ISSN/0393-3016

M. DE ROSA

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Implementazione Nuovi Progetti
ed Applicazioni in Rete
Centro Ricerche Portici, Napoli

C. FERRELLI, S. PECORARO

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Implementazione Nuovi Progetti
ed Applicazioni in Rete
Centro Ricerche Casaccia, Roma

GUIDA ALLA INTEGRAZIONE DEI NUOVI CONTROLLER ED ACCESS-POINT HUAWEI NELLA INFRASTRUTTURA WI-FI ENEA

RT/2017/42/ENEA

AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE,
L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

M. DE ROSA

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Implementazione Nuovi Progetti
ed Applicazioni in Rete
Centro Ricerche Portici, Napoli

C. FERRELLI, S. PECORARO

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Implementazione Nuovi Progetti
ed Applicazioni in Rete
Centro Ricerche Casaccia, Roma

GUIDA ALLA INTEGRAZIONE DEI NUOVI CONTROLLER ED ACCESS-POINT HUAWEI NELLA INFRASTRUTTURA WI-FI ENEA

RT/2017/42/ENEA

AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE,
L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

GUIDA ALLA INTEGRAZIONE DEI NUOVI CONTROLLER ED ACCESS-POINT HUAWEI NELLA INFRASTRUTTURA WI-FI ENEA

M. De Rosa, C. Ferrelli, S. Pecoraro

Riassunto

Dopo una breve esposizione della architettura Wi-Fi in esercizio in Enea sino a fine 2016, il documento descrive i passi necessari per installare, configurare e rilasciare all'utenza il Controller wi-fi Huawei AC6005 e gli Access Point AP5130DN, nel rispetto delle policy d'Agenzia in essere ed in modalità congruente con l'installato.

Parole chiave: Wi-Fi, Wireless, Controller, Access-Point, Rete Locale, Dispositivi mobili, BYOD (Bring YOur Device), LAN, Huawei, Alcatel.

Abstract

After a brief exposure of Wi-Fi architecture working in Enea until the end of 2016, the document describes the steps needed to install, configure, and release the Huawei wi-fi Controller AC6005 and AP5130DN Access Points, in compliance with Agency policies and in accordance with the installed one.

Key words: *Wi-Fi, Wireless, Controller, Access-Point, Local Network, Mobile Devices, BYOD (Bring YOur Device), LAN, Huawei, Alcatel.*

INDICE

Premessa

Questa vuole essere una sintetica guida per noi scriventi in prima istanza, per i colleghi di Laboratorio, attuali e futuri, e per tutti coloro che ne avranno necessità.
Il pregio della sintesi ovviamente andrà in conflitto con la profondità dei dettagli: il lettore dovrà necessariamente aver un minimo di conoscenze di informatica e di esperienza sul campo, non ultimo in quello Enea.

Introduzione

Per un numero in costante aumento di persone, essere connessi è ormai diventata una necessità. Lo smartphone, il tablet o in generale i dispositivi mobili permettono infatti di essere informati, di socializzare, di lavorare, di pianificare, etc.
Questo "trend" è ormai inevitabile ed inarrestabile, visto anche che sempre più spesso alcune problematiche correlate allo svolgimento quotidiano del lavoro all'interno degli uffici della Pubblica Amministrazione vengono risolte grazie alla sempre maggiore disponibilità di strumenti informatici, sempre più spesso Wireless.

Le nuove esigenze che la diffusione di sistemi Wi-Fi ha introdotto possono essere sintetizzate in:

- ✓ la comunicazione tra dispositivi wireless deve essere sicura almeno quanto quella wired;
- ✓ la comunicazione wireless deve poter essere utilizzata con le stesse policy di sicurezza in uso alla wired;
- ✓ l'aspettativa dell'utenza è quella di poter usufruire comodamente e con semplicità del Wi-Fi all'interno degli uffici della Pubblica Amministrazione.

Sin dall'inizio del fenomeno, la Divisione ICT ha studiato e seguito l'evolversi della tecnologia, individuando gli apparati Wireless che meglio rispondessero ai principi di sicurezza e facilità di utilizzo. Per situazioni già sviluppatesi spontaneamente, ha guidato la configurazione dei dispositivi in modo che fosse congruente con l'installato.

Negli ultimi tempi inoltre ICT ha posto particolare attenzione alla integrazione dei vari sistemi che negli anni si sono affiancati nell'erogazione del servizio; alla pluralità di tipologie di utenti (Dipendenti, Ospiti, Ditte esterne, Borsisti, etc); alla adesione alla Federazione Eduroam (che permette l'accesso alla rete Wi-fi con le credenziali del proprio Ente di appartenenza in qualunque Istituto Federato ci si trovi).

Con l'ultima acquisizione di apparati wi-fi, Huawei questa volta, (le leggi di mercato spesso si impongono a qualsiasi altra strategia), la sfida era continuare l'integrazione con il parco di Access Point già istallato facendo in modo che il tutto risultasse trasparente all'utenza ENEA.

1 L'infrastruttura in esercizio

Nei principali Centri di Ricerca Enea l'infrastruttura wifi viene offerta attraverso 3 diverse tecnologie:

- Controller centralizzato Alcatel
- Controller centralizzato WatchGuard
- Nuvole Instant Access Point (Alcatel)

In tutti i Centri vengono presentati gli stessi SSID e le stesse modalità di autenticazione.

Nello specifico:

- SSID: UTENTI-ENEA(ASIE): autenticazione mediante ASIE
- SSID: Eduroam: autenticazione mediante RADIUS server federato con Eduroam
- SSID: VISITATORI-ENEA: l'autenticazione varia in funzione del Controller a cui sono attestati gli AP (questo SSID e' in fase di dismissione):
    - gli AP attestati al Controller centralizzato ALCATEL forniscono accesso tramite la creazione di utenze temporanee attivabili dalle singole guardianie/servizi attraverso un tool disponibile sul Controller stesso
    - gli AP attestati al Controller WatchGuard forniscono accesso tramite la creazione di utenze temporanee attraverso un tool disponibile sul Controller stesso
    - gli AP presenti nelle nuvole Istant Access Point forniscono accesso tramite la creazione di utenze temporanee attraverso un tool disponibile sugli iAP stessi

- SSID: VISITATORI-ENEA(ASIE): autenticazione mediante ASIE

Per quanto riguarda il sezionamento e controllo del traffico al variare degli SSID si ha:

- per UTENTI-ENEA(ASIE), il traffico è tutto interno alla LAN del Centro in cui è ubicato l'AP
- per SSID VISITATORI-ENEA(ASIE), VISITATORI-ENEA ed Eduroam (per i soli AP attestati al Controller ALCATEL) , il traffico è interno al tunnel verso Casaccia e questo consente il controllo del traffico differenziando i dipendenti dagli ospiti. Negli altri casi il traffico è gestito dal centro in cui risiede l'AP.

2 Prime configurazioni “sul posto”

L’apparato si presenta così:

2.1 Impostazione indirizzo tcp/ip

È consigliabile realizzarla via cavo seriale ed un PC sul posto con installato un emulatore-terminale, “patchando” le rispettive porte seriali;
sia il Controller che gli Access Point Huawei hanno di default credenziali:

Utente	admin
Pass	admin@huawei.com

il Controller inoltre ha di default

indirizzo tcp/ip 169.254.1.1

2.2 Utenze locali amministratore

Al 1^ collegamento al Controller sarà richiesto di impostare la password dell’utenza admin (utenza amministratore per l’accesso via seriale).
Esistono però altrettante utenze *admin* nell’ambito dei procolli ssh e http; per entrambe va configurata la password e il protocollo autorizzato attraverso comandi del tipo:

[AC6005]aaa
[AC6005-aaa]local-aaa-user
[AC6005-aaa]local-user derosa service-type ssh http
Warning: The user access modes include Telnet, FTP, or HTTP, so security risks exist.
Info: After you change the rights (including the password, access type, FTP directory, and level) of a local

user, the rights of users already online do not change. The change takes effect to users who go online after the change.

[AC6005-aaa]local-user admin password irreversible-cipher Enterasys1
Please enter old password:
Info: The password is changed successfully.

2.3 Layout, porte, vlan, tagging

Per erogare WiFi Huawei nel rispetto delle policy di sicurezza, si sceglie di posizionare il Controller come ulteriore "zampa" del FireWall. Segue a titolo di esempio il layout e le reti per Portici.

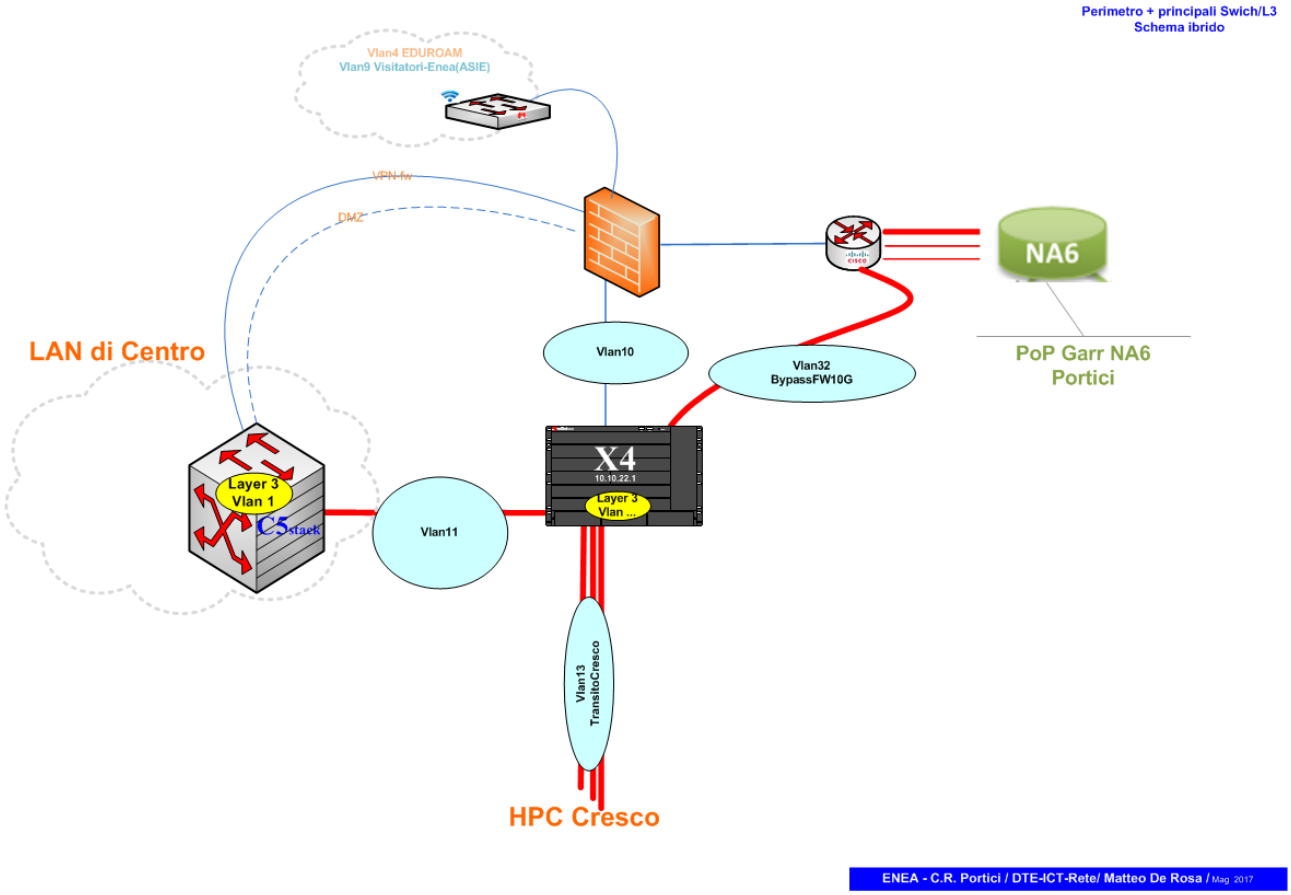


Figura 1

Avendo individuato per il collegamento Controller - FireWall la subnet con le assegnazioni che seguono:

90.147.171.48 subnet ID		non utilizzabile come ind host !!!
49	Controller WiFi Huawei	
		"
...		"
..		"
...		
62	FireWall - zampa verso controller WiFi	**GW def per questa subnet**
	broadcast di questa subnet	non utilizzabile come ind host !!!

