BELKIN

Modem ADSL con Router Wireless G

Progettato per soddisfare le specifiche ADSL2+

Condivisione

Per collegare in rete diversi computer e condividere uno stesso accesso ad Internet in ADSL

802.11g

54 Mbps

2.4GHz • Wireless

Manuale utente

F5D7632it4v3000

Indice

Grazie per aver scelto il Modem ADSL con Router Wireless G Belkin (il router). Con questo nuovo router sarà possibile condividere in pochi minuti una stessa connessione ad Internet e collegare in rete diversi computer. Di seguito è riportato un elenco delle caratteristiche che fanno di questo nuovo router una soluzione ideale per la creazione di una rete in casa o in un piccolo ufficio. Vi invitiamo a leggere con attenzione questo manuale, in particolare l'Allegato B intitolato "Considerazioni importanti per il posizionamento e la configurazione".

Caratteristiche del prodotto

Compatibile sia con computer PC che Mac®

Il router supporta diversi ambienti di rete, tra cui Mac OS® 8.x, 9.x, X v10.x, AppleTalk®, Linux®, Windows® 95, 98SE, Me, NT®, 2000, XP e altri. Il suo utilizzo richiede la disponibilità di un browser Internet e di un adattatore di rete in grado di supportare la modalità TCP/IP (la lingua standard di Internet).

Indicazioni LED sul pannello frontale

I LED illuminati sul lato anteriore del router indicano quali sono le funzioni in corso e consentono, con un semplice colpo d'occhio, di conoscere lo stato di collegamento del router ad Internet. Questa funzione elimina la necessità di eseguire altre procedure avanzate di monitoraggio stato e software.

Interfaccia utente basata sul web

Tutte le funzioni avanzate del router possono essere impostate facilmente tramite il browser web, senza dover installare altro software nel computer. Non ci sono dischetti da installare o da conservare e le funzioni di installazione possono essere modificate ed eseguite in modo rapido e semplice da qualsiasi computer collegato in rete.

Switch integrato a 4 porte 10/100

Questo Router dispone di uno switch di rete integrato a 4 porte, per consentire ai vostri computer in rete cablata di condividere stampanti, dati e file MP3, foto digitali e altro ancora. Lo switch prevede una funzione di rilevamento automatico, che consente di regolare la velocità dei dispositivi collegati. Inoltre, trasferisce dati fra i computer ed Internet contemporaneamente, senza interruzioni e senza consumare risorse.

Access Point Wireless 802.11g integrato
La tecnologia 802,11g è una nuova ed entusiasmante tecnologia wireless che consente la trasmissione dei dati a 54Mbps, quasi cinque volte più velocemente dell'opzione 802.11b.

Dynamic Host Configuration Protocol (DHCP) integrato
Il Dynamic Host Configuration Protocol (DHCP) integrato nella scheda semplifica al massimo la connessione alla rete. Il server DHCP assegna automaticamente gli indirizzi IP a ciascun computer, eliminando l'esigenza di qualsiasi complicata predisposizione della rete.

Condivisione dell'indirizzo IP NAT
Il router implementa il servizio Network Address Translation (NAT) per condividere l'unico indirizzo IP assegnato all'utente dal Provider Internet, consentendo di risparmiare il costo di eventuali indirizzi IP supplementari per il proprio account di servizio Internet.

Protezione Firewall SPI
Il router è dotato di una protezione firewall per proteggere la rete da una vasta gamma di attacchi comuni degli hacker, tra cui IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect e fragment flooding.

Filtraggio degli indirizzi MAC
Per una maggiore sicurezza, è possibile creare un elenco di indirizzi MAC (identificatori unici client) cui consentire l'accesso alla propria rete. Ad ogni computer corrisponde un indirizzo MAC specifico, è sufficiente inserire questi indirizzi MAC in un elenco tramite l'interfaccia utente basata sul Web e controllare in questo modo l'accesso alla rete.

Compatibilità con la tecnologia Universal Plug-and-Play (UPnP)
Quella Universal Plug-and-Play (UPnP) è una tecnologia in grado di offrire un funzionamento diretto delle opzioni di trasmissione di messaggi vocali, video, giochi ed altre applicazioni conformi agli standard UPnP.

Supporto del servizio VPN Pass-Through
Se si desidera collegarsi alla propria rete in ufficio da casa utilizzando una connessione VPN, il router consente al computer dotato del servizio VPN di passare attraverso il router ed arrivare alla rete dell'ufficio.

I vantaggi di una rete domestica

Seguendo le nostre semplici istruzioni di configurazione è possibile utilizzare la propria rete domestica Belkin per:

- Condividere un'unica connessione ad Internet ad alta velocità tra tutti i computer di casa
- Condividere risorse, quali file e dischi fissi, tra tutti i computer di casa
- Condividere una sola stampante tra tutta la famiglia
- Condividere documenti, musica, video e fotografie digitali
- Memorizzare, recuperare e copiare i file da un computer all'altro
- Disputare partite online, controllare la posta elettronica e chattare da diversi computer contemporaneamente

I vantaggi di una rete wireless Belkin

Mobilità - la "stanza per il computer" non è più necessaria: da oggi si può lavorare da un portatile o da un computer desktop collegato in rete da un qualsiasi punto all'interno della propria copertura wireless

Facilità di installazione - il programma di impostazione guidata Belkin facilita la procedura di configurazione

Versatilità - si ha la possibilità di accedere a stampanti, computer e altri dispositivi di rete da qualsiasi punto all'interno della propria abitazione

Facilità di espansione - la vasta gamma dei prodotti di rete Belkin permette
di espandere la propria rete, aggiungendo altri dispositivi tra i quali stampanti e
console di gioco

Niente cavi - non è più necessario spendere soldi e perdere tempo per cablare la propria abitazione o l'ufficio per creare una connessione Ethernet

Accettazione incondizionata di altre marche - si ha la possibilità di scegliere tra una vasta gamma di prodotti di rete interoperabili

Materiale necessario

Contenuto della confezione

- Modem ADSL con Router Wireless G
- Cavo telefonico RJ11 - Grigio
- Cavo di rete RJ45 Ethernet - Giallo
- Cavo USB 1.0 — Blu
- Microfiltro ADSL*
- Adattatore di corrente
- CD con Manuale utente

  *il microfiltro ADSL varia di Paese in Paese. Se non fosse compreso nella fornitura, sarà necessario acquistarne uno.

Requisiti del sistema

- Un servizio ADSL attivo con una presa telefonica a muro per collegare il router
- Almeno un computer con una scheda di interfaccia di rete (NIC) ed un browser Internet installato e configurato correttamente
- Protocollo di rete TCP/IP installato su ogni computer e collegato al router
- Nessun altro server DHCP sulla propria rete locale che assegni gli indirizzi IP ai computer e agli altri dispositivi

Impostazioni di connessione a Internet

Prima di configurare il router G wireless con modem ADSL è necessario richiedere le seguenti informazioni al proprio ISP .

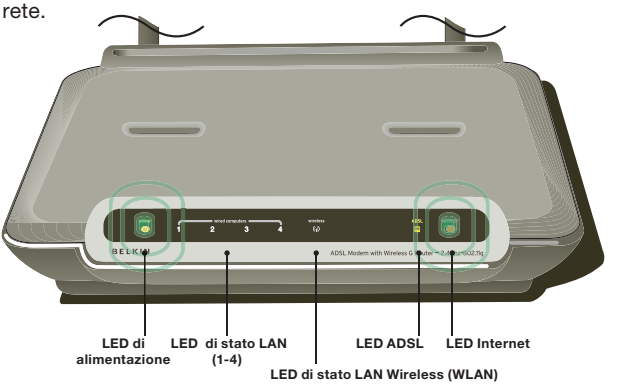
- Protocollo di connessione a Internet: _____ (PPPoE, PPPoA, IP dinamico, IP statico)
- Metodo Multiplexing o incapsulamento: _____ (LLC oppure VC MUX)
- Circuito virtuale: VPI (Virtual Path Identifier) _____ (un numero compreso tra 0 e 255)
- VCI (Virtual Channel Identifier) _____ (un numero compreso tra 1 e 65535)
- Per utenti PPPoE e PPPoA: nome utente _____ e password _____ dell'account ADSL
- Per gli utenti IP statici: Indirizzo IP ___ . ___ . ___ Subnet Mask ___ . ___ . ___ Server Gateway predefinito ___ . ___ . ___ .
- Indirizzo IP del Domain Name Server ___ . ___ . ___ . ___ (se assegnato dal proprio ISP)

Nota: per conoscere alcuni dei parametri di impostazione Internet DSL comuni, vedere l'Appendice C di questo Manuale Utente. Nel dubbio, contattare il proprio ISP.

Conoscere il router

Il router è stato progettato per essere posizionato sulla scrivania. Tutti i cavi escono dal retro del router, consentendo una migliore organizzazione e utilizzabilità. Gli indicatori LED sono facilmente visibili sulla parte anteriore del router e mantengono informati sull'attività e sullo stato della rete.

Pannello anteriore
L'illustrazione rappresenta il pannello anteriore del router.



1. LED alimentazione
L'accensione o il riavvio del router richiedono un breve intervallo di attesa. Una volta riavviato completamente il router, nel LED che segnala lo stato di alimentazione si accende una spia VERDE, che sta ad indicare che il router è pronto all'uso.

Alimentazione ⏻	**SPENTO**	Spegnimento
	Verde	Accensione
	Rossa	Il router non si è attivato

2. LED di stato LAN
Questi LED di indicazione dello stato LAN sono contrassegnati con i numeri da 1 a 4 e corrispondono alle porte numerate previste sul retro del router. Quando un computer viene collegato correttamente ad una delle porte LAN sul retro del router, si accendono i LED. Una spia VERDE fissa indica la presenza di un computer o di un dispositivo di rete collegato. Quando l'informazione viene trasmessa attraverso la porta, il LED lampeggia rapidamente. La spia ARANCIONE indica la presenza di una connessione 10Base-T.

Rete locale (LAN) 1–4	**Spenta**	Nessun dispositivo collegato
	Arancione	Il collegamento alla rete Ethernet è attivo e il dispositivo 10Base-T è collegato
	Arancione lampeggiante	Il dispositivo 10Base-T sta ricevendo o trasmettendo i dati
	Verde	Il collegamento alla rete Ethernet è attivo e il dispositivo 100Base-T è collegato
	Verde lampeggiante	Il dispositivo 100Base-T sta ricevendo o trasmettendo i dati

3. LED di segnalazione stato WLAN

Nel LED di segnalazione stato WLAN quando la funzione LAN wireless viene attivata si accende una spia VERDE fissa. Se lampeggia, significa che il router sta trasmettendo o ricevendo i dati in modalità wireless.

WLAN	**Spenta**	La connessione WLAN non è attiva
	Verde	La connessione WLAN è attiva
	Verde lampeggiante	Durante la trasmissione o la ricezione dei dati

4. LED ADSL

Nel LED ADSL durante la fase di negoziazione con l'ISP si accende una spia VERDE lampeggiante. Rimane VERDE una volta che il router è correttamente collegato al proprio servizio ADSL.

ADSL	**Spenta**	Assenza di connessione ADSL
	Verde lampeggiante	Negoziazione della connessione in corso
	Verde	Collegamento ADSL attivo

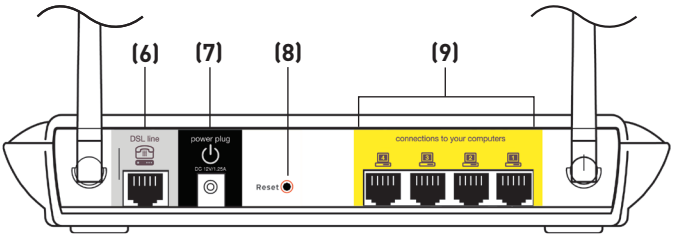
5. LED Internet

Il LED Internet serve ad indicare se il router è collegato ad Internet. Se il LED è SPENTO, significa che il router NON è collegato ad Internet. Se il LED è VERDE e acceso in maniera fissa, significa che il router è collegato ad Internet. Se il LED lampeggia, significa che il router sta trasmettendo o ricevendo dati da Internet.

Internet	**Spenta**	Assenza di collegamento a Internet
	Verde	Collegamento a Internet in corso
	Verde lampeggiante	Durante la trasmissione o la ricezione dei dati
	Rossa	Mancata ricezione dell'IP

Pannello posteriore

La seguente illustrazione rappresenta il pannello posteriore del router.



6. Linea ADSL

Questa porta consente di impostare il collegamento con la propria linea ADSL. La linea ADSL deve essere collegata a questa porta.

7. Spina di alimentazione

L'alimentatore da 15V CC fornito deve essere collegato a questa presa. L'utilizzo di un tipo di adattatore di alimentazione sbagliato può danneggiare il router.

8. Pulsante di reset

Il pulsante di reset viene utilizzato in alcuni casi rari, se il router dovesse funzionare in maniera inadeguata. Resettando il router, si ripristina la normale modalità di funzionamento del router pur mantenendo le impostazioni programmate. Il pulsante di reset consente anche di ripristinare le impostazioni predefinite. L'opzione di ripristino si può utilizzare ad esempio nel caso sia stata dimenticata la password cliente.

a. Reset del router

Premere per un secondo il pulsante di Reset, quindi rilasciarlo. Quando la spia "Power/Ready" (alimentazione/pronto) è di nuovo fissa, significa che l'operazione di reset è stata completata.

b. Ripristino delle impostazioni del produttore

Premere e tenere premuto il pulsante di reset per cinque secondi, quindi lasciarlo. Quando la spia alimentazione/pronto è di nuovo fissa, significa che l'operazione di ripristino è stata completata.

9. Porte Ethernet

Le porte Ethernet sono RJ45, 10/100 auto-negoziazione. Queste porte sono contrassegnate con i numeri da 1 a 4 e corrispondono ai LED numerati presenti sulla parte anteriore del router. I propri computer abilitati alla connessione in rete e tutti gli altri dispositivi di rete vanno collegati ad una di queste porte.

Collocazione del router

Minore è la distanza tra il computer e il router o l'access point e maggiore è l'intensità della connessione wireless. La copertura tipica per i dispositivi wireless in un ambiente chiuso è compresa tra i 30 e i 60 metri. Analogamente, la qualità della connessione e delle prestazioni wireless sarà leggermente inferiore aumentando la distanza tra i dispositivi collegati al router. Tuttavia, questa condizione potrebbe passare inosservata. All'aumentare della distanza dal router, la velocità della connessione potrebbe diminuire. Apparecchiature in metallo, ostacoli e muri rientrano tra i fattori che indeboliscono i segnali, invadendo il raggio d'azione delle onde radio della rete. Vedere l'"Allegato B: Considerazioni importanti per il posizionamento e la configurazione" in questo Manuale per ulteriori informazioni in merito.

Per verificare se eventuali problemi di prestazione della rete siano dovuti alla presenza di ostacoli nell'area di copertura, provare a posizionare il computer ad una distanza compresa tra 1,5 m e 3 m dal router. Se i problemi persistono anche ad una distanza inferiore, consultare la sezione dedicata alla rilevazione e risoluzione delle anomalie.

Collegamento dei computer

1. Staccare i computer e l'attrezzatura di rete.
2. Collegare il proprio computer ad una delle porte RJ45 GIALLE sul retro del router contrassegnate con "connections to your computers" utilizzando un cavo di rete Ethernet (un cavo di rete Ethernet è fornito).

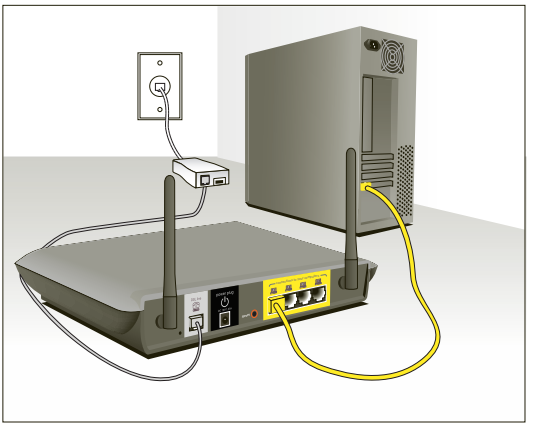
Collegamento della linea ADSL

Il collegamento per il router alla linea ADSL varia in base al Paese e alla regione. Generalmente prevede un microfiltro o un microfiltro con splitter integrato per l'utilizzo contemporaneo del servizio ADSL e del servizio telefonico sulla stessa linea. Leggere con attenzione i seguenti passaggi e scegliere il metodo più adatto.

1. Se il servizio telefonico e il servizio ADSL non sono sulla stessa linea telefonica, sono necessari alcuni microfiltri ADSL per ogni telefono e altro apparecchio, quale la segreteria telefonica, il fax e il display di visualizzazione dell'ID del chiamante. Per separare le linee telefoniche ed il router si possono utilizzare altri splitter supplementari.

   Nota: non collegare il microfiltro ADSL tra la presa a muro ed il router, in quanto questo accorgimento impedirebbe al servizio ADSL di raggiungere il modem.

2. Se il servizio telefonico e il servizio ADSL non sono sulla stessa linea telefonica e si sta utilizzando un microfiltro ADSL con splitter integrato, collegare lo splitter alla presa a muro del telefono che eroga il servizio ADSL. Quindi, collegare il cavo telefonico dalla porta RJ11 del microfiltro ADSL generalmente contrassegnata con "DSL" alla porta RJ11 grigia contrassegnata con "DSL line" sul retro del router. Collegare il dispositivo telefonico ad un'altra porta dello splitter ADSL generalmente contrassegnata con "Phone". Per aggiungere un altro telefono e dispositivo sulla stessa linea è necessario prevedere un microfiltro ADSL supplementare.



Nota: un cavo telefonico RJ11 è fornito. Inserendo il connettore RJ11, assicurarsi che la levetta posta sul connettore scatti in posizione per garantire il corretto inserimento.

3. Se si dispone di una linea di servizio telefonico ADSL dedicata con una presa a muro RJ11, è sufficiente collegare un cavo telefonico dalla presa a muro alla porta grigia RJ11 etichettata “DSL line” sul retro del router.

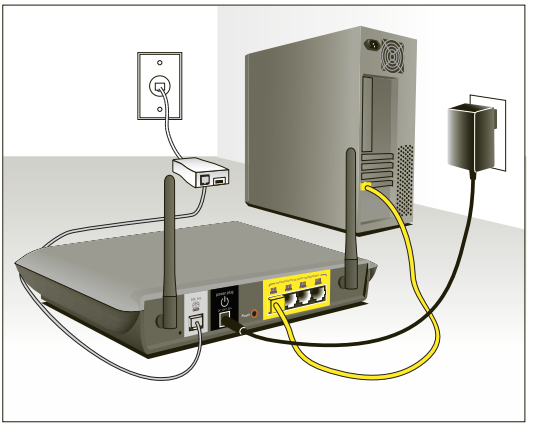
4. Se per il proprio servizio ADSL si dispone di una presa a muro RJ45, collegare un convertitore RJ45-RJ11 alla presa a muro. Quindi collegare un’estremità del cavo telefonico al convertitore e l’altra estremità alla porta grigia RJ11 etichettata “DSL line” sul retro del router.

   Nota: il microfiltro ADSL può essere previsto o meno nella fornitura a seconda del Paese di destinazione.

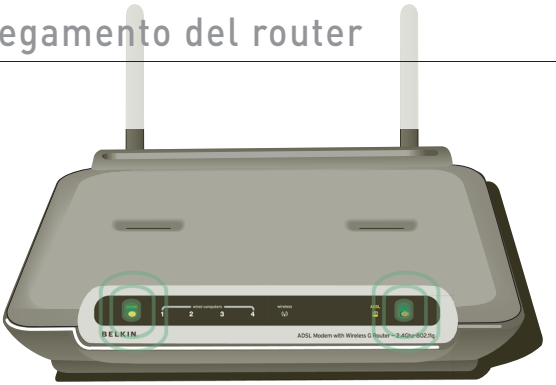
Accensione del router

1. Collegare l’adattatore di alimentazione fornito alla presa di corrente del router etichettata “Power”.

   Nota:per motivi di protezione e prestazioni, e per evitare danni al router, utilizzare soltanto l’adattatore di alimentazione fornito.



