LABORATORIO DIDATTICO 1

Installazione, configurazione e verifica della copertura radio di un Access Point (AP)

In questo Laboratorio Didattico si illustra una procedura per installare un Access Point, configurarlo e verificarne la copertura radio.

Strumentazione consigliata:

- un access point (AP), preferibilmente 802.11n (qui viene utilizzato l'AP DLINK DAP 2553);
- PC portatile con scheda Wi-Fi, preferibilmente 802.11n;
- software di scansione per reti Wi-Fi, qui viene utilizzato **InSSIDer** (www.inssider.com e metageek.net); il software era gratuito fino alla versione 3;
- software per l'analisi della copertura radio (site survey) di reti Wi-Fi, qui viene utilizzato **HeatMapper** scaricabile gratuitamente (previa registrazione) dal sito www.ekahau.com; www.ekahau.com/wifidesign/ekahau-heatmapper.

Operazioni preliminari.

- Facciamo un sopraluogo dell'area che dovrà essere servita dalla rete Wi-Fi; scegliamo un possibile punto di installazione per l'AP che sia in posizione elevata, libero da oggetti metallici circostanti e sufficientemente lontano da persone che stazionano in uno stesso punto in modo continuativo (lontano da banchi, scrivanie, ecc.), e il più possibile baricentrico rispetto all'area da servire.
- Ci posizioniamo nell'intorno del punto prescelto per l'installazione ed effettuiamo una scansione radio, ad esempio con *InSSDer*, per rilevare la presenza di altri AP e individuare i canali sui quali essi operano (FIGURA 1).

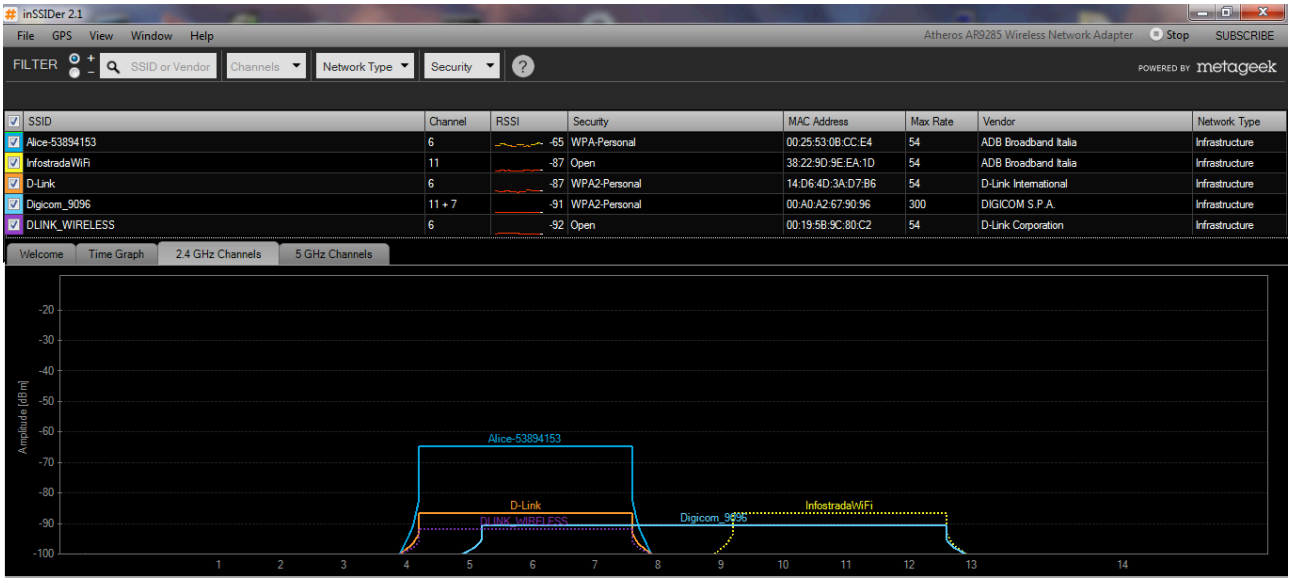

FIGURA 1 Scansione radio alla ricerca di AP Wi-Fi effettuata con inSSIDer.

Dalla FIGURA 1 si rileva la presenza di diversi AP dei quali ben 3 sono stati configurati per operare sul canale N. 6, mentre un quarto AP opera sul canale 11 ed un quinto AP è di tipo 802.11n ed opera con un canale da 40 MHz, ottenuto raggruppando (*bonding*) i canali 11 e 7.
In questa situazione il canale migliore su cui far operare il nostro AP è il canale N. 1.
Nel caso in cui non si trovi un canale libero selezioniamo il canale meno soggetto a interferenza, cioè nel quale gli spettri dei canali che si sovrappongono siano associati a livelli di potenza ricevuta più bassa (fornita dal parametro RSSI, *Received Signal Strenght Indicator*, indicatore dell'intensità del segnale ricevuto).

