

NGWCおよびACS 5.2によるダイナミック VLAN割り当ての設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[RADIUS サーバによるダイナミック VLAN 割り当て設定](#)

[ネットワーク図](#)

[前提](#)

[WLC の設定 \(CLI \)](#)

[WLAN の設定](#)

[WLC での RADIUS サーバの設定](#)

[クライアント VLAN の DHCP プールの設定](#)

[WLC の設定 \(GUI \)](#)

[WLAN の設定](#)

[WLC での RADIUS サーバの設定](#)

[RADIUS サーバの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、ダイナミック VLAN 割り当ての概念について説明します。また、無線 LAN (WLAN) クライアントを特定の VLAN にダイナミックに割り当てるようにワイヤレス LAN コントローラ (WLC) および RADIUS サーバを設定する方法について説明します。このドキュメントでは、RADIUS サーバは Cisco Secure Access Control System バージョン 5.2 が稼働する アクセスコントロール サーバ (ACS) です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WLC および Lightweight アクセス ポイント (LAP) に関する基本的な知識

- 認証、許可、アカウントイング (AAA) サーバの機能に関する知識
- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS® XE ソフトウェア リリース 3.2.2 が稼働する Cisco 5760 ワイヤレス LAN コントローラ (次世代ワイヤリング クローゼット (NGWC))
- Cisco Aironet 3602 シリーズ Lightweight アクセス ポイント
- Microsoft Windows XP と Intel Proset サプリカント
- Cisco Secure Access Control System バージョン 5.2
- Cisco Catalyst 3560 シリーズ スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

RADIUS サーバによるダイナミック VLAN 割り当て

一般的な WLAN システムでは、Service Set Identifier (SSID) (コントローラの用語では WLAN) に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。この方法は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを継承するために各クライアントを異なる SSID に関連付ける必要があるため、さまざまな制約があります。

一方、Cisco WLAN ソリューションでは、アイデンティティ ネットワーキングがサポートされています。この場合、ネットワーク上で 1 つの SSID のみをアドバタイズすることにより、特定のユーザはユーザ クレデンシャルに基づいて異なる QoS、VLAN 属性、セキュリティ ポリシーを継承できるようになります。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザを特定の VLAN に割り当てる機能です。ユーザを特定の VLAN に割り当てるタスクは、Cisco Secure ACS などの RADIUS 認証サーバによって処理されます。たとえば、この機能を利用すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てることができます。

したがって、クライアントがコントローラに登録済みの LAP への関連付けを試みると、LAP から RADIUS サーバにユーザのクレデンシャルが渡されて検証されます。認証に成功すると、RADIUS サーバからユーザに特定の Internet Engineering Task Force (IETF) アトリビュートが渡されます。これらの RADIUS アトリビュートにより、ワイヤレス クライアントに割り当てられる VLAN ID が決定されます。ユーザはこの事前設定済みの VLAN ID に常に割り当てられるので、クライアント (WLC に関しては WLAN) の SSID は無視されます。

VLAN ID の割り当てに使用される RADIUS ユーザ アトリビュートは次のとおりです。

- IETF 64 (Tunnel Type) : VLAN に設定します。
- IETF 65 (Tunnel Medium Type) : 802 に設定します。
- IETF 81 (Tunnel-Private-Group-ID) : VLAN ID に設定します。

VLAN ID は 12 ビットで、1 ~ 4094 の値 (両端の値を含む) を取ります。『[RFC 2868, RADIUS Attributes for Tunnel Protocol Support](#)』で定義されているように、IEEE 802.1X で使用される Tunnel-Private-Group-ID は文字列型であるため、VLAN ID の整数値は文字列としてエンコードされます。これらのトンネル アトリビュートが送信される際には、Tag フィールドの値を設定する必要があります。

RFC2868 の第 3.1 項には次のように明記されています。

「Tag フィールドは 1 オクテットの長さを持ち、同じトンネルを参照する同じパケット内の属性をグループ化する手段を提供することを目的としています。」

Tag フィールドで有効な値は、0x01 ~ 0x1F (両端の値を含む) です。Tag フィールドを使用しない場合は、このフィールドをゼロ (0x00) に設定する必要があります。すべての RADIUS 属性の詳細は、RFC 2868 を参照してください。

