

Una scelta consapevole

Alessandra Cimatti*

Per le pmi la scelta degli apparati può essere complicata. Alcune linee guida aiutano a orientarsi tra le numerose offerte

Chi desidera o deve installare una rete wireless, si trova spesso di fronte alla difficoltà di dover scegliere tra una serie di prodotti differenti, un'infinità di sigle e altrettanta pubblicità. Situazioni che, nella maggior parte dei casi, invece di contribuire a fare chiarezza, suscitano una serie di dubbi negli utenti finali; e questo perché, se da un lato può sembrare facile

decidere per il wireless, dall'altro pochi sanno quali aspetti tenere in considerazione per fare la giusta scelta.

Allora, cosa fare?

Di fronte a tanta complessità, prima di compiere delle scelte è indispensabile valutare attentamente tre aspetti. In primo luogo è necessario analizzare le

reali esigenze dell'organizzazione, poiché solo conoscendo l'obiettivo che si vuole perseguire è possibile scegliere tra prodotti che siano correttamente dimensionati rispetto ai requisiti richiesti. Due errori che si riscontrano frequentemente consistono nel sottostimare le necessità attuali e future del "carico" che la rete wireless deve garantire, oppure nel sovradimensionare l'impianto rispetto alle esigenze con conseguenti costi inutili. In seguito si dovrà svolgere un'accurata "diagnosi ambientale", tesa a individuare la presenza di strutture o condizioni che possano limitare il corretto passaggio delle onde elettromagnetiche. Muri, armadi, alberi e qualunque altro oggetto si frapponga fra il trasmettitore e il ricevitore hanno infatti un effetto

negativo sulla comunicazione. Va infine tenuto presente che i campi elettromagnetici generati da un sistema wireless finiscono anche all'esterno del perimetro dell'area di lavoro, favorendo l'azione di quanti cercano di collegarsi indebitamente alla rete. Simili collegamenti non autorizzati possono essere sfruttati per carpire i dati, utilizzare la rete in modo fraudolento o interrompere volontariamente le comunicazioni. A fronte di simili problemi, esistono soluzioni specifiche di sicurezza, che devono essere scelte in funzione del rapporto costi/benefici.

Non tutti sanno...

Non tutti sanno che la banda disponibile, ovvero la frequenza radio, è una risorsa condivisa tra tutti gli utilizzatori di una rete wireless. Quindi, più utenti ci sono, minore è la banda a disposizione di ciascuno e, di



Apparato multifunzione USR809108
MAXg Adsl2+ Wireless Gateway

conseguenza, la velocità. In prospettiva futura è perciò opportuno prevedere un margine di crescita, in grado di soddisfare un eventuale aumento del numero di utenti collegati. Allo stesso modo, anche le applicazioni hanno un'incidenza differente sull'utilizzo della banda: esistono infatti applicazioni più leggere, come le chat, e altre decisamente pesanti, come quelle che richiedono il continuo scambio di file grafici o multimediali. Ogni singolo rallentamento, apparentemente marginale, può avere ripercussioni sulla produttività e generare senso di frustrazione negli utilizzatori. L'analisi preliminare, tesa a identificare necessità e aspettative, deve prendere in considerazione i dispositivi che saranno collegati alla rete wireless: oltre a pc, palmari e stampanti, infatti, potrebbe essere necessario connettere anche telecamere o sistemi d'identificazione. Per tale ragione, nella scelta degli apparati, è indispensabile identificare sempre soluzioni compatibili con i dispositivi e i sistemi operativi impiegati.

Una diagnosi indispensabile

Una volta terminata l'analisi delle esigenze, è necessario affrontare l'"analisi ambientale". Il sopralluogo ha una rilevanza fondamentale per la corretta riuscita dell'intero lavoro. Ogni ambiente, infatti, è differente da un altro e, anche se appare identico "fisicamente", le interferenze elettromagnetiche pre-

senti possono essere completamente diverse. Nel corso di questa analisi è necessario verificare anche lo stato della rete Ethernet, visto che gli access point sono normalmente collegati alla rete cablata, e un comune doppino in rame, tipicamente in Cat. 5, non può superare una lunghezza di 100 m.

La scelta di utilizzare apparati in radiofrequenza, però, non può essere compiuta senza prendere in considerazione le possibili interferenze presenti in ogni ambiente. Alberi, terreno, mattoni, muri in cartongesso e persone, ad esempio, assorbono le microonde, limitando il raggio di copertura teorica. Allo stesso tempo, la presenza di oggetti metallici, recinzioni, finestre a vetri colorati, film plastici, tubi, schermi o bacini d'acqua può contribuire a riflettere e disperdere i segnali trasmessi dai singoli apparati. Non vanno infine trascurate tutte quelle fonti di rumore che sono presenti nell'ambiente e che sovente vengono sottovalutate, quali: forni a microonde, telefoni cordless, webcam wireless, altre reti wireless, antenne di radioamatori... Solo dopo aver individuato e valutato tutte queste possibili interferenze, si può scegliere in

modo corretto la posizione dei singoli access point, il cui numero deve essere adeguato alla copertura richiesta. Gli access point sono collegati fisicamente non solo alla rete dati, ma anche alla rete di alimentazione elettrica; esigenza quest'ultima, alla quale è comunque possibile sopperire grazie all'impiego della tecnologia Power over Ethernet.

Per una rete sicura

La sicurezza costituisce un aspetto importante di qualsiasi rete, soprattutto per un'infrastruttura wireless, visto che l'accesso non può essere fisicamente limitato. Per tale ragione, quando si affronta questo tema, è necessario porsi tre semplici domande:

- che valore hanno le informazioni che risiedono sulla nostra rete?
- quali inconvenienti siamo disposti a sopportare?
- quanto siamo disposti a spendere per proteggere la nostra rete?

Sulla scorta di queste riflessioni è possibile affrontare il tema della sicurezza in modo consapevole. Anche se può apparire incredibile, la maggior parte

delle reti wireless sono installate senza nessuna protezione, in quanto utilizzano i parametri di default che, ovviamente, sono conosciuti da chiunque.

Per tale ragione, prima di implementare qualsiasi misura aggiuntiva di sicurezza, è necessario cambiare le impostazioni di default e abilitare una crittografia appropriata.

Proprio la crittografia è oggi uno dei fattori sui quali i produttori hanno investito maggiormente, mettendo a disposizione una serie di soluzioni identificate da acronimi sconosciuti alla maggior parte delle persone. Volendo concentrarsi solo sulle opzioni di base e, quindi, indispensabile abilitare almeno il Wep (a 64 o 128 bit) o il Wpa-Psk con Tkip o Aes. Affrontare una configurazione di questo tipo, però, può suscitare non pochi dubbi in chi non possiede competenze specifiche. In ogni caso è opportuno ricordare, quantomeno, che più la chiave crittografica è lunga, più è difficile scoprirla. Quindi scegliamo chiavi lunghe, con almeno 20 caratteri e senza parole che esistono sul dizionario. Le chiavi, poi, devono essere scritte su un documento cartaceo e poste in un luogo comu-

Materiali che inducono degradazione del segnale in radiofrequenza		
Barriera RF	Livello di degrado	Esempio
Legno	Basso	Tramezzo d'ufficio
Plastica	Basso	Muri interni
Materiali sintetici	Basso	Tramezzo d'ufficio
Amianto	Basso	Soffitto
Vetro	Basso	Finestra
Acqua	Medio	Legno umido o acquario
Mattoni	Medio	Muri interni ed esterni
Marmo	Medio	Muri interni
Carta	Alto	Grandi cartine o giornali
Cemento armato	Alto	Pavimenti e muri interni
Vetro antiproiettile	Alto	Separé di sicurezza
Metalli	Molto alto	Scrivanie, tramezzi d'ufficio o armadi metallici

nemente inaccessibile alle persone non autorizzate. In ambito aziendale, per una maggiore protezione, sarebbe opportuno implementare un sistema di sicurezza di livello superiore quale il Wpa2/802.11i con autenticazione 802.1x tramite server Radius.

Nella scelta degli apparati da installare è importante ricordare che non tutte le soluzioni, anche se firmate dallo stesso produttore, possiedono le medesime opzioni di sicurezza. È quindi necessario controllare che access point e client dispongano del livello di protezione che intendiamo utilizzare. In questa scelta è importante ricordare che il numero di opzioni da attivare non dipende dalle dimensioni di un'azienda, ma dalla criticità dei dati in transito e dall'evoluzione degli stessi. Così, se in una prima fase potrebbe essere sufficiente (e necessario!) attivare solo le opzioni di base, è difficile conoscere l'evolu-

Access point professionale
USR805453 con supporto
clustering



USRobotics mette a disposizione dei lettori di C&C una wireless checklist, scaricabile dall'indirizzo www.usr.com/it/checklist.

zione di queste necessità. Pertanto, al fine di consentire la possibilità di incrementare nel tempo il livello di sicurezza della rete, gli apparati devono supportare gli stessi standard.

Mai dagli sconosciuti

Al termine di queste analisi, per molti versi "teoriche", giunge il momento di confrontarsi con il mercato "reale", ovvero con le offerte dei singoli produttori. Un compito decisamente complesso. Al momento dell'acquisto è necessario chiedersi: quali caratteristiche sono importanti nella scelta di un access point?

Il primo parametro da valutare è rappresentato, senza dubbio, dall'aderenza agli standard. In commercio, infatti, esistono ancora moltissimi apparati IEEE 802.11b. Uno standard che, viste le caratteristiche di larghezza di banda e velo-

cià, potrebbe essere sufficiente per un impiego domestico, ma che non è in grado di soddisfare le necessità di un utilizzo professionale. Per questo ambito, infatti, è necessario orientarsi verso lo standard 802.11g: basta che la tecnologia utilizzi solo un canale, e non due, per avere una maggior possibilità di ampliare la rete e minimizzare le interferenze con le reti vicine.

Altrettanta attenzione deve essere prestata alla scelta dell'antenna, che generalmente è omnidirezionale, con un guadagno di 2 dBi; passando a un'antenna di 5 dBi si amplia la copertura sul piano orizzontale. Le antenne, inoltre, possono essere rimovibili. Una simile caratteristica permette, in qualunque istante, di sostituirla con una più adatta alla copertura necessaria e magari direzionale. Potrebbe anche essere utile scegliere apparati multifunzione, quindi che non svolgono solo il compito di access point, ma anche di router, firewall, switch, modem Adsl e persino print server. Consolidare più funzioni in un unico apparato può semplificare notevolmente la gestione della rete. Nel caso invece di installazioni che richiedono una serie di access point, esistono apparati con funzioni di clustering per configurare e gestire il gruppo in modo centra-

lizzato. Nella scelta del prodotto hanno un'influenza determinate anche le tecnologie di sicurezza supportate. I vecchi prodotti, e magari apparentemente economici, potrebbero non supportare gli standard più recenti. È pertanto fondamentale verificare che i client wireless e gli access point supportino gli stessi standard; infatti, è sufficiente un solo client inadeguato per declassare la sicurezza dell'intera infrastruttura di comunicazione. È consigliabile quindi acquistare apparati compatibili con Wpa2 e 802.1x.

La tentazione di scegliere la soluzione più economica, senza valutare il fornitore, può essere tra le cause di problemi di comunicazione. La reputazione del produttore, infatti, costituisce comunque una garanzia per l'acquirente. Il tutto senza dimenticare, nell'analisi del rapporto costi/benefici, di prestare attenzione nell'acquisto di prodotti di aziende sconosciute. Può darsi che si risparmi sul costo iniziale, ma con il grosso rischio di difficoltà nel reperire informazioni e supporto tecnico post vendita. In ogni caso, una buona prassi rimane quella di affidarsi ad un rivenditore qualificato e competente in materia.

**Training Manager di USRobotics*

USROBOTICS

www.usr.com/it