Preparazione alla configurazione dell'AP

- Posizioniamo l'AP nel punto prescelto e lo colleghiamo in rete attraverso l'interfaccia Ethernet (LAN).
  Normalmente l'AP ha configurato un indirizzo IP di default (si veda il manuale d'uso), per esempio il **192.168.0.1**, in modo tale che esso possa venire configurato in modalità GUI (*Graphical User Interface*) tramite il browser di un PC collegato in rete. Inoltre spesso l'AP integra un server DHCP (*Dynamic Host Configuration Protocol*) che, se abilitato, può fornire automaticamente gli indirizzi IP (ed i parametri correlati) ai PC che si collegano in rete tramite esso.
  Nel caso in cui l'AP sia già stato precedentemente configurato e si vuole procedere a una riconfigurazione completa è consigliabile procedere ad un *reset*, per ripristinare la configurazione di fabbrica, tipicamente premendo per qualche secondo un apposito pulsante di reset.
- Colleghiamo un PC in rete (o direttamente alla porta Ethernet dell'AP) e verifichiamo se l'AP ha attivato il server DHCP interno:
  - ci assicuriamo che il PC sia configurato per ottenere un indirizzo IP in modo automatico (*Ottieni automaticamente un indirizzo IP*);
  - apriamo il *Prompt dei comandi* e digitiamo il comando <*ipconfig /all*>;
  - se dalla risposta si rileva, tra l'altro, che l'indirizzo IP del server DHCP corrisponde a quello dell'AP allora il server DHCP dell'AP è abilitato; prendiamo anche nota dell'indirizzo IP assegnato al PC;
  - se invece la risposta è: indirizzo IP 0.0.0.0 oppure se l'indirizzo IP è del tipo 169.254.xx.xx (indirizzo autoconfigurato dal PC, per esempio 169.254.25.145) allora l'AP non integra il server DHCP (o esso è disabilitato).
- Se l'AP non ha attivato un server DHCP interno e più in generale se nella risposta al comando <*ipconfig /all*> non compare l'indirizzo IP dell'AP configuriamo il PC con un indirizzo IP statico, assegnandogli un indirizzo che appartenga alla stessa sottorete IP (subnet IP) dell'AP, che nel nostro caso può essere il **192.168.0.2**, come *subnet mask* utilizziamo quella specificata dal costruttore (se non è specificata impieghiamo la *subnet mask* di default 255.255.255.0).
- Da *Prompt dei comandi* digitiamo quindi **ping 192.168.0.1** (più in generale *ping* <*indirizzo IP dell'AP*>) per verificare se il PC è in grado di comunicare con l'AP e ottenere da esso una risposta.
- Lanciamo un *browser* e digitiamo sulla barra degli indirizzi l'indirizzo IP dell'AP.
  Inseriamo lo *username* e/o la *password* indicata nel manuale d'uso (spesso sono *username* **admin** e *nessuna password* iniziale, oppure *admin admin*), accedendo così al menu di configurazione.

Configurazione di base dell'AP

La configurazione di base dell'AP può essere effettuata nel seguente modo (ricordarsi di cliccare su *Apply* o *Save configuration*).

- Iniziamo cambiando lo *username* e/o la *password di accesso* (con l'AP DLINK sotto il menu *Maintenance*, *Administration*, *Login settings*) scegliendo una password che abbia almeno 8 caratteri e che comprenda lettere minuscole, maiuscole, numeri e caratteri speciali (!, & ecc.), come per esempio la seguente **Ac1es9oV2e8At7!**

Passiamo quindi alla configurazione di base (*Basic settings*) della sezione *Wireless*, scegliendo i seguenti parametri (FIGURA 2):

- *SSID* (*ESSID o Nome della rete*), per esempio LAB_TELE;
- *SSID Visibility* (o *SSID broadcast*): *enable* (disable); si abilita la trasmissione in broadcast (a tutti i client) da parte dell'AP dell'SSID configurato, in modo da semplificarne la configurazione; se vi sono stringenti requisiti di sicurezza è possibile disabilitare l'invio dell'SSID, che però deve essere configurato manualmente sui client;
- *Channel* (canale radio): scegliamo il canale meno disturbato, nel nostro caso il N. 1 (FIGURA 1).
- Scelta della modalità operativa: *Access Point*;
  spesso gli apparati Wi-Fi possono anche operare come:
  - *Bridge* o WDS (*Wireless Distribution System*), per interconnettere via Wi-Fi delle LAN poste, per esempio, in edifici diversi;
  - *Repeater* o *Wireless Client*, per estendere la copertura radio a punti non raggiunti da un AP principale, ecc.

Negli AP a standard *802.11n* è anche possibile scegliere:

- la banda radio (*Radio band o Wireless band*) su cui operare: **2,4 GHz** oppure **5 GHz**; scegliamo la banda dei 2,4 GHz; alcuni AP hanno una doppia sezione radio (*dual radio*) per cui possono operare contemporaneamente sia a 2,4 GHz sia a 5 GHz; va notato che la banda a 5 GHz è meno soggetta a interferenze, consente di operare con più AP che impiegano canali da 40 MHz, ma al momento non è supportata da tutte le schede Wi-Fi dei client;
- la larghezza di banda del canale (*Channel Width*): *20 MHz oppure 40 MHz*; se si impiega un solo AP e i client sono di tipo 802.11n allora risulta conveniente operare con canali da 40 MHz, in modo da massimizzare le prestazioni.

Configurazione della sicurezza wireless

- Si sceglie il tipo di *autenticazione* (*Authentication*): Open o Shared key, WPA-PSK (o WPA Personal), **WPA2-PSK** (detta anche **WPA2 Personal**); la scelta può essere messa in relazione al tipo di client che devono essere serviti dall'AP; se sono tutti computer recenti conviene scegliere la **WPA2-PSK**, più robusta ma che richiede maggiore capacità elaborativa; in caso contrario si sceglie la WPA-PSK oppure, solo se i client non supportano altro, la Open o la Shared key; normalmente l'autenticazione *WPA Enterprise* viene utilizzata solo in ambito aziendale in quanto richiede la presenza in rete di un apposito server di autenticazione (*server RADIUS*).
- Si sceglie il tipo di crittografia in relazione al tipo di autenticazione configurata: **AES** per la **WPA2-PSK**; **TKIP** per la **WPA-PSK**; **WEP** con chiave a 128 bit per l'autenticazione Open o Shared Key.
- Per la **WPA/WPA2-PSK** si configura la *PassPhrase* (*Chiave di sicurezza*) da utilizzare con i criteri delle password sicure; è anche possibile configurare il tempo dopo cui la chiave di crittografia viene cambiata (*Key Renewal o Key update*, tipicamente ogni 1800 o 3600 secondi di default), conviene diminuire tale tempo solo se vi sono stringenti requisiti di sicurezza; per la WEP si configura una chiave WEP (statica) a 128 bit, costituita da una stringa di 26 caratteri esadecimali.

