Troubleshoot Identity-Based Network Services (IBNS) 2.0

Inhoud

Inleiding

Dit document beschrijft de procedure voor het oplossen van problemen van authenticaties op switches die op Identity gebaseerde Network Services (IBNS) 2.0 gebruiken

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE)
- IEEE 802.1X-concepten (dot1X)
- MAC-verificatieBypass (MAB)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies, maar is niet beperkt tot:

- Cisco-switch - C3750X-48PF-S met IOS 15.2.1E3(ED)
- Identity Services Engine 2.1

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

Achtergrondinformatie

IBNS 2.0 is een nieuwe beleidsmotor die de traditionele auteur vervangt. Het is uitgerust met een reeks verbeterde capaciteiten die flexibele configuratie met de Cisco Common Classification Policy Language (C3PL) bieden. Nu het beheer van de toegangssessie wordt genoemd, geeft IBNS 2.0 de beheerders opties om beleid en acties te configureren op basis van specifieke omstandigheden en endpointgebeurtenissen. In plaats van regelmatige omstandigheden wordt C3PL gebruikt om de echtheidsvoorwaarden, parameters en de acties te definiëren. Voor meer informatie over IBNS 2.0, volg de link in de Verwante Informatie sectie.

Er zijn verschillende soorten beleidskaarten die voor verschillende doeleinden worden gebruikt. Deze paragraaf is gericht op abonneetype. Er zijn drie onderdelen in een beleidsplan.

- Event sectie
- Sectie klasse
- Actie

Zij volgen de hiërarchie **gebeurtenis > Klasse > Actie.** Wanneer een beleidskaart op een interface wordt toegepast, worden alle gebeurtenissen die in de beleidskaart zijn gedefinieerd, geëvalueerd. Op basis van de huidige gebeurtenis wordt de passende actie die in de beleidskaart is vastgesteld, toegepast op het interfaceniveau.

Zodra het evenement is gematcht, is er een optie om de klassen te evalueren op basis van de gebeurtenis/methode/resultaat van de echtheidscontrole/vergunning. De resultaten van deze klassen kunnen **ALTIJD** worden **UITGEVOERD** of worden opgeroepen op extra klassenkaarten.

In het actiedeel kunnen de volgende belangrijke maatregelen worden opgenomen:

- Specificeer een authenticatiemethode met prioriteit

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

- Specificeer een lijst van een verificatiemethode voor een bepaalde authenticatiemethode

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

- Specificeer een lijst van de machtigingsmethode voor een verificatiemethode

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

- Aantal opnieuw proberen

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

- Vervang de bestaande vergunnings-/vergunninggegevens door nieuwe authenticatie-/vergunningsgegevens

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

- Auditing dwingen

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

- Mastergebrek

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

- Een servicessjabloon activeren

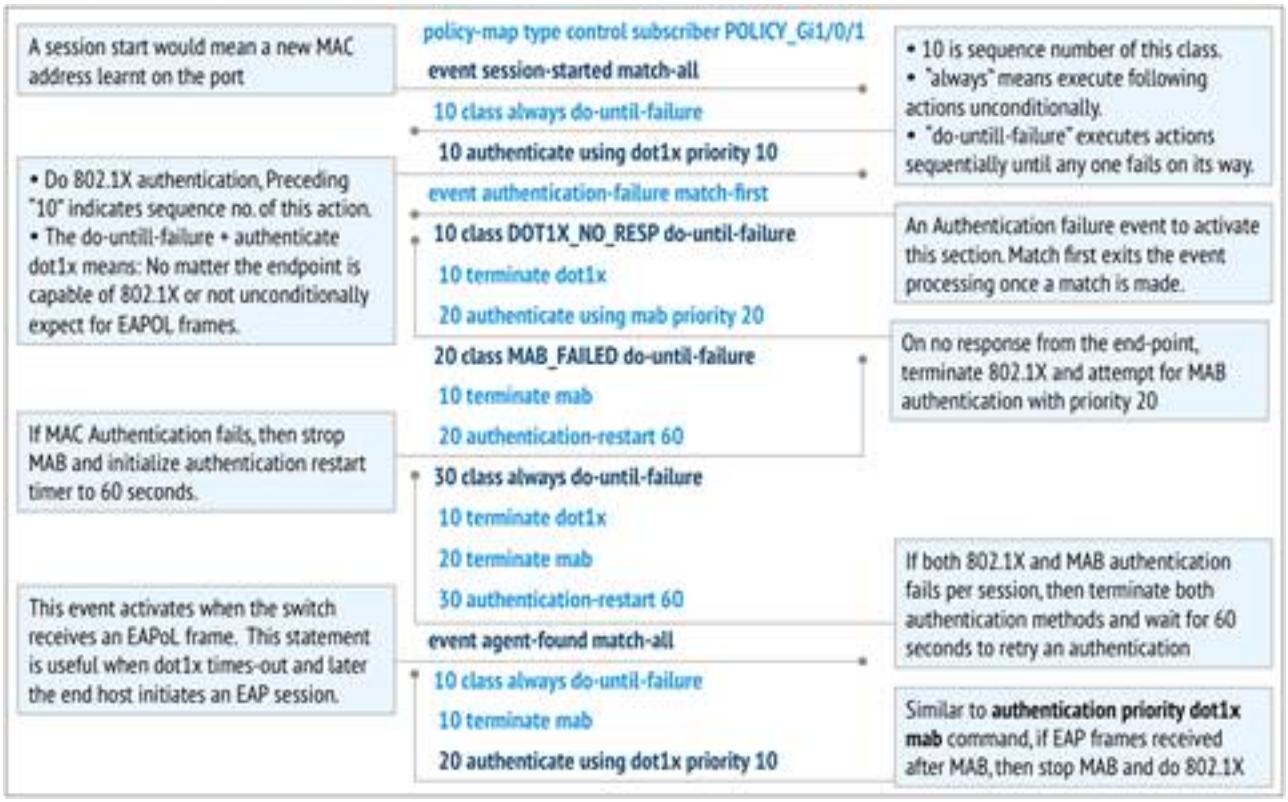
```
event timer-expiry match-all
  10 class do-until-failure 10 activate service-template
```

In de traditionele IOS-switches was er geen optie om een methodelijst toe te passen die specifiek is voor een geauthentiseerde sessie. IBNS 2.0 biedt deze mogelijkheid met behulp van een servicesjabloon. De servicessjabloon is lokaal ingesteld op de -schakelaar en is na een geslaagde sessie van toepassing. Er is ook een optie om de vereiste servicesjabloon vanaf een AAA-server in te drukken.

De Straaleigenschap die wordt gebruikt om hetzelfde te doen is *abonnee:service-naam = <naam van de servicessjabloon>.* In Identity Services Engine (ISE) kunt u het autorisatieprofiel precies dezelfde naam geven als van de plaatselijke servicessjabloon die in de switch is geconfigureerd en het vakje *Service sjabloon* controleren. Dit vergunningprofiel en elk ander vergunningprofiel kunnen als gevolg van de vergunning worden geduwd.

In het rapport met de resultaten van de autorisatie is er een Cisco-AV-Pair met de naam *abonnee:service-naam = <naam van de servicessjabloon>* . Dit duidt erop dat de switch is geïnformeerd om die servicesjabloon voor die sessie toe te passen.

Dit is een plaatje dat de exacte betekenis van elke entiteit van een steekproefbeleidsplan toont.



Configureren

AAA-configuratie

```
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
```

Configuratie van RADIUS-servers

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

Beleidskaartconfiguratie

```
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
```

Configuratie van klaskaarten

```
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
```

Interfaceconfiguratie

```
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
```

Problemen oplossen

De beste manier om problemen op te lossen is het vergelijken van de werkende logbestanden en de niet-werkende logbestanden. Op deze manier is precies bekend welke stap het proces verkeerde. Er zijn een paar debugs die nodig zijn om problemen met de mab/dot1x-problemen op te lossen. Hier zijn de opdrachten om deze apparaten in te schakelen.

- debug van verificatie
- debug AAA-autorisatie
- doekje
- dot1x debug
- straal deken

Hier zijn de werklogs met punt1x en mab ingeschakeld op hetzelfde moment.

doekje

```
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
```

dot1x debug

Omdat dot1x veel berichten heeft uitgewisseld vanwege de protocolonderhandelingen, de uitwisseling van certificaten enzovoort, zijn niet alle debug-logbestanden hier genoemd. De stroom van gebeurtenissen in de volgorde waarin ze zouden moeten voorkomen en hun corresponderende debug-bestanden is hier gedocumenteerd.

```
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
```

straal deken

Aangezien er veel EAP-berichten zijn, worden er ook meer RADIUS-pakketten naar de server verzonden en ontvangen. Niet elke stip1x-verificatie eindigt met een toegangsaanvraag. Vandaar

dat hier de blogs zijn die belangrijk zijn en zoals de stroom gaat.

//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 van verificatie/autorisatie

debug van de echtheidscontrole en debug van een vergunning, die nuttige informatie bevat tijdens verschillende authenticatie-/autorisatiemethoden. In dit geval is het slechts één regel die de gebruikte methodelijst specificeert.

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

Dit toont aan of een van de authenticatiemethoden niet beschikbaar of niet ingeschakeld is.

De procedure om problemen op te lossen CWA/Posture/DACL's enz. is dezelfde als die van de traditionele IOS-switches. Verificatie van configuratie is de eerste stap in het oplossen van problemen. Zorg ervoor dat de configuratie aan de eisen voldoet. Als de configuratie van de beleidslijn, class map op het teken staat, dan kan het debugg problemen, als ze er zijn, heel makkelijk zijn. Raadpleeg het gedeelte Verwante informatie voor meer informatie over configuratie met IBNS 2.0.

Gerelateerde informatie

- IBNS 2000 implementatiegids