# 身分型網路服務(IBNS)2.0疑難排解

## 目錄

## 簡介

本檔案介紹對使用身分型網路服務(IBNS)2.0的交換器上的驗證進行疑難排解的程式

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 身分識別服務引擎(ISE)
- IEEE 802.1X概念(dot1X)
- MAC Authentication Bypass(MAB)

### 採用元件

本檔案中的資訊是根據以下軟體和硬體版本，但不限於：

- Cisco交換器 — C3750X-48PF-S(含IOS 15.2.1E3(ED)
- 身分識別服務引擎2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

IBNS 2.0是一個新的策略引擎，取代了傳統的身份驗證管理器。它配備了一組增強功能，可通過思科通用分類策略語言(C3PL)提供靈活的配置。 IBNS 2.0現在稱為訪問會話管理器，它讓管理員可以

根據特定條件和終端事件配置策略和操作。C3PL用於定義身份驗證條件、引數和操作，而不是常規條件。有關IBNS 2.0的更多資訊，請訪問相關資訊部分中提供的連結。

有不同型別的策略對映用於各種用途。本段重點介紹使用者型別。策略對映中有三個部分需要注意。

- 事件部分
- Class部分
- 操作部分

它們遵循層次**事件>類>操作。**當策略對映應用於介面時，將評估策略對映中定義的所有事件。根據當前事件，在策略對映中定義的適當操作在介面級別應用。

一旦匹配了事件，就會有一個選項可以根據身份驗證/授權的事件/方法/結果評估類。這些類的結果可以是**ALWAYS EXECUTE**，也可以在其他類對映中呼叫。

在「操作」部分中，可以包含的重要操作包括：

- 指定具有優先順序的身份驗證方法

```
 event session-started match-all
  10 class do-until-failure 10 authenticate using priority
```

- 為特定身份驗證方法指定身份驗證方法清單

```
event session-started match-all
  10 class do-until-failure 10 authenticate using aaa authc-list
```

- 為身份驗證方法指定授權方法清單

```
event session-started match-all
  10 class do-until-failure 10 authenticate using aaa authz-list
```

- 指定重試次數

```
event session-started match-all
  10 class do-until-failure 10 authenticate using retries
```

- 用新的身份驗證/授權資料替換現有的身份驗證/授權資料

```
event timer-expiry match-all
  10 class do-until-failure 10 authenticate using replace aaa
```

- 強制授權

```
event session-started match-all
  10 class do-until-failure 10 authorize
```

- 強製取消授權

```
event timer-expiry match-all
  10 class do-until-failure 10 unauthorize
```

- 啟用服務模板

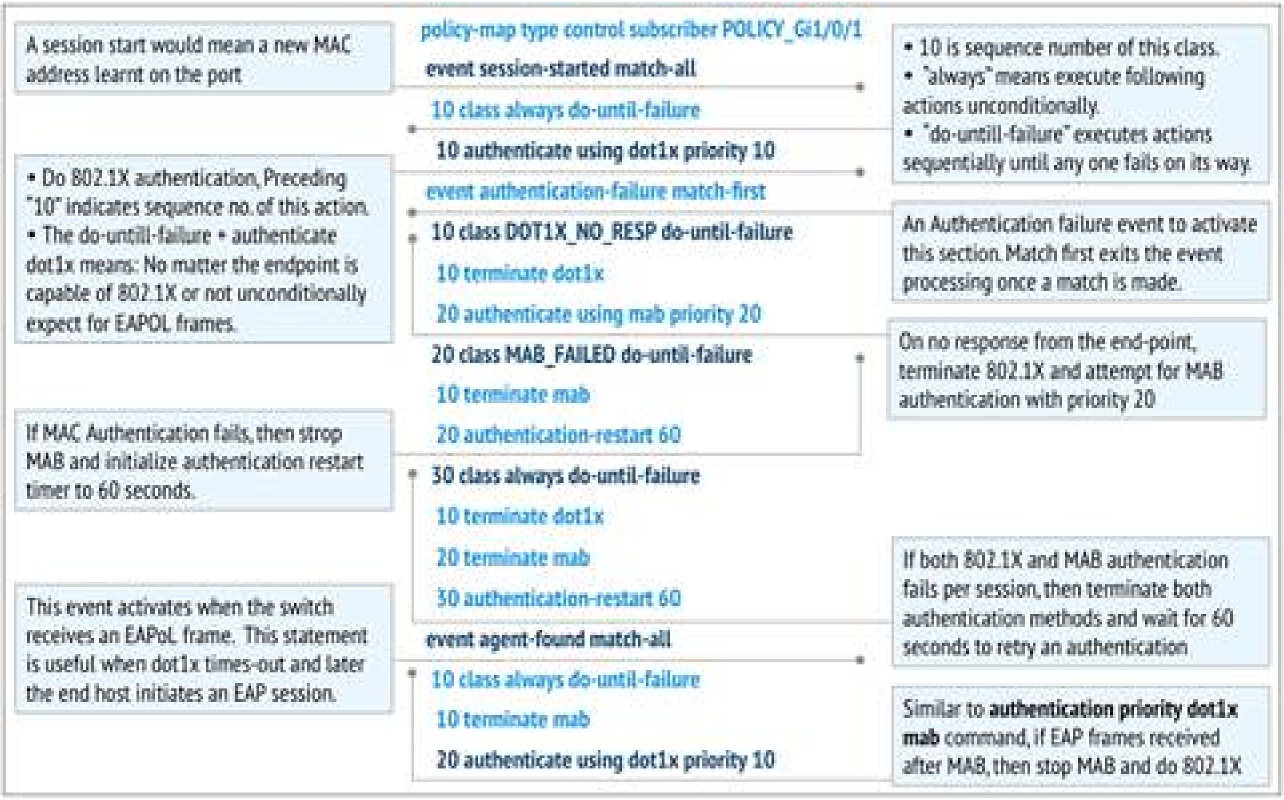
```
    event timer-expiry match-all
      10 class do-until-failure 10 activate service-template
```

在傳統IOS交換機中，沒有選項可以應用特定於已驗證會話的方法清單。IBNS 2.0使用服務模板提供此功能。服務模板在交換機上本地配置，並在成功後應用會話授權。還有一個選項可以從AAA伺服器推送所需的服務模板。

用於相同操作的radius屬性是*subscriber:service-name = <服務模板的名稱>。在身份服務引擎*(ISE)中，可以命名授權配置檔案與交換機上配置的本地服務模板完全相同，並選中*Service Template*覈取方塊。此授權配置檔案以及任何其他授權配置檔案都可以作為授權結果推送。

在授權結果報告中，有一個名為*subscriber:service-name = <服務模板名稱>*的Cisco-AV配對。這表示已通知交換機為該會話應用該服務模板。

下圖顯示了示例策略對映的每個實體的確切含義。



```
policy-map type control subscriber POLICY_Gi1/0/1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  30 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
```

A session start would mean a new MAC address learnt on the port

- Do 802.1X authentication, Preceding "10" indicates sequence no. of this action.
- The do-untill-failure • authenticate dot1x means: No matter the endpoint is capable of 802.1X or not unconditionally expect for EAPOL frames.

If MAC Authentication fails, then strop MAB and initialize authentication restart timer to 60 seconds.

This event activates when the switch receives an EAPoL frame. This statement is useful when dot1x times-out and later the end host initiates an EAP session.

- 10 is sequence number of this class.
- "always" means execute following actions unconditionally.
- "do-untill-failure" executes actions sequentially until any one fails on its way.

An Authentication failure event to activate this section. Match first exits the event processing once a match is made.

On no response from the end-point, terminate 802.1X and attempt for MAB authentication with priority 20

If both 802.1X and MAB authentication fails per session, then terminate both authentication methods and wait for 60 seconds to retry an authentication

Similar to **authentication priority dot1x mab** command, if EAP frames received after MAB, then stop MAB and do 802.1X

# 設定

## AAA配置

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
aaa session-id common

dot1x system-auth-control
```

## RADIUS伺服器配置

```
radius server ise
 address ipv4 X.X.X.X auth-port 1812 acct-port 1813
 automate-tester username probe-user
 key XXXXXXXXXX
```

### 策略對映配置

```
policy-map type control subscriber Inter_Gi_3/0/48
 event session-started match-all          //On session-start event 10 class always do-until-
failure //Both mab and dot1x start at the same time 10 authenticate using dot1x priority 10 20
authenticate using mab priority 20 event authentication-failure match-first //On authentication
event failure 10 class DOT1X_NO_RESP do-until-failure //If dot1x fails 10 terminate dot1x 20
authenticate using mab priority 20 20 class MAB_FAILED do-until-failure //If mab fails 10
terminate mab 20 authentication-restart 60 30 class always do-until-failure //If both mab and
dot1x fail 10 terminate dot1x 20 terminate mab 30 authentication-restart 60 event agent-found
match-all //On dot1x agent found event 10 class always do-until-failure 10 terminate mab 20
authenticate using dot1x priority 10
```

### 類對映配置

```
class-map type control subscriber match-all DOT1X_NO_RESP //If dot1x and no response from client
match method dot1x match result-type method dot1x agent-not-found
class-map type control subscriber match-all MAB_FAILED //On mab failure match method mab match
result-type method mab authoritative
```

### 介面配置

```
interface GigabitEthernet3/0/48
 description ** Access Port **
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 10
 ip access-group IPV4-PRE-AUTH-ACL in
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber Inter_Gi_3/0/48
```

# 疑難排解

最佳故障排除方法是比較工作日誌和非工作日誌。這樣，就知道該過程出錯的確切步驟。需要啟用一些調試才能解決mab/dot1x問題。以下是啟用這些調試的命令。

- debug aaa authentication
- debug aaa authorization
- debug mab all
- debug dot1x all
- debug radius

以下是同時啟用dot1x和mab的工作日誌。

### debug mab all

```
mab-ev: [28d2.4496.5376, Gi3/0/48] Received MAB context create from AuthMgr // New mac-address
detected mab-ev: MAB authorizing 28d2.4496.5376 //mab authorization event should start mab-ev:
Created MAB client context 0xB0000001 mab : initial state mab_initialize has enter //Initialize
mab mab-ev: [28d2.4496.5376, Gi3/0/48] Sending create new context event to EAP from MAB for
0xB0000001 (28d2.4496.5376) mab-ev: [28d2.4496.5376, Gi3/0/48] MAB authentication started for
0x0782A870 (28d2.4496.5376) //mab authentication initialized %AUTHMGR-5-START: Starting 'mab'
for client (28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID 0A6A258E0000003300C586C2 mab-
ev: [28d2.4496.5376, Gi3/0/48] Invalid EVT 9 from EAP mab-sm: [28d2.4496.5376, Gi3/0/48]
Received event 'MAB_CONTINUE' on handle 0xB0000001 mab : during state mab_initialize, got event
1(mabContinue) @@@ mab : mab_initialize -> mab_authorizing //mab authorizing event started mab-
ev: [28d2.4496.5376] formatted mac = 28d244965376 //mac-address formatted as required mab-ev:
[28d2.4496.5376] created mab pseudo dot1x profile dot1x_mac_auth_28d2.4496.5376 //peuso dot1x
profile formed (username=macaddress) mab-ev: [28d2.4496.5376, Gi3/0/48] Starting MAC-AUTH-BYPASS
for 0xB0000001 (28d2.4496.5376) //starting mab authentication mab-ev: [28d2.4496.5376, Gi3/0/48]
Invalid EVT 9 from EAP mab-ev: [28d2.4496.5376, Gi3/0/48] MAB received an Access-Accept for
0xB0000001 (28d2.4496.5376) //received mab success from the server %MAB-5-SUCCESS:
Authentication successful for client (28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID
0A6A258E0000003300C586C2 mab-sm: [28d2.4496.5376, Gi3/0/48] Received event 'MAB_RESULT' on
handle 0xB0000001 // mab authorization result received mab : during state mab_authorizing, got
event 5(mabResult) @@@ mab : mab_authorizing -> mab_terminate //mab authorization process
terminate mab-ev: [28d2.4496.5376, Gi3/0/48] Deleted credentials profile for 0xB0000001
(dot1x_mac_auth_28d2.4496.5376) //deleted pseudo dot1x profile %AUTHMGR-5-SUCCESS: Authorization
succeeded for client (28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID
0A6A258E0000003300C586C2 // posting mab authorization succeeded
```

## debug dot1x all

由於dot1x由於協定協商、證書交換等原因而具有大量的消息交換，因此這裡並沒有提到所有的調試日誌。此處記錄了事件按照發生順序的流程以及相應的調試日誌。

```
dot1x-packet:EAPOL pak rx - Ver: 0x1  type: 0x1 // Initial EAPoL packet received by switch
dot1x-packet: length: 0x0000 dot1x-ev:[28d2.4496.5376, Gi3/0/48] New client detected, sending
session start event for 28d2.4496.5376 // dot1x client detected dot1x-ev:[28d2.4496.5376,
Gi3/0/48] Dot1x authentication started for 0x26000007 (28d2.4496.5376) //dot1x started %AUTHMGR-
5-START: Starting 'dot1x' for client (28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID
0A6A258E0000003500C9CFC3 dot1x-sm:[28d2.4496.5376, Gi3/0/48] Posting !EAP_RESTART on Client
0x26000007 //requesting client to restart the EAP Proces dot1x-sm:[28d2.4496.5376, Gi3/0/48]
Posting RX_REQ on Client 0x26000007 //waiting fot the EAPoL packet fromt he client dot1x-
sm:[28d2.4496.5376, Gi3/0/48] Posting AUTH_START for 0x26000007 // Starting authentication
process dot1x-ev:[28d2.4496.5376, Gi3/0/48] Sending out EAPOL packet // Identity Request dot1x-
packet:EAPOL pak Tx - Ver: 0x3 type: 0x0 dot1x-packet: length: 0x0005 dot1x-packet:EAP code: 0x1
id: 0x1 length: 0x0005 dot1x-packet: type: 0x1 dot1x-packet:[28d2.4496.5376, Gi3/0/48] EAPOL
packet sent to client 0x26000007 dot1x-ev:[Gi3/0/48] Received pkt saddr =28d2.4496.5376 , daddr
= 0180.c200.0003, pae-ether-type = 888e.0100.000a dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x0
// Identity Response dot1x-packet: length: 0x000A dot1x-sm:[28d2.4496.5376, Gi3/0/48] Posting
EAPOL_EAP for 0x26000007 //EAPoL packet(EAP Response) received, preparing request to server
dot1x-sm:[28d2.4496.5376, Gi3/0/48] Posting EAP_REQ for 0x26000007 //Server response received,
EAP Request is being prepared dot1x-ev:[28d2.4496.5376, Gi3/0/48] Sending out EAPOL packet
dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0 dot1x-packet: length: 0x0006 dot1x-packet:EAP
code: 0x1 id: 0xE5 length: 0x0006 dot1x-packet: type: 0xD dot1x-packet:[28d2.4496.5376,
Gi3/0/48] EAPOL packet sent to client 0x26000007 //EAP request sent out dot1x-ev:[Gi3/0/48]
Received pkt saddr =28d2.4496.5376 , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006
//EAP response received dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x0 dot1x-packet: length:
0x0006 || || || || Here a lot of EAPOL-EAP and EAP_REQ events occur as a lot of information is
exchanged between the switch and the client
|| If the events after this do not follow, then the timers and the information sent till now
need to be checked || || || dot1x-packet:[28d2.4496.5376, Gi3/0/48] Received an EAP Success
//EAP Success recieved from Server dot1x-sm:[28d2.4496.5376, Gi3/0/48] Posting EAP_SUCCESS for
0x26000007 //Posting EAP Success event dot1x-sm:[28d2.4496.5376, Gi3/0/48] Posting AUTH_SUCCESS
on Client 0x26000007 //Posting Authentication success %DOT1X-5-SUCCESS: Authentication
successful for client (28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID
0A6A258E0000003500C9CFC3
```

```
dot1x-packet:[28d2.4496.5376, Gi3/0/48] EAP Key data detected adding to attribute list
//Additional key data detected sent by server
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (28d2.4496.5376) on Interface Gi3/0/48
AuditSessionID 0A6A258E0000003500C9CFC3 dot1x-ev:[28d2.4496.5376, Gi3/0/48] Received Authz
Success for the client 0x26000007 (28d2.4496.5376) //Authorization Success dot1x-
ev:[28d2.4496.5376, Gi3/0/48] Sending out EAPOL packet //Sending EAP Success to the client
dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0 dot1x-packet: length: 0x0004 dot1x-packet:EAP
code: 0x3 id: 0xED length: 0x0004 dot1x-packet:[28d2.4496.5376, Gi3/0/48] EAPOL packet sent to
client 0x26000007
```

## debug radius

由於有許多EAP消息，傳送到伺服器並接收的RADIUS資料包也會更多。並非每個dot1x身份驗證都以on Access-Request結束。因此，此處顯示的日誌是重要的日誌，隨著流的進行。

```
   //mab and dot1x start at the same time as per the configuration
%AUTHMGR-5-START: Starting 'dot1x' for client (28d2.4496.5376) on Interface Gi3/0/48
AuditSessionID 0A6A258E0000003600CCC037 %AUTHMGR-5-START: Starting 'mab' for client
(28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID 0A6A258E0000003600CCC037
RADIUS/ENCODE(00000000):Orig. component type = Invalid RADIUS(00000000): Config NAS IP: 0.0.0.0
//Since dot1x client didn't respond yet, mab authentication is done
RADIUS(00000000): sending RADIUS/ENCODE: Best Local IP-Address 10.106.37.142 for Radius-Server
10.106.73.143 RADIUS(00000000): Send Access-Request to 10.106.73.143:1812 id 1645/56, len 267
RADIUS: authenticator F0 E4 E3 28 7E EA E6 83 - 43 55 7F DC 96 19 EB 42 RADIUS: User-Name [1] 14
"28d244965376" RADIUS: User-Password [2] 18 * RADIUS: Service-Type [6] 6 Call Check [10] RADIUS:
Vendor, Cisco [26] 31 RADIUS: Cisco AVpair [1] 25 "service-type=Call Check" RADIUS: Framed-MTU
[12] 6 1500 RADIUS: Called-Station-Id [] 19 "CC-EF-48-AD-6B-" RADIUS: Calling-Station-Id [31] 19
"28-D2-44-96-53-76" RADIUS: Message-Authenticato[80] 18 RADIUS: AD DC 22 D7 83 8C 02 C5 1E 11 B2
94 80 85 2F 3D [ "/=] RADIUS: EAP-Key-Name [102] 2 * RADIUS: Vendor, Cisco [26] 49 RADIUS: Cisco
AVpair [1] 43 "audit-session-id=0A6A258E0000003600CCC037" RADIUS: Vendor, Cisco [26] 18 RADIUS:
Cisco AVpair [1] 12 "method=mab" RADIUS: Framed-IP-Address [8] 6 1.1.1.2 RADIUS: NAS-IP-Address
[4] 6 10.106.37.142 RADIUS: NAS-Port [5] 6 60000 RADIUS: NAS-Port-Id [87] 23
"GigabitEthernet3/0/48" RADIUS: NAS-Port-Type [61] 6 Ethernet [15] RADIUS(00000000): Sending a
IPv4 Radius Packet RADIUS(00000000): Started 5 sec timeout RADIUS: Received from id 1645/56
10.106.73.143:1812, Access-Accept, len 176 RADIUS: authenticator 7B D6 DA E1 70 49 6E 6D - 3D AC
5C 1D C0 AC CF D0 RADIUS: User-Name [1] 19 "28-D2-44-96-53-76" RADIUS: State [24] 40 RADIUS: 52
65 61 75 74 68 53 65 73 73 69 6F 6E 3A 41 [ReauthSession:0A] RADIUS: 36 41 32 35 38 45 33 36
[6A258E0000003600] RADIUS: 43 43 43 33 37 [ CCC037] RADIUS: Class [25] 51 RADIUS: 43 41 43 53 3A
41 36 41 32 35 38 45 [CACS:0A6A258E000] RADIUS: 33 36 43 43 43 33 37 3A 69 73 [0003600CCC037:is]
RADIUS: 65 31 34 2F 32 35 35 38 35 37 38 34 2F 36 34 [e14/255857804/64] RADIUS: 36 [ 6] RADIUS:
Message-Authenticato[80] 18 RADIUS: D3 F3 6E 9A 25 09 01 8C D6 B1 20 D6 84 D3 18 3D [ n? =]
RADIUS: Vendor, Cisco [26] 28 RADIUS: Cisco AVpair [1] 22 "profile-name=Unknown" //mab succeeds
%MAB-5-SUCCESS: Authentication successful for client (28d2.4496.5376) on Interface Gi3/0/48
AuditSessionID 0A6A258E0000003600CCC037 %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(28d2.4496.5376) on Interface Gi3/0/48 AuditSessionID 0A6A258E0000003600CCC037 //A dot1x client
is detected and mab is stopped as per the configuration and dot1x authentication starts
%AUTHMGR-7-STOPPING: Stopping 'mab' for client 28d2.4496.5376 on Interface Gi3/0/48
AuditSessionID 0A6A258E0000003600CCC037 RADIUS/ENCODE(00000000):Orig. component type = Invalid
RADIUS(00000000): Config NAS IP: 0.0.0.0 RADIUS(00000000): sending RADIUS/ENCODE: Best Local IP-
Address 10.106.37.142 for Radius-Server 10.106.73.143 RADIUS(00000000): Send Access-Request to
10.106.73.143:1812 id 1645/57, len 252 RADIUS: authenticator 1B E9 37 F4 AC C7 73 BE - F4 95 CB
5F FC 2D 3D E1 RADIUS: User-Name [1] 7 "cisco" RADIUS: Service-Type [6] 6 Framed [2] RADIUS:
Vendor, Cisco [26] 27 RADIUS: Cisco AVpair [1] 21 "service-type=Framed" RADIUS: Framed-MTU [12]
6 1500 RADIUS: Called-Station-Id [] 19 "CC-EF-48-AD-6B-" RADIUS: Calling-Station-Id [31] 19 "28-
D2-44-96-53-76" RADIUS: EAP-Message [79] 12 RADIUS: 02 01 00 0A 01 63 69 73 63 6F [ cisco]
RADIUS: Message-Authenticato[80] 18 RADIUS: 7B 42 C2 C2 69 CB 73 49 1A 40 81 28 71 CF CC 86 [
{BisI@(q] RADIUS: EAP-Key-Name [102] 2 * RADIUS: Vendor, Cisco [26] 49 RADIUS: Cisco AVpair [1]
43 "audit-session-id=0A6A258E0000003600CCC037" RADIUS: Vendor, Cisco [26] 20 RADIUS: Cisco
AVpair [1] 14 "method=dot1x" RADIUS: Framed-IP-Address [8] 6 1.1.1.2 RADIUS: NAS-IP-Address [4]
6 10.106.37.142 RADIUS: NAS-Port [5] 6 60000 RADIUS: NAS-Port-Id [87] 23 "GigabitEthernet3/0/48"
RADIUS: NAS-Port-Type [61] 6 Ethernet [15] RADIUS(00000000): Sending a IPv4 Radius Packet //More
information is being requested by the AAA Server RADIUS: Received from id 1645/57
```

```
10.106.73.143:1812, Access-Challenge, len 120 RADIUS: authenticator A7 2A 6E 8C 75 9C 28 6F - 32
85 B9 87 5B D2 E4 FB RADIUS: State [24] 74 RADIUS: 33 37 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D
[37CPMSessionID=0] RADIUS: 41 36 41 32 35 38 45 33 36 [A6A258E000000360] RADIUS: 43 43 43 33 37
3B 32 39 53 65 73 73 69 6F [0CCC037;29Sessio] RADIUS: 6E 49 44 3D 69 73 65 31 34 2F 32 35 35 38
35 37 [nID=ise14/255857] RADIUS: 38 34 2F 36 34 38 3B [ 804/648;] RADIUS: EAP-Message [79] 8
RADIUS: 01 0A 00 06 0D 20 [ ] RADIUS: Message-Authenticato[80] 18 RADIUS: E2 7C 2B 0E CA AB E3
21 B8 CD 04 8A 7F 23 7A D2 [ |+!#z] || || || || As mentioned before, the excess logs of Access-
Requestes and Access-Challenges come here || || || //Authentication and Authorization succeeds
for dot1x
RADIUS: Received from id 1645/66 10.106.73.143:1812, Access-Accept, len 325 RADIUS:
authenticator F0 CF EE 59 3A 26 25 8F - F7 0E E4 03 E1 11 7E 86 RADIUS: User-Name [1] 7 "cisco"
RADIUS: State [24] 40 RADIUS: 52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 41 [ReauthSession:0A]
RADIUS: 36 41 32 35 38 45 33 36 [6A258E0000003600] RADIUS: 43 43 43 33 37 [ CCC037] RADIUS:
Class [25] 51 RADIUS: 43 41 43 53 3A 41 36 41 32 35 38 45 [CACS:0A6A258E000] RADIUS: 33 36 43 43
43 33 37 3A 69 73 [0003600CCC037:is] RADIUS: 65 31 34 2F 32 35 35 38 35 37 38 34 2F 36 34
[e14/255857804/64] RADIUS: 38 [ 8] RADIUS: EAP-Message [79] 6 RADIUS: 03 12 00 04 RADIUS:
Message-Authenticato[80] 18 RADIUS: 3F 7A DA 59 F7 8A DE 1D 33 4B 07 88 62 F3 3B 71 [ ?zY3Kb;q]
RADIUS: EAP-Key-Name [102] 67 * RADIUS: Vendor, Microsoft [26] 58 RADIUS: MS-MPPE-Send-Key [16]
52 * RADIUS: Vendor, Microsoft [26] 58 RADIUS: MS-MPPE-Recv-Key [17] 52 * RADIUS(00000000):
Received from id 1645/66 RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes //Dot1x succeeds
%DOT1X-5-SUCCESS: Authentication successful for client (28d2.4496.5376) on Interface Gi3/0/48
AuditSessionID 0A6A258E0000003600CCC03
```

## debug aaa authentication/authorization

debug aaa authentication and debug aaa authorization顯示各種身份驗證/授權方法期間有用的資訊。在這種情況下，它只是指定所使用的方法清單的單個行。

```
AAA/AUTHEN/8021X (00000000): Pick method list 'default'
```

這顯示是否有任何身份驗證方法不可用/未啟用。

對CWA/Posture/DACL等進行故障排除的過程與傳統IOS交換機相同。配置驗證是故障排除的第一步。確保配置符合要求。如果配置策略對映，類對映達到標準，則調試問題（如果有）會非常容易。有關使用IBNS 2.0進行配置的詳細資訊，請參閱相關資訊部分。

# 相關資訊

- IBNS 2.0部署指南