

Fehlerbehebung bei Dot1x auf Catalyst Switches der Serie 9000

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Basiskonfiguration](#)

[Überprüfung von Konfiguration und Betrieb](#)

[Einführung in 802.1x](#)

[Konfiguration](#)

[Authentifizierungssitzung](#)

[Erreichbarkeit zum Authentifizierungsserver](#)

[Fehlerbehebung](#)

[Methodik](#)

[Symptome am Beispiel](#)

[Plattformspezifische Funktionen](#)

[Nachverfolgungsbeispiele](#)

[Zusätzliche Informationen](#)

[Standardeinstellungen](#)

[Optionale Einstellungen](#)

[Flussdiagramme](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie 802.1x Network Access Control (NAC) auf Switches der Serie Catalyst 9000 konfigurieren, validieren und Fehler beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen.


- Catalyst Switches der Serie 9000
- Identity Services Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x und spätere Version
- ISE-VM-K9 Version 3.0.0.458

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

 Hinweis: Informationen zu den Befehlen, die zur Aktivierung dieser Funktionen auf anderen Cisco Plattformen verwendet werden, finden Sie im entsprechenden Konfigurationsleitfaden.

Hintergrundinformationen

Der 802.1x-Standard definiert ein Client-Server-basiertes Zugriffssteuerungs- und Authentifizierungsprotokoll, das nicht autorisierte Clients daran hindert, über öffentlich zugängliche Ports eine Verbindung zu einem LAN herzustellen, sofern sie nicht ordnungsgemäß authentifiziert sind. Der Authentifizierungsserver authentifiziert jeden Client, der an einen Switch-Port angeschlossen ist, bevor er die vom Switch oder vom LAN angebotenen Dienste bereitstellt.


Die 802.1x-Authentifizierung umfasst drei verschiedene Komponenten:

Supplicant - Client, der Anmeldeinformationen zur Authentifizierung sendet

Authenticator - Das Netzwerkgerät, das die Netzwerkverbindung zwischen dem Client und dem Netzwerk bereitstellt und Netzwerkverkehr zulassen oder blockieren kann.

Authentifizierungsserver - Der Server, der Anforderungen für den Netzwerkzugriff empfangen und darauf reagieren kann, teilt dem Authentifizierer mit, ob die Verbindung zugelassen werden kann, und gibt verschiedene andere Einstellungen an, die für die Authentifizierungssitzung gelten würden.

Dieses Dokument richtet sich an Techniker und Support-Mitarbeiter, die nicht unbedingt auf die Sicherheit ausgerichtet sind. Weitere Informationen zur 802.1x Port-basierten Authentifizierung und zu Komponenten wie der ISE finden Sie im entsprechenden Konfigurationsleitfaden.

 Hinweis: Die genaueste Konfiguration der 802.1x-Standardauthentifizierung finden Sie im entsprechenden Konfigurationsleitfaden für die jeweilige Plattform und Codeversion.

Basiskonfiguration

In diesem Abschnitt wird die erforderliche Basiskonfiguration für die Implementierung der portbasierten 802.1x-Authentifizierung beschrieben. Weitere Erläuterungen zu den Funktionen finden Sie auf der Registerkarte "Addendums" (Ergänzungen) dieses Dokuments. Es gibt geringfügige Abweichungen bei den Konfigurationsstandards von Version zu Version. Validieren Sie Ihre Konfiguration anhand Ihres aktuellen Konfigurationsleitfadens.

Vor der Konfiguration der postbasierten 802.1x-Authentifizierung müssen Authentifizierung, Autorisierung und Konto (AAA) aktiviert und eine Methodenliste erstellt werden.

- Methodenlisten beschreiben die Sequenz und die Authentifizierungsmethode, die zur Authentifizierung eines Benutzers abgefragt werden müssen.
- 802.1x muss auch global aktiviert sein.

```
<#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
```

Definieren eines RADIUS-Servers auf dem 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
```

Aktivieren Sie 802.1x auf der Client-Schnittstelle.

```
<#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
```

Überprüfung von Konfiguration und Betrieb

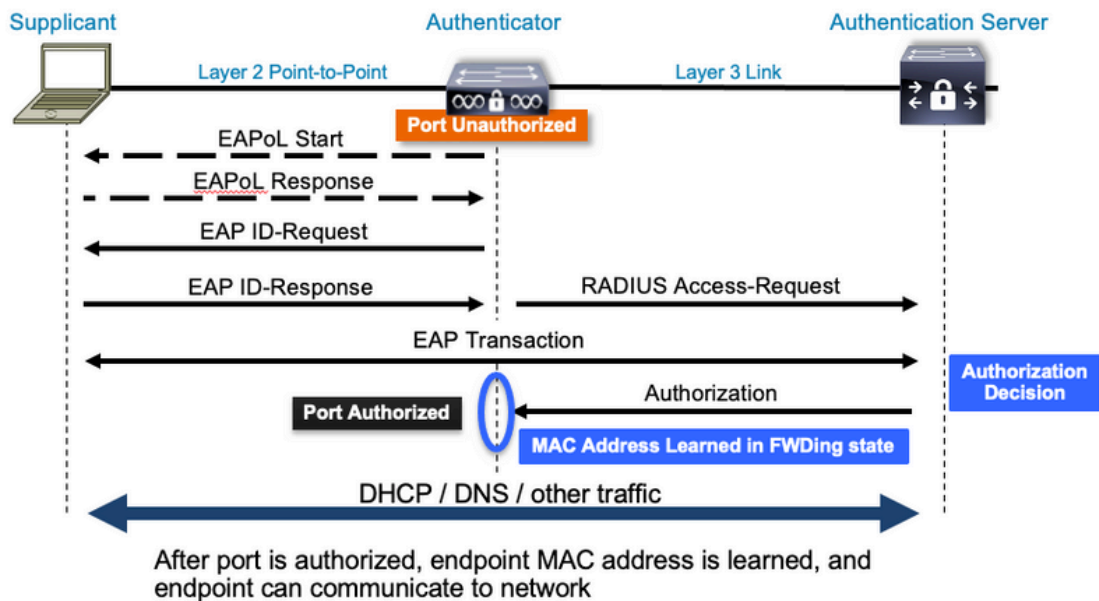
In diesem Abschnitt finden Sie Hintergrundinformationen zu 801.1x sowie Informationen zum Überprüfen der Konfiguration und des Betriebs.

Einführung in 802.1x

802.1x umfasst zwei verschiedene Arten von Datenverkehr: Datenverkehr zwischen Client und Authentifizierer (Point-to-Point) über EAPoL (Extensible Authentication Protocol over LAN) und Datenverkehr zwischen Authentifizierer und Authentifizierungsserver, der über RADIUS gekapselt wird.

Dieses Diagramm stellt den Datenfluss für eine einfache dot1x-Transaktion dar.

802.1X Message Exchange



Der Authenticator (Switch) und der Authentifizierungsserver (ISE, zum Beispiel) werden oft durch Layer 3 getrennt. RADIUS-Datenverkehr wird über das Netzwerk zwischen Authentifizierer und Server geleitet. EAPoL-Datenverkehr wird über die direkte Verbindung zwischen Supplicant (Client) und Authenticator ausgetauscht.

Beachten Sie, dass das MAC-Lernen nach der Authentifizierung und Autorisierung stattfindet.

Bei der Lösung eines 802.1x-Problems sollten Sie folgende Fragen beachten:

- Ist sie korrekt konfiguriert?
- Ist der Authentifizierungsserver erreichbar?
- Welchen Status hat der Authentifizierungs-Manager?
- Gibt es Probleme bei der Paketübermittlung zwischen Client und Authentifizierer oder zwischen Authentifizierer und Authentifizierungsserver?

Konfiguration

Einige Konfigurationen unterscheiden sich geringfügig zwischen den Hauptversionen. Plattform-/codespezifische Informationen finden Sie im entsprechenden Konfigurationsleitfaden.

AAA muss für die Verwendung von 802.1x Port-Based Authentication konfiguriert werden.

- Für "dot1x" muss eine Authentifizierungsmethodenliste erstellt werden. Dies stellt eine gängige AAA-Konfiguration dar, bei der 802.1X aktiviert ist.

```
<#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

```

Dies ist eine Beispiel-Schnittstellenkonfiguration, bei der 802.1x aktiviert ist. MAB (MAC Authentication Bypass) ist eine gängige Backup-Methode zur Authentifizierung von Clients, die keine dot1x-Suppliants unterstützen.

```
<#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

```

Bestimmen Sie, ob eine MAC-Adresse an der Schnittstelle mit "show mac address-table interface <Schnittstelle>" erfasst wird. Die Schnittstelle erhält eine MAC-Adresse erst nach erfolgreicher Authentifizierung.

```

<#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

```

Authentifizierungssitzung

Show-Befehle stehen für die Validierung der 802.1x-Authentifizierung zur Verfügung.

Verwenden Sie "show authentication sessions" oder "show authentication sessions <Schnittstelle>", um Informationen über die aktuellen Authentifizierungssitzungen anzuzeigen. In diesem Beispiel wurde nur für Te1/0/4 eine aktive Authentifizierungssitzung eingerichtet.

```

<#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 <Schnittstelle> details" (Details der Authentifizierungssitzungen anzeigen) enthält weitere Details zu einer bestimmten Schnittstellenauthentifizierungssitzung.

<#root>

C9300#

show authentication session interface tel1/0/4 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.
```

Wenn die Authentifizierung auf einer Schnittstelle aktiviert ist, aber keine aktive Sitzung vorhanden ist, wird die Liste der ausführbaren Methoden angezeigt. "Keine Sitzungen entsprechen den angegebenen Kriterien" wird ebenfalls angezeigt.

```
<#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

Wenn auf der Schnittstelle keine Authentifizierung aktiviert ist, wird auf der Schnittstelle kein Auth Manager erkannt. "Keine Sitzungen entsprechen den angegebenen Kriterien" wird ebenfalls angezeigt.

```
<#root>
```

```
C9300#
```

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

```
No sessions match supplied criteria.
```

```
No Auth Manager presence on this interface
```

Erreichbarkeit zum Authentifizierungsserver

Die Erreichbarkeit des Authentifizierungsservers ist eine Voraussetzung für eine erfolgreiche 802.1x-Authentifizierung.

Verwenden Sie "ping <server_ip>", um die Erreichbarkeit schnell zu testen. Stellen Sie sicher, dass Ihr Ping von der RADIUS-Quellschnittstelle stammt.

```
<#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
```

Der Befehl "show aaa servers" identifiziert den Serverstatus und liefert Statistiken zu Transaktionen mit allen konfigurierten AAA-Servern.

```
<#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
```

Verwenden Sie das Dienstprogramm "test aaa", um die Erreichbarkeit des Switches zum Authentifizierungsserver zu bestätigen. Beachten Sie, dass dieses Dienstprogramm veraltet ist und nicht unbegrenzt verfügbar ist.

```
<#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

```

Fehlerbehebung

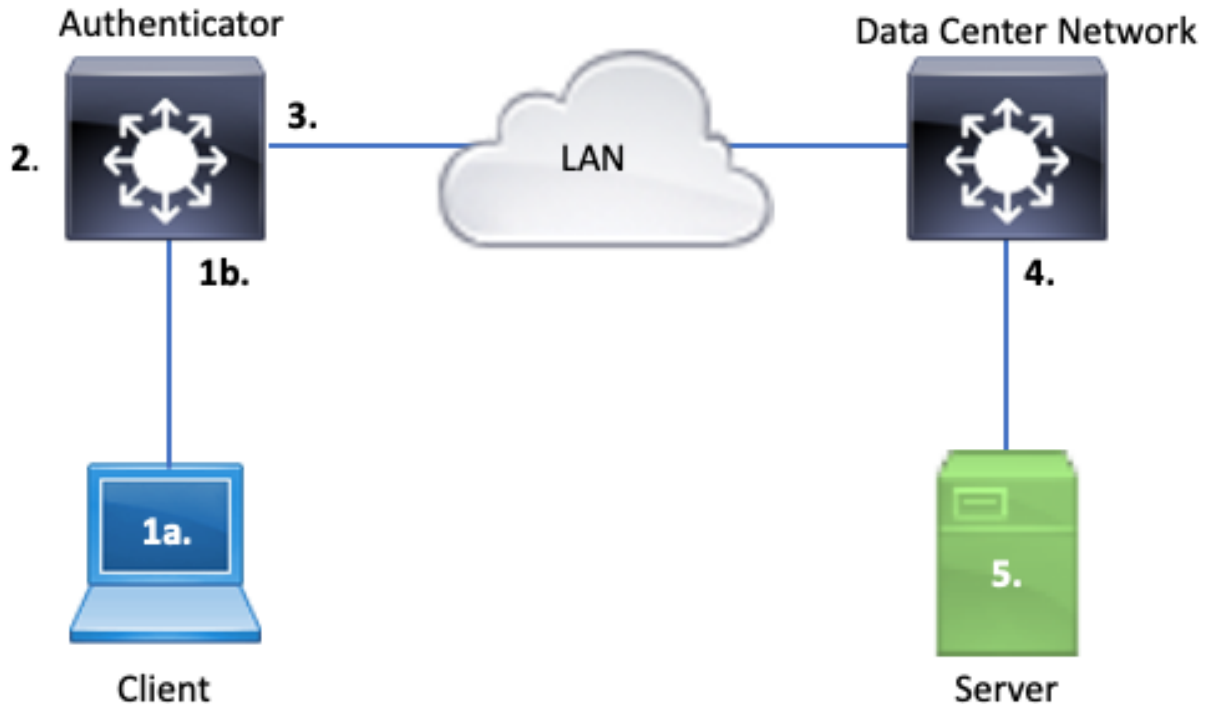
Dieser Abschnitt enthält Anleitungen zur Fehlerbehebung bei den meisten 802.1x-Problemen mit einem Catalyst Switch.

Methodik

Gehen Sie methodisch auf Probleme mit 802.1x und der Authentifizierung ein, um optimale Ergebnisse zu erzielen. Hier einige gute Fragen, die beantwortet werden sollten:

- Ist das Problem auf einen einzelnen Switch beschränkt? Ein einzelner Port? Ein einziger Client-Typ?
- Wurde die Konfiguration validiert? Ist der Authentifizierungsserver erreichbar?
- Tritt das Problem jedes Mal auf, oder tritt es nur gelegentlich auf? Tritt sie nur bei einer erneuten Authentifizierung oder einer Autorisierungsänderung auf?

Untersuchen Sie eine einzelne fehlgeschlagene Transaktion von Ende zu Ende, wenn die Probleme bestehen bleiben, nachdem das Offensichtliche ausgeschlossen wurde. Der beste und vollständigste Datensatz für die Untersuchung einer 802.1x-Transaktion von Client zu Server umfasst:



1a) Erfassung auf Client und/oder

1b) Auf der Zugriffsschnittstelle, über die der Client eine Verbindung herstellt

Dieser Bezugspunkt ist wichtig, um Einblicke in die EAPoL-Pakete zu erhalten, die zwischen dem Zugriffspoint, auf dem dot1x aktiviert ist, und dem Client ausgetauscht werden. SPAN ist das zuverlässigste Tool zum Anzeigen des Datenverkehrs zwischen Client und Authentifizierer.

2. Debugger auf Authentifizierer

Mithilfe von Debugs können wir die Transaktion über den Authentifikator hinweg verfolgen.

- Der Authentifizierer muss die empfangenen EAPoL-Pakete durchsuchen und RADIUS-gekapselten Unicast-Datenverkehr generieren, der für den Authentifizierungsserver bestimmt ist.
- Stellen Sie sicher, dass für maximale Effektivität die entsprechenden Debugging-Level festgelegt sind.

3. Erfassung neben dem Authentifikator

Diese Erfassung ermöglicht es uns, die Kommunikation zwischen Authentifizierer und Authentifizierungsserver zu sehen.

- Diese Erfassung zeigt die gesamte Konversation aus der Perspektive des Authenticators genau an.

- In Verbindung mit der Erfassung unter Punkt 4 können Sie feststellen, ob ein Verlust zwischen dem Authentifizierungsserver und dem Authentifizierer besteht.

4. Erfassung neben dem Authentifizierungsserver

Diese Erfassung ist ein Begleiter der Erfassung in Punkt 3.

- Diese Aufzeichnung bietet die gesamte Konversation aus der Sicht des Authentifizierungsservers.
- In Verbindung mit der Erfassung in Punkt 3 können Sie feststellen, ob ein Verlust zwischen Authenticator und Authentication Server besteht.

5. Erfassung, Debugging, Protokolle auf dem Authentifizierungsserver

Der letzte Teil des Puzzles, Server-Debugs sagen uns, was der Server über unsere Transaktion weiß.

- Mit diesem End-to-End-Datensatz kann ein Netzwerktechniker feststellen, wo die Transaktion abgebrochen wird, und Komponenten ausschließen, die nicht zum Problem beitragen.

Symptome am Beispiel

Dieser Abschnitt enthält eine Liste gängiger Symptome und Problemszenarien.

- Keine Antwort vom Client

Wenn der vom Switch generierte EAPoL-Datenverkehr keine Antwort auslöst, wird dieses Syslog erkannt:

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

Der Ursachencode "No Response from Client" (Keine Antwort vom Client) gibt an, dass der Switch den dot1x-Prozess gestartet hat, aber dass innerhalb der Zeitüberschreitungszeit keine Antwort vom Client empfangen wurde.

Das bedeutet, dass entweder der Client den vom Switch-Port gesendeten Authentifizierungsdatenverkehr nicht empfangen hat oder verstanden hat, oder dass die Antwort vom Client nicht am Switch-Port empfangen wurde.

- Sitzung für Client-Abbrüche

Wenn eine Authentifizierungssitzung gestartet wird, aber nicht abgeschlossen wird, meldet der Authentifizierungsserver (z. B. ISE), dass der Client eine Sitzung gestartet, die Sitzung jedoch vor dem Abschluss abgebrochen hat.

Häufig bedeutet dies, dass der Authentifizierungsprozess nur teilweise abgeschlossen werden kann.

Stellen Sie sicher, dass die gesamte Transaktion zwischen dem Authentifizierungs-Switch und dem Authentifizierungsserver als End-to-End-Transaktion bereitgestellt und vom Authentifizierungsserver korrekt interpretiert wird.

Wenn RADIUS-Datenverkehr im Netzwerk verloren geht oder in einer Weise zugestellt wird, in der er nicht ordnungsgemäß assembliert werden kann, ist die Transaktion unvollständig, und der Client versucht erneut, die Authentifizierung durchzuführen. Der Server wiederum meldet, dass der Client seine Sitzung abgebrochen hat.

- MAB-Client fällt aus DHCP/fällt zurück auf APIPA

MAC Authentication Bypass (MAB) ermöglicht die Authentifizierung auf Basis der MAC-Adresse. Häufig authentifizieren sich Clients, die keine Supplicant-Software unterstützen, über MAB.

Wenn MAB als Fallback-Methode für die Authentifizierung verwendet wird, während dot1x die bevorzugte und erste Methode ist, die auf einem Switch-Port ausgeführt wird, kann ein Szenario entstehen, in dem der Client DHCP nicht abschließen kann.

Das Problem lässt sich auf die Reihenfolge der Vorgänge zurückführen. Während dot1x ausgeführt wird, verbraucht der Switch-Port andere Pakete als EAPoL, bis entweder die Authentifizierung abgeschlossen ist oder das 1-fache der Laufzeit überschritten wird. Der Client versucht jedoch sofort, eine IP-Adresse zu erhalten, und sendet seine DHCP-Erkennungsmeldungen. Diese Erkennungsmeldungen werden vom Switch-Port verbraucht, bis dot1x seine konfigurierten Timeout-Werte überschreitet und MAB ausgeführt werden kann. Wenn die DHCP-Zeitüberschreitung des Clients kürzer als die 802.1x-Zeitüberschreitung ist, schlägt DHCP fehl, und der Client greift auf APIPA zurück, oder wie immer seine Fallback-Strategie dies vorschreibt.

Dieses Problem wird auf vielfältige Weise verhindert. bevorzugen MAB auf Schnittstellen, bei denen MAB-authentifizierte Clients eine Verbindung herstellen. Wenn dot1x zuerst ausgeführt werden muss, achten Sie auf das DHCP-Verhalten des Clients, und passen Sie die Timeoutwerte entsprechend an.

Achten Sie darauf, das Verhalten des Clients zu berücksichtigen, wenn dot1x und MAB verwendet werden. Eine gültige Konfiguration kann, wie oben beschrieben, zu einem technischen Problem führen.

Plattformspezifische Funktionen

In diesem Abschnitt werden viele der plattformspezifischen Dienstprogramme beschrieben, die für die Catalyst Switches der Serie 9000 zur Fehlerbehebung bei dot1x-Problemen verfügbar sind.

- Switch Port Analyzer (SPAN)

SPAN ermöglicht dem Benutzer die Spiegelung des Datenverkehrs von einem oder mehreren Ports zu einem Zielport zur Erfassung und Analyse. Lokales SPAN ist das zuverlässigste Erfassungsdienstprogramm.

Details zur Konfiguration und Implementierung finden Sie in diesem Konfigurationsleitfaden:

[Konfigurieren von SPAN und RSPAN, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Embedded Packet Capture (EPC)

EPC nutzt CPU- und Speicherressourcen, um integrierte lokale Paketerfassungsfunktionen bereitzustellen.

Der EPC weist Einschränkungen auf, die sich auf seine Wirksamkeit bei der Untersuchung bestimmter Probleme auswirken. Die Übertragungsraten von EPC sind auf 1.000 Pakete pro Sekunde begrenzt. EPC kann auch von der CPU injizierte Pakete am Ausgang physischer Schnittstellen nicht zuverlässig erfassen. Dies ist von Bedeutung, wenn der Schwerpunkt auf der RADIUS-Transaktion zwischen dem Authentifizierungs-Switch und dem Authentifizierungsserver liegt. Häufig übersteigt die Datenverkehrsrate an der Schnittstelle zum Server 1.000 Pakete pro Sekunde erheblich. Ein EPC am Ausgang der Schnittstelle, der zum Server zeigt, kann außerdem den vom Authentifizierungs-Switch generierten Datenverkehr nicht erfassen.

Verwenden Sie bidirektionale Zugriffslisten, um den EPC zu filtern und die Beeinträchtigung durch die Beschränkung auf 1000 Pakete pro Sekunde zu vermeiden. Wenn der RADIUS-Datenverkehr zwischen dem Authentifizierer und dem Server wichtig ist, konzentrieren Sie sich auf den Datenverkehr zwischen der RADIUS-Quellschnittstellenadresse des Authentifizierers und der Adresse des Servers.

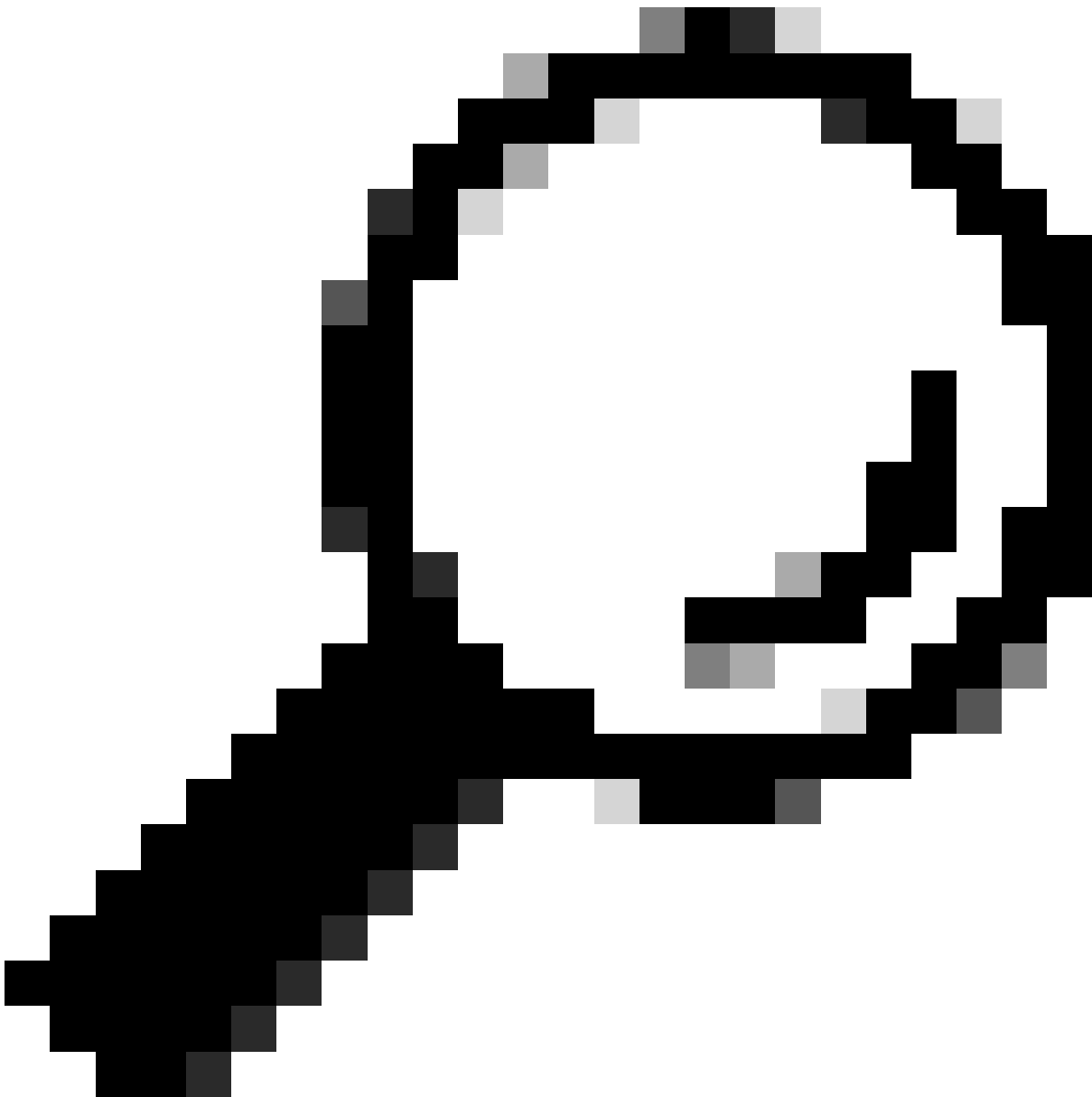
Wenn das nächste Upstream-Gerät zum Authentifizierungsserver ein Catalyst-Switch ist, verwenden Sie einen gefilterten EPC am Downlink zum Authentifizierungsserver, um die besten Ergebnisse zu erzielen.

Details zur Konfiguration und Implementierung finden Sie in diesem Konfigurationsleitfaden:

[Konfigurieren der Paketerfassung, Cisco IOS Bengaluru 17.6.x \(Catalyst 9300\)](#)

- Cisco IOS XE-Fehlerbehebung

Durch Änderungen der Softwarearchitektur, die mit Cisco IOS XE Version 16.3.2 beginnen, wurden AAA-Komponenten auf einen separaten Linux-Daemon verschoben. Bekannte Debugs ermöglichen keine sichtbaren Debugs im Protokollierungspuffer mehr. Stattdessen



Tipp: Herkömmliche IOS AAA-Debugging-Verfahren liefern keine Ausgabe mehr in Systemprotokollen zur Port-Authentifizierung an der Vorderseite im Syslog-Puffer.

Diese klassischen Cisco IOS-Debugging-Funktionen für dot1x und RADIUS ermöglichen keine sichtbaren Debugging-Funktionen mehr im Protokollpuffer des Switches:

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

Auf AAA-Komponentendebugs kann jetzt über die Systemüberwachung unter dem SMD (Session Manager Daemon) zugegriffen werden.

- Wie bei herkömmlichen Syslogs erfolgt der Catalyst System-Traces-Bericht auf einer Standardebene, und es muss eine Anweisung zum Sammeln detaillierterer Protokolle gegeben werden.
- Ändern Sie mit dem Befehl "set platform software trace smd switch active r0 <component> debug" die Routine-Ablaufverfolgungsebene für die gewünschte Unterkomponente.

```
<#root>
```

```
Switch#
```

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

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

Diese Tabelle ordnet herkömmliche IOS-Debugs ihrer Ablaufverfolgungsentsprechung zu.

Befehl im alten Stil	Befehl New style
#debug Radius	#set platform software trace smd switch active R0 radius debug
#debug dot1x alle	#set platform software trace smd switch active R0 dot1x-all debug
#debug für Zugriffssitzung alle	#set platform software trace smd switch active R0 auth-mgr-all debug
#debug epm all	#set platform software trace smd switch active R0 epm-all debug

Bei klassischen Debugs werden alle zugehörigen Komponentenverfolgungen auf die Ebene "debug" gesetzt. Plattformbefehle werden auch verwendet, um bei Bedarf bestimmte Ablaufverfolgungen zu aktivieren.

Verwenden Sie den Befehl "show platform software trace level smd switch active R0", um die aktuelle Trace-Ebene für SMD-Unterkomponenten anzuzeigen.

```
<#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>
```

Die Ablaufverfolgungsebene der Unterkomponenten kann auf zwei Arten auf den Standardwert zurückgesetzt werden.

- Verwenden Sie entweder "underbug all" oder "set platform software trace smd switch active R0 <sub-component> notice", um die Wiederherstellung durchzuführen.
- Wenn das Gerät neu geladen wird, werden auch die Ablaufverfolgungsebenen auf den Standard zurückgesetzt.

```
<#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.
```

Komponentenprotokolle können auf der Konsole angezeigt oder in das Archiv geschrieben und offline angezeigt werden. Traces werden in ZIP-Binärarchiven archiviert, die dekodiert werden müssen. Wenden Sie sich an das TAC, um Unterstützung beim Debuggen beim Umgang mit archivierten Traces zu erhalten. In diesem Workflow wird erläutert, wie die Ablaufverfolgungen in der CLI angezeigt werden.

Verwenden Sie den Befehl "show platform software trace message smd switch active R0", um die im Speicher für die SMD-Komponente gespeicherten Ablaufverfolgungsprotokolle anzuzeigen.

```
<#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>

```

Die Ausgabe ist ausführlich, daher ist es nützlich, die Ausgabe in eine Datei umzuleiten.

- Die Datei kann entweder mithilfe des Dienstprogramms "mehr" über die CLI gelesen oder zur Anzeige im Texteditor offline verschoben werden.

```
<#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" ist das aktualisierte Programm für Traces und den Standard in der Version Cisco IOS XE 17.9.x und höher.

<#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" bietet die gleiche Funktionalität wie "show platform software trace" in einem eleganteren und zugänglicheren Format.

<#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
```

Nachverfolgungsbeispiele

Dieser Abschnitt enthält Ablaufverfolgungen des Sitzungs-Managers für Punkt1x- und Radius-Komponenten für eine vollständige, fehlgeschlagene Transaktion (der Server lehnt Client-Anmeldeinformationen ab). Es soll eine grundlegende Richtlinie für die Navigation in System-Traces im Zusammenhang mit der Authentifizierung an der Vorderseite bereitstellen.

- Ein Test-Client versucht, eine Verbindung mit GigabitEthernet1/0/2 herzustellen, und wird abgelehnt.

In diesem Beispiel werden SMD-Komponentenverfolgungen auf "debug" gesetzt.

```
<#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 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: EAP-ANFORDERUNGS-IDENTITÄT

```
[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: EAP-ANTWORT

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on I2
[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: ZUGRIFF - HERAUSFORDERUNG

```
[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: EAP-ANTWORT

```
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: ZUGRIFF - HERAUSFORDERUNG

```
[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: EAP-ANFRAGE

```
[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: EAP-ANTWORT

```
[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 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: ZUGRIFF ABGELEHNT

```
[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: EAP-ABLEHNUNG

```

[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

```

Zusätzliche Informationen

Standardeinstellungen

Funktion	Standardeinstellung
Switch 802.1x-Aktivierungsstatus	Deaktiviert.

Funktion	Standardeinstellung
802.1x-Aktivierungsstatus pro Port	Deaktiviert (zwangsweise genehmigt). Der Port sendet und empfängt normalen Datenverkehr ohne 802.1x-basierte Authentifizierung des Clients.
AAA	Deaktiviert.
RADIUS-Server <ul style="list-style-type: none"> • IP-Adresse • UDP-Authentifizierungsport • Standard-Accounting-Port • Wichtigste 	<ul style="list-style-type: none"> • Keine angegeben. • 1645. • 1646. • Keine angegeben.
Host-Modus	Single-Host-Modus.
Steuerrichtung	Bidirektionale Steuerung.
Periodische erneute Authentifizierung	Deaktiviert.
Anzahl der Sekunden zwischen erneuten Authentifizierungsversuchen	3600 Sekunden.
Nummer für erneute Authentifizierung	2 Mal (Anzahl der Male, die der Switch den Authentifizierungsprozess neu startet, bevor der Port in den nicht autorisierten Status wechselt).
Ruhezeit	60 Sekunden (Anzahl der Sekunden, die der Switch nach einem fehlgeschlagenen Authentifizierungsaustausch mit dem Client im Ruhezustand bleibt).
Übertragungszeit	30 Sekunden (die Anzahl der Sekunden, die der Switch auf eine Antwort auf eine EAP-Anfrage/einen EAP-Identitäts-Frame vom Client wartet, bevor er die Anfrage erneut

Funktion	Standardeinstellung
	sendet).
Maximale Anzahl der erneuten Übertragungen	2 Mal (Anzahl der Male, die der Switch eine EAP-Anfrage/einen Identitäts-Frame sendet, bevor der Authentifizierungsprozess neu gestartet wird).
Client-Zeitüberschreitungszeitraum	30 Sekunden (beim Weiterleiten einer Anforderung vom Authentifizierungsserver an den Client die Zeit, die der Switch auf eine Antwort wartet, bevor er die Anforderung an den Client erneut sendet).
Timeout-Zeitraum für Authentifizierungsserver	30 Sekunden (beim Weiterleiten einer Antwort vom Client an den Authentifizierungsserver die Zeit, die der Switch auf eine Antwort wartet, bevor er die Antwort an den Server zurücksendet). Sie können diese Zeitüberschreitung mit dem Befehl <code>dot1x timeout server-timeout interface configuration</code> ändern.
Timeout bei Inaktivität	Deaktiviert.
Gast-VLAN	Keine angegeben.
Unzugängliche Authentifizierungsumgehung	Deaktiviert.
Eingeschränktes VLAN	Keine angegeben.
Authentifizierer-Modus (Switch)	Keine angegeben.
Umgehung der MAC-Authentifizierung	Deaktiviert.
Sprachbasierte Sicherheit	Deaktiviert.

Optionale Einstellungen

Periodische erneute Authentifizierung

Sie können die regelmäßige 802.1x-Client-Neuauthentifizierung aktivieren und angeben, wie oft diese auftritt:

- Authentifizierung periodisch - ermöglicht eine regelmäßige erneute Authentifizierung des Clients
- Inaktivität - Intervall in Sekunden, nach dem der Client nicht autorisiert wird, wenn keine Aktivität vom Client vorliegt
- reauthentication - Zeit in Sekunden, nach der ein automatischer Versuch zur erneuten Authentifizierung initiiert wird
- restartvalue - Intervall in Sekunden, nach dem versucht wird, einen nicht autorisierten Port zu authentifizieren.
- unauthorizedValue - Intervall in Sekunden, nach dem eine nicht autorisierte Sitzung gelöscht wird

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

Verletzungsmodi

Sie können einen 802.1x-Port so konfigurieren, dass er heruntergefahren wird, einen Syslog-Fehler generiert oder Pakete von einem neuen Gerät verwirft, wenn ein Gerät eine Verbindung mit einem 802.1x-fähigen Port herstellt oder die maximale Anzahl von Geräten, die über Geräte authentifiziert wurden, auf dem Port authentifiziert wurde.

- shutdown - Fehler beim Deaktivieren des Ports.
- restricted: Generiert einen Syslog-Fehler.
- protect - Verwirft Pakete von jedem neuen Gerät, das Datenverkehr an den Port sendet.
- replace- Entfernt die aktuelle Sitzung und authentifiziert sich mit dem neuen Host.

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

Ändern der Ruhezeit

Der Schnittstellenkonfigurationsbefehl `authentication timer restart` steuert den Leerlaufzeitraum, der den festgelegten Zeitraum vorgibt, in dem der Switch im Leerlauf bleibt, nachdem ein Switch den Client nicht authentifizieren kann. Der Bereich für den Wert liegt zwischen 1 und 65535

Sekunden.

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

Ändern der Zeit für die erneute Switch-to-Client-Übertragung

Der Client antwortet auf den EAP-Anforderungs-/Identitäts-Frame vom Switch mit einem EAP-Antwort-/Identitäts-Frame. Wenn der Switch diese Antwort nicht erhält, wartet er einen festgelegten Zeitraum (die so genannte Zeit für die erneute Übertragung) und sendet dann den Frame erneut.

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

Einstellen der Frame-Retransmission-Nummer des Switch-to-Client

Sie können vor dem Neustart des Authentifizierungsprozesses ändern, wie oft der Switch eine EAP-Anforderung/einen Identitäts-Frame an den Client sendet (vorausgesetzt, es wird keine Antwort empfangen). Der Bereich liegt zwischen 1 und 10.

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

Konfigurieren des Hostmodus

Sie können mehrere Hosts (Clients) auf einem autorisierten 802.1x-Port zulassen.

- multi-auth: Mehrere authentifizierte Clients im Sprach-VLAN und Daten-VLAN zulassen.
- multi-host - Mehrere Hosts auf einem 802.1x-autorisierten Port zulassen, nachdem ein einzelner Host authentifziert wurde.
- multi-domain: Ermöglicht die Authentifizierung sowohl eines Hosts als auch eines Sprachgeräts, z. B. eines IP-Telefons (von Cisco oder einem Drittanbieter), an einem nach IEEE 802.1x autorisierten Port.

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

Aktivieren von MAC Move

MAC-Verschiebungen ermöglichen es authentifizierten Hosts, sich von einem Port auf dem Gerät zu einem anderen zu bewegen.

```
authentication mac-move permit
```

Aktivieren des MAC-Ersatzes

Mit MAC Replace kann ein Host einen authentifizierten Host an einem Port ersetzen.

- `protect` - Der Port verwirft Pakete mit unerwarteten MAC-Adressen, ohne eine Systemmeldung zu generieren.
- `restricted` - Pakete, die die Anforderungen verletzen, werden von der CPU verworfen, und es wird eine Systemmeldung generiert.
- `shutdown` - Der Port wird aufgrund eines Fehlers deaktiviert, wenn er eine unerwartete MAC-Adresse empfängt.

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

Festlegen der Nummer für die erneute Authentifizierung

Sie können auch ändern, wie oft das Gerät den Authentifizierungsprozess neu startet, bevor der Port in den nicht autorisierten Status wechselt. Der Bereich liegt zwischen 0 und 10

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

Konfigurieren eines Gast-VLAN

Wenn Sie ein Gast-VLAN konfigurieren, werden Clients, die nicht 802.1x-fähig sind, in das Gast-VLAN eingefügt, wenn der Server keine Antwort auf seine EAP-Anforderung/seinen Identitäts-Frame erhält.

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

Konfigurieren eines eingeschränkten VLAN

Wenn Sie ein eingeschränktes VLAN auf einem Gerät konfigurieren, werden Clients, die IEEE

802.1x-kompatibel sind, in das eingeschränkte VLAN verschoben, wenn der Authentifizierungsserver keinen gültigen Benutzernamen und kein gültiges Kennwort erhält.

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

Konfigurieren der Anzahl von Authentifizierungsversuchen in einem eingeschränkten VLAN

Sie können die maximale Anzahl von Authentifizierungsversuchen konfigurieren, die zulässig sind, bevor ein Benutzer dem eingeschränkten VLAN zugewiesen wird. Verwenden Sie dazu den Konfigurationsbefehl `authentication event fail retry count`interface. Der Bereich der zulässigen Authentifizierungsversuche liegt zwischen 1 und 3.

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

Konfigurieren des nicht zugänglichen 802.1x-Authentifizierungs-Bypasses mit kritischem Sprach-VLAN

Sie können ein kritisches Sprach-VLAN an einem Port konfigurieren und die Funktion zur Umgehung der nicht zugänglichen Authentifizierung aktivieren.

- `Authorize` - Verschieben Sie alle neuen Hosts, die eine Authentifizierung versuchen, in das benutzerspezifische kritische VLAN
- `reinitialize`: Verschieben Sie alle autorisierten Hosts auf dem Port in das vom Benutzer angegebene kritische VLAN.

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

Konfigurieren der 802.1x-Authentifizierung mit WoL

Sie können die 802.1x-Authentifizierung mit Wake on LAN (WoL) aktivieren.

```
authentication control-direction both
```

Konfigurieren der MAC-Authentifizierungsumgehung

```
mab
```

Konfiguration der flexiblen Authentifizierungsreihenfolge

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

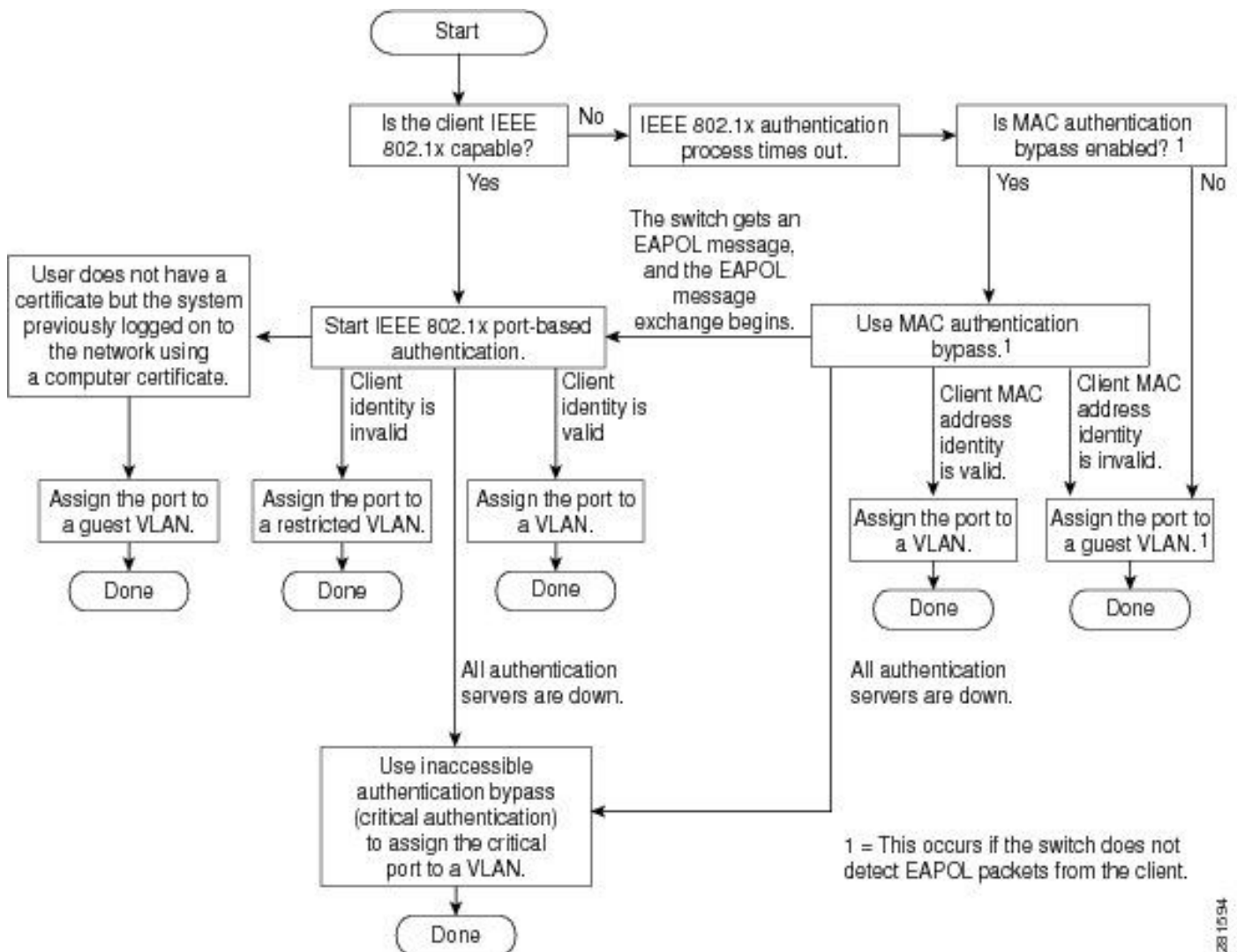
Konfigurieren der sprachbasierten 802.1x-Sicherheit

Sie verwenden die sprachbasierte 802.1x-Sicherheitsfunktion auf dem Gerät, um nur das VLAN zu deaktivieren, in dem eine Sicherheitsverletzung auftritt, unabhängig davon, ob es sich um ein Daten- oder Sprach-VLAN handelt. Eine im Daten-VLAN festgestellte Sicherheitsverletzung führt dazu, dass nur das Daten-VLAN heruntergefahren wird. Dies ist eine globale Konfiguration.

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

Flussdiagramme

Authentifizierungs-Flussdiagramm

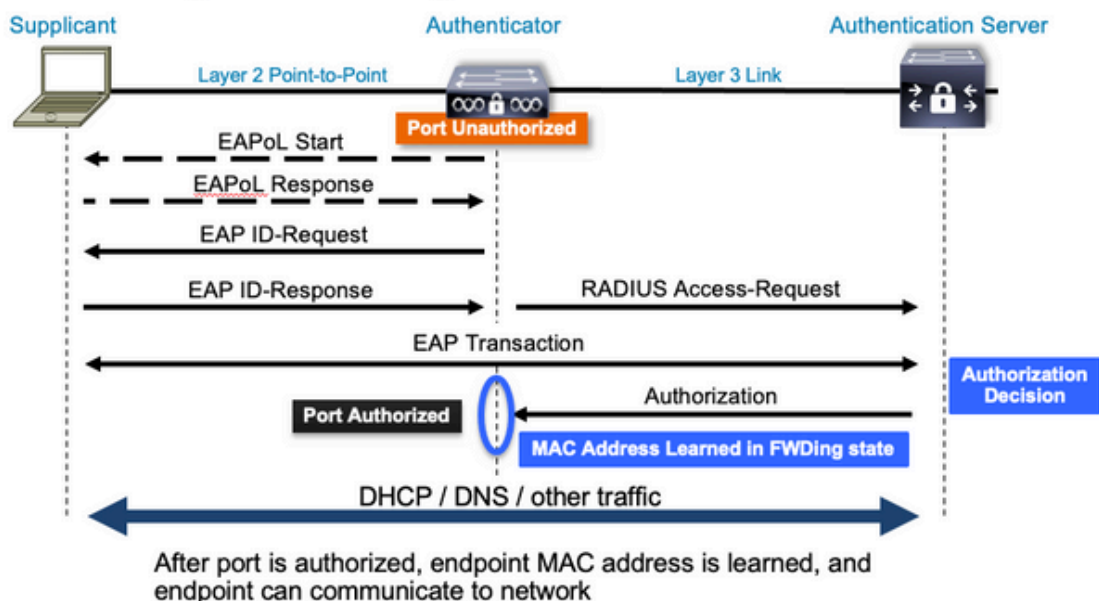


28 1594

Portbasierte Authentifizierungsinitiierung und Nachrichtenaustausch

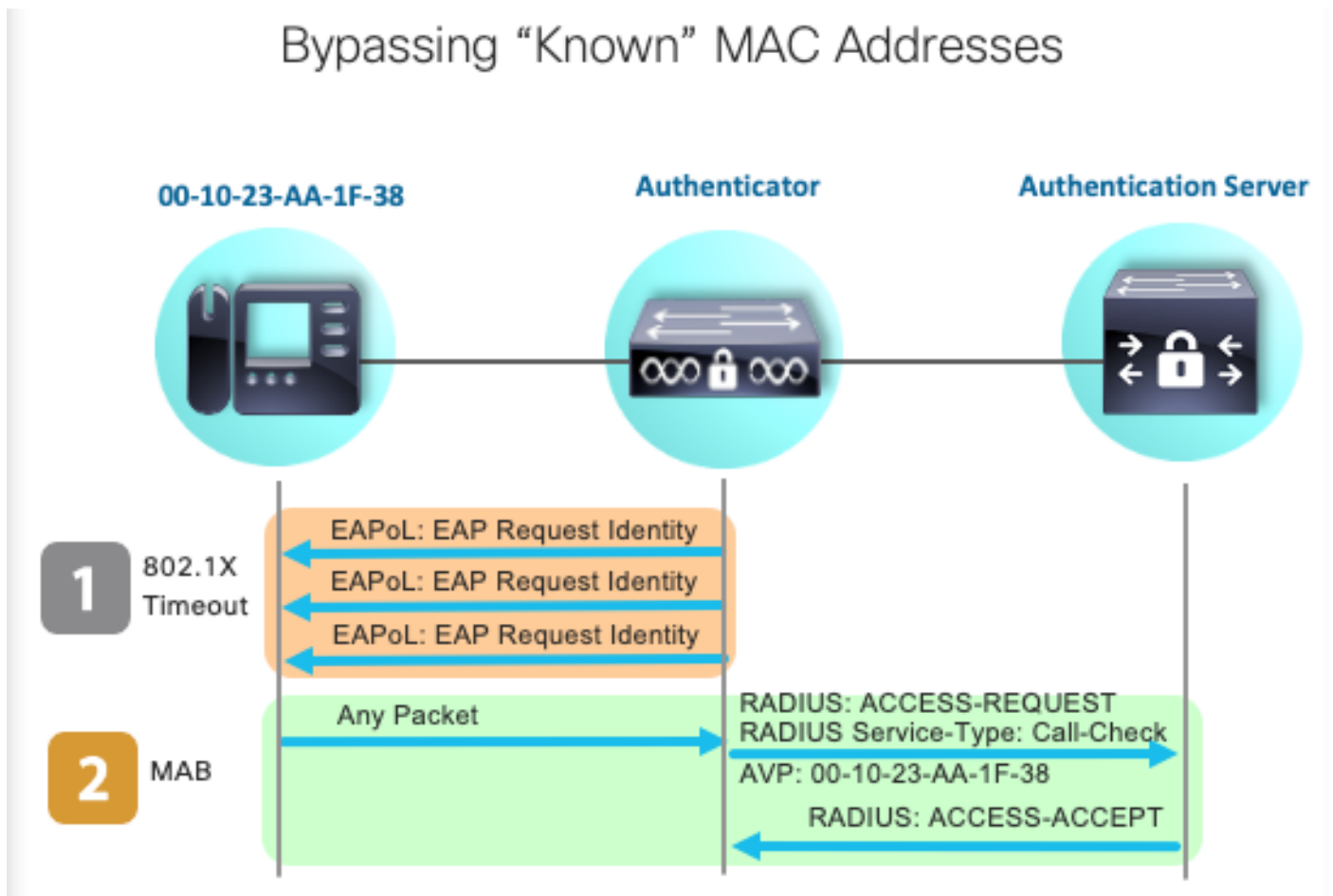
Diese Abbildung zeigt den Client, der den Nachrichtenaustausch mit dem RADIUS-Server initiiert.

802.1X Message Exchange



Initiierung der MAB-Authentifizierung und Nachrichtenaustausch

Diese Abbildung zeigt den Nachrichtenaustausch während des MAC Authentication Bypass (MAB).



Zugehörige Informationen

- [RADIUS-Serverkonfigurationen entmystifizieren](#)
- [Bereitstellungsleitfaden für MAC Authentication Bypass](#)
- [Bereitstellungsleitfaden für kabelgebundene 802.1x-Netzwerke](#)
- [Catalyst 9300 SPAN - Konfigurationsleitfaden](#)
- [Catalyst 9300 EPC - Konfigurationsleitfaden](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.