Configurazione di OEAP e RLAN su Catalyst 9800 WLC

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete AP Join dietro NAT Configurazione Verifica Accedere a OEAP e configurare il SSID personale Configurazione di RLAN su 9800 WLC Risoluzione dei problemi

Introduzione

Questo documento spiega come configurare Cisco OfficeExtend access point (OEAP) e la RLAN (Remote Local Area Network) su 9800 WLC.

Un punto di accesso Cisco OfficeExtend (OEAP) fornisce comunicazioni sicure da un controller a un Cisco AP in una postazione remota, estendendo senza problemi la WLAN aziendale su Internet fino alla residenza di un dipendente. L'esperienza dell'utente nel suo ufficio di casa è esattamente la stessa che avrebbe nel suo ufficio aziendale. La crittografia Datagram Transport Layer Security (DTLS) tra un punto di accesso e il controller assicura che tutte le comunicazioni abbiano il massimo livello di sicurezza.

Una LAN remota (RLAN) viene utilizzata per autenticare i client cablati tramite il controller. Quando il client cablato si unisce correttamente al controller, le porte LAN commutano il traffico tra la modalità di commutazione centrale e locale. Il traffico proveniente dai client cablati viene considerato traffico client wireless. L'access point RLAN invia la richiesta di autenticazione per autenticare il client cablato. L'autenticazione dei client cablati nella RLAN è simile a quella del client wireless centrale autenticato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- 9800 WLC
- Accesso CLI (Command-Line Interface) ai controller e ai punti di accesso wireless

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9800 WLC versione 17.02.01
- Serie 1815/1810 AP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



AP Join dietro NAT

Nei codici 16.12.x, è necessario configurare l'indirizzo IP NAT dalla CLI. Nessuna opzione GUI disponibile. È inoltre possibile selezionare il rilevamento CAPWAP tramite IP pubblico o privato.

```
(config) #wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface) #capwap-discovery ?
  private Include private IP in CAPWAP Discovery Response
```

public Include public IP in CAPWAP Discovery Response

Nei codici 17.x, selezionare **Configurazione > Interfaccia > Wireless** e fare clic su **Wireless Management Interface** (Interfaccia di gestione wireless) per configurare il tipo di rilevamento NAT IP e CAPWAP dalla GUI.

Configuration * > Interface * > Wireless	Edit Management Interface		×
+ Add X Delete	Interface Trustpoint	Vian1119 Search or Select	•
Interface Name ✓ Interface Type ✓ Trustpoint Name ✓ VLAN ID Vian1119 Management 1119 I I Imagement 1119 I I Imagement 1119	NAT Status IPv4 / IPv6 Server Address CAPWAP Discovery	ENABLED X.X.X. Invalid IP address Private	Public
	Cancel		Update & Apply to Device

Configurazione

1. Per creare un profilo Flex, abilitare **Office Extend AP** e passare a **Configurazione > Tag e profili > Flex.**

Add Flex Profile						
General Local Authentication Policy ACL VLAN Umbrella						
Name*	OEAP-FLEX	Fallback Radio Shut				
Description	OEAP-FLEX	Flex Resilient				
Native VLAN ID	37	ARP Caching				
HTTP Proxy Port	0	Efficient Image Upgrade				
HTTP-Proxy IP Address	0.0.0.0	Office Extend AP				
CTS Policy		Join Minimum Latency				

2. Per creare un tag del sito e un profilo Flex mappa, passare a **Configurazione > Tag e profili > Tag.**

Add Site Tag



3. Passare alla voce 1815 AP con il tag del sito creato da **Configuration > Wireless Setup >** Advanced > Tag AP.



Changing AP Tag(s) will cause associated AP(s) to reconnect



Verifica

Una volta che l'access point 1815 si è nuovamente unito al WLC, verificare questo output:

vk-9800-1#show ap name AP1815 config general

Cisco AP Name : AP1815	
Cisco AP Identifier	: 002c.c8de.3460
Country Code	: Multiple Countries : IN,US
Regulatory Domain Allowed by Country	: 802.11bg:-A 802.11a:-ABDN
AP Country Code	: US - United States
Site Tag Name	: Home-Office
RF Tag Name	: default-rf-tag
Policy Tag Name	: default-policy-tag
AP join Profile	: default-ap-profile
Flex Profile	: OEAP-FLEX
Administrative State	: Enabled
Operation State	: Registered
AP Mode	: FlexConnect
AP VLAN tagging state	: Disabled
AP VLAN tag	: 0
CAPWAP Preferred mode	: IPv4
CAPWAP UDP-Lite	: Not Configured
AP Submode	: Not Configured
Office Extend Mode	: Enabled
Dhcp Server	: Disabled
Remote AP Debug	: Disabled

vk-9800-1**#show ap link-encryption**

	Encryption	Dnstream	Upstream	Last
AP Name	State	Count	Count	Update
N2	Disabled	0	0	06/08/20 00:47:33

865

when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled automatically.

43

AP1815#show capwap client config

AdminState	:	ADMIN_ENABLED(1)
Name	:	AP1815
Location	:	default location
Primary controller name	:	vk-9800-1
ssh status	:	Enabled
ApMode	:	FlexConnect
ApSubMode	:	Not Configured
Link-Encryption	:	Enabled
Link-Encryption OfficeExtend AP	:	Enabled
Link-Encryption OfficeExtend AP Discovery Timer	:	Enabled Enabled
Link-Encryption OfficeExtend AP Discovery Timer Heartbeat Timer	•••••••••••••••••••••••••••••••••••••••	Enabled 10 30
Link-Encryption OfficeExtend AP Discovery Timer Heartbeat Timer Syslog server	•	Enabled 10 30 255.255.255.255
Link-Encryption OfficeExtend AP Discovery Timer Heartbeat Timer Syslog server Syslog Facility	• • • •	Enabled Enabled 10 30 255.255.255.255

Nota: È possibile abilitare o disabilitare la crittografia dei dati DTLS per un punto di accesso specifico o per tutti i punti di accesso utilizzando il comando ap link-encryption

vk-9800-1(config)#ap profile default-ap-profile

vk-9800-1(config-ap-profile) #no link-encryption

Disabling link-encryption globally will reboot the APs with link-encryption.

Are you sure you want to continue? (y/n)[y]:y

Accedere a OEAP e configurare il SSID personale

1. È possibile accedere all'interfaccia Web dell'OEAP con il relativo indirizzo IP. Le credenziali predefinite per l'accesso sono **admin** e **admin**.

2. Si consiglia di modificare le credenziali predefinite per motivi di sicurezza.

uluilu cisco	НОМЕ	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP	
<u>System</u> 2.4GHz	Configura	tion				
5GHz	Username		admin			
SSID	Password					
DHCP	Radio					
WAN	Radio Interfa	ce	5Ghz			
	Status		Enabled 😳			
Firewall	802.11 n-mo	de	Enabled 😳			
Declary (Dectary	802.11 ac-me	ode	Enabled 📀			
Backup/Restore	Bandwidth		40 Mhz ᅌ			
	Channel Sele	ction	40 ᅌ			
	@2010 - 2016 Cisco Sy	stems Inc. All rights reserved.				

3. Passare a Configuration> SSID> 2.4GHz/5GHz per configurare il SSID personale.

cisco	HOME CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP	Refresh Logout TELEWORKER
CISCO System SSID 2.4GHz SGHz DHCP WAN	Configuration Personal Network Recio Interfee Ensited Breadmark SSID MAC Filter	2.4 0.4z 2 2 Home-ssid	DMGNOSTICS		
Firewall	Enabled	_0			
Backup/Restore		MAC Address	Description	MAC Address Description	
	Security WPA-P5K WPA2-P5K WPA Encryption WPA passphrase	Clashied C Brabled C	Click here to display		

- 4. Abilitare l'interfaccia radio.
- 5. Inserire il SSID e abilitare la trasmissione

6. Per la cifratura, scegliere **WPA-PSK** o **WPA2-PSK** e inserire la passphrase per il tipo di sicurezza corrispondente.

7. Fare clic su Applica per rendere effettive le impostazioni.

8. Per impostazione predefinita, i client che si connettono al SSID personale ottengono l'indirizzo IP dalla rete 10.0.0.1/24.