In FIGURA 2 si mostra un esempio di configurazione.

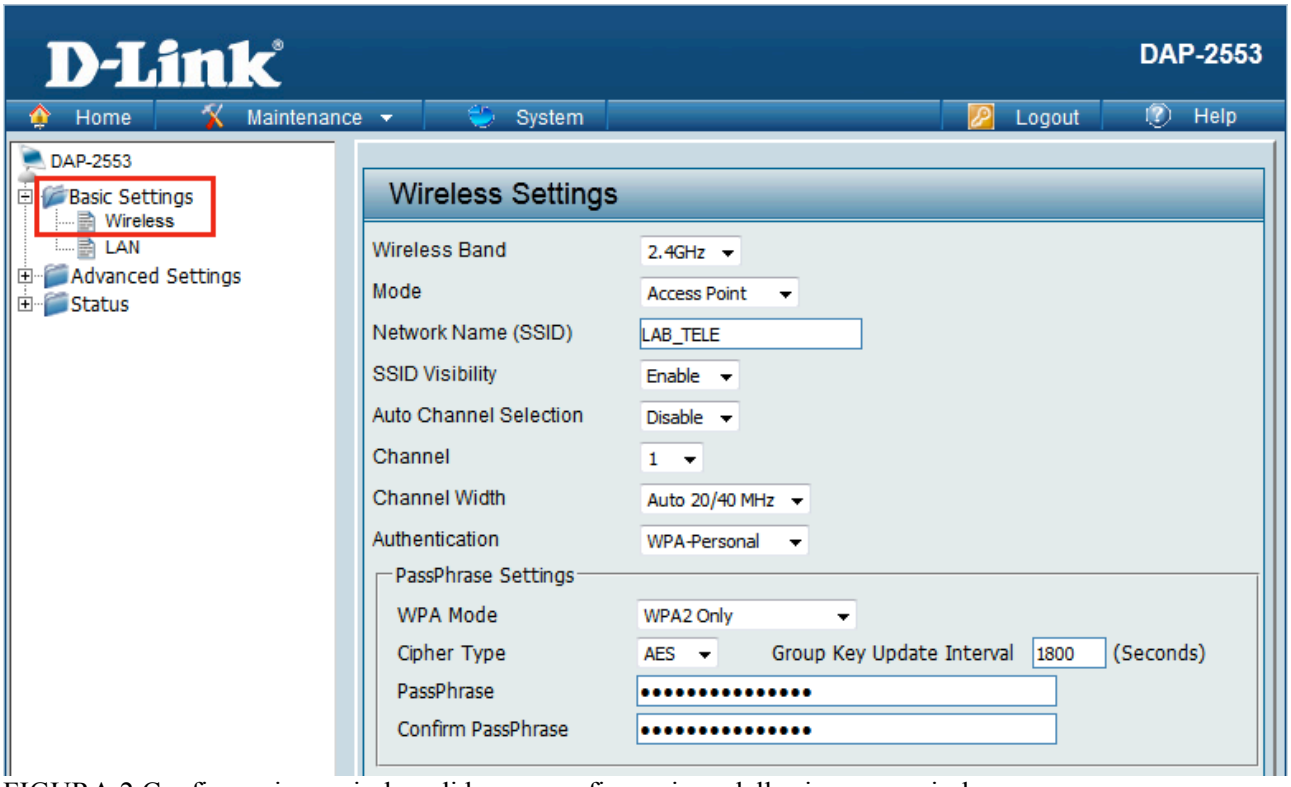

FIGURA 2 Configurazione wireless di base e configurazione della sicurezza wireless

Configurazione della sezione LAN
Configuriamo ora la sezione LAN (FIGURA 3), cioè l'interfaccia Ethernet tramite cui l'AP viene collegato a uno switch.

- Scegliamo di configurare un *indirizzo statico*, diverso da quello di default, in modo da semplificare la configurazione in rete dell'AP, in quanto l'indirizzo IP dell'AP non cambia ed è noto.
- Configuriamo un indirizzo IP e la relativa subnet mask che appartenga alla sottorete (subnet) IP su cui si opera, ma che non rientri nel range di indirizzi a disposizione del server DHCP che assegna in modo automatico e dinamico gli indirizzi IP ai client; in questo modo si evitano conflitti tra gli indirizzi IP dei client e dell'AP; per esempio se la subnet IP a cui appartengono i client è la 10.0.0.0 con subnet mask 255.255.255.0 e il server DHCP distribuisce gli indirizzi IP a partire dal 10.0.0.40, possiamo scegliere come l'indirizzo IP **10.0.0.15,** con subnet mask la **255.255.255.0**.
- Il *Default Gateway* va configurato obbligatoriamente solo se si desidera che l'AP possa essere configurato in remoto, da un PC appartenente a un'altra sottorete (subnet) IP, diversa da quella a cui appartiene l'AP stesso, ed è dato dall'indirizzo IP del router tramite cui si accede alle reti/sottoreti IP esterne;

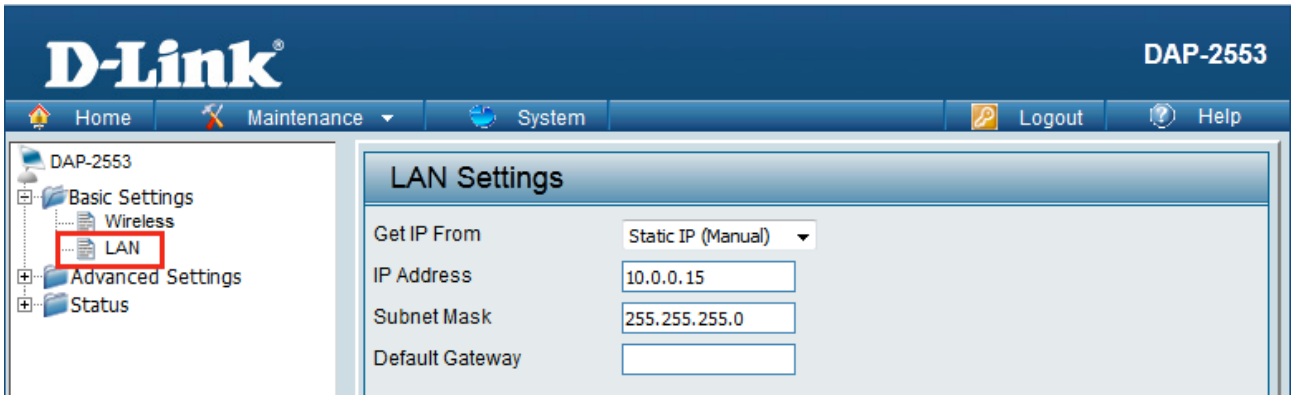

FIGURA 3 Configurazione della sezione LAN.

La configurazione di base è terminata per cui possiamo iniziare ad utilizzare l'AP. Ricordiamoci di ripristinare sul PC utilizzato la configurazione IP corretta per l'utilizzo sulla sottorete IP a cui appartiene l'AP, ripristinando per esempio la configurazione automatica acquisita da un server DHCP o modificando manualmente l'indirizzo IP del PC.
Se vi sono stringenti requisiti di sicurezza è possibile creare una VLAN a cui possono accedere solo i client Wi-Fi e/o una VLAN dedicata esclusivamente all'amministrazione dell'AP (e di altri apparati di rete) tramite uno specifico PC.

Configurazioni avanzate
Per massimizzare le prestazioni della rete Wi-Fi è possibile agire sulle seguenti configurazioni avanzate (FIGURA 4).

- Scelta del tipo di client da servire (*Wireless mode*):
  - **Mixed 802.11b/g/n**, l'AP supporta contemporaneamente tutti gli standard Wi-Fi e quindi può servire sia client (PC) vecchi sia client nuovi;
  - **Only 802.11n** (oppure Only 802.11g per gli AP meno recenti), l'AP serve esclusivamente i client che impiegano schede Wi-Fi in grado di supportare lo standard selezionato.

  La scelta del *Mixed mode* peggiora le prestazioni della rete per cui se si impiegano solo PC recenti, con schede Wi-Fi 802.11n, è consigliabile scegliere la modalità *Only 802.11n* in modo da massimizzare le prestazioni della rete Wi-Fi (che con lo standard 802.11n può arrivare a 150 Mbit/s se i client sono dotati di una sola antenna trasmittente integrata e a 300 Mbit/s se i client hanno schede Wi-Fi dotate di 3 antenne).
- Abilitazione dello *Short GI* (*Guard Interval*), si diminuisce l'intervallo di tempo in cui non si trasmette nulla, intervallo detto *tempo di guardia* e necessario per evitare problemi di interferenza intersimbolica

(da 800 ns il GI viene portato a 400 ns); ciò consente di aumentare il *throughput* supportato dalla rete, cioè la velocità dell'effettivo scambio dati.

- Abilitazione del *Wi-Fi Multimedia* (WMM) nel caso in cui si impieghi la rete Wi-Fi anche per comunicazioni audio e/o video.

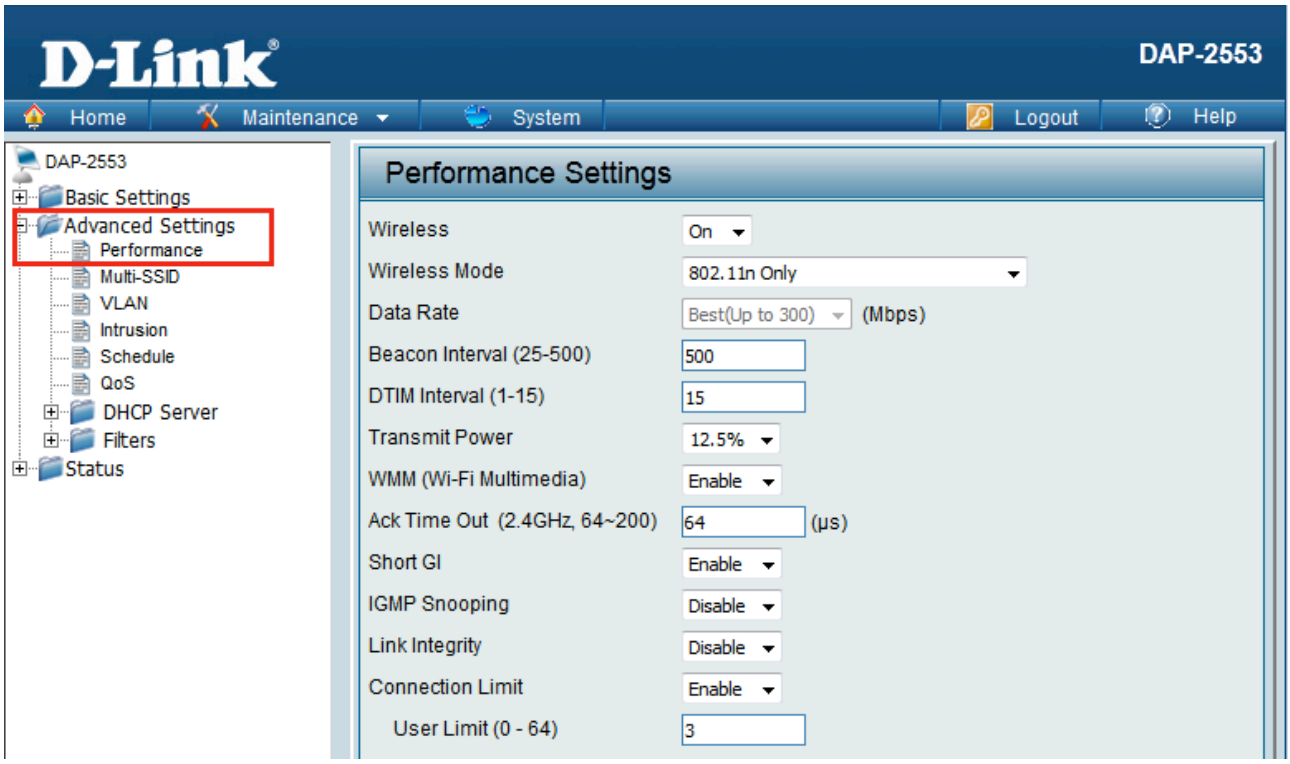

FIGURA 4 Configurazioni avanzate per massimizzare le prestazioni

Per aumentare la sicurezza della rete Wi-Fi è possibile agire sulle seguenti configurazioni avanzate.

- *Regolazione della potenza di trasmissione* (*Transmit Power*); su molti AP è possibile diminuire la potenza di trasmissione rispetto al valore massimo consentito dalle normative (EIRP = +20 dBm); questa scelta è consigliabile quando l'area da servire è piccola (un ufficio, un laboratorio, ecc.) in modo da rendere più sicura la rete, in quanto si limita la copertura radio all'esterno, limitare l'inquinamento elettromagnetico, limitare le interferenze create verso altri AP che operano sullo stesso canale.
- *Limitazione del numero di client che possono associarsi all'AP*; se il numero di client Wi-Fi che devono accedere alla WLAN è noto e fisso è possibile configurare tale numero sull'AP, in modo da aumentare la sicurezza oppure consentire un bilanciamento del traffico fra più AP (raggiunto il numero massimo di client l'AP non ne accetta altri per cui essi devono tentare l'associazione con un altro AP).
- *Filtraggio degli indirizzi MAC* (*Wireless MAC Filter o Access Control List,* FIGURA 5); abilitando questa opzione è possibile indicare all'AP gli indirizzi MAC delle schede Wi-Fi dei client ai quali *è permesso* **(***permit o accept***)** l'accesso alla rete Wi-Fi oppure a cui *va impedito* (*prevent o reject*) l'accesso alla rete Wi-Fi; è questo un modo per aumentare la sicurezza della rete, anche se va notato che è relativamente semplice (specie in ambiente LINUX) configurare un client affinché operi con l'indirizzo MAC desiderato (diverso da quello della scheda configurato dal costruttore).

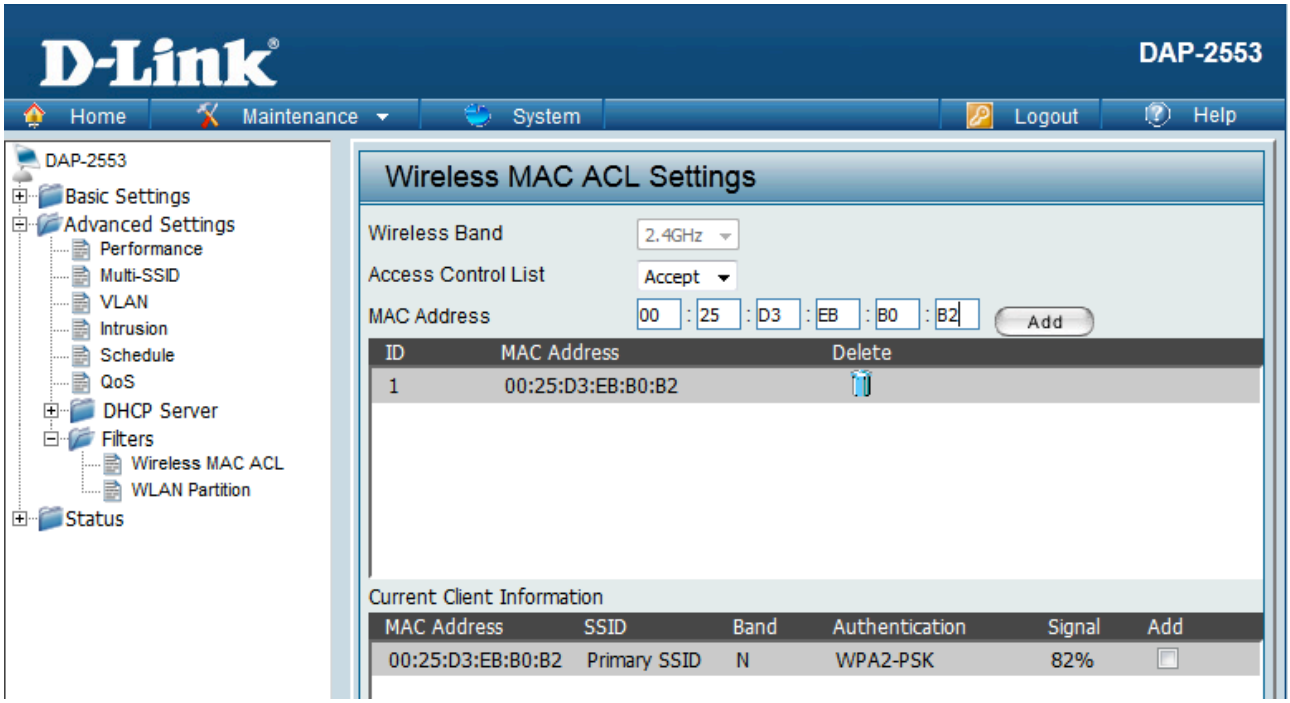

FIGURA 5 Configurazione del filtro MAC

Altre configurazioni avanzate sono le seguenti

- *Beacon Interval* (tipico: 100 ms): a intervalli di tempo regolari, configurabili, l'AP trasmette in broadcast un segnale detto *Beacon* (segnale di guida) che comunica ai client l'esistenza della rete Wi-Fi e varie informazioni di servizio, quali l'SSID (nome della rete), se ne è abilitato il broadcast, le velocità supportate dall'AP, ecc.
- *DTIM* (*Delivery Traffic Indication Message*); è un parametro impiegato da client portatili che si possono porre in *low power mode* (*stand by*), in modo da consumare meno le batterie; l'AP bufferizza le informazioni destinate a tali client, i quali a intervalli di tempo regolari possono "risvegliarsi" (*wake up*) e controllare se l'AP ha del traffico destinato ad esse; l'AP indica attraverso il parametro DTIM (espresso come numero di beacons) ogni quanto tempo il client deve controllare se vi è traffico bufferizzato ad esso destinato.

  Per gli AP a standard 802.11b/g si possono anche configurare i seguenti parametri:
  - *Fragmentation Threshold* (tipico 2346 byte), indica la lunghezza massima che può avere un frame senza che debba essere frammentato, cioè suddiviso in frame più piccoli; la frammentazione degrada le prestazioni per cui è conveniente disabilitarla configurando come Fragmentation Threshold la lunghezza massima che può assumere un frame 802.11, pari a 2346 byte;
  - *RTS Threshold* (tipico 2347 byte); indica la dimensione minima che deve avere un frame affinché venga impiegato il meccanismo RTS/CTS impiegato dal metodo CSMA/CA per evitare le collisioni: prima di inviare dei dati si deve trasmettere l'RTS (Request To Send, richiesta di trasmissione) ed attendere il CTS (Clear To Send, trasmissione autorizzata), con un rallentamento dello scambio dati; fissando il valore a 2347, maggiore della dimensione massima dei frame 802.11 si disabilita il meccanismo RTS/CTS, migliorando le prestazioni della rete Wi-Fi
- *Server DHCP*; alcuni AP comprendono anche un server DHCP che può essere configurato ed abilitato per fornire automaticamente gli indirizzi IP ai client che accedono in rete (FIGURA 6); se però nella LAN cablata è già presente un server DHCP disabilitiamo quello dell'AP.

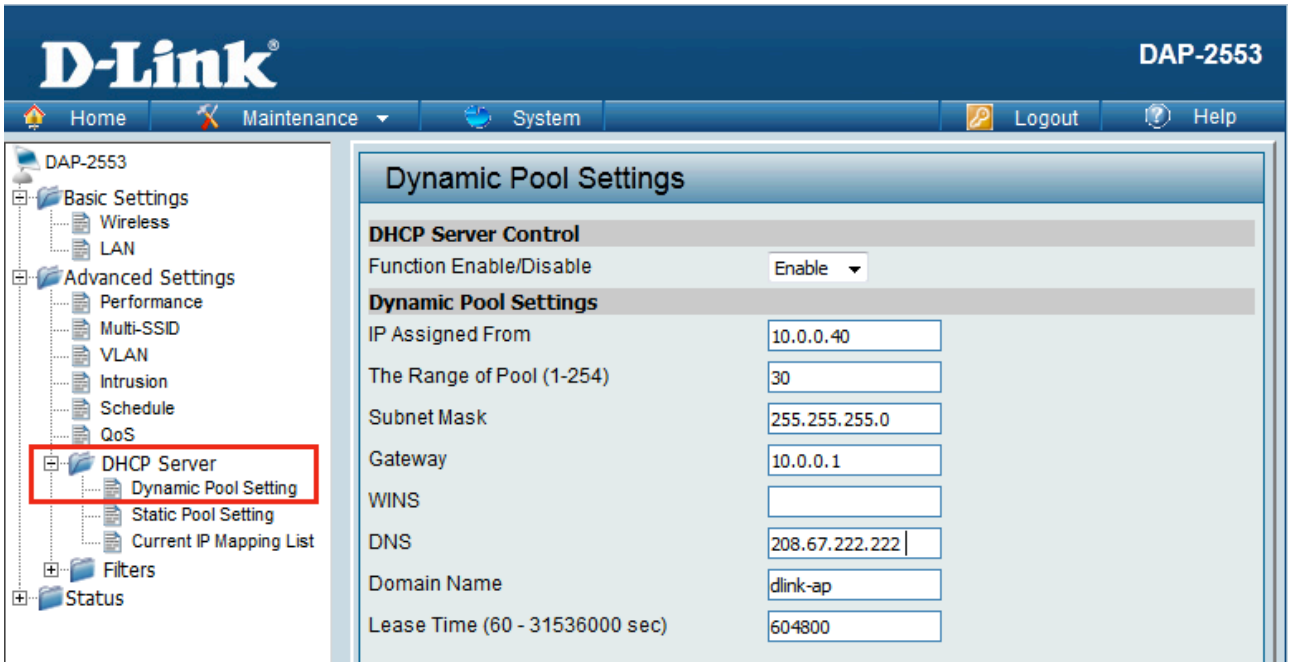

FIGURA 6 Configurazione del server DHCP

Gli AP a standard 802.11n supportano numerose altre opzioni avanzate: SSID multipli (multi SSID), VLAN (Virtual LAN), QoS (Quality of Service), ecc.

Verifica del funzionamento e della copertura radio dell'AP
Una volta configurato l'AP effettuiamo le seguenti verifiche.

- *Tipo di connettività fornita ai client*; su un PC (preferibilmente portatile) verifichiamo che la connessione wireless sia attiva; clicchiamo quindi col tasto sinistro del mouse sull'icona delle connessioni di rete, clicchiamo col tasto destro sulla rete Wi-Fi (LAB_TELE) e selezioniamo *Stato*. Dalla FIGURA 7 si rileva che il PC client si è connesso in modalità 802.11n, alla velocità (lorda) di 150 Mbps (Megabit per second, Mbit/s).

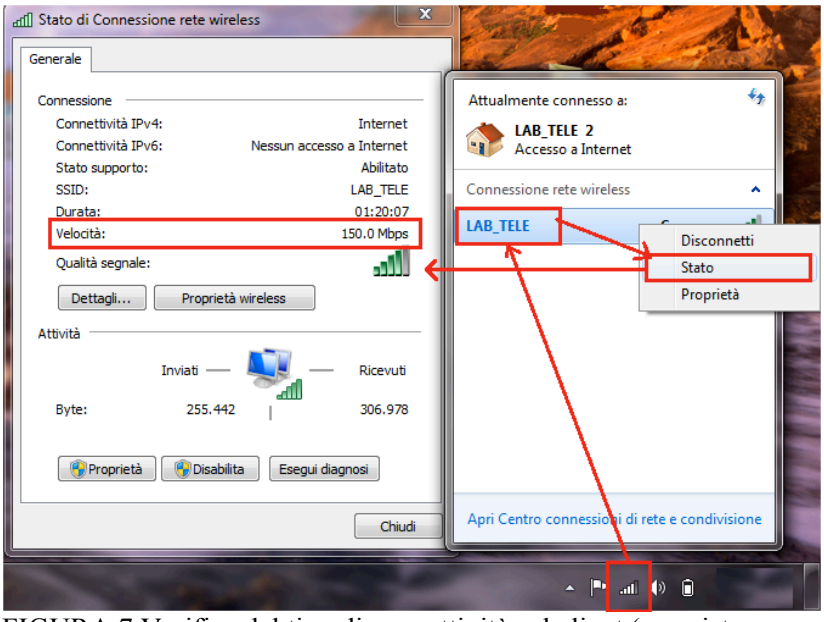

FIGURA 7 Verifica del tipo di connettività sul client (con sistema operativo Windows 7)

Verifica del canale radio utilizzato
Su un PC portatile lanciamo un software di scansione radio Wi-Fi, per esempio **InSSIDer**, e rileviamo le caratteristiche del canale radio configurato. Dalla FIGURA 8 si rileva che:

- l'AP opera con un canale da 40 MHz, ottenuto raggruppando (*bonding*) due canali da 20 MHz (i canali N. 1 e 5);
- vi sono delle inevitabili piccole interferenze da parte di altri AP che operano sul canale N. 6.

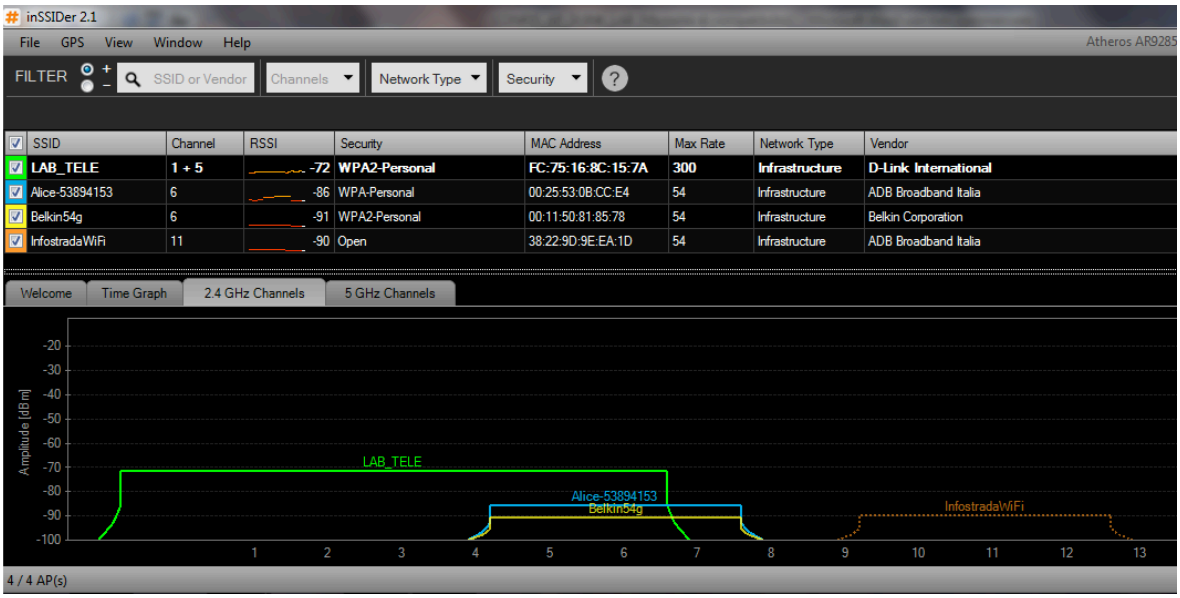

FIGURA 8 Scansione radio con InSSIDer

Verifica della copertura radio offerta dall'AP

Se si possiede una piantina digitalizzata dell'area da servire è possibile verificare la copertura radio offerta dall'AP, sia all'interno dell'edificio sia all'esterno, installando su un PC portatile il software di mappatura radio (*site survey*) **HeatMapper** ed operando nel seguente modo:

- dopo aver lanciato *HeatMapper*, si seleziona l'icona che permette di caricare la piantina dell'area da mappare;
- ci si posiziona nelle immediate vicinanze dell'AP, si clicca col pulsante sinistro per avviare la mappatura, ci si sposta lungo il perimetro dell'area da servire, prima all'interno e poi all'esterno cliccando col tasto sinistro nei punti più significativi;
- si termina la mappatura cliccando col tasto destro.

In FIGURA 9 è riportato un esempio di mappatura della copertura radio, da cui si evince che pur operando con potenza ridotta (12,5%) si ottiene una buona copertura radio all'interno dell'edificio monitorato.
La colorazione della mappa di FIGURA 9 indica (qualitativamente) che la copertura radio è:

- eccellente o molto buona se il livello di potenza in ricezione è superiore a circa -55 dBm;
- buona o discreta se il livello di potenza in ricezione è compreso all'incirca fra -55 e -70 dBm;
- sufficiente se il livello di potenza in ricezione è compreso all'incirca fra -70 e -80 dBm;
- mediocre o scarsa se il livello di potenza in ricezione è inferiore a -80 dBm

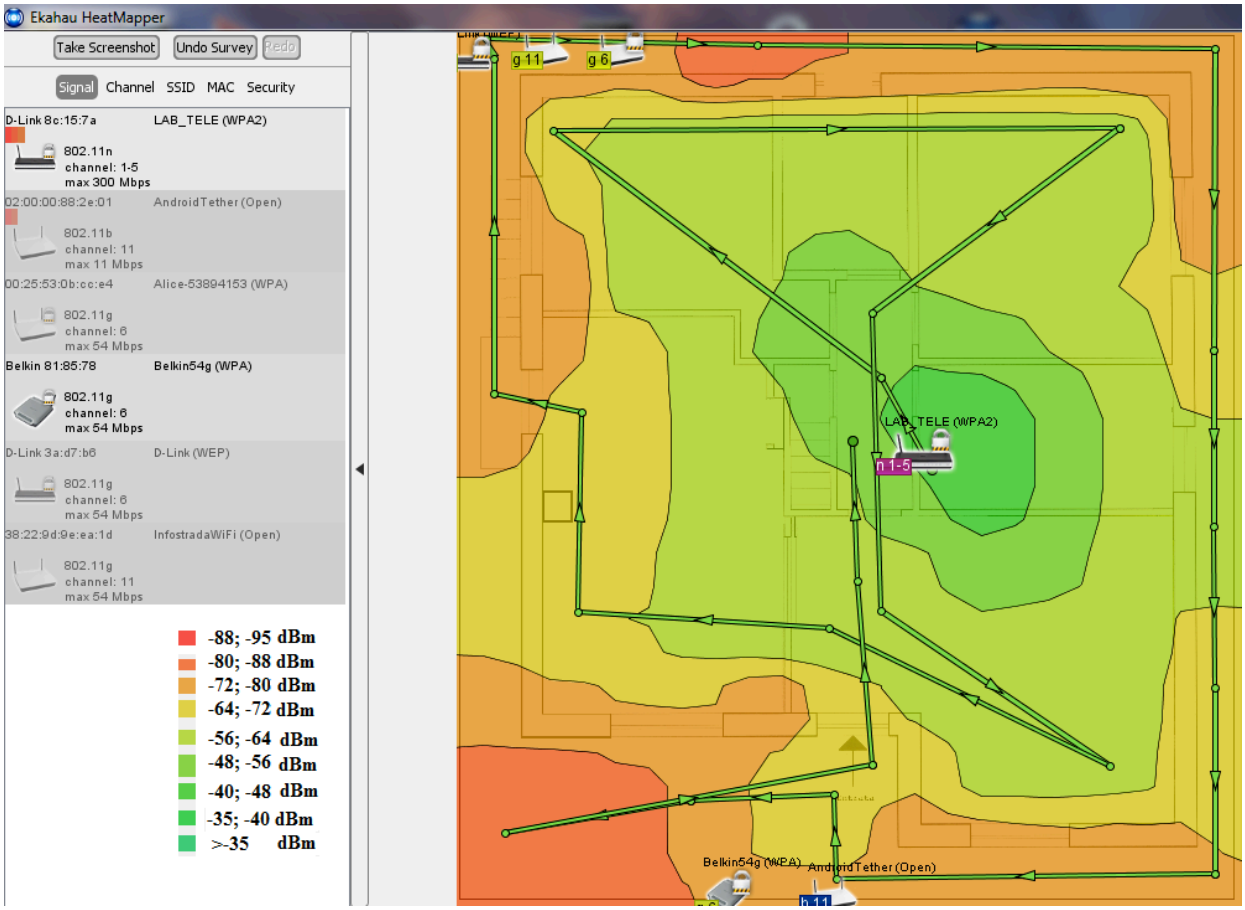

FIGURA 9 Mappatura della copertura radio effettuata con HeatMapper.