

Alcatel · Lucent

IAP DYNAMIC VLAN

Technote

Versie: 1.0 Auteur: Herwin de Rijke Datum: 27 juli 2015

Alcadis | Vleugelboot 8 | 3991 CL Houten | www.alcadis.nl | 030 - 65 85 125

Inhoud

1	Inleiding		2
1.1		DOELSTELLING	2
1.2		BEOOGD PUBLIEK	2
1.3		VOORKENNIS/BENODIGDHEDEN	2
2	Configura	tie	3
2.1		INTERNAL DATABASE	3
2.2		EXTERNAL RADIUS SERVER	5
3	Gebruike	rservaring	9
3.1		WINDOWS CLIENTS	Э
3.2		ANDROID CLIENTS	Э
3.3		IPноме 10)

1 Inleiding

In dit document wordt beschreven hoe u een Alcatel-Lucent IAP moet configureren om gebruik te maken van het dynamisch toewijzen van VLAN's.

De instructies die in dit document gegeven worden gaan uit van een Engelstalige web interface van het access point en eventuele Engelstalige documentatie. Mocht u de web interface ingesteld hebben op de Nederlandse taal dan zullen de stappen hetzelfde zijn, maar de benaming van de menu's zullen verschillen.

De instructies die in dit document gegeven worden zijn op basis van firmware versie 6.4.2.3-4.1.1.3_48994. Wij raden aan om uw access points te upgraden naar deze versie of hoger. Mogelijk is deze functie in eerdere versies niet beschikbaar of werkt de functie anders als in deze technote wordt aangegeven.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met de configuratie stappen om Dynamic VLAN's werkend te krijgen met een IAP. Dit kan door gebruik te maken van de interne gebruikers database of door het gebruik van een externe RADIUS server. Het toewijzen van een Dynamische VLAN kan worden gebruikt als u het aantal SSID's wilt beperken maar draadloze gebruikers toch wilt onderverdelen in verschillende netwerken. Een voorbeeld hiervan is een Business Center waar veel bedrijven zijn samengevoegd in 1 pand.

Bij het gebruik van een access point of SSID voor ieder bedrijf zal de SSID overhead te groot worden of zullen de vele access points elkaar negatief gaan beïnvloeden wat ten koste gaat van de performance van het Wi-Fi netwerk.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel die een Alcatel-Lucent IAP willen configureren voor het gebruik van dynamische VLAN's.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- Alcatel-Lucent IAP web interface.
- Beheren van een omgeving met verschillende VLAN's, ook het achterliggende netwerk met bijbehorende DHCP server(s) worden hiermee bedoeld.
- Eventueel configuratie van een externe RADIUS server zoals FreeRADIUS.

2 Configuratie

Een Alcatel-Lucent IAP kan op twee verschillende manier worden geconfigureerd voor het gebruik van Dynamische VLAN's. Beide opties werken op een vergelijkbare manier maar er zijn andere stappen hiervoor vereist. Daarom zullen de twee methoden apart worden behandeld.

2.1 Internal Database

Er zijn meerdere manieren om met behulp van de interne database dynamische VLAN's te gebruiken. In dit voorbeeld zal worden gefilterd op een gedeelte van de gebruikersnaam. Voor elke gebruiker zal een gebruikersnaam moeten worden aangemaakt in de interne database die een unieke waarde (bijvoorbeeld naam van het bedrijf) bevat. Om Dynamische VLAN's te configureren met het gebruik van de interne database volgt u onderstaande stappen:

- 1. Login op de web GUI van de virtuele controller.
- 2. Onder "3 Networks" klikt u op "New".

		•				
Alcatel·Lucent 🕢 Urgan Instant-	CC:69:C9					Search
🛞 3 Networks +	1 Access Point	+	🔜 1			+
New	Name 🚽	Clients	Name +	IP Address	Network	Access Point
	24:de:c6:cc:69:c9 *	8	android-472ba8277	192.168.11.37		24:de:c6:cc:69:c9

- 3. Er wordt een tabblad geopend "New WLAN".
- 4. In het tabblad **"1 WLAN Settings"** geeft u een SSID op en kiest u bij **"Primary usage"** voor **"Employee"**.
- 5. Eventueel kunt u door middel van **"Show advanced options"** extra instellingen zoals een bandbreedte beperking configureren.

New WLAN					<u>Help</u>
1 WLAN Settings	2 VLAN	3	Security	4	Access
WLAN Settings					
Name & Usage					
Name (SSID):	Business Center				
Primary usage:	 Employee Voice Guest 				
Show advanced options					Next Cancel

- 6. In het tabblad "2 VLAN" kiest u bij "Client IP assignment" voor "Network assigned". Let hierbij wel op dat in elke VLAN een DHCP server actief moet zijn. Ook is het mogelijk een DHCP server te gebruiken die op basis van de VLAN-id's een IP-adres toewijst. Het gebruik van de interne DHCP server is niet mogelijk.
- 7. Bij "Client VLAN assignment" kiest u voor "Dynamic".
- 8. Onder **"VLAN assignment Rules"** maakt u voor ieder bedrijf een regel aan zoals aangegeven is in onderstaand afbeelding.

Ne	w WLAN								<u>Help</u>
1	WLAN Settings	2 \	'LAN	3	Security		4	Access	
C	ient IP & VLAN As	ssignment							
	Client IP assignment:	O Virtual Cor	troller managed						
		Network a	ssigned						
	Client VLAN assignment:	Default							
		Static							
		Oynamic							
[VLAN Assignment Rules								
	If User-Name contains B	edrijfX assign	VLAN 10						
	If User-Name contains E	edrijfY assign	VLAN 20						
	Default VLAN: 1								
ĺ	New VLAN Assignment	Rule				I			
	Attribute: Op	erator:	String:	VLAN:					
	User-Name V Co	ntains 🔻	BedriifZ	30					
				OK Can	cel				

- 9. In het tabblad "3 Security" kiest u bij "Security Level" voor "Enterprise".
- 10. Bij "Key Management" kiest u voor "WPA-2 Enterprise".
- 11. Bij "Authentication server 1:" kiest u voor "Internalserver".
- 12. Bij "Reauth interval:" kiest u voor "O minuten".
- 13. Achter **"Internal Server"** kunt u door op **"Users"** te klikken gebruikers aanmaken in de interne database.

Edit Business Center				<u>Help</u>
1 WLAN Settings	2 VLAN	3 Security	4 Access	
Security Level				
More Secure Personal Open Less Secure	Key management: Termination: Authentication server 1: Reauth interval: MAC authentication: Internal server: Internal server: Blacklisting: Fast Roaming Opportunistic Key Caching(OKC	WPA-2 Enterprise Disabled InternalServer Perform MAC authenticati MAC authentication fail-th <u>6 Users</u> Default certificate <u>Upload cer</u> Disabled C):	 T T on before 802.1X ru ertificate T 	
	802.11r: 802.11k:			
	802.11v:			

14. In het venster "Users" wat nu opent kunt u de verschillende gebruikers aanmaken. Elke gebruikersnaam moet een unieke waarde van het bedrijf bevatten zoals aangegeven is in onderstaande afbeelding. Deze unieke waarde moet weer corresponderen met de waarden die u heeft opgegeven in "stap 8".

New WL	AN .				<u>Help</u>
1 WLA	N Settings	2 VLAN	3 Security	4 Access	
More Secure Pe Ol Less Secure	Users(5) BedrijfX-User1 BedrijfX-User2 BedrijfY-User1 BedrijfZ-User1	Type Employee Employee Employee Employee	Add new user: Username: BedrijfZ-User2 Password: Retype: Type Type Employee Add	Help 3P	
_				OK Cancel	

15. In het tabblad **"4 Access"** kunt u **"Access Rules"** gewoon op **"Unrestricted"** laten staan.

					neip
2	VLAN	3	Security	4	Access
No re	strictions on access based on d	estin	ation or type of traffic		
	2 No re	2 VLAN	2 VLAN 3	2 VLAN 3 Security	2 VLAN 3 Security 4 No restrictions on access based on destination or type of traffic

2.2 External Radius server

Dynamische VLAN's zijn ook mogelijk door het gebruik van een externe RADIUS server zoals **"FreeRADIUS"**. In dit voorbeeld zal gebruik worden gemaakt van het attribute **"Filter-id"**. Elke attribute die in de lijst kan worden geselecteerd en door de RADIUS server kan worden teruggegeven als unieke waarde per bedrijf kan hiervoor worden gebruikt. Het voordeel van deze methode is dat u geen bedrijfsnaam in de gebruikersnaam hoeft te verwerken. Om Dynamische VLAN's te configureren met gebruik van een externe RADIUS server volgt u onderstaande stappen:

- 1. Login op de web GUI van de virtuele controller.
- 2. Onder "3 Networks" klikt u op "New".

Alcatel-Lucent 🕡 Vitai Controler Instant-CC:69:C9								
🖗 3 Networks +	1 Access Point	+	🔜 1			+		
New	Name – Clie	nts	Name +	IP Address	Network	Access Point		
	24:de:c6:cc:69:c9 *	8	android-472ba8277	192.168.11.37		24:de:c6:cc:69:c9		

- 3. Er wordt een tabblad geopend "New WLAN".
- 4. In het tabblad **"1 WLAN Settings"** geeft u een SSID op en kiest u bij **"Primary usage"** voor **"Employee"**.
- 5. Eventueel kunt u door middel van **"Show advanced options"** extra instellingen zoals een bandbreedte beperking instellen.

New WLAN			He
1 WLAN Setting	s 2 VLAN	3 Security	4 Access
WLAN Settings			
Name & Hoage			
Name & Usage			
Name (SSID):	Business Center		
Primary usage:	Employee		
	Voice		
	Guest		
Show advanced optio	ns		Next Cancel

- 6. In het tabblad "2 VLAN" kiest u bij "Client IP assignment" voor "Network assigned". Let hierbij wel op dat in elke VLAN een DHCP server actief moet zijn. Ook is het mogelijk een DHCP server te gebruiken die op basis van de VLAN-id's een IP-adres toewijst. Het gebruik van de interne DHCP server is niet mogelijk.
- 7. Bij "Client VLAN assignment" kiest u voor "Dynamic".
- 8. Onder **"VLAN assignment Rules"** maakt u voor ieder bedrijf een regel aan zoals aangegeven in onderstaand afbeelding.

New WLAN							<u>Help</u>
1 WLAN Settings	2	/LAN	3	Security	4	Access	
Client IP & VLAN As	signment						
Client IP assignment:	 Virtual Co Network a 	ntroller managed ssigned					
Client VLAN assignment:	 Default Static Dynamic 						
VLAN Assignment Rules If Filter-Id equals Bedriji If Filter-Id equals Bedriji Default VLAN: 1	fX assign VLAI f <mark>Y assign VLAI</mark>	V 10 V 20					
New VLAN Assignment Attribute: Op Filter-Id V eq	Rule erator: µuals ▼	String: BedrijfZ	VLAN: 30 OK Cance	- - -			

- 9. Onder "Security Level" kiest u voor "Enterprise".
- 10. Achter "Key management" kiest u voor "WPA-2 Enterprise".
- 11. Achter **"Authentication Server 1:"** kiest u een RADIUS server die u eerder heeft geconfigureerd of u kiest voor **"New"** om een nieuwe RADIUS server in te stellen. Omdat er veel verschillende RADIUS servers gebruikt kunnen worden zal de configuratie van deze server in dit document niet worden beschreven. Belangrijk is dat de RADIUS server de juiste attributes teruggeeft op basis van de inloggegevens van de gebruikers.

Edit	Business Center				<u>Help</u>
1	WLAN Settings	2 VLAN	3 Security	4 Access	
Sec	curity Level				
Mo	ore	Key management:	WPA-2 Enterprise 🔻		
1	1	Termination:	Disabled v		
	- Enterprise	Authentication server 1:	FreeRadiusq 🔹	Edit	
		Authentication server 2:	Select Server 🔻		
	Personal	Reauth interval:	0 hrs. ▼		
	Open	Authentication survivability:	Disabled 🔻		
		MAC authentication:	Perform MAC authentication	before 802.1X	
			MAC authentication fail-thru		
Se	cure	Accounting:	Disabled 🔻		
		Blacklisting:	Disabled 🔻		
		Fast Roaming			
		Opportunistic Key Caching(OKC)	:		
		802.11r:			
		802.11k:			
		802.11v:			

12. In het tabblad **"4 Access"** kunt u **"Access Rules"** gewoon op **"Unrestricted"** laten staan.

New WLAN				<u>Help</u>
1 WLAN Settings	2 VLAN	3 Security	4 Access	
Access Rules				
More Control - Role-based - Network-based - Unrestricted Less Control	No restrictions on access b	ased on destination or type of traffic		

3 Gebruikerservaring

Nadat u de instellingen hebt aangemaakt, zoals aangegeven in hoofdstuk "**2 Configuratie**" en u het IAP heeft aangesloten in het netwerk waarop de juiste DHCP server(s) actief zijn, is het systeem gereed voor gebruik.

In onderstaande beschrijving wordt weergegeven welke stappen de gebruikers moeten nemen om verbinding te maken met het netwerk.

3.1 Windows clients

Om een Windows client toe te voegen aan het eerder genoemde netwerk met Dynamische VLAN's verbindt u de client met het SSID en vult u de gebruikersnaam en het wachtwoord van de gebruiker in. Op basis van de gebruikersnaam en-of groep waartoe deze behoort wordt deze het bijbehorende VLAN geplaatst.

Business Center	lte.	Windows-beveiliging Netwerkverificatie Voer uw gebruikersgegevens in
Automatisch Verbinding maken	Verbinding <u>m</u> aken	Sebruikersnaam Wachtwoord OK Annuleren

3.2 Android Clients

Om een Android client toe te voegen aan het eerder genoemde netwerk met Dynamische VLAN's verbindt u de client met het SSID en vult u de gebruikersnaam en het wachtwoord van de gebruiker in. Op basis van de gebruikersnaam en-of groep waartoe deze behoort wordt deze in het bijbehorende VLAN geplaatst.

	★ ▼⊿ 🖹 11:32
۷	Business Center
A	IP-adres 192.168.10.118
	EAP-methode PEAP
	Phase 2-verificatie Geen
	CA-certificaat (niet opgegeven)
	Identiteit
	BedrijfX-User1
	Anonieme identiteit
	Wachtwoord
	(ongewijzigd)
	Wachtwoord weergeven
	ANNULEREN OPSLAAN

3.3 IPhone

Om een iPhone client toe te voegen aan het eerder genoemde netwerk met Dynamische VLAN's verbindt u de client met het SSID en vult u de gebruikersnaam en het wachtwoord van de gebruiker in. Het gevraagde certificaat kunt u accepteren. Op basis van de gebruikersnaam en-of groep waartoe deze behoort wordt deze in het bijbehorende VLAN geplaatst.

Geen simkaart	11:35	e -	Geen simkaart 11:35 @	Geen simkaart 🗢 11:36	•
Voer het wachtwoord in voor 'Business Center'			Wachtwoord Certificaat Wi-Fi Business Center		ter
Annuleer	Wachtwoord	Verbind			
securelogin.arubanetwo			Vergeet dit netwerk		
Gebruikersnaam BedrijfY-User1		User1	Niet gecontroleerd Accepteer	IP-ADRES	
			Beschrijving Clientidentiteitscontrole	DHCP BootP	Statisch
			Verloopt 11 aug. 2017 06:40:59	ID advact d	00 100 00 00
			Meer details >	IP-adres 1	92.168.20.60
123	4 5 6 7	890		Subnetmasker 2	55.255.255.0
- / :	; () €	& @ "		Router	192.168.20.2
#+=	, ? !	, 💌		DNS	8.8.8.8
ABC	spatie	return		Zoekdomeinen	VLAN20