9. Gli utenti privati possono usare lo stesso access point per connettersi e per comunicare che il traffico non viene trasmesso tramite il tunnel DTLS.

10. Per controllare le associazioni client su OEAP, selezionare **Home > Client**. È possibile visualizzare i client locali e aziendali associati a OEAP.

ululu cisco	HOME	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP			Refresh Logout TELEWORKER
AP Info	Associatio	on						
SSID								Show all
Client	Local Clien Client MAC	ts	Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	00:17:7C:88:	13:08	10.0.0.59		Home-ssid	2.4GHz	00d:00h:24m:55s	332/101
	Corporate	Clients	Client ID		WI AN OFT	Profile (1.6M	Accession Time	Bisto Te / Out
	Cheft MAC	AF.F.	Chent IP		WLAN SSID	Radio/LAN	Association Time	PRES IN/ OUC
	50:36:AA:B7:	06354	10.106.37.115		corporate-ssid	2.4GHz	000:00n:07m:095	433/503

To clear personal ssidfrom office-extend ap

ewlc#ap name cisco-ap clear-personalssid-config

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP

Configurazione di RLAN su 9800 WLC

Una LAN remota (RLAN) viene utilizzata per autenticare i client cablati tramite il controller. Quando il client cablato si unisce correttamente al controller, le porte LAN commutano il traffico tra la modalità di commutazione centrale e locale. Il traffico proveniente dai client cablati viene considerato traffico client wireless. L'access point RLAN invia la richiesta di autenticazione per autenticare il client cablato. OSPF (Open Shortest Path First)

L'autenticazione dei client cablati nella RLAN è simile a quella del client wireless centrale autenticato.

Nota: In questo esempio, per l'autenticazione dei client RLAN viene utilizzato il protocollo EAP locale. La configurazione EAP locale deve essere presente sul WLC per configurare i passaggi seguenti. Include metodi di autenticazione e autorizzazione aaa, profilo EAP locale e credenziali locali.

Esempio di autenticazione EAP locale su Catalyst 9800 WLC

1. Per creare il profilo RLAN, selezionare **Configurazione > Wireless > LAN remota** e immettere un nome e un ID RLAN per il profilo RLAN, come mostrato nell'immagine.

Add	I RLAN Profile		×
Ger	neral Security		
	Profile Name*	RLAN-TEST	
	RLAN ID*	1	
	Status		-
	Client Association Limit	0	
	mDNS Mode	Bridging •	
_			
5	Cancel		Apply to Device

2. Selezionare **Security > Layer2** per abilitare 802.1x per una RLAN, impostare lo stato 802.1x su Enabled, come mostrato nell'immagine.

Edit RLAN Profile						
General	Security					
Layer2	ayer3	AAA				
802.1x						
MAC Filtering			Not Configured	•		
Authentication	List		default	•		

3. Passare a **Sicurezza > AAA**, impostare Autenticazione EAP locale su Abilitata e scegliere il nome del profilo EAP richiesto dall'elenco a discesa, come mostrato nell'immagine.

Edit RLAN Profile						
General	Security					
Layer2	Layer3	AAA				
Local EAP	Authenticatio	n	ENABLED			
EAP Profile	e Name		Local-EAP 🔹			

4. Per creare la policy RLAN, selezionare **Configurazione > Wireless > LAN remota** e nella pagina LAN remota fare clic sulla scheda **Policy RLAN**, come mostrato nell'immagine.

Ec	lit RLAN	Policy			×
G	eneral	Access Policies	Advanced		
		A (Configuring in enabled state will result in lo	ss of connectivity for clients associated with this policy.	
	Policy N	ame*	RLAN-Policy	RLAN Switching Policy	
	Descript	tion	Enter Description	Central Switching	
	Status			Central DHCP	
	PoE				
	Power L	evel	4 •		

Passare a Criteri di accesso, configurare la VLAN e la modalità host e applicare le impostazioni.

dit RLAN Policy		
General Access Policies	Advanced	
Pre-Authentication		Host Mode singlehost
VLAN	VLAN0039 +	
Remote LAN ACL		
IPv4 ACL	Not Configured	
IPv6 ACL	Not Configured	

