Probleemoplossing DotX op Catalyst 9000 Series Switches

Inhoud

Inleiding

Dit document beschrijft hoe 802.1x-netwerktoegangscontrole (NAC) op Catalyst 9000 Series switches moet worden geconfigureerd, gevalideerd en probleemoplossing kan worden uitgevoerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- Catalyst 9000 Series switches
- Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x en hoger
- ISE-VM-K9 versie 3.0.0.458

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Opmerking: raadpleeg de juiste configuratiehandleiding voor de opdrachten die worden gebruikt om deze functies op andere Cisco-platforms in te schakelen.

Achtergrondinformatie

De 802.1x-standaard definieert een op een clientserver gebaseerd toegangscontrole- en verificatieprotocol dat verhindert dat onbevoegde clients met een LAN verbinden via openbaar toegankelijke poorten, tenzij deze op de juiste manier zijn geverifieerd. De verificatieserver verifieert elke client die is verbonden met een switch voordat deze diensten beschikbaar stelt die door de switch of het LAN worden aangeboden.

802.1x-verificatie omvat 3 verschillende onderdelen:

Supplicant - client die aanmeldingsgegevens voor verificatie indient
Authenticator - Het netwerkapparaat dat netwerkconnectiviteit tussen de client en het netwerk biedt en netwerkverkeer kan toestaan of blokkeren.
Verificatieserver — Server die verzoeken om netwerktoegang kan ontvangen en beantwoorden, vertelt de verificateur of de verbinding kan worden toegestaan en verschillende andere instellingen die van toepassing zijn op de verificatiesessie.

Het beoogde publiek voor dit document is ingenieurs en ondersteunend personeel dat niet noodzakelijk op beveiliging is gericht. Raadpleeg de juiste configuratiehandleiding voor meer informatie over 802.1x-poortgebaseerde verificatie en componenten zoals ISE.

Opmerking: raadpleeg de juiste configuratiehandleiding voor uw specifieke platform en de versie van de code voor de meest accurate 802.1x-verificatieconfiguratie.

Basisconfiguratie

In dit gedeelte wordt de basisconfiguratie beschreven die vereist is voor de implementatie van 802.1x-poortgebaseerde verificatie. Aanvullende uitleg over de functies vindt u in het tabblad Toevoegen van dit document. Er zijn kleine variaties in configuratienormen van versie aan versie. Bevestig uw configuratie aan de hand van uw huidige versieconfiguratiegids.

Verificatie, autorisatie en account (AAA) moeten zijn ingeschakeld voordat 802.1x-postgebaseerde verificatie kan worden geconfigureerd, en er moet een methodelijst worden opgesteld.

- De methodelijsten beschrijven de opeenvolging en de authentificatiemethode die moet worden gevraagd om een gebruiker voor authentiek te verklaren.
- 802.1x moet ook wereldwijd worden ingeschakeld.

<#root>

```
C9300>

enable

C9300#

configure terminal

C9300(config)#

aaa new-model

C9300(config)#

aaa authentication dot1x default group radius

C9300(config)#

dot1x system-auth-control
```

Een RADIUS-server op de switch definiëren

<#root>

```
C9300(config)#

radius server RADIUS_SERVER_NAME

C9300(config-radius-server)#

address ipv4 10.0.1.12

C9300(config-radius-server)#

key rad123

C9300(config-radius-server)#
```

```
exit
```

Schakel 802.1x in op de clientinterface.

```
<#root>
C9300(config)#
interface TenGigabitEthernet 1/0/4

C9300(config-if)#
switchport mode access

C9300(config-if)#
authentication port-control auto

C9300(config-if)#
dot1x pae authenticator

C9300(config-if)#
end
```

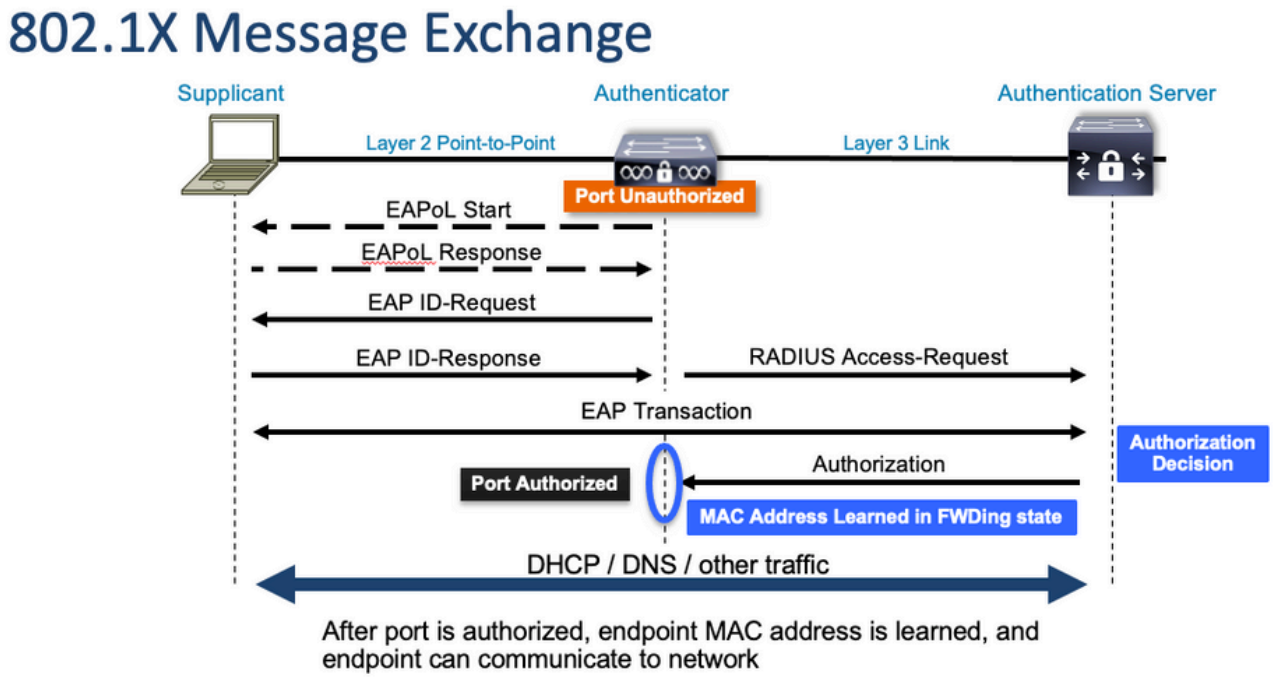
Controleer de configuratie en bewerkingen

Deze paragraaf geeft achtergrondinformatie over 801.1x en hoe de configuratie en de bewerkingen moeten worden geverifieerd.

Inleiding tot 802.1x

802.1x omvat twee verschillende typen verkeer: Client to Authenticator (point-to-point) verkeer via EAPoL (Extensible Authentication Protocol over LAN) en Authenticator aan Verificatieserververkeer dat via RADIUS is ingesloten.

Dit diagram geeft een gegevensstroom weer voor een eenvoudige dot1x-transactie



De Authenticator (switch) en de Verificatieserver (ISE, bijvoorbeeld) worden vaak gescheiden door Layer 3. RADIUS-verkeer wordt via het netwerk tussen de verificator en de server gerouteerd. EAPoL-verkeer wordt uitgewisseld via de directe koppeling tussen aanvrager (client) en verificator.

Merk op dat MAC learning plaatsvindt na authenticatie en autorisatie.

Hier zijn een paar vragen in gedachten te houden als u een probleem benadert dat 802.1x betreft:

- Is het correct geconfigureerd?
- Is de verificatieserver bereikbaar?
- Wat is de status van Verificatiebeheer?
- Zijn er problemen met de pakketleverbaarheid tussen client en verificator of tussen verificator en verificatieserver?

Configuratie

Sommige configuraties variëren enigszins tussen de belangrijkste releases. Raadpleeg de relevante configuratiegids voor platform-/codespecifieke richtlijnen.

AAA moet worden geconfigureerd om 802.1x poortgebaseerde verificatie te gebruiken.

- Er moet een lijst met verificatiemethoden worden vastgesteld voor "dot1x". Dit vertegenwoordigt een veelvoorkomende AAA-configuratie waarin 802.1X is ingeschakeld.

