings include (top portion shown):

```
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
```

The local MKA policy is created and applied to the interface. Also, MACsec is enabled on the interface.

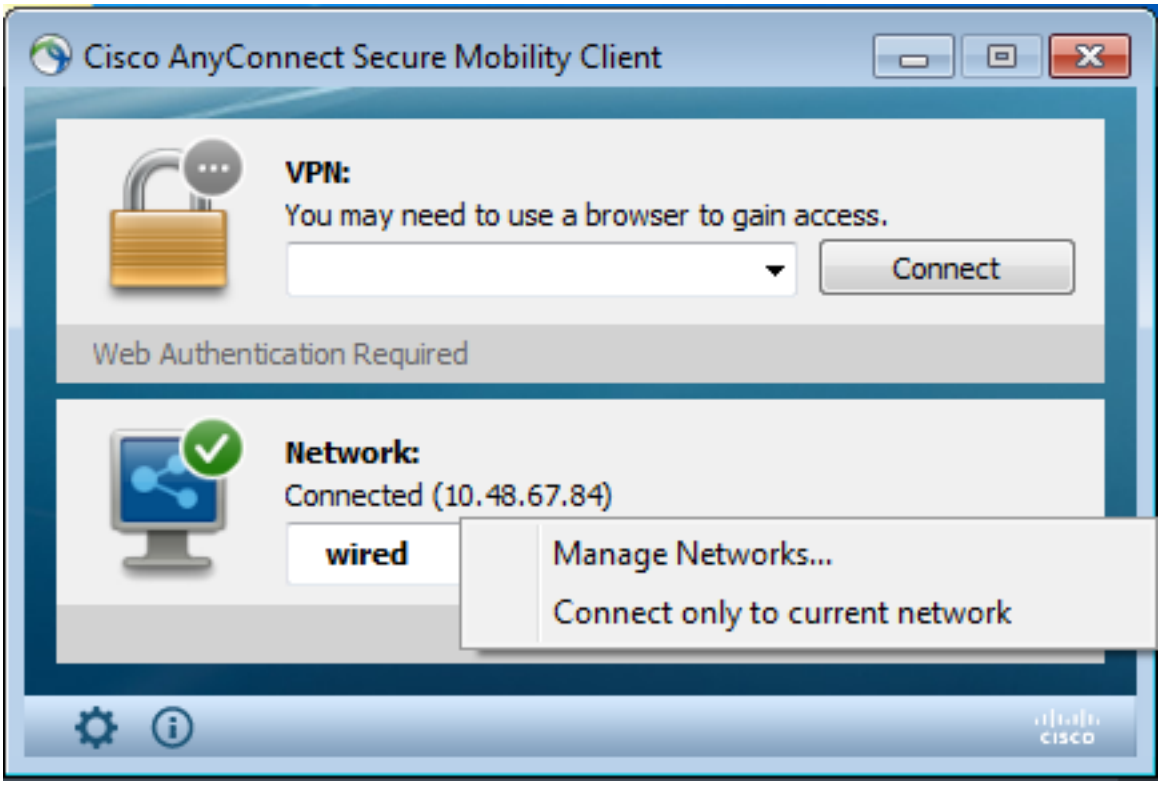
```
mka policy mka-policy
 replay-protection window-size 5000

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

The local MKA policy allows you to configure detailed settings which cannot be pushed from the ISE. The local MKA policy is optional.

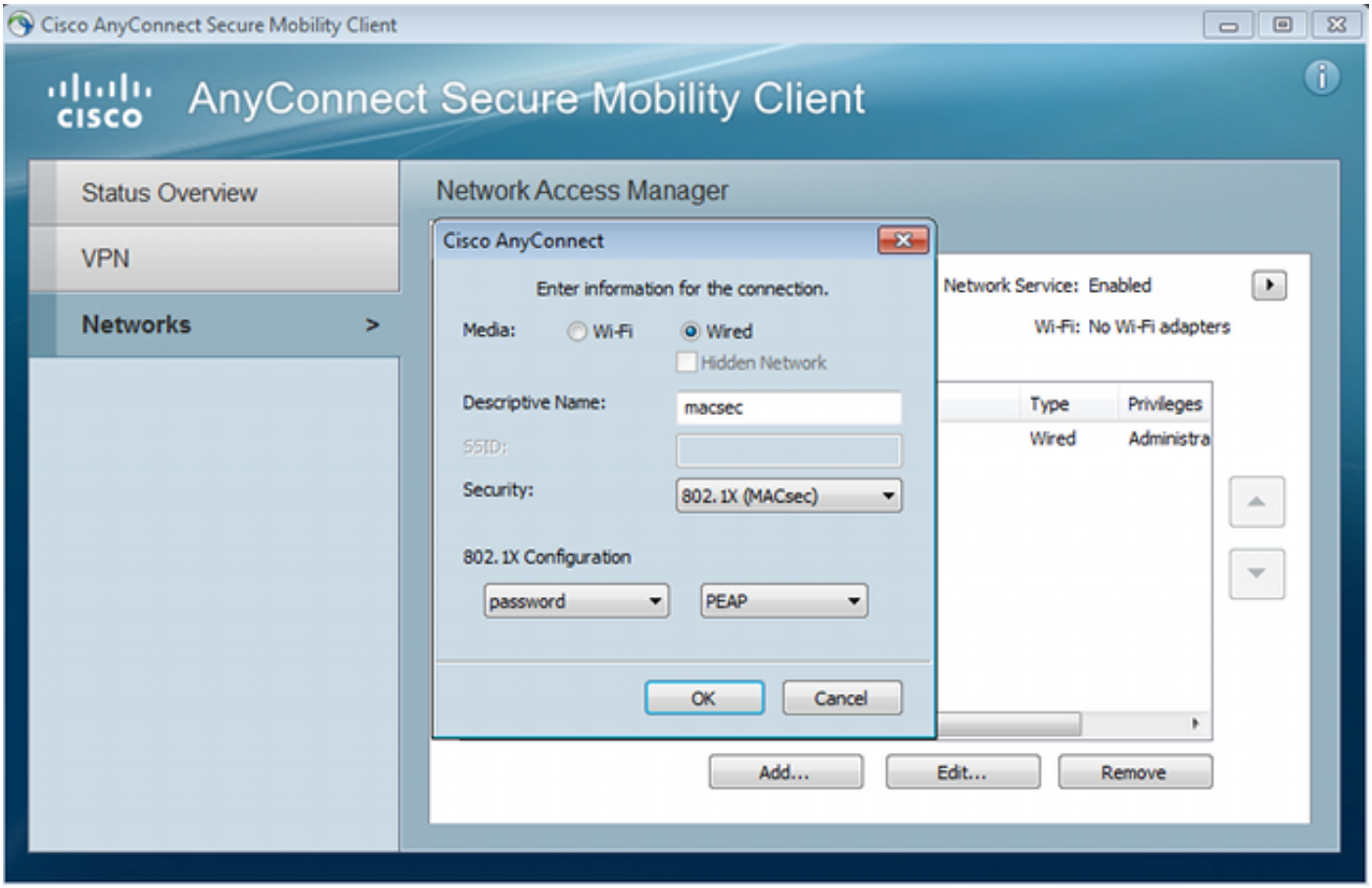
AnyConnect NAM

The profile for the 802.1x supplicant can be configured manually or pushed via Cisco ASA. The next steps present a manual configuration.

In order to manage NAM profiles:



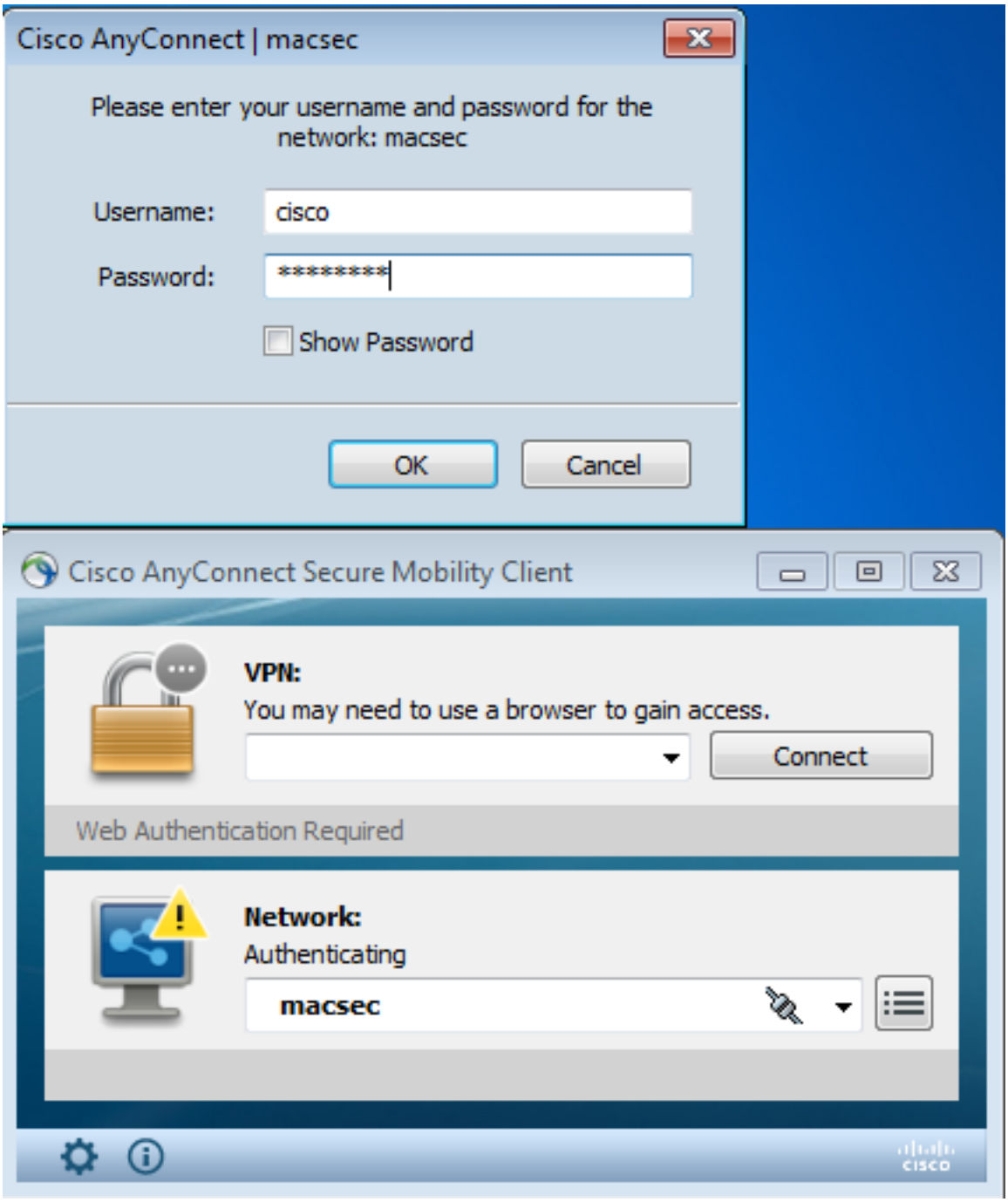
Add a new 802.1x profile with MACsec. For 802.1x, Protected Extensible Authentication Protocol (PEAP) is used (configured user "cisco" on ISE):



Verify

Use this section to confirm that your configuration works properly.

The AnyConnect NAM configured for EAP-PEAP requires correct credentials.



The session on the switch should be authenticated and authorized. The security status should be "Secured":

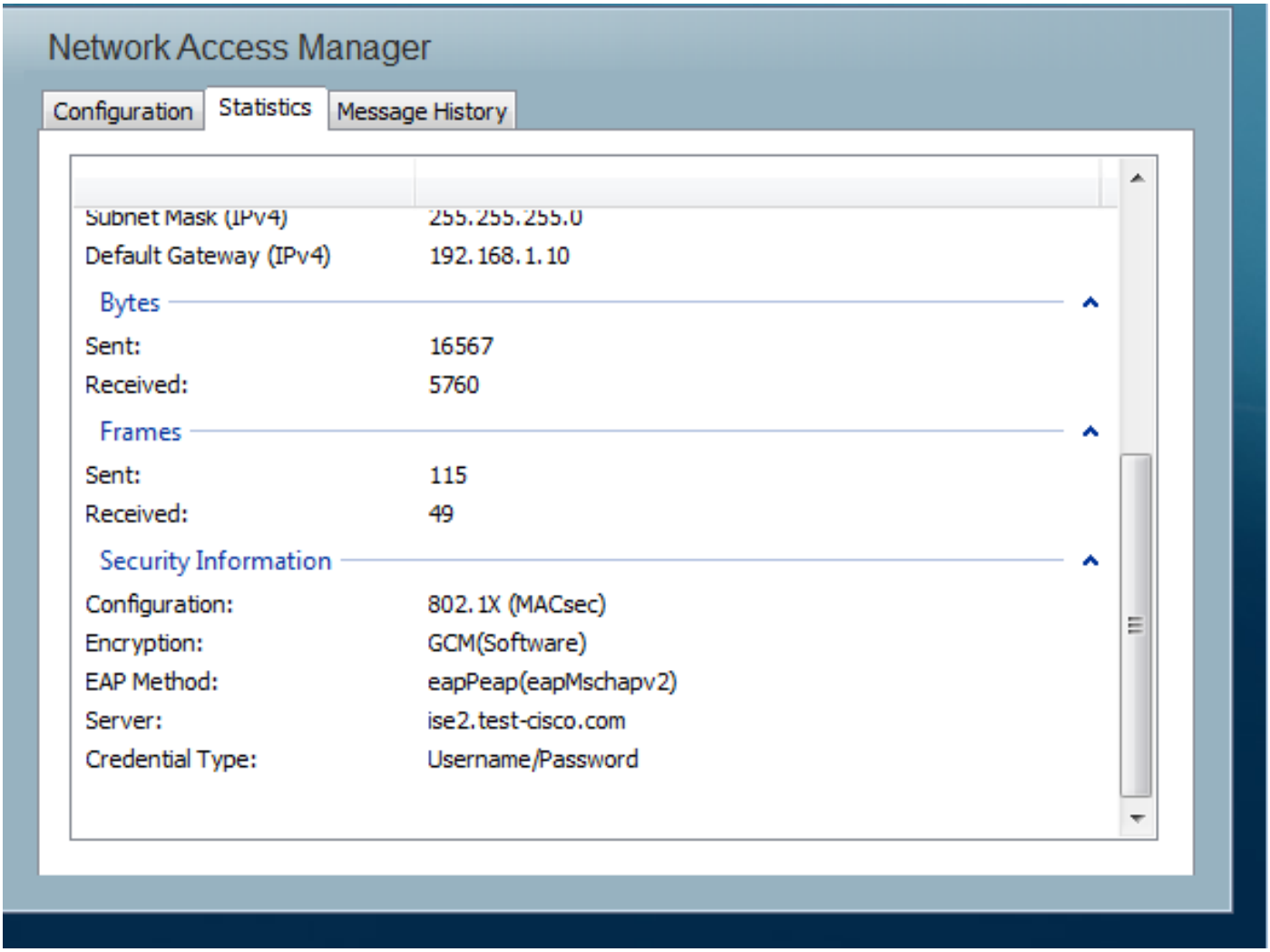
```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Must 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
```

The MACsec statistics on the switch provide the details in regards to local policy setting, secure channel identifiers (SCIs) for received/sent traffic, and also port statistics and errors.

```
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
```

On AnyConnect, the statistics indicate encryption usage and packet statistics.



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Debugs for a Working Scenario

Enable debugs on the switch (some output has been omitted for clarity).

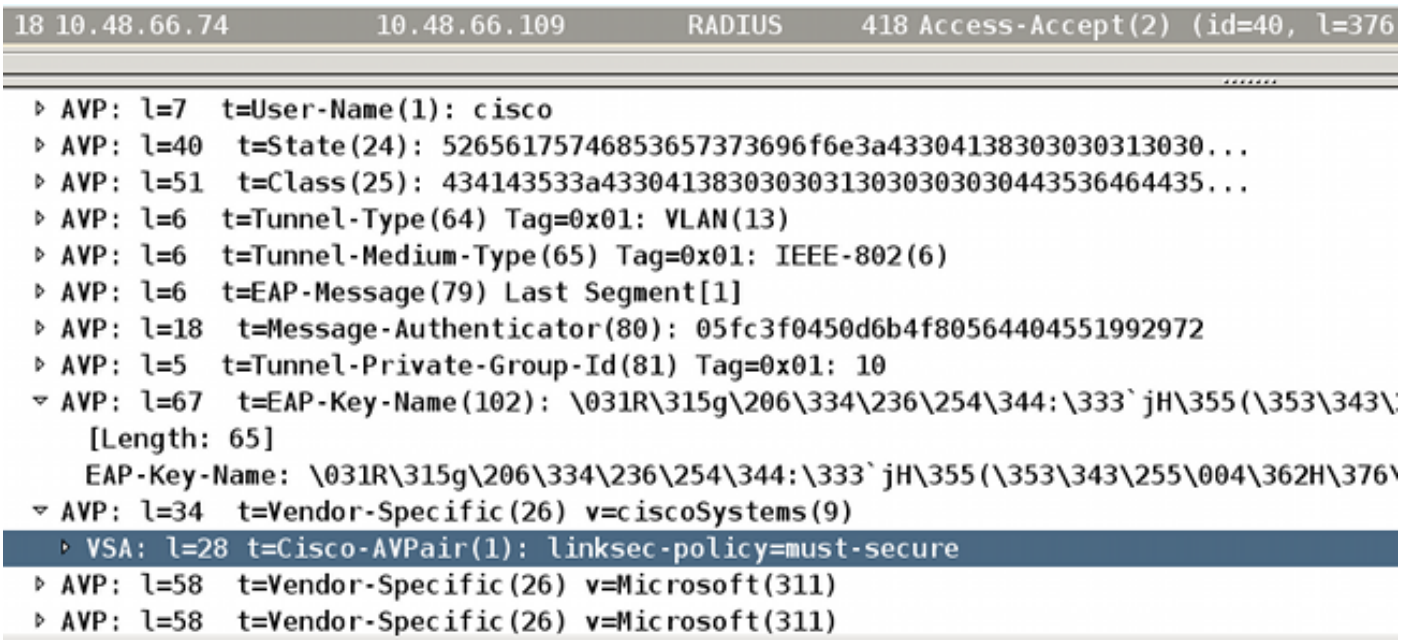
```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