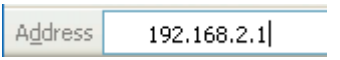
2. **e**Dopo aver collegato l’adattatore di alimentazione ed aver attivato il dispositivo, l’icona ⏻ di alimentazione del router sul pannello anteriore dovrebbe essere attiva. L’avvio completo del router potrebbe richiedere alcuni minuti.



3 Accendere i computer. Dopo aver avviato i computer, si accederà un LED di indicazione di stato LAN sulla parte frontale del router per ciascuna porta alla quale è connesso un computer cablato. Queste spie servono ad indicare lo stato di connessione e attività. A questo punto si può procedere con la configurazione del router per eseguire il collegamento ADSL.

Esecuzione del programma di impostazione guidata

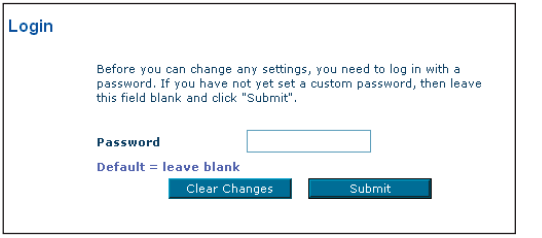
1 Per accedere all'interfaccia utente di gestione del router basata sul web, utilizzare il browser Internet da un computer collegato al router. Nella barra di indirizzo del proprio browser, digitare "192.168.2.1" (non digitare niente del tipo "http://" o "www") e premere il tasto "Enter" (Invio).



Nota: per la configurazione iniziale, si consiglia vivamente di utilizzare un computer fisicamente collegato al router tramite un cavo RJ45. Non è consigliabile utilizzare per la configurazione iniziale un computer collegato in modalità wireless.

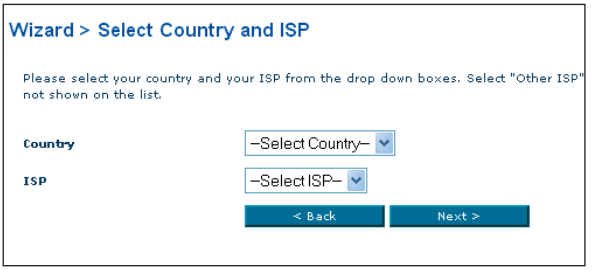
2. Nel browser compare la seguente schermata che invita ad effettuare il login. Il router viene fornito senza alcuna password. Nella schermata di connessione, lasciare vuoto lo spazio per la password e fare clic su "Submit" (Inoltra) per collegarsi.

Nota:per maggiore sicurezza, si consiglia vivamente di cambiare la password. Per ulteriori informazioni su come cambiare la password e sulle altre opzioni di **protezione,**leggere la sezione intitolata "Configurazione manuale del router".



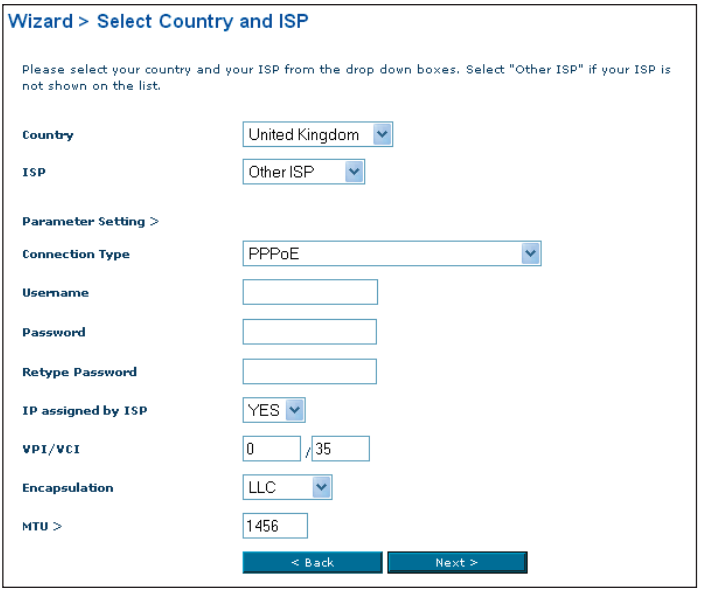
3. La procedura di impostazione guidata sarà avviata automaticamente per eseguire la configurazione rapida (consigliata). Fare clic su “Next” (Avanti) per continuare.

4. Il primo passaggio consiste nel selezionare il proprio Paese e ISP, quindi fare clic su “Next” (Avanti). Se il proprio Paese e/o ISP non fossero in elenco, selezionare “Other Country” (Altro Paese) oppure “Other ISP” (Altro ISP).



5. Quindi selezionare il proprio tipo di connessione: PPPoE, PPPoA o un altro. Per la pagina “PPPoE” o “PPPoA” apparirà la seguente schermata (riportata alla pagina a fianco). Inserire i valori richiesti forniti dal proprio ISP e fare clic su “Next” (Avanti).

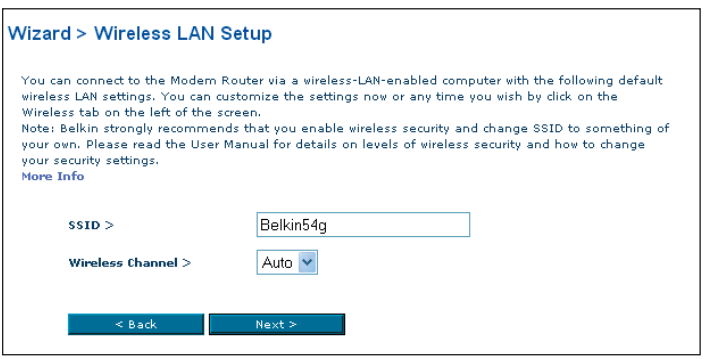
Nota: per istruzioni più dettagliate relative ad altri tipi di connessione, fare riferimento alla sezione intitolata “Configurazione manuale del router” di questo manuale.



6 Viene visualizzata la schermata di configurazione della rete LAN Wireless. Il collegamento con il router può essere eseguito tramite un computer con rete LAN wireless attivata con le seguenti impostazioni di rete LAN wireless predefinite:

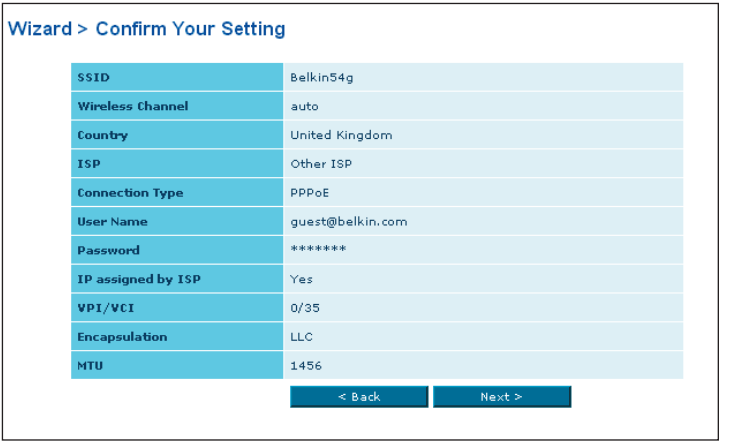
SSID = Belkin54g Canale Wireless = Auto Protezione = inattiva

Nota: Belkin consiglia vivamente di attivare la protezione wireless WEP o WPA e cambiare a piacere l'SSID. Per ulteriori dettagli sui livelli di protezione wireless e su come modificare le impostazioni di sicurezza, vedere il Manuale Utente.

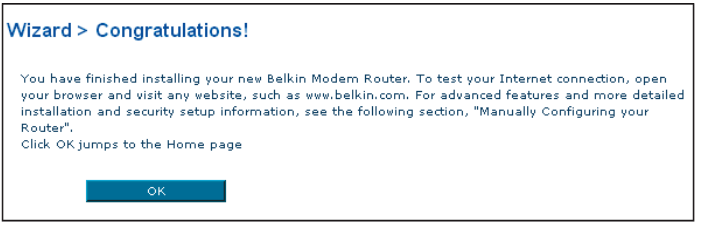


7 **.**Controllare con attenzione le impostazioni riportate nella schermata successiva. Per modificare le impostazioni, fare clic su “Back” (Indietro) o fare clic su “Next” (Avanti) per confermarle.

Nota:per modificare le proprie impostazioni, è possibile riavviare in qualsiasi momento il programma di impostazione guidata o utilizzare il menu di navigazione a sinistra.

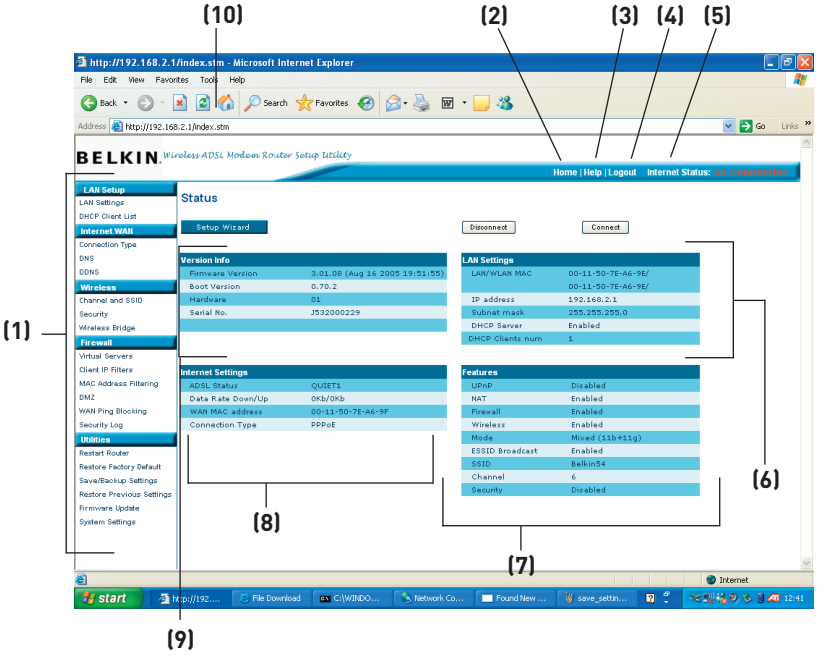


8. Congratulazioni! La procedura di installazione del router Belkin è terminata. Fare clic su “OK” per attivare le impostazioni. Per verificare la connessione ad Internet, aprire il browser e consultare una pagina web qualsiasi, come ad esempio **www.belkin.com**. Per le funzioni avanzate e per informazioni più dettagliate sull’installazione e la configurazione della protezione, vedere la **seguente sezione intitolata “Configurazione manuale del router”.**



Per una migliore comprensione dell'interfaccia utente basata sul web
Nella pagina principale viene riportata una breve sintesi dello stato e delle impostazioni del router. Da questa pagina è possibile accedere a tutte le pagine di impostazione avanzata.

1. **Link di navigazione rapida**
   Facendo clic su questi link è possibile passare direttamente a qualsiasi altra pagina dell'interfaccia utente del router. I link sono suddivisi per categorie logiche e raggruppati per schede, in questo modo si facilita la ricerca di una particolare impostazione. Facendo clic sul titolo di ogni scheda appare una breve descrizione delle funzioni della scheda scelta.



2. **Pulsante Home**
   Il pulsante "Home" è presente in ogni pagina dell'interfaccia utente. Premendo questo pulsante si ritorna alla pagina iniziale.
3. **Pulsante Help**
   Il pulsante "Help" consente di accedere alle pagine guida del router. La guida è disponibile anche in molte pagine, è sufficiente fare clic su "more info" (maggiori informazioni) accanto ad alcune sezioni specifiche di ogni pagina.

4. Pulsante Login/Logout

Questo pulsante attiva e disattiva la connessione del router. Quando si è collegati al router, il pulsante riporta l'indicazione "Logout" (Disconnetti). Collegandosi al router si viene condotti in una pagina di connessione a parte dove viene richiesta una password. Una volta collegati al router, è possibile modificare le impostazioni. Una volta terminate le modifiche, per scollegarsi dal router fare clic sul pulsante "Logout" (Disconnetti). Per maggiori informazioni sulla connessione al router, vi rimandiamo al capitolo "Connessione al router".

5. Indicatore di stato Internet

Questo indicatore è presente in tutte le pagine del router ed ha lo scopo di indicare lo stato del collegamento al router. Quando il messaggio "connection OK" (connessione ok) è VERDE, significa che il router è collegato ad Internet. Quando il router non è collegato ad Internet, appare il messaggio "no connection" (nessuna connessione) in ROSSO. L'indicatore viene aggiornato automaticamente modificando le impostazioni del router.

6. LAN settings (Impostazioni LAN)

Mostra le impostazioni della rete locale (Local Area Network - LAN) del router. Le impostazioni si possono modificare facendo clic sul collegamento di navigazione rapida LAN sulla sinistra della schermata.

7. Features (Caratteristiche)

Visualizza lo stato delle caratteristiche UPnP, NAT e firewall del router. Per apportare delle modifiche, è sufficiente fare clic su uno qualsiasi dei link o sul link "Quick Navigation" (Navigazione rapida) nella parte sinistra dello schermo.

8. Internet Settings (Impostazioni Internet)

Visualizza le impostazioni della sezione Internet/WAN del router che si collega ad Internet. Per apportare eventuali modifiche, è sufficiente fare clic sul link di navigazione rapida "Internet/WAN" nella parte sinistra dello schermo.

9. Version Info (Info versione)

Visualizza le informazioni relative alla versione del firmware, del bootcode, dell'hardware ed il numero di serie del router.

10. Page Name (Nome pagina)

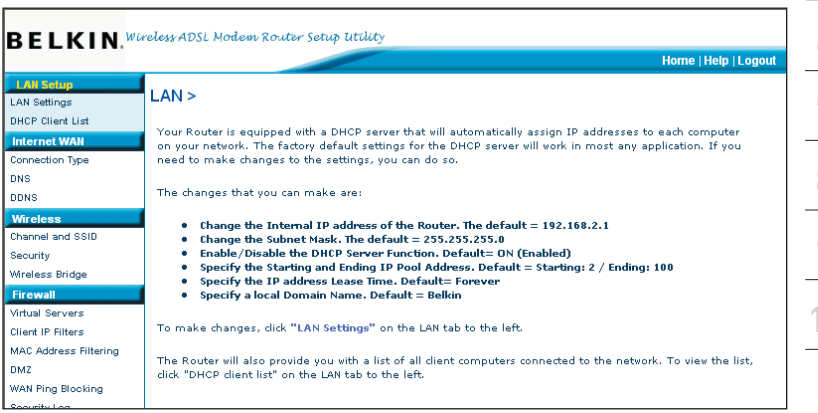
Il nome che identifica la pagina in cui ci si trova. Questo manuale a volte farà riferimento alle pagine chiamandole per nome. Ad esempio, con "LAN > LAN Settings" (LAN > Impostazioni LAN) si intende la pagina "LAN Settings".

Changing LAN Settings (Modifica delle impostazioni LAN)

Da qui possono essere visualizzate o modificate tutte le impostazioni di configurazione della LAN interna del router.

LAN Settings (Impostazioni LAN)

Facendo clic sul titolo della scheda LAN (A) si entra nella pagina di titolo della scheda LAN che contiene una rapida descrizione delle funzioni. Per visualizzare le impostazioni o modificare una qualsiasi delle impostazioni LAN, fare clic su “LAN Settings” (Impostazioni LAN) (B), o per visualizzare la lista dei computer collegati, fare clic su “DHCP client list” (Lista client DHCP) (C).

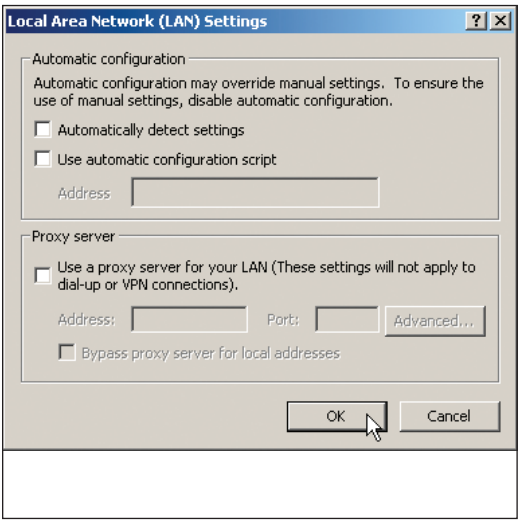


1. **IP Address (Indirizzo IP)**
   Per “Indirizzo IP” si intende l’indirizzo IP interno del router. L’indirizzo IP predefinito è “192.168.2.1”. Per accedere all’interfaccia di configurazione, digitare l’indirizzo IP nell’apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l’indirizzo IP, digitare il nuovo indirizzo IP e fare clic su “Apply Changes” (Esegui modifiche). L’indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

   192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)

   10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

2. **Subnet Mask (Maschera di sottorete)**
   Non è necessario modificare la subnet mask. Si tratta di un’opzione unica, avanzata, prevista dal router Belkin.



3. Server DHCP

La funzione server DHCP semplifica l'impostazione di una rete, in quanto gli indirizzi IP vengono assegnati automaticamente ad ogni computer nella rete. L'impostazione predefinita è "On" (Attiva). Il server DHCP può essere DISATTIVATO, se necessario, ma per farlo è necessario impostare manualmente un indirizzo IP statico per ogni computer in rete. Per disattivare il server DHCP, selezionare "Off" (Inattivo) e fare clic su "Apply Changes" (Esegui modifiche).

4. Pool IP

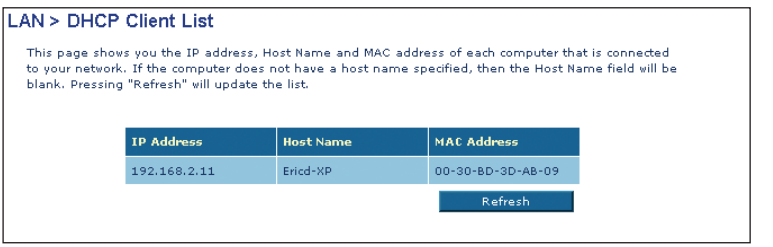
Per "pool IP" si intende la gamma di indirizzi IP messa da parte per l'assegnazione dinamica dei computer alla rete. Il valore predefinito è 2–100 (99 computer). Per modificare questa cifra, digitare un nuovo indirizzo IP di inizio e fine e facendo clic su "Apply Changes" (Esegui modifiche). Il server DHCP può assegnare automaticamente 100 indirizzi IP. Questo significa che non si può specificare un pool di indirizzi IP maggiore di 100 computer. Ad esempio, partendo da 50 significa che bisogna fermarsi a 150 o prima, in modo da non superare il limite dei 100 client. L'indirizzo IP di partenza deve essere un numero inferiore rispetto all'indirizzo IP finale.

5. Lease Time (Disponibilità)
Per disponibilità si intende la durata dell'intervallo durante il quale il server DHCP mantiene riservato l'indirizzo IP per ogni computer. È consigliabile lasciare questo intervallo impostato su "Forever" (Per sempre). L'impostazione predefinita "Forever" (Per sempre) sta ad indicare che ogni volta che ad un computer verrà assegnato un indirizzo IP dal server DHCP, l'indirizzo IP per quel particolare computer non cambierà più. Impostando la disponibilità per intervalli minori, come un giorno o un'ora, una volta trascorso quello specifico intervallo gli indirizzi IP si libereranno. Questo significa anche che l'indirizzo IP di un particolare computer potrebbe cambiare nel corso del tempo. Eventuali altre opzioni avanzate del router, tra cui DMZ o filtri IP client, dipendono dall'indirizzo IP. Per questo motivo è bene che l'indirizzo IP non cambi.

6. Local Domain Name (Dominio locale)
L'impostazione predefinita è "Belkin". Per la propria rete è possibile impostare un dominio locale (nome della rete). Questa impostazione non deve essere necessariamente modificata a meno che non vi sia un'esigenza specifica per farlo. Alla rete può essere assegnato un nome qualsiasi, come ad esempio "MY NETWORK" (LA MIA RETE).

DHCP Client List (Elenco dei Client DHCP)

È possibile visualizzare un elenco dei computer (conosciuti come client) collegati alla rete. È possibile visualizzare l'indirizzo IP (1) del computer, il nome di host (2) (se al computer ne è stato assegnato uno) e l'indirizzo MAC (3) della scheda di interfaccia di rete NIC. Premendo il pulsante "Refresh" (Ripristina) (4), l'elenco viene aggiornato. Nel caso fossero state fatte delle modifiche, l'elenco verrà aggiornato.

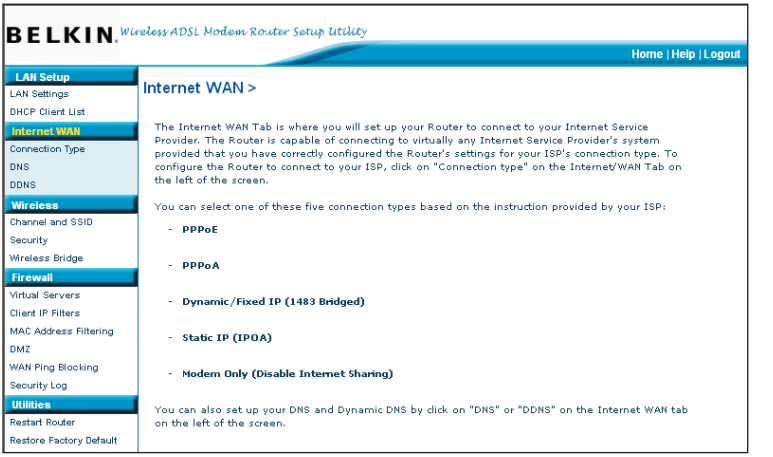


Internet WAN

Nella scheda "Internet/WAN" è possibile configurare il router per potersi collegare al proprio provider Internet (ISP). Il router è in grado di collegarsi praticamente a qualsiasi sistema di provider ADSL, a condizione che le impostazioni siano state configurate correttamente per il tipo di connessione al provider desiderato. Le impostazioni di connessione sono fornite dal provider stesso.

Per configurare il router con le impostazioni indicate dal provider, fare clic su “Connection Type” (Tipo di connessione) (1) nel lato sinistro dello schermo. Selezionare il tipo di connessione utilizzato. Se il provider avesse fornito le impostazioni DNS, facendo clic su “DNS” (2) si possono inserire le informazioni relative all’indirizzo DNS per quei provider che richiedono alcune specifiche impostazioni.

Terminate queste impostazioni, l’indicatore “Internet Status” (Stato Internet), se il router è stato impostato correttamente, visualizzerà il messaggio “Connected” (collegato).



Connection Type (Tipo di connessione)

Dalla pagina “Connection Type” (Tipo di connessione) è possibile scegliere tra cinque tipi di connessione sulla base delle istruzioni fornite dal proprio ISP:

PPPoE

PPPoA

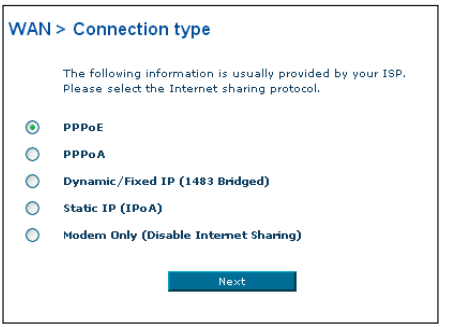
IP dinamico (1483 Bridged)

IP statico (IPOA)

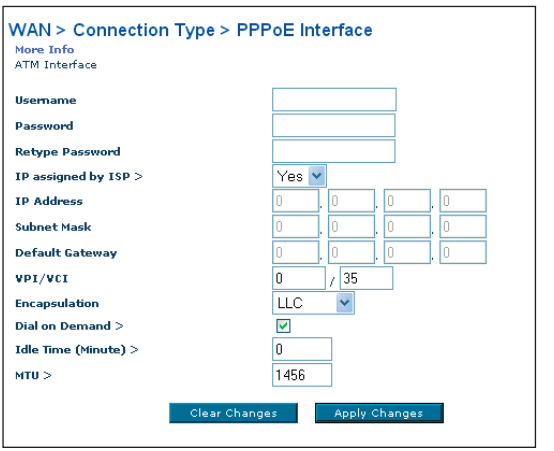
Soltanto modem (disattivare la condivisione Internet)

Nota: per conoscere alcuni dei parametri di impostazione Internet DSL comuni, vedere l’Appendice C di questo Manuale Utente. Nel dubbio, contattare il proprio ISP.

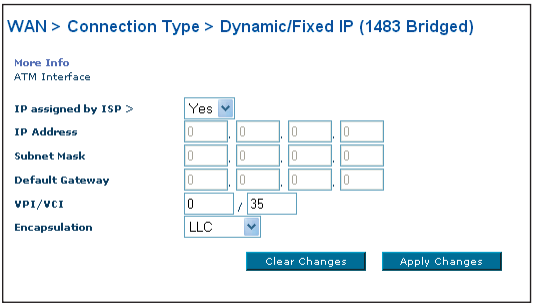
Selezionare il tipo di connessione utilizzata facendo clic sul pulsante radio (1) accanto al tipo di connessione e facendo quindi clic su “Next” (Avanti).



Configurazione del proprio tipo di connessione ISP su PPPoE o PPPoA
PPPoE (Point-to-Point Protocol over Ethernet) rappresenta il metodo standard per collegare i dispositivi collegati in rete. Per accedere alla rete del proprio ISP e collegarsi ad Internet questo tipo di connessione richiede un nome utente ed una password. Lo standard PPPoA (PPP over ATM) è simile allo standard PPPoE, ma è utilizzato principalmente nel Regno Unito. Selezionare PPPoE o PPPoA e fare clic su “Next” (Avanti). Quindi inserire le informazioni fornite dal proprio ISP e fare clic su “Apply Changes” (Esegui modifiche) per attivare le impostazioni.

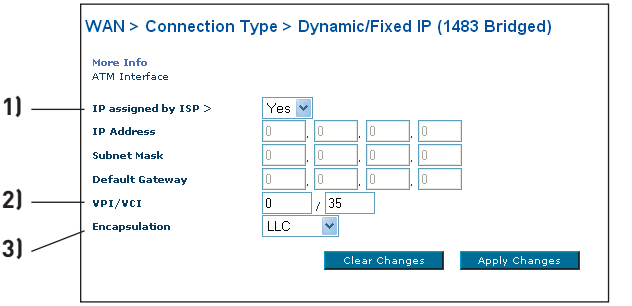


1. **User Name (Nome utente)** - Digitare il nome utente. (fornito dal proprio ISP).
2. **Password** - Digitare la password. (fornita dal proprio ISP).
3. **Retype Password (Ridigita password)** - Confermare la password. (fornita dal proprio ISP).
4. **IP Assigned by ISP (IP assegnato dall'ISP)** – Lasciare "Yes" (Sì) l'ISPassegna automaticamente un indirizzo IP. Se l'ISP assegna un indirizzo IP fisso, selezionare "No" e digitare i dati forniti.
5. **VPI/VCI** - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).
6. **Encapsulation (Incapsulamento)** - Scegliere il tipo di incapsulamento (fornito dal proprio ISP) per specificare come gestire i protocolli multipli sul livello di trasporto ATM. VC-MUX: Lo standard PPPoA Virtual Circuit Multiplexer (incapsulamento nullo) consente di avere un solo protocollo in funzione per ciascun circuito virtuale con un numero inferiore di overhead. LLC: Lo standard PPPoA Logical Link Control consente a diversi protocolli multipli di funzionare su un unico circuito virtuale (maggior numero di overhead).
7. **Dial on Demand (Composizione a richiesta)**- Selezionando l'opzione "Dial on Demand" il router si collegherà automaticamente ad Internet ogni volta che un utente aprirà un browser web.
8. **Idle Time (Minutes) (Intervallo di inattività - Minuti)** - Indicare il tempo di inattività massimo per la connessione a Internet. Superato questo intervallo, la connessione verrà interrotta.
9. **MTU**- L'impostazione MTU non dovrebbe mai essere modificata, sempre che il proprio ISP non fornisca un'impostazione MTU specifica. La modifica delle impostazioni MTU può comportare dei problemi con la propria connessione ad Internet, tra cui la disconnessione da Internet, il rallentamento dell'accesso ad Internet e problemi a livello di funzionamento corretto delle applicazioni Internet.



Configurazione del tipo di connessione su IP dinamico (1483 Bridged)

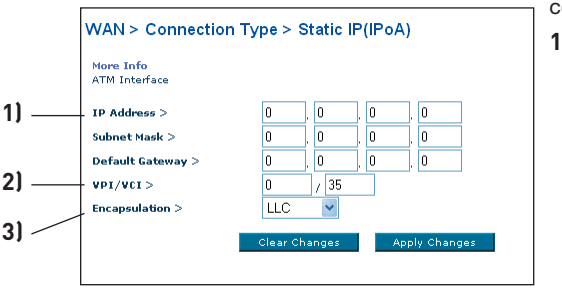
Questo metodo di connessione consente di creare un ponte di collegamento tra la propria rete e quella dell'ISP. Il router riceve l'indirizzo IP automaticamente dal server DHCP dell'ISP.



1. **IP Assigned by ISP (IP assegnato dall'ISP)** – Lasciare "Yes" (Sì) l'ISPassegna automaticamente un indirizzo IP. Se l'ISP assegna un indirizzo IP fisso, selezionare "No" e digitare i dati forniti.
2. **VPI/VCI** - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). Questi parametri di identificazione vengono assegnati dall'ISP.
3. **Encapsulation (Incapsulamento)** - Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostazione del proprio tipo di connessione ISP sull'IP statico (IPoA)

Questo tipo di connessione viene anche chiamato "Classical IP over ATM" o "CLIP", ed è quello fornito dall'ISP come IP fisso del router da collegare ad Internet.

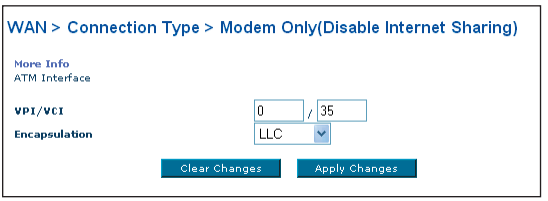


1. **IP Address (Indirizzo IP)** – Digitare un indirizzo IP assegnato dal proprio ISP per l'interfaccia WAN del router.

2. **Subnet Mask (Maschera di sottorete)** - Digitare una subnet mask assegnata dal proprio ISP.
3 **Default Route (Percorso predefinito)** - Digitare un indirizzo IP gateway predefinito. Se il router non riesce a trovare l'indirizzo di destinazione entro la propria rete locale, trasmette i pacchetti al gateway predefinito assegnato dal proprio ISP.
4. **VPI/VCI** - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI).

   Questi parametri di identificazione vengono assegnati dall'ISP.
5. **Encapsulation (Incapsulamento)** - Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

Impostazione del tipo di connessione su Modem Only (Disable Internet Sharing) (Soltanto modem- disabilita la condivisione a Internet)



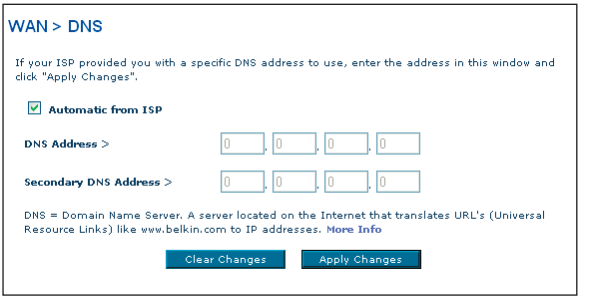
In questa modalità, il router agisce semplicemente come ponte per trasferire i pacchetti attraverso la porta ADSL. Per accedere ad Internet è necessario disporre di altro software supplementare installato nei propri computer.

1. **VPI/VCI** - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).
2. **Encapsulation (Incapsulamento)** - Selezionare i parametri LLC o VC MUX. (forniti dal proprio ISP).

Impostazioni DNS (Domain Name Server)

Un "Domain Name Server" è un server presente in Internet che traduce gli Universal Resource Link (URL) come "www.belkin.com" in indirizzi IP. Molti ISP non richiedono l'immissione di questa informazione nel router. Se non è stato inserito alcun indirizzo DNS specifico, la casella "Automatic from ISP" (Automaticamente dall'ISP) (1) dovrebbe essere spuntata. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo

DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse di tipo dinamico o PPPoE, potrebbe non essere necessario inserire un indirizzo DNS. Lasciare la casella “Automatic from ISP” (Automatico da ISP) selezionata. Per digitare le impostazioni dell’indirizzo DNS, togliere il segno di spunta dalla casella “Automatic from ISP” (Automatico da ISP) e digitare i propri dati DNS negli spazi disponibili. Fare clic su “Apply Changes” (Esegui modifiche) (2) per salvare le impostazioni.



Utilizzo del DNS dinamico

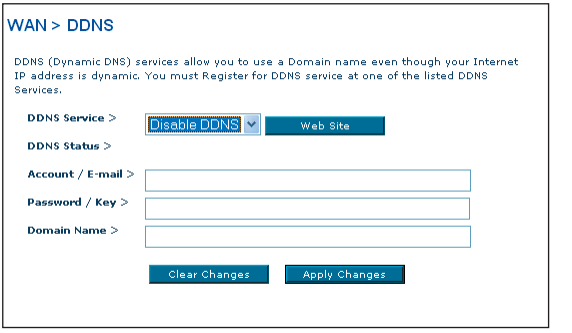
Il servizio Dynamic DNS (DNS dinamico) permette di trasformare un indirizzo IP dinamico in un nome host statico in uno qualsiasi dei domini offerti dalla DynDNS.org. Ciò permette di accedere ai computer di rete più facilmente da varie postazioni Internet. DynDNS.org offre questo servizio, per un massimo di 5 host name, gratuitamente alla comunità Internet. TZO.com è un’alternativa a DynDNS.org.

Il servizio DDNS è ideale per i siti web domestici, file server o per semplificare l’accesso ai file archiviati ed al PC in casa. Con questo servizio si può essere certi che il proprio nome host porti sempre al proprio indirizzo IP, anche se l’ISP lo cambia. Quando l’indirizzo IP cambia, i vostri amici e colleghi saranno sempre in grado di rintracciarvi andando su tuonome.dyndns.org!

Per registrarsi gratuitamente al servizio di nome host DNS dinamico, andare **su http://www.dyndns.org**.

Impostazione dell'aggiornamento client del DNS dinamico del router
Prima di poter usufruire del servizio di aggiornamento gratuito, bisogna registrarsi con DynDNS.org. Una volta effettuata la registrazione, seguire le seguenti istruzioni:

1. Inserire il proprio nome utente DynDNS.org nel campo "Account / E-mail" (1).
2. Inserire la propria password DynDNS.org nel campo "Password / Key" (2).
3. Nel campo "Domain Name"(Nome dominio) (3), digitare il nome del dominio DynDNS.org creato con DynDNS.org.
4. Fare clic su "Apply Changes" (Esegui modifiche) per aggiornare l'indirizzo IP.

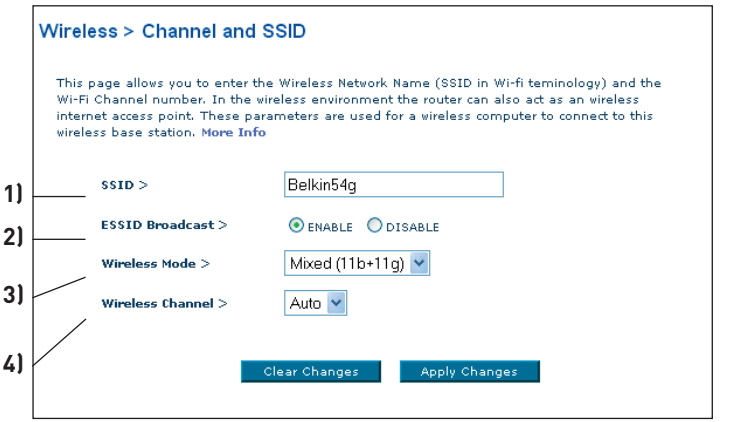


Ogni volta che l'indirizzo IP fornito dall'ISP cambia, il router aggiornerà automaticamente i server di DynDNS.org con il nuovo indirizzo IP. È possibile effettuare questa operazione anche manualmente, facendo clic sul pulsante "Apply Changes" (Esegui modifiche) (4).

Wireless

Nella scheda "Wireless" è possibile modificare le impostazioni di configurazione di rete. Da questa scheda è possibile modificare il nome della rete wireless (SSID), il canale operativo e le impostazioni di protezione crittografata.

Canale e SSID



1. Modifica del nome della rete wireless (SSID)

Per identificare la propria rete wireless, viene utilizzato un nome chiamato SSID (Service Set Identifier). L'SSID predefinito del router è "belkin54g". È possibile sostituire questo nome con un altro qualsiasi o lasciarlo invariato. In presenza di altre reti wireless nella stessa area, è consigliabile utilizzare un SSID unico (diverso da quello di un'eventuale altra rete wireless in zona). Per modificare il nome SSID, digitare il nuovo SSID che si desidera utilizzare nel campo SSID (1) e fare clic su "Apply Changes" (Esegui modifiche) (2). La modifica è immediata. Nel caso il nome SSID venga modificato, è necessario riconfigurare anche i computer wireless per consentirne il collegamento al nuovo nome della rete. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

2. Utilizzo del servizio di trasmissione ESSID

Per questioni di sicurezza si può scegliere di non trasmettere la propria SSID di rete. In questo modo, il proprio nome di rete rimarrà nascosto a quei computer che eseguiranno un'analisi per rilevare la presenza di eventuali reti wireless. Per disattivare la trasmissione SSID, selezionare "DISABLE" (disattiva) e fare clic su "Apply Changes" (Esegui modifiche). La modifica è immediata. A questo punto, tutti i computer devono essere impostati in modo da potersi collegare al proprio SSID specifico; un SSID "QUALSIASI" non sarà più accettato. Per ulteriori indicazioni su come eseguire le modifiche necessarie, vedere la documentazione relativa alla scheda di rete wireless.

Nota: Questa funzione avanzata dovrebbe essere implementata soltanto dagli utenti esperti.

3. Utilizzo della modalità switch wireless

Il router può funzionare in tre diverse modalità wireless: "Mixed (11b+11g)", "11g Only" e "11b Only". Le diverse modalità sono spiegate di seguito.

Modalità "Mixed (11b+11g)"—In questa modalità, il router è compatibile contemporaneamente con i client wireless 802.11b e 802.11g. Questa modalità è impostata dal produttore e garantisce un corretto funzionamento con tutti i dispositivi Wi-Fi. Se nella propria rete sono presenti client 802.11b e 802.11g, è consigliabile non toccare le impostazioni predefinite. Questa impostazione andrà modificata soltanto per motivi ben specifici.

Modalità "11g –Only"—La modalità 802.11g-Only funziona esclusivamente con i client 802.11g. Questa modalità è consigliata soltanto nel caso si desideri impedire ai client 802.11b di accedere alla propria rete. Per cambiare modalità, selezionare quella desiderata dall'elenco a discesa "Wireless Mode" (Modalità wireless). Quindi fare clic su "Apply Changes" (Esegui modifiche).

Modalità "11b Only" —NON è consigliabile utilizzare questa modalità, a meno che non se ne abbia un motivo specifico. Questa modalità è stata creata per risolvere problematiche uniche che si possono verificare con alcuni adattatori per client 802.11b e NON è necessaria per garantire l'interoperabilità tra gli standard 802.11g e 802.11b.

4. Modifica del canale wireless

Esistono numerosi canali operativi tra cui scegliere. Negli Stati Uniti i canali sono 11. Nel Regno Unito e in gran parte d'Europa i canali sono 13. In pochi altri paesi ancora i requisiti per i canali sono diversi. Il Router è stato configurato per funzionare sui canali adatti al paese di residenza dell'utente. Il canale predefinito è "Auto".

Questo canale, se necessario, può essere cambiato. In presenza di altre reti wireless nella stessa area, la rete dovrà essere impostata in modo da funzionare su un canale diverso dalle altre reti wireless. Per ottenere prestazioni migliori, utilizzare un canale che sia almeno a cinque canali di distanza dalla rete wireless. Ad esempio, in presenza di un'altra rete che funziona sul canale 11, impostare la propria rete sul canale 6 o su un canale minore. Per cambiare canale, selezionare il canale desiderato dall'elenco a tendina. Fare clic su "Apply Changes" (Esegui modifiche). La modifica è immediata.

Crittografia/Sicurezza

Protezione della rete Wi-Fi

Di seguito sono descritte alcune soluzioni per rendere più efficiente la rete wireless e per proteggere i propri dati da intrusioni indesiderate. Questo capitolo è dedicato agli utenti che usano la rete da casa, dall'ufficio in casa e da piccoli uffici. Al momento della stampa di questo manuale, i tipi di crittografia disponibili sono tre.

Nome	64 bit Wired Equivalent Privacy	128 bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Accesso protetto Wi-Fi AES
Acronimo	64-bit WEP	128-bit WEP	WPA-TKIP	WPA-AES
Protezione	Buona	Migliore	Ottima	Ottima
Caratteristiche	Chiavi statiche	Chiavi statiche	Crittografia a chiave dinamica e autenticazione reciproca.	Crittografia a chiave dinamica e autenticazione reciproca.
	Chiavi di crittografia basate sull'algoritmo RC4 (generalmente chiavi a 40 bit)	Più sicura rispetto alla protezione WEP a 64 bit con una chiave lunga 104 bit, più 24 bit aggiuntivi dei dati generati dal sistema	Protocollo TKIP (temporal key integrity protocol) aggiunto che permette la rotazione delle chiavi e il rafforzamento della crittografia	La crittografia AES (Advanced Encryption Standard) non causa alcuna perdita di trasferimento dati.

WEP (Wired Equivalent Privacy)

WEP è un protocollo che aggiunge protezione a tutti i prodotti wireless conformi allo standard Wi-Fi. Questo protocollo comune offre alle reti wireless lo stesso livello di protezione della privacy di una rete cablata simile.

WEP a 64 bit

La WEP a 64 bit fu introdotta per la prima volta con la crittografia da 64 bit, che include una lunghezza di codice di 40 bit più 24 bit aggiuntivi di dati generati dal sistema (64 bit in totale). Alcuni produttori di hardware si riferiscono alla crittografia a 64 bit come crittografia a 40 bit. Poco tempo dopo l'introduzione della tecnologia, i ricercatori scoprirono che la crittografia a 64 bit poteva essere decodificata molto facilmente.

WEP a 128 bit

Per riparare alle potenziali debolezze della crittografia a 64 bit, si progettò il metodo più sicuro della crittografia a 128 bit. La crittografia a 128 bit comprende una chiave da 104 bit più 24 bit aggiuntivi di dati generati dal sistema (128 bit in totale). Alcuni produttori di hardware si riferiscono alla crittografia a 128 bit come crittografia a 104 bit.

La maggior parte delle apparecchiature wireless attualmente in commercio supporta entrambi i tipi di crittografia, a 64 e 128 bit, tuttavia alcune apparecchiature più vecchie supportano solo la WEP a 64 bit. Tutti i prodotti wireless Belkin supportano entrambi i tipi di crittografia, a 64 e 128 bit.

Codici di crittografia

Dopo aver scelto tra la modalità di crittografia "64-bit" oppure "128-bit WEP" è fondamentale generare una chiave di crittografia. La chiave di crittografia dovrà essere sempre la stessa per tutta la rete wireless, altrimenti i dispositivi di rete wireless non saranno in grado di comunicare tra loro e l'utente non sarà in grado di comunicare all'interno della rete.

La chiave di crittografia può essere inserita manualmente in modalità esadecimale, oppure inserendo una frase di accesso nel campo "Passphrase" (frase di accesso) e cliccando quindi sulla richiesta di generare la chiave. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 64 bit è necessario inserire una chiave composta da 10 caratteri esadecimali. Per la protezione WEP a 128 bit, bisogna inserire 26 codici esadecimali.

Ad esempio:

AF 0F 4B C3 D4 = chiave WEP a 64 bit

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = chiave WEP a 128 bit

La frase di accesso WEP NON è la stessa cosa della chiave WEP. La scheda wireless fornita utilizza la frase di accesso per generare le chiavi WEP, ma i metodi per generare le chiavi potrebbero cambiare a seconda del produttore. Se nella rete sono presenti dispositivi di varie marche, la cosa più semplice da fare è usare la chiave WEP esadecimale del router o dell'access point wireless ed inserirlo manualmente nella tabella dei codici esadecimali WEP nella schermata di configurazione della scheda.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) è un nuovo standard Wi-Fi che offre maggiore sicurezza rispetto alla WEP. Per poter utilizzare la protezione WPA, i driver ed il software dell'apparecchiatura wireless devono essere aggiornati in maniera adatta a supportarla. Tali aggiornamenti sono disponibili nel sito web del rivenditore dei dispositivi wireless. Esistono due tipi di protezione WPA: WPA-PSK (senza server) e WPA (con server radius 802.1x).

WPA-PSK (no server)
Questo metodo si avvale di una chiave pre-condivisa come chiave di rete. Una chiave di rete pre-condivisa è una password la cui lunghezza varia da 8 a 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa la stessa chiave di rete per accedere alla rete. Generalmente, questa è la modalità che viene utilizzata in un ambiente domestico.

WPA (con server radius 802.1x)
Questo sistema consente ad un server radius di distribuire automaticamente la chiave di rete ai client. Generalmente, questa modalità viene utilizzata in un ambiente di lavoro.

WPA2
Il router è provvisto della protezione WPA2, la seconda generazione della crittografia WPA basata sullo standard 802.11i. Offre un maggiore livello di protezione combinando un'autenticazione di rete avanzata ed un metodo di crittografia AES rafforzato.

Requisiti WPA2
IMPORTANTE: Per utilizzare la protezione WPA2, tutti i computer e gli adattatori di rete devono essere aggiornati con patch, driver e software utility client che supportano la WPA2. Al momento della pubblicazione di questo manuale, è possibile scaricare gratuitamente un paio di security patch da Microsoft Questi patch sono adatti soltanto al sistema operativo Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

Per i computer con Windows XP che non hanno Service Pack 2 (SP2), è possibile scaricare gratuitamente un file da Microsoft chiamato "Windows XP Support Patch for Wireless Protected Access (KB 826942)" .

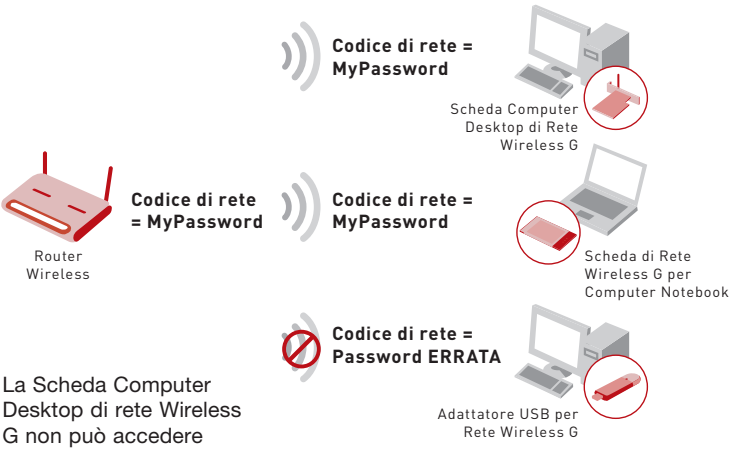
Per Windows XP con Service Pack 2, Microsoft mette a disposizione un download gratuito per aggiornare i componenti del client wireless in modo da poter supportare la protezione WPA2(KB893357). L'aggiornamento può essere scaricato dal sito: http://support.microsoft.com/default.aspx?scid=kb;en-us;893357

IMPORTANTE: È necessario accertarsi inoltre che il produttore della scheda/adattatori wireless supporti la protezione WAP2 e di aver scaricato e installato il driver più recente. Per la maggior parte delle schede wireless Belkin è possibile scaricare un driver di aggiornamento dal sito Belkin: www.belkin.com/networking.

Un elenco dei prodotti wireless Belkin che supportano le protezioni WPA/WPA2 è riportato al sito web **www.belkin.com/networking**.

Condivisione dei codici di rete

Nella maggior parte dei prodotti Wi-Fi la sicurezza è disattivata. Dopo aver installato la rete e quando questa è in funzione, bisognerà attivare la protezione WEP o WPA ed assicurarsi che tutti i dispositivi wireless usino la stessa chiave di rete.



La Scheda Computer Desktop di rete Wireless G non può accedere alla rete perché usa una chiave di rete diversa da quella configurata nel router wireless G.

Utilizzo di una chiave esadecimale

Una chiave esadecimale è composta da numeri e lettere che vanno dalla A alla F e dallo 0 al 9. Le chiavi a 64 bit sono composte da cinque numeri a due cifre. Le chiavi a 128 bit sono composte da 13 numeri a due cifre.

Per esempio:
AF 0F 4B C3 D4 = chiave a 64 bit
C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = chiave a 128 bit

Nelle caselle riportate di seguito va creata la propria chiave, inserendo in ogni casella due caratteri compresi tra A-F e 0–9. Questa chiave sarà utilizzata per programmare le impostazioni di crittografia del router e dei propri computer wireless.

Esempio	AF	0F	4B	C3	D4								
chiave a 64 bit													
chiave a 128 bit													

Nota per gli utenti Mac:I prodotti originali Apple AirPort® supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 possono supportare la modalità di crittografia a 64 o 128 bit. Verificare quale sia la versione utilizzata. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

Configurazione WEP

1. Selezionare “WEP” dal menu a discesa.
2. Scegliere “WEP Mode” a 64 bit o 128-bit
3. Una volta selezionata la modalità di crittografia WEP, sarà possibile inserire la propria chiave esadecimale digitandola manualmente.

   Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 64 bit è necessario inserire una chiave composta da 10 caratteri esadecimali. Per la protezione WEP a 128 bit, bisogna inserire 26 codici esadecimali.

   Per esempio:
   AF 0F 4B C3 D4 = chiave a 64 bit
   C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = chiave a 128 bit

3. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. La crittografia del router è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione.

   AVVERTENZA: Se si stesse eseguendo la configurazione del router o access point wireless da un computer con un client wireless, sarà necessario accertarsi che la protezione per questo client wireless sia ATTIVA. In caso contrario si perderà la connessione wireless.

Modifica delle impostazioni di protezione della rete wireless

Il vostro router è protetto da crittografia WPA/WPA2 (Wi-fi Protected Access), il più recente standard di protezione wireless. Esso supporta anche lo standard di protezione legacy WEP (Wired Equivalent Privacy). L’impostazione predefinita prevede che la protezione wireless sia disattivata. Per abilitare la protezione, è necessario stabilire prima lo standard che si desidera utilizzare. Per accedere alle impostazioni di protezione, fare clic su “Security” (Protezione) nella scheda Wireless.

Configurazione WPA

Nota:per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo manuale, un security patch di Microsoft è disponibile gratuitamente, adatto soltanto al sistema operativo Windows XP. E’ necessario inoltre scaricare dal sito di supporto Belkin il driver più recente per la propria scheda di rete wireless G desktop o notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

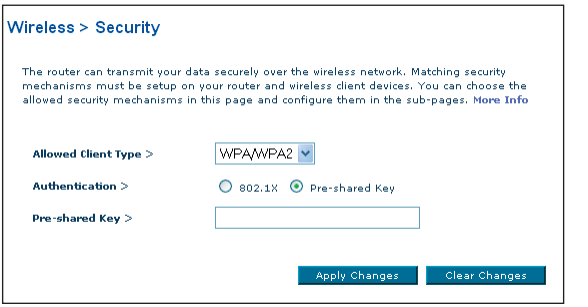
Esistono due tipi di protezione WPA: WPA-PSK (senza server) e WPA (con server radius). La protezione WPA-PSK (senza server) sfrutta la cosiddetta chiave pre-condivisa come codice di protezione. Una chiave pre-condivisa è una password la cui lunghezza varia da 8 a 63 caratteri, tra lettere, numeri ed altri caratteri. Ogni client usa lo stesso codice per accedere alla rete. Generalmente, questa modalità viene utilizzata in un ambiente domestico.

La protezione WPA (con server radius) è una configurazione nell’ambito della quale un server radius distribuisce automaticamente i codici ai client. Questa soluzione viene generalmente utilizzata nell’ambiente lavorativo.

La protezione WPA2 è la seconda generazione della WPA ed offre una tecnica di crittografia più avanzata rispetto alla WPA.

Impostazione della protezione WPA/WPA2-PSK (senza server)

1. Dal menu a discesa “Allowed Client Type”, selezionare “WPA/WPA2”.
2. Come autenticazione, scegliere “Pre-shared Key” per un uso domestico o in un piccolo ufficio. Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare la propria chiave precondivisa, che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: “Chiave di rete famiglia Rossi”.



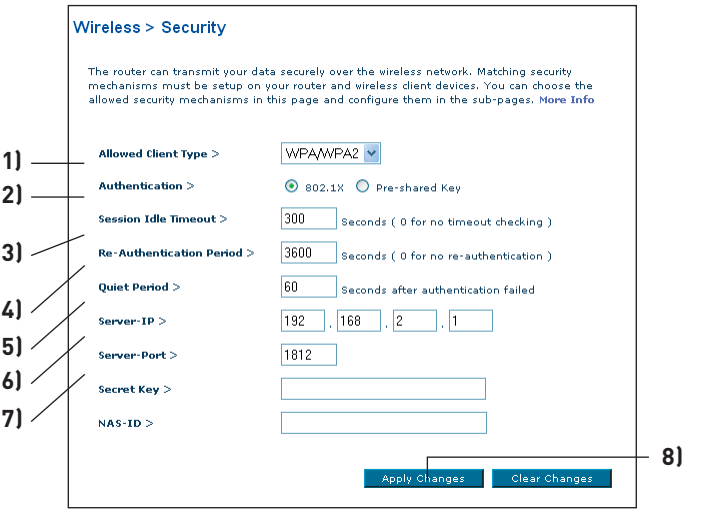
4. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Configurazione delle impostazioni WPA/WPA2 (con server radius)

Se la rete utilizza un server radius per distribuire le chiavi ai client, utilizzare questa impostazione.

1. Dal menu a discesa “Allowed Client Type”, selezionare “WPA/WPA2”.
2. Come tecnica di crittografia, scegliere “802.1x” se si tratta di ambienti con server radius. Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare l’intervallo di inattività del server radius nel campo “Session Idle Timeout” .
4. Digitare l’intervallo della chiave, ovvero ogni quanto le chiavi sono distribuite (in pacchetti), nel campo “Re-Authentication Period”

5. Digitare l'intervallo di attesa dopo la fallita autenticazione nel campo "Quiet Period".
6. Digitare l'indirizzo IP e il numero della porta del server radius nei campi "Server-IP" e "Server-Port".
7. Digitare la chiave radio nel campo "Secret Key" (chiave segreta).
8. Fare clic su "Apply Changes" (Esegui modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.



Nota: Accertarsi che i computer wireless siano stati aggiornati in modo tale da poter funzionare con la protezione WPA2 e che le impostazioni siano corrette per poter effettuare la connessione con il router.

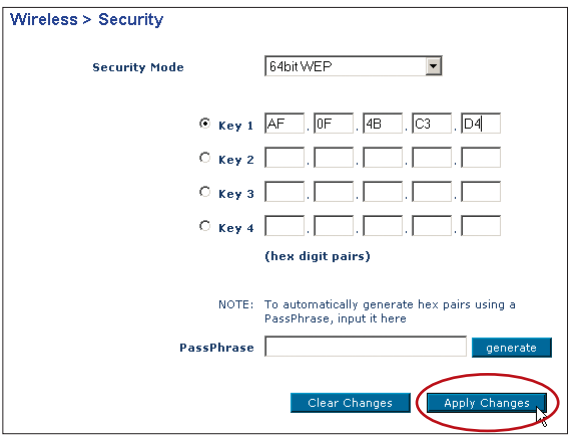
Configurazione delle Schede di Rete Wireless G Belkin per l'utilizzo della protezione

Nota:questa sezione contiene le informazioni su come configurare le schede di rete wireless G di Belkin per utilizzare la protezione.

A questo punto il router e l'access point wireless dovrebbero essere stati già configurati per l'utilizzo della crittografia WPA o WEP. Per ottenere una connessione wireless, bisognerà configurare le schede di rete wireless per computer notebook e desktop con le medesime impostazioni di protezione.

Collegamento del computer ad un router o wireless access point che richiede una chiave WEP a 64 o 128 bit

1. Fare doppio clic sull' icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda “Wireless Network Properties” , selezionare un nome dall'elenco “Available networks” (Reti disponibili) e fare clic su “Configure” (configura).
3. In “Data Encryption” (Crittografia dati), selezionare “WEP”.
4. Disattivare la casella in basso “Network key is provided for me automatically” (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.
5. Digitare la chiave WEP nella casella “Network key” (Chiave di rete).

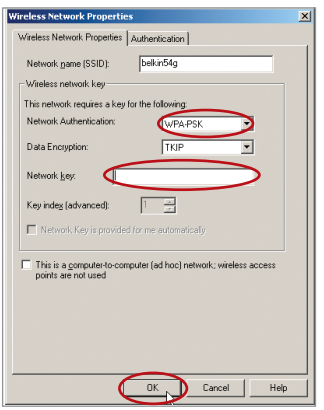


Importante: una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri. Per la protezione WEP a 64 bit, bisogna inserire 10 codici. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

6. Fare clic su “OK” per salvare le impostazioni.

Collegamento del computer ad una rete wireless che usa la protezione WPA-PSK (senza server)

1. Fare doppio clic sull' icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda “Wireless Network”, selezionare un nome dall'elenco “Available networks” (Reti disponibili) e fare clic su “Configure” (configura).
3. In “Network Authentication” (Autenticazione di rete) selezionare “WPA-PSK (No Server)”.
4. Digitare la chiave WPA nella casella “Network key” (Chiave di rete).

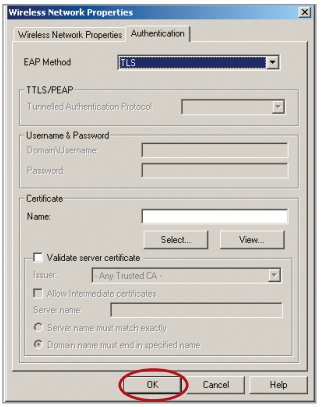


Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

5. Fare clic su “OK” per salvare le impostazioni.

Collegamento del computer ad una rete wireless che usa la protezione WPA (con server radius)

1. Fare doppio clic sull' icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.
2. Nella scheda “Wireless Network”, selezionare un nome dall'elenco “Available networks” (Reti disponibili) e fare clic su “Configure” (configura).
3. In “Network Authentication” (Autenticazione di rete) selezionare “WPA”.
4. Nella scheda “Authentication” (Autenticazione), selezionare le impostazioni indicate dall'amministratore di rete.



5. Fare clic su “OK” per salvare le impostazioni.

Impostazione della protezione WPA per schede wireless desktop e notebook di altre marche

Per le schede di rete wireless WPA per computer desktop e notebook di altre marche sprovviste del software WPA, è possibile scaricare gratuitamente un file da Microsoft chiamato “Windows XP Support Patch for Wireless Protected Access”.

Nota:il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati.

> **Importante:** È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA e di aver scaricato e installato il driver più recente dal suo sito.

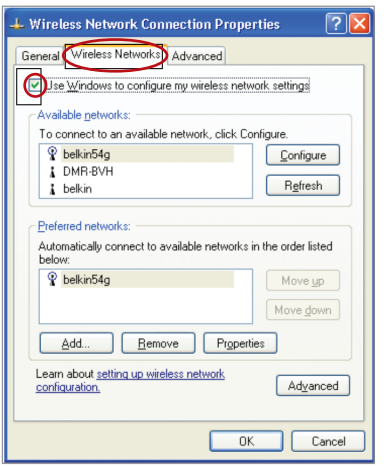
Sistemi operativi supportati:

- Windows XP Professional
- Windows XP Home Edition

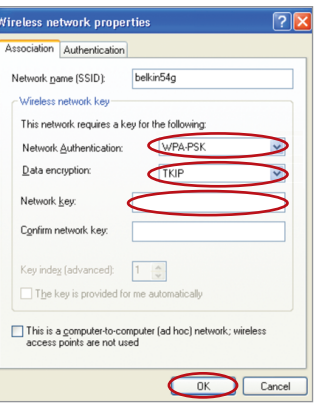
Impostazione della utility wireless Windows XP per utilizzare la protezione WPA-PSK

Per utilizzare la protezione WPA-PSK, accertarsi di utilizzare la utility di rete wireless Windows nel seguente modo:

1. In Windows XP, fare clic su “Start > Control Panel (Pannello di controllo) > Network Connections (Connessioni di rete)”.
2. Con il tasto destro del mouse, fare clic sull’opzione “Wireless Network Connection” (Connessione rete wireless), e selezionare “Properties” (Proprietà).
3. Cliccando sulla scheda “Wireless Networks” (Reti wireless) si aprirà la seguente schermata. Accertarsi che l’opzione “Use Windows to configure my wireless network settings” (Utilizza Windows per configurare le impostazioni di rete wireless) sia attivata.



4. Nella scheda “Wireless Networks” (Reti wireless), fare clic su “Configure” (Configura) per fare aprire la seguente schermata.



5. Nel caso di una rete domestica o simile, selezionare “WPA-PSK” da “Network Authentication” (Autenticazione rete).

Nota: selezionare “WPA” se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come può essere un radius server. Per ulteriori informazioni, rivolgersi all’amministratore di rete.

6. Selezionare “TKIP” o “AES” da “Data Encryption” (Crittografia dati). Questa impostazione dovrà essere identica a quella del router configurato.
7. Digitare la propria chiave di crittografia nella casella “Network key” (Chiave di rete).

   Importante:inserire la propria chiave precondivisa che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.
8. Fare clic su “OK” per confermare le impostazioni.

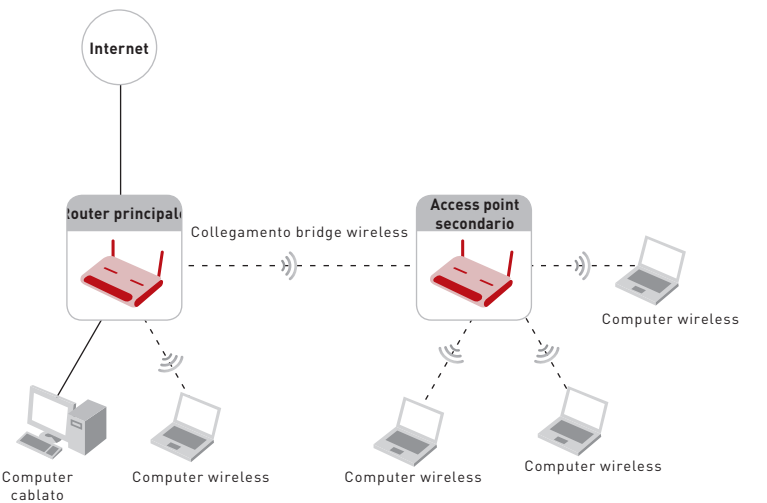
Modalità di estensione range wireless e bridging

Cos’è un Bridge Wireless?

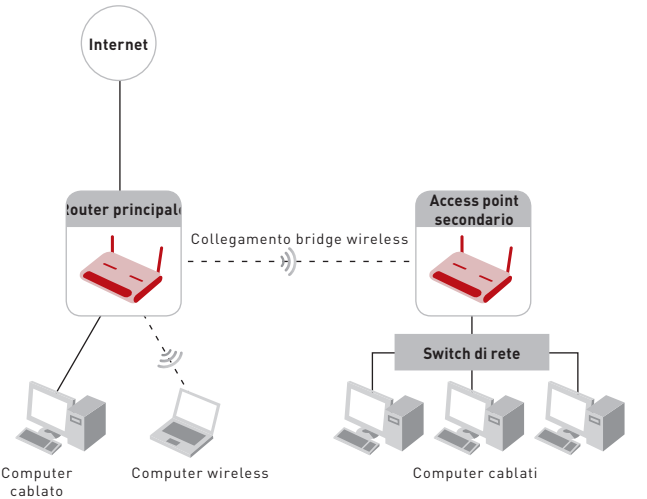
La modalità bridge wireless può essere utilizzata per ampliare la portata della propria rete wireless o per aggiungere un’estensione della propria rete in un’altra zona del proprio ufficio o a casa senza dover ricorrere all’uso dei cavi.

Nota: non possiamo garantire che questa opzione funzionerà con hardware wireless di altre marche.

Nota: Per contare su prestazioni eccellenti, accertarsi di aver scaricato la più recente versione firmware per il router o access point: http://web.belkin.com/support



Aggiunta di un altro segmento di rete wireless
La connessione di uno switch o un hub di rete al jack R45 dell'access point consente a numerosi computer collegati allo switch di accedere al resto della rete.

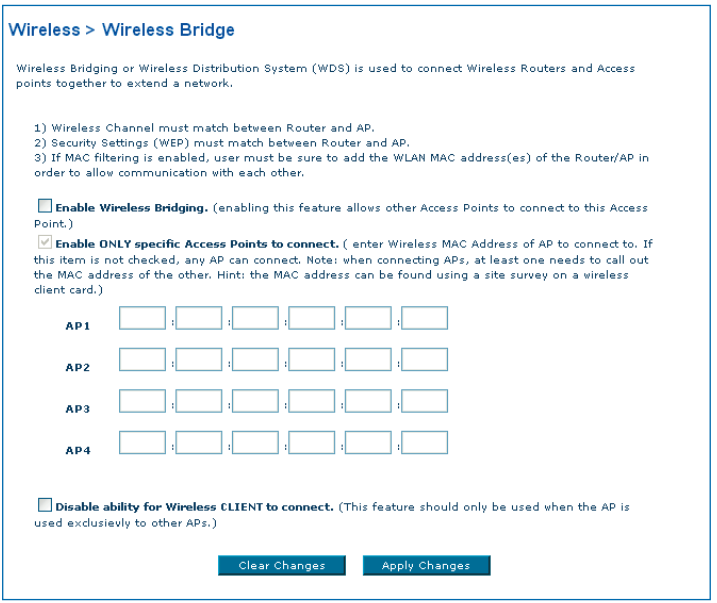


Impostazione di una connessione bridge tra il proprio router wireless ed un access point secondario

Per creare una connessione di tipo bridge tra il proprio router Belkin ed un access point secondario è necessario accedere alla utility di configurazione avanzata del router e digitare l'indirizzo MAC dell'access point nello spazio apposito. Si devono inoltre osservare alcune altre indicazioni. **ACCERTARSI DI SEGUIRE QUESTE FASI CON ATTENZIONE.**

1. Impostare il proprio access point sullo stesso canale del router. per ulteriori informazioni sulla variazione dei canali, vedere il capitolo "Canale wireless e SSID".
2. Trovare l'indirizzo MAC dell'access point sull'etichetta prevista sotto l'access point. Nell'etichetta sono riportati due indirizzo MAC. Fare riferimento all'indirizzo MAC "WLAN MAC Address". L'indirizzo MAC inizia con 0030BD ed è seguito da altri sei numeri o lettere (ad es. 0030BD-XXXXXX). Scrivere di seguito l'indirizzo MAC. Passare alla fase successiva.

3. Posizionare l'access point secondario entro il raggio di azione del router wireless e vicino all'area dove si desidera estendere la portata o aggiungere il segmento di rete. Normalmente, la portata in un ambiente chiuso dovrebbe essere compresa tra 30 e 70 metri circa.
4. Collegare l'access point alla fonte di alimentazione. Accertarsi che l'access point sia acceso e procedere alla fase successiva.
5. Da un computer già collegato al router, accedere alla utility di configurazione avanzata aprendo il proprio browser. Nella barra indirizzi digitare "192.168.2.1". Non digitare "www" o "http://" prima del numero. Nota: Se il proprio indirizzo IP del router è stato modificato, usare quell'indirizzo IP.
6. Nella finestra del browser compare l'interfaccia utente del router. Fare clic su "Wireless Bridge" (2) sul lato sinistro dello schermo. Si apre questa finestra.



7. Spuntare la casella che dice “Enable ONLY specific Access Points to connect” (Abilita alla connessione SOLTANTO access point specifici) (1).
8. Nel campo “AP1” (3), digitare l’indirizzo MAC del proprio access point secondario. Dopo aver inserito l’indirizzo, fare clic su “Apply Changes” (Esegui modifiche).
9. La connessione di tipo bridge è stata impostata.

Nota: Prima di stabilire la connessione di tipo bridge potrebbe trascorrere un minuto. In alcunic asi potrebbe essere necessario riavviare l’access point ed il router per poter avviare la connessione di tipo bridge.

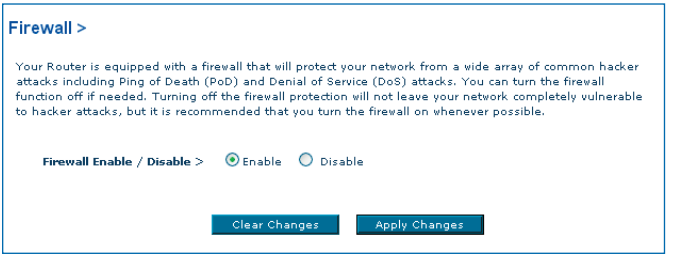
Firewall

Il router è dotato di una protezione firewall per proteggere la rete da una vasta

gamma di attacchi comuni degli hacker, tra cui:

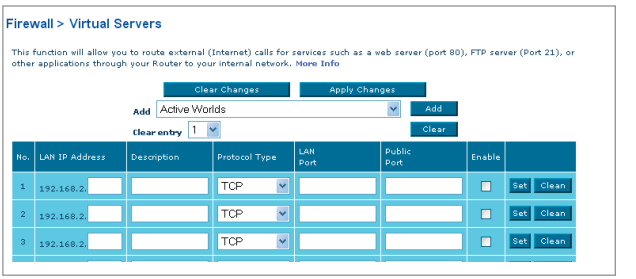
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

La protezione firewall inoltre maschera le porte comuni, che generalmente sono utilizzate per attaccare le reti. Queste porte appaiono “nascoste”, il che significa che un potenziale hacker non le rileva. Se necessario, la funzione di protezione firewall può essere disattivata, ma è consigliabile lasciarla attiva. Disattivando la protezione firewall, la rete non rimarrà completamente vulnerabile agli attacchi degli hacker, ma è comunque indicato lasciare la protezione firewall attiva.



Server virtuali

I server virtuali consentono di instradare eventuali richieste di servizio esterne (di Internet), tra cui le richieste di vari servizi come quello di un server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li “vedono”. Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell’applicazione per conoscere le impostazioni delle porte necessarie. Questa informazione può essere inserita nel router manualmente.



Scelta di un’applicazione

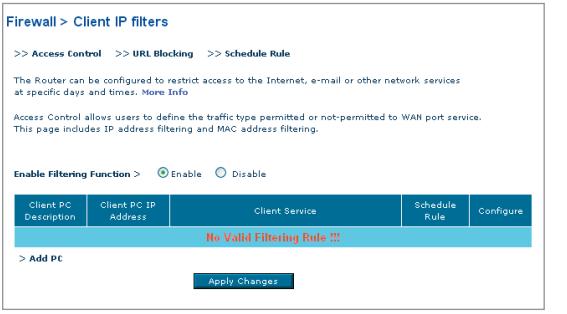
Selezionare la propria applicazione dall’elenco a discesa. Fare clic su “Add” (Aggiungi). Le impostazioni saranno trasferite nel successivo spazio disponibile nello schermo. Fare clic su “Apply Changes” (Esegui modifiche) per salvare le impostazioni per quella specifica applicazione. Per eliminare un’applicazione, selezionare il numero della riga che si desidera eliminare e fare clic su “Clear” (Cancella).

Immissione manuale delle impostazioni nel server virtuale

Per immettere manualmente le impostazioni, inserire l’indirizzo IP nello spazio previsto per la macchina interna (server), le porte da cui passare, selezionare il tipo di porta (TCP o UDP) e fare clic su “Apply Changes” (Esegui modifiche). Ciascuna voce relativa alle porte inbound prevede due campi di massimo 5 caratteri che consentono di stabilire un punto di partenza e di arrivo della portata ad es. [xxxxx]-[xxxxx]. Per ciascuna voce si può inserire un valore porta unico compilando i due campi con il medesimo valore (ad es. [7500]-[7500] oppure una vasta gamma di porte (ad es. [7500]-[9000]). Se si desidera utilizzare diversi valori porta unici o un insieme di range ed un solo valore, è necessario ricorrere ad un massimo di 20 voci (ad es. 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). È possibile passare soltanto attraverso una porta per ciascun indirizzo IP interno. L’apertura delle porte nella protezione firewall può comportare un rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un’applicazione specifica.

Filtri IP Client

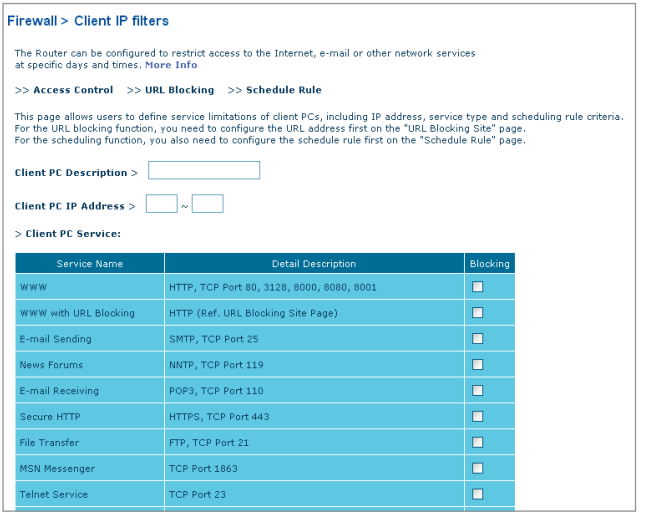
Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti. Il limite può essere impostato per un solo computer, una serie di computer o numerosi computer.



Controllo dell'accesso

Il controllo dell'accesso permette agli utenti di definire il traffico in uscita, sia esso consentito o negato, mediante l'interfaccia WAN. Per impostazione predefinita è permesso il traffico in uscita. Per limitare l'accesso ai computer, seguire il seguente procedimento:

1. Nella schermata "Access Control" (controllo dell'accesso) fare clic su "Add PC" (aggiungi un PC).
2. Stabilire le impostazioni corrette per i servizi del client PC (come indicato nella seguente schermata).



Firewall > Client IP filters

The Router can be configured to restrict access to the Internet, e-mail or other network services at specific days and times. More Info

>> Access Control >> URL Blocking >> Schedule Rule

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Description >

Client PC IP Address > ~

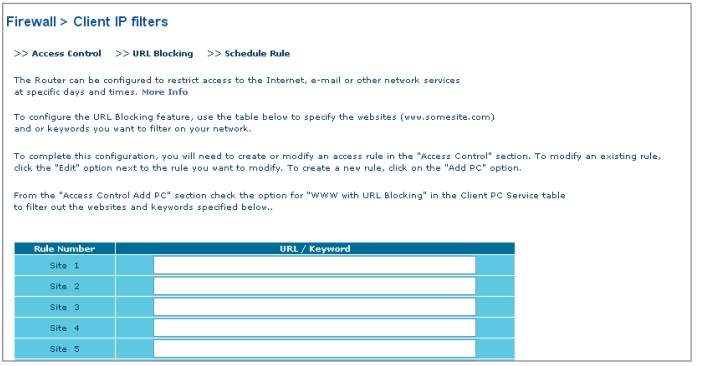
> Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	☐
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐

3. Fare clic su “OK” e, quindi, su “Apply Changes” (Esegui modifiche) per salvare le impostazioni.

Blocco di URL

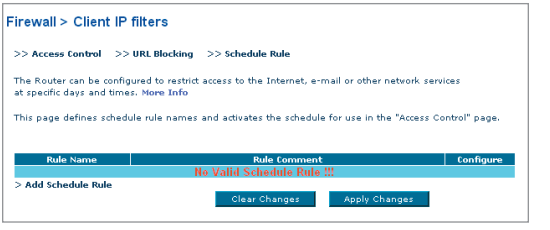
Per poter configurare il blocco URL, specificare i siti web (www.sitoweb.com) e/o le parole che si vuole filtrare dalla rete. Fare clic su “Apply Changes” (Esegui modifiche) per salvare la modifica. Per completare la configurazione bisognerà creare o modificare la regola dell’accesso nella sezione “Client IP filters”(Filtri IP Client).. Per modificare una regola esistente, fare clic sull’opzione “Edit” vicina alla regola che si vuol modificare. Per creare una nuova regola, fare clic su “Add PC”(Aggiungi PC). Dalla sezione “Access Control > Add PC” , apporre il segno di spunta accanto all’opzione “WWW with URL Blocking” (www con blocco URL) nella scheda “Client PC Service” per eliminare i siti web e le parole specificate.



Regola di pianificazione

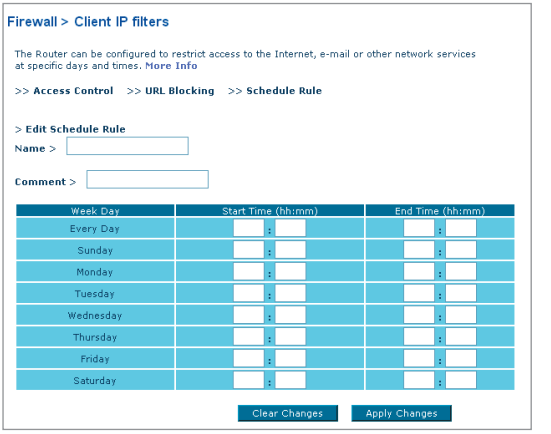
Si può filtrare l’accesso ad Internet per clienti locali servendosi delle regole. Ogni regola

per il controllo dell’accesso può essere pianificata. Stabilire l’orario nella regola “Schedule Rule” e applicarla nella pagina “Access Control”.



Per aggiungere un'altra pianificazione, seguire queste fasi.

1. Fare clic su "Add Schedule Rule" (Aggiungi pianificazione).
2. Si apre questa finestra.



3. Per configurare la regola di pianificazione, specificare il nome, il commento, l'orario di inizio e di fine del filtraggio della rete.
4. Fare clic su "OK" e, quindi, su "Apply Changes" (Esegui modifiche) per salvare le impostazioni.
5. Per completare la configurazione bisognerà creare o modificare la regola dell'accesso nella sezione "Client IP filters" (Filtri IP Client). In questo modo si attiva la pianificazione dell'accesso nella pagina "Access Control".

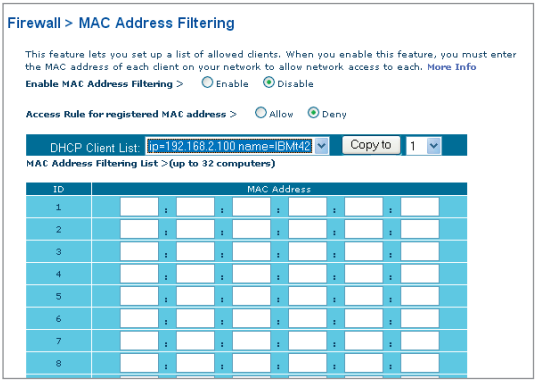
Impostazione del filtro indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. Sarà negato l'accesso a qualsiasi computer che dovesse tentare di accedere alla rete e che non fosse specificato nell'elenco dei filtri. Quando questa opzione viene attivata, per consentirne l'accesso alla rete, è necessario digitare l'indirizzo MAC di ogni client (computer) presente nella propria rete. L'opzione "Block" (Blocca) consente di disattivare ed attivare facilmente l'accesso alla rete per qualsiasi computer senza dover aggiungere e togliere l'indirizzo MAC del computer dalla lista.

Per attivare questa opzione, selezionare "Enable MAC Address Filtering" (Attiva filtro indirizzi MAC) (1). Successivamente, scegliere quale regola si vuole applicare: "Allow" (Permetti) o "Deny" (Nega).

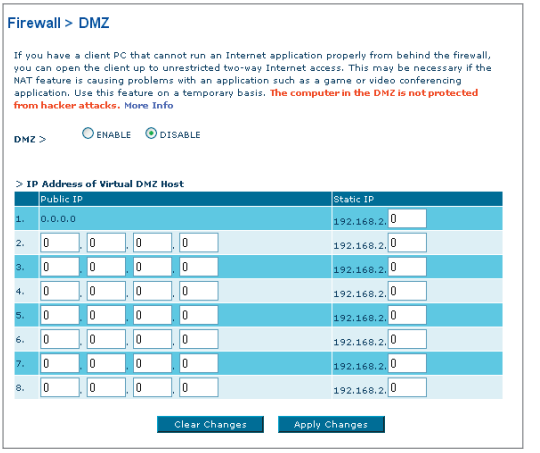
Quindi digitare l'indirizzo MAC di ogni computer, selezionandoli dall'elenco a discesa "DHCP client". Bisogna scegliere i computer ai quali si vuole garantire o negare l'accesso alla retee, quindi, fare clic su "copy to". Oppure si può fare clic nello spazio previsto (4) ed inserire l'indirizzo MAC del computer che si desidera aggiungere alla lista. Fare clic su "Apply Changes" (Esegui modifiche) (5) per salvare le impostazioni.

Per cancellare un indirizzo MAC dalla lista, è sufficiente fare clic su "Delete" (Cancella) accanto all'indirizzo MAC che si desidera eliminare. Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica. Nota: L'indirizzo MAC del computer utilizzato per accedere alle funzioni amministrative del router (il computer utilizzato in questo momento) non può essere cancellato.



DMZ (Demilitarized Zone)

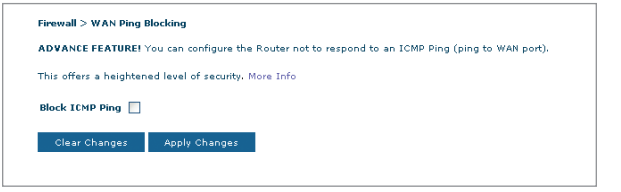
Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da dietro una protezione firewall, per il client è possibile aprire un accesso a Internet illimitato a due vie. Questa operazione potrebbe rivelarsi necessaria nel caso l'opzione NAT stesse causando problemi con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Questa opzione va sfruttata solo provvisoriamente. Il computer nella DMZ non è protetto dagli attacchi degli hacker.



Per inserire un computer nella DMZ, inserire le ultime cifre del suo indirizzo IP nel campo IP e selezionare “Enable” (Abilita). Fare clic su “Apply Changes” (Esegui modifiche) perché le modifiche abbiano effetto. Se si stessero utilizzando diversi indirizzi statici WAN IP, è possibile selezionare a quale indirizzo WAN IP dirigere l’host DMZ. Digitare l’indirizzo WAN IP al quale si desidera indirizzare l’host DMZ, digitare le ultime due cifre dell’indirizzo IP del computer host DMZ, selezionare “Enable” (Attiva) e fare clic su “Apply Changes” (Esegui modifiche).

Arresto di un Ping ICMP

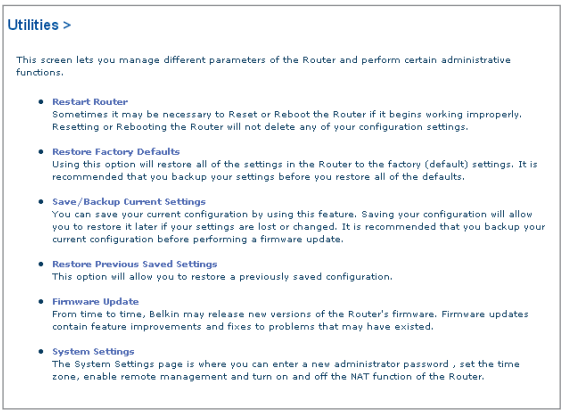
Gli hacker informatici utilizzano quello che è noto come “pinging” per scoprire le potenziali vittime in Internet. Colpendo uno specifico indirizzo IP e ricevendo una risposta da detto indirizzo IP, un hacker è in grado di stabilire se ci sia qualcosa di interessante o meno. Il router può essere impostato in modo da non rispondere ad un ping ICMP proveniente dall’esterno. In questo modo, il livello di protezione del proprio router aumenta.



Per disattivare la risposta al ping, selezionare “Block ICMP Ping” (Blocca ping ICMP) (1) e fare clic su “Apply Changes” (Esegui modifiche). Il router in questo modo non reagirà se colpito da un ping ICMP.

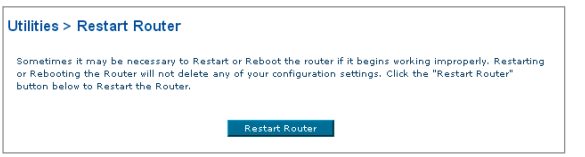
Utilities (Utility)

La schermata “Utilities” consente di gestire diversi parametri del router ed eseguire alcune specifiche funzioni amministrative.



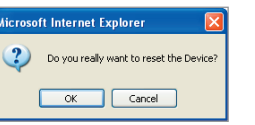
Riavvio del router

A volte, se inizia a funzionare in modo scorretto, può essere necessario riavviare il router. Se il router dovesse essere riavviato, le impostazioni di configurazione NON saranno cancellate.



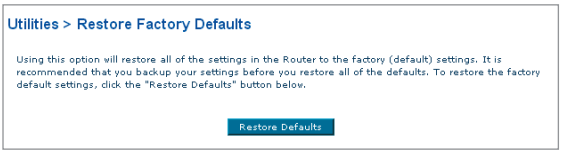
Riavvio del router per ripristinare il normale funzionamento

1. Fare clic sul pulsante “Restart Router” (Riavvia il router).
2. Compare il seguente messaggio. Fare clic su “OK” per riavviare il router.



Restore Factory Defaults (Ripristina impostazioni predefinite)

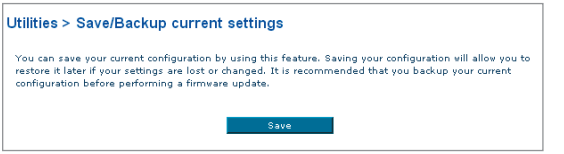
Con questa opzione si possono ripristinare tutte le impostazioni eseguite dal produttore del router. È consigliabile fare una copia di tutte le impostazioni prima di ripristinare quelle predefinite.



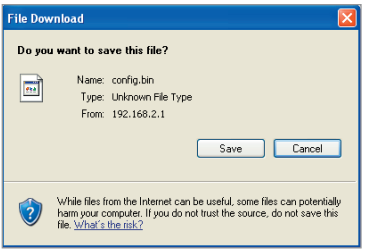
1. Fare clic sul pulsante “Restore Default” (Ripristina impostazioni predefinite).
2. Compare il seguente messaggio. Fare clic su “OK” per ripristinare le impostazioni predefinite.

Saving/Backup Current Settings (Salvataggio/Creazione di un copia di backup delle impostazioni correnti)

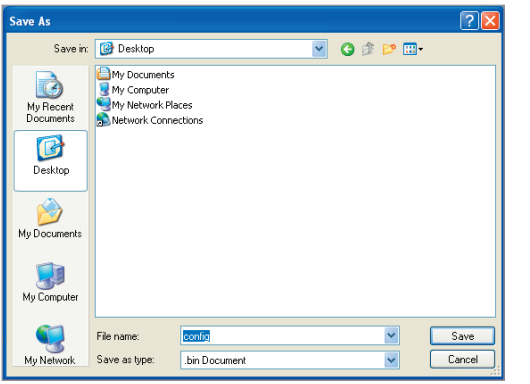
Questa opzione consente di salvare una configurazione corrente. Il salvataggio della propria configurazione consente di ripristinarla in un momento successivo nel caso le impostazioni andassero perdute o venissero modificate. È consigliabile fare una copia della configurazione corrente prima di eseguire un aggiornamento del firmware.



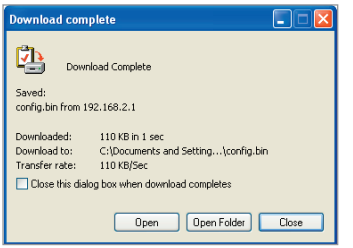
1. Fare clic su “Save” (Salva). Compare una finestra chiamata “File Download” (Scaricamento file). Fare clic su “Save” (Salva).



2. Si apre una finestra che consente di selezionare la posizione in cui salvare il file di configurazione. Selezionare una posizione. Non ci sono limiti rispetto al nome del file, tuttavia è necessario assegnare un nome che si è certi di ricordare anche in un momento successivo. Una volta selezionata la posizione ed il nome del file, fare clic su “Save” (Salva).



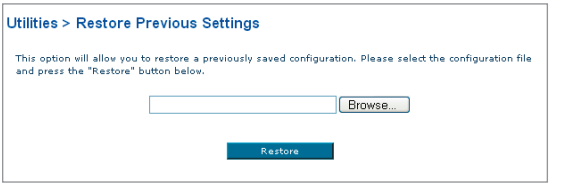
3. A salvataggio terminato, compare la finestra illustrata di seguito. Selezionare “Close” (Chiudi).



La configurazione è stata salvata.

Restore Previous Settings (Ripristina impostazioni precedenti)

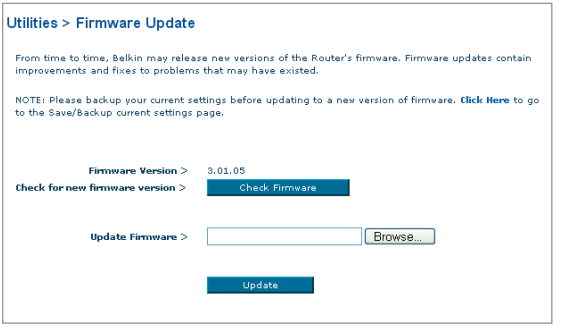
Questa opzione consente di ripristinare qualsiasi configurazione salvata in precedenza.



1. Fare clic su “Browse” (Sfoglia). Si apre una finestra che consente di selezionare la posizione del file di configurazione. Trovare il file di configurazione “config.bin” e fare doppio clic su di esso.
2. Quindi, fare clic su “Open” (Apri).

Aggiornamento del firmware

Di tanto in tanto, Belkin potrebbe pubblicare delle nuove versioni del firmware del router. Gli aggiornamenti del firmware contengono alcuni miglioramenti e consentono di risolvere possibili problemi esistenti nelle versioni precedenti. I nuovi firmware pubblicati da Belkin si possono scaricare dal sito Belkin, aggiornando in questo modo il firmware del router alla versione più recente.



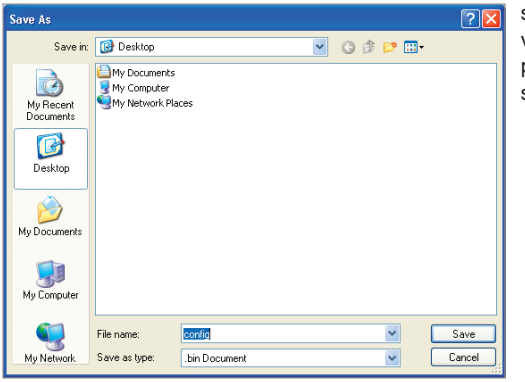
Controllo di una nuova versione del firmware

Il pulsante “Check Firmware” (Verifica firmware) (1) consente di verificare istantaneamente se esista una nuova versione del firmware. Facendo clic su questo pulsante, compare una nuova finestra di browser che informa che non è disponibile nessun nuovo firmware o che esiste una nuova versione. Se esiste una nuova versione, è necessario scaricarla.

Download di una nuova versione del firmware

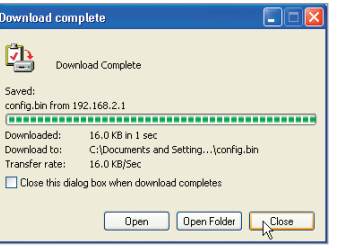
Facendo clic su “Check Firmware” (Verifica firmware), e se una nuova versione è disponibile, compare una schermata simile alla seguente.

1. Per scaricare la nuova versione di firmware, fare clic su “Download” (Scarica).
2. Si apre una finestra che consente di selezionare la posizione in cui salvare il file firmware. Selezionare una posizione. A questo file può essere assegnato qualsiasi nome si desideri, oppure si può utilizzare il nome predefinito. Accertarsi di collocare il file in una posizione tale da consentirne il ritrovamento in un momento successivo. Una volta selezionata la posizione, fare clic su “Save” (Salva).



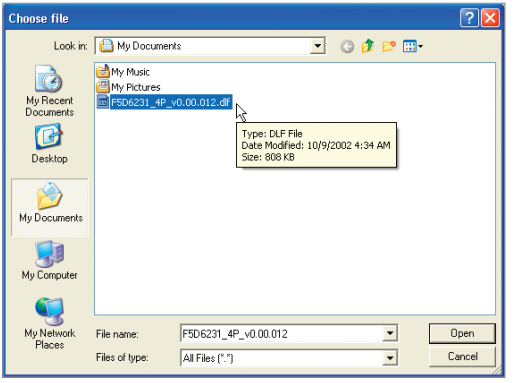
3. A salvataggio terminato, compare la finestra illustrata di seguito. Selezionare “Close” (Chiudi).

   Il download del firmware è terminato. Per aggiornare il firmware, seguire le indicazioni riportate di seguito in “Aggiornamento del firmware del router”.

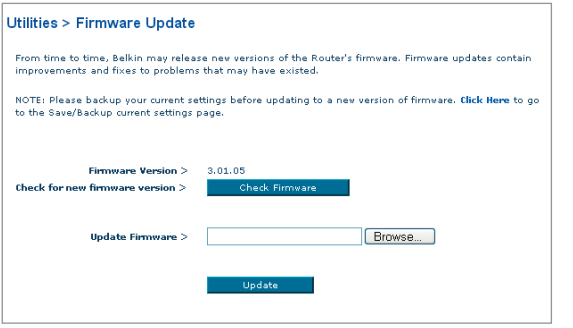


Aggiornamento del firmware del router

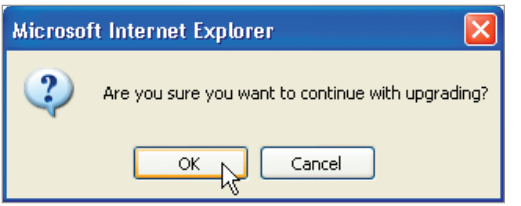
1. Dalla pagina “Firmware Update” (Aggiornamento firmware), fare clic su “Browse” (Sfoglia) (2). Si apre una finestra che consente di selezionare la posizione del file di aggiornamento firmware.



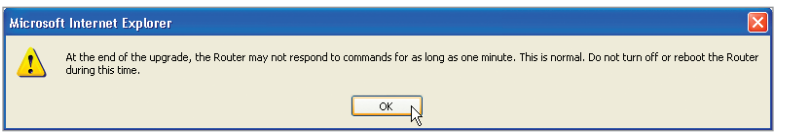
2. Andare al file di firmware scaricato. Selezionarlo facendo doppio clic sul nome del file.
3. La casella “Update Firmware” (Aggiornamento firmware) ora visualizza la posizione ed il nome del file di firmware appena selezionato. Fare clic su “Update” (Aggiorna).



4. Vi verrà chiesto se si è certi di voler continuare. Fare clic su “OK”.



5. Compare un ulteriore messaggio. Questo messaggio dice che il router potrebbe non rispondere per un massimo di un minuto, in quanto il firmware è stato caricato nel router ed il router viene riavviato. Fare clic su “OK”.



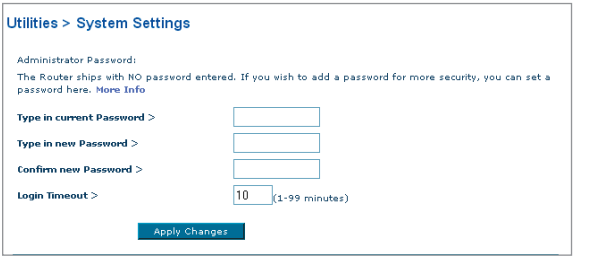
Sullo schermo compare un conto alla rovescia di 60 secondi. Quando il conto alla rovescia raggiunge lo zero, l’aggiornamento del firmware del router è completo. La home page del router dovrebbe apparire automaticamente. In caso contrario, digitare l’indirizzo del router (predefinito = 192.168.2.1) nella barra di navigazione del proprio browser.

System Settings (Impostazioni del sistema)

Nella pagina “System Settings” è possibile inserire una nuova password per l’amministratore, impostare il fuso orario, attivare la gestione a distanza ed attivare e disattivare la funzione UPnP del router.

Impostazione o modifica della password amministratore

Il router viene fornito senza alcuna password. Se si desidera impostare una password per avere una maggiore protezione, lo si può fare da qui. La password deve essere annotata e custodita in un posto sicuro, in quanto sarà necessaria per connettersi al router in futuro. È anche consigliabile inserire una password nel caso si intenda utilizzare l’opzione di gestione a distanza del router.



Modifica della durata di connessione

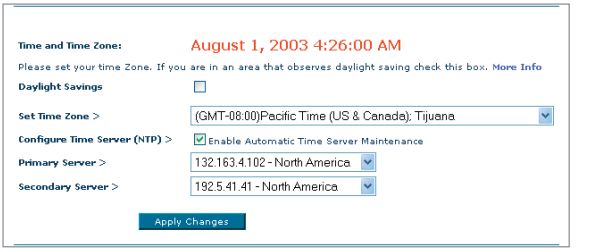
L'opzione di durata della connessione consente di impostare un intervallo di tempo di connessione all'interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all'interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su "Logout". Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Per apportare ulteriori modifiche sarà quindi necessario connettersi di nuovo al router. L'opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti.

Nota: è possibile connettere all'interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Impostazione dell'ora e del fuso orario

Il router mantiene l'orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l'orologio del sistema con la rete Internet mondiale. L'orologio sincronizzato presente nel router viene utilizzato per registrare l'elenco di protezione e controllare il filtro client. Selezionare il fuso orario della propria regione di residenza. Se si risiede in un paese in cui è in vigore l'ora estiva, spuntare la casella accanto a "Automatically Adjust Daylight Saving". L'orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell'orario su Internet e riceva una risposta. L'utente non può impostare autonomamente l'orologio.

Viene data la possibilità di scegliere un server NTP primario e uno di backup per poter mantenere l'orologio del router sincronizzato con diverso server di orario su Internet. Dalle caselle a tendina scegliere il server NTP desiderato. Lasciarlo così come appare.



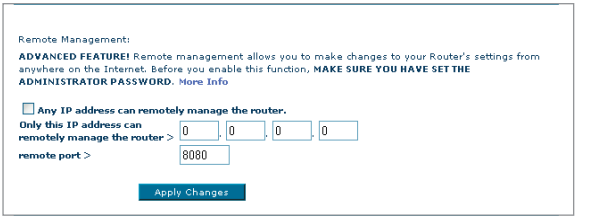
Attivazione della gestione a distanza

Prima di attivare questa funzione avanzata del router Belkin, **ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE**. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

Esistono due metodi per gestire a distanza il router. Il primo consente di accedere al router da qualsiasi punto di Internet selezionando “Any IP address can remotely manage the Router” (Qualsiasi indirizzo IP può gestire a distanza il router). Digitando il proprio indirizzo WAN IP da qualsiasi computer in Internet, compare una schermata di connessione nella quale è necessario digitare la password del proprio router.

Il secondo metodo consiste nel consentire ad uno specifico indirizzo IP di gestire soltanto a distanza il router. Questo metodo è più sicuro, ma meno comodo. Per utilizzare questo metodo, digitare l’indirizzo IP dal quale si sa di accedere al router nello spazio previsto e selezionare “Only this IP address can remotely manage the Router” (Soltanto questo indirizzo IP può gestire a distanza il router). Prima di attivare questa funzione è FORTEMENTE CONSIGLIATO aver impostato la propria password amministratore. Lasciando la password vuota, potenzialmente si apre il router ad eventuali intrusioni esterne.

Per impostazione predefinita la porta di accesso remoto è 8080. Si può scegliere un’altra porta digitando un nuovo numero nel campo “remote port” (porta remota).



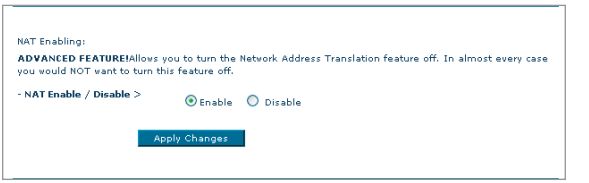
Fare clic su “Apply Changes” (Esegui modifiche) per salvare le proprie impostazioni.

Enabling/Disabling NAT (Network Address Translation) (Abilitazione / disabilitazione NAT)

Nota: questa funzione avanzata dovrebbe essere scelta soltanto dagli utenti esperti.

Prima di attivare questa funzione,
ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE.

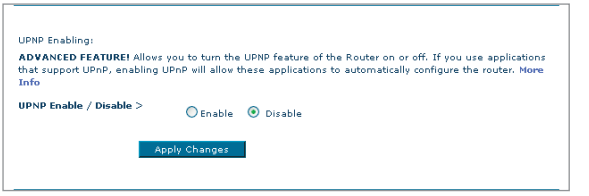
Il NAT (Network Address Translation) è il metodo attraverso il quale il router condivide un unico indirizzo IP assegnato dal proprio ISP con gli altri computer presenti nella rete. Utilizzare questa funzione soltanto se l'ISP assegna all'utente diversi indirizzi IP o se si desidera che l'opzione NAT venga disattivata per una configurazione avanzata del sistema. Se si ha un solo indirizzo IP e si disattiva l'opzione NAT, i computer all'interno della rete non sono in grado di accedere ad Internet. Si potrebbero verificare anche altri problemi. La disattivazione dell'opzione NAT disattiva le funzioni della protezione firewall.



Abilitazione / disabilitazione del servizio UPnP

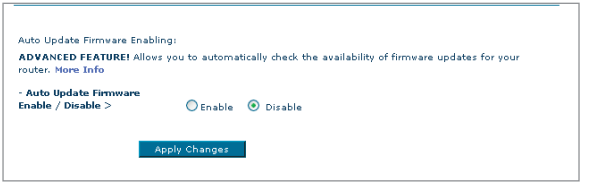
Il servizio UPnP (Universal Plug-and-Play) è un'altra opzione avanzata messa a disposizione dal router Belkin. Si tratta di una tecnologia in grado di offrire un funzionamento diretto delle opzioni di trasmissione di messaggi vocali, video, giochi ed altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. Per farlo è generalmente necessario aprire le porte TCP e UDP e, in alcuni casi, impostare le porte trigger. Un'applicazione conforme al servizio UPnP ha la capacità di comunicare con il router,

fondamentalmente "dicendo" al router come configurare la protezione firewall. Il router viene fornito con l'opzione UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste si possono attivare. È sufficiente selezionare "Enable" (Abilita) nella sezione "UPnP Enabling" (Abilitazione UpnP) della pagina "Utilities" (Utility). Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica.



Abilitazione / disabilitazione del servizio Auto Firmware Update

Questa novità mette a disposizione del router la capacità integrata di ricercare automaticamente una nuova versione di firmware ed avvisare l'utente della disponibilità del nuovo firmware. Nel momento in cui avviene la connessione con l'interfaccia utente avanzata basata sul web del router, il router esegue un controllo per verificare la disponibilità di nuovo firmware. In questo caso, si viene avvisati. È possibile scegliere se scaricare la nuova versione o ignorarla. Il router viene fornito con questa opzione disabilitata. Per abilitarla, selezionare "Enable" (abilita) e fare clic su "Apply Changes" (Esegui modifiche).

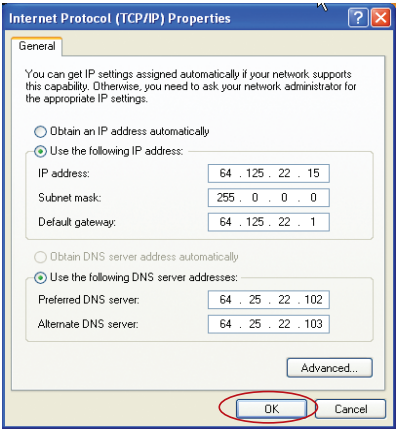


Per consentire al computer di comunicare correttamente con il router, è necessario modificare le impostazioni “TCP/IP Ethernet” e impostarle su “Obtain an IP address automatically/Using DHCP” (Ottieni un indirizzo IP automaticamente/Utilizzando DHCP). Si tratta dell’impostazione normalmente predefinita nella maggior parte dei computer d’uso domestico.

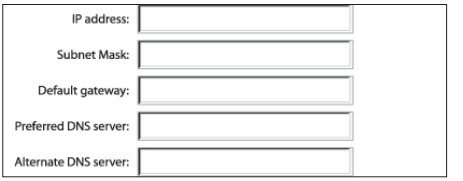
INNANZITUTTO, impostare il computer collegato al modem ADSL seguendo queste fasi. Le medesime operazioni si possono eseguire anche per aggiungere altri computer al router dopo averne impostato il collegamento ad Internet.

Configurazione manuale degli adattatori di rete in Windows 2000, NT o XP

1. Fare clic su “Start”, “Settings” (Impostazioni) e quindi su “Control Panel” (Pannello di controllo).
2. Fare doppio clic sull’icona “Network and dial-up connections” (Connessione di rete ed accesso remoto) (Windows 2000) o sull’icona “Network” (Rete) (Windows XP).
3. Fare clic con il tasto destro del mouse sull’opzione “Local Area Connection” (Connessione locale) associata alla propria scheda di rete e selezionare “Properties” (Proprietà) dal menu a tendina.
4. Dalla finestra “Local Area Connection Properties” (Proprietà connessione locale) fare clic su “Internet Protocol (TCP/IP) (Protocollo Internet (TCP/IP) e fare clic sul pulsante “Properties” (Proprietà). Compare la seguente schermata.



5. Se l'opzione "Use the following IP address" (Specifica l'indirizzo IP) (2) è selezionata, il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all'indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.

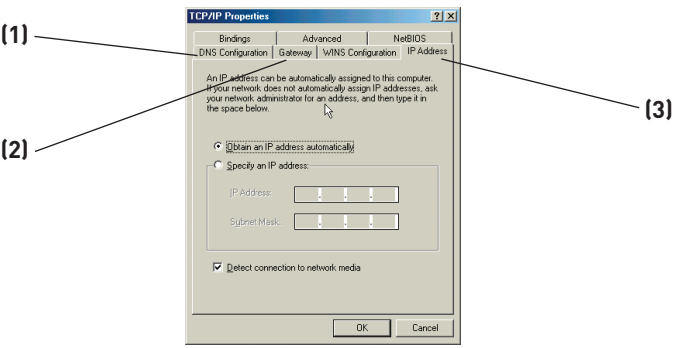


6. Se non fosse già selezionata, selezionare l'opzione "Obtain an IP address automatically" (Ottieni automaticamente un indirizzo IP) (3) e Obtain DNS server address automatically" (Ottieni automaticamente un indirizzo server DNS) (3). Fare clic su "OK".

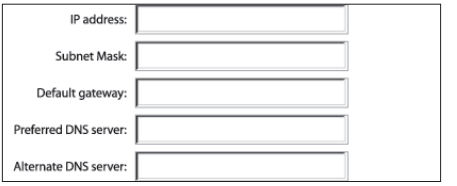
L'adattatore/i di rete è/sono ora configurato/ i per consentire l'utilizzo del router.

Configurazione manuale degli adattatori di rete in Windows 98SE o Me

1. Con il tasto destro del mouse, fare clic su “My Network Neighborhood” e selezionare “Properties” (Proprietà).
2. Selezionare “TCP/IP -> settings” (Impostazioni TCP/IP) per l’adattatore di rete installato. Si apre questa finestra.



3. Se è stata selezionata l’opzione “Specify an IP address” (Specifica l’indirizzo IP), il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



4. Annotare l'indirizzo IP e la subnet mask dalla scheda "IP Address" (Indirizzo IP) (3).
5. Fare clic sulla scheda "Gateway" (2). Trascrivere l'indirizzo gateway nella tabella.
6. Fare clic sulla scheda "DNS Configuration" (Configurazione DNS)(1). Trascrivere l'indirizzo (gli indirizzi) DNS nello schema.
7. Se non fosse già selezionata, selezionare l'opzione "Obtain an IP address automatically" (Ottieni automaticamente un indirizzo IP) (1) dalla scheda di indirizzo IP. Fare clic su "OK".

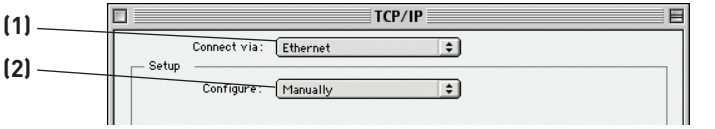
Riavviare il computer. Quando il computer verrà riavviato, gli adattatori di rete saranno configurati per essere utilizzati con il router.

INNANZITUTTO, impostare il computer collegato al modem via cavo o ADSL seguendo queste fasi. Le medesime operazioni si possono eseguire anche per aggiungere altri computer al router dopo averne impostato il collegamento ad Internet.

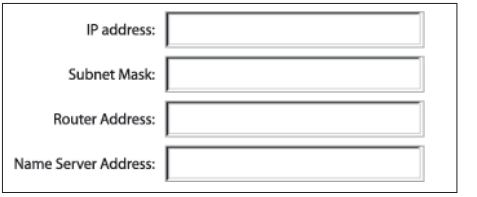
Configurazione manuale delle impostazioni degli adattatori nei sistemi operativi Mac OS fino alla versione 9.x

Per consentire al computer di comunicare correttamente con il router, è necessario modificare le impostazioni TCP/IP del computer Mac in DHCP.

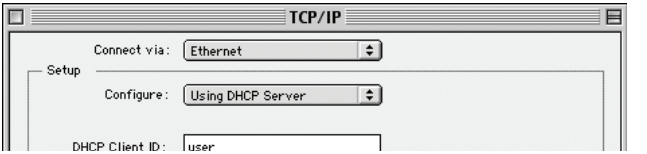
1. Aprire il menu “Apple” Selezionare dapprima “Control Panels”(Pannelli di controllo) e quindi “TCP/IP”.
2. Compare il pannello di controllo TCP/IP. Dal menu a tendina “Connect via” (Collega via), selezionare “Ethernet Built In” (Ethernet Integrato) o “Ethernet”. (1).



3. Accanto a “Configure” (Configura) (2), se è stato selezionato “Manually” (Manualmente), il router deve essere impostato per consentire una connessione IP statica. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



4. Se non fosse già impostato, in “Configure:” (Configura), selezionare “Using DHCP Server” (Utilizzando server DHCP). Questo indicherà al computer di ottenere un indirizzo IP dal Router.



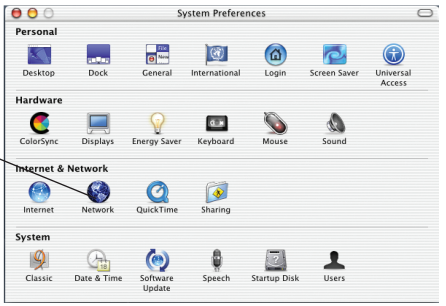
5. Chiudere la finestra. Nel caso fossero state fatte alcune modifiche, compare la seguente videata: Fare clic su “Save” (Salva).

Riavviare il computer. Quando il computer verrà riavviato, le impostazioni di rete saranno configurate per essere utilizzate con il router.

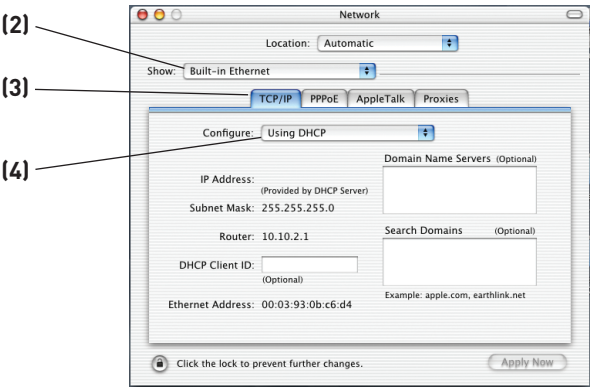
Configurazione manuale degli adattatori di rete nei sistemi operativi Mac

1. Fare clic sull'icona "System Preferences" (Preferenze del sistema).

2. Selezionare "Network" (Rete) (1) dal menu "System Preferences" (Preferenze del sistema).

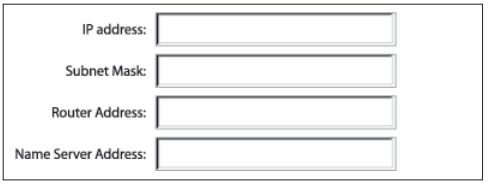


3. Selezionare "Built-in Ethernet" (2) accanto all'opzione "Show" (Mostra) nel menu Network (Rete).



4. Selezionare la scheda "TCP/IP" (3). Accanto a "Configure" (Configura) (4), dovrebbero comparire "Manually" (Manualmente) o "Using DHCP" (Utilizzando l'opzione DHCP). In caso contrario, verificare nella scheda PPPoE (5) che l'opzione "Connect using PPPoE" (Connetti utilizzando PPPoE) NON sia selezionata. Se lo fosse, il router deve essere configurato per un tipo di connessione PPPoE, usando il proprio nome utente e password.

5. Se è stato selezionato “Manually” (Manualmente), il router deve essere impostato in modo da eseguire un tipo di connessione IP statico. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



6. Se non fosse già selezionato, selezionare “Using DHCP Server” (Utilizzando server DHCP) accanto a “Configure” (Configura) (4), quindi fare clic su “Apply Now” (Esegui ora).

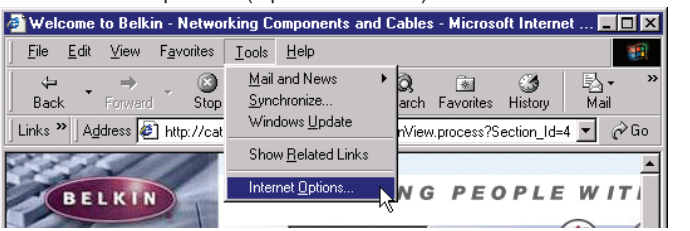
L’adattatore/i di rete è/sono ora configurato/i per consentire l’utilizzo del router.

Impostazioni del browser web consigliate

Nella maggior parte dei casi non è necessario eseguire molte modifiche alle impostazioni del browser web. Nel caso l'accesso ad Internet o l'utilizzo dell'interfaccia utente avanzata basata sul web creassero qualche problema, modificare le impostazioni del browser in base alle impostazioni consigliate in questo capitolo.

Internet Explorer versione 4.0 o superiore

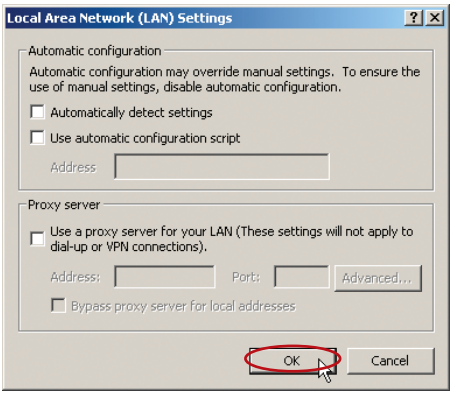
1. Avviare il browser Web. Selezionare "Tools" (Strumenti) e "Internet Options" (Opzioni Internet)



2. Nella schermata "Internet Options" (Opzioni Internet) compaiono tre selezioni. "Never dial a connection"(Non utilizzare mai connessioni remote), "Dial whenever a network connection is not present" (Usa connessione remota se non è disponibile una connessione di rete) e "Always dial my default connection" (Utilizza sempre la connessione remota predefinita). Se è possibile, selezionare "Non utilizzare mai connessioni remote". Nel caso non fosse possibile eseguire una selezione, passare alla fase successiva.

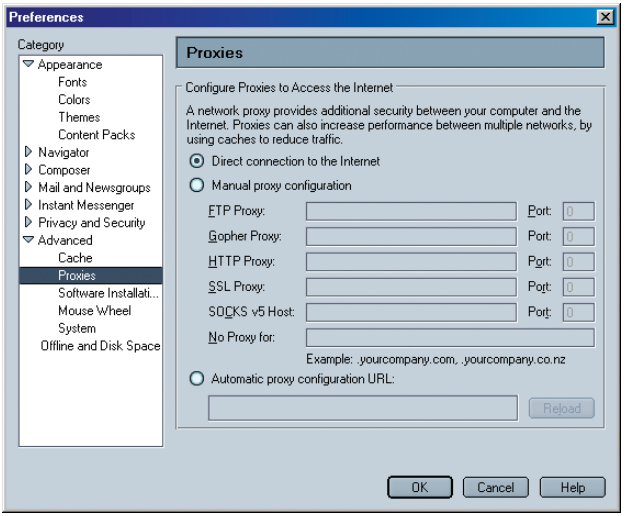
3. Nella finestra "Internet Options" (Opzioni Internet), cliccare su "Connections" (Connessioni) e selezionare "LAN Settings..." (Impostazioni LAN).

4. Accertarsi che non vi siano segni di spunta vicino a nessuna delle opzioni visualizzate: "Automatically detect settings" (Rileva automaticamente impostazioni) e "Use a proxy server" (Utilizza un server proxy). Fare clic su "OK". Ancora un clic nella pagina delle "Opzioni Internet".



Netscape Navigator versione 4.0 o superiore

1. Avviare Netscape. Clic su “Edit” (Modifica), quindi su “Preferences” (Preferenze).
2. Nella finestra delle preferenze, cliccare su “Advanced” (Avanzate), quindi selezionare “Proxies”. Nella finestra “Proxies”, selezionare “Direct connection to the Internet” (Connessione diretta a Internet).



Rilevazione e risoluzione delle anomalie

Problema:

Il LED ADSL è spento.

Soluzione:

1. Controllare lo stato della connessione tra il router e la linea ADSL. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata “DSL Line”.
2. Assicurarsi che il router sia alimentato. Il LED Power (Alimentazione) sul pannello anteriore dovrebbe essere illuminato.

Problema:

Il LED Internet è spento.

Soluzione:

1. Accertarsi che il cavo della linea ADSL sia collegato alla porta del router marcata “DSL Line” e che il LED ADSL sia acceso.
2. Accertarsi di aver ricevuto i parametri VPI/VCI, nome utente e password corretti dal proprio ISP.

Problema:

Il mio tipo di connessione prevede un indirizzo IP statico. Non riesco a connettermi a Internet.

Soluzione:

Se la vostra connessione prevede un indirizzo IP statico, il vostro ISP deve assegnarvi un indirizzo IP, una subnet mask e l’indirizzo gateway. Al posto di usare il programma di impostazione guidata, andare in “Connection Type” (Tipo di connessione) e selezionare il proprio tipo di connessione. Fare clic su “Next” (Avanti), selezionare “Static IP” (IP statico) e digitare il proprio indirizzo IP, la subnet mask e le informazioni relative al gateway predefinito.

Problema:

Ho dimenticato o smarrito la password.

Soluzione:

Premere per almeno 6 secondi il pulsante “Reset” sul pannello posteriore per ripristinare le impostazioni predefinite.

Problema:

Il mio PC wireless non riesce a collegarsi al router.

Soluzione:

1. Accertarsi che le impostazioni SSID del PC wireless siano le stesse del router e che le impostazioni di sicurezza, come ad esempio la crittografia WPA o WEP, siano uguali per tutti i client.
2. Accertarsi che il router e il PC wireless non siano troppo distanti tra loro.

Problema:

La rete wireless si interrompe spesso.

Soluzione:

1. Avvicinare il PC wireless al router per ottenere un segnale migliore.
2 Ci potrebbero essere anche alcune interferenze, causate da un forno a microonde o dai telefoni cordless da 2,4 GHz. Spostare il router o utilizzare un canale wireless diverso.

Problema:

Non riesco ad impostare un collegamento a Internet in modalità wireless.

Soluzione:

Se non si riesce a collegarsi ad internet da un computer wireless, si consiglia di controllare quanto segue:

1. Controllare le spie del router. Se si sta usando un Router Belkin, le spie dovrebbero essere così:
   - La spia “Power” (alimentazione) dovrebbe essere accesa.
   - La spia “Connected” dovrebbe essere accesa, non lampeggiante.
   - La spia “WAN” dovrebbe essere accesa o lampeggiare.
2. Aprire il software della utility wireless facendo clic sull’icona nel desktop di sistema nell’angolo in basso a destra dello schermo (l’icona può essere verde o rossa).

3. La finestra che si apre può cambiare secondo il modello della Scheda Wireless; tuttavia, una delle utility dovrebbe contenere un elenco con le “Available Networks”: le reti wireless disponibili alle quali è possibile collegarsi.

Il nome della rete wireless appare nei risultati?

Sì, il nome della mia rete è in elenco – passare alla soluzione dal titolo “Non riesco a collegarmi ad internet in modalità wireless, ma il nome della mia rete è in elenco”.

No, il nome della mia rete non è in elenco—passare alla soluzione delle anomalie dal titolo “Non riesco a collegarmi ad Internet in modalità wireless e il nome della mia rete non è in elenco”.

Problema:

Non riesco a collegarmi ad Internet in modalità wireless, ma il nome della mia rete è in elenco.

Soluzione:

Se il nome della rete appare nell’elenco “Available Networks”, seguire le seguenti indicazioni per collegarsi in modalità wireless:

1. Fare clic sul nome corretto della rete nell’elenco “Available Networks”.

   Se la protezione (crittografia) della rete è stata attivata, bisognerà digitare il codice di rete. Per ulteriori informazioni sulla protezione, vedere la pagina “Modifica delle impostazioni di protezione della rete wireless”.

2. In pochi secondi, l’icona di sistema nell’angolo in basso a sinistra dello schermo dovrebbe diventare verde, indicando la corretta connessione alla rete.

Problema:

Non riesco a collegarmi ad Internet in modalità wireless e il nome della mia rete non è in elenco.

Soluzione:

Se il nome corretto della rete non appare nell'elenco "Available Networks", seguire le seguenti indicazioni per risolvere il problema:

1. Se possibile, spostare provvisoriamente il computer a 1,5/3 m dal router. Chiudere la utility Wireless ed aprirla di nuovo. Se il nome corretto della rete ora appare nell'elenco "Available Networks", potrebbe trattarsi di un problema di copertura o di interferenza. Vedere i suggerimenti nell'allegato B intitolato "Considerazioni importanti per il posizionamento e la configurazione".
2. Se si sta usando un computer collegato al router mediante un cavo di rete (anziché in modalità wireless), assicurarsi che la funzione "Broadcast SSID" (Trasmetti SSID) sia abilitata. Questa impostazione può essere trovata nella pagina di configurazione wireless "Channel and SSID" (Canale e SSID).

   Se, dopo aver seguito queste istruzioni, non fosse ancora possibile accedere ad Internet, **contattare l'Assistenza Tecnica Belkin**.

Problema:

- Il livello delle prestazioni della rete wireless non è buono
- Il trasferimento dei dati a volte è lento.
- Il segnale è debole.
- Si incontrano difficoltà nell'impostare e/o mantenere una connessione con una rete VPN (Virtual Private Network).

Soluzione:

La tecnologia wireless è basata sulla tecnologia radio. Ciò significa che la connettività e la produttività tra i dispositivi diminuiscono quando la distanza tra questi aumenta. Altri fattori che possono causare un indebolimento del segnale (il metallo è generalmente l'indiziato numero uno) sono gli ostacoli quali muri e apparecchiature in metallo. Di conseguenza, la copertura tipica per i dispositivi wireless in un ambiente chiuso è compresa tra i 30 e i 60 metri. Inoltre, se ci si allontana ulteriormente dal router o dall'access point wireless, la velocità della connessione diminuisce.

Per determinare se i problemi wireless siano dovuti a fattori di copertura, provare a posizionare il computer a 1,5/ 3 metri di distanza dal router.

Cambiare il canale wireless - A seconda del traffico wireless locale e delle interferenze, cambiare il canale wireless della rete può migliorarne le prestazioni e l'affidabilità. Il canale predefinito del router è l'11, tuttavia, si possono scegliere altri canali, a seconda del paese nel quale ci si trova. Consultare il capitolo intitolato "Modifica del canale wireless" a pagina XX per le istruzioni su come scegliere altri canali wireless.

Limitazione della trasmissione dati wireless- Limitare la trasmissione dati può aiutare a migliorare la copertura wireless e la stabilità della connessione. La maggior parte delle schede di rete offre la possibilità di limitare la trasmissione dati. Per cambiare questa proprietà, andare sul pannello di controllo di Windows, aprire "Network Connections" (Connessioni di rete) e fare doppio clic sulla connessione della propria scheda wireless. Nella finestra di dialogo "Properties" (Proprietà), nella tabella "General" (Generale) selezionare il pulsante "Configure" (Configura) (gli utenti Windows 98 dovranno selezionare la scheda wireless nell'elenco e quindi fare clic su "Properties" (Proprietà), quindi fare clic su la tabella "Advanced" (Avanzate) e selezionare le caratteristiche di trasmissione. Le velocità di trasmissione delle schede di rete dei client wireless sono generalmente preimpostate, tuttavia si possono verificare periodiche disconnessioni quando il segnale wireless è troppo basso. Generalmente, le velocità di trasmissione più lente sono le più stabili. Provare varie velocità fino a trovare la migliore per la propria rete; notare che tutte le trasmissioni di rete disponibili dovrebbero essere accettabili per la navigazione in Internet. Per maggiori chiarimenti consultare il manuale della scheda wireless.

Problema:

Ho difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in un router o access point Belkin

Soluzione:

1. Collegarsi al router o all'access point wireless.
2. Aprire il browser web e digitare l'indirizzo IP del router o dell'access point wireless. (Il router è preimpostato su "192.168.2.1", l'access point 802.11g su "192.168.2.254").

Collegarsi al router cliccando il pulsante “Login” nell’angolo in alto a destra dello schermo. Viene richiesto di inserire una password. Se non fosse mai stata impostata alcuna password, lasciare il campo password in bianco e cliccare “Submit” (Inoltra).

3. Fare clic su “Wireless” sul lato sinistro dello schermo. Selezionare la scheda “Encryption” (Crittografia) o “Security” (Protezione) per accedere alla pagina delle impostazioni di sicurezza.
4. Selezionare “128-bit WEP” dal menu a tendina.
5. Dopo aver selezionato la propria modalità di crittografia WEP, si può digitare a mano la propria chiave esadecimale WEP, oppure si può digitare una frase di accesso nel campo “Passphrase” (Frase di accesso) e fare clic su “Generate” per creare una chiave WEP dalla frase di accesso. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora tutti i propri client vanno adattati a queste impostazioni. Una chiave esadecimale è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit è necessario inserire una chiave composta da 26 caratteri esadecimali.

   Ad esempio:

   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = chiave a 128 bit

6. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. La crittografia del router wireless è impostata. Ogni computer presente nella rete wireless deve essere configurato con le medesime impostazioni di protezione.

AVVERTENZA: Se si stesse eseguendo la configurazione del router o access point wireless da un computer con un client wireless, sarà necessario accertarsi che la protezione per questo client wireless sia ATTIVA. In caso contrario si perderà la connessione wireless.

Nota per gli utenti Mac: i prodotti originali Apple AirPort supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 possono supportare le modalità di crittografia a 64 o 128 bit. Verificare quale sia la versione utilizzata nel proprio prodotto Apple AirPort. Non potendo configurare la rete con una crittografia a 128 bit, provare una crittografia a 64 bit.

Problema:

Ho difficoltà nell'impostare la protezione Wired Equivalent Privacy (WEP) in una scheda wireless Belkin.

Soluzione:

La scheda wireless deve utilizzare la stessa chiave del router wireless o dell'access point. Ad esempio, se il router wireless o l'access point utilizza la chiave 00112233445566778899AABBCC, la scheda client deve essere impostata esattamente con la stessa chiave.

1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante "Advanced", appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda "Wireless Network Properties", selezionare un nome dall'elenco "Available networks" (Reti disponibili) e fare clic su "Properties" (Proprietà).
5. In "Data Encryption" (Crittografia dati), selezionare "WEP".
6. Disattivare la casella in basso "The key is provided for me automatically" (Fornisci automaticamente la chiave di rete). Se si usa il computer per collegarsi ad una rete aziendale, chiedere al proprio amministratore di rete se la casella deve essere attivata.
7. Digitare la chiave WEP nella casella "Network key" (Chiave di rete).

   Importante:una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, vanno inseriti 26 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

   Ad esempio:

   C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = codice a 128 bit
8. Fare clic su "OK" e, quindi, su "Apply" (Esegui) per salvare le impostazioni.

   Se NON si utilizza una scheda wireless Belkin, richiedere al produttore il manuale d'uso per la scheda client wireless utilizzata.

Problema:

I prodotti Belkin supportano la modalità WPA?

Soluzione:

Nota:per utilizzare la protezione WPA, tutti i client devono disporre dei driver e del software in grado di supportarla. Al momento della pubblicazione di questo elenco di domande e risposte, è possibile scaricare gratuitamente un security patch da Microsoft, adatto soltanto al sistema operativo Windows XP.

Il patch può essere scaricato dal sito:
http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en

Dal sito di assistenza Belkin è necessario anche scaricare il driver più recente per la propria scheda di rete wireless 802.11g per computer desktop o notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

Il driver più recente si può scaricare dal sito:
http://web.belkin.com/support/networkingsupport.asp

Problema:

Ho difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete domestica.

Soluzione:

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA-PSK (no server)".
2. Come tecnica di crittografia, scegliere "TKIP" o "AES". Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare la propria chiave precondivisa, che può essere composta da una combinazione di lettere, numeri o caratteri o spazi, da un minimo di 8 a un massimo di 63. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati. Ad esempio, la propria PSK potrebbe essere qualcosa del tipo: "Codice rete famiglia Rossi".

4. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Ho difficoltà nell’impostare la protezione Wi-Fi Protected Access (WPA) in un router o access point Belkin per una rete aziendale.

Soluzione:

Se la rete utilizza un server radius per distribuire le chiavi ai client, utilizzare questa impostazione. Questa soluzione viene generalmente utilizzata nell’ambiente lavorativo.

1. Dal menu a tendina “Security mode” (Modalità di protezione), selezionare “WPA-PSK (with server)”.
2. Come tecnica di crittografia, scegliere “TKIP” o “AES”. Questa impostazione dovrà essere identica per tutti i client configurati.
3. Digitare l’indirizzo IP del radius server nei campi “Radius Server”.
4. Digitare la chiave radio nel campo “Radius Key”.
5. Digitare l’intervallo chiave. L’intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
6. Fare clic su “Apply Changes” (Esegui modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Ho difficoltà nell’impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete domestica.

Soluzione:

I client devono utilizzare la stessa chiave del router wireless o dell’access point. Ad esempio, se la chiave nel router wireless o nell’access point è “Codice rete famiglia Rossi”, anche i client devono utilizzare la stessa chiave.

1. Fare doppio clic sull’ icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.

3. Dopo aver premuto il pulsante “Advanced”, appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda “Wireless Network Properties”, selezionare un nome dall’elenco “Available networks” (Reti disponibili) e fare clic su “Properties” (Proprietà).
5. In “Network Authentication” (Autenticazione di rete) selezionare “WPA-PSK (No Server)”.
6. Digitare la chiave WPA nella casella “Network key” (Chiave di rete).

   Importante:una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questo codice di rete deve essere uguale a quello assegnato al router wireless (o all’access point).
7. Fare clic su “OK” e, quindi, su “Apply” (Esegui) per salvare le impostazioni.

Problema:

Ho difficoltà nell’impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless Belkin per una rete aziendale.

Soluzione:

1. Fare doppio clic sull’ icona “Signal Indicator” per aprire la schermata “Wireless Network” (Rete wireless). Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
2. Il pulsante “Advanced” (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda.
3. Dopo aver premuto il pulsante “Advanced”, appare la Utility LAN Wireless Belkin. Questa utility consente di gestire tutte le opzioni della scheda wireless Belkin.
4. Nella scheda “Wireless Network Properties”, selezionare un nome dall’elenco “Available networks” (Reti disponibili) e fare clic su “Properties” (Proprietà).
5. In “Network Authentication” (Autenticazione di rete) selezionare “WPA”.
6. Nella scheda “Authentication” (Autenticazione), selezionare le impostazioni indicate dall’amministratore di rete.
7. Fare clic su “OK” e, quindi, su “Apply” (Esegui) per salvare le impostazioni.

Problema:

Ho difficoltà nell'impostare la protezione Wi-Fi Protected Access (WPA) in una scheda wireless NON Belkin per una rete domestica.

Soluzione:

Per le schede di rete wireless per computer desktop e notebook di altre marche, sprovviste del software WPA, si può scaricare gratuitamente un file da Microsoft chiamato "Windows XP Support Patch for Wireless Protected Access". Scaricare il patch da Microsoft ricercando nei dati base per Windows XP WPA.

Nota:il file messo a disposizione da Microsoft funziona soltanto con Windows XP. Attualmente gli altri sistemi operativi non sono supportati. È necessario accertarsi inoltre che il produttore della scheda wireless supporti la protezione WPA e di aver scaricato e installato il driver più recente dal suo sito.

Sistemi operativi supportati:

- Windows XP Professional
- Windows XP Home Edition

Attivazione dell'opzione WPA-PSK (senza server)

1. In Windows XP, fare clic su "Start > Control Panel (Pannello di controllo) > Network Connections (Connessioni di rete)".
2. Cliccando con il tasto destro del mouse sulla scheda "Wireless Networks" (Reti wireless) si aprirà la seguente schermata. Accertarsi che l'opzione "Use Windows to configure my wireless network settings" (Utilizza Windows per configurare le impostazioni di rete wireless) sia attivata.
3. Nella scheda "Wireless Networks" (Reti wireless), cliccare il pulsante "Configure" (Configura) e sarà visualizzata la seguente schermata.
4. Nel caso di una rete domestica o simile, selezionare "WPA-PSK" da "Network Administration" (Amministrazione rete).

   Nota: Selezionare "WPA (with radius server)" se si sta utilizzando il computer per collegarsi ad una rete aziendale che supporta un server di autenticazione come un server radius. Per ulteriori informazioni, rivolgersi all'amministratore di rete.

5. Selezionare "TKIP" o "AES" da "Data Encryption" (Crittografia dati). Questa impostazione deve essere identica a quella del router wireless o dell'access point configurato.
6. Digitare la propria chiave di crittografia nella casella "Network key" (Chiave di rete).

   Importante: Inserire la propria chiave precondivisa che può essere lunga da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.
7. Fare clic su "OK" per confermare le impostazioni.

Qual è la differenza tra 802.11b, 802.11g, 802.11a e Pre-N?

Attualmente vi sono quattro tipi di standard di rete wireless, che trasferiscono dati a velocità massime molto diverse tra loro. Ognuno di loro inizia per 802.11(x), nome dato loro dall' IEEE, l'ente responsabile della certificazione degli standard di rete. Lo standard di rete più comune, l'802.11b, trasferisce dati a 11 Mbps, gli standard 802.11a e 802.11g trasferiscono i dati a 54 Mbps e Pre-N a 108 Mbps. Pre-N, il precursore dell'imminente versione 802.11n promette velocità superiori a 802.11g e fino al doppio dell'area di copertura wireless. Per ulteriori informazioni vedere la tabella di seguito riportata.

Tabella di confronto wireless

Tecnologia wireless	802.11b	802.11g	802.11a	Pre-N Belkin
Velocità	11Mbps	54Mbps	54Mbps	108Mbps
Frequenza	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz	5 GHz- banda poco trafficata	I comuni dispositivi domestici, quali telefoni cordless e forni a microonde, potrebbero interferire con la banda, non provvista di licenza, da 2,4 GHz
Compatibilità	Compatibile con 802.11g	Compatibile con 802.11b	Incompatibile con 802.11b o 802.11g	Compatibile con 802.11g o 802.11b
Copertura	Dipende dall'interferenza-normalmente 30-60 metri al coperto	Dipende dall'interferenza-normalmente 30-60 metri al coperto	Meno interferenze - la copertura è generalmente di 15-30 metri	8 volte la copertura dello standard 802.11g
Uso	Esteso – ampliamento utilizzato	Si prevede un aumento della popolarità	Non molto usato dai consumatori-più usato negli ambienti di lavoro	Si prevede un aumento della popolarità

Assistenza tecnica Belkin

Per i più recenti aggiornamenti software o per qualsiasi dubbio riguardante l'installazione di questo prodotto, visitare il sito

www.belkin.com/networking

Allegato A: Glossario

Indirizzo IP

Per “Indirizzo IP” si intende l’indirizzo IP interno del router. Per accedere all’interfaccia di impostazione avanzata, digitare l’indirizzo IP nell’apposita barra indirizzi del browser. Questo indirizzo, se necessario, può essere modificato. Per modificare l’indirizzo IP, digitare il nuovo indirizzo IP e fare clic su “Apply Changes” (Esegui modifiche). L’indirizzo IP scelto dovrebbe essere un IP non instradabile. Esempi di indirizzi IP non instradabili sono:

192.168.x.x (dove x indica qualsiasi cifra tra 0 e 255)

10.x.x.x (dove x indica qualsiasi cifra tra 0 e 255)

Subnet Mask (Maschera di sottorete)

Alcune reti sono troppo grandi per consentire che il traffico scorra in tutte le loro parti. Queste reti devono essere suddivise quindi in sezioni più piccole, meglio gestibili, dette sottoreti. La subnet mask (maschera di sottorete) è l’indirizzo accompagnato da altre informazioni necessarie ad identificare la “sottorete”.

DNS

DNS è l’acronimo di Domain Name Server. Un “Domain Name Server” è un server presente in Internet che traduce gli URL (Universal Resource Links) come “www.belkin.com” in indirizzi IP. Molti ISP non richiedono l’immissione di questa informazione nel router. Se si utilizza un tipo di connessione IP statica, perché la propria connessione funzioni correttamente, potrebbe essere necessario inserire uno specifico indirizzo DNS ed un indirizzo DNS secondario. Se il proprio tipo di connessione fosse dinamico o PPPoE, è probabile che non sia necessario inserire un indirizzo DNS.

PPPoE (modalità router, per vari PC)

La maggior parte dei provider ADSL utilizza un tipo di connessione PPPoE. Nel caso si utilizzasse un modem ADSL per collegarsi ad Internet, il proprio ISP potrebbe utilizzare il tipo di connessione PPPoE per collegarsi al servizio. Il proprio tipo di connessione è PPPoE se:

1. Il proprio ISP ha fornito un nome utente ed una password per collegarsi ad Internet

2. Il proprio ISP ha fornito un software del tipo WinPOET o Enternet300 da utilizzare per collegarsi ad Internet
3. Per entrare in Internet, è necessario fare doppio clic su un'icona del desktop diversa da quella del proprio browser.

Per impostare il router in modo da utilizzare il servizio PPPoE, digitare il proprio nome utente e la password negli appositi spazi. Dopo aver inserito i propri dati, fare clic su "Apply Changes" (Esegui modifiche). Una volta eseguite le modifiche, l'indicatore "Internet Status" (Stato Internet), se il router è stato impostato correttamente, visualizzerà il messaggio "connection OK" (connessione OK).

PPPoE (modalità router, per vari PC)

Digitare le informazioni PPPoA negli appositi spazi e fare clic su "Next" (Avanti). Fare clic

Fare clic su "Apply" (Applica) per attivare le impostazioni.

1. User name (Nome utente) - Digitare il nome utente. (fornito dal proprio ISP).
2. Password - Digitare la propria password (fornita dal proprio ISP).
3. Retype Password (Ridigita password) - Confermare la password. (fornita dal proprio ISP).
4. VPI/VCI - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).

Disconnetti dopo X...

Questa opzione viene utilizzata per disconnettere automaticamente il router dall'ISP quando non vi sono attività in corso per un intervallo di tempo specifico. Ad esempio, posizionando un segno di spunta accanto a questa opzione e digitando "5" nello spazio riservato ai minuti, si farà in modo che il router si disconnetta da Internet dopo cinque minuti di inattività di Internet. Questa opzione dovrebbe essere utilizzata nel caso il servizio di Internet venga pagato a minuti.

Canale e SSID

Per cambiare il canale di funzionamento del router, selezionare il canale desiderato dal menu a discesa e selezionare il proprio canale. Fare clic su "Apply Changes" (Esegui modifiche) per salvare le impostazioni. È possibile modificare anche i parametri SSID. I parametri SSID sono l'equivalente del nome della rete wireless. I parametri SSID possono essere di qualsiasi tipo si desideri. In presenza di altre reti wireless nella propria area, assegnare alla propria rete wireless un nome univoco. Fare clic nella casella SSID e digitare un nuovo nome. Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica.

Trasmissione ESSID

Molte schede di rete wireless attualmente sul mercato prevedono una funzione detta “site survey”(analisi sito). Essa consente di esaminare attorno per rilevare qualsiasi rete disponibile e consentire al computer di selezionare la rete tramite la funzione di descrizione generale del sito. Questa condizione si verifica se l’SSID è impostato su “ANY” (QUALSIASI). Il router Belkin può bloccare questa ricerca casuale di una rete. Disattivando la funzione di trasmissione “ESSID Broadcast”, l’unico modo in cui un computer è in grado di entrare nella rete è tramite la propria SSDI impostata con il nome specifico della rete (WLAN ad esempio). Accertarsi di conoscere i propri parametri SSID (nome della rete) prima di attivare questa opzione. È possibile rendere la propria rete wireless quasi invisibile. Disattivando la trasmissione SSID, la rete non sarