

Dynamische VLAN-toewijzing met NGWC en ACS 5.2 configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Dynamische VLAN-toewijzing met RADIUS-server](#)

[Configureren](#)

[Netwerkdigram](#)

[veronderstellingen](#)

[WLC configureren met CLI](#)

[WLAN configureren](#)

[RADIUS-server op WLC configureren](#)

[DHCP-pool voor client-VLAN configureren](#)

[WLC configureren met GUI](#)

[WLAN configureren](#)

[RADIUS-server op WLC configureren](#)

[RADIUS-server configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft het concept dynamische VLAN-toewijzing. Het beschrijft ook hoe u de draadloze LAN-controller (WLC) en een RADIUS-server moet configureren om draadloze LAN-clients (WLAN) dynamisch aan een specifiek VLAN toe te wijzen. In dit document is de RADIUS-server een toegangscontroleserver (ACS) met Cisco Secure Access Control System versie 5.2.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de WLC en Lichtgewicht Access Point (LAP's)
- Functionele kennis van de AAA-server

- Grondig kennis van draadloze netwerken en draadloze beveiligingsproblemen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5760 draadloze LAN-controller met Cisco IOS XE-software-release 3.2.2 (Next Generation Wding Cloud, of NGWC)
- Cisco Aironet 3602 Series lichtgewicht access point
- Microsoft Windows XP met Intel Proset-applicatie
- Cisco Secure Access Control System versie 5.2
- Cisco Catalyst 3560 Series Switch

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.

Dynamische VLAN-toewijzing met RADIUS-server

In de meeste WLAN-systemen heeft elke WLAN-functie een statisch beleid dat van toepassing is op alle klanten die bij een Service Set Identifier (SSID) of WLAN in de controller-terminologie worden aangesloten. Hoewel krachtig, heeft deze methode beperkingen omdat het van cliënten vereist om met verschillende SSIDs te associëren om verschillend QoS en veiligheidsbeleid te erven.

De Cisco WLAN-oplossing ondersteunt echter identiteitsnetwerken. Dit staat het netwerk toe om één enkele SSID te adverteren, maar staat specifieke gebruikers toe om verschillende QoS, eigenschappen van VLAN en/of veiligheidsbeleid te erven dat op de gebruikersgeloofsbrieven wordt gebaseerd.

Dynamische VLAN-toewijzing is één dergelijke functie die een draadloze gebruiker in een specifiek VLAN plaatst op basis van de referenties die door de gebruiker worden geleverd. Deze taak van gebruikershandleiding naar een specifiek VLAN wordt verwerkt door een RADIUS-verificatieserver, zoals een Cisco Secure ACS. Deze optie kan bijvoorbeeld gebruikt worden om de draadloze host op hetzelfde VLAN te laten blijven als deze binnen een campus-netwerk beweegt.

Als resultaat hiervan, wanneer een client probeert om zich te associëren met een LAP geregistreerd met een controller, geeft LAP de aanmeldingsgegevens van de gebruiker voor validatie door naar de RADIUS-server. Zodra de authenticatie succesvol is, passeert de RADIUS-server bepaalde eigenschappen van Internet Engineering Task Force (IETF) aan de gebruiker. Deze RADIUS-eigenschappen bepalen de VLAN-ID die aan de draadloze client moet worden toegewezen. De SSID van de client (WLAN, in termen van de WLC) is niet belangrijk omdat de gebruiker altijd aan deze vooraf bepaalde VLAN-id wordt toegewezen.

De RADIUS-gebruikerseigenschappen die gebruikt worden voor de VLAN-ID-toewijzing zijn:

- IETF64 (tunneltype) - ingesteld op VLAN.
- IETF 65 (Middelgroot tunneltype) - ingesteld op 802.

- IETF 81 (Tunnel-Private-Group-ID) - ingesteld op VLAN-id.

De VLAN-ID is 12 bits en neemt een waarde tussen 1 en 4094, inclusief. Omdat de Tunnel-Private-Group-ID van type string is, zoals gedefinieerd in [RFC 2868, RADIUS Attributes voor Tunnel Protocol-ondersteuning](#) voor gebruik met IEEE 802.1X, wordt de integerwaarde van VLAN ID gecodeerd als een string. Wanneer deze tunnelkenmerken worden verzonden, moet het veld Markering worden ingevuld.

Zoals opgemerkt in RFC2868, rubriek 3.1:

"Het veld Markering is één octet lang en is bedoeld om kenmerken in hetzelfde pakket te groeperen die naar dezelfde tunnel verwijzen."

Geldige waarden voor het veld Tag zijn 0x01 tot 0x1F, inclusief. Als het veld Tag niet is gebruikt, moet het nul zijn (0x00). Raadpleeg RFC 2868 voor meer informatie over alle RADIUS-kenmerken.

Configureren

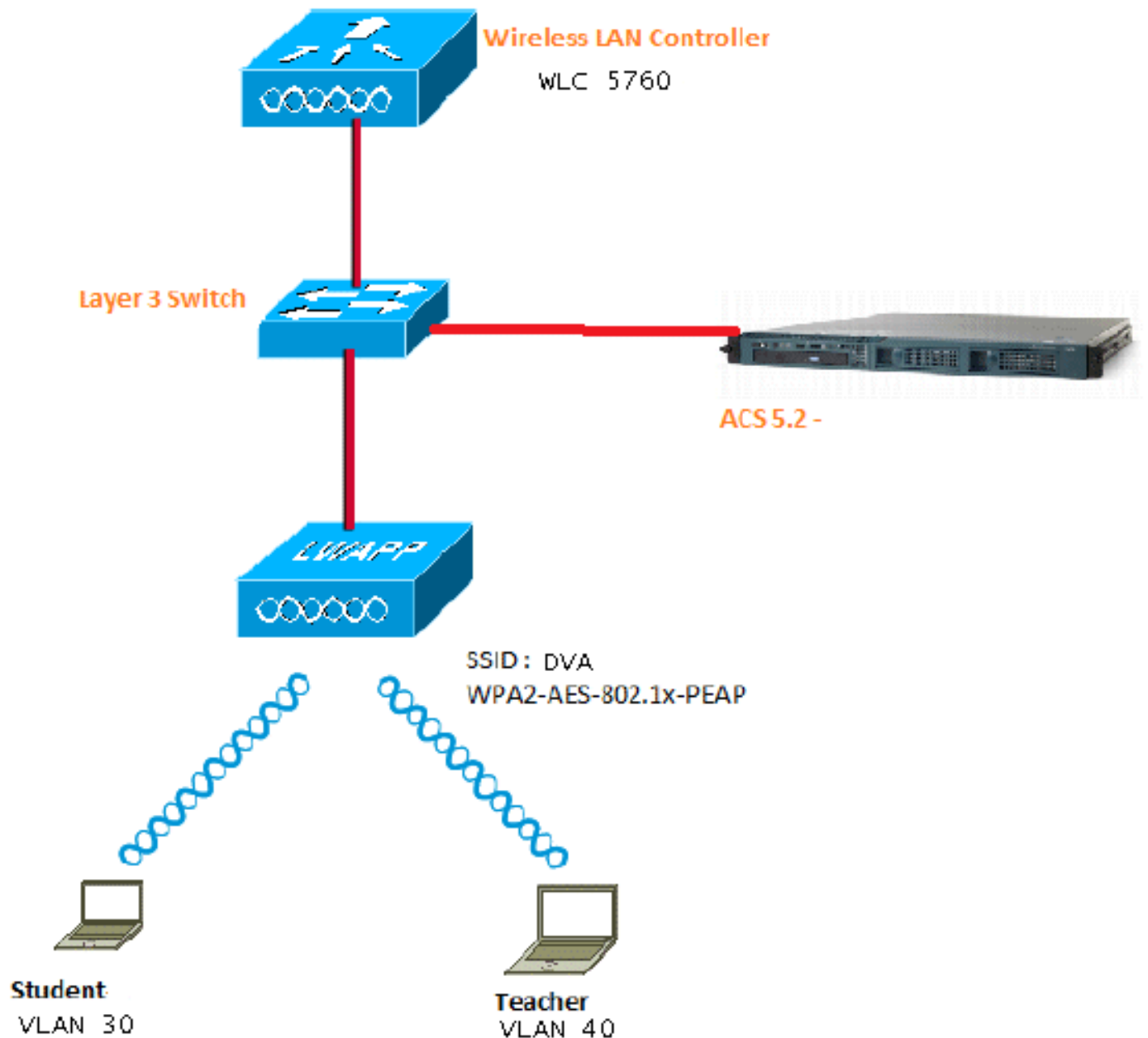
De configuratie van een dynamische VLAN-toewijzing bestaat uit twee verschillende stappen:

1. Configureer de WLC met de opdrachtregel-interface (CLI) of met de GUI.
2. Configuratie van de RADIUS-server.

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.](#)

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Dit document gebruikt 802.1X met Protected Extensible Verification Protocol (PEAP) als het beveiligingsmechanisme.

veronderstellingen

- Switches worden geconfigureerd voor alle Layer 3 (L3) VLAN's.
- De DHCP-server krijgt een DHCP-bereik toegewezen.
- L3-connectiviteit bestaat tussen alle apparaten in het netwerk.
- De LAP is al aangesloten bij de WLC.
- Elk VLAN heeft een /24 masker.
- ACS 5.2 heeft een zelfondertekend certificaat geïnstalleerd.

WLC configureren met CLI

WLAN configureren

Dit is een voorbeeld van hoe u een WLAN met de SSID van DVA kunt configureren:

```
wlan DVA 3 DVA
aaa-override
client vlan VLAN0020
security dot1x authentication-list ACS
session-timeout 1800
no shutdown
```

RADIUS-server op WLC configureren

Dit is een voorbeeld van de configuratie van de RADIUS-server op de WLC:

```
aaa new-model
!
!
aaa group server radius ACS
server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
key Cisco123

dot1x system-auth-control
```

DHCP-pool voor client-VLAN configureren

Dit is een voorbeeld van de configuratie van de DHCP-pool voor de client-VLAN 30 en VLAN 40:

```
interface Vlan30
ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
network 30.30.30.0 255.255.255.0
default-router 30.30.30.1
!
ip dhcp pool vlan40
network 40.40.40.0 255.255.255.0
default-router 40.40.40.1

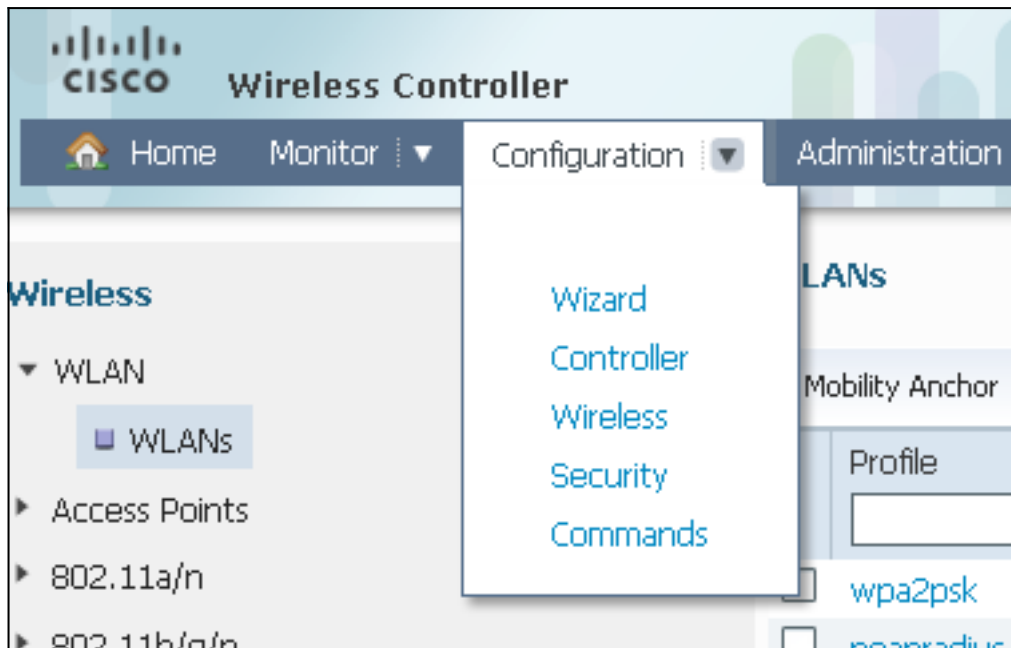
ip dhcp snooping vlan 30,40
ip dhcp snooping
```

WLC configureren met GUI

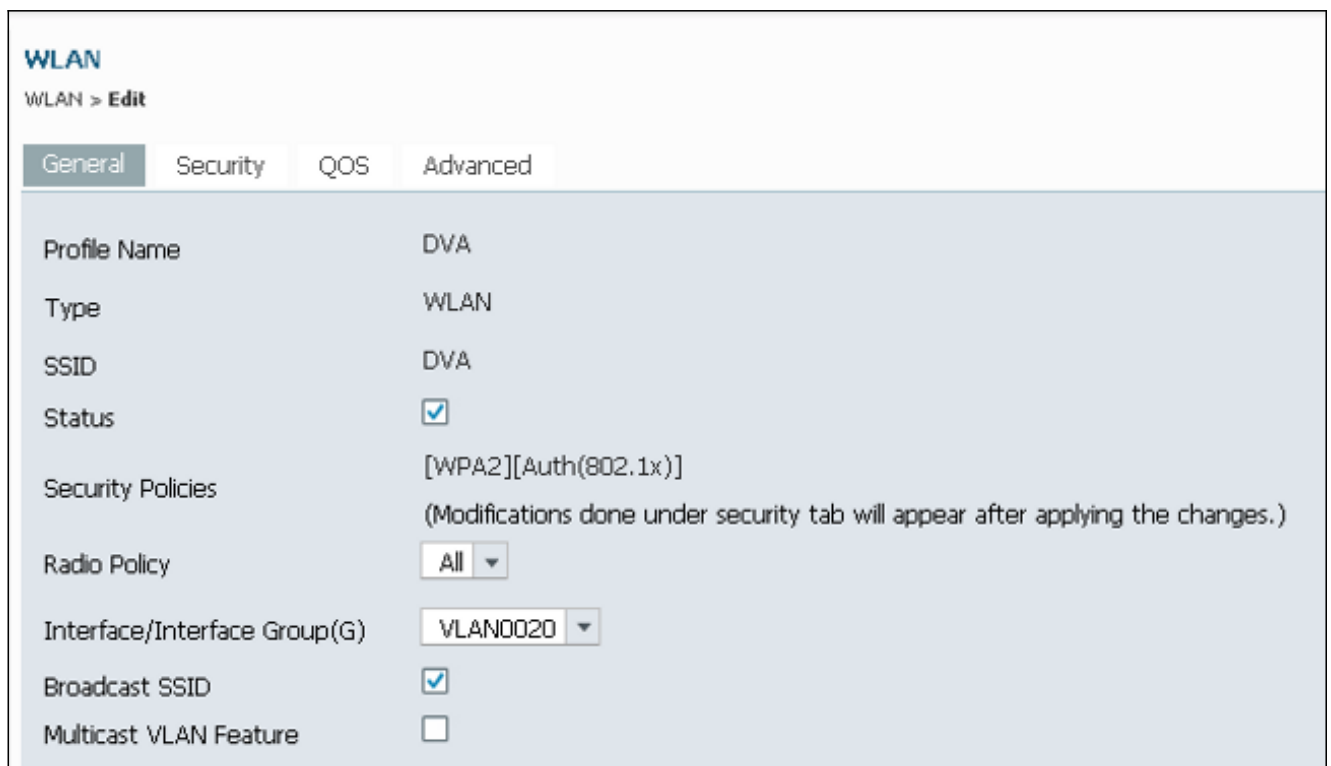
WLAN configureren

Deze procedure beschrijft hoe u de WLAN's kunt configureren.

1. Navigeer naar **Configuration > Wireless > WLAN > NEW** tab.



2. Klik op het **tabblad Algemeen** om te zien dat de WLAN is geconfigureerd voor WPA2-802.1X en kaart de interface/interfacegroep (G) naar VLAN 20 (VLAN0020) in kaart.



3. Klik op het tabblad **Geavanceerd** en controleer het vakje **AAA-negeren toestaan**. Het negeren moet ingeschakeld zijn zodat deze functie kan werken.

WLAN
WLAN > **Edit**

General Security QOS **Advanced**

Allow AAA Override

Coverage Hole Detection

Session Timeout (secs)

4. Klik op het tabblad **Beveiliging** en het tabblad **Layer 2**, controleer het dialoogvenster WAP2-encryptie **AES** en selecteer **802.1x** in de vervolgkeuzelijst Auth Key Mgmt.

WLAN
WLAN > **Edit**

General **Security** QOS Advanced

Layer2 Layer3 AAA Server

Layer 2 Security

MAC Filtering

WPA+WPA2 Parameters

WPA Policy

WPA2 Policy

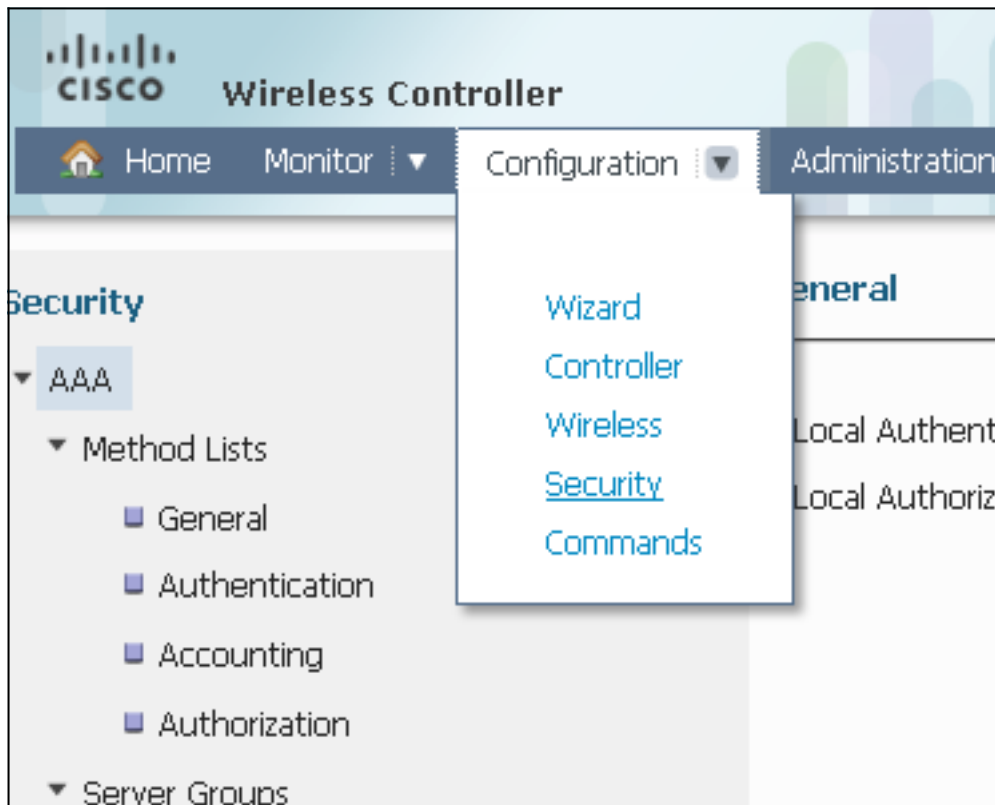
WPA2 Encryption AES TKIP

Auth Key Mgmt

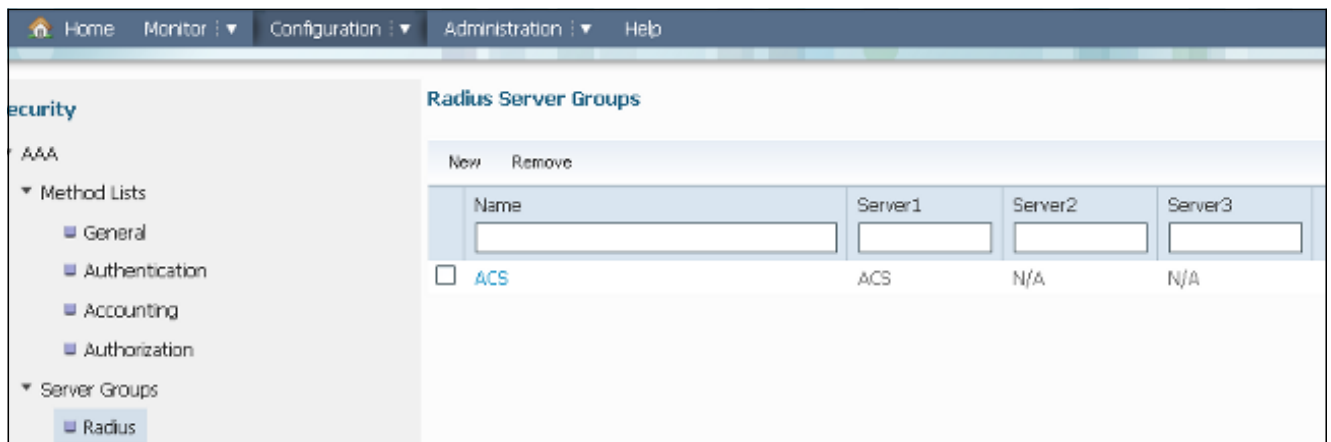
RADIUS-server op WLC configureren

In deze procedure wordt beschreven hoe u de RADIUS-server op de WLC kunt configureren.

1. navigeren naar **Configuration > Security** tabblad.



2. Navigeer naar **AAA > servergroepen > Radius** om de Radius servergroepen te maken. In dit voorbeeld wordt de Radius Server Group ACS genoemd.



3. Bewerk de optie Radius Server om het IP-adres van de server en het gedeelde geheim toe te voegen. Dit gedeelte Gezicht moet overeenkomen met het gedeelte Gebied op de WLC en de RADIUS-server.

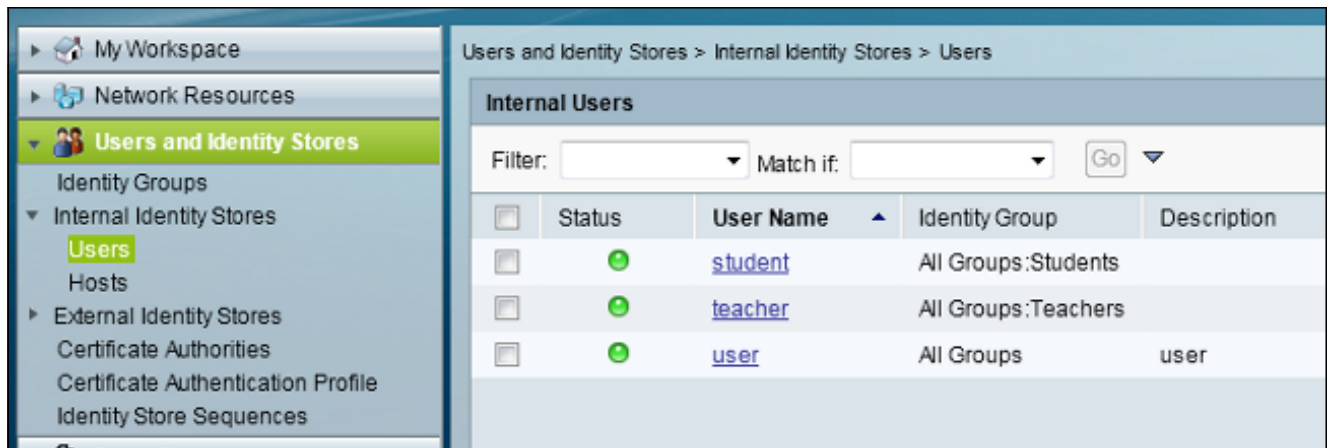
Dit is een voorbeeld van een complete configuratie:

	Server Name	Address	Auth Port	Acct Port
<input type="checkbox"/>	ACS	10.106.102.50	1645	1646

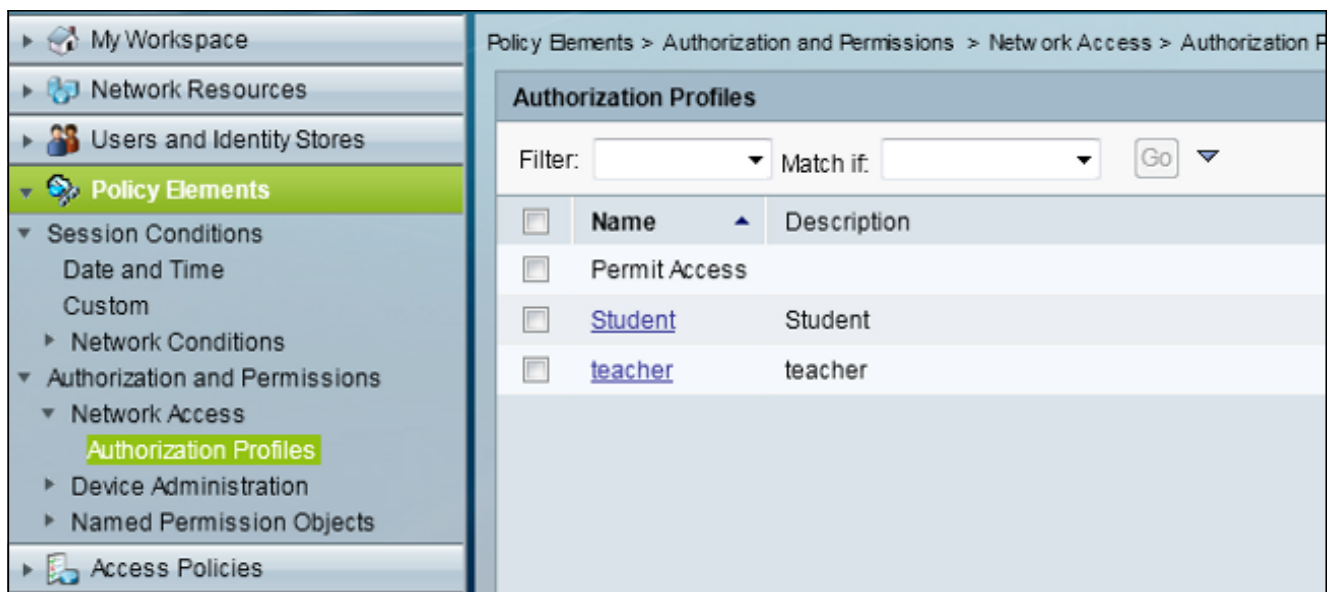
RADIUS-server configureren

In deze procedure wordt beschreven hoe u de RADIUS-server kunt configureren.

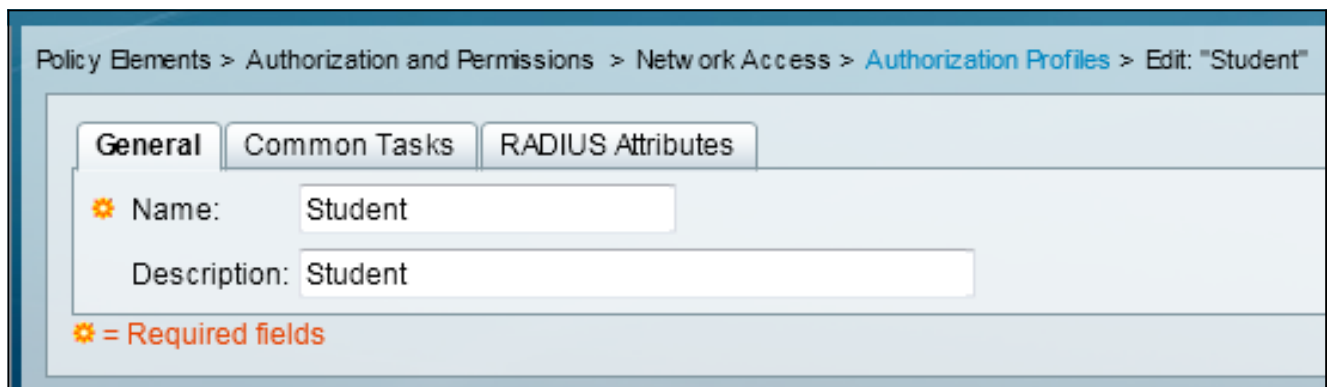
1. Navigeer op de RADIUS-server naar **gebruikers en identiteitsopslag > Interne identiteitsopslag > gebruikers**.
2. Maak de juiste gebruikersnamen en identiteitsgroepen. In dit voorbeeld zijn het studenten en alle groepen:studenten, leraren en alle groepen:leraren.



3. Navigeer in op **Beleidselementen > Vergunning en toegangsrechten > Toegang tot netwerk > Verificatieprofielen** en maak de machtigingsprofielen voor AAA-voorrang.



4. Bewerk het autorisatieprofiel voor student.



5. Stel de VLAN ID/Name in als **Static** met een waarde van **30** (VLAN 30).

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Student"

General Common Tasks RADIUS Attributes

ACLS
Downloadable ACL Name: Not in Use
Filter-ID ACL: Not in Use
Proxy ACL: Not in Use

Voice VLAN
Permission to Join: Not in Use

VLAN
VLAN ID/Name: Static Value 30

Reauthentication
Reauthentication Timer: Not in Use
Maintain Connectivity during Reauthentication:

QOS
Input Policy Map: Not in Use
Output Policy Map: Not in Use

802.1X-REV
LinkSec Security Policy: Not in Use

URL Redirect
When a URL is defined for Redirect an ACL must also be defined
URL for Redirect: Not in Use
URL Redirect ACL: Not in Use

⚙ = Required fields

6. Bewerk het autorisatieprofiel voor docent.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "teacher"

General Common Tasks RADIUS Attributes

⚙ Name: teacher
Description: teacher

⚙ = Required fields

7. Stel de VLAN ID/Name in als **Static** met een waarde van **40** (VLAN 40).

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "teacher"

General Common Tasks RADIUS Attributes

ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Not in Use

VLAN

VLAN ID/Name: Static Value 40

Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

QOS

Input Policy Map: Not in Use

Output Policy Map: Not in Use

802.1X-REV

LinkSec Security Policy: Not in Use

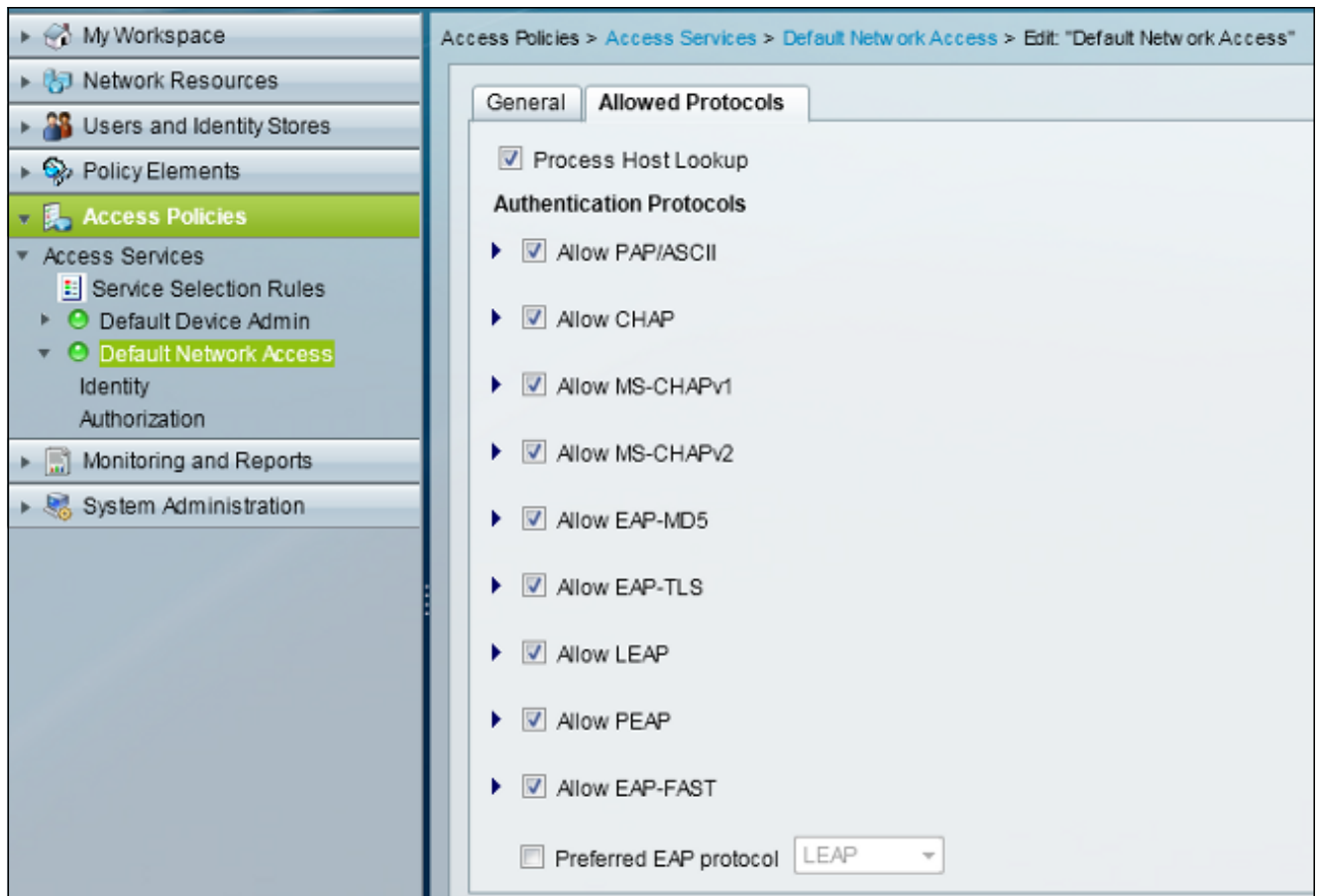
URL Redirect

When a URL is defined for Redirect an ACL must also be defined

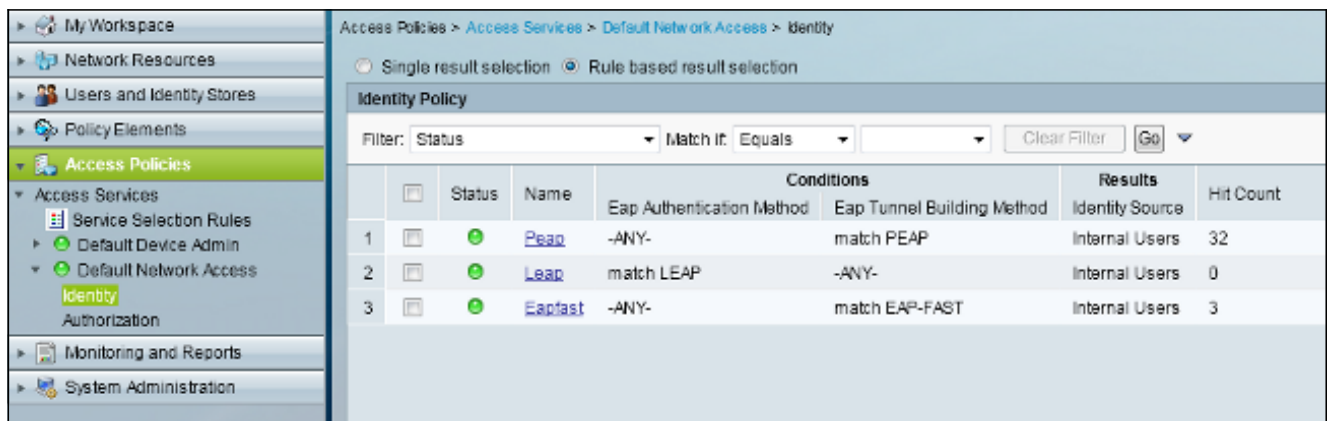
URL for Redirect: Not in Use

URL Redirect ACL: Not in Use

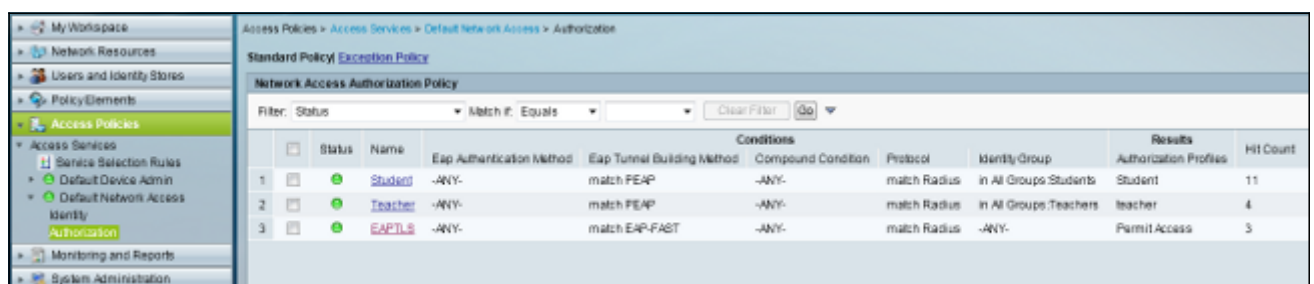
8. Navigeer naar **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang** en klik op het tabblad **Toegestane protocollen**. Controleer het selectieteken **Toestaan PEAP**.



9. Navigeer naar **Identity** en definieer de regels om PEAP-gebruikers mogelijk te maken.



10. navigeren naar **autorisatie**, en studenten en leerkrachten in kaart brengen naar het autorisatiebeleid; in dit voorbeeld, zou de mapping Student voor VLAN 30 en Leraar voor VLAN 40 moeten zijn.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt. Dit zijn de verificatieprocessen:


- Controleer de pagina op ACS die toont welke klanten voor authentiek zijn verklaard.


Sep 1, 13 4:56:49.220 AM	✓	teacher	00-21-5C-8C-C7-81	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.136.176	Capwap1	acstemplate
Sep 1, 13 4:50:54.483 AM	✓	student	00-21-5C-8C-C7-81	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Device	10.105.136.176	Capwap1	acstemplate

- Sluit aan op de DVA WLAN met studentengroep en herzie het client WiFi-verbinding hulpprogramma.

Intel® PROSet/Wireless WiFi Connection Utility

File Tools Advanced Profiles Help












 **You are connected to DVA.**

Network Name: DVA
 Speed: 144.0 Mbps
 Signal Quality: Excellent
 IP Address: 30.30.30.2

[Details...](#)

WiFi Networks (46)

	DVA Connected	
	This network has security enabled	
	<SSID not broadcast>	
	This network has security enabled	
	<SSID not broadcast>	
	This network has security enabled	
	<SSID not broadcast>	
	This network has security enabled	

[Disconnect](#) [Properties...](#) [Refresh](#)

To manage profiles of previously connected WiFi networks, click the Profiles button. [Profiles...](#)

[WiFi On](#) Hardware radio switch: ON [Help?](#) [Close](#)

- Sluit aan op de DVA WLAN met de lerarengroep en bekijk het client-WiFi-verbinding hulpprogramma.

Intel® PROSet/Wireless WiFi Connection Utility

File Tools Advanced Profiles Help

You are connected to DVA.

Network Name: DVA
Speed: 78.0 Mbps
Signal Quality: Excellent
IP Address: 40.40.40.2

Details...

WiFi Networks (47)

Signal Strength	Network Name	Status	Security	Standards
Full	DVA	Connected	Enabled	a, g, n
Full	<SSID not broadcast>	Not Connected	Enabled	a, n
Full	<SSID not broadcast>	Not Connected	Enabled	g
Full	<SSID not broadcast>	Not Connected	Enabled	a, n

Disconnect Properties... Refresh

To manage profiles of previously connected WiFi networks, click the Profiles button.

Profiles...

WiFi On Hardware radio switch: ON Help? Close

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opmerkingen:

Gebruik de [Command Lookup Tool \(alleen voor geregistreeerde gebruikers\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

De [Output Interpreter Tool \(alleen voor geregistreerde klanten\)](#) ondersteunt bepaalde opdrachten met `show`. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht `show`.

Raadpleeg [Important Information on Debug Commands \(Belangrijke informatie over opdrachten met debug\)](#) voordat u opdrachten met `debug` opgeeft.

Handige debugs zijn onder meer het `debug mac-adres` *mac van client* en deze NGWC-overzichten voor sporen:

- `debug` van niveau van spoorgroep-draadloze client
- het instellen van een bandbreedtegroep met draadloze client filterkaart `xxxx.xxxx.xxx`
- sporen van systeemgefilterde sporen weergeven

Het NGWC-spoor bevat geen punt1x/AAA, dus gebruik deze hele lijst met gecombineerde sporen voor dot1x/AAA:

- `debug` van niveau van spoorgroep-draadloze client
- u kunt een overtrek met dot1x-incidentniveau instellen
- overtrekken met dot1x a-niveau instellen
- u kunt overtrekken vanuit een draadloos events level debug instellen
- `debug` van kern-niveau voor toegang tot sporen instellen
- instellen van dot1x-debug met toegangsmethode
- het instellen van een bandbreedtegroep met draadloze client filterkaart `xxxx.xxxx.xxx`
- overtrekken met dot1x-filter instellen `xxxx.xxxx.xxx`
- overtrekken met dot1x a filter instellen `xxxx.xxxx.xxx`
- spoor achter draadloze gebeurtenissen filter `mac xxxx.xxxx.xxx`
- Sm-filterkaart instellen voor toegang tot de sessie `xxxx.xxxx.xxx`
- instellen van dot1x filter-mac voor elke toegangssessie `xxxx.xxxx.xxx`
- sporen van systeemgefilterde sporen weergeven

Wanneer dynamische VLAN-toewijzing correct werkt, dient u dit type uitvoer uit de debugs te zien:

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf: intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
--More-- [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station 0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
```

Wireless client in WCM(NGWC)

[09/01/13 12:13:28.598 IST lcd6 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile

MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST lcd7 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761

[09/01/13 12:13:28.598 IST lcd8 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0030', aclName: ''

--More-- [09/01/13 12:13:28.598 IST lcd9 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST lcda 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST lcdb 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 30, interface 'VLAN0030'

[09/01/13 12:13:28.598 IST lcdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config

[09/01/13 12:13:28.598 IST lcdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds

[09/01/13 12:13:28.598 IST lcde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID Cache entry (RSN 1)

[09/01/13 12:13:28.598 IST lcdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0

[09/01/13 12:08:59.553 IST lae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0) Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13) Tunnel-Private-Id (40)

[09/01/13 12:08:59.553 IST lae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40

--More-- [09/01/13 12:08:59.553 IST lae3 5933] 0021.5C8C.C761 Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf: VLAN0040 New GroupIntf: intfChanged: 1

[09/01/13 12:08:59.553 IST lae4 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761

[09/01/13 12:08:59.553 IST lae5 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST lae6 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---

[09/01/13 12:08:59.553 IST lae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client

[09/01/13 12:08:59.553 IST lae8 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC)

[09/01/13 12:08:59.553 IST lae9 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile

MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST laea 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761

[09/01/13 12:08:59.553 IST laeb 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0040', aclName: ''

--More--
[09/01/13 12:08:59.553 IST laec 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:08:59.553 IST laed 5933] 0021.5C8C.C761 Override values (cont..) dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1

vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'

[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config

[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds

[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)