After an 802.1x session is established, multiple EAP packets are exchanged over EAPOL. The last successful response from ISE (EAP success) carried inside Radius-Acccept also includes several Radius attributes.

```
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 is used for the MKA session. The linksec-policy forces the switch to use MACsec (authorization fails if that is not complete). Those attributes can be also verified in the packet captures.



Authentication is successful.

```
%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
```

The switch applies the attributes (these include an optional VLAN number which has also been sent).

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

The switch then starts the MKA session when it sends and receives EAPOL packets.

```
%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
```

After 4 packet exchange secure identifiers are created along with the Receive (RX) security association.

```
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
```

The session is finished and the Transmit (TX) security association is added.

```
%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/
```

The policy "must-secure" is matched and authorization is successful.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

Every 2 seconds MKA Hello packets are exchanged in order to ensure that all participants are alive.

```
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
```

Debugs for a Failing Scenario

When the supplicant is not configured for MKA and the ISE requests encryption after a successful 802.1x authentication:

```
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
```

The switch tries to initiate an MKA session when it sends 5 EAPOL packets.

```
%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
```

And finally times out and fails authorization.

```
 %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
```

The 802.1x session reports successful authentication, but failed authorization.

```
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
```

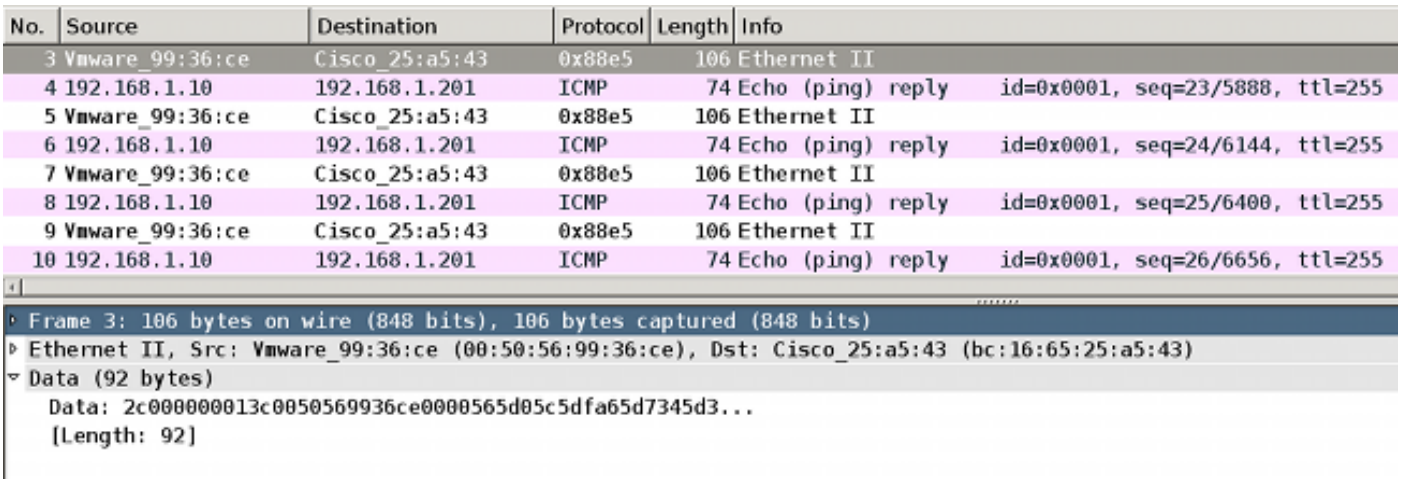
Data traffic will be blocked.

Packet Captures

When traffic is captured on the supplicant site 4 Internet Control Message Protocol (ICMP) echo requests/replies are sent and received, there will be:

- 4 encrypted ICMP echo requests sent to the switch (88e5 is reserved for 802.1AE)
- 4 decrypted ICMP echo replies received

That is because of how AnyConnect hooks on Windows API (before libpcap when packets are sent and before libpcap when packets are received):



> **Note**: The ability to sniff MKA or 802.1AE traffic on the switch with features such as Switched Port Analyzer (SPAN) or Embedded Packet Capture (EPC) is not supported.

MACsec and 802.1x Modes

Not all 802.1x modes are supported for MACsec.

The *Cisco TrustSec 3.0 How-To Guide: Introduction to MACsec and NDAC* states that:

- **Single-Host Mode**: **MACsec is fully supported** in single-host mode. In this mode, only a single MAC or IP address can be authenticated and secured with MACsec. If a different MAC address is detected on the port after an endpoint has authenticated, a security violation will be triggered on the port.
- **Multi-Domain Authentication (MDA) Mode**: In this mode, one endpoint may be on the data domain and another endpoint may be on the voice domain. **MACsec is fully supported in MDA mode**. If both endpoints are MACsec-capable, each will be secured by its own independent MACsec session. If only one endpoint is MACsec-capable, that endpoint can be secured while the other endpoint sends traffic in the clear.
- **Multi-Authentication Mode**: In this mode, a virtually unlimited number of endpoints may be authenticated to a single switch port. **MACsec is not supported in this mode.**
- **Multi-Host Mode**: While MACsec usage in this mode is technically possible, **it is not recommended**. In Multi-Host Mode, the first endpoint on the port authenticates, and then any additional endpoints will be permitted onto the network via the first authorization. MACsec would work with the first connected host, but no other endpoint's traffic would actually pass, since it would not be encrypted traffic.

Related Information

- **Cisco TrustSec Configuration Guide for 3750**
- **Cisco TrustSec Configuration Guide for ASA 9.1**
- **Identity-Based Networking Services: MAC Security**
- **TrustSec Cloud with 802.1x MACsec on Catalyst 3750X Series Switch Configuration Example**
- **ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide**
- **Cisco TrustSec Deployment and RoadMap**
- **Technical Support & Documentation - Cisco Systems**