

Dynamische VLAN-Zuordnung mit NGWC und ACS 5.2 - Konfigurationsbeispiel

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Dynamische VLAN-Zuweisung mit RADIUS-Server](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Annahmen](#)

[Konfigurieren von WLC mit CLI](#)

[WLAN konfigurieren](#)

[Konfigurieren des RADIUS-Servers auf dem WLC](#)

[Konfigurieren des DHCP-Pools für das Client-VLAN](#)

[Konfigurieren von WLC über GUI](#)

[WLAN konfigurieren](#)

[Konfigurieren des RADIUS-Servers auf dem WLC](#)

[Konfigurieren des RADIUS-Servers](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

Dieses Dokument beschreibt das Konzept der dynamischen VLAN-Zuweisung. Außerdem wird beschrieben, wie der WLAN-Controller (WLC) und ein RADIUS-Server konfiguriert werden, um WLAN-Clients dynamisch einem bestimmten VLAN zuzuweisen. In diesem Dokument ist der RADIUS-Server ein Zugriffssteuerungsserver (ACS), auf dem das Cisco Secure Access Control System Version 5.2 ausgeführt wird.

Voraussetzungen

Anforderungen

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

- Grundkenntnisse der WLC- und Lightweight Access Points (LAPs)

- Funktionale Kenntnisse des AAA-Servers (Authentication, Authorization, Accounting)
- Umfassendes Wissen über Wireless-Netzwerke und Wireless-Sicherheitsfragen

Verwendete Komponenten

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

- Cisco 5760 Wireless LAN Controller mit Cisco IOS[®] XE Software Version 3.2.2 (Next Generation Wiring Closet, NGWC)
- Cisco Aironet Lightweight Access Point der Serie 3602
- Microsoft Windows XP mit Intel Proset-Komponente
- Cisco Secure Access Control System Version 5.2
- Cisco Catalyst Switches der Serie 3560

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Dynamische VLAN-Zuweisung mit RADIUS-Server

In den meisten WLAN-Systemen verfügt jedes WLAN über eine statische Richtlinie, die für alle Clients gilt, die einer Service Set Identifier (SSID) oder WLAN in der Controller-Terminologie zugeordnet sind. Diese Methode ist zwar leistungsstark, bietet jedoch Einschränkungen, da Clients verschiedene SSIDs verknüpfen müssen, um unterschiedliche QoS- und Sicherheitsrichtlinien zu erben.

Die Cisco WLAN-Lösung unterstützt jedoch Identitätsnetzwerke. Dadurch kann das Netzwerk eine einzelne SSID angeben, aber bestimmte Benutzer können je nach Benutzeranmeldeinformationen verschiedene QoS-, VLAN-Attribute und/oder Sicherheitsrichtlinien erben.

Die dynamische VLAN-Zuweisung ist eine dieser Funktionen, die einen Wireless-Benutzer anhand der vom Benutzer angegebenen Anmeldeinformationen in ein bestimmtes VLAN versetzt. Diese Aufgabe der Benutzerzuweisung zu einem bestimmten VLAN wird von einem RADIUS-Authentifizierungsserver, z. B. einem Cisco Secure ACS, übernommen. Diese Funktion kann beispielsweise verwendet werden, um dem Wireless-Host zu ermöglichen, im selben VLAN zu bleiben, wie er sich innerhalb eines Campus-Netzwerks bewegt.

Wenn ein Client versucht, eine Verbindung zu einer LAP herzustellen, die bei einem Controller registriert ist, übergibt die LAP die Anmeldeinformationen des Benutzers zur Validierung an den RADIUS-Server. Nach erfolgreicher Authentifizierung übergibt der RADIUS-Server bestimmte IETF-Attribute (Internet Engineering Task Force) an den Benutzer. Diese RADIUS-Attribute legen die VLAN-ID fest, die dem Wireless-Client zugewiesen werden soll. Die SSID des Clients (das WLAN im WLC) spielt keine Rolle, da dem Benutzer immer diese vordefinierte VLAN-ID zugewiesen wird.

Die für die VLAN-ID-Zuweisung verwendeten RADIUS-Benutzerattribute sind:

- IETF 64 (Tunneltyp) - Auf VLAN eingestellt.

- IETF 65 (Tunnel Medium Type) - Einstellung auf 802.
- IETF 81 (Tunnel-Private-Group-ID) - Legen Sie die VLAN-ID fest.