<#root>

C9300#

show running-config | section aaa

aaa new-model

<-- This enables AAA.

```
aaa group server radius ISEGROUP

<-- This block establishes a RADIUS server group named "ISEGROUP".
 server name DOT1x

 ip radius source-interface Vlan1
aaa authentication dot1x default group ISEGROUP

<-- This line establishes the method list for 802.1X authentication. Group ISEGROUP is be used.
aaa authorization network default group ISEGROUP

aaa accounting update newinfo periodic 2880
aaa accounting dot1x default start-stop group ISEGROUP

C9300#

show running-config | section radius

aaa group server radius ISEGROUP
 server name DOT1x
 ip radius source-interface Vlan1

<-- Notice 'ip radius source-interface' configuration exists in both global configuration and the aaa se

ip radius source-interface Vlan1
radius server DOT1x
 address ipv4 10.122.141.228 auth-port 1812 acct-port 1813

<-- 1812 and 1813 are default auth-port and acct-port, respectively.

 key secretKey
```

Dit is een voorbeeldinterfaceconfiguratie waarin 802.1x is ingeschakeld. MAB (MAC Authenticatie Bypass) is een veelgebruikte back-upmethode voor het verifiëren van clients die geen dot1x-applicaties ondersteunen.

<#root>

```
C9300#

show running-config interface te1/0/4

Building configuration...

Current configuration : 148 bytes
!
interface TenGigabitEthernet1/0/4
 switchport access vlan 50
 switchport mode access
 authentication order dot1x mab

<-- Specifies authentication order, dot1x and then mab


 authentication priority dot1x mab

<-- Specifies authentication priority, dot1x and then mab


 authentication port-control auto
```

```
<-- Enables 802.1x dynamic authentication on the port

 mab
<-- Enables MAB
 dot1x pae authenticator
<-- Puts interface into "authenticator" mode.
end
```

Bepaal of een MAC-adres wordt geleerd op de interface met "show mac address-table interface <interface>". De interface leert alleen een MAC-adres wanneer deze met succes wordt geverifieerd.

```
<#root>
C9300#
show mac address-table interface te1/0/4

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  50    0800.2766.efc7    STATIC      Te1/0/4
<-- The "type" is STATIC and the MAC persists until the authentication session is cleared.
Total Mac Addresses for this criterion: 1
```

Verificatiesessie

Laat zien dat er opdrachten beschikbaar zijn voor validatie van 802.1x verificatie.

Gebruik "toon verificatiesessies" of "toon verificatiesessies <interface>" om informatie weer te geven over de huidige verificatiesessies. In dit voorbeeld, slechts heeft Te1/0/4 een actieve authentificatiesessie gevestigd.

```
<#root>
C9300#
show authentication sessions interface te1/0/4

Interface               MAC Address    Method  Domain  Status Fg  Session ID
---------------------------------------------------------------------------------------
Te1/0/4                 0800.2766.efc7 dot1x   DATA    Auth        13A37A0A0000011DC85C34C5
<-- "Method" and "Domain" in this example are dot1x and DATA, respectfully. Multi-domain authentication
```

```
Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker

Runnable methods list:
  Handle  Priority  Name
      13         5  dot1xSup
       1         5  dot1x
       2        10  webauth
      14        15  mab
```

"Toon authenticatiesessies interface <interface> details" geeft aanvullende informatie over een specifieke interface authenticatie sessie.

<#root>

```
C9300#

show authentication session interface te1/0/4 details

            Interface:  TenGigabitEthernet1/0/4
               IIF-ID:  0x14D66776
          MAC Address:  0800.2766.efc7
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  alice
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
  Acct update timeout:  172800s (local), Remaining: 152363s
    Common Session ID:  13A37A0A0000011DC85C34C5
      Acct Session ID:  0x00000002
               Handle:  0xe8000015
       Current Policy:  POLICY_Te1/0/4

<-- If a post-authentication ACL is applied, it is listed here.



Local Policies:
    Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
        dot1x           Authc Success
```

```
<-- This example shows a successful 801.1x authentication session.
```

Als de verificatie op een interface is ingeschakeld maar er nog geen actieve sessie is, wordt de lijst met instelbare methoden weergegeven. Er wordt ook "Geen sessies overeenkomen met de meegeleverde criteria" weergegeven.

```
<#root>

C9300#

show authentication sessions interface te1/0/5

No sessions match supplied criteria.

Runnable methods list:
  Handle  Priority  Name
      13         5  dot1xSup
       1         5  dot1x
       2        10  webauth
      14        15  mab
```

Als geen verificatie is ingeschakeld op de interface, wordt er geen aanwezigheid van Autoream gedetecteerd op de interface. Er wordt ook "Geen sessies overeenkomen met de meegeleverde criteria" weergegeven.

```
<#root>

C9300#

show authentication sessions interface te1/0/6


No sessions match supplied criteria.
No Auth Manager presence on this interface
```

Bereikbaarheid naar verificatieserver

De bereikbaarheid van de verificatieserver is een voorwaarde voor het succes van de 802.1x-verificatie.

Gebruik "ping <server_ip>" voor een snelle test van bereikbaarheid. Zorg ervoor dat uw ping afkomstig is van de RADIUS-broninterface.

```
<#root>

C9300#

ping 10.122.141.228 source vlan 1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.122.141.228, timeout is 2 seconds:
Packet sent with a source address of 10.122.163.19
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

De opdracht "AAA-servers tonen" identificeert de serverstatus en verschaft statistieken over transacties met alle geconfigureerde AAA-servers.

<#root>

C9300#

show aaa servers

```
RADIUS: id 3, priority 1, host 10.122.141.228, auth-port 1812, acct-port 1813, hostname DOT1x <-- Speci
     State: current UP, duration 84329s, previous duration 0s <-- Current State
     Dead: total time 0s, count 1
     Platform State from SMD: current UP, duration 24024s, previous duration 0s
     SMD Platform Dead: total time 0s, count 45
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP
     Platform State from WNCD (6) : current UP
     Platform State from WNCD (7) : current UP
     Platform State from WNCD (8) : current UP, duration 0s, previous duration 0s
     Platform Dead: total time 0s, count 0UP
     Quarantined: No

 Authen: request 510, timeouts 468, failover 0, retransmission 351   <-- Authentication Statistics

             Response: accept 2, reject 2, challenge 38
             Response: unexpected 0, server error 0, incorrect 12, time 21ms
             Transaction: success 42, failure 117
             Throttled: transaction 0, timeout 0, failure 0
             Malformed responses: 0
             Bad authenticators: 0
             Dot1x transactions:
             Response: total responses: 42, avg response time: 21ms
             Transaction: timeouts 114, failover 0
             Transaction: total 118, success 2, failure 116
             MAC auth transactions:
             Response: total responses: 0, avg response time: 0ms
             Transaction: timeouts 0, failover 0
             Transaction: total 0, success 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
             Malformed responses: 0
             Bad authenticators: 0
             MAC author transactions:
             Response: total responses: 0, avg response time: 0ms
             Transaction: timeouts 0, failover 0
```

```
        Transaction: total 0, success 0, failure 0
    Account: request 3, timeouts 0, failover 0, retransmission 0
        Request: start 2, interim 0, stop 1
        Response: start 2, interim 0, stop 1
        Response: unexpected 0, server error 0, incorrect 0, time 11ms
        Transaction: success 3, failure 0
        Throttled: transaction 0, timeout 0, failure 0
        Malformed responses: 0
        Bad authenticators: 0
    Elapsed time since counters last cleared: 1d3h4m
    Estimated Outstanding Access Transactions: 0
    Estimated Outstanding Accounting Transactions: 0
    Estimated Throttled Access Transactions: 0
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Transactions: access 0, accounting 0
    Consecutive Response Failures: total 115
        SMD Platform : max 113, current 0 total 113
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 2, current 2 total 2
    Consecutive Timeouts: total 466
        SMD Platform : max 455, current 0 total 455
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 11, current 11 total 11
    Requests per minute past 24 hours:
        high - 23 hours, 25 minutes ago: 4
        low  - 3 hours, 4 minutes ago: 0
        average: 0
```

Gebruik het hulpprogramma "Test Aa" om de bereikbaarheid van de switch naar de verificatieserver te bevestigen. Merk op dat deze voorziening wordt afgekeurd en niet voor onbepaalde tijd beschikbaar is.

