

Risoluzione dei problemi relativi al dot1x sugli switch Catalyst serie 9000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione di base](#)

[Verifica della configurazione e delle operazioni](#)

[Introduzione a 802.1x](#)

[Configurazione](#)

[Sessione di autenticazione](#)

[Raggiungibilità del server di autenticazione](#)

[Risoluzione dei problemi](#)

[Metodologia](#)

[Sintomi di esempio](#)

[Utility specifiche della piattaforma](#)

[Esempi di traccia](#)

[Ulteriori informazioni](#)

[Impostazioni predefinite](#)

[Impostazioni opzionali](#)

[Diagrammi di flusso](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare, convalidare e risolvere i problemi relativi al controllo dell'accesso alla rete 802.1x (NAC) sugli switch Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.


- Switch Catalyst serie 9000
- Identity Services Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x e versioni successive
- ISE-VM-K9 versione 3.0.0.458

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

 Nota: per i comandi che vengono usati per abilitare queste funzionalità su altre piattaforme Cisco, consultare la guida alla configurazione appropriata.

Premesse

Lo standard 802.1x definisce un protocollo di autenticazione e controllo degli accessi basato su client-server che impedisce ai client non autorizzati di connettersi a una rete LAN tramite porte accessibili pubblicamente, a meno che non vengano autenticati correttamente. Il server di autenticazione autentica ogni client connesso a una porta dello switch prima di rendere disponibili i servizi offerti dallo switch o dalla LAN.


L'autenticazione 802.1x comprende 3 componenti distinti:

Supplicant - Client che invia le credenziali per l'autenticazione

Autenticatore - Dispositivo di rete che fornisce la connettività di rete tra il client e la rete e che può consentire o bloccare il traffico di rete.

Server di autenticazione: server in grado di ricevere e rispondere alle richieste di accesso alla rete, indica all'autenticatore se la connessione può essere consentita e se esistono diverse altre impostazioni da applicare alla sessione di autenticazione.

I destinatari di questo documento sono i tecnici e il personale di supporto che non si occupa necessariamente di sicurezza. Per ulteriori informazioni sull'autenticazione basata sulla porta 802.1x e su componenti come ISE, consultare la guida alla configurazione appropriata.

 Nota: per una configurazione di autenticazione 802.1x più accurata, consultare la guida alla configurazione appropriata per la piattaforma e la versione di codice specifiche.

Configurazione di base

In questa sezione viene descritta la configurazione di base necessaria per implementare l'autenticazione basata sulla porta 802.1x. Ulteriori informazioni sulle caratteristiche sono disponibili nella scheda Componenti aggiuntivi di questo documento. Esistono lievi variazioni negli standard di configurazione da versione a versione. Convalidare la configurazione in base alla versione corrente della guida alla configurazione.

È necessario abilitare l'autenticazione, l'autorizzazione e l'account (AAA) prima di configurare l'autenticazione post-basata su 802.1x ed è necessario stabilire un elenco di metodi.

- Gli elenchi di metodi descrivono la sequenza e il metodo di autenticazione da interrogare per autenticare un utente.
- È inoltre necessario abilitare 802.1x a livello globale.

```
<#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
```

Definire un server RADIUS sullo switch

```
<#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
```

Abilitare 802.1x sull'interfaccia client.

```
<#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
```

Verifica della configurazione e delle operazioni

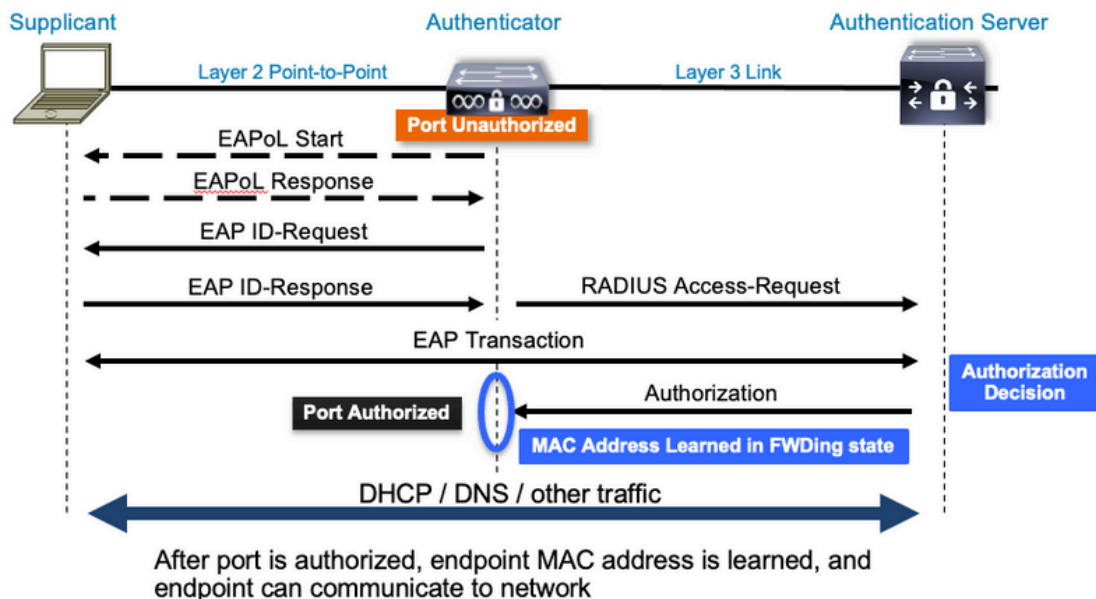
In questa sezione vengono fornite informazioni di base su 801.1x e viene illustrato come verificare la configurazione e le operazioni.

Introduzione a 802.1x

802.1x implica due tipi distinti di traffico: traffico da client a autenticatore (point-to-point) su EAPoL (Extensible Authentication Protocol over LAN) e traffico da autenticatore a server di autenticazione incapsulato tramite RADIUS.

Questo diagramma rappresenta il flusso di dati per una semplice transazione dot1x

802.1X Message Exchange



L'autenticatore (switch) e il server di autenticazione (ad esempio ISE) sono spesso separati dal layer 3. Il traffico RADIUS viene instradato sulla rete tra autenticatore e server. Il traffico EAPoL viene scambiato sul collegamento diretto tra il richiedente (client) e l'autenticatore.

Si noti che l'apprendimento degli indirizzi MAC avviene dopo l'autenticazione e l'autorizzazione.

Di seguito sono riportate alcune domande da tenere presenti quando si affronta un problema che interessa 802.1x:

- È configurato correttamente?
- Il server di autenticazione è raggiungibile?
- Qual è lo stato di Authentication Manager?
- Sono presenti problemi con il recapito dei pacchetti tra client e autenticatore o tra autenticatore e server di autenticazione?

Configurazione

Alcune configurazioni variano leggermente tra le versioni principali. Fare riferimento alla guida alla configurazione pertinente per le guide specifiche sulla piattaforma/codice.

Il server AAA deve essere configurato per utilizzare l'autenticazione basata sulla porta 802.1x.

- È necessario stabilire un elenco di metodi di autenticazione per "dot1x". Questa configurazione rappresenta una configurazione AAA comune in cui è abilitato 802.1X.

```
<#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

```

Questa è una configurazione di interfaccia di esempio in cui è abilitato 802.1x. MAB (MAC Authentication Bypass) è un metodo di backup comune per l'autenticazione dei client che non supportano i supplicant dot1x.

```
<#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

```

Determinare se un indirizzo MAC è stato appreso sull'interfaccia con "show mac address-table interface <interface>". L'interfaccia impara un indirizzo MAC solo quando viene autenticata correttamente.

```

<#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

```

Sessione di autenticazione

I comandi show sono disponibili per la convalida dell'autenticazione 802.1x.

Utilizzare "show authentication sessions" o "show authentication sessions <interface>" per visualizzare informazioni sulle sessioni di autenticazione correnti. In questo esempio, solo Te1/0/4 dispone di una sessione di autenticazione attiva.

```

<#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

"Show authentication sessions interface <interface> details" fornisce dettagli aggiuntivi su una sessione di autenticazione di interfaccia specifica.

<#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.
```

Se l'autenticazione è abilitata su un'interfaccia ma non vi è alcuna sessione attiva, viene visualizzato l'elenco dei metodi eseguibili. Viene inoltre visualizzato "No session match provided criteria" (Nessuna sessione corrispondente ai criteri forniti).

```
<#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

se sull'interfaccia non è abilitata l'autenticazione, non è rilevata alcuna presenza di Auth Manager. Viene inoltre visualizzato "No session match provided criteria" (Nessuna sessione corrispondente ai criteri forniti).

```
<#root>
```

```
C9300#
```

```
show authentication sessions interface te1/0/6
```

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

Raggiungibilità del server di autenticazione

La raggiungibilità del server di autenticazione è un prerequisito per la riuscita dell'autenticazione 802.1x.

Utilizzare "ping <server_ip>" per verificare rapidamente la raggiungibilità. Accertarsi che il ping provenga dall'interfaccia di origine RADIUS.

```
<#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
```

Il comando "show aaa servers" identifica lo stato del server e fornisce statistiche sulle transazioni con tutti i server AAA configurati.

```
<#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 WNCN (1) : current UP
```

```
Platform State from WNCN (2) : current UP
```

```
Platform State from WNCN (3) : current UP
```

```
Platform State from WNCN (4) : current UP
```

```
Platform State from WNCN (5) : current UP
```

```
Platform State from WNCN (6) : current UP
```

```
Platform State from WNCN (7) : current UP
```

```
Platform State from WNCN (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
  WNCB Platform: max 0, current 0 total 0
  IOSB Platform : max 2, current 2 total 2
Consecutive Timeouts: total 466
  SMD Platform : max 455, current 0 total 455
  WNCB Platform: max 0, current 0 total 0
  IOSB 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
```

Utilizzare l'utility "test aaa" per verificare la raggiungibilità dallo switch al server di autenticazione. Questa utilità è obsoleta e non è disponibile per un periodo di tempo indefinito.

```
<#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 server
```

```
User rejected
```

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

```
*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
```

Risoluzione dei problemi

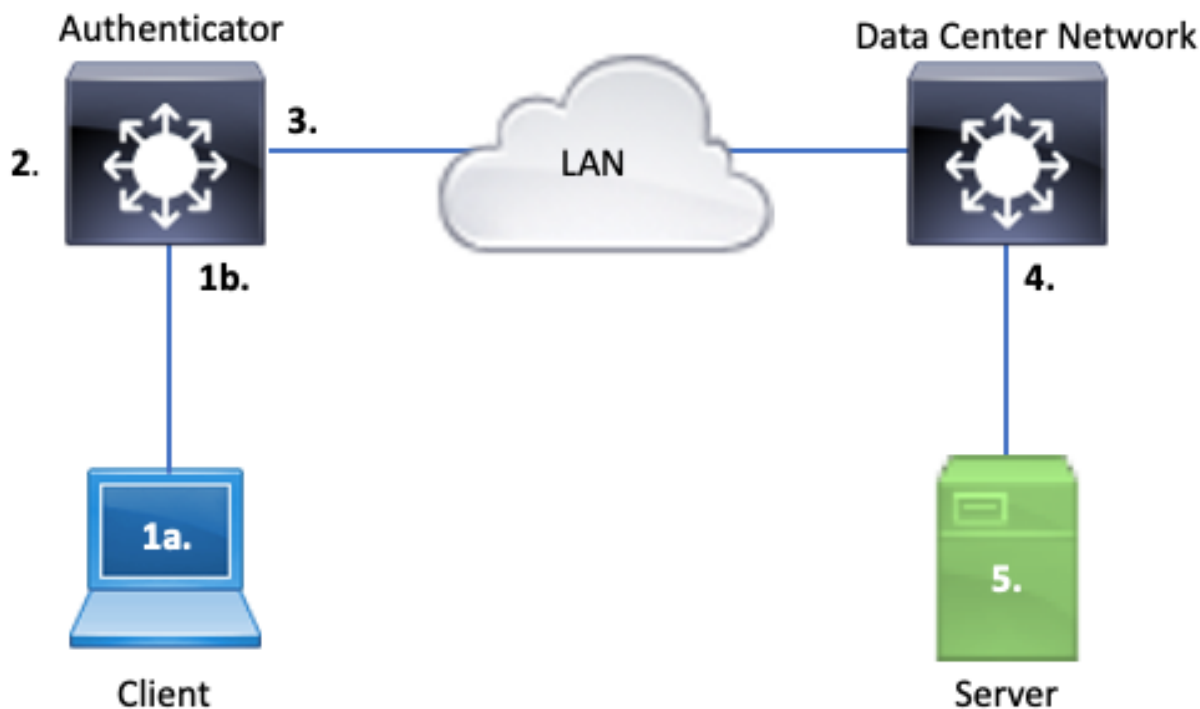
In questa sezione viene spiegato come risolvere la maggior parte dei problemi relativi allo switch Catalyst 802.1x.

Metodologia

Problemi di approccio che coinvolgono 802.1x e l'autenticazione metodica per ottenere risultati ottimali. Ecco alcune delle domande a cui è bene rispondere:

- Il problema è isolato a un singolo switch? Una porta singola? Un singolo tipo di client?
- La configurazione è stata convalidata? Il server di autenticazione è raggiungibile?
- Il problema si verifica ogni volta o è intermittente? Si verifica solo con la riautenticazione o la modifica dell'autorizzazione?

Esaminare una singola transazione non riuscita end-to-end se i problemi persistono dopo che l'ovvio è stato escluso. I dati migliori e più completi per l'analisi di una transazione 802.1x dal client al server includono:



1 bis. Acquisizione sul client e/o

1 ter. Sull'interfaccia di accesso a cui il client si connette

Questo punto di riferimento è fondamentale per consentirci di comprendere meglio i pacchetti EAPoL scambiati tra la porta di accesso dove è abilitato il dot1x e il client. SPAN è lo strumento più affidabile per visualizzare il traffico tra client e autenticatore.

2. Debug sull'autenticatore

I debug consentono di tracciare la transazione attraverso l'autenticatore.

- L'autenticatore deve puntare i pacchetti EAPoL ricevuti e generare traffico unicast con incapsulamento RADIUS destinato al server di autenticazione.
- Accertarsi che siano impostati i livelli di debug appropriati per garantire la massima efficacia.

3. Acquisizione adiacente all'autenticatore

Questa acquisizione consente di visualizzare la conversazione tra Authenticator e il server di autenticazione.

- Questa acquisizione consente di visualizzare in modo accurato l'intera conversazione dal punto di vista dell'autenticatore.
- Se abbinato all'acquisizione di cui al punto 4, è possibile determinare se vi è una perdita tra Authentication Server e Authenticator.

4. Acquisizione adiacente al server di autenticazione

Questa cattura è complementare alla cattura di cui al punto 3.

- Questa acquisizione fornisce l'intera conversazione dalla prospettiva del server di autenticazione.
- Se abbinato all'acquisizione di cui al punto 3, è possibile determinare se esiste una perdita tra Authenticator e Authentication Server.

5. Acquisizione, debug, accesso al server di autenticazione

L'ultimo tassello del puzzle, i debug dei server, ci dicono cosa il server sa della nostra transazione.

- Grazie a questo insieme di dati end-to-end, un tecnico di rete può determinare il punto in cui la transazione si interrompe ed escludere i componenti che non contribuiscono al problema.

Sintomi di esempio

In questa sezione viene fornito un elenco dei sintomi e degli scenari più comuni.

- Nessuna risposta dal client

Se il traffico EAPoL generato dallo switch non genera una risposta, viene visualizzato questo syslog:

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

Il codice motivo "Nessuna risposta dal client" indica che lo switch ha avviato il processo dot1x, ma che non è stata ricevuta alcuna risposta dal client entro il periodo di timeout.

Il client non ha ricevuto o non è in grado di comprendere il traffico di autenticazione inviato dalla porta dello switch oppure la risposta del client non è stata ricevuta sulla porta dello switch.

- Il client abbandona la sessione

Se una sessione di autenticazione viene avviata ma non completata, il server di autenticazione (ad esempio ISE) segnala che il client ha avviato una sessione, ma l'ha abbandonata prima del completamento.

Ciò significa spesso che il processo di autenticazione può essere completato solo parzialmente.

Verificare che l'intera transazione tra lo switch di autenticazione e il server di autenticazione sia recapitata in modo completo e sia interpretata correttamente dal server di autenticazione.

Se il traffico RADIUS viene perso sulla rete o viene recapitato in un modo in cui non può essere assemblato correttamente, la transazione è incompleta e il client ritenta l'autenticazione. Il server a sua volta segnala che il client ha abbandonato la propria sessione.

- Il client MAB non riesce a eseguire il comando DHCP/fallback su APIPA

MAC Authentication Bypass (MAB) consente l'autenticazione basata sull'indirizzo MAC. Spesso i client che non supportano l'autenticazione del software supplicant tramite MAB.

Se MAB viene utilizzato come metodo di fallback per l'autenticazione mentre dot1x è il metodo preferito e iniziale in esecuzione su una porta dello switch, si può verificare uno scenario in cui il client non è in grado di completare il protocollo DHCP.

Il problema si riduce all'ordine delle operazioni. Durante l'esecuzione di dot1x, la porta dello switch consuma pacchetti diversi da EAPoL fino al completamento dell'autenticazione o al timeout di dot1x. Il client, tuttavia, tenta immediatamente di ottenere un indirizzo IP e invia i messaggi di individuazione DHCP. Questi messaggi vengono utilizzati dalla porta dello switch finché il punto1x non supera i valori di timeout configurati e il MAB non può essere eseguito. Se il periodo di timeout DHCP del client è inferiore al periodo di timeout dot1x, DHCP ha esito negativo e il client torna all'APIPA o a qualsiasi altra strategia di fallback.

Questo problema viene evitato in diversi modi. Favorire MAB sulle interfacce in cui si connettono i client autenticati MAB. Se dot1x deve essere eseguito per primo, prestare attenzione al comportamento DHCP del client e regolare i valori di timeout in modo appropriato.

Quando si utilizzano dot1x e MAB, è necessario tenere in considerazione il comportamento del client. Una configurazione valida può causare un problema tecnico, come descritto in precedenza.

Utility specifiche della piattaforma

In questa sezione vengono descritte molte delle utility specifiche della piattaforma disponibili sugli switch Catalyst serie 9000, utili per risolvere i problemi del dot1x.

- SPAN (Switch Port Analyzer)

SPAN consente all'utente di eseguire il mirroring del traffico da una o più porte a una porta di destinazione per l'acquisizione e l'analisi. L'SPAN locale è l'utilità di acquisizione più affidabile.

Per i dettagli sulla configurazione e l'implementazione, consultare questa guida alla configurazione:

[Configurazione di SPAN e RSPAN, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9300\)](#)

- EPC (Embedded Packet Capture)

L'EPC sfrutta le risorse di CPU e memoria per fornire funzionalità di acquisizione locale dei pacchetti integrate.

L'EPC presenta delle limitazioni che ne condizionano l'efficacia nell'individuazione di determinati problemi. La velocità di EPC è limitata a 1000 pacchetti al secondo. EPC non è inoltre in grado di acquisire in modo affidabile i pacchetti iniettati dalla CPU in uscita dalle interfacce fisiche. Ciò è significativo quando lo stato attivo si trova sulla transazione RADIUS tra lo switch di

autenticazione e il server di autenticazione. Spesso la velocità del traffico sull'interfaccia rivolta al server supera di gran lunga i 1000 pacchetti al secondo. Inoltre, un EPC all'uscita dell'interfaccia che si trova di fronte al server non è in grado di acquisire il traffico generato dallo switch di autenticazione.

Utilizzare elenchi di accesso bidirezionali per filtrare l'EPC in modo da evitare l'impatto del limite di 1000 pacchetti al secondo. Se si è interessati al traffico RADIUS tra l'autenticatore e il server, concentrarsi sul traffico tra l'indirizzo dell'interfaccia di origine RADIUS dell'autenticatore e l'indirizzo del server.

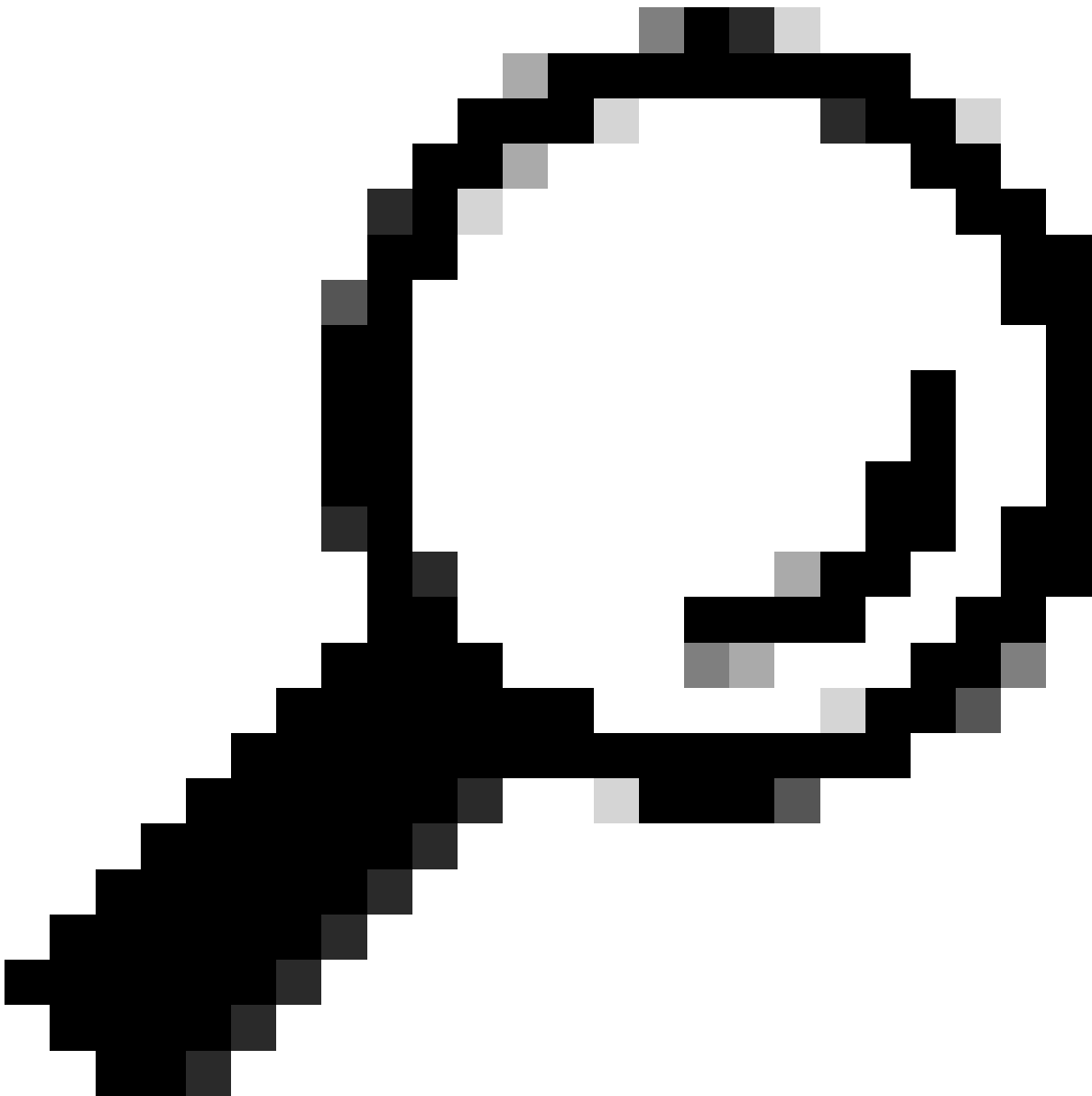
Se il successivo dispositivo a monte verso il server di autenticazione è uno switch Catalyst, per ottenere risultati ottimali utilizzare un EPC filtrato sul collegamento a valle verso lo switch di autenticazione.

Per i dettagli sulla configurazione e l'implementazione, consultare questa guida alla configurazione:

[Configurazione dell'acquisizione del pacchetto, Cisco IOS Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Debug di Cisco IOS XE

Le modifiche all'architettura software che iniziano con Cisco IOS XE versione 16.3.2 hanno spostato i componenti AAA in un daemon Linux separato. I debug familiari non consentono più i debug visualizzabili nel buffer di registrazione. Invece,



Suggerimento: i debug IOS AAA tradizionali non forniscono più l'output nei log di sistema per l'autenticazione della porta del pannello anteriore nel buffer syslog

I seguenti debug Cisco IOS classici per dot1x e RADIUS non consentono più i debug visualizzabili all'interno del buffer di registrazione dello switch:

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

I debug dei componenti AAA sono ora accessibili tramite la traccia di sistema in SMD (Session Manager Daemon).

- Analogamente ai syslog tradizionali, il sistema Catalyst traccia il report a un livello predefinito e deve ricevere istruzioni per la raccolta di log più dettagliati.
- Modificare il livello di traccia della routine per il sottocomponente desiderato con il comando "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.
```

In questa tabella vengono mappati i debug IOS tradizionali ai relativi equivalenti di traccia.

Stile precedente, comando	Nuovo stile, comando
raggio #debug	#set platform software trace smd switch attivo R0 radius debug
#debug dot1x all	#set platform software trace smd switch attivo R0 dot1x-all debug
#debug access-session all	#set platform software trace smd switch attivo R0 auth-mgr-all debug
#debug epm all	#set platform software trace smd switch attivo R0 epm-all debug

I debug classici abilitano tutte le tracce dei componenti correlati al livello 'debug'. I comandi della piattaforma vengono inoltre utilizzati per abilitare le tracce specifiche, in base alle esigenze.

Usare il comando "show platform software trace level smd switch active R0" per visualizzare il livello di traccia corrente per i sottocomponenti SMD.

```
<#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>
```

Il livello di traccia del sottocomponente può essere ripristinato ai valori predefiniti in due modi.

- Utilizzare "undebbug all" o "set platform software trace smd switch active R0 <sottocomponente> notice" per eseguire il ripristino.
- Se il dispositivo viene ricaricato, anche i livelli di traccia vengono ripristinati ai valori predefiniti.

```
<#root>
```

```
Switch#
```

```
undebbug 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.
```

I registri di traccia dei componenti possono essere visualizzati sulla console oppure scritti per l'archiviazione e visualizzati offline. Le tracce vengono archiviate in archivi binari compressi che richiedono la decodifica. Per assistenza sul debug delle tracce archiviate, contattare TAC. Questo flusso di lavoro spiega come visualizzare le tracce nella CLI.

Usare il comando "show platform software trace message smd switch active R0" per visualizzare i log di traccia archiviati in memoria per il componente SMD.

```
<#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>

```

Poiché l'output è dettagliato, è utile reindirizzarlo su file.

- Il file può essere letto tramite CLI con l'utility "more" o spostato offline per la visualizzazione nell'editor di testo.

```
<#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_R0-0}{2}: [auth-mgr] [16908]: (debug): [0800.27dd.3016:Gi2/0/11] Starte
2022/12/02 15:04:47.434271 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [0800.27dd.3016:Gi2/0/11] Account
2022/12/02 15:04:43.366688 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [5057.a8e1.6f49:Gi2/0/11] Starte

```

```

2022/12/02 15:04:43.366558 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [5057.a8e1.6f49:Gi2/0/11] Account
2022/12/02 15:01:03.629116 {smd_R0-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 15:00:19.350560 {smd_R0-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 01:28:39.841376 {smd_R0-0}{2}: [auth-mgr] [16908]: (ERR): [0000.0000.0000:unknown] sm ctx un
<snip>

```

"Show logging process" è l'utility aggiornata per le tracce e lo standard Cisco IOS XE 17.9.x e versioni successive.

<#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

```

"Show logging process" offre le stesse funzionalità di "show platform software trace" in un formato più elegante e accessibile.

<#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_R0-0}{1}: [radius] [22624]: (ERR): Failed to mark Identifier for reu
2023/05/02 16:44:03.625123382 {smd_R0-0}{1}: [radius] [22624]: (ERR): RSPE- Set Identifier Free for Re
2023/05/02 16:44:03.625116747 {smd_R0-0}{1}: [radius] [22624]: (info): Valid Response Packet, Free the
2023/05/02 16:44:03.625091040 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: authenticator 2b f4 ea
2023/05/02 16:44:03.625068520 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Received from id 1813/9
2023/05/02 16:44:03.610151863 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Started 5 sec timeout
2023/05/02 16:44:03.610097362 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Delay-Time [41
2023/05/02 16:44:03.610090044 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Event-Timestamp [55
2023/05/02 16:44:03.610085857 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Status-Type [40
2023/05/02 16:44:03.610040912 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Class [25
2023/05/02 16:44:03.610037444 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Authentic [45
2023/05/02 16:44:03.610032802 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Acct-Session-Id [44
2023/05/02 16:44:03.610028677 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Called-Station-Id [30
2023/05/02 16:44:03.610024641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Nas-Identifier [32
2023/05/02 16:44:03.610020641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Calling-Station-Id [31
2023/05/02 16:44:03.610016809 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port [5]
2023/05/02 16:44:03.610012487 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port-Type [61
2023/05/02 16:44:03.610007504 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-Port-Id [87
2023/05/02 16:44:03.610003581 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: NAS-IP-Address [4]
2023/05/02 16:44:03.609998136 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Calling-Station-Id [31
2023/05/02 16:44:03.609994109 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Called-Station-Id [30
2023/05/02 16:44:03.609989329 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Cisco AVpair [1]
2023/05/02 16:44:03.609985171 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Vendor, Cisco [26
2023/05/02 16:44:03.609981606 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Cisco AVpair [1]
2023/05/02 16:44:03.609976961 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Vendor, Cisco [26
2023/05/02 16:44:03.609969166 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: User-Name [1]
2023/05/02 16:44:03.609963241 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: authenticator 0b 99 e3
2023/05/02 16:44:03.609953614 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Send Accounting-Request
2023/05/02 16:44:03.609863172 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Handl
2023/05/02 16:44:03.609695649 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAPOL pa
2023/05/02 16:44:03.609689224 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:unknown] Pkt body
2023/05/02 16:44:03.609686794 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAP Pack
2023/05/02 16:44:03.609683919 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Sent EAP
2023/05/02 16:44:03.609334292 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Sending
2023/05/02 16:44:03.609332867 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Setting
2023/05/02 16:44:03.609310820 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Posting
2023/05/02 16:44:03.609284841 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Raisi

Esempi di traccia

In questa sezione sono incluse le tracce di gestione sessioni per i componenti dot1x e radius per una transazione completa non riuscita (il server rifiuta le credenziali del client). Il suo scopo è fornire una guida di base per navigare nelle tracce del sistema relative all'autenticazione del pannello anteriore.

- Un client di prova tenta di connettersi a Gigabit Ethernet1/0/2 ed è rifiutato.

In questo esempio, le tracce dei componenti SMD sono impostate su "debug".

```
<#root>
```

```
C9300#
```

```
set platform software trace smd sw active r0 dot1x-all
```

```
C9300#
```

```
set platform software trace smd sw active r0 radius debug
```

EAPoL: AVVIO

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12 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 1
[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: IDENTITÀ RICHIESTA EAP

```
[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 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:idle request action
```

EAPoL: RISPOSTA EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12
[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 0x0A00000E
[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: ACCESS-REQUEST

```
[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-CHALLENGE

```
[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 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: RISPOSTA EAP

```
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: ACCESS-REQUEST

```
[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 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-CHALLENGE

```
[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 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: RICHIESTA EAP

```
[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 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: RISPOSTA EAP

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on 12 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 0x0A00000E
[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: ACCESS-REQUEST

```
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 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 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: RIFIUTO DI ACCESSO

```
[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 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting authenticating state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering authc result state
[errmsg]: [16498]: UUID: 0, ra: 0 (note): %DOT1X-5-FAIL: Authentication failed for client (0040.E93E.0000:Gi1/0/2)
[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 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: held

```

EAPoL: RIFIUTO EAP

```

[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 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting FAILOVER_RETRY on Client 0x0A00000E
[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 0x0A00000E
[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

```

Ulteriori informazioni

Impostazioni predefinite

Funzionalità	Impostazione predefinita
Stato abilitazione switch 802.1x	Disabled.
Stato abilitazione 802.1x per porta	Disabilitato (autorizzazione forzata). La porta invia e riceve il traffico normale senza autenticazione

Funzionalità	Impostazione predefinita
	basata su 802.1x del client.
AAA	Disabled.
server RADIUS <ul style="list-style-type: none"> • Indirizzo IP • porta di autenticazione UDP • Porta di accounting predefinita • Chiave 	<ul style="list-style-type: none"> • Nessuno specificato. • 1645. • 1646. • Nessuno specificato.
Modalità host	Modalità host singolo.
Direzione di controllo	Controllo bidirezionale.
Riautenticazione periodica	Disabled.
Numero di secondi tra i tentativi di riautenticazione	3600 secondi.
Numero di riautenticazione	2 volte (numero di volte in cui lo switch riavvia il processo di autenticazione prima che la porta passi allo stato non autorizzato).
Periodo di silenzio	60 secondi (numero di secondi durante i quali lo switch rimane in modalità non interattiva dopo un errore nello scambio di autenticazione con il client).
Tempo di ritrasmissione	30 secondi (numero di secondi di attesa da parte dello switch per la risposta a una richiesta EAP/frame di identità prima di inviare nuovamente la richiesta).
Numero massimo di ritrasmissioni	2 volte (numero di volte in cui lo switch invia un frame di richiesta EAP/identità prima di riavviare il processo di autenticazione).

Funzionalità	Impostazione predefinita
Periodo di timeout client	30 secondi (quando si inoltra una richiesta dal server di autenticazione al client, il tempo di attesa dello switch per una risposta prima di inviare nuovamente la richiesta al client).
Periodo di timeout del server di autenticazione	30 secondi (quando si inoltra una risposta dal client al server di autenticazione, l'intervallo di tempo in cui lo switch attende una risposta prima di inviarla nuovamente al server). È possibile modificare questo periodo di timeout utilizzando il comando di configurazione dell'interfaccia server-timeout dot1x.
Timeout di inattività	Disabled.
VLAN guest	Nessuno specificato.
Bypass autenticazione inaccessibile	Disabled.
VLAN con restrizioni	Nessuno specificato.
Modalità autenticatore (switch)	Nessuno specificato.
Bypass autenticazione MAC	Disabled.
Sicurezza con riconoscimento vocale	Disabled.

Impostazioni opzionali

Riautenticazione periodica

È possibile abilitare la riautenticazione periodica del client 802.1x e specificare la frequenza con cui si verifica:

- autenticazione periodica: consente la riautenticazione periodica del client
- inattività: intervallo in secondi dopo il quale, se non vi è attività da parte del client, questa

non è autorizzata

- reauthentication: tempo in secondi trascorso il quale viene avviato un tentativo di riautenticazione automatica
- restartvalue: intervallo in secondi dopo il quale viene eseguito un tentativo di autenticazione di una porta non autorizzata
- unauthorizedvalue: intervallo in secondi dopo il quale una sessione non autorizzata viene eliminata

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

Modalità di violazione

È possibile configurare una porta 802.1x in modo che si spenga, generi un errore syslog o ignori i pacchetti da un nuovo dispositivo quando un dispositivo si connette a una porta abilitata per 802.1x o quando sulla porta è stato autenticato il numero massimo di informazioni consentite sui dispositivi.

- shutdown: errore durante la disabilitazione della porta.
- restrict: genera un errore syslog.
- protect: rilascia i pacchetti da qualsiasi nuovo dispositivo che invia il traffico alla porta.
- replace: rimuove la sessione corrente e autentica il nuovo host.

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

Modifica del periodo non interattivo

Il comando di configurazione dell'interfaccia di configurazione authentication timer restart controlla il periodo di inattività, ossia il periodo di tempo impostato in cui lo switch rimane inattivo dopo che non è in grado di autenticare il client. L'intervallo per il valore è compreso tra 1 e 65535 secondi.

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

Modifica del tempo di ritrasmissione da switch a client

Il client risponde al frame di richiesta EAP/identità dallo switch con un frame di risposta

EAP/identità. Se lo switch non riceve questa risposta, attende un determinato periodo di tempo (noto come tempo di ritrasmissione) e quindi invia nuovamente il frame.

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

Impostazione del numero di ritrasmissione del frame dal client

È possibile modificare il numero di volte in cui lo switch invia una richiesta EAP/frame di identità (presupponendo che non venga ricevuta alcuna risposta) al client prima di riavviare il processo di autenticazione. L'intervallo è compreso tra 1 e 10.

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

Configurazione della modalità host

È possibile consentire più host (client) su una porta autorizzata 802.1x.

- multi-auth: permette di usare più client autenticati sia sulla VLAN voce che sulla VLAN dati.
- multi-host: consente la presenza di più host su una porta autorizzata 802.1x dopo l'autenticazione di un singolo host.
- multidominio: consente l'autenticazione di un host e di un dispositivo voce, ad esempio un telefono IP (Cisco o non Cisco), su una porta autorizzata IEEE 802.1x.

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

Abilitazione dello spostamento MAC

Lo spostamento MAC consente a un host autenticato di spostarsi da una porta del dispositivo a un'altra.

```
authentication mac-move permit
```

Abilitazione della sostituzione MAC

La sostituzione MAC consente a un host di sostituire un host autenticato su una porta.

- protect: la porta scarta i pacchetti con indirizzi MAC imprevisti senza generare un messaggio

di sistema.

- limit - i pacchetti non conformi vengono scartati dalla CPU e viene generato un messaggio di sistema.
- shutdown - la porta viene disabilitata a causa di un errore quando riceve un indirizzo MAC imprevisto.

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

Impostazione del numero di riautenticazione

È inoltre possibile modificare il numero di volte in cui il dispositivo riavvia il processo di autenticazione prima che la porta passi allo stato non autorizzato. L'intervallo è compreso tra 0 e 10

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

Configurazione di una VLAN guest

Quando si configura una VLAN guest, i client che non sono compatibili con 802.1x vengono inseriti nella VLAN guest quando il server non riceve una risposta alla richiesta EAP o al frame di identità.

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

Configurazione di una VLAN con restrizioni

Quando si configura una VLAN con restrizioni su un dispositivo, i client conformi a IEEE 802.1x vengono spostati nella VLAN con restrizioni quando il server di autenticazione non riceve un nome utente e una password validi.

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

Configurazione del numero di tentativi di autenticazione su una VLAN con restrizioni

È possibile configurare il numero massimo di tentativi di autenticazione consentiti prima che un utente venga assegnato alla VLAN con restrizioni utilizzando il comando di configurazione

authentication event fail retry interface. L'intervallo di tentativi di autenticazione consentiti è compreso tra 1 e 3.

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

Configurazione del bypass di autenticazione inaccessibile 802.1x con VLAN voce critica

È possibile configurare una VLAN voce critica su una porta e abilitare la funzione di bypass dell'autenticazione non accessibile.

- authorization - Sposta tutti i nuovi host che tentano di eseguire l'autenticazione sulla VLAN critica specificata dall'utente
- reinitialize: sposta tutti gli host autorizzati sulla porta sulla VLAN critica specificata dall'utente

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

Configurazione dell'autenticazione 802.1x con WoL

È possibile abilitare l'autenticazione 802.1x con Wake on LAN (WoL)

```
authentication control-direction both
```

Configurazione del bypass dell'autenticazione MAC

```
mab
```

Configurazione dell'ordine di autenticazione flessibile

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

Configurazione della sicurezza 802.1x con riconoscimento vocale

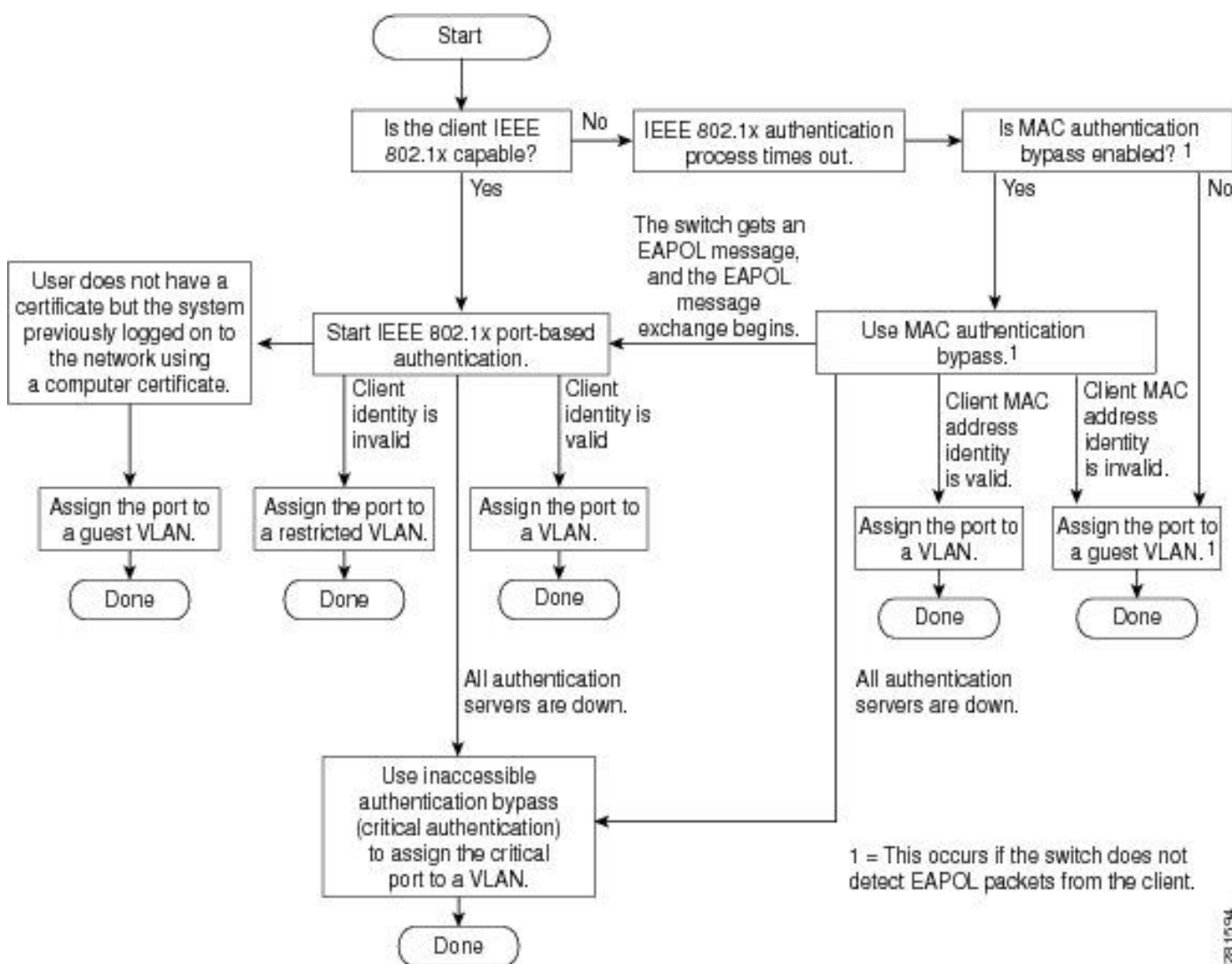
La funzione di sicurezza 802.1x con riconoscimento vocale viene usata sul dispositivo per disabilitare solo la VLAN su cui si è verificata una violazione della sicurezza, sia essa una VLAN

dati o vocale. Una violazione della sicurezza rilevata sulla VLAN dati determina la disabilitazione solo della VLAN dati. Si tratta di una configurazione globale.

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

Diagrammi di flusso

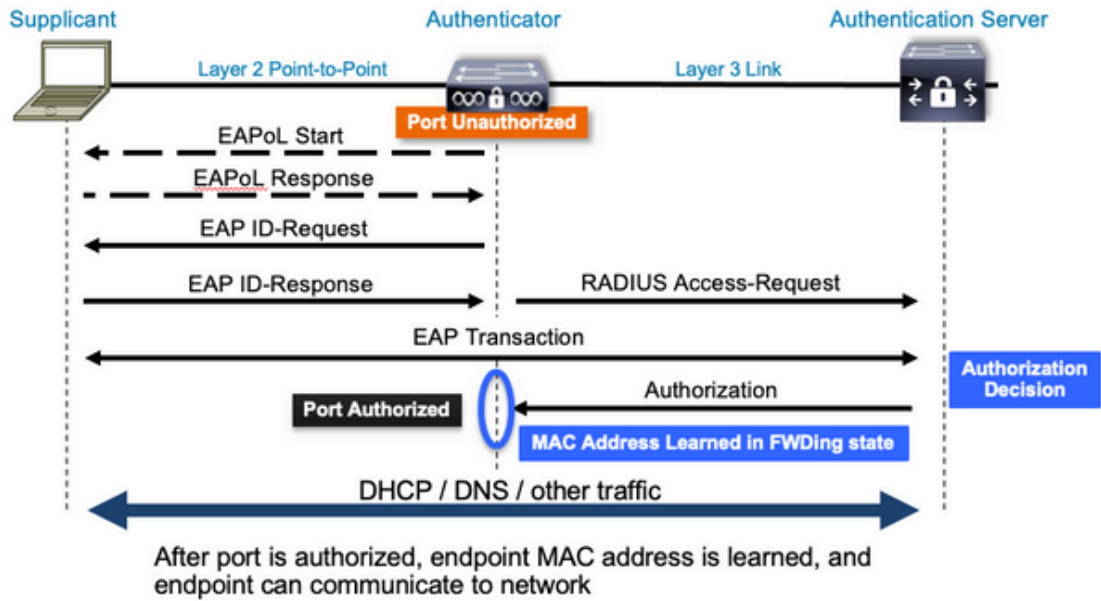
Diagramma di flusso autenticazione



Avvio dell'autenticazione basata sulla porta e scambio di messaggi

Nella figura viene illustrato lo scambio di messaggi tra client e server RADIUS.

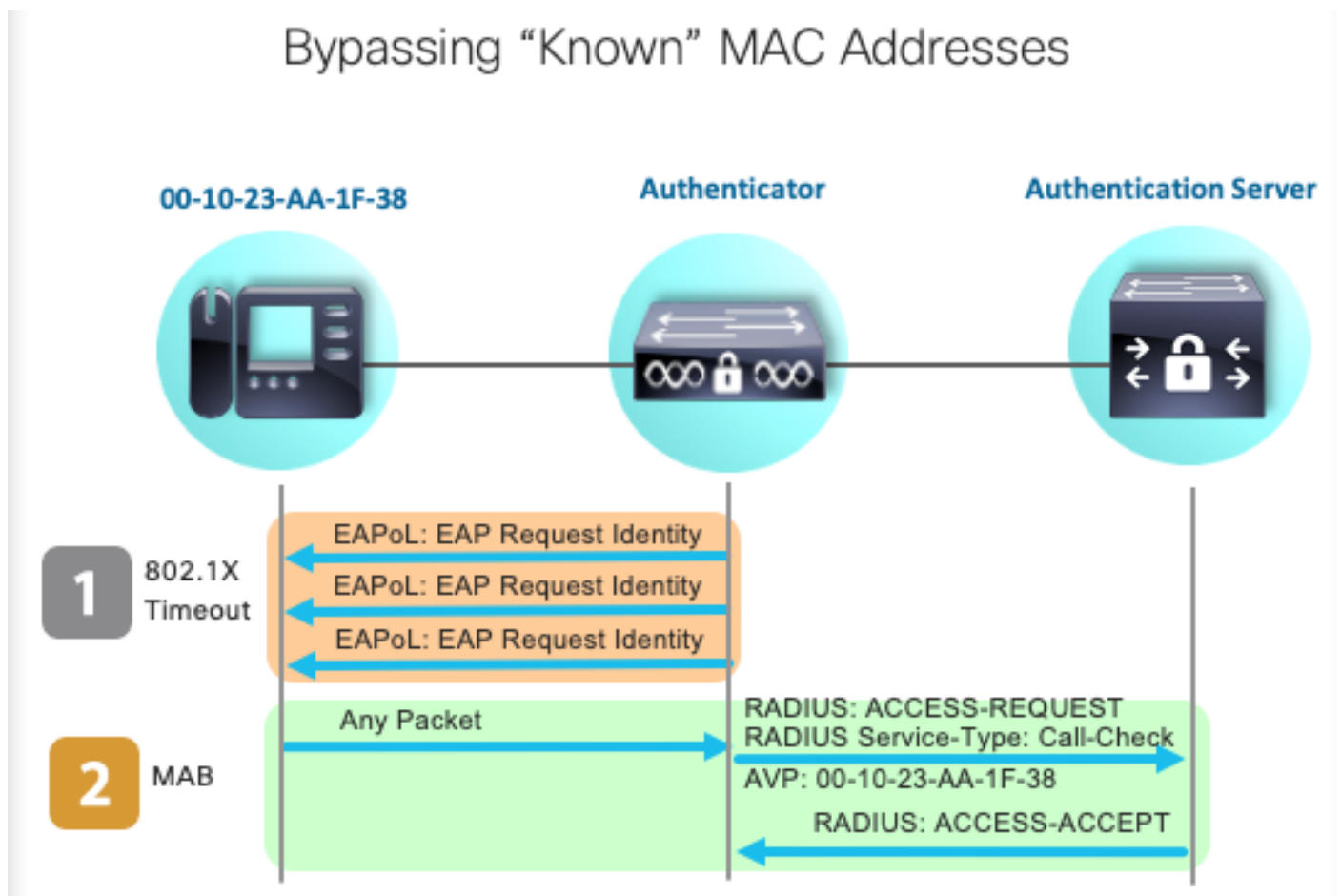
802.1X Message Exchange



Avvio dell'autenticazione MAB e scambio di messaggi

La figura mostra lo scambio di messaggi durante il bypass dell'autenticazione MAC (MAB)

Bypassing "Known" MAC Addresses



Informazioni correlate

- [Demistificazione delle configurazioni dei server RADIUS](#)
- [Guida alla distribuzione del bypass dell'autenticazione MAC](#)
- [Guida alla distribuzione di Wired 802.1x](#)
- [Catalyst 9300 SPAN Configuration Guide](#)
- [Catalyst 9300 - Guida alla configurazione di EPC](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).