Die VLAN-ID beträgt 12 Bit und hat einen Wert zwischen 1 und 4094 (einschließlich). Da die Tunnel-Private-Group-ID wie in [RFC 2868](#) definiert vom Typ String ist, [werden RADIUS Attributes for Tunnel Protocol Support](#) für die Verwendung mit IEEE 802.1X verwendet, wird der VLAN-ID-Integer-Wert als Zeichenfolge kodiert. Wenn diese Tunnelattribute gesendet werden, muss das Feld Tag ausgefüllt werden.

Wie in RFC 2868, Abschnitt 3.1 beschrieben:

"Das Tag-Feld ist ein Oktett lang und soll eine Möglichkeit zur Gruppierung von Attributen in demselben Paket bieten, die sich auf denselben Tunnel beziehen."

Gültige Werte für das Tag-Feld sind 0x01 bis 0x1F, einschließlich. Wenn das Feld Tag nicht verwendet wird, muss es 0 (0 x 00) sein. Weitere Informationen zu allen RADIUS-Attributen finden Sie unter RFC 2868.

Konfigurieren

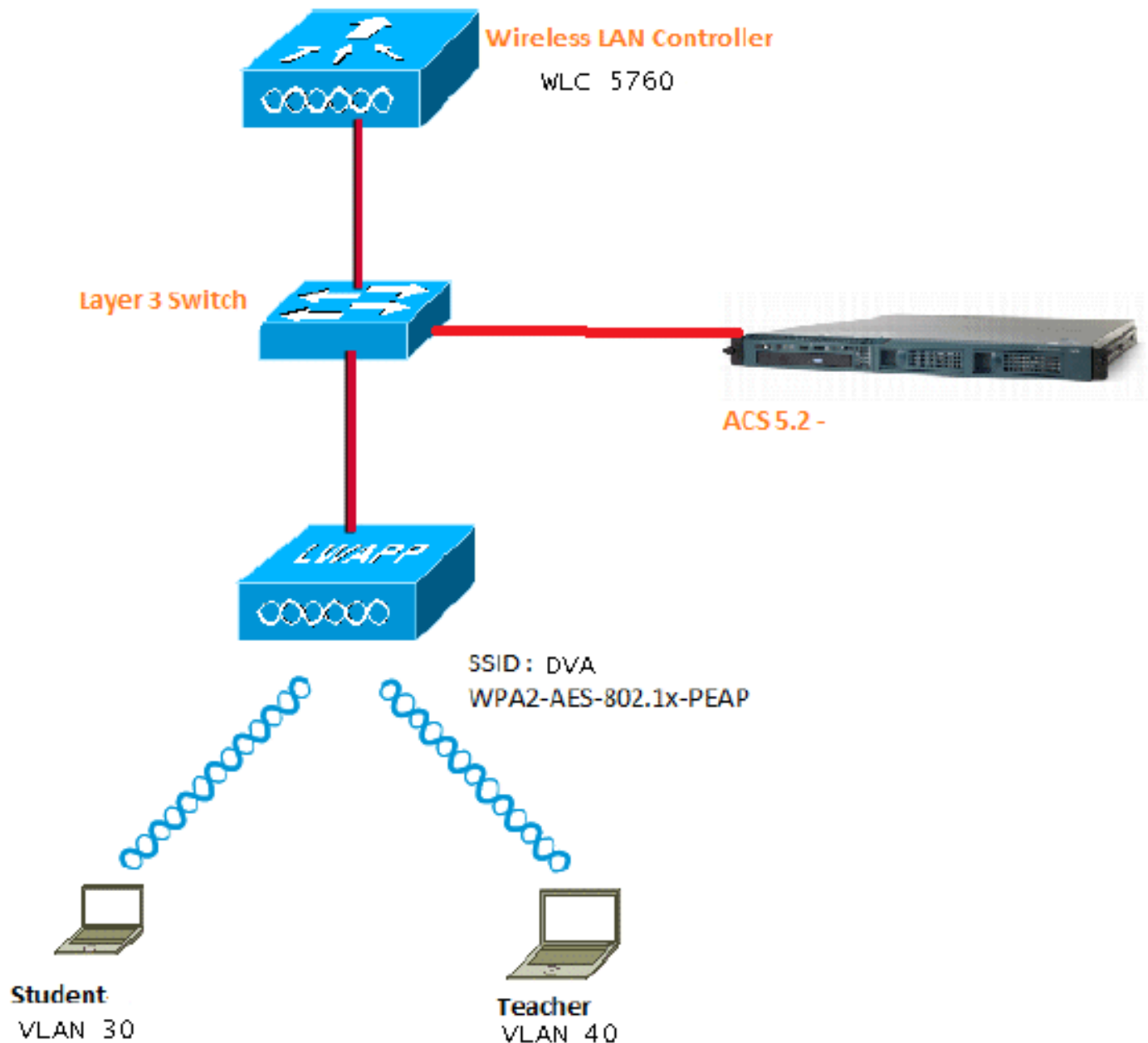
Die Konfiguration einer dynamischen VLAN-Zuweisung besteht aus zwei unterschiedlichen Schritten:

1. Konfigurieren Sie den WLC über die Befehlszeilenschnittstelle (CLI) oder die Benutzeroberfläche.
2. Konfigurieren Sie den RADIUS-Server.

Anmerkung: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Dokument wird 802.1X mit PEAP (Protected Extensible Authentication Protocol) als Sicherheitsmechanismus verwendet.

Annahmen

- Switches werden für alle Layer-3-VLANs (L3) konfiguriert.
- Dem DHCP-Server wird ein DHCP-Bereich zugewiesen.
- Die L3-Verbindung besteht zwischen allen Geräten im Netzwerk.
- Die LAP ist bereits dem WLC beigetreten.
- Jedes VLAN hat eine /24-Maske.
- ACS 5.2 verfügt über ein selbstsigniertes Zertifikat.

Konfigurieren von WLC mit CLI

WLAN konfigurieren

Dies ist ein Beispiel für die Konfiguration eines WLAN mit der SSID von DVA:

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

Konfigurieren des RADIUS-Servers auf dem WLC

Dies ist ein Beispiel für die Konfiguration des RADIUS-Servers im 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
```

Konfigurieren des DHCP-Pools für das Client-VLAN

Dies ist ein Beispiel für die Konfiguration des DHCP-Pools für das Client-VLAN 30 und 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
```

Konfigurieren von WLC über GUI

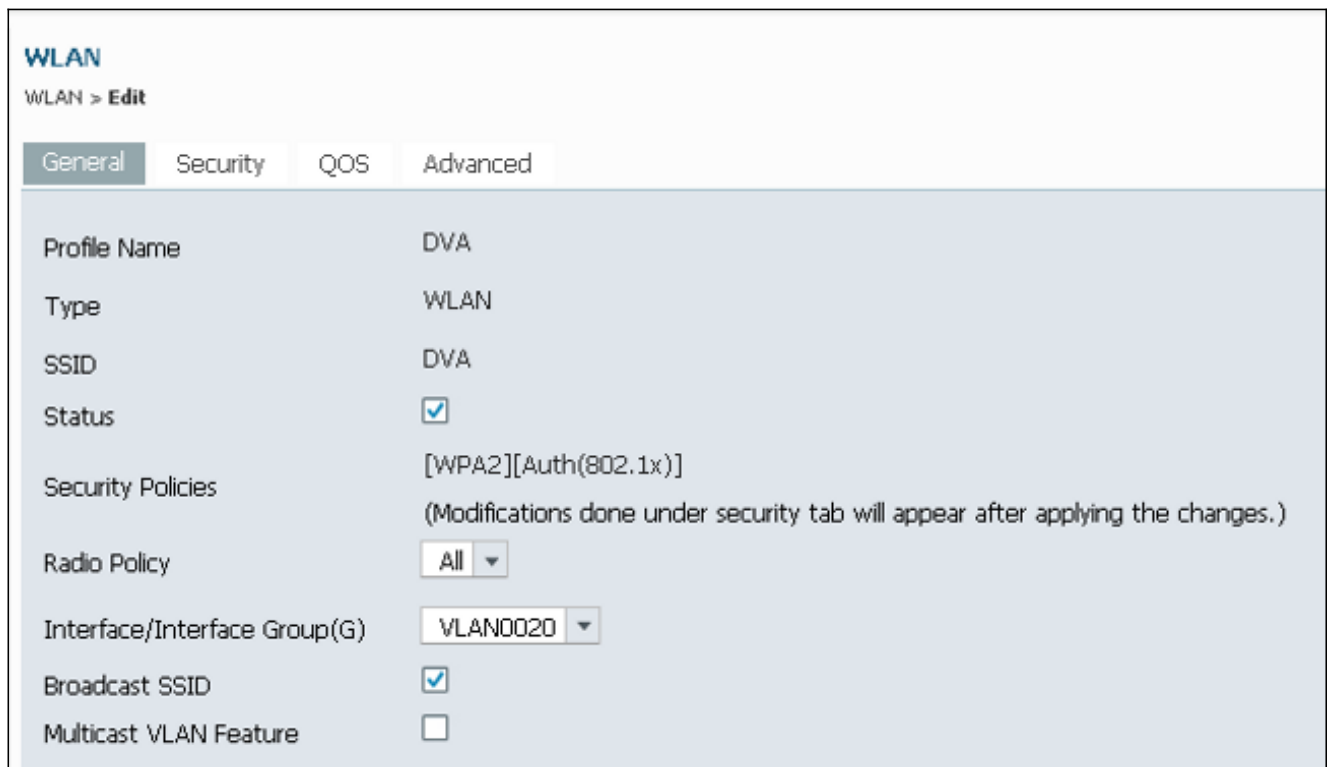
WLAN konfigurieren

Dieses Verfahren beschreibt die Konfiguration des WLAN.

1. Navigieren Sie zu **Configuration > Wireless > WLAN > NEW** tab.



2. Klicken Sie auf die Registerkarte **Allgemein**, um anzuzeigen, dass das WLAN für WPA2-802.1X konfiguriert ist, und ordnen Sie die Schnittstelle/Schnittstellengruppe(G) VLAN 20 (**VLAN020**) zu.



3. Klicken Sie auf die Registerkarte **Erweitert**, und aktivieren Sie das Kontrollkästchen **AAA-Überschreibung zulassen**. Damit diese Funktion funktioniert, muss die Option Override aktiviert sein.

WLAN
WLAN > Edit

General Security QOS **Advanced**

Allow AAA Override

Coverage Hole Detection

Session Timeout (secs)

4. Klicken Sie auf die Registerkarte **Sicherheit** und die Registerkarte **Layer2**, aktivieren Sie das Kontrollkästchen WPA2 Encryption **AES**, und wählen Sie **802.1x** aus der Dropdown-Liste Auth Key Mgmt (Auth-Schlüsselverwaltung) aus.

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

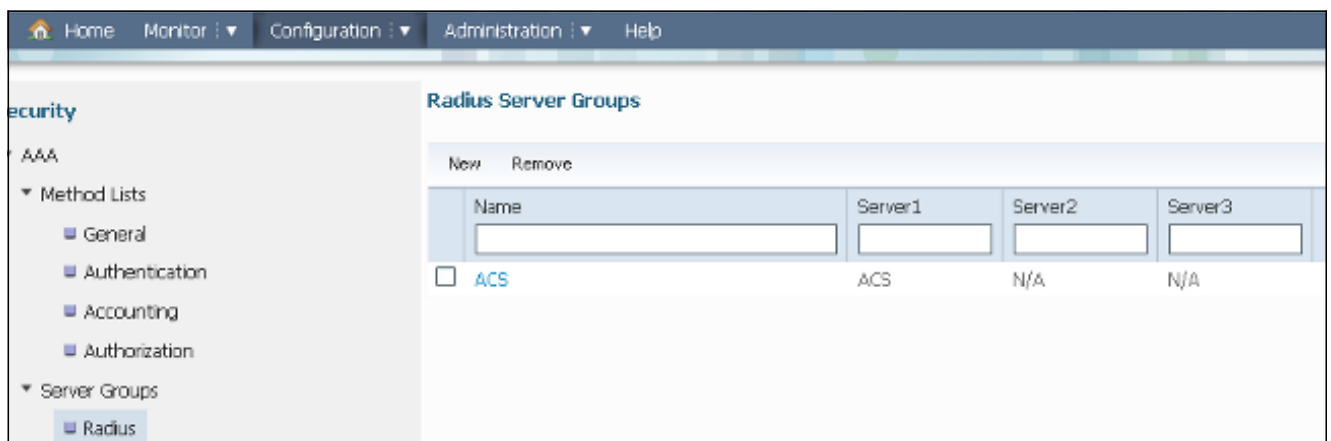
Konfigurieren des RADIUS-Servers auf dem WLC

Dieses Verfahren beschreibt die Konfiguration des RADIUS-Servers auf dem WLC.

1. Navigieren Sie zur Registerkarte **Konfiguration > Sicherheit**.



2. Navigieren Sie zu **AAA > Servergruppen > Radius**, um die Radius-Servergruppen zu erstellen. In diesem Beispiel wird die Radius-Servergruppe ACS genannt.



3. Bearbeiten Sie den Radius-Server-Eintrag, um die Server-IP-Adresse und den Shared Secret hinzuzufügen. Dieser Shared Secret muss mit dem Shared Secret auf dem WLC und dem RADIUS-Server übereinstimmen.

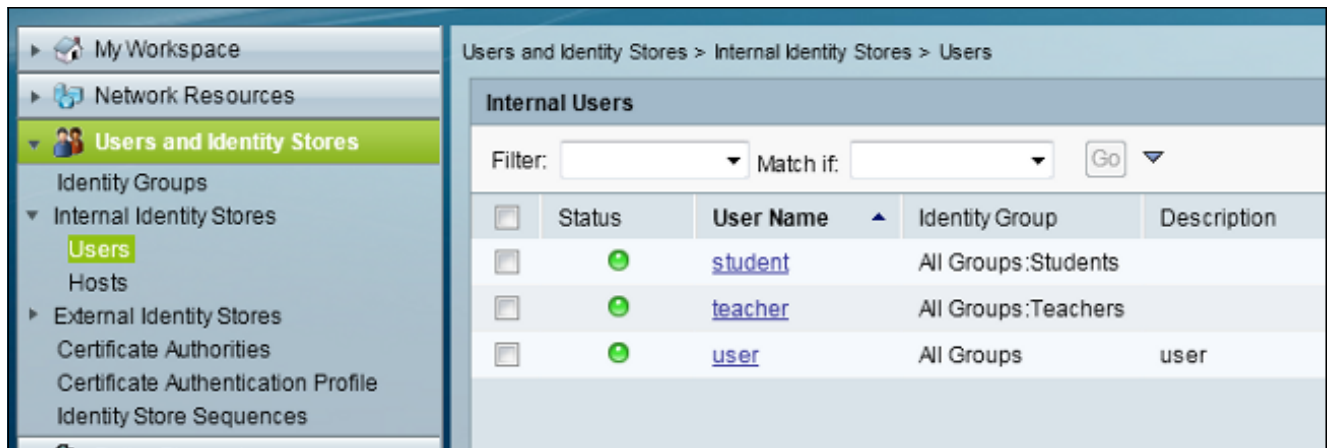
Dies ist ein Beispiel für eine vollständige Konfiguration:

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

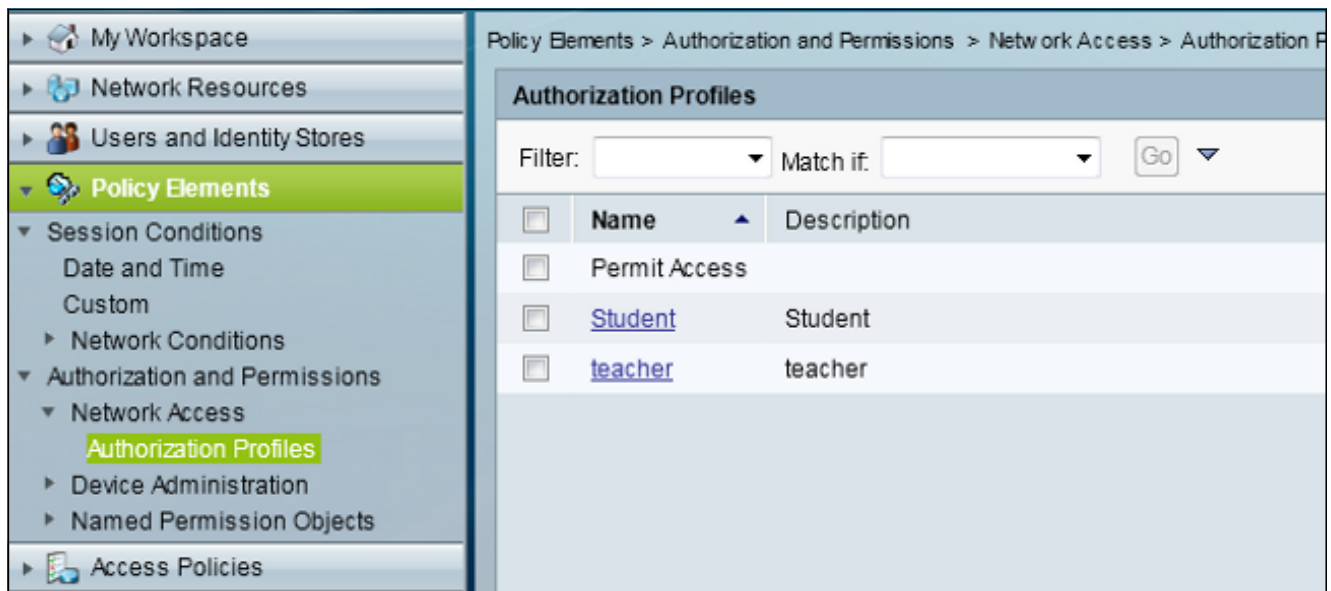
Konfigurieren des RADIUS-Servers

Dieses Verfahren beschreibt die Konfiguration des RADIUS-Servers.

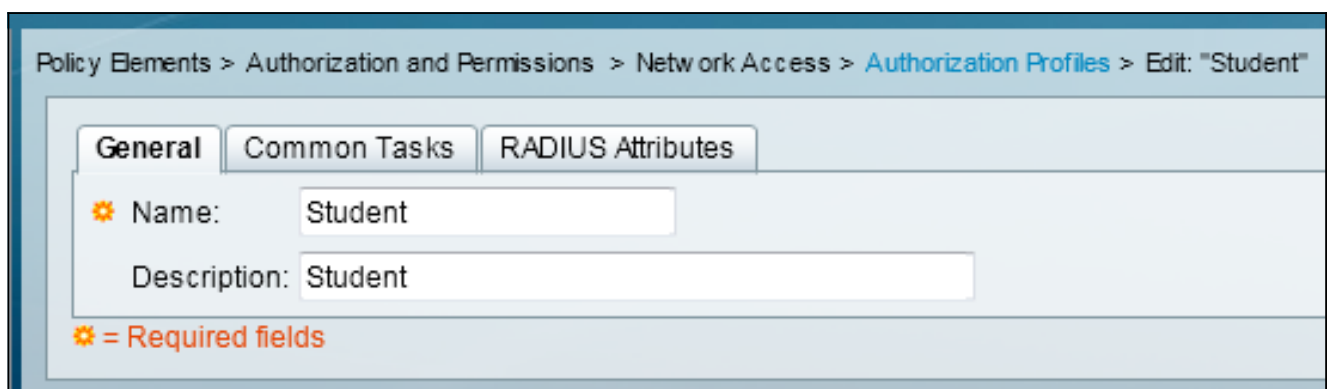
1. Navigieren Sie auf dem RADIUS-Server zu **Benutzer und Identitätsdaten > Interne Identitätsdaten > Benutzer**.
2. Erstellen Sie die entsprechenden Benutzernamen und Identitätsgruppen. In diesem Beispiel ist es Student und All Groups:Students, Teacher und AllGroups:Teachers.



3. Navigieren Sie zu **Richtlinienelemente > Autorisierung und Berechtigungen > Netzwerkzugriff > Autorisierungsprofile**, und erstellen Sie die Autorisierungsprofile für die AAA-Überschreibung.



4. Bearbeiten Sie das Autorisierungsprofil für Kursteilnehmer.



5. Legen Sie die VLAN-ID/-Name als **Statisch** mit dem Wert **30** (VLAN 30) fest.

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. Bearbeiten Sie das Autorisierungsprofil für Lehrer.

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

General Common Tasks RADIUS Attributes

⚙ Name: teacher
Description: teacher

⚙ = Required fields

7. Legen Sie die VLAN-ID/-Name als **Statisch** mit dem Wert **40** (VLAN 40) fest.

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 ▼

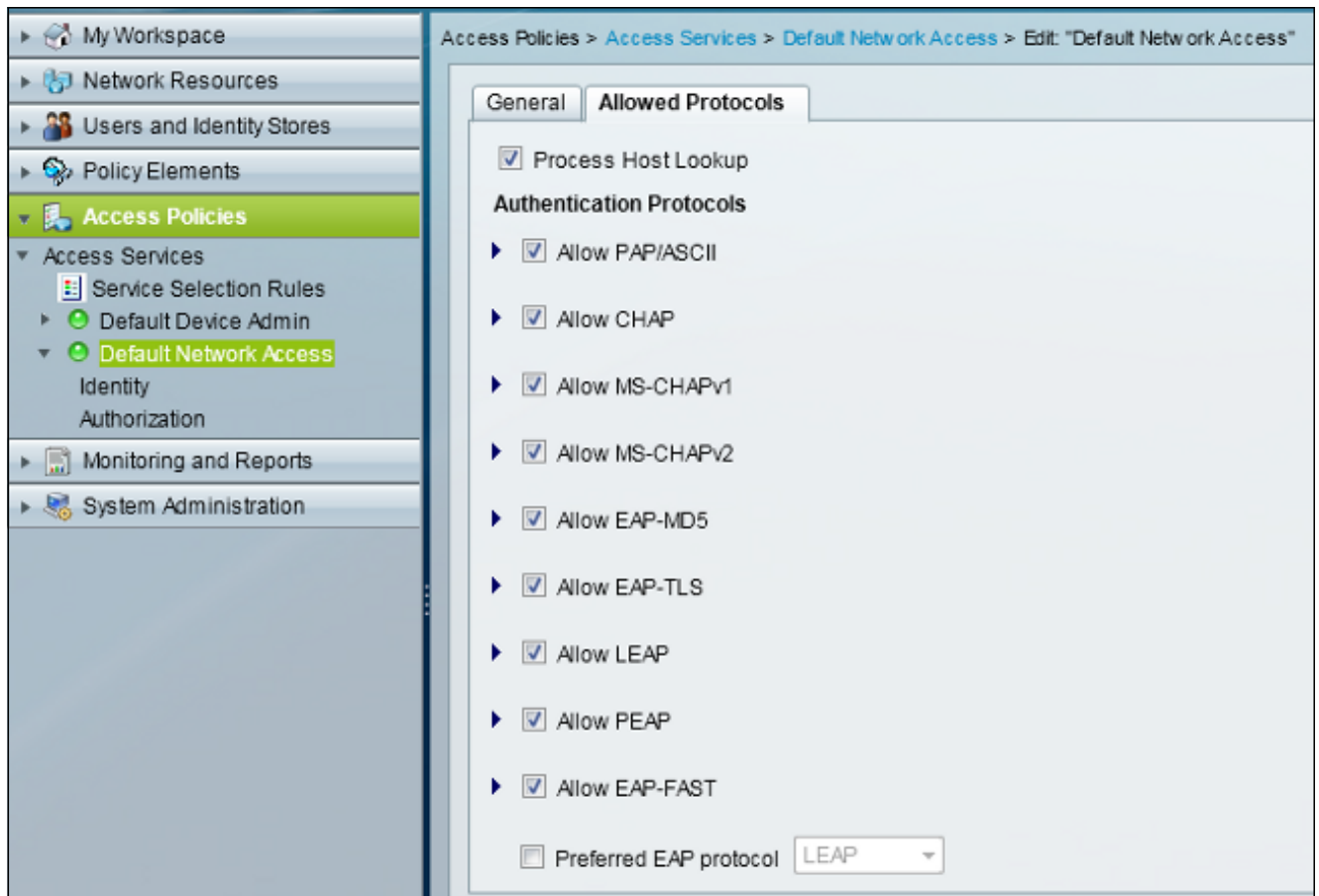
URL Redirect

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

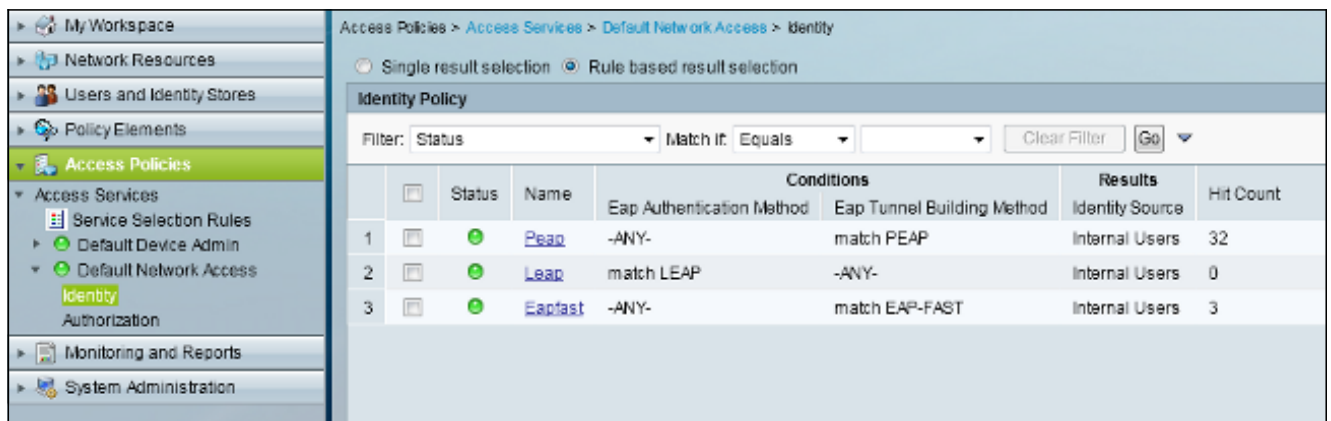
URL for Redirect: Not in Use ▼

URL Redirect ACL: Not in Use ▼

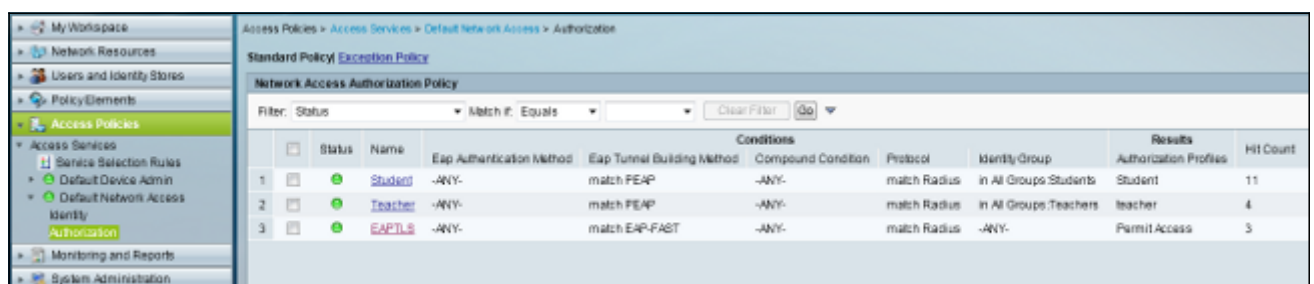
8. Navigieren Sie zu **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff**, und klicken Sie auf die Registerkarte **Zugelassene Protokolle**. Aktivieren Sie das Kontrollkästchen **PEAP zulassen**.



9. Navigieren Sie zu **Identität**, und definieren Sie die Regeln, um PEAP-Benutzern zu erlauben.



10. Navigieren Sie zu **Autorisierung**, und ordnen Sie Student und Lehrer der Autorisierungsrichtlinie zu. In diesem Beispiel sollte die Zuordnung Student für VLAN 30 und Lehrer für VLAN 40 sein.



Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert. Dabei handelt es sich um die Überprüfungsverfahren:

- Überwachen Sie die Seite des ACS, die anzeigt, welche Clients authentifiziert werden.

Sep 1, 13 4:56:49.220 AM	✓	teacher	00-21-5C-8C-C7-81	Default Network Access	PEAP (EAP-MSCHAPv2)	Default Network Group	10.105.135.176	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 Group	10.105.135.176	Capwap1	acstemplate

- Stellen Sie eine Verbindung zum DVA-WLAN mit der Student Group her, und überprüfen Sie die WiFi Connection Utility für Clients.

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

WiFi Networks (46)

Signal Strength	Network Name	Status	Security	Capabilities
Full	DVA	Connected	Yes	a, g, n
Full	<SSID not broadcast>		Yes	a, n
Full	<SSID not broadcast>		Yes	g, n
Full	<SSID not broadcast>		Yes	g, n

Buttons: Disconnect, Properties..., Refresh

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

WiFi On | Hardware radio switch: ON | Help? | Close

- Stellen Sie eine Verbindung zum DVA-WLAN mit der Teacher Group her, und überprüfen Sie die WiFi Connection Utility für Clients.

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

WiFi Networks (47)

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

Buttons: Disconnect, Properties..., Refresh, Profiles..., Close

WiFi On | Hardware radio switch: ON | Help?

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Hinweise:

Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

Nützliche Debugging-Tools umfassen **Debug-Client MAC-Adresse MAC** sowie folgende NGWC-Ablaufverfolgungsbefehle:

- **Ablaufverfolgungsgruppen-Wireless-Client-Level-Debuggen festlegen**
- **set trace group-wireless-client filter mac xxxx.xxxx.xxxx**
- **Spuren mit Spuren-Filter anzeigen**

Der NGWC-Trace enthält keinen dot1x/AAA-Wert. Verwenden Sie daher die gesamte Liste der kombinierten Traces für dot1x/AAA:

- **Ablaufverfolgungsgruppen-Wireless-Client-Level-Debuggen festlegen**
- **Ablaufverfolgung auf wcm-dot1x Ereignisebene debuggen**
- **Festlegen von trace wcm-dot1x aaa level debuggen**
- **Festlegen des Ablaufverfolgungs- und Wireless-Ereignisebenenendebuggens**
- **Festlegen des Ablaufverfolgungs-Zugriffssitzungs-Kerndebuggens**
- **Festlegen des Ablaufverfolgungszugriffs-Sitzungsmethode auf der 802.1x-Ebene-Debugging**
- **set trace group-wireless-client filter mac xxxx.xxxx.xxxx**
- **set trace wcm-dot1x event filter mac xxxx.xxxx.xxxx**
- **trace wcm-dot1x aaa filter mac festlegen xxxx.xxxx.xxxx**
- **Festlegen von Trace aaa Wireless-Ereignissen Filter MAC xxxx.xxxx.xxxx**
- **set trace access-session core sm filter mac xxxx.xxxx.xxxx**
- **Festlegen der Trace Access-Session-Methode dot1x filter mac xxxx.xxxx.xxxx**
- **Spuren mit Spuren-Filter anzeigen**

Wenn die dynamische VLAN-Zuweisung ordnungsgemäß funktioniert, sollte diese Ausgabe aus dem Debugger angezeigt werden:

```
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 lcd5 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 1ae1 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 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40

--More-- [09/01/13 12:08:59.553 IST 1ae3 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 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761

[09/01/13 12:08:59.553 IST 1ae5 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 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---

[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client

[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC)

[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile

MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761

[09/01/13 12:08:59.553 IST 1aeb 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 1aec 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 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)