Lato Controller:

scelta la porta GE0/0/7 e vlan1, individuate eventuali altre vlan da veicolare, si configurano:

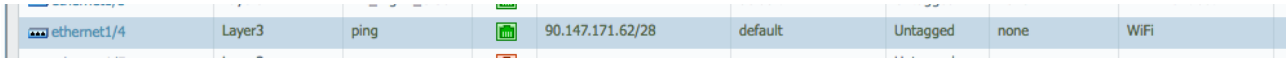
la vlan e l'indirizzo tcp/ip del Controller:

```
<AC6005>system-view
[AC6005]vlan 1
[AC6005-vlan1]name UTENTI
[AC6005-vlan1]quit
[AC6005]interface Vlanif 1
[AC6005-Vlanif1]ip address 90.147.171.49 255.255.255.240
[AC6005-Vlanif1] management-interface
[AC6005-Vlanif1] quit

[AC6005] ip route-static 0.0.0.0 0.0.0.0 90.147.171.62
[AC6005] dns server 192.107.81.23
```

Lato FireWall:

scelta la porta eth1/4, si configura:

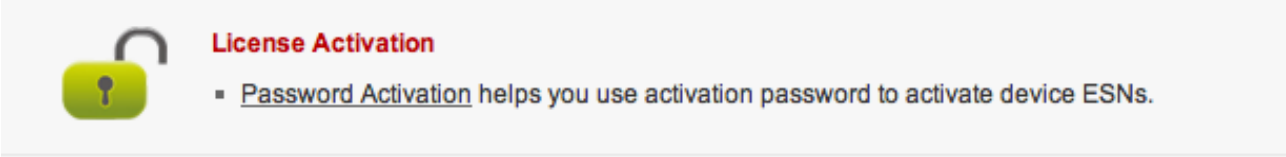


e la Zona WiFi:

3 Licensing

3.1 Attivazione della licenza in formato elettronico

E' necessario registrarsi al sito app.huawei.com/isdp ed eccedervi previa autenticazione; licenza cartacea (Proof of Entitlement) alla mano si eseguono gli step previsti in:

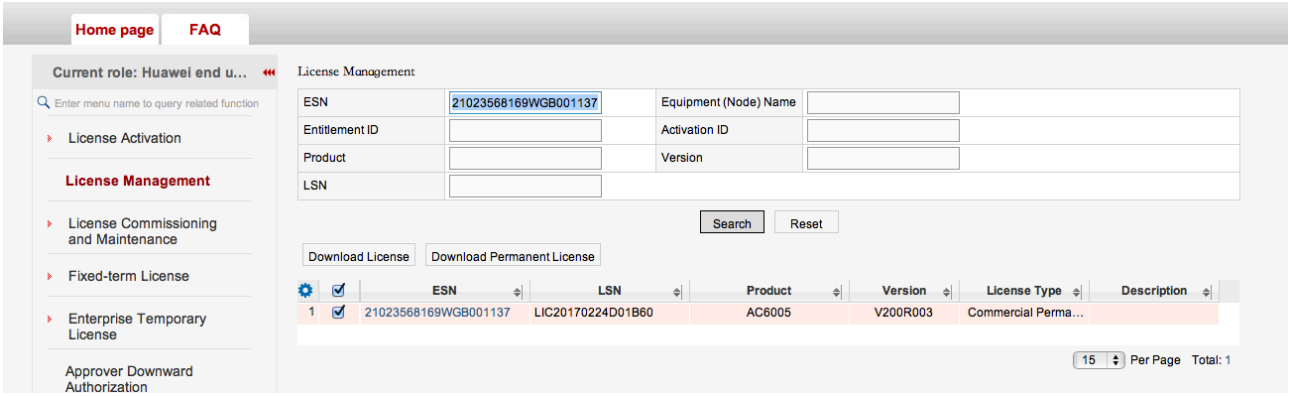


sino al download della licenza elettronica stessa.

Nota: ESN (Equipment SN(ESN)) può essere copiato dalla interfaccia web del Controller via i menu' Maintenace – Electronic Label

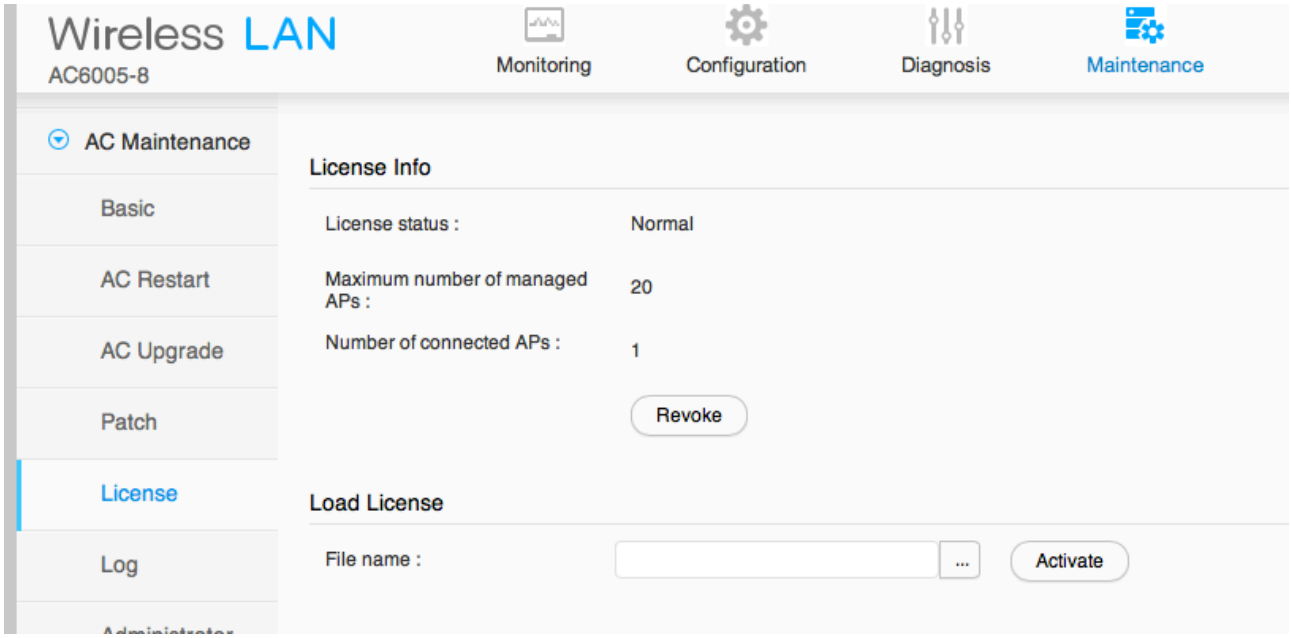
3.2 Attivazione e rilascio della licenza

Tramite il suddetto Sito, da menu License Management - valorizzo il campo ESN - search: il Sistema trova la specifica licenza – la seleziono e ne faccio il download in locale:



3.3 Applicazione della licenza

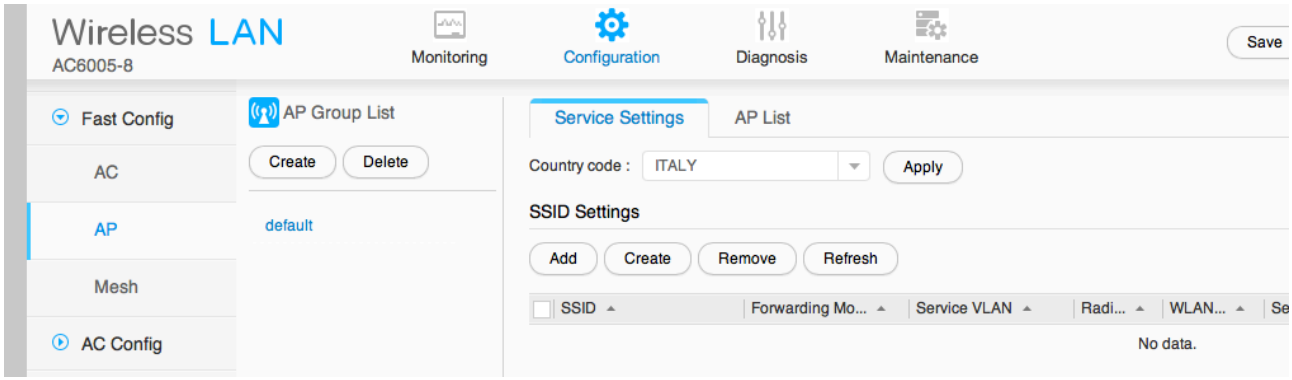
Dalla interfaccia web del Controller individuo il file appena scaricato – tap su "activate" – segue il download e ad operazione ultimate ritrovo:



ovvero: max num of managed Aps: 20 !

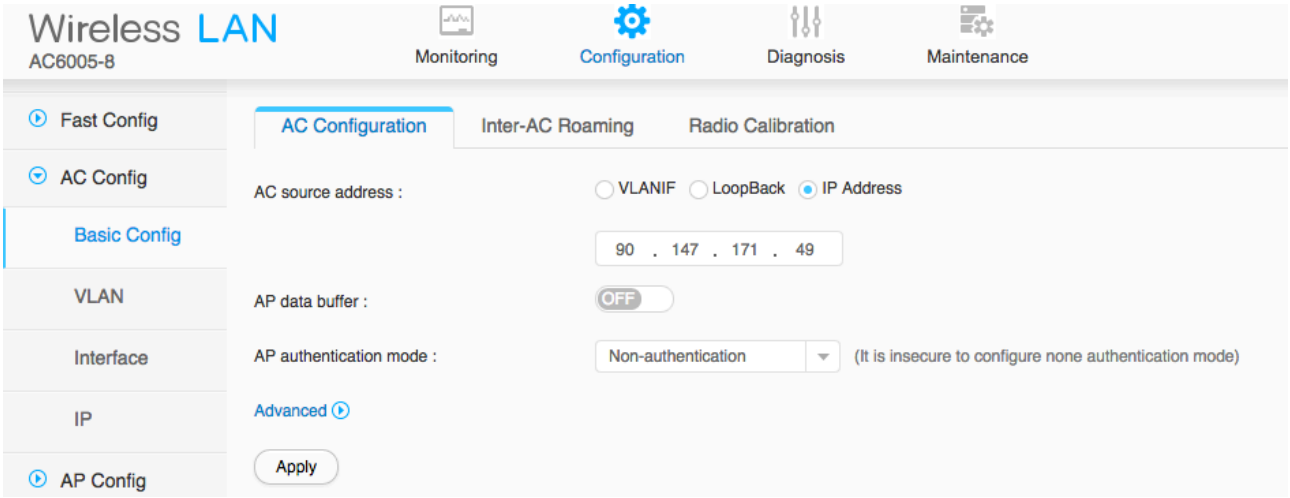
Attenzione: via Mac/OSx l'upload della licenza non va a buon fine !

