

Mobile & Wireless

Di Simone Zanardi



Senza fili le funzioni evolute per l'azienda

L'Italia è il paese delle piccole e piccolissime aziende, realtà che spesso dispongono di strutture informatiche poco più complesse rispetto a quelle di un piccolo ufficio domestico e che altrettanto frequentemente sfruttano dispositivi di derivazione Soho (*Small Office Home Office*) per la propria struttura informatica, pensando in questo modo di risparmiare sui costi.

A volte, però, chi più spende meno spende: in ambito wireless, ad esempio, acquistare un sistema Wi-Fi di livello professionale può richiedere un esborso iniziale leggermente maggiore ma consente di risparmiarsi in seguito tempo e problemi, grazie ad alcune funzioni che semplificano e rendono più efficiente

la gestione dei collegamenti senza fili in azienda. Quando si imposta la protezione della rete wireless attraverso il protocollo Wpa2 (quello che ci sentiamo di consigliare a tutti gli amministratori di una rete wireless), lo standard Wi-Fi mette ad esempio a disposizione due modalità di autenticazione: la prima, più adatta agli ambienti consumer e agli uffici di ridottissime dimensioni, utilizza una password pre-condivisa (Psk, *Pre-Shared Key*) che deve essere nota a tutti gli utenti che vogliano accedere alla rete. La seconda, spesso chiamata *Wpa(2) Enterprise*, si appoggia a un server di autenticazione esterno per fornire i codici di accesso alla rete. Il server stesso comunica con il punto di accesso wireless attraverso

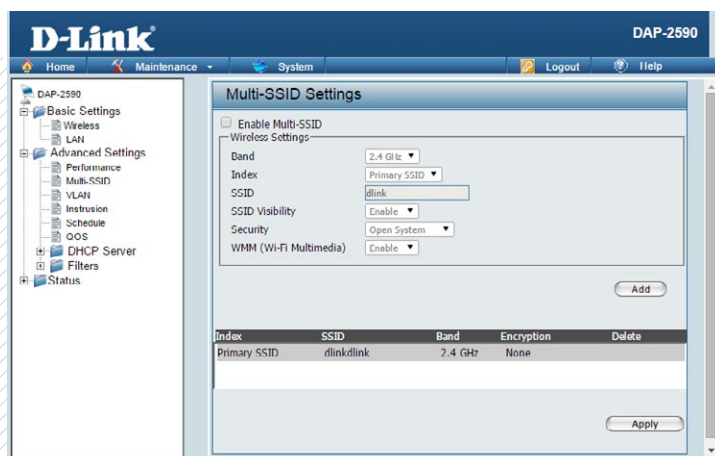
In ambito professionale è bene affidarsi ad access point di livello business, in grado di offrire servizi evoluti estremamente utili.

il protocollo Radius, mentre l'access point sfrutta lo standard 802.1x per bloccare le interfacce di comunicazione ai client non autenticati.

In una piccola azienda non è detto sia però presente un server compatibile con il protocollo Radius. In questi casi può tornare utile un access point con database utenti interno: l'amministratore di rete può così definire gli utenti autorizzati ad accedere alla rete direttamente sul pannello di controllo dell'access point, senza dover predisporre alcun server extra.

Il vantaggio dell'accesso tramite autenticazione è la possibilità di abilitare e disabilitare gli account in ogni momento: se ad esempio un dipendente lascia l'azienda, è sufficiente disattivare il suo profilo per escluderlo dalla rete wireless senza alcun impatto sul rimanente personale. Una soluzione a chiave pre-condivisa obbliga invece a cambiare la password, comunicarla a tutti i dipendenti e riconfigurare gli apparati.

Altra funzione particolarmente utile in ambito aziendale e non sempre



L'access point Draytek VigorAP 810, uno dei modelli con server Radius integrato: l'amministratore può definire account di accesso separati per ogni utente.



Gli access point professionali D-Link, tra cui il modello DAP-2590, permettono di configurare più Ssid impostando poi delle Vlan separate per gestire l'accesso differenziato alle risorse di rete.

supportata dagli access point entry level è la possibilità di definire reti wireless virtuali multiple, dedicandone ad esempio una agli accessi ospiti. Spesso le aziende che dispongono di una struttura wireless riservata ai dipendenti si vedono infatti in condizione di ospitare fornitori, clienti o altri partner che è utile dotare di accesso Internet Wi-Fi. È però indispensabile che questi utenti non possano raggiungere risorse sensibili e riservate della rete interna, ad esempio i server di produzione.

Molti access access point wireless fortunatamente permettono di definire per ciascun apparato radio più Ssid (*Service Set Identifier*), ovvero reti Wi-Fi separate agli occhi dei client. Ogni Ssid può essere quindi configurato secondo opportune regole di accesso e protezione. Per configurare un accesso guest limitato a Internet ci sono diverse strade: se l'access point funge anche da router a banda larga e prevede la funzione guest, è spesso disponibile una semplice opzione che limita appunto

le comunicazioni provenienti dai client ospiti verso la sola Wan (*Wide Area Network*, la rete esterna). Se l'access point è invece collegato a una struttura di rete più complessa si deve ricorrere alle Vlan (*Virtual Lan*) per segmentare opportunamente il traffico. Le Vlan possono operare a livello 2 o livello 3 della comunicazione Tcp/Ip/Ethernet, ma essenzialmente permettono di assegnare ciascuna porta di comunicazione (e anche gli Ssid) a un gruppo (Vlan). Per ciascuna Vlan sono poi definibili delle regole di accesso alle varie risorse di rete anche posizionate a distanza. Le Vlan sono utilizzabili non solo per definire accessi ospiti, ma anche per creare reti wireless dipartimentali, ciascuna gestita con specifiche policy della rete aziendale. Se la rete wireless della vostra azienda deve servire un'area o un numero di utenti troppo elevati per un singolo access point,

la soluzione migliore è poi quella di rivolgersi a un sistema distribuito con gestione centralizzata. I vantaggi di una struttura wireless multi-access point sono innumerevoli, sia per gli utenti finali che per gli amministratori di rete. In primo luogo, l'intelligenza della rete è centralizzata, con gli access point che divengono essenzialmente delle periferiche radio a cui vengono assegnati di volta in volta specifici parametri di funzionamento. Le regole di accesso e gli aggiornamenti di sistema vengono distribuiti a partire dal controller unificato, garantendo l'allineamento di tutti i punti di accesso alle policy aziendali.

La gestione degli access point multipli prevede anche le procedure di roaming, che permettono ai terminali di passare da una cella all'altra senza alcuna interruzione di servizio percepibile, in modo analogo a quanto avviene normalmente nelle reti cellulari mobili. In caso di reti particolarmente affollate, è poi possibile impostare meccanismi di load-balancing che distribuiscono automaticamente le connessioni dei terminali sui diversi punti di accesso per non sovraccaricare uno in particolare. Utile per le realtà di medie e grandi dimensioni è poi la rilevazione dei cosiddetti *roving access point*, dispositivi non autorizzati che possono essere collegati alle reti cablate per fornire accesso fraudolento. In questi casi il controller centrale rileva la periferica e ne blocca immediatamente l'accesso a qualsiasi risorsa, oltre a segnalare l'anomalia all'amministratore. •

Radius

Protocollo per l'autenticazione di utenti su strutture di rete distribuite.

Il controller Netgear ProSafe WC7520 può gestire una flotta di access point con funzioni di roaming, load balacing e rilevazione dei punti di accesso non autorizzati.