設定

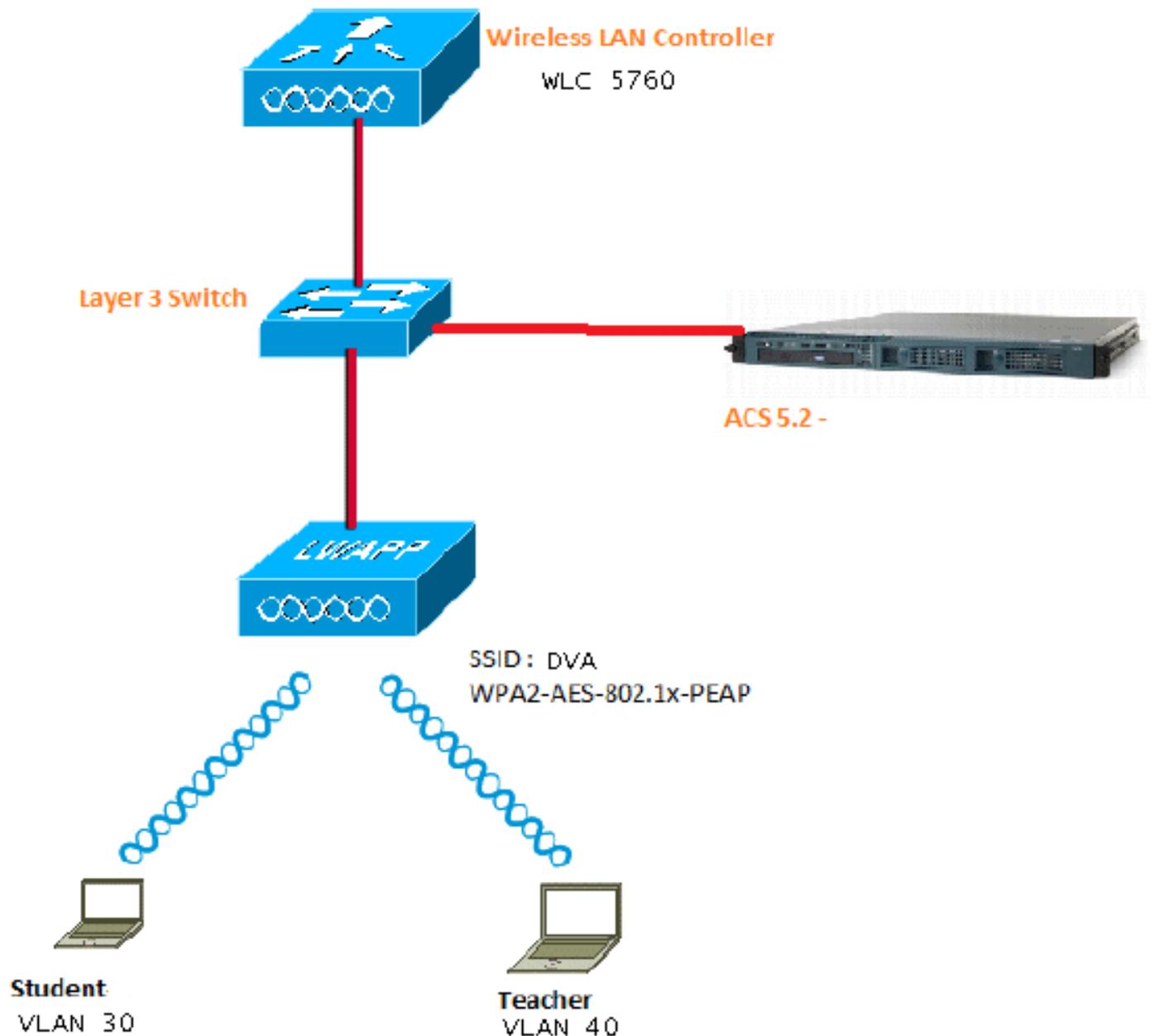
ダイナミック VLAN 割り当ての設定は、2 つの手順で行います。

1. コマンドライン インターフェイス (CLI) または GUI を使用して WLC を設定します。
2. RADIUS サーバを設定します。

注：このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録ユーザ専用 \)](#) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



このドキュメントでは、セキュリティメカニズムとして 802.1x と Protected Extensible Authentication Protocol (PEAP) を使用します。

前提

- スイッチには、レイヤ 3 (L3) VLAN がすべて設定されています。
- DHCP サーバには DHCP スコープが割り当てられています。
- ネットワーク内すべてのデバイス間では L3 接続が確立しています。
- LAP はすでに WLC に登録されています。
- 各 VLAN は /24 マスクを使用しています。
- ACS 5.2 には自己署名証明書がインストールされています。

WLC の設定 (CLI)

WLAN の設定

DVA の SSID を使用して WLAN を設定する方法を次の例に示します。

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

WLC での RADIUS サーバの設定

WLC での RADIUS サーバの設定例を次に示します。

```
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
```

クライアント VLAN の DHCP プールの設定

クライアント VLAN30 および VLAN40 の DHCP プールの設定例を次に示します。

```
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

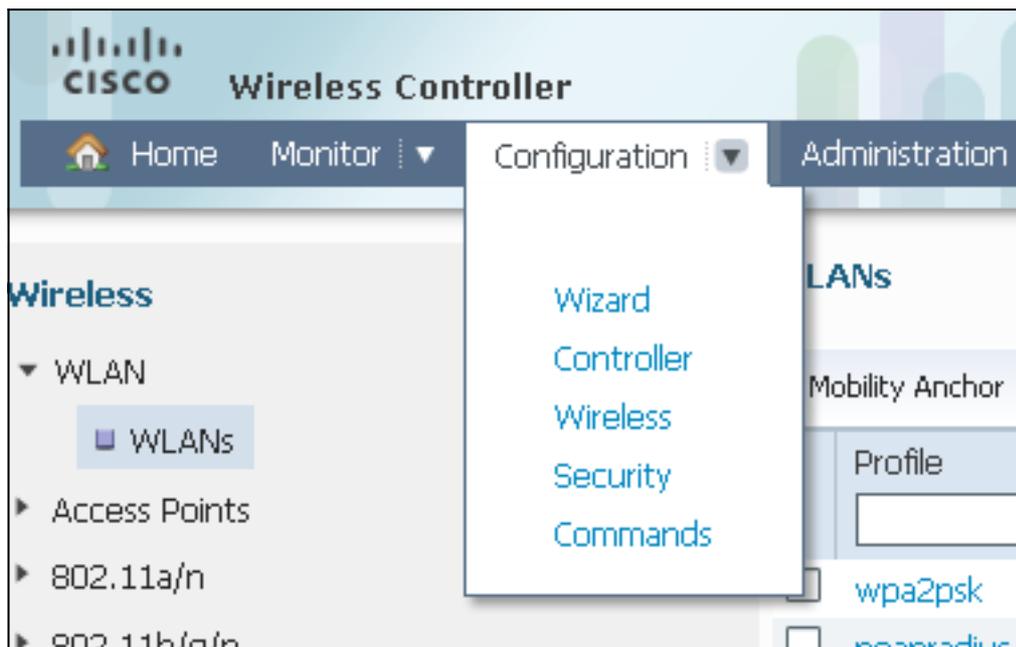
ip dhcp snooping vlan 30,40
ip dhcp snooping
```

WLC の設定 (GUI)

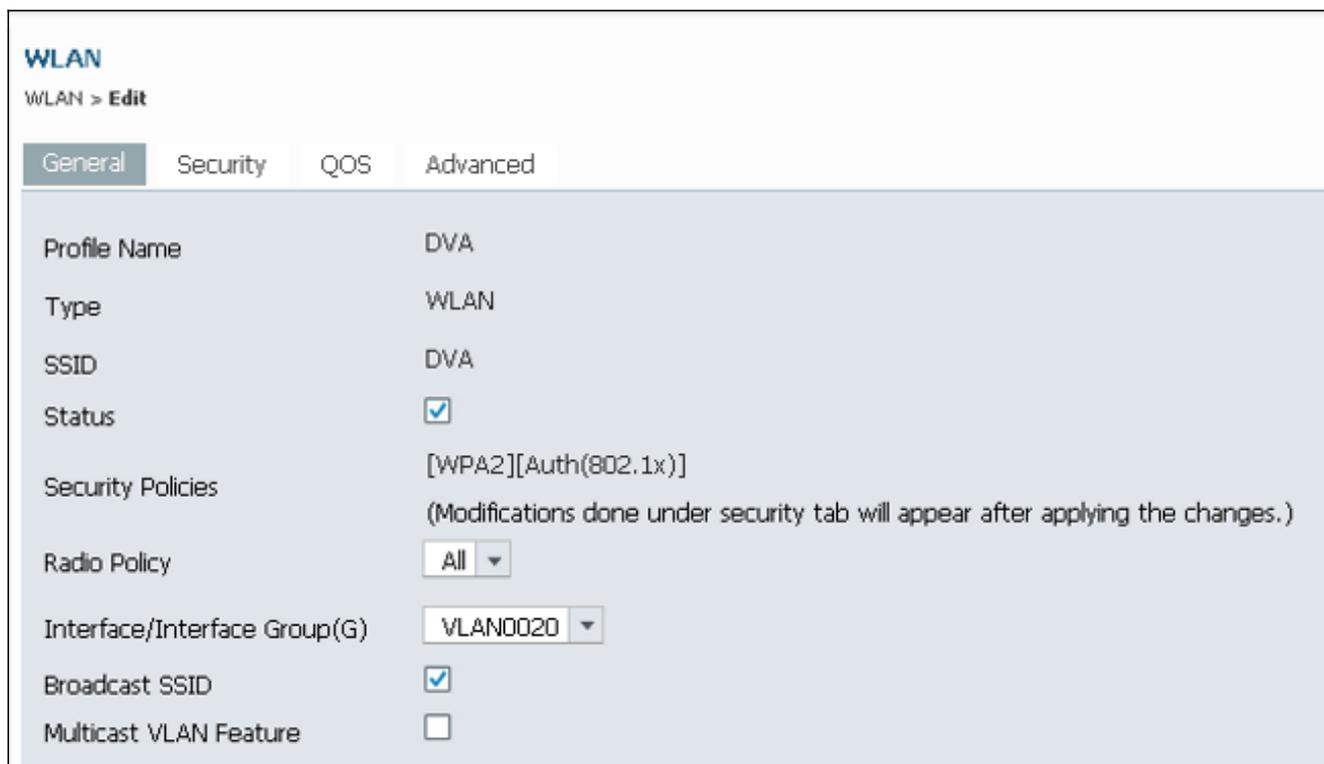
WLAN の設定

この手順では、WLAN を設定する方法について説明します。

1. [Configuration] > [Wireless] > [WLAN] > [New] タブに移動します。



2. [General] タブをクリックして、WLAN が WPA2-802.1X 向けに設定されており、インターフェイス/インターフェイス グループ (G) が VLAN 20 (VLAN0020) にマップされていることを確認します。



3. [Advanced] タブをクリックし、[Allow AAA Override] チェックボックスをオンにします。この機能を動作させるには、オーバーライドをイネーブルにする必要があります。

WLAN
WLAN > Edit

General Security QOS **Advanced**

Allow AAA Override

Coverage Hole Detection

Session Timeout (secs)

4. [Security] タブと [Layer2] タブをクリックし、[WPA2 Encryption AES] チェックボックスをオンにし、[Auth Key Mgmt] ドロップダウンリストから [802.1x] を選択します。

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

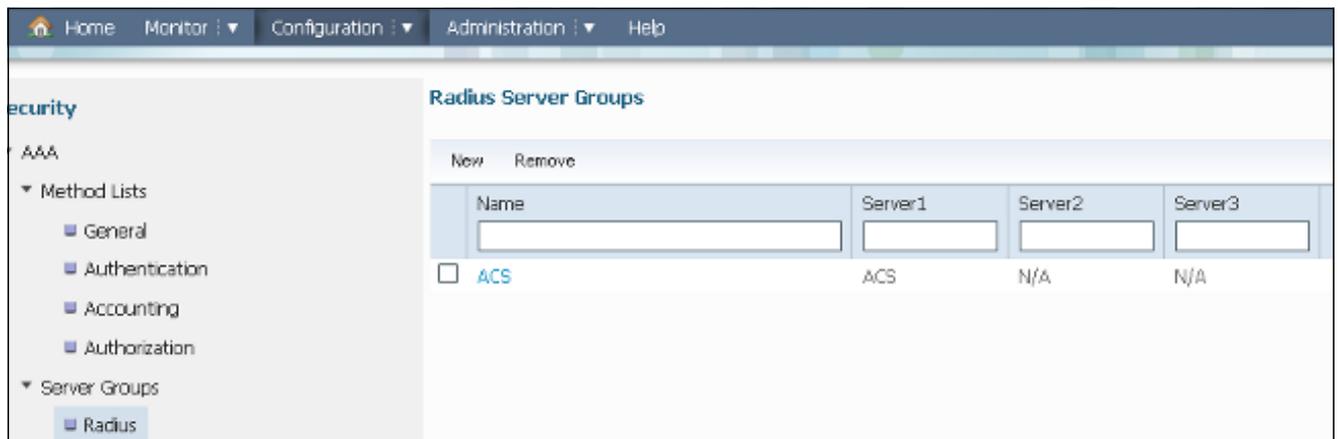
WLC での RADIUS サーバの設定

この手順では、WLC 上でローカル RADIUS サーバを設定する方法について説明します。

1. [Configuration] > [Security] タブに移動します。



2. RADIUS サーバグループを作成するため、[AAA] > [Server Groups] > [Radius] に移動します。次の例では、RADIUS サーバグループは ACS と呼ばれます。



3. RADIUS サーバのエントリを編集し、サーバ IP アドレスと共有秘密を追加します。この共有秘密は、WLC および RADIUS サーバの共有秘密と一致している必要があります。

The screenshot shows the Cisco Wireless Controller configuration interface. The top navigation bar includes Home, Monitor, Configuration, Administration, and Help. The left sidebar is under 'Security' and includes AAA, Method Lists (General, Authentication, Accounting, Authorization), Server Groups (Radius, Tacacs+, Ldap), and RADIUS (Servers). The main content area is titled 'Radius Servers' and shows the configuration for a server named 'ACS'. The fields are: Server Name: ACS; Server IP Address: 10.106.102.50; Shared Secret: [masked]; Confirm Shared Secret: [masked]; Acct Port (0-65535): 1646; Auth Port (0-65535): 1645; Server Timeout (0-1000) secs: [empty]; Retry Count (0-100): [empty].

完全な設定の例を次に示します。

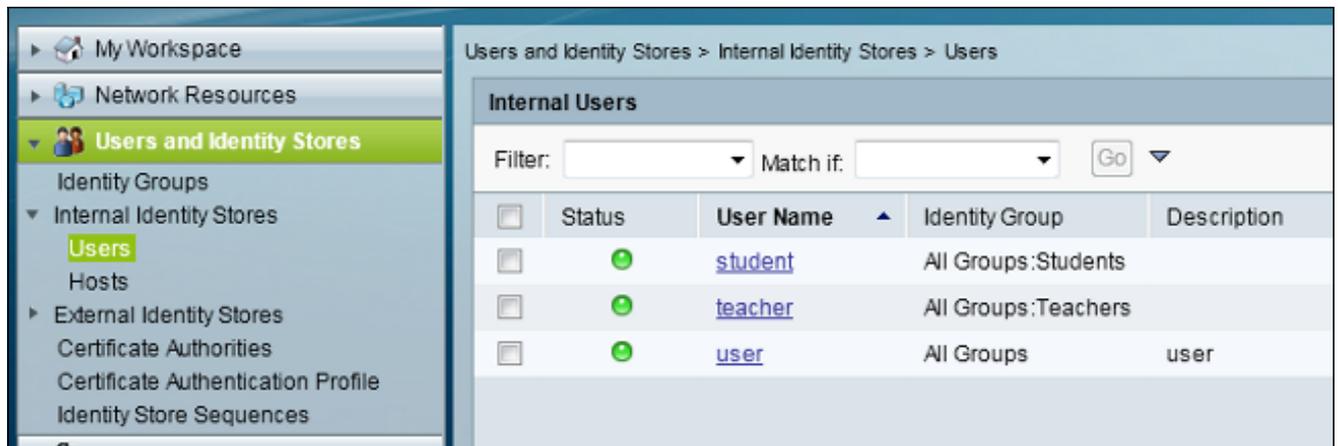
The screenshot shows the 'Radius Servers' configuration page with a table of servers. The table has columns for Server Name, Address, Auth Port, and Acct Port. There are 'New' and 'Remove' buttons above the table. One server is listed with the name 'ACS', address '10.106.102.50', auth port '1645', and acct port '1646'. There is a checkbox next to the server name.

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

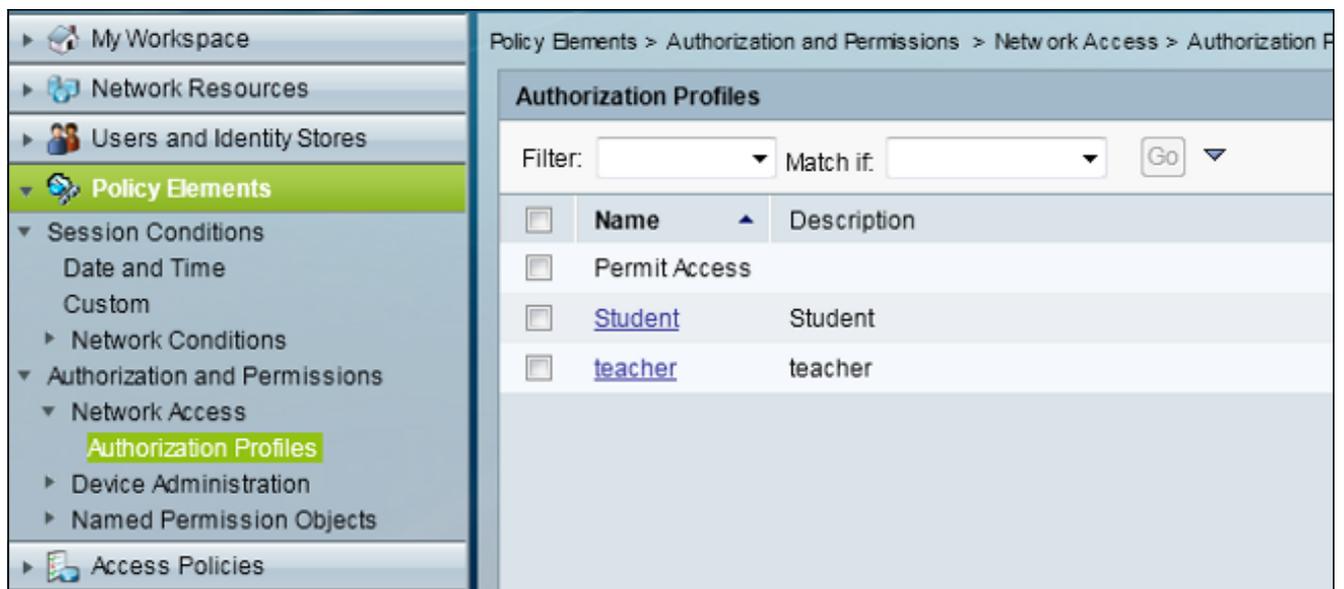
RADIUS サーバの設定

この手順では、RADIUS サーバを設定する方法について説明します。

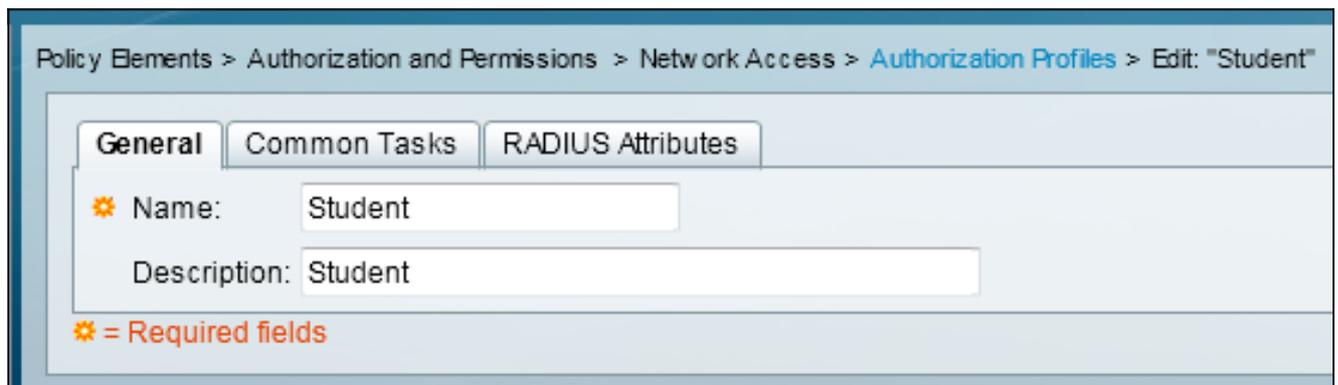
1. RADIUS サーバで、[Users and Identity Stores] > [Internal Identity Stores] > [Users] に移動します。
2. 適切なユーザ名と ID グループを作成します。この例では、[Student and All Groups:Students]と[Teacher and AllGroups:Teachers]です。



3. [Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] に移動し、AAA オーバーライドのための認証プロファイルを作成します。



4. Student の認証プロファイルを編集します。



5. [VLAN ID/Name] を [Static] に設定し、[Value] を 30 (VLAN 30) に設定します。

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. Teacher の認証プロファイルを編集します。

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

General Common Tasks RADIUS Attributes

⚙ Name: teacher
Description: teacher

⚙ = Required fields

7. [VLAN ID/Name] を [Static] および値 40 (VLAN 40) に設定します。

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

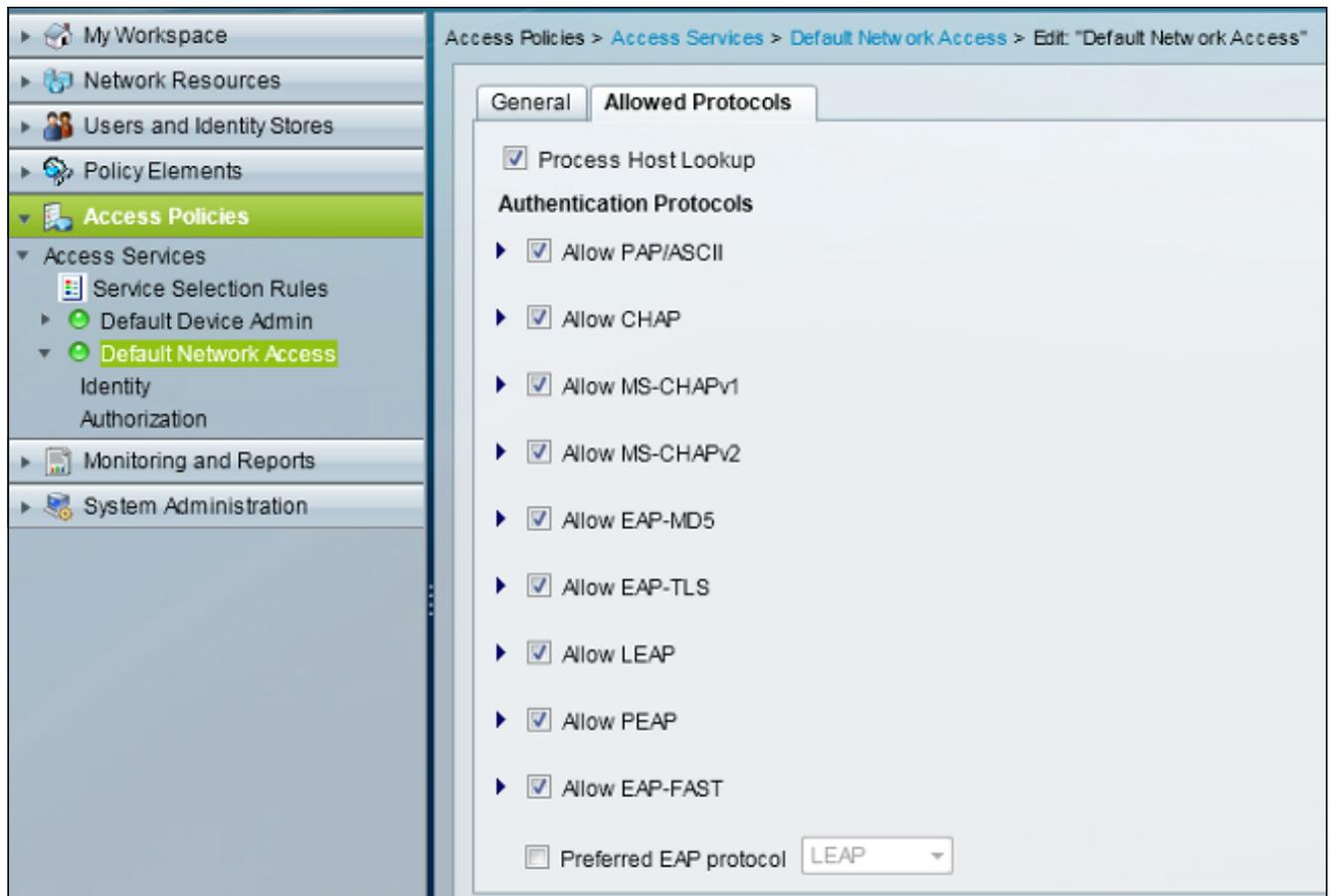
Reauthentication
Reauthentication Timer: Not in Use
Maintain Connectivity during Reauthentication:

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

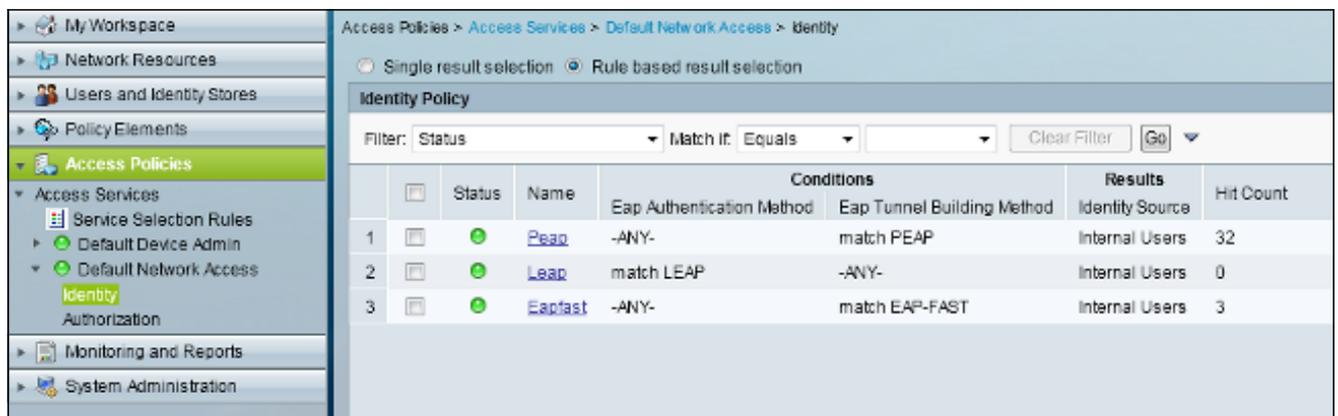
802.1X-REV
LinkSec Security Policy: Not in Use

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

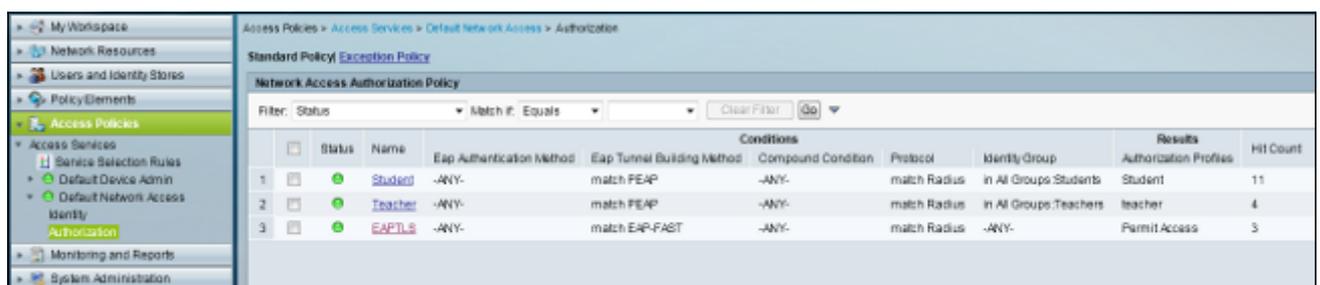
8. [Access Policies] > [Access Services] > [Default Network Access] に移動し、[Allowed Protocols] タブをクリックします。[Allow PEAP] チェックボックスをオンにします。



9. [Identity] に移動し、PEAP ユーザを許可するためのルールを定義します。



10. [Authorization] に移動し、Student と Teacher を Authorization Policy にマップします。この例では、マッピングは VLAN 30 の Student と VLAN 40 の Teacher です。



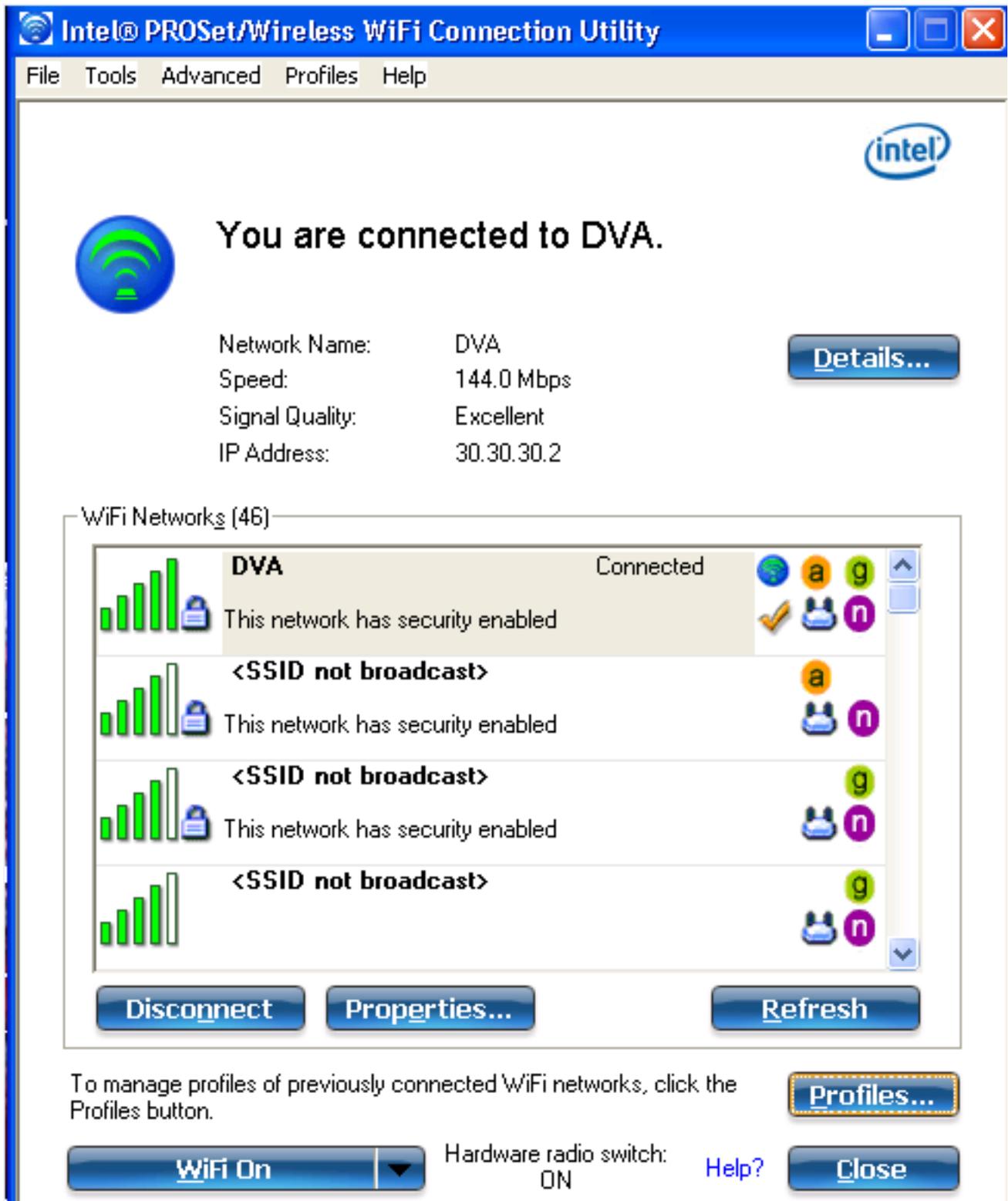
確認

ここでは、設定が正常に機能しているかどうかを確認します。次に検証プロセスを示します。

- ACS で、認証されるクライアントを示すページをモニタします。

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	ac.stemplete
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	ac.stemplete

- Student Group を使用して DVA WLAN に接続し、クライアントの Wifi Connection Utility を確認します。



- Teacher Group を使用して DVA WLAN に接続し、クライアントの WiFi Connection Utility を

確認します。

Intel® PROSet/Wireless WiFi Connection Utility

File Tools Advanced Profiles Help

intel

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	Icons
	DVA	Connected	This network has security enabled	a g n
	<SSID not broadcast>		This network has security enabled	a n
	<SSID not broadcast>		This network has security enabled	g
	<SSID not broadcast>		This network has security 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

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注：

このセクションで使用されるコマンドの詳細については、[Command Lookup Tool \(登録\)](#)

[ユーザ専用 \) を使用してください。](#)

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

debug コマンドを使用する前に、[「デバッグ コマンドの重要な情報」を参照してください](#)

有効なデバッグには、debug client mac-address *mac* や次の NGWC トレース コマンドがありません。

- set trace group-wireless-client level debug
- set trace group-wireless-client filter mac *xxxx.xxxx.xxxx*
- show trace sys-filtered-traces

NGWC トレースには dot1x/AAA が含まれないため、dot1x/AAA にはリストに示されているすべての結合トレースを使用します。

- set trace group-wireless-client level debug
- set trace wcm-dot1x event level debug
- set trace wcm-dot1x aaa level debug
- set trace aaa wireless events level debug
- set trace access-session core sm level debug
- set trace access-session method dot1x level debug
- set trace group-wireless-client filter mac *xxxx.xxxx.xxxx*
- set trace wcm-dot1x event filter mac *xxxx.xxxx.xxxx*
- set trace wcm-dot1x aaa filter mac *xxxx.xxxx.xxxx*
- set trace aaa wireless events filter mac *xxxx.xxxx.xxxx*
- set trace access-session core sm filter mac *xxxx.xxxx.xxxx*
- set trace access-session method dot1x filter mac *xxxx.xxxx.xxxx*
- show trace sys-filtered-traces

ダイナミック VLAN 割り当てが正しく機能している場合は、次のようなデバッグ出力が表示されます。

```
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 lcd4 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 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 laee 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 laef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config

[09/01/13 12:08:59.553 IST laf0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds

[09/01/13 12:08:59.553 IST laf1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)