4.1 Configurazione country-code



4.2 Specifica AC source address

Bisogna specificare la porta/interfaccia/indirizzo sul quale il Controller sarà in ascolto. Nell'esempio di Portici:



5 Inserimento di un nuovo Access Point

5.1 Configurazione iniziale all'AP

Una volta collegato un nuovo AP alla infrastruttura, per configurazione di default assumerà un indirizzo rilasciato dal DHCP-Server della LAN. Esplorando poi il dhcp-server, individuo l'indirizzo effettivamente assegnato (es 192.168.13.22) e si suggerisce di impostare in modo permanente:

ssh admin@192.168.13.22
admin@huawei.com
[Huawei_SalaRete]sys
[Huawei_SalaRete]ap-address mode static
Info: The configuration takes effect after the AP is restarted.
[[Huawei_SalaRete]ap-address static ip-address 192.168.12.2 255.255.255.0 192.168.12.254
Info: The configuration takes effect after the AP is restarted.

Ulteriore configurazione che si suggerisce realizzare in modo permanente è specificare l'indirizzo del Controller locale (più uno remoto, che entrerebbe in gioco ovemai quello locale andasse in fault) :

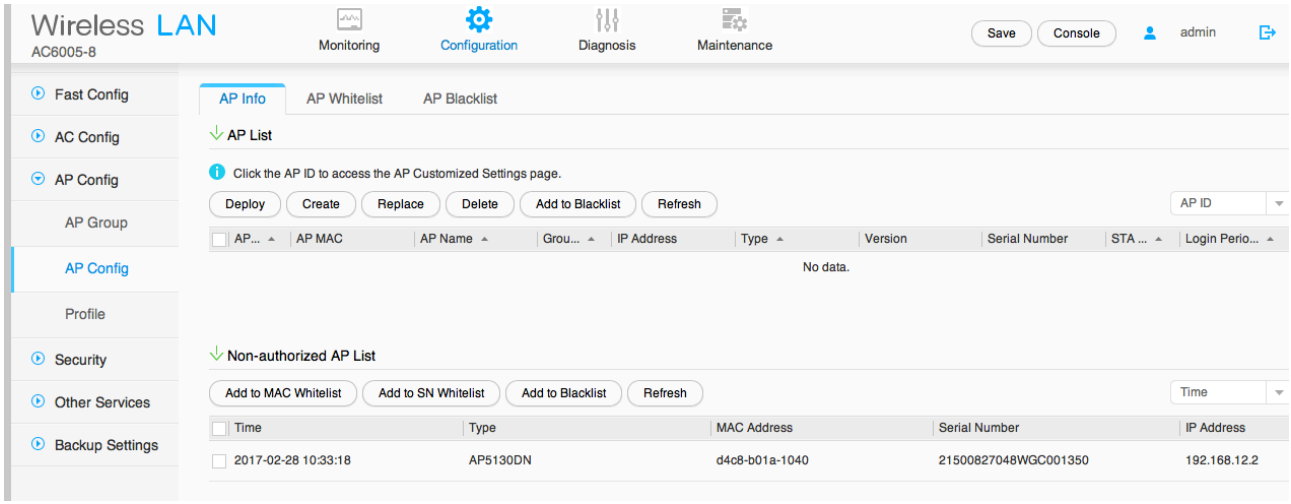
[Huawei_SalaRete]ap-address static ac-list 90.147.171.49

A questo punto si riavvia l'apparato:

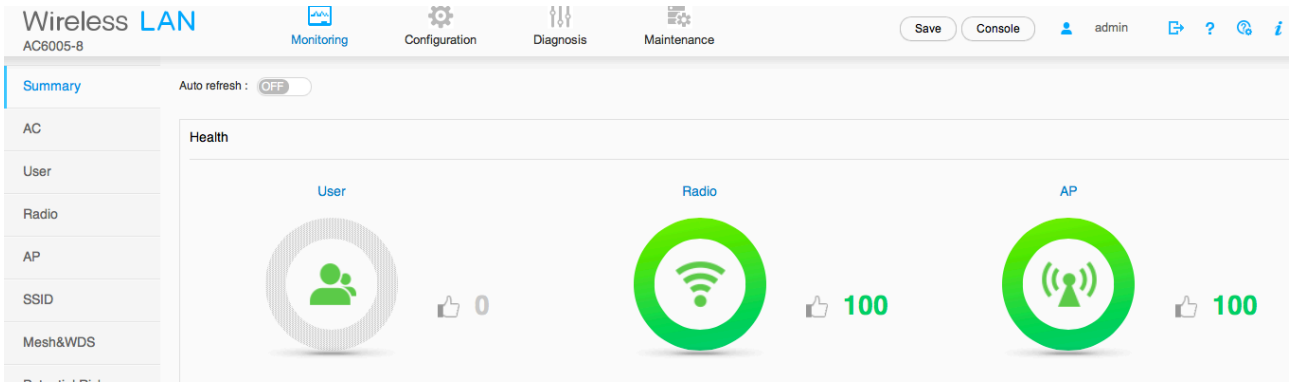
<Huawei_SalaRete>q
<Huawei_SalaRete>reboot

5.2 Rilevamento AP

Un AP configurato come nel paragrafo precedente sarà rilevato dal Controller nella finestra che segue, alla voce "Non-authorized AP List":



una volta selezionatolo: add Mac whitelist; l'AP, dopo diversi minuti, transiterà dallo stato "config" a "normal".
Da quel punto, apparirà OK nella finestra:



e l'apparato è da questo momento in poi "ricosciuto" dal Controller. Nulla è stato fatto ancora affinché

questo possa erogare alcunchè.

5.3 Configurazione degli SSID

Di seguito sono descritti i passi rilevanti per la configurazione degli SSID già in esercizio nella maggior parte dei Centri ma erogati da HardWare diverso: UTENTI-ENEA(ASIE), VISITATORI-ENEA(ASIE) ed EDUROAM.

5.3.1 SSID: UTENTI-ENEA(ASIE)

5.3.1.1 Configurazioni propedeutiche su apparati diversi

Radius-Server

AL fine di perfezionare l'autenticazione Radius occorre che il Controller Huawei sia definito client del Radius-Server.

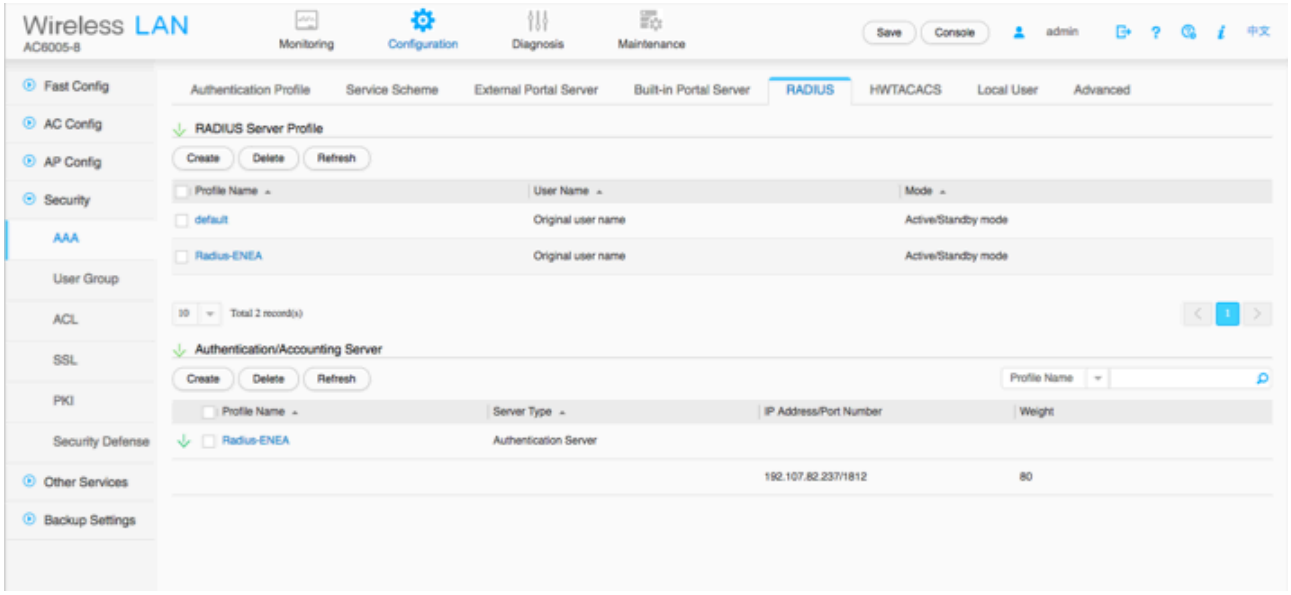
FireWall

Se, come nel caso di Portici, il Radius-Server è immerso nella Lan in cui insiste il Controller, non occorre fare altro, in altri casi potrebbe essere necessario agire sul FireWall per garantire il colloquio, sui protocolli specifici, tra controller e server-radius.

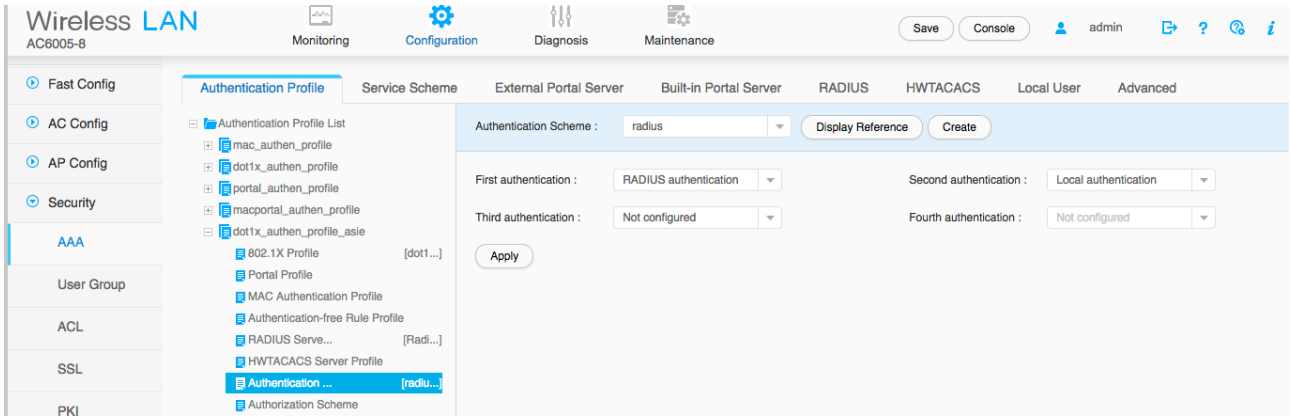
5.3.1.2 Configurazioni sul Controller Huawei

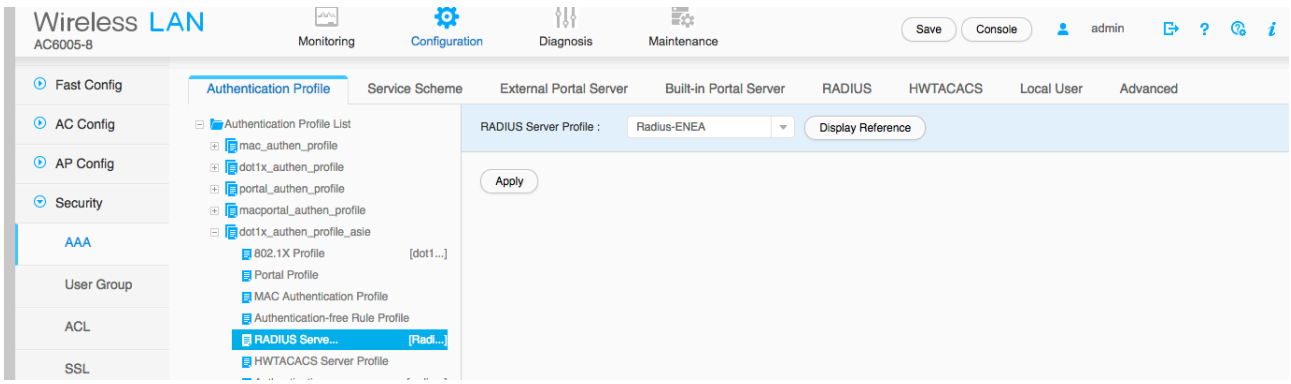
[1]In Configuration – Security – AAA – Radius si creano i RADIUS Server Profile ed Authentication/ Accountig Server come segue:

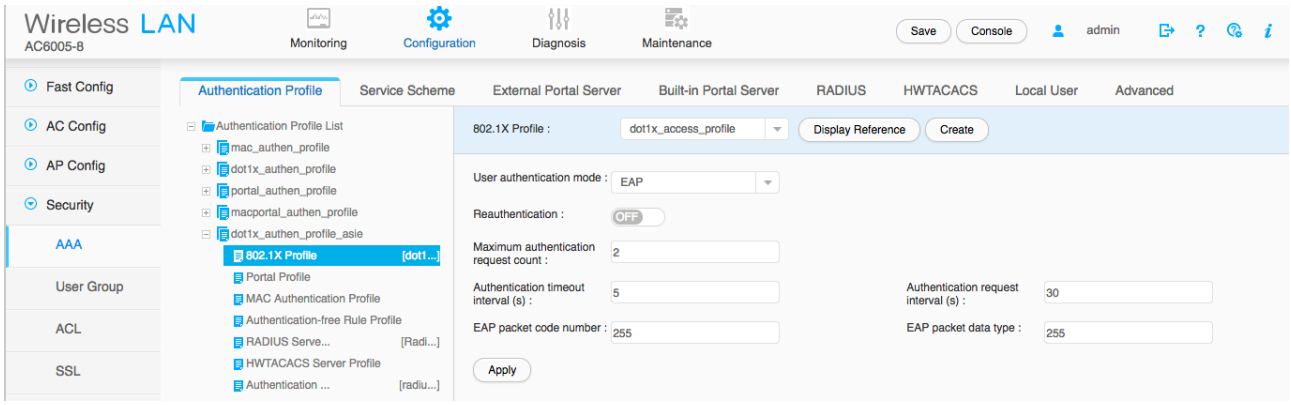
[1] *Nel mettere a punto un SSID via la GUI del Controller, come linea di principio relativamente all'ordine da seguire, bisogna creare entità a partire dal menù a sinistra più bassi e, all'interno di questi, dare priorità a quelli più a destra.*



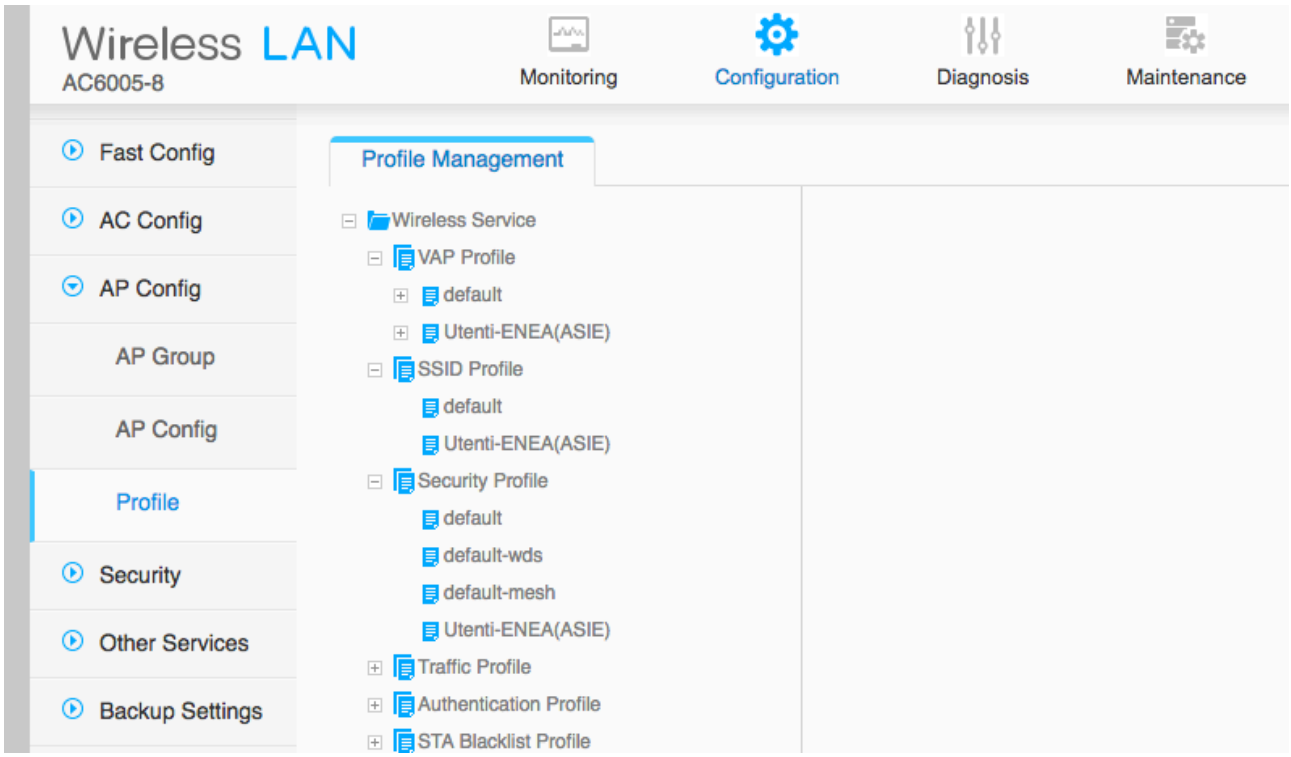
In Configuration – Security – AAA – Authentication Profile si crea dot1x_authen_profile_asie (ereditando i valori dal preesistente dot1x_authen_profile) e lo si configura come nelle figure:



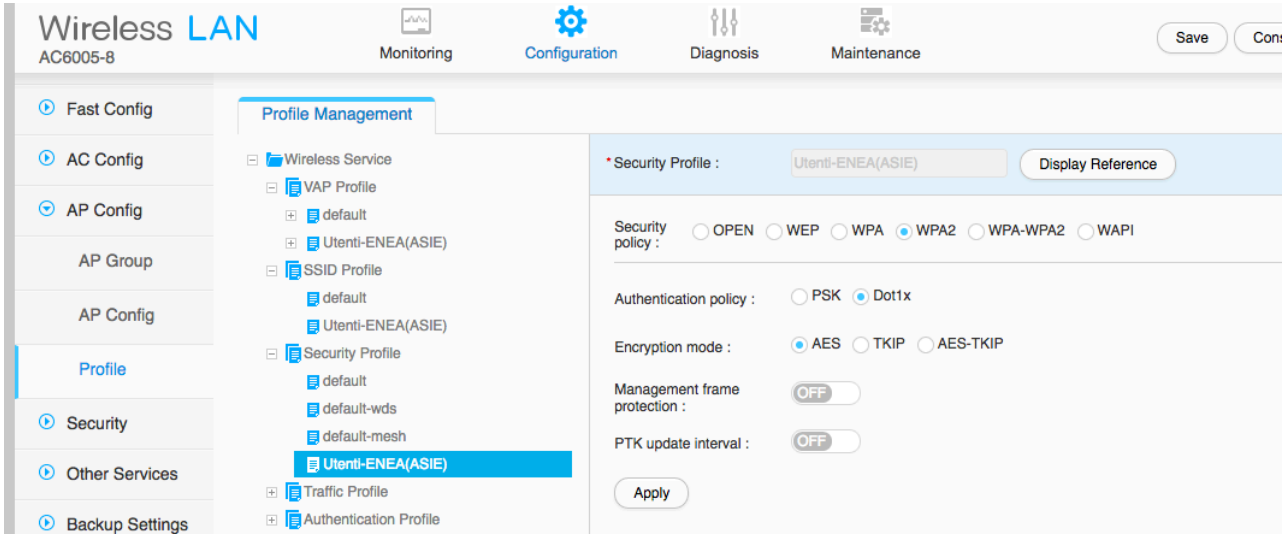


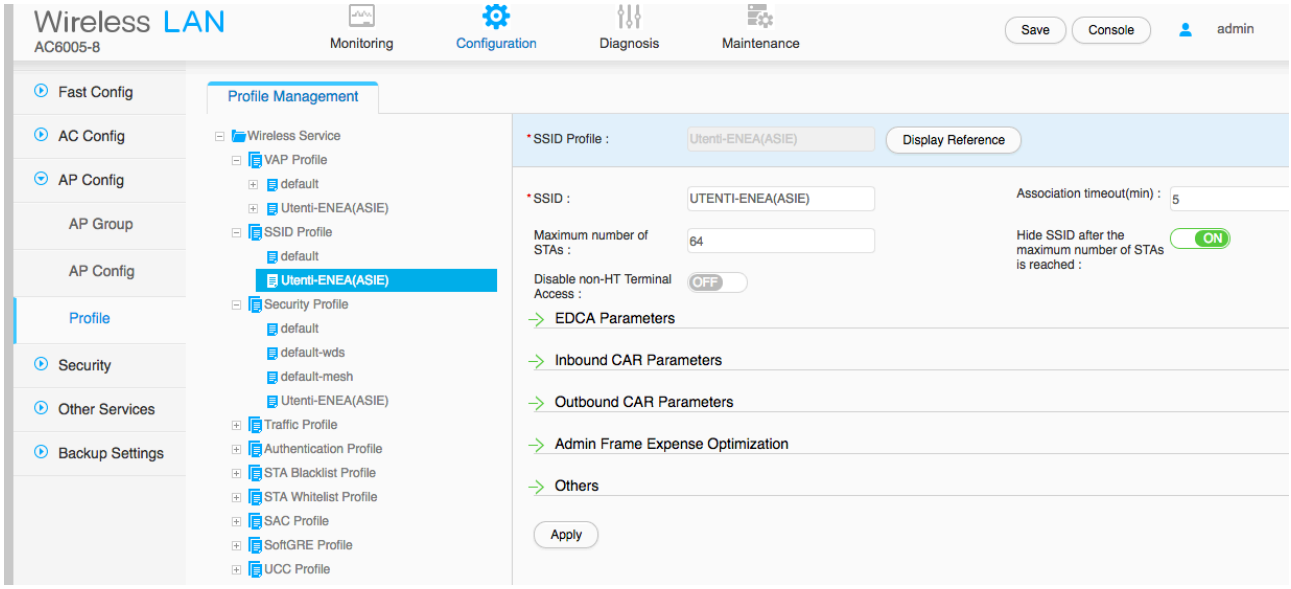


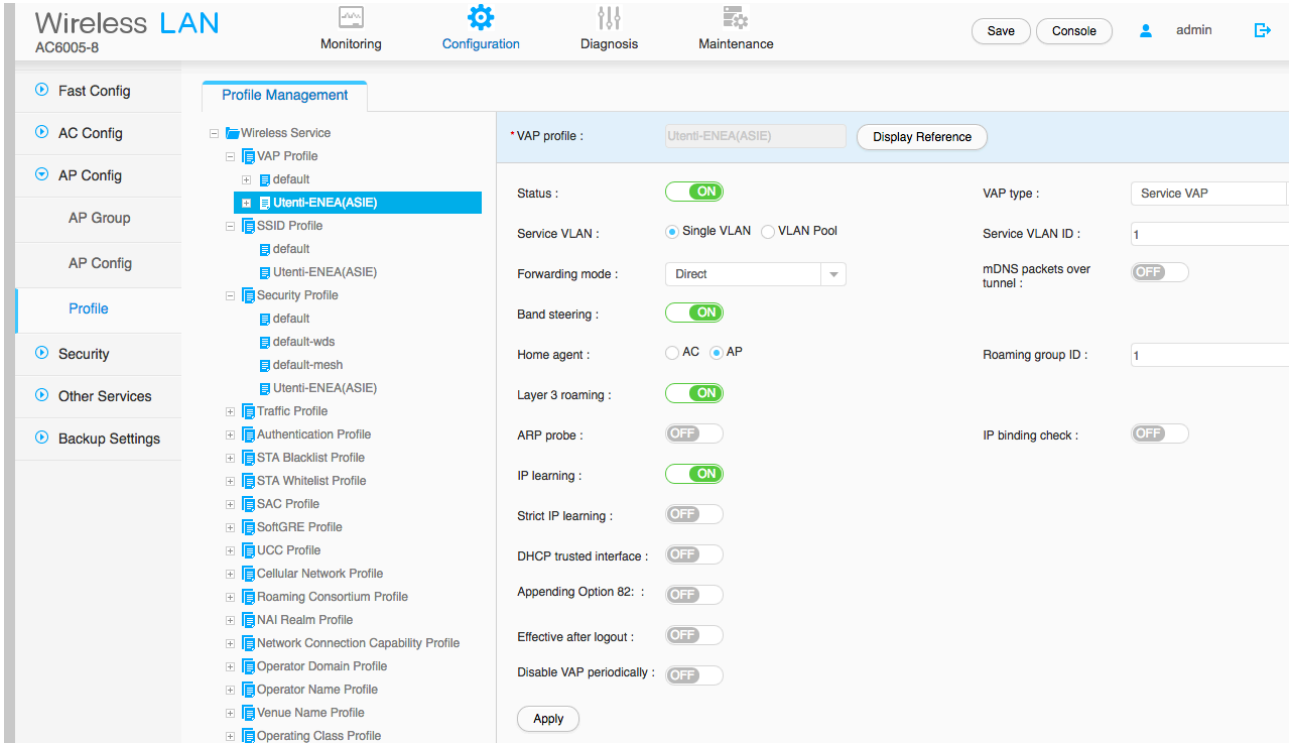
In Configuration – AP Config – Profile si creano VAP Profile, SSID Profile e Security Profile:



con le seguenti personalizzazioni:


Wireless LAN
AC6005-8
Monitoring
Configuration
Diagnosis
Maintenance
Save
Fast Config
AC Config
AP Config
AP Group
AP Config
Profile
Security
Other Services
Backup Settings
Profile Management
Wireless Service
VAP Profile
default
Utenti-ENEA(ASIE)
SSID Profile
default
Utenti-ENEA(ASIE)
Security Profile
default
default-wds
default-mesh
Utenti-ENEA(ASIE)
Traffic Profile
Authentication Profile
*Security Profile :
Utenti-ENEA(ASIE)
Display Reference
Security policy :
OPEN
WEP
WPA
WPA2
WPA-WPA2
WAPI
Authentication policy :
PSK
Dot1x
Encryption mode :
AES
TKIP
AES-TKIP
Management frame protection :
OFF
PTK update interval :
OFF
Apply


Wireless LAN
AC6005-8
Monitoring
Configuration
Diagnosis
Maintenance
Save
Console
admin
Fast Config
AC Config
AP Config
AP Group
AP Config
Profile
Security
Other Services
Backup Settings
Profile Management
Wireless Service
VAP Profile
default
Utenti-ENEA(ASIE)
SSID Profile
default
Utenti-ENEA(ASIE)
Security Profile
default
default-wds
default-mesh
Utenti-ENEA(ASIE)
Traffic Profile
Authentication Profile
STA Blacklist Profile
STA Whitelist Profile
SAC Profile
SoftGRE Profile
UCC Profile
*SSID Profile :
Utenti-ENEA(ASIE)
Display Reference
*SSID :
UTENTI-ENEA(ASIE)
Association timeout(min) :
5
Maximum number of STAs :
64
Hide SSID after the maximum number of STAs is reached :
ON
Disable non-HT Terminal Access :
OFF
EDCA Parameters
Inbound CAR Parameters
Outbound CAR Parameters
Admin Frame Expense Optimization
Others
Apply



dove i campi “Forward mode: Direct” ed “Home Agent: AP” implicano che il traffico tra wifi-client à AP à mondo, dopo gli step iniziali, NON passi più il Controller (modalità bridge).

5.3.2 SSID: VISITATORI-ENEA(ASIE)

5.3.2.1 Configurazioni propedeutiche su apparati diversi

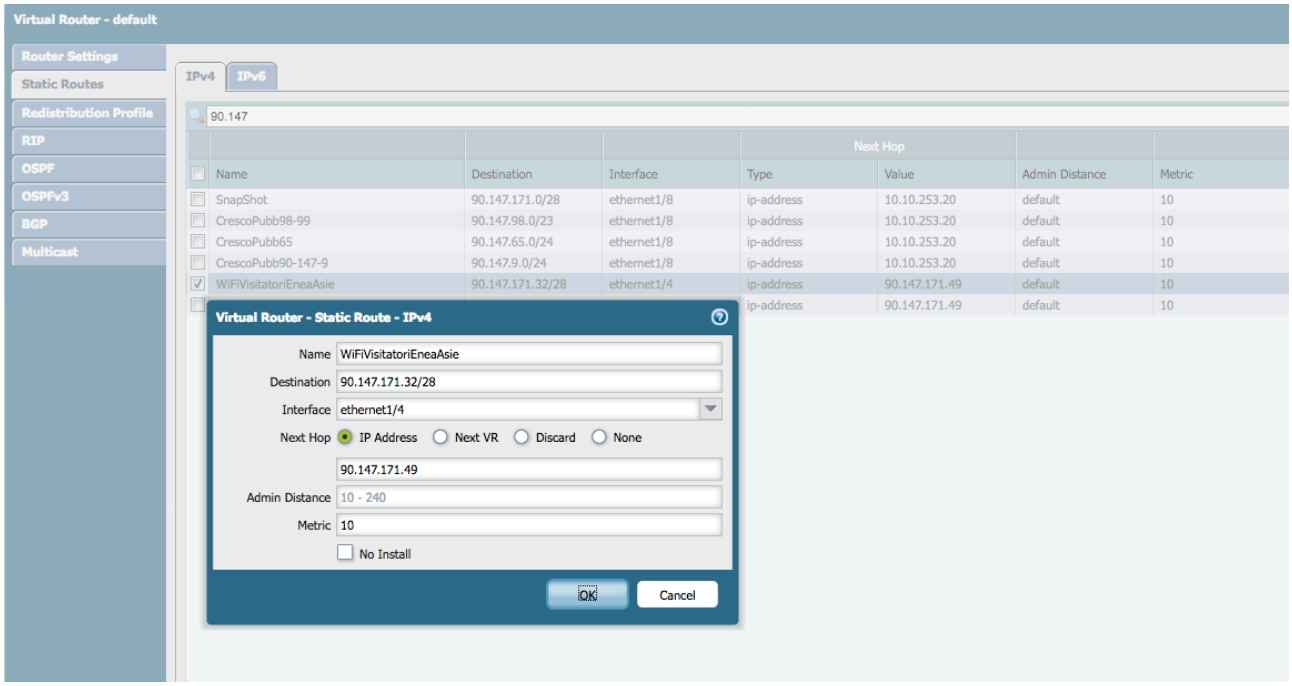
Radius-Server

Al fine di perfezionare l’autenticazione Radius occorre che il Controller Huawei sia definito client del Radius-Server all’uopo dedicato (in questo momento è configurato in Casaccia; a breve lo sarà anche a Portici per HA)

FireWall

a) Ove necessario, bisogna realizzare le regole che permettano il passaggio di transazioni radius tra questi ed il Controller.

b) Ovemai non configurata, bisogna solo aggiungere la rotta per il traffico di ritorno come descritto in fig. che segue:



Router perimetrale

a) Ovemai non configurata, bisogna aggiungere la rotta per instradare il traffico di ritorno:

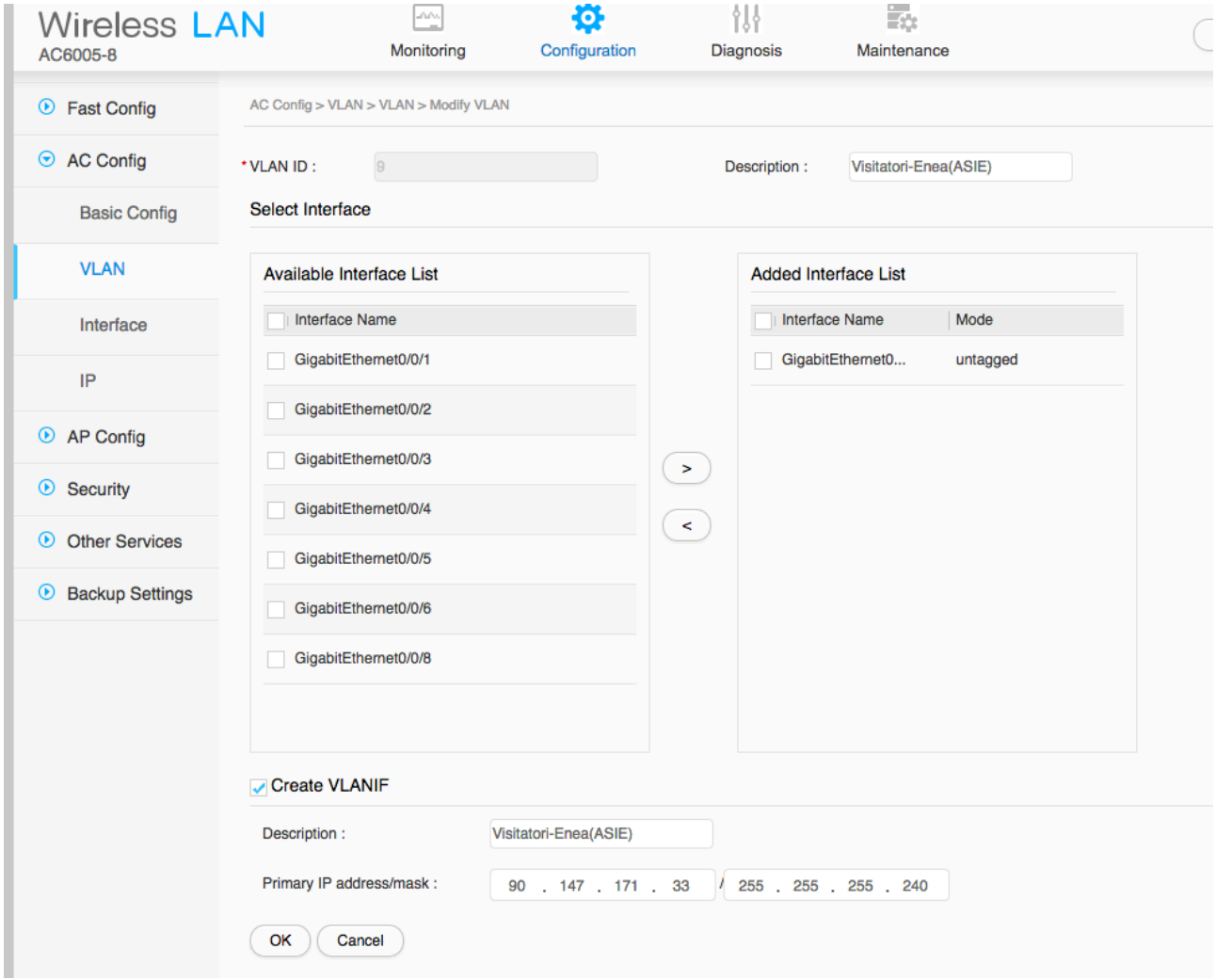
ip route 90.147.171.0 255.255.255.0 10.10.254.2

5.3.2.2 Configurazioni sul Controller Huawei

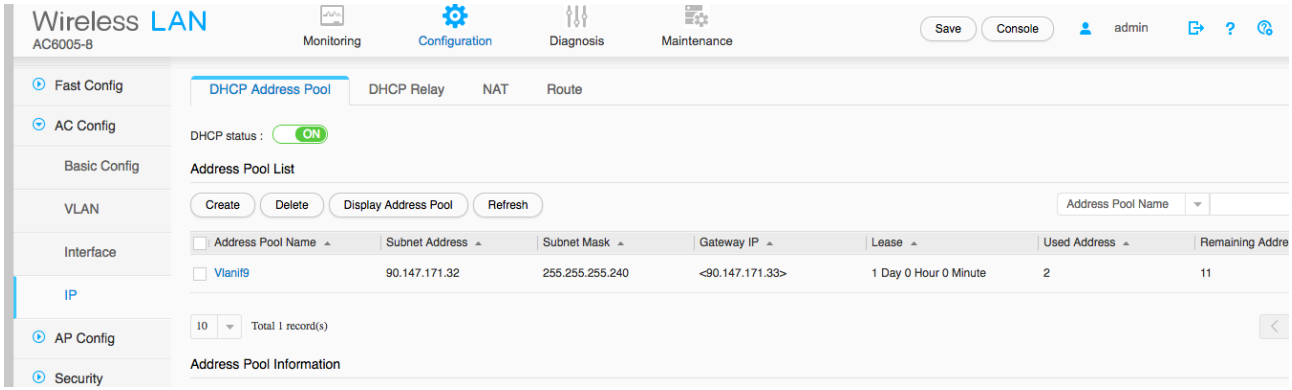
Diversamente da UTENTI-ENEA(ASIE), per SSID in titolo (e relativo instradamento e policy) è indispensabile che il traffico **attraversi il FireWall**. Quindi, avendo preventivamente individuato la rete pubblica:

90.147.171.32	*subnet ID*	mask 255.255.255.240 (=/28)	non utilizzabile come ind host !!!	
	33	primary ip add definito sul controller WiFi Hauwei per SSID Visitatori-Enea(ASIE)	client WiFi SSID VISITATORI-ENEA(ASIE) **VLAN 9**	sia per Enea Portici che per gli altri Centri e' una rete NON ENEA (i client non possono visitare la INTRANET)
	...		"	
	46	**FireWall 1/4**	**GW def per questa subnet**	
90.147.171.47		broadcast di questa subnet	non utilizzabile come ind host !!!	

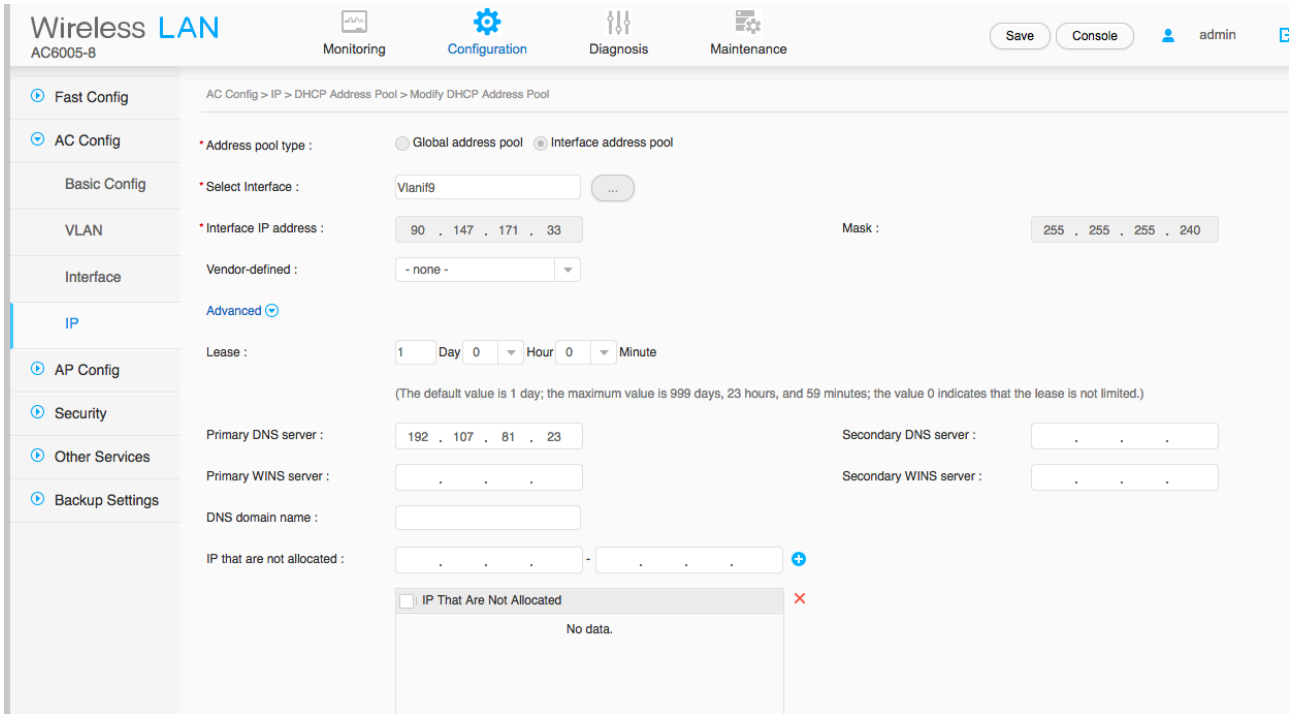
via una scorciatoia (diversamente dalla regola generale) Configurarion – AC config – VLAN si configura:



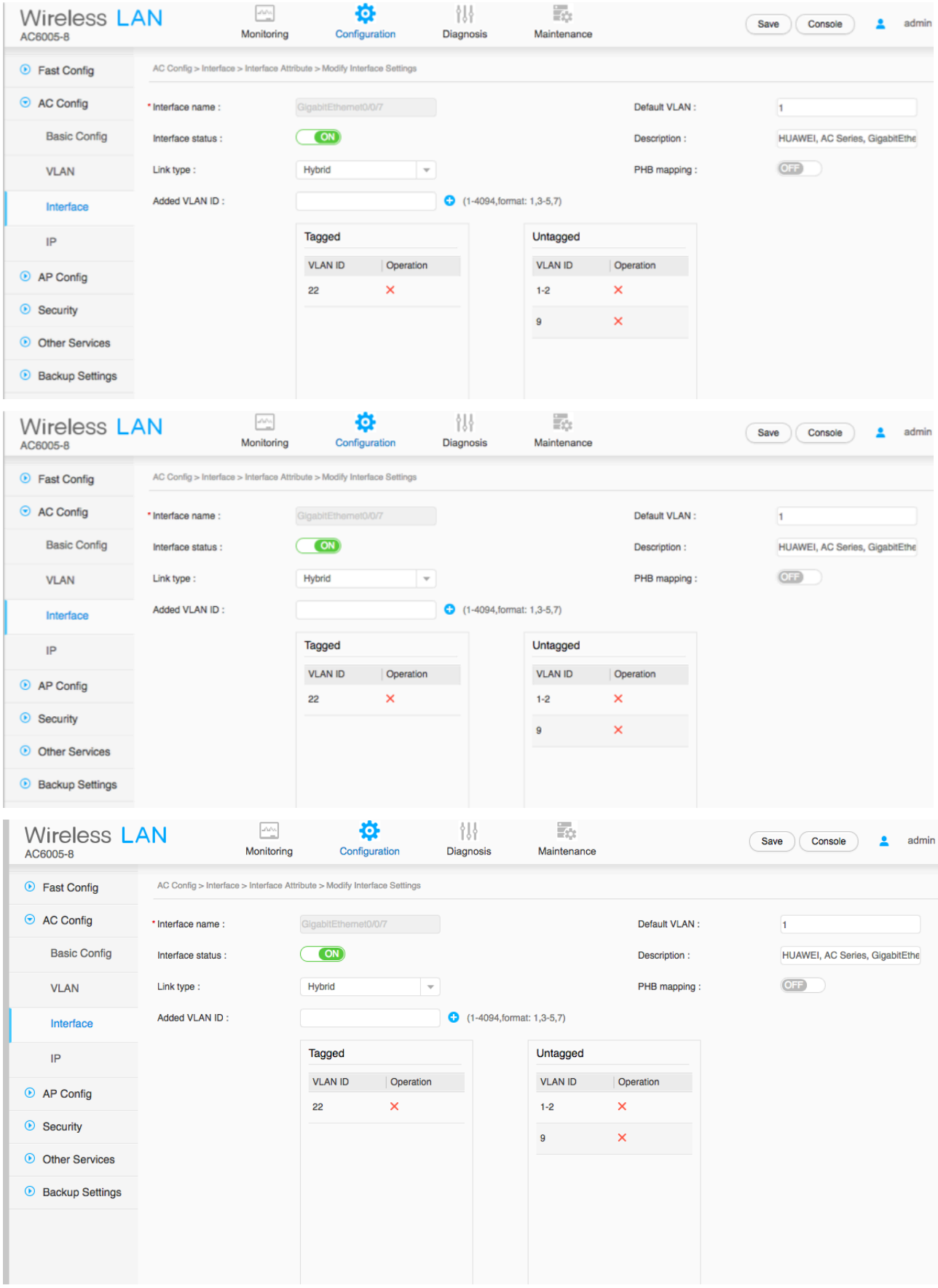
Deve risultare creata la vlan9:



cosi' personalizzata:

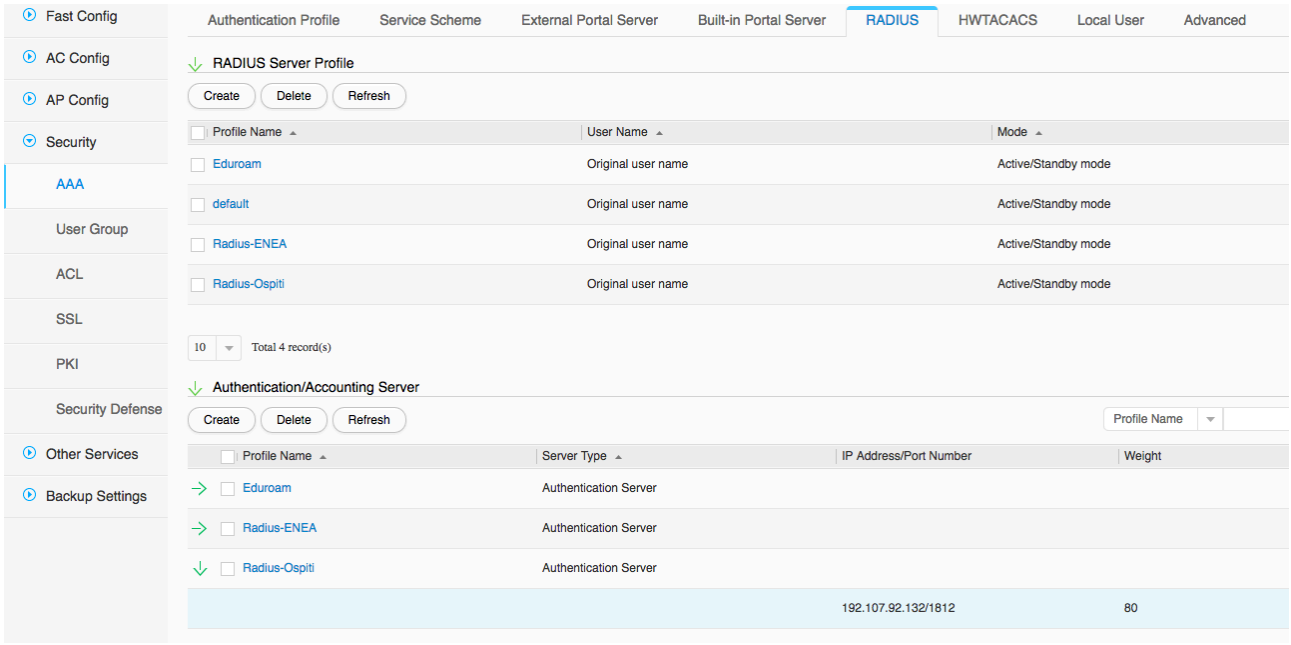


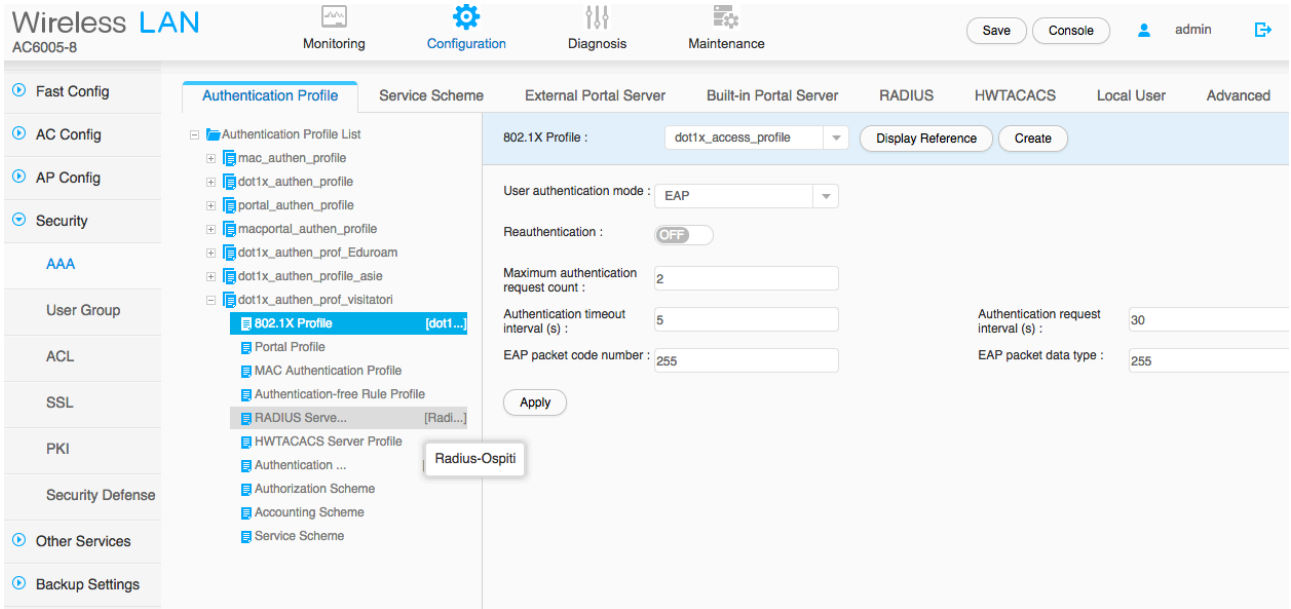
In Configuration – AC Config – Interface si specifica inoltre che la vlan9 è untagged su interfaccia di uplink:

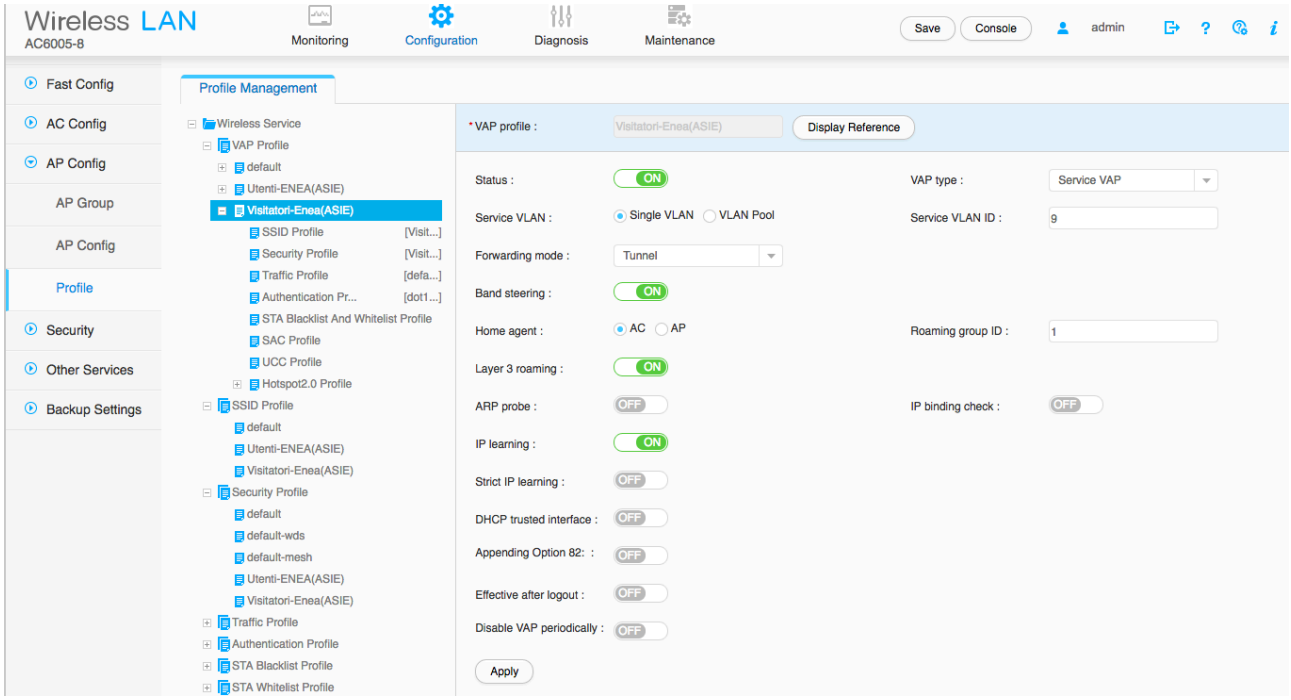


Per quanto riguarda i Profili AAA, si procede pedissequamente a quanto già fatto per SSID UTENTI-ENEA (ASIE), con le particolarità :

1) il Radius Server di riferimento deve essere per ora la macchina appositamente creata in Casaccia (per HA, a breve sarà replicata a Portici)
2) il tipo di traffico sarà Tunnel come nel seguito dettagliato.







dove, nel dettaglio, i campi “Forward mode: Tunnel” ed “Home Agent: AC” implicano che il traffico tra wifi-client à AP à mondo, passi sempre per il Controller (modalità Tunnel).

5.3.3 SSID: EDUROAM

5.3.3.1 Configurazioni propedeutiche su apparati diversi

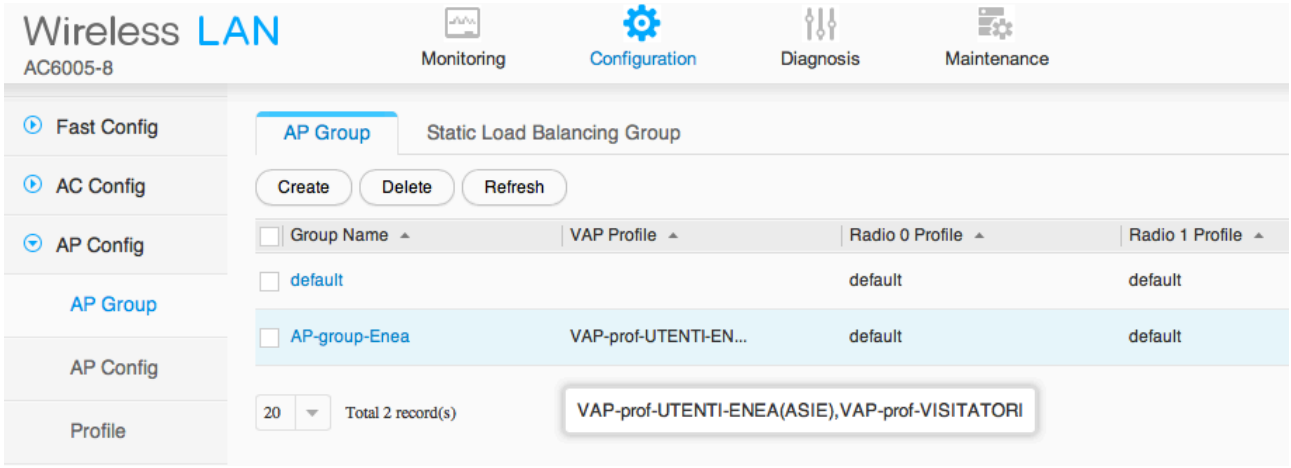
Operazioni analoghe fanno fatte agli apparati perimetrali (FireWall e Router).
Per i motivi di sinteticità citati in premessa, non vengono dettagliati.

5.3.3.2 Configurazioni sul Controller Huawei

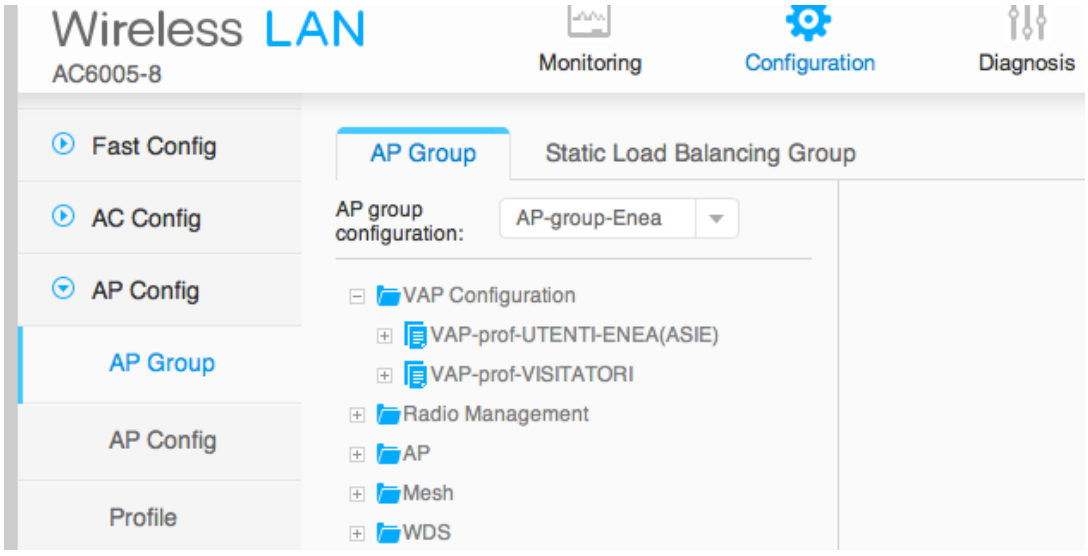
Per questo SSID bisogna approntare tutti gli oggetti (Profili, reti, dhcp-pool, ecc.) del tutto analoghi a quelli già creati per SSID: VISITATORI-ENEA(ASIE).
Per i motivi di sinteticità citati in premessa, non vengono dettagliati.

5.4 Creazione di un AP Group

Nel menu che segue si crea il nuovo AP Group “AP-ENEA”:



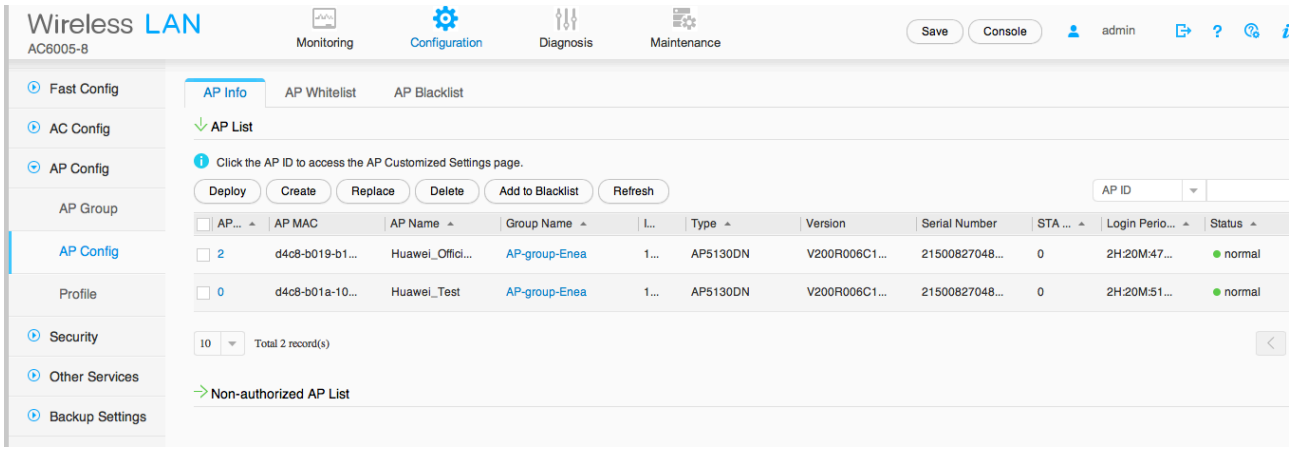
selezionatolo, vi si addizionano i Virtual Access Point (VAP) creati in precedenza e risulterà:



5.5 Joining dell'AP

Si è giunti allo step finale in cui, per far in modo che l'AP 0, al momento solo rilevato dal Controller, erediti tutto quanto predisposto nel gruppo AP-ENEA:

Configuration – AP Config – AP Config – si spunta il particolare AP e tap sul Group-Name:



Al menu successive si specifica AP-Group cui si vuol associare il dispositivo.

6) Verifiche continuità di servizio inter-Centro degli AP

Per default, ogni AP si registra al Controller della LAN in cui si trova. È possibile tuttavia "fissare" l'IP del Controller di riferimento affinchè ovunque l'AP sarà posizionato (in un Centro Enea diverso, in altro Istituto, uno Stand Fieristico, ecc.), dopo aver ottenuto un indirizzo DHCP, contatterà il Controller (o i Controller che gli sono stati configurati). Su ogni AP è possibile configurare fino a 4 Controller. La sintassi è quella del par. 4.1

7) Cluster di Controller

La continuità di servizio di cui al paragrafo precedente si affianca al "cluster di Controller" che ci è stato proposto come possibile dalla società Huawei. In effetti però il cluster sarebbe del tipo "active/stand-by" mentre la soluzione di utilizzare più Controller sugli AP farebbe "lavorare" tutti i Controller contemporaneamente e solo in caso di necessità alcuni di questi, opportunamente configurati, potrebbero continuare ad erogare il servizio sul Controller di backup.

Appendice

A1) Comandi utili in ambito cmd (command line)

I comandi che seguono possono essere dati una volta collegatosi con successo all'apparato via ad es :

MdRs-iMac:~ derosa$ **ssh admin@90.147.171.49**

admin@192.107.81.35's password:

User last login information:

Access Type: Web

IP-Address : 192.168.18.251

Time : 2017-02-28 10:12:48+01:00

A1.1) display current-configuration

<AC6005>**system-view**

Enter system view, return user view with Ctrl+Z.

[AC6005]**display current-configuration**

#

http secure-server ssl-policy default_policy

http server enable

#

dns server 192.107.81.23

….

….

A1.2) reset save-configuration

È il comando che ripristina i valori di fabbrica se esercitato nel modo che segue:

…..

The action will delete the saved configuration in the device.

The configuration will be erased to reconfigure. Continue? [Y/N]:**y**

…..

<Gulshan-02>

<Gulshan-02>reboot ?

fast Reboot system fast

<cr>

<Gulshan-02>**reboot**

Info: The system is now comparing the configuration, please wait.

Warning: All the configuration will be saved to the configuration

file for the next startup:, Continue?[Y/N]:**n**

System will reboot! Continue?[Y/N]:**y**

…….

….

Attenzione: seguire e verificare che l'operazione si completi; impiega oltre 10 minuti.

Recover configuration...OK!

Press ENTER to get started.

Please configure the login password (6-16)

Enter Password:

Confirm Password:

<Quidway>

<Quidway>

A1.3) Impostazione nome apparato

Nell'esempio di un AP, una volta autenticatosi via le credenziali di default:

MdRs-iMac:~ derosa$ ssh admin@192.168.12.2

admin@192.168.12.2's password:

Info: You are advised to change the password to ensure security.

<d4c8-b01a-1040>system-view

[d4c8-b01a-1040]**ap-sysname Huawei_Test**

Info: The configuration takes effect after the AP is restarted.

A1.4) AP monitoring

<AC6005>**display ap all**

Total AP information:

idle : idle [1]

nor : normal [2]

ID MAC Name Group IP Type State STA Uptime

---

0 d4c8-b01a-1040 Huawei_SalaRete AP-group-Enea 192.168.12.2 AP5130DN nor 4 1H:49M:26S

2 d4c8-b019-b1a0 Huawei_Officina AP-group-Enea 192.168.12.3 AP5130DN nor 0 1H:49M:9S

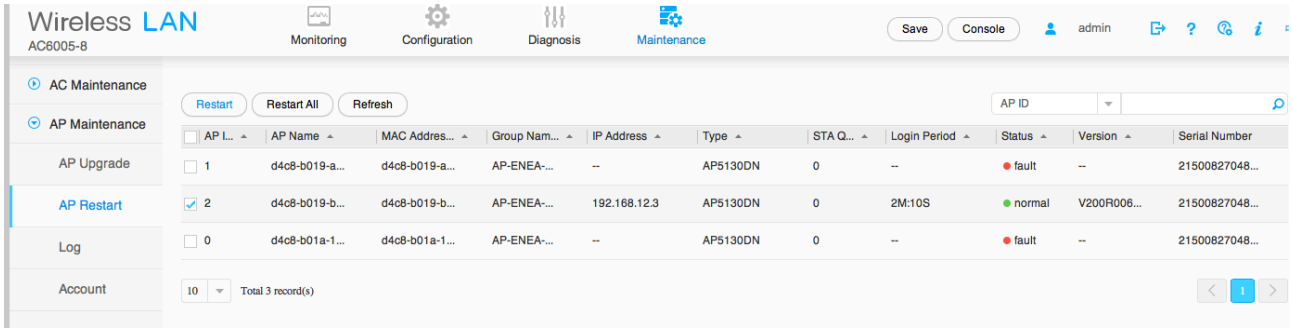
3 d4c8-b019-aa80 d4c8-b019-aa80 default - AP5130DN idle 0 -

Total: 3

A2) Azioni utili via GUI

A2.1) Restart un AP

Tap su restart nella finestra che segue:



A2.2) Modifiche ad un AP

Presente in menu Configuration – AP Config – AP Config –

Individuato un AP, facendo TAP sul gruppo, si evidenziano tutti i campi modificabili, tra cui il nome del dispositivo.

Per terminare la configurazione di un “nuovo” AP può essere indicato NON usare la modalità prima descritta ma usare il tasto “deploy”. In questo caso sarà possibile configurare:
il NOME dell’AP; il gruppo di appartenenza; la modalità di assegnazione dell’IP (statico o dhcp): in caso di IP statico sarà possibile definirlo dalla stessa schermata.

ENEA
Servizio Promozione e Comunicazione
www.enea.it

Stampa: Laboratorio Tecnografico ENEA - C.R. Frascati
gennaio 2018