

► Di Simone Zanardi



# BANDA LARGA AL SICURO

*Sfruttare la connessione Internet al massimo senza correre rischi? È possibile, configurando a dovere il router broadband. Ecco qualche utile consiglio.*



**Internet e sicurezza:** un binomio ormai inscindibile quando si parla di reti informatiche. In più occasioni abbiamo trattato l'argomento sulle pagine di *PC Professionale*, analizzandolo di volta in volta sotto diversi punti di vista, dal singolo dispositivo agli apparati di rete dedicati, dal mondo mobile a quello dei pacchetti software per Pc. In ambito domestico e Soho (*Small Office Home Office*) è però innegabile che la prima linea di difesa verso potenziali minacce provenienti dal Web sia costituita dal router a banda larga, ovvero dal dispositivo che funge da interfaccia tra la Lan (*Local Area Network*) e il mondo esterno.

Configurare correttamente il router è quindi il primo passo verso una rete sicura. Attualmente la topologia più diffusa nelle reti locali di piccole dimensioni prevede infatti un apparato all-in-one che si occupa non solo dell'accesso diretto alla linea a banda larga (Adsl o fibra), ma anche delle regole di condivisione e della gestione del traffico in transito attraverso un firewall di base integrato. Inoltre, la maggior parte dei router integra un access point Wi-Fi e diviene così il centro della rete senza fili attraverso cui si collegano i dispositivi mobili di ultima generazione come smartphone e tablet.

Nelle prossime pagine vi proponiamo alcuni suggerimenti per configurare al meglio il vostro router broadband

in modo da rendere la rete più sicura. Si tratta di consigli mirati alle reti di piccole dimensioni, dove per l'appunto i dispositivi all-in-one sono più diffusi. All'interno dei network più grandi molte delle funzioni qui citate sono suddivise su apparati diversi e spesso presentano modalità di configurazione completamente differenti.

Una situazione abbastanza diffusa per le reti Soho prevede il router in comodato d'uso da parte del provider. In queste situazioni a volte non tutte le opzioni di configurazione sono a disposizione dell'utente finale; se il vostro fornitore limita eccessivamente le possibilità di intervento sul dispositivo di accesso il nostro consiglio è quello di acquistare un apparato di proprietà; oggi un

buon router dotato di funzionalità base e accesso Wi-Fi integrato è disponibile a poco più di 50 euro, mentre alzando un poco il budget si può ottenere senza sforzo un dispositivo di fascia superiore rispetto alla maggior parte delle unità offerte dai provider.

Il router di proprietà può sostituire quello fornito dal vostro Isp (in questo caso ricordate di acquistare un dispositivo con modem Adsl integrato in caso di accesso su linea telefonica) o essere posto in cascata con l'apparecchio in comodato d'uso, andando a gestire la rete locale senza che si debba compiere alcun intervento sulla macchina dell'Isp. Questa seconda configurazione richiede l'acquisto di un router con interfaccia Wan Ethernet, ovvero *senza* modem.

## LA SICUREZZA PERIFERICA NON BASTA

In questo articolo ci concentriamo sulle funzioni di sicurezza che il router mette a disposizione della rete per proteggere i dispositivi dagli attacchi provenienti dall'esterno, ovvero da Internet o da utenti non autorizzati. Una protezione a 360 gradi non può però prescindere anche da pacchetti di sicurezza installati a bordo di ciascun dispositivo, anche per bloccare le minacce provenienti dall'interno della rete (ad esempio i virus che si propagano attraverso una apparentemente innocua chiavetta Usb). In ambito Windows è fondamentale che su ciascun client sia installato un antivirus, sia attivato il firewall personale e che il sistema operativo sia sempre aggiornato. Il centro operativo di Windows 7 e 8 (disponibile all'interno del pannello di controllo) aiuta l'utente a identificare lo stato di sicurezza del computer, rilevando la presenza di antivirus, firewall e aggiornamenti. Il problema della sicurezza locale riguarda anche i sistemi Android, per i quali si stanno diffondendo sul mercato apposite suite di sicurezza con caratteristiche analoghe a quelle per personal computer.



Il centro operativo di Windows aiuta a identificare potenziali problematiche di protezione sul Pc.

# PROTEGGERE IL ROUTER PER UNA RETE SICURA



**P**rima ancora di capire come un router ben configurato possa proteggere la rete locale di casa o del piccolo ufficio, è importante accertare che il router stesso non sia fonte di vulnerabilità. Essendo infatti questo dispositivo il centro della rete, un problema di sicurezza si ripercuoterebbe automaticamente su tutti i dispositivi collegati sulla Lan. Tra le pratiche da mettere in campo immediatamente vi è la più banale, ma spesso sottovalutata: cambiare le credenziali di accesso all'interfaccia di amministrazione del router. Molti utenti si concentrano su aspetti di sicurezza avanzati per poi lasciare invariati nome utente e password impostati di default dal produttore. Questa scelta lascia ai potenziali malintenzionati una facile strada di accesso al router dal momento che spesso i parametri in questione sono facilissimi da indovinare (*admin/admin*, *admin/password* e simili) o possono facilmente essere ricavati scaricando i manuali d'uso dell'apparato.

Anche nel caso in cui il produttore imposti nome utente e password con valori pseudo-casuali al momento della configurazione di fabbrica, è sempre opportuno procedere alla modifica personalizzata, nel caso in cui l'hacker scopra l'algoritmo di generazione delle password. Le regole per la creazione di una password sicura esulano dagli scopi di questo articolo, ma non è mai troppo banale ricordare come i nomi propri o dei propri cari, le date di nascita o le password troppo corte siano tra le scelte meno opportune.

**L'amministrazione da remoto** è una funzione che molti router mettono a disposizione degli utenti per consentire l'accesso al dispositivo attraverso Internet quando non ci si trova sul posto. Può essere molto utile in ambito aziendale per fornire assistenza a distanza, ma costituisce una potenziale porta aperta verso gli attacchi di malintenzionati e va

per questo configurata con attenzione. Una buona norma è ad esempio quella di cambiare la porta di accesso al pannello di controllo: indicando una porta differente rispetto alle classiche 80 o 8080 si fornisce un minimo di mascheratura per l'accesso da remoto. Per contattare il router su una porta differente (ad esempio 1234) sarà sufficiente indicare nel browser l'indirizzo IP pubblico seguito dai due punti e dalla porta scelta (ad esempio <http://80.76.128.36:1234>). Per cifrare le comunicazioni durante il controllo remoto è bene abilitare, se disponibile, l'accesso tramite protocollo sicuro Https.

Alcuni router permettono poi di indicare uno o più indirizzi IP remoti ai quali concedere l'accesso a distanza; le richieste provenienti da indirizzi differenti sono bloccate.

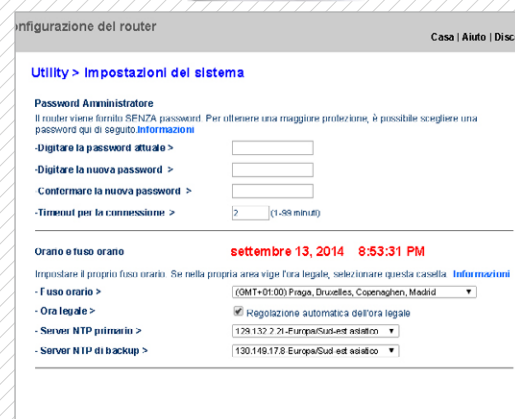
## Sessione amministrazione

Se potete, impostate sessioni a tempo: il logout automatico aumenta la sicurezza

L'aggiornamento del firmware è un aspetto a cui prestare particolare attenzione: come un normale computer, anche il router è dotato di un proprio "sistema operativo", spesso basato su core Linux. I produttori rilasciano costanti aggiornamenti per i modelli sul mercato, sia per aggiungere nuove funzioni sia, e soprattutto in questo contesto, per riparare eventuali falle che possono mettere a rischio la stabilità e la sicurezza del sistema.

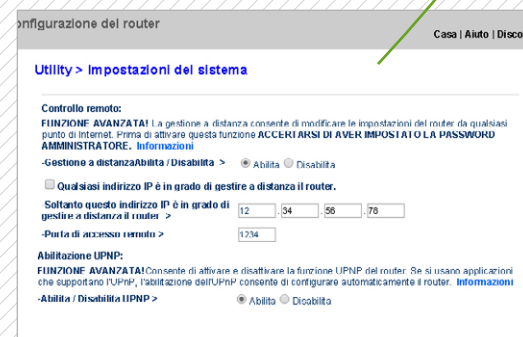
I router più avanzati dispongono di un meccanismo di controllo automatico degli aggiornamenti: a intervalli periodici interrogano i server della casa madre e verificano la disponibilità di update, avvisando poi l'utente che può quindi scaricare la nuova versione e installarla.

Se il vostro router non dispone di questa funzione è invece importante controllare personalmente sul sito di supporto del produttore eventuali rilasci. Un check mensile può essere sufficiente.

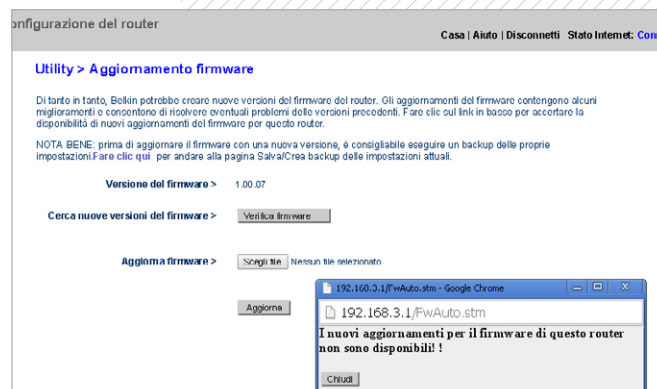


**Cambiare la password di amministrazione di default** è un passaggio banale ma spesso dimenticato.

Il **controllo da remoto** è uno strumento utile, ma va configurato con attenzione.



Se il router non lo fa automaticamente, controllate gli **aggiornamenti del firmware**.





# IL FIREWALL

## protezione contro gli attacchi



**T**utti i moderni modem/router a banda larga integrano un firewall, ovvero un modulo che si occupa di filtrare il traffico in transito dall'esterno prevenendo attacchi e accessi non autorizzati alla rete locale. In realtà i firewall a bordo dei router possono assumere caratteristiche molto differenti in base ai servizi offerti e a quelli per cui il produttore decide di lasciare il controllo all'utente.

Configurare un firewall a basso livello può essere infatti impresa non semplice per i non addetti ai lavori e l'impostazione non corretta di alcuni parametri rischia di compromettere la connettività a Internet inibendo anche le trasmissioni lecite. Il giusto compromesso tra semplicità di utilizzo, versatilità dello strumento e adeguato livello di protezione non è semplice da offrire: di seguito riportiamo alcune funzioni che tipicamente trovano spazio sui router consumer e Soho.

**Una prima protezione dall'esterno** è fornita non dal firewall in sé, quanto dai meccanismi di Nat (*Network Address Translation*, traduzione degli indirizzi di rete), implementati in

tutti i router e, nei modelli Soho in particolare, del tutto trasparenti per l'utente finale.

Per poter accedere a Internet, un qualsiasi dispositivo necessita di un indirizzo IP pubblico tramite il quale essere rintracciato sulla rete. Il protocollo IP permette di definire un numero limitato di indirizzi univoci e per questo gli Internet Service Provider forniscono ai propri abbonati un numero limitato di indirizzi IP (per gli accessi Soho tipicamente un solo indirizzo). La Nat si occupa di trasformare i pacchetti IP in transito sul router "cambiando" l'indirizzo IP di mittente e destinatario, anche in modalità *uno-a-molti*.

**Questo sistema permette** ad esempio a tutti i dispositivi della Lan (ciascuno dotato di un IP locale) di condividere l'unico indirizzo IP pubblico messo a disposizione dal provider. In senso contrario questa configurazione funge da protezione implicita, dal momento che un pacchetto proveniente dall'esterno non ha modo, se non sotto indicazione del router stesso, di raggiungere un dispositivo locale specifico, conoscendo appunto solo l'indirizzo IP pubblico.

**Oltre al Nat**, la maggior parte dei router in commercio è fornita con un firewall di base abilitato di default. Questo consente di bloccare attacchi classici di tipo Dos (*Denial Of Service*) come i *Syn-Flood* e i *Ping Of Death*.

Tutti questi attacchi non puntano a penetrare nella rete locale per carpire informazioni o dati, ma hanno il semplice obiettivo di mandare in crash i sistemi inviando pacchetti IP mal formati o in quantità eccessiva. Disattivare il firewall del router è operazione altamente sconsigliata.

In caso di assoluta necessità è però possibile definire sulla rete locale una Dmz (*DeMilitarized Zone*, zona demilitarizzata), ovvero un'area della rete locale che di fatto vive all'esterno del firewall ed è quindi totalmente esposta verso l'esterno. La Dmz è definita sulla base degli indirizzi IP locali dei dispositivi che devono essere esposti e rappresenta un sistema rapido per creare ad esempio dei server pubblici.

Va però utilizzata solo in casi di estrema necessità, badando a fornire gli apparati esposti di opportuni protezioni locali (antivirus, firewall personali). Per specifiche necessità di apertura delle comunicazioni dall'esterno esistono comunque strumenti ad hoc come il *port forwarding* o i *server virtuali*, che analizzeremo tra poco.

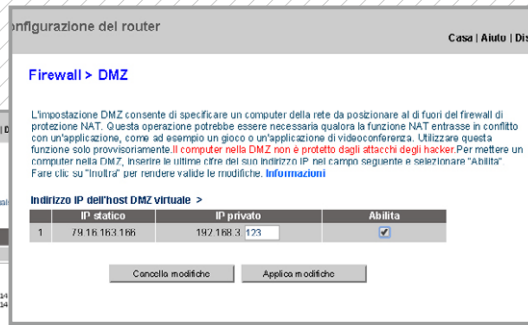
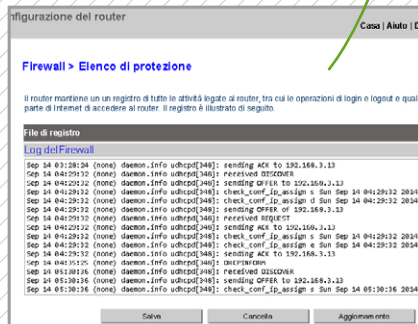
### Denial Of Service

Attacco che punta a rendere un dispositivo o risorsa di rete inutilizzabile causa sovraccarico o errore provocato

**Il registro di sistema** può essere un valido ausilio per identificare attacchi o tentativi di accesso non autorizzati.



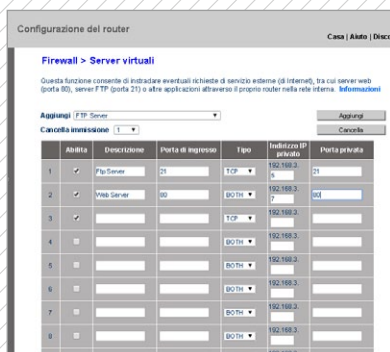
**Il firewall di base** è abilitato di default su quasi tutti i router. Non disattivatelo se non in casi di estrema necessità.



**Definire una zona demilitarizzata** è un metodo semplice per creare un server pubblico, che però non sarà protetto dal firewall.

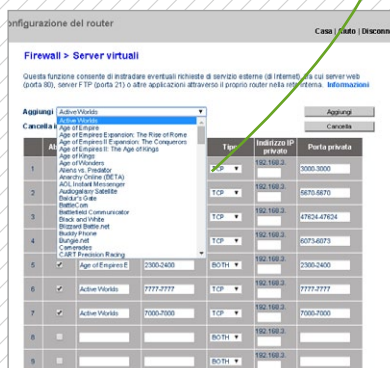
# OLTRE IL FIREWALL

## gestire le comunicazioni



Le regole di **port forwarding** o **virtual server** permettono di abilitare richieste legittime provenienti dall'esterno verso server locali.

Molti router offrono un set di **regole precompilate** per alcuni servizi o giochi online noti.



Alcuni portali online consentono di verificare la robustezza del **protocollo Upnp** implementato dal router.

**S**e il compito principale del firewall è quello di bloccare gli accessi non autorizzati dall'esterno verso la rete locale, è indispensabile che il router offra meccanismi adeguati per aprire le comunicazioni legittime in ingresso. Si pensi ad esempio a un server locale che debba offrire uno o più servizi pubblici o a una particolare applicazione che necessiti di una comunicazione bidirezionale evoluta con l'esterno.

Abbiamo già parlato della possibilità di istituire una zona demilitarizzata, che però è uno strumento spesso troppo rischioso e, soprattutto, scarsamente personalizzabile. Un'alternativa certamente più efficace è costituita dai servizi di **port forwarding** e **virtual server**. Sebbene queste due funzioni non siano tecnicamente identiche, possono essere utilizzate con il medesimo scopo.

Alla base del loro funzionamento vi è il sistema di trasmissione adottato dai protocolli Tcp/IP. I servizi di comunicazione sono infatti identificati dalla **porta** sulla quale il server attende le comunicazioni in ingresso. La porta, insieme all'indirizzo IP del server, identifica quindi il servizio attivo. Con una buona analogia si può pensare alla porta come al numero interno di un condominio: per identificare un appartamento si deve conoscere l'indirizzo civico dell'edificio (indirizzo IP del dispositivo

informatico) e il suo interno (numero di porta del servizio attivo).

Il sistema delle porte di comunicazione può essere utilizzato dalle funzioni **virtual server** e **port forwarding** per consentire a più dispositivi della Lan di offrire i propri servizi all'esterno. Essenzialmente l'amministratore del router può definire una serie di regole che fanno corrispondere alle richieste esterne indirizzate a una determinata porta un indirizzo IP e una porta interna della Lan. Ipotezziamo ad esempio che l'amministratore di una rete con indirizzo IP pubblico

80.76.128.36 voglia installare un server Ftp su un computer con indirizzo locale 192.168.3.5. Il protocollo Ftp è generalmente impostato per ascoltare sulla porta 21. L'amministratore non dovrà far altro che creare una regola di inoltro che indirizzi tutte le richieste esterne alla porta 21 verso l'indirizzo 192.168.3.5. Per accedere dall'esterno al server sarà sufficiente indicare al client l'indirizzo 80.76.128.36 e la porta 21.

In un secondo tempo sulla rete viene installato un server Web in ascolto sulla porta 80 del personal computer locale 192.168.3.7. Per abilitare questa

comunicazione basterà creare una nuova regola di inoltro da 80.76.128.36:80 a 129.168.3.7:80. Non è necessario che le porte esterna e interna corrispondano (in questo modo si possono ad esempio installare due server Ftp distinti in ascolto su porte differenti).

Una versione evoluta del **port forwarding** è il **port triggering**: in questo caso il router inoltra dinamicamente il traffico in ingresso su determinate porte verso i computer della Lan che stanno utilizzando specifiche applicazioni. Se ad esempio un computer sta

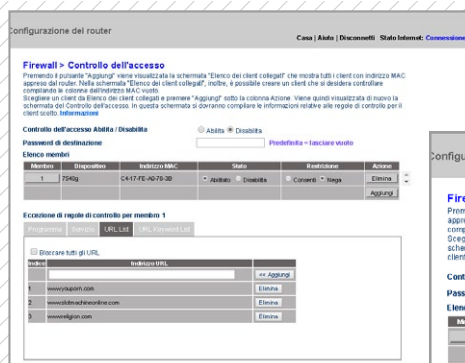
eseguendo un gioco online operante in uscita sulla porta 123 e che deve ricevere comunicazioni sulla 456, il router inoltrerà le richieste alla porta 456 verso tale computer (solo quando il suddetto software è in esecuzione).

Un meccanismo ancor più automatizzato di apertura delle porte è l'**Upnp** (Universal Plug&Play): se abilitato sul router, permette a determinate applicazioni locali di aprire di propria iniziativa delle porte di comunicazione. L'**Upnp** è potenziale fonte di vulnerabilità: prima di abilitarlo sul vostro router, verificate la robustezza dell'implementazione su siti come <http://upnp-check.rapid7.com>.

**Well Known Ports**  
Alcuni servizi standard come l'Ftp o i server Web e e-mail sfruttano porte ormai storicamente definite

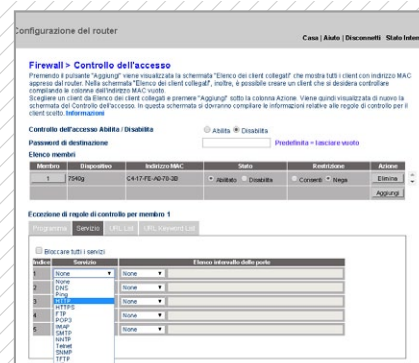


# CONTROLLARE gli accessi Internet dalla Lan



Le regole di filtraggio degli indirizzi Url permettono di bloccare l'accesso a determinati siti Internet.

Le policy di accesso possono essere calendarizzate per bloccare la navigazione solo a determinati orari.



Molti router permettono di definire regole di accesso anche sulla base delle porte di comunicazione Tcp/IP.

Un buon router non è solo in grado di proteggere la rete locale dagli attacchi informatici provenienti da Internet, ma anche di controllare gli accessi al Web da parte degli utenti locali. Questo tipo di controllo può essere utile, se non fondamentale, sia in ambito domestico (per gestire la navigazione Internet dei bambini da parte dei genitori) sia in contesti professionali (per bloccare l'accesso a siti e servizi online che possono abbattere la produttività del personale).

I router Soho offrono numerosi meccanismi per il controllo degli accessi in grado di operare su indirizzi locali e remoti, orari di connessione, Url e parole chiave, oltre che di interfacciarsi con servizi esterni per un controllo dinamico dei contenuti a rischio. Il nome con cui vengono identificate queste funzioni variano di modello in modello; generalmente sono *Controllo degli accessi*, *Parental control* o *Content Filtering*, tra gli altri.

Quale che sia il nome attribuito dal produttore del vostro router, il processo di configurazione delle regole di accesso segue regole precise: in primo luogo è necessario identificare i dispositivi che chiedono l'accesso a Internet. Per farlo, il router può ricorrere essenzialmente al Mac address o all'indirizzo IP. Il primo è il codice identificativo che

contrassegna ogni interfaccia hardware che si collega a una rete. È generalmente indicato con la notazione esadecimale del tipo 01:23:45:67:89:AB ed è unico per ogni dispositivo, oltre a non essere modificabile (perlomeno in modo semplice e intuitivo). In alternativa, il dispositivo è identificabile tramite l'indirizzo IP, che però spesso nelle reti locali Soho è assegnato dinamicamente dal router stesso o è modificabile dagli utenti senza eccessiva difficoltà; per questo è meno adatto agli scopi di filtraggio. Molti router offrono all'amministratore una lista di client collegati e permettono di scegliere direttamente da questo elenco il dispositivo a cui si vogliono applicare le regole di accesso.

Una volta identificato il device che si vuole gestire, si devono indicare le risorse a cui si vuole consentire o negare l'accesso. Un primo metodo per farlo è basato sulle porte di comunicazione di cui abbiamo già parlato nelle pagine precedenti: se ad esempio non si vuole fornire accesso al protocollo Ftp da una determinata macchina, basterà definire un blocco alla porta 21 sulla relativa regola di accesso. In ambito Web è poi possibile definire un elenco di

siti verso cui non è consentito l'accesso, indicando semplicemente il relativo Url (indirizzo). In alternativa all'indirizzo preciso alcuni router permettono di indicare una serie di parole chiave che si trovino all'interno dell'indirizzo medesimo. Questi due metodi sono generalmente definiti di *content filtering statico*.

Un approccio più versatile è il *content filtering dinamico*, che sta via via prendendo piede anche sui router

Soho. In questo caso l'amministratore non si limita a indicare una serie di indirizzi e parole chiave, ma può selezionare da un elenco esaustivo una serie di argomenti che devono essere evitati. Il router si collega poi a un servizio esterno dove un

apposita piattaforma contiene un elenco sempre aggiornato di siti e dei relativi argomenti trattati. Se si dipende l'accesso ai siti sportivi, si bloccheranno automaticamente non solo i siti come *www.gazzetta.it*, ma anche i nuovi portali che trattano l'argomento e che potrebbero vedere la luce in futuro. I siti di *content filtering dinamico* offrono numerose categorie tra cui sesso, religioni, guerre, sport, gioco online, e molti altri.

## Navigazione anonima

Permette di navigare senza conservare dati sul Pc. Non elude le policy di accesso del router



# WI-FI SICURO

## contro gli accessi non autorizzati alla rete



In ambito consumer e Soho il router svolge tipicamente anche il ruolo di access point Wi-Fi ed è quindi al suo interno che vanno configurate le politiche di accesso alla rete wireless. Per garantire la massima sicurezza al network evitando l'accesso da parte di client non autorizzati è innanzitutto indispensabile selezionare il protocollo di protezione adeguato. Oggigiorno la scelta è obbligata: Wpa2 con algoritmo crittografico Aes (*Advanced Encryption Standard*); supportato ormai dalla totalità dei router e dei dispositivi client, il Wpa di seconda generazione garantisce infatti un livello di protezione nettamente superiore rispetto al Wpa originale e all'ormai totalmente insicuro Wep. Per quanto riguarda l'autenticazione degli utenti, il Wpa2 può essere configurato in modo da appoggiarsi a un server esterno che gestisca gli account singoli (attraverso i protocolli 802.1x/Radius) o attraverso un più semplice meccanismo a Psk (*Pre-Shared Key*, chiave precondivisa). Quest'ultima opzione, effettivamente più comoda da utilizzare nelle piccole reti, richiede però particolare attenzione nella scelta

della password che deve essere sufficientemente complessa per evitare attacchi di tipo *brute force*. Inoltre, è sempre bene cambiare la password di sistema a intervalli periodici. Molti router supportano procedure Wps (*Wireless Protected Setup*) per semplificare la configurazione del canale Wi-Fi sicuro; si tratta di sistemi di sincronizzazione che prevedono la pressione contestuale di pulsanti (hardware o software) su client e router, o l'inserimento di codici provvisori per l'inizializzazione del canale. Quale che sia il metodo di configurazione scelto, il livello di protezione dipende comunque dal protocollo di sicurezza adottato.

**Il limite principale** dei protocolli di autenticazione basati su password condivisa è che se questa viene in qualche modo esposta al personale non autorizzato, è necessario cambiarla e quindi riconfigurare tutti i client. Per evitare questo tipo di problemi, molti router

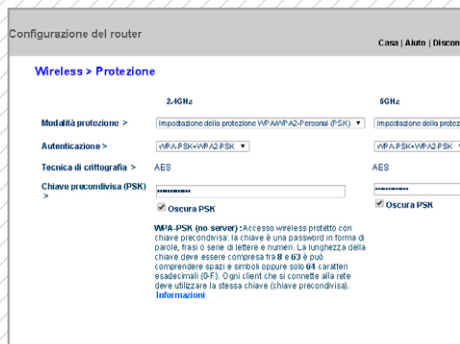
offrono la possibilità di definire un accesso guest; essenzialmente si crea un secondo access point virtuale al quale vengono applicati criteri di autenticazione e protezione dedicati. L'accesso guest, inoltre, consente tipicamente la navigazione su Internet, ma non il collegamento ad altri client e server sulla rete locale. Se il vostro router lo consente, potete inoltre abilitare l'accesso guest con autenticazione di tipo hot spot. In questo caso l'utente che inizia una sessione di navigazione viene accolto dal browser con una schermata di login all'interno del quale inserisce le credenziali fornite dall'amministratore. Questi dati di autenticazione sono personali e una volta terminata la sessione possono essere disabilitati dall'amministratore senza che questo influenzi altri account, né tantomeno l'accesso primario non guest.

### Client isolation

Opzione offerta da molti router Wi-Fi, inibisce la comunicazione diretta tra client, limitando l'accesso alla sola Internet

Un'ulteriore precauzione per rendere ancora più sicura la connessione Wi-Fi alla rete consiste nella creazione di una Acl (*Access Control List*) basata sugli indirizzi Mac dei dispositivi. In questo modo solo i device presenti sulla lista hanno diritto di collegamento. Si tratta di un sistema molto efficace per evitare accessi non autorizzati da parte di utenti comuni, anche se per i più esperti non è difficile presentarsi sulla rete con un Mac address fittizio. Per questo le liste Acl vanno utilizzate comunque in abbinamento a un robusto sistema di autenticazione e codifica.

La sicurezza della rete Wi-Fi passa innanzitutto dalla scelta del **protocollo di protezione** più avanzato, ovvero il Wpa2.



I router che supportano l'**accesso guest** permettono di creare un profilo alternativo per consentire il collegamento da parte di client ospiti.

Un **filtro sugli indirizzi Mac** è un buon coadiuvante per aumentare la sicurezza, ma non è infallibile contro gli hacker più esperti.

