IBNS(Identity-Based Networking Services) 2.0 문제 해결

목차

소개

이 문서에서는 IBNS(Identity-Based Networking Services) 2.0을 사용하는 스위치의 인증 문제 해결 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine)
- IEEE 802.1X 개념(dot1X)
- MAB(MAC 인증 우회)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 하지만 다음에 국한되지 않습니다.

- Cisco 스위치 - C3750X-48PF-S with IOS 15.2.1E3(ED)
- Identity Service Engine 2.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

IBNS 2.0은 기존 인증 관리자를 대체하는 새로운 정책 엔진입니다.Cisco Common Classification Policy Language(C3PL)로 유연한 구성을 제공하는 향상된 기능 집합을 갖추고 있습니다. 이제 Access Session Manager라는 이름을 가진 IBNS 2.0은 특정 조건 및 엔드포인트 이벤트를 기반으로 정책 및 작업을 구성하는 옵션을 관리자에게 제공합니다.일반 조건 대신 C3PL을 사용하여 인증 조건, 매개변수 및 작업을 정의합니다.IBNS 2.0에 대한 자세한 내용은 Related Information 섹션에 나와 있는 링크를 참조하십시오.

다양한 용도로 사용되는 정책 맵의 유형은 서로 다릅니다.이 단락은 가입자 유형에 중점을 둡니다.정책 맵에는 세 개의 섹션이 표시됩니다.

- 이벤트 섹션
- 클래스 섹션
- 작업 섹션

Event(이벤트) > Class(클래스) > Action(작업) 계층 구조를 따릅니다.정책 맵이 인터페이스에 적용되면 정책 맵에 정의된 모든 이벤트가 평가됩니다.현재 이벤트에 따라 정책 맵에 정의된 적절한 작업이 인터페이스 레벨에서 적용됩니다.

이벤트가 일치하면 인증/권한 부여의 이벤트/방법/결과를 기반으로 클래스를 평가하는 옵션이 있습니다.이러한 클래스의 결과는 ALWAYS EXECUTE 또는 추가 클래스 맵에서 호출할 수 있습니다.

작업 섹션에서 포함할 수 있는 중요한 작업은 다음과 같습니다.

- 우선 순위를 가진 인증 방법 지정

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

- 특정 인증 방법에 대한 인증 방법 목록 지정

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

- 인증 방법에 대한 권한 부여 방법 목록 지정

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

- 재시도 횟수 지정

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

- 기존 인증/권한 부여 데이터를 새 인증/권한 부여 데이터로 교체

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

- 강제 권한 부여

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

- 강제 권한 해제

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

- 서비스 템플릿 활성화

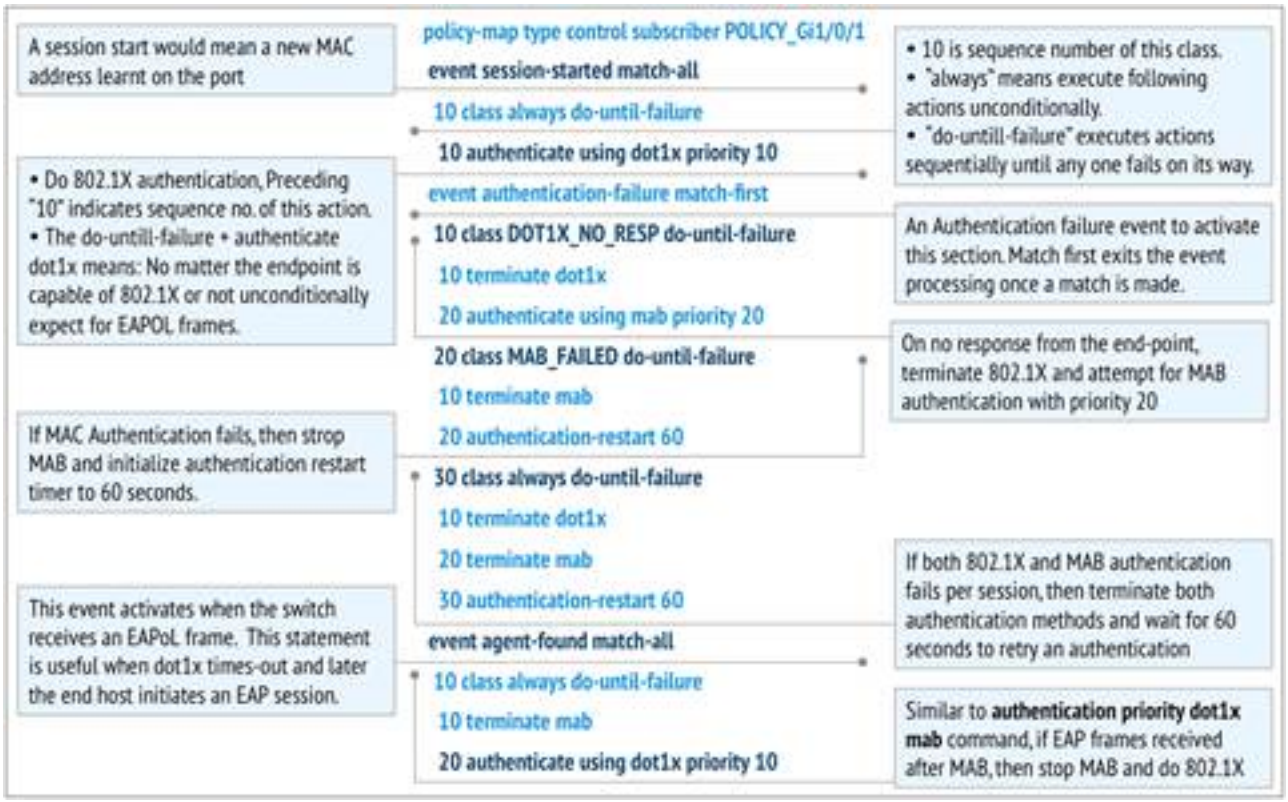
```
event timer-expiry match-all
  10 class do-until-failure 10 activate service-template
```

기존 IOS 스위치에서는 인증된 세션에만 메서드 목록을 적용할 수 있는 옵션이 없었습니다.IBNS 2.0은 서비스 템플릿을 사용하여 이 기능을 제공합니다.서비스 템플릿은 스위치에서 로컬로 구성되며 사후 세션 권한 부여가 적용됩니다.AAA 서버에서 필요한 서비스 템플릿을 푸시할 수도 있습니다.

동일한 작업을 수행하는 데 사용되는 radius 특성은 *subscriber:service-name = <서비스 템플릿 이름>입니다.* ISE(Identity Service Engine)에서 권한 부여 프로파일의 이름을 스위치에 구성된 로컬 서비스 템플릿과 정확히 동일하게 지정하고 *서비스 템플릿* 확인란을 선택할 수 있습니다.이 권한 부여 프로파일은 다른 권한 부여 프로파일과 함께 권한 부여 결과로 푸시될 수 있습니다.

권한 부여 결과 보고서에는 이름이 subscriber*:service-name = <서비스 템플릿 이름>인* Cisco-AV-*Pair가 있습니다*.이는 해당 세션에 해당 서비스 템플릿을 적용하라는 알림을 받았음을 나타냅니다.

다음은 샘플 정책 맵의 모든 엔티티의 정확한 의미를 보여주는 그림입니다.



구성

AAA 컨피그레이션

```
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 서버 구성

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

정책 맵 컨피그레이션

```
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
```

클래스 맵 컨피그레이션

```
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
```

인터페이스 구성

```
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
```

문제 해결

문제를 해결하는 가장 좋은 방법은 작업 로그와 작동하지 않는 로그를 비교하는 것입니다.이렇게 하면 프로세스가 잘못되는 정확한 단계를 알 수 있습니다.mab/dot1x 문제를 해결하기 위해 사용하도록 설정해야 하는 몇 가지 디버그가 있습니다.이러한 디버그를 활성화하는 명령은 다음과 같습니

다.

- 디버그 aaa 인증
- 디버그 aaa 권한 부여
- 모두 디버그
- debug dot1x all
- 디버그 반경

다음은 dot1x 및 mab가 동시에 활성화된 작업 로그입니다.

모두 디버그

```
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

dot1x는 프로토콜 협상, 인증서 교환 등으로 인해 많은 메시지 교환이 있으므로 여기에 일부 디버그 로그가 언급되지는 않았습니다.이벤트 발생 순서와 해당 디버그 로그가 여기에 설명되어 있습니다.

```
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

디버그 반경

EAP 메시지가 많으므로 서버로 전송되고 수신된 RADIUS 패킷도 더 많아집니다.Access-Request에서 모든 dot1x 인증이 종료되는 것은 아닙니다.따라서 여기에 표시된 로그는 중요한 로그이며 플로우가 진행됨에 따라 중요합니다.

//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

디버그 aaa 인증/권한 부여

debug aaa authentication and debug aaa authorization은 다양한 인증/권한 부여 방법 중에 유용한 정보를 표시합니다.이 경우 사용 중인 메서드 목록을 지정하는 단일 행만 사용됩니다.

AAA/AUTHEN/8021X (00000000): Pick method list 'default'
이는 인증 방법 중 하나를 사용할 수 없거나 사용할 수 없는지 여부를 보여줍니다.

CWA/Posture/DACL 등의 문제를 해결하는 절차는 기존 IOS 스위치와 동일합니다.컨피그레이션 확인은 트러블슈팅의 첫 번째 단계입니다.구성이 요구 사항을 충족하는지 확인합니다.정책 맵의 컨피그레이션이 마크까지 설정된 경우 문제(있는 경우)를 디버깅하는 것이 매우 쉽습니다.IBNS 2.0을 사용한 구성에 대한 자세한 내용은 관련 정보 섹션을 참조하십시오.

관련 정보

- IBNS 2.0 구축 설명서