```
<#root>

C9300#

debug radius <-- Classic Cisco IOS debugs are only useful in certain scenarios. See "Cisco IOS XE Debugs


C9300#

test aaa group ISE username password new-code <-- This sends a RADIUS test probe to the identified serve


User rejected

<-- This means that the RADIUS server received our test probe, but rejected our user. We can conclude th


*Jul 16 21:05:57.632: %PARSER-5-HIDDEN: Warning!!! ' test platform-aaa group server-group ISE user-name
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000):Orig. component type = Invalid
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IP: 10.122.161.63
*Jul 16 21:05:57.644: vrfid: [65535] ipv6 tableid : [0]
*Jul 16 21:05:57.644: idb is NULL
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IPv6: ::
*Jul 16 21:05:57.644: RADIUS(00000000): sending
*Jul 16 21:05:57.644: RADIUS/DECODE(00000000): There is no General DB. Want server details may not be s
*Jul 16 21:05:57.644: RADIUS(00000000): Send Access-Request to 10.122.141.199:1812 id 1645/8, len 50
```

```
<-- Sending Access-Request to RADIUS server


RADIUS: authenticator 3B 65 96 37 63 E3 32 41 - 3A 93 63 B6 6B 6A 5C 68
*Jul 16 21:05:57.644: RADIUS: User-Password [2] 18 *
*Jul 16 21:05:57.644: RADIUS: User-Name [1] 6 "username"
*Jul 16 21:05:57.644: RADIUS: NAS-IP-Address [4] 6 10.122.161.63
*Jul 16 21:05:57.644: RADIUS(00000000): Sending a IPv4 Radius Packet
*Jul 16 21:05:57.644: RADIUS(00000000): Started 5 sec timeout
*Jul 16 21:05:57.669: RADIUS: Received from id 1645/8 10.122.141.199:1812, Access-Reject, len 20

<-- Receiving the Access-Reject from RADIUS server


RADIUS: authenticator 1A 11 32 19 12 F9 C3 CC - 6A 83 54 DF 0F DB 00 B8
*Jul 16 21:05:57.670: RADIUS/DECODE(00000000): There is no General DB. Reply server details may not be
*Jul 16 21:05:57.670: RADIUS(00000000): Received from id 1645/8
```

Problemen oplossen

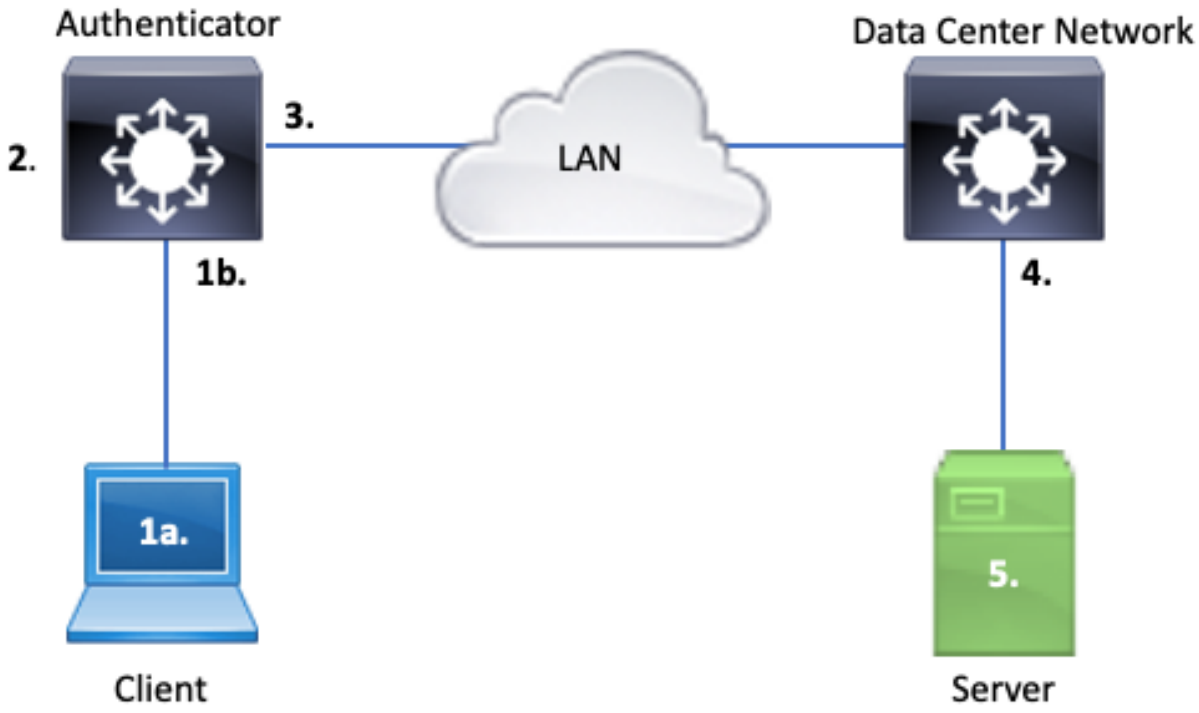
Deze sectie geeft richtlijnen voor het oplossen van de meeste 802.1x-problemen op een Catalyst switch.

Methodologie

Benader problemen met 802.1x en authenticatie methodisch voor de beste resultaten. Een aantal goede vragen om te beantwoorden zijn:

- Is het probleem geïsoleerd voor één enkele switch? Een enkele haven? Een enkele klant type?
- Is de configuratie gevalideerd? Is de verificatieserver bereikbaar?
- Komt het probleem elke keer voor of is het intermitterend? Komt het alleen voor bij een nieuwe authenticatie of wijziging van de autorisatie?

Controleer een enkele mislukte transactie van begin tot eind als er problemen blijven bestaan nadat het voor de hand liggende is uitgesloten. De beste, meest complete dataset voor onderzoek van een 802.1x-transactie van client naar server bevat:



1 bis. Opname op client en/of

1 ter. Op de toegangsinterface waar de client verbinding maakt

Dit referentiepunt is van cruciaal belang om ons inzicht te geven in de EAPoL-pakketten die worden uitgewisseld tussen de toegangshaven waar dot1x is ingeschakeld en de client. SPAN is het meest betrouwbare gereedschap voor het weergeven van verkeer tussen client en verificator.

2. Debugs op authenticator

Debugs laten ons toe de transactie over de authenticator te traceren.

- De verificator moet de ontvangen EAPoL-pakketten doorgeven en het verkeer met eenmalige RADIUS-versleuteling genereren dat bestemd is voor de verificatieserver.
- Zorg ervoor dat de juiste debug-niveaus zijn ingesteld voor een maximale effectiviteit.

3. Opname naast de verificator

Deze opname laat ons toe het gesprek te zien tussen Authenticator en Verificatieserver.

- Deze opname geeft de gehele conversatie nauwkeurig weer vanuit het perspectief van de Authenticator.
- Wanneer u de opname in punt 4 koppelt, kunt u bepalen of er verlies is tussen de verificatieserver en de verificator.

4. Opname naast de verificatieserver

Deze opname is een metgezel met de opname in punt 3.

- Deze opname biedt de gehele conversatie vanuit het perspectief van de verificatieserver.
- Wanneer u de opname in punt 3 koppelt, kunt u bepalen of er verlies is tussen Authenticator en Verificatieserver.

5. Opnemen, debuggen, inloggen op verificatieserver

Het laatste stukje van de puzzel, server debugs vertellen ons wat de server weet over onze transactie.

- Met deze gegevens van begin tot eind kan een netwerkingenieur bepalen waar de transactie breekt en componenten uitsluiten die niet aan het probleem bijdragen.

Voorbeeldsymptomen

Deze paragraaf geeft een lijst van gebruikelijke symptomen en probleemscenario's.

- Geen respons van client

Als het EAPoL-verkeer dat door de switch wordt gegenereerd geen respons uitlokt, wordt deze syslog weergegeven:

```
Aug 23 11:23:46.387 EST: %DOT1X-5-FAIL: Switch 1 R0/0: sessmgrd: Authentication failed for client (aaaa
```

De oorzaakcode "Geen antwoord van klant" geeft aan dat de switch het dot1x-proces is gestart, maar er is binnen de tijdspanne geen antwoord ontvangen van de klant.
Dit betekent dat de client het door de switch verzonden authenticatieverkeer niet heeft ontvangen of begrepen, of dat de reactie van de client niet is ontvangen op de switch poort.

- Client verlaat sessie

Als een verificatiesessie is gestart maar niet is voltooid, meldt de verificatieserver (bijvoorbeeld ISE) dat de client een sessie is gestart, maar de sessie is afgebroken voordat de sessie is voltooid.
Vaak betekent dit dat het authenticatieproces slechts gedeeltelijk kan worden voltooid.

Zorg ervoor dat de gehele switch tussen de verificatieserver en de verificatieserver end-to-end wordt aangeboden en door de verificatieserver correct wordt geïnterpreteerd.

Als RADIUS-verkeer op het netwerk verloren gaat of op een manier wordt geleverd waarop het niet juist kan worden geassembleerd, is de transactie onvolledig en probeert de client opnieuw verificatie. De server meldt op zijn beurt dat de client de sessie heeft afgebroken.

- MAB-client faalt DHCP/Falls Terug naar APIPA

MAC-verificatie-omleiding (MAB) maakt verificatie op basis van MAC-adres mogelijk. Klanten die geen software ondersteunen die een aanvraag doet, authenticeren vaak via MAB.

Als MAB wordt gebruikt als een fallback methode voor verificatie terwijl dot1x de voorkeurs- en initiële methode is die op een switch poort wordt uitgevoerd, kan een scenario mogelijk resulteren waar de client niet in staat is om DHCP te voltooien.

Het probleem komt neer op de volgorde van de werkzaamheden. Tijdens de dot1x-uitvoering verbruikt de switch-poort andere pakketten dan EAPoL totdat de verificatie is voltooid of de dot1x-tijd is verlopen. De client probeert echter onmiddellijk een IP-adres te krijgen en zendt de DHCP-detectieberichten uit. Deze ontdekken berichten worden verbruikt door de switch poort totdat dot1x de ingestelde time-out waarden overschrijdt en MAB kan draaien. Als de client DHCP-time-out periode minder is dan de dot1x-time-out periode, mislukt DHCP en valt de client terug naar APIPA of wat zijn fall-back strategie dicteert.

Dit probleem wordt op meerdere manieren voorkomen. Kies MAB op interfaces waar MAB geverifieerde klanten verbinding maken. Als dot1x eerst moet worden uitgevoerd, moet u rekening houden met het DHCP-gedrag van de client en de tijdelijke waarden correct aanpassen.

Wees voorzichtig met het gedrag van de klant als dot1x en MAB worden gebruikt. Een geldige configuratie kan leiden tot een technisch probleem, zoals hierboven beschreven.

Platformspecifieke hulpprogramma's

In deze sectie worden veel platformspecifieke hulpprogramma's beschreven die beschikbaar zijn op de Catalyst 9000-reeks switches die handig zijn om problemen met dot1x op te lossen.

- Switch Port Analyzer (SPAN)

Met SPAN kan de gebruiker verkeer van een of meer poorten naar een bestemmingshaven spiegelen voor opname en analyse. Local SPAN is het meest 'betrouwbare' opnameprogramma.

Zie deze configuratiehandleiding voor meer informatie over configuratie en implementatie:

Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300) configureren voor SPAN en RSPAN

- Ingesloten pakketvastlegging (EPC)

EPC maakt gebruik van CPU- en geheugenbronnen om on-board lokale pakketopnamemogelijkheden te bieden.

Er zijn beperkingen aan EPC die invloed hebben op de effectiviteit ervan voor het onderzoeken van bepaalde problemen. De EPC heeft een snelheidsbeperking van 1000 pakketten per seconde. EPC kan ook niet op betrouwbare wijze CPU-geïnjecteerde pakketten opnemen bij het verlaten van fysieke interfaces. Dit is belangrijk wanneer de focus ligt op de RADIUS-transactie tussen de verificator-switch en de verificatieserver. Vaak overschrijdt de snelheid van het verkeer op de interface met de server de 1000 pakketten per seconde. Een EPC aan het begin van een interface met de server kan geen verkeer opnemen dat gegenereerd is door de authenticator switch.

Gebruik tweerichtingstoegangslijsten om de EPC te filteren om impact met het 1000-pakket per seconde te voorkomen. Als u geïnteresseerd bent in het RADIUS-verkeer tussen verificator en server, richt u zich op verkeer tussen het broninterfaceadres van de verificator RADIUS en het adres van de server.

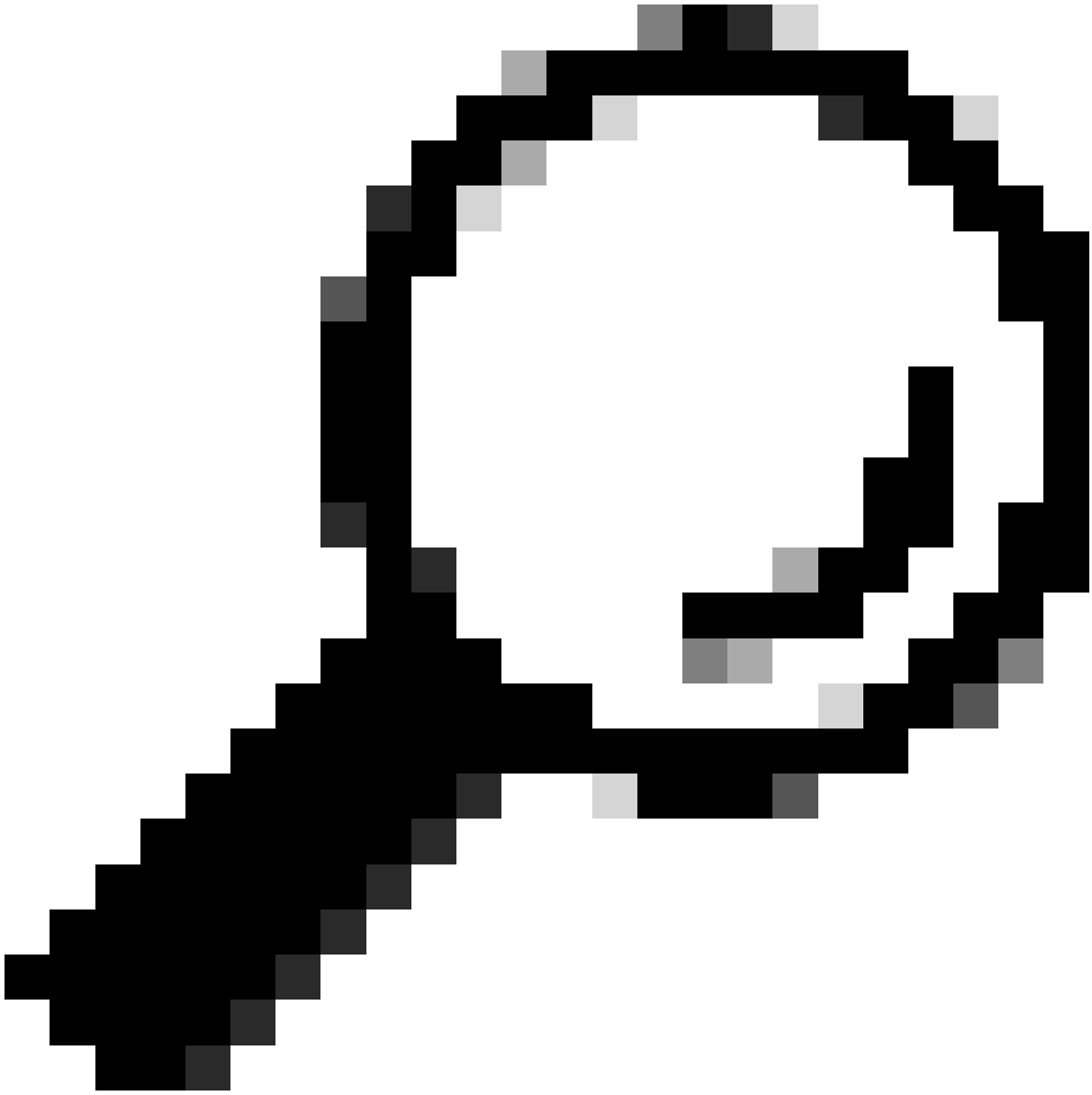
Als het volgende upstream apparaat naar de verificatieserver een Catalyst-switch is, gebruikt u een gefilterde EPC op de downlink naar de verificator-switch voor het beste resultaat.

Zie deze configuratiehandleiding voor meer informatie over configuratie en implementatie:

Packet Capture configureren, Cisco IOS Bengaluru 17.6.x (Catalyst 9300)

- Cisco IOS XE-debugs

De veranderingen van de softwarearchitectuur die met Cisco IOS XE versie 16.3.2 beginnen verplaatsten AAA componenten naar een afzonderlijke daemon van Linux. Vertrouwelijke debugs maken geen zichtbare debugs meer mogelijk in de logboekbuffer. In plaats daarvan



Tip: Traditionele IOS AAA-debugs bieden niet langer uitvoer in systeemlogbestanden voor poortverificatie op het voorpaneel binnen de syslogbuffer

Deze klassieke Cisco IOS-debugs voor dot1x en RADIUS maken niet langer viewable debugs mogelijk binnen de switch logging buffer van de switch:

```
debug radius
debug access-session all
debug dot1x all
```

AAA component debugs zijn nu toegankelijk via systeemtracering onder de SMD (Session Manager Daemon).

- Net als traditionele syslogs rapporteert het Catalyst-systeem overtredingen op een standaardniveau en moet het worden geïnstrueerd om meer diepgaande logbestanden te verzamelen.
- Verander het routineniveau voor het gewenste subcomponent met de opdracht "set platform software trace smd switch active r0 <component> debug".

<#root>

```
Switch#
```

set platform software trace smd switch active R0 auth-mgr debug

```
 <<<--- This sets the "auth-mgr" subcomponent to "debug" log level.
```

Deze tabel brengt traditionele IOS debugs aan hun sportequivalent in kaart.

Opdracht Oude stijl	Opdracht Nieuwe stijl
#debug	#set platform software traceren smd switch actieve R0 straal debug
#debug dot1x allemaal	#set platform software traceren smd switch actief R0 dot1x-all debug
#debug-toegangssessie alles	#set platform software traceren smd switch actief R0 auth-mgr-all debug
Alles #debug	#set platform software traceren smd switch actief R0 epm-all debug

Klassieke debugs maken het mogelijk om alle gerelateerde componentsporen te 'debuggen' niveau. Platform commando's worden ook gebruikt om specifieke traces mogelijk te maken.

Gebruik de opdracht "show platform software trace level smd switch active R0" om het huidige traceerniveau voor SMD subcomponenten te tonen.

<#root>

```
Switch#
```

show platform software trace level smd switch active R0

```
Module Name                      Trace Level
----------------------------------------------
aaa
```

Notice

<--- Default level is "Notice"

```
aaa-acct                         Notice
aaa-admin                        Notice
```

```
aaa-api                         Notice
aaa-api-attr                    Notice
<snip>
auth-mgr

Debug <--- Subcomponent "auth-mgr" traces at "debug" level


auth-mgr-all                    Notice
<snip>
```

Het niveau van het sub-componentspoor kan op twee manieren worden hersteld aan gebrek.

- Gebruik "undebug all" of "set platform software trace smd switch active R0 <sub-component> notice" om te herstellen.
- Als het apparaat opnieuw wordt geladen, worden ook de standaardwaarden voor de overtrek hersteld.

```
<#root>

Switch#

undebug all


All possible debugging has been turned off

or

Switch#

set platform software trace smd switch active R0 auth-mgr notice


<--- Sets sub-component "auth-mgr" to trace level "Notice", the system default.
```

Logbestanden voor samengestelde tracering kunnen op console worden bekeken of naar archief worden geschreven en offline worden bekeken. Sporen worden gearchiveerd in gezipte binaire archieven die decoderen vereisen. Contact TAC voor debug assistentie bij het omgaan met gearchiveerde sporen. Dit werkschema verklaart hoe te om de sporen in CLI te bekijken.

Gebruik de opdracht "show platform software trace message smd switch active R0" om de overtrek logbestanden te bekijken die in het geheugen zijn opgeslagen voor de SMD-component.

```
<#root>

Switch#

show platform software trace message smd switch active R0


2016/11/26 03:32:24.790 [auth-mgr]: [1422]: UUID: 0, ra: 0 (info): [0000.0000.0000:unknown] Auth-mgr aa
2016/11/26 03:32:29.678 [btrace]: [1422]: UUID: 0, ra: 0 (note): Single message size is greater than 10
```

```
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Delay-Time [41] 6 0 RADI
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1646/52 10.4
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeo
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radi
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Packets [48] 6 0
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Packets [47] 6 8
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Octets [43] 6 0
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Octets [42] 6 658
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Time [46] 6 125
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Event-Timestamp [55] 6 148013
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Status-Type [40] 6 Stop
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 36 36 33 36 36 39 30 30 2f 33
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 68 72 65 6e 65 6b 2d 69 73 65
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 30 30 30 32 41 39 45 41 45 46
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Class [25] 63
RADIUS: 43 41 43 53 3a 30 41 30 30 30 41 46 45 30 30 30 [CACS:0A000AFE000]
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Terminate-Cause[49] 6 ad
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Authentic [45] 6 Remote
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Id [44] 10 "0000
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50108
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitE
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 17 "C3850
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 10.48.44
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "0
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Called-Station-Id [30] 19 "00
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 12 "method=m
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 18
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-se
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 19 "00-50-56-99
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Framed-IP-Address [8] 6 10.0.
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 205 "cts-pac
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 211
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 95 52 40 05 8f
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Accounting-Req
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): abcdefghijklmno:NO EAP-MESSAGE
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): sending
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Config NAS IP: 10.4
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): Config for source interface found in
<snip>
```

De output is breedsprakig, zodat is het nuttig om de output aan dossier opnieuw te richten.

- Het bestand kan worden gelezen via CLI met behulp van het "meer" hulpprogramma, of offline worden verplaatst voor weergave in teksteditor.

<#root>

```
Switch#

show platform software trace message smd switch active R0 | redirect flash:SMD_debugs.txt

Switch#more flash:SMD_debugs.txt

This command is being deprecated. Please use 'show logging process' command.
executing cmd on chassis 1 ...
```

```
2022/12/02 15:04:47.434368 {smd_RO-0}{2}: [auth-mgr] [16908]: (debug): [0800.27dd.3016:Gi2/0/11] Starte
2022/12/02 15:04:47.434271 {smd_RO-0}{2}: [auth-mgr] [16908]: (info): [0800.27dd.3016:Gi2/0/11] Account
2022/12/02 15:04:43.366688 {smd_RO-0}{2}: [auth-mgr] [16908]: (debug): [5057.a8e1.6f49:Gi2/0/11] Starte
2022/12/02 15:04:43.366558 {smd_RO-0}{2}: [auth-mgr] [16908]: (info): [5057.a8e1.6f49:Gi2/0/11] Account
2022/12/02 15:01:03.629116 {smd_RO-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 15:00:19.350560 {smd_RO-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 01:28:39.841376 {smd_RO-0}{2}: [auth-mgr] [16908]: (ERR): [0000.0000.0000:unknown] sm ctx un
<snip>
```

"Show logging process" is het geactualiseerde hulpprogramma voor traces en de standaard in versie Cisco IOS XE 17.9.x en hoger.

<#root>

```
C9300#

show logging process smd ?

  <0-25>            instance number
  end               specify log filtering end location
  extract-pcap      Extract pcap data to a file
  filter            specify filter for logs
  fru               FRU specific commands
  internal          select all logs. (Without the internal keyword only
                    customer curated logs are displayed)
  level             select logs above specific level
  metadata          CLI to display metadata for every log message
  module            select logs for specific modules
  reverse           show logs in reverse chronological order
  start             specify log filtering start location
  switch            specify switch number
  to-file           decode files stored in disk and write output to file
  trace-on-failure  show the trace on failure summary
  |                 Output modifiers
```

"Toon registratieproces" biedt dezelfde functionaliteit als "toon platform software spoor" in een eleganter en toegankelijker formaat.

<#root>

```
C9300#

clear auth sessions

C9300#

show logging process smd reverse

Logging display requested on 2023/05/02 16:44:04 (UTC) for Hostname: [C9300], Model: [C9300X-24HX], Ver

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 1 ...
============================================================
```

```
 UTM [LUID NOT FOUND] ..... 0
 UTM [PCAP] ..... 0
 UTM [MARKER] ..... 0
 UTM [APP CONTEXT] ..... 0
 UTM [TDL TAN] ..... 5
 UTM [MODULE ID] ..... 0
 UTM [DYN LIB] ..... 0
 UTM [PLAIN TEXT] ..... 6
 UTM [ENCODED] ..... 85839
 UTM [Skipped / Rendered / Total] .. 85128 / 722 / 85850
 Last UTM TimeStamp ..... 2023/05/02 16:44:03.775663010
 First UTM TimeStamp ..... 2023/05/02 15:52:18.763729918
============================================================
----------------- Decoder Output Information --------------
============================================================
 MRST Filter Rules ..... 1
 UTM Process Filter ..... smd
 Total UTM To Process ... 85850
 Total UTF To Process ... 1
 Num of Unique Streams .. 1
============================================================
----------------- Decoder Input Information ---------------
============================================================
======= Unified Trace Decoder Information/Statistics ======
============================================================
2023/05/02 16:44:03.625123675 {smd_RO-0}{1}: [radius] [22624]: (ERR): Failed to mark Identifier for reu
2023/05/02 16:44:03.625123382 {smd_RO-0}{1}: [radius] [22624]: (ERR): RSPE-  Set Identifier Free for Re
2023/05/02 16:44:03.625116747 {smd_RO-0}{1}: [radius] [22624]: (info): Valid Response Packet, Free the
2023/05/02 16:44:03.625091040 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 2b f4 ea
2023/05/02 16:44:03.625068520 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Received from id 1813/9
2023/05/02 16:44:03.610151863 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Started 5 sec timeout
2023/05/02 16:44:03.610097362 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Delay-Time     [41]
2023/05/02 16:44:03.610090044 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Event-Timestamp     [55]
2023/05/02 16:44:03.610085857 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Status-Type    [40]
2023/05/02 16:44:03.610040912 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Class              [25]
2023/05/02 16:44:03.610037444 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Authentic      [45]
2023/05/02 16:44:03.610032802 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Session-Id     [44]
2023/05/02 16:44:03.610028677 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id   [30]
2023/05/02 16:44:03.610024641 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Nas-Identifier      [32]
2023/05/02 16:44:03.610020641 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id  [31]
2023/05/02 16:44:03.610016809 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port           [5]
2023/05/02 16:44:03.610012487 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Type       [61]
2023/05/02 16:44:03.610007504 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Id         [87]
2023/05/02 16:44:03.610003581 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-IP-Address      [4]
2023/05/02 16:44:03.609998136 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id  [31]
2023/05/02 16:44:03.609994109 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id   [30]
2023/05/02 16:44:03.609989329 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair       [1]
2023/05/02 16:44:03.609985171 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco       [26]
2023/05/02 16:44:03.609981606 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair       [1]
2023/05/02 16:44:03.609976961 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco       [26]
2023/05/02 16:44:03.609969166 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  User-Name          [1]
2023/05/02 16:44:03.609963241 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 0b 99 e3
2023/05/02 16:44:03.609953614 {smd_RO-0}{1}: [radius] [22624]: (info): RADIUS: Send Accounting-Request
2023/05/02 16:44:03.609863172 {smd_RO-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Handl
2023/05/02 16:44:03.609695649 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAPOL pa
2023/05/02 16:44:03.609689224 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:unknown] Pkt body
2023/05/02 16:44:03.609686794 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAP Pack
2023/05/02 16:44:03.609683919 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Sent EAP
2023/05/02 16:44:03.609334292 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Sending
2023/05/02 16:44:03.609332867 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Setting
2023/05/02 16:44:03.609310820 {smd_RO-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Posting
2023/05/02 16:44:03.609284841 {smd_RO-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Raisi
```

Sporenvoorbeelden

Deze sectie bevat overtrekken van Session Manager voor dot1x- en radiuscomponenten voor een volledige, mislukte transactie (server wijst clientreferenties af). Het is bedoeld als basisrichtlijn om te navigeren systeem sporen met betrekking tot voorpaneelauthentificatie.

- Een testclient probeert verbinding te maken met Gigabit Ethernet1/0/2 en wordt afgewezen.

In dit voorbeeld, SMD component sporen worden geplaatst aan "zuiveren".

<#root>

C9300#

set platform software trace smd sw active r0 dot1x-all

C9300#

set platform software trace smd sw active r0 radius debug

EAPoL: START

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] queuing an EAPOL pkt on Auth Q
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 0,TYPE= 0,LEN= 0
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Couldn't find the supplicant in the l
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] New client detected, sending session
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: initialising
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: disconnected
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering init state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Created a client entry (0x0A00000E)
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x authentication started for 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: IDENTITEIT EAP-AANVRAAG

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:idle request action
```

EAPoL: EAP-RESPONS

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 1,LEN= 14
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radius
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: TOEGANGSAANVRAAG

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 59 c9 e0 be 4d b5 1c 11 - 02 cb 5b eb
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
0e 01 69 78 69 61 5f 64 61 74 61 [ ixia_data]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 16
69 87 3c 61 80 3a 31 a8 73 2b 55 76 f4 [ Ei<a:1s+Uv]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: ACCESS-UITDAGING

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/82 172.28.99.252:0, Access-Cha
```

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014 RADIUS: authenticator 82 71 61
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 f9 00 06 0d 20 [ ]
02/15 14:01:28.986 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
RADIUS: 78 66 ec be 2c a4 af 79 5e ec c6 47 8b da 6a c2 [ xf,y^Gj]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/82
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state###
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: EAP-RESPONS

```
02/15 14:01:28.988 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pk
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL p
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enteri
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to t
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:reques
02/15 14:01:28.989 [aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick met
02/15 14:01:28.990 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.
02/15 14:01:28.990 [radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C
02/15 14:01:28.990 [aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: TOEGANGSAANVRAAG

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 3d 31 3f ee 14 b8 9d 63 - 7a 8b 52 90
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 f9 00 06 03 04
02/15 14:01:28.991 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
RADIUS: 8b 2a 2e 75 90 a2 e1 c9 06 84 c9 fe f5 d0 98 39 [ *.u9]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
```

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: ACCESS-UITDAGING

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/83 172.28.99.252:0, Access-Cha
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 0c 8d 49 80 0f 51 89 fa - ba 22 2f 96
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 fa 00 21 04 10 5b d0 b6 4e 68 37 6b ca 5e 6f 5a 65 78 04 77 bf 69 73 65 2d [![Nh7k^oZexwise-]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 35
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 70 6f 6c 2d 65 73 63 [ pol-esc]
RADIUS: a3 0d b0 02 c8 32 85 2c 94 bd 03 b3 22 e6 71 1e [ 2,"q]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/83
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: EAP-AANVRAAG

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: EAP-RESPONS

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 4,LEN= 31
```

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radiu
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: TOEGANGSAANVRAAG

```
radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645 i
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 41 4d 76 8e 03 93 9f 05 - 5e fa f1 d6
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 fa 00 1f 04 10 02 b6 bc aa f4 91 2b d6 cf 9e 3b d5 44 96 78 d5 69 78 69 61 5f 64 61 74 61 [
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 33
RADIUS: 3b 70 b1 dd 97 ac 47 ae 81 ca f8 78 5b a3 7b fe [ ;pGx[{]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: TOEGANGSWEIGERING

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/84 172.28.99.252:0, Access-Rej
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator d1 a3 eb 43 11 45 6b 8f - 07 a7 34 dd
RADIUS: 04 fa 00 04
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 6
RADIUS: 80 77 07 f7 4d f8 a5 60 a6 b0 30 e4 67 85 ae ba [ wM`0g]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 3, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/84
```

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received an EAP Fail
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_FAIL for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering fail state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response fail action
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_FAIL on Client 0x0A0000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting authenticating st
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering authc result sta
[errmsg]: [16498]: UUID: 0, ra: 0 (note): %DOT1X-5-FAIL: Authentication failed for client (0040.E93E.00
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Added username in dot1x
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x did not receive any key data
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received Authz fail (result: 2) for t
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting_AUTHZ_FAIL on Client 0x0A000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: held
```

EAPoL: EAP REJECT

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting FAILOVER_RETRY on Client 0x0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: exiting held state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:restart action called
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RESTART on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

Aanvullende informatie

Standaardinstellingen

Feature	Standaard instelling
Switch 802.1x activeert status	Uitgeschakeld.
Status per poort inschakelen 802.1x	Uitgeschakeld (met toestemming tot overmacht). De poort verzendt en ontvangt normaal verkeer zonder 802.1x-

Feature	Standaard instelling
	gebaseerde verificatie van de client.
AAA	Uitgeschakeld.
RADIUS-server • IP-adres • UDP-verificatiepoort • Standaard accounting poort • Sleutel	• Geen opgegeven. • 1645. • 1646. • Geen opgegeven.
Hostmodus	Single-host modus.
Bedieningsrichting	Bidirectionele controle.
Periodieke herverificatie	Uitgeschakeld.
Aantal seconden tussen herverificatiepogingen	360 seconden.
Herverificatienummer	2 keer (aantal keren dat de switch het verificatieproces opnieuw start voordat de poort in de niet-geautoriseerde status verandert).
Stille periode	60 seconden (aantal seconden dat de switch in de stille toestand blijft na een mislukte authenticatiewisseling met de client).
Heruitzendtijd	30 seconden (aantal seconden dat de switch wacht op een antwoord op een EAP-verzoek/identiteitskader van de client voordat hij het verzoek opnieuw verstuurt).
Maximum aantal wederuitzendingen	2 keer (aantal keren dat de switch een EAP-verzoek/identiteitskader verstuurt voordat het verificatieproces wordt herstart).

Feature	Standaard instelling
Time-outperiode voor client	30 seconden (bij het doorgeven van een verzoek van de verificatieserver aan de client, de tijd die de switch wacht op een antwoord voordat hij het verzoek opnieuw verstuurt naar de client.)
Time-outperiode voor verificatieserver	30 seconden (bij het doorgeven van een reactie van de client naar de verificatieserver, de tijd die de switch wacht op een antwoord voordat hij de reactie op de server opnieuw verstuurt). U kunt deze timeout periode wijzigen met de dot1x timeout server-timeout interface configuratie commando.
Time-out voor inactiviteit	Uitgeschakeld.
Gast-VLAN	Geen opgegeven.
Ontoegankelijke verificatie-omzeiling	Uitgeschakeld.
Beperkt VLAN	Geen opgegeven.
Verificatormodus (switch)	Geen opgegeven.
MAC-verificatie-omzeiling	Uitgeschakeld.
Spraakbewuste beveiliging	Uitgeschakeld.

Optionele instellingen

Periodieke herverificatie

U kunt periodieke 802.1x-client-herverificatie inschakelen en opgeven hoe vaak dit gebeurt:

- periodieke verificatie - maakt periodieke verificatie van de client mogelijk
- inactiviteit— Interval in seconden waarna, als er geen activiteit van de cliënt is dan is het niet toegestaan
- opnieuw verifiëren— Tijd in seconden waarna een automatische herverificatiepoging wordt gestart

- restartwaarde— Interval in seconden waarna wordt geprobeerd om een niet-geautoriseerde poort te authenticeren
- niet-toegestane waarde— Interval in seconden waarna een niet-geautoriseerde sessie wordt verwijderd

```
authentication periodic
authentication timer {{[inactivity | reauthenticate | restart | unauthorized]} {value}}
```

Schendingen

U kunt een 802.1x-poort zo configureren dat deze wordt uitgeschakeld, een syslogfout genereert of pakketten van een nieuw apparaat verwijdert wanneer een apparaat verbinding maakt met een 802.1x-poort of het maximale aantal toegestane apparaten over apparaten op de poort is geverifieerd.

- shutdown - fout schakelt de poort uit.
- limiteren- Een syslog-fout genereren.
- bescherm - Drop pakketten tegen elk nieuw apparaat dat verkeer naar de poort verstuurt.
- replace- Verwijdert de huidige sessie en authenticeert met de nieuwe host.

```
authentication violation {shutdown | restrict | protect | replace}
```

De stille periode wijzigen

De opdracht voor het configureren van de interfaceconfiguratie voor het opnieuw starten van de verificatietimer regelt de periode tijdens welke de switch inactief blijft nadat een switch de client niet kan authenticeren. Het bereik van de waarde is 1 tot 65535 seconden.

```
authentication timer restart {seconds}
```

De Switch-naar-client hertransmissietijd wijzigen

De client reageert op het EAP-verzoek/identiteitskader van de switch met een EAP-respons/identiteitskader. Als de switch deze reactie niet ontvangt, wacht hij op een bepaalde tijdsperiode (de wederuitzendtijd) en verstuurt hij het frame opnieuw.

```
authentication timer reauthenticate {seconds}
```

Het Switch-to-client frame-hertransmissienummer instellen

U kunt het aantal keren wijzigen dat de switch een EAP-verzoek/identiteitskader verstuurt (ervan uitgaande dat er geen antwoord wordt ontvangen) naar de client voordat het verificatieproces wordt herstart. Het bereik is 1 tot 10.

```
dot1x max-reauth-req {count}
```

De hostmodus configureren

U kunt meerdere hosts (clients) toestaan op een 802.1x geautoriseerde poort.

- multi-auth - Sta meerdere geverifieerde clients toe op zowel spraak VLAN als data VLAN.
- multi-host - Meerdere hosts toestaan op een 802.1x-geautoriseerde poort nadat één host is geauthenticeerd.
- multi-domein - hiermee kan zowel een host als een spraakapparaat, zoals een IP-telefoon (Cisco of niet-Cisco), worden geverifieerd op een door IEEE 802.1x geautoriseerde poort.

```
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]
```

MAC Move inschakelen

De beweging van MAC staat een voor authentiek verklaarde gastheer toe om van één haven op het apparaat aan een andere te bewegen.

```
authentication mac-move permit
```

MAC-vervanging inschakelen

MAC replace staat een host toe om een geverifieerde host te vervangen op een poort.

- te beveiligen - de poort laat vallen pakketten met onverwachte MAC-adressen zonder een systeembericht te genereren.
- limiteren - overtredende pakketten worden door de CPU gedropt en er wordt een systeembericht gegenereerd.

- sluiting - de poort is fout uitgeschakeld wanneer het een onverwacht MAC-adres ontvangt.

```
authentication violation {protect | replace | restrict | shutdown}
```

Het herverificatienummer instellen

U kunt ook het aantal keren wijzigen dat het apparaat het verificatieproces opnieuw start voordat de poort verandert in de niet-geautoriseerde status. Het bereik is 0 tot 10

```
dot1x max-req {count}
```

Een gast VLAN configureren

Wanneer u een gast-VLAN configureert, worden clients die niet geschikt zijn voor 802.1x in het gast-VLAN geplaatst wanneer de server geen antwoord ontvangt op zijn EAP-verzoek/identiteitskader.

```
authentication event no-response action authorize vlan {vlan-id}
```

Een beperkt VLAN configureren

Wanneer u een beperkt VLAN op een apparaat configureert, worden clients die IEEE 802.1x-compatibel zijn, naar het beperkte VLAN verplaatst wanneer de verificatieserver geen geldige gebruikersnaam en wachtwoord ontvangt.

```
authentication event fail action authorize vlan {vlan-id}
```

Het configureren van het aantal verificatiepogingen op een beperkt VLAN

U kunt het maximale aantal toegestane verificatiepogingen configureren voordat een gebruiker is toegewezen aan het beperkte VLAN door de verificatiegebeurtenis fail retry Countinterface Configuration commando te gebruiken. Het bereik van de toegestane verificatiepogingen is 1 tot 3.

```
authentication event fail retry {retry count}
```

802.1x ontoegankelijke verificatie-omleiding configureren met kritisch spraak-VLAN

U kunt een kritisch spraak-VLAN configureren op een poort en de ontoegankelijke omzeilingsfunctie voor verificatie inschakelen.

- autoriseren - Verplaats nieuwe hosts die proberen te verifiëren naar het door de gebruiker opgegeven kritieke VLAN
- reinitialize - Verplaats alle geautoriseerde hosts op de poort naar het door de gebruiker opgegeven kritieke VLAN

```
authentication event server dead action {authorize | reinitialize} vlan vlan-id]
authentication event server dead action authorize voice
```

802.1x-verificatie configureren met WoL

U kunt 802.1x-verificatie inschakelen met Wake on LAN (WoL)

```
authentication control-direction both
```

MAC-verificatie-omzeiling configureren

```
mab
```

Flexibele verificatie configureren - opdracht geven tot

```
authentication order [ dot1x | mab ] | {webauth}
authentication priority [ dot1x | mab ] | {webauth}
```

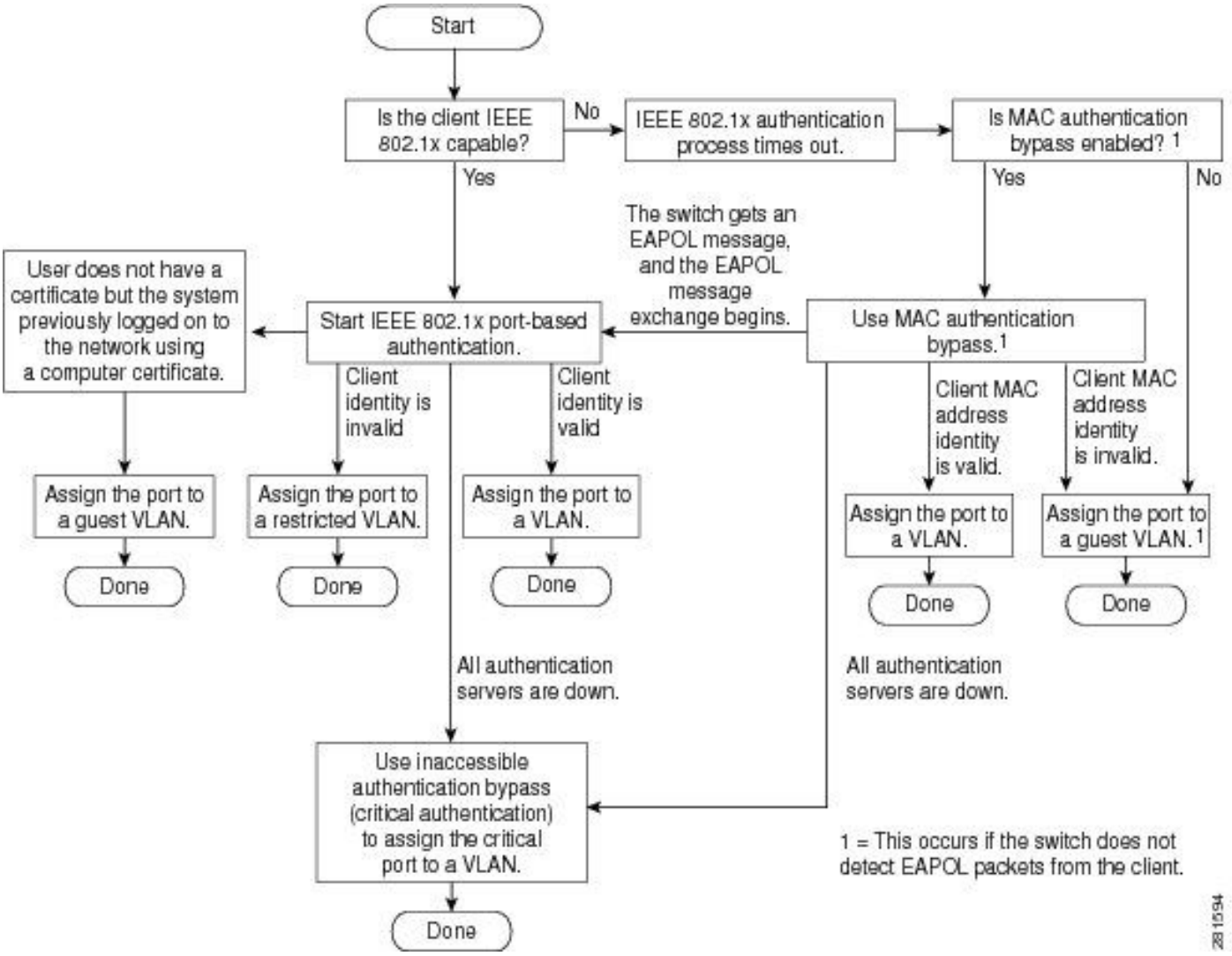
Spraakbewuste 802.1x-beveiliging configureren

U gebruikt de beveiligingsfunctie 802.1x op het apparaat om alleen het VLAN uit te schakelen waarop een beveiligingsovertreding plaatsvindt, of het nu om gegevens of spraak-VLAN gaat. Een veiligheidsschending die op de gegevens VLAN wordt gevonden resulteert in de sluiting van slechts de gegevens VLAN. Dit is een globale configuratie.

```
errdisable detect cause security-violation shutdown vlan
errdisable recovery cause security-violation
```

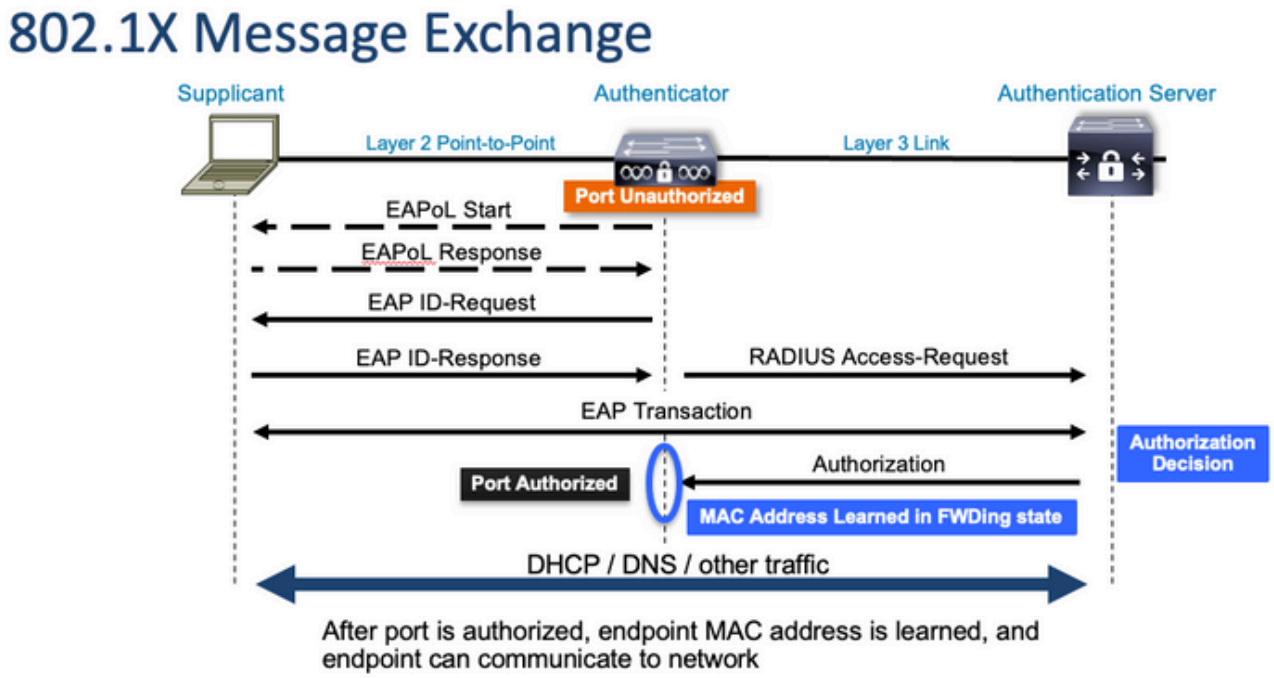
Stroomdiagrammen

Verificatiestroomschema



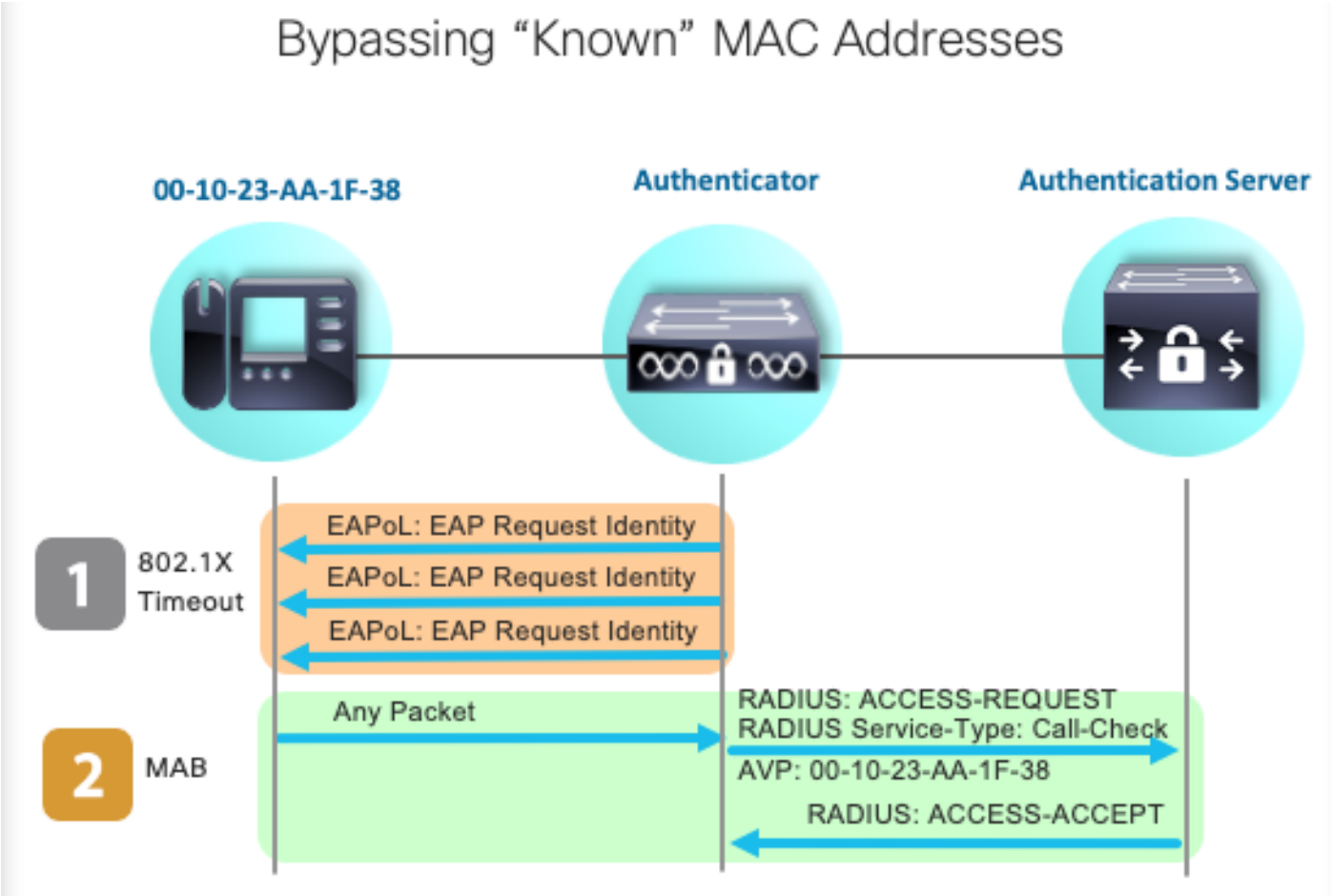
Poortgebaseerde verificatie-initiatie en berichtenuitwisseling

Dit getal toont de client die het bericht uitwisselt met de RADIUS-server.



MAB-verificatie, initiatie en berichtenuitwisseling

Dit cijfer toont de berichtuitwisseling tijdens de omleiding van de MAC-verificatie (MAB)



Gerelateerde informatie

- Duidelijke RADIUS-serverconfiguraties
- Implementatiegids voor MAC-verificatie en omzeiling
- Implementatiegids voor bekabelde 802.1x
- Catalyst 9300 Configuratiehandleiding voor SPAN
- Catalyst 9300 EPC-configuratiehandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.