5. Per creare un tag di policy e mappare il profilo RLAN sulla policy RLAN, selezionare **Configurazione > Tag e profili > Tag.**

Add Policy Tag			×
Name*	RLAN-TAG		
Description	Enter Description		
> WLAN-POLICY	/ Maps: 0		
✓ RLAN-POLICY	Maps: 0		
+ Add × Del	ete		
Port ID	 RLAN Profile 	KLAN Policy Prof	ile 🗸
⊲ ⊲ 0 ⊨ ⊨	10 🔻 items per page		No items to display
Map RLAN and Poli	су		
Port ID*	3 🔹		
RLAN Profile*	RLAN-TEST 🔻	RLAN Policy Profile*	RLAN-Policy v
Cancel			Apply to Device

Add Policy Tag					×
Name*	RLAN-TAG				
Description	Enter Description				
> WLAN-POLICY	/ Maps: 0				
✓ RLAN-POLICY	Maps: 1				
+ Add × Del	ete				
Port ID	 ✓ F 	RLAN Profile	~	RLAN Policy Profile	~
3	R	RLAN-TEST		RLAN-Policy	
	10 🔻 items p	er page			1 - 1 of 1 items
Cancel					Apply to Device

6. Abilitare la porta LAN e applicare il codice di matricola all'access point. Selezionare **Configurazione > Wireless > Access Point** e fare clic sull'**access point**.

Location* default location Predownloaded Status N/A Base Radio MAC 0042.5ab7.8f60 Predownloaded Version N/A Ethernet MAC 0042.5ab6.4ab0 Next Retry Time N/A Admin Status ENABLED Boot Version 1.1.2.4 AP Mode Local OS Version 17.2.1.11 Operation Status Registered Mini IOS Version 0.0.0.0 Fabric Status Disabled IP Config Image: Status 0.0.0.0 LED State Image: Status 0ISABLED CAPWAP Preferred Mode Not -status LED State Image: Status 0.10.0 Image: Status 10.106.39.198 LED State S OHCP IPv4 Address 10.106.39.198 Tags Image: Status 10.106.39.198 Image: Status A Changing Tags will cause the Pt to momentarily lose association with the Controller. Image: Status 0 days 13 hrs 33 mins 40 secs Policy RLAN-TAC Controller Association Latency 20 secs RE Idefault-rite.ag Image: Status 20 secs	dit AP			
Base Radio MAC 0042.5ab7.8f60 Predownloaded Version N/A Ethernet MAC 0042.5ab6.4ab0 Next Retry Time N/A Admin Status ENABLED 1 OS Version 1.1.2.4 AP Mode Local OS Version 17.2.1.11 AP Mode Local OS Version 0.0.0 Disabled IP Config 0.0.0 ELED Status Disabled IP Config Not Configured LED Brightness 8 LED Brightness 8 CAPWAP Preferred Mode Not Configured DHCP IPv4 Address 10.106.39.198 Static IP (IPv4/IPv6) Time Statistics Policy RLAN-TAGI V DISABLED 0 days 13 hrs State default-site-tag ↓ RF default-rf-tag ↓	Location*	default location	Predownloaded Status	N/A
Ethernet MAC 0042.5ab6.4ab0 Next Retry Time N/A Admin Status ENABLED Boot Version 1.1.2.4 AP Mode Local IOS Version 17.2.1.11 Operation Status Registered Mini IOS Version 0.0.0 Fabric Status Disabled IP Config LED State DISABLED CAPWAP Preferred Mode Not Configured LED Brightness 8< •	Base Radio MAC	0042.5ab7.8f60	Predownloaded Version	N/A
Admin Status ENABLED Boot Version 1.1.2.4 AP Mode Local IOS Version 17.2.1.11 Operation Status Registered Min IOS Version 0.0.0 Fabric Status Disabled IP Config Image: Config Conf	Ethernet MAC	0042.5ab6.4ab0	Next Retry Time	N/A
AP Mode Local IOS Version 17.2.1.11 Operation Status Registered Mini IOS Version 0.0.0 Fabric Status Disabled IP Config LED State DISABLED CAPWAP Preferred Mode Not Configured LED Brightness 8 DHCP IPv4 Address 10.106.39.198 Tags Static IP (IPv4/IPv6) Time Statistics A Changing Tags will cause the AP to momentarily lose association with the Controller. Up Time 0 days 13 hrs 33 mins 40 secs Policy RLAN-TAG Controller Association Latency 20 secs RF default-rf-tag	Admin Status		Boot Version	1.1.2.4
Operation Status Registered Fabric Status Disabled LED State DISABLED & DISABLED CAPWAP Preferred Mode LED Brightness 8 B DHCP IPv4 Address 10.106.39.198 Tags Static IP (IPv4/IPv6) Changing Tags will cause the AP to momentarily lose association with reformable. Policy RLAN-TAGI Wini IOS Version 0.0.0 Image: Controller Association Later to g RF default-rf-tag	AP Mode	Local	IOS Version	17.2.1.11
Fabric Status Disabled IP Config LED State DISABLED CAPWAP Preferred Mode Not Configured LED Brightness 8 DHCP IPv4 Address 10.106.39.198 Tags Static IP (IPv4/IPv6) Tags will cause the AP to momentarily lose association with the Controller. Up Time Policy RLAN-TAG Up Time State default-site-tag RF default-rf-tag	Operation Status	Registered	Mini IOS Version	0.0.0.0
LED State LEV Brightness Level Tags CAPWAP Preferred Mode Not Configured DHCP IPv4 Address 10.106.39.198 Static IP (IPv4/IPv6) Time Statistics Up Time Statistics Up Time 0 days 13 hrs 33 mins 40 secs State default-rf-tag RF default-rf-tag	Fabric Status	Disabled	IP Config	
LED Brightness 8 Level DHCP IPv4 Address Tags Static IP (IPv4/IPv6) Changing Tags will cause the AP to momentarily lose association with the Controller. Time Statistics Up Time 0 days 13 hrs 33 mins 40 secs Policy RLAN-TAGI RF default-rf-tag	LED State	DISABLED	CAPWAP Preferred Mode Not Co	onfigured
Tags A Changing Tags will cause the AP to momentarily lose association with the Controller. Up Time Up Time O days 13 hrs 33 mins 40 secs Site default-site-tag RF	LED Brightness Level	8 🔻	DHCP IPv4 Address 10.108	5.39.198
▲ Changing Tags will cause the AP to momentarily lose association with the Controller. Policy RLAN-TAG Controller Association Latency 20 secs RF default-rf-tag	Tags		Static IP (IPv4/IPv6)	
▲ Changing Tags will cause the AP to momentarily lose association with the Controller. Up Time 0 days 13 hrs 33 mins 40 secs Policy RLAN-TAG Controller Association Latency 20 secs Site default-site-tag RF default-rf-tag			Time Statistics	
Policy RLAN-TAG Controller Association Latency 20 secs Site default-site-tag RF default-rf-tag	Changing Tags will cause association with	the AP to momentarily lose the Controller.	Up Time	0 days 13 hrs 33 mins 40 secs
Site default-site-tag RF default-rf-tag	Policy	RLAN-TAG V	Controller Association Latency	20 secs
RF default-rf-tag 🔻	Site	default-site-tag 🗸		
	RF	default-rf-tag 🔻		

Applicare l'impostazione e l'access point si unisce nuovamente al WLC. Fare clic su nell'**access point**, quindi selezionare **Interfacce** e abilitare la porta LAN.

Baneral Interfaces High Availability Inventory ICap Advanced Radio Interfaces Status Operation Spectrum Spectrum Operation Status Regulatory 0 802.11n - 2.4 GHz All Enabled Disabled Image: Advanced Image: Advanced 0 802.11n - 2.4 GHz All Enabled Disabled Image: Advanced Image: Advanced 1 802.11ac All Enabled Disabled Image: Advanced Image: Advanced Med 1 Image: Advanced Image: Advanced Disabled Image: Advanced Image: Advanced Power Over Ethernet Settings Image: Advanced Image: Advanced Image: Advanced Image: Advanced Image: Advanced Power Type/Mode Power Mode Power Mode Image: Advanced Image: Advanced Image: Advanced Image: Advanced PoE Power Injector MAC Address Disabled Image: Advanced Image: Advanced Image: Advanced Image: Advanced Image: Advanced Max Image: Advanced Image: Advanced Image: Advanced Image: Advanced Image: Advanced	lit AP										
Radio Interfaces Slot Interface Band Admin Status Operation Status Spectrum Admin Status Spectrum Operation Status Regulatory Operation Status Regulatory Domain Regulatory Demain Regulatory Operation Status Regulatory Domain Regulatory Domain Regulatory Demain Regulatory Demain Regulatory Demain Regulatory Demain Regulatory Disabled Poperation Status Spectrum Admin Status Spectrum Disabled Spectrum Disabled <th>eneral</th> <th>Interfaces</th> <th>High Availabi</th> <th>lity Inv</th> <th>rentor</th> <th>у ІСар</th> <th>Adv</th> <th>anced</th> <th></th> <th></th> <th></th>	eneral	Interfaces	High Availabi	lity Inv	rentor	у ІСар	Adv	anced			
Slot Interface Band Admin Operation Spectrum Spectrum Spectrum Regulatory 0 802.11n - 2.4 GHz All Enabled Disabled O -A 1 802.11ac All Enabled Disabled O -D H 1 H 10 items per page 1 - 2 of 2 Power Type/Mode PoE Pre-Standard Switch PoE Power Injector MAC Address Address Addmin VLAN ID VLAN ID PoE Power Injector MAC Address	Radio Int	erfaces									
D 802.11n - 2.4 GHz All Enabled Disabled Image: Second sec	Slot √ No	Interface	√ Band √	Admin Status	×	Operation Status	Spect Admin	rum 🕔	Spe Ope	ctrum ration Status	Regulatory Domain
1 802.11ac All Enabled Disabled Image: marked stress of the stre	D	802.11n - 2.4 GHz	: All	Enabled		ο	Disable	ed		0	-A
H 1 H 10 Items per page 1 - 2 of 2 Power Over Ethernet Settings Power Type/Mode Power Injector/Normal Mode Pot ID < Status	I	802.11ac	All	Enabled		O	Disable	ed		0	-D
LAN Port Settings Power Type/Mode Power Injector/Normal Mode Port ID 、 Status VLAN ID 、 PoE Power Level RLAN PoE Pre-Standard Switch Disabled LAN2 0 NA Ø PoE Power Injector MAC Address Disabled LAN3 39 NA Ø	H 4	1 🕨 🗏	10 🔻 items	per page							1 - 2 of 2
Power Type/Mode Power Injector/Normal Mode Port ID < Status VLAN ID PoE Power Level RLAN PoE Pre-Standard Switch Disabled LAN2 0 NA Ø PoE Power Injector MAC Address Disabled LAN3 Image: Status VLAN ID PoE Power Level RLAN Image: Note that the state sta	Power O	ver Ethernet Set	tings			LAN Por	t Setting	S			
Node LAN1 0 NA Ø PoE Pre-Standard Switch Disabled LAN2 0 NA NA Ø PoE Power Injector MAC Address Disabled LAN3 Ø 39 NA NA Ø	Power Typ	oe/Mode	Power	r/Normal		Port ID 🖂	Status	VLAN ID 🖂	PoE	Power Level	RLAN
PoE Pre-Standard Switch Disabled LAN2 0 NA NA Ø PoE Power Injector MAC Address Disabled Image: Comparison of the standard st			Mode	, worman		LAN1		0		NA 🔻	Ø
PoE Power Injector MAC Address Disabled	PoE Pre-S	Standard	Disabl	ed		LAN2		0	NA	NA 🔻	\oslash
PoE Power Injector Disabled MAC Address Id I Id I Image: Ima	0.50					LAN3	 Image: A start of the start of	39	NA	NA v	Ø
	MAC Addr	ress	Disabi	ea	I	ia a	1 ⊧	▶ 10	• iter	ms per page	

Applicare le impostazioni e verificare lo stato.

dit AP												
eneral	Interfaces	High A	vailabili	ty Inv	ento	ry ICap	Adv	anced				
Radio In	terfaces											
Slot √ No	Interface		nd 🖂	Admin Status	~	Operation Status	Spect Admin	rum v	Spe Ope	ectrum eration Status	F	≀egulatory)omain
D	802.11n - 2.4 GH	iz All		Enabled		0	Disabl	ed		0	-	A
1	802.11ac	All		Enabled		0	Disabl	ed		0	-	D
M 4	1 ▶ ⊨	10 🔻	items p	er page								1 - 2 of 3
Power O	ver Ethernet Se	ttings				LAN Por	t Setting	js				
Power Ty	pe/Mode		Power	/Normal		Port ID 🗸	Status	VLAN ID 🗸	PoE	Power Lev	rel	RLAN
			Mode			LAN1		0		NA ,	•	\oslash
PoE Pre-S	Standard		Disable	d		LAN2		0	NA	NA	•	\oslash
owneed						LAN3		39	NA	NA ,	,	۲
PoE Powe MAC Add	er Injector ress		Disable	d		H4 - 4	1 ▶	▶ 10	• ite	ms per page	- 3 (of 3 items

7. Collegare un PC alla porta LAN3 dell'access point. Il PC verrà autenticato tramite 802.1x e riceverà un indirizzo IP dalla VLAN configurata.

Passare a **Monitoraggio > Wireless > Client** per controllare lo stato del client.

Monitoring * > Wireless * > Clients

Clients	Sleeping Clients		Excluded Clients																	
×	× Delete																			
Total (Total Client(s) in the Network: 2																			
Numb	er of Cilent(s) selected:	0																		
	Client MAC Address	×	IPv4 Address ~	IPv6 Address	AP Name	\sim	SSID v	WL	AN ID	×.	State	×	Protocol	×	User Name	×	Device Type	×.	Role	~
	503e.aab7.0ff4	×	10.105.39.227	2001::c	AP1815		corporate-ssid	3			Run		11n(2.4)	_			N/A		Local	
	b496.9126.dd6c	×	10.106.39.191	fe80::d8ca:e582:2703:f24e	AP1810	Γ	RLAN-TEST	1			Run		Ethernet	L	vinodh		N/A		Local	
н	< 1 → 10	•	items per page														1 - 2 of	2 cli	onts	0

Client

360 View	Genera	QOS Statistic	cs ATF Statistics	Mobility History	Call Statistics	
Client Prope	rties	AP Properties	Security Information	Client Statistics	QOS Propertie	s EoGRE
Session Ma	nager					
IIF ID			0x9000000C			
Authorized			TRUE			
Common S	ession ID		000000000000000000000000000000000000000	00E79E8C7A9A		
Acct Sessi	on ID		0x00000000			
Auth Metho	od Status	List				
Method			Dot1x			
SM State				ED		
SM Bood S	toto.		IDLE			
Sivi berid S	late		IDLE			
vk-9800-1#s	how wir	eless client s	ummary			
Number of C	lients:	2	1			
MAC Address	AP	Name		Туре	ID State	
Protocol Me	thod	Role				
		815		WT.ZN	3 Run	
11n(2.4) No	ne	Local		NALW .	5 I(all	
b496.9126.d	d6c AP1	.810		RLAN	1 Run	
Ethernet Do	t1x	Local				

Number of Excluded Clients: 0

Risoluzione dei problemi

Problemi comuni:

- Funziona solo il SSID locale, il SSID configurato sul WLC non viene trasmesso: verificare che l'AP si sia unito correttamente al controller.
- Impossibile accedere alla GUI OEAP: Verificare se l'access point ha un indirizzo IP e verificare la raggiungibilità (firewall, ACL, ecc. nella rete)
- I client wireless o cablati con commutazione centrale non sono in grado di autenticarsi o ottenere l'indirizzo IP: Prendere tracce RA, sempre su tracce, ecc.

Esempio di tracce Always on per il client Wired 802.1x:

[client-orch-sm] [18950]: (note): MAC: <client-mac> Association received. BSSID 00b0.e187.cfc0, old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB =
False, 11r = False, 11w = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.el87.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000 Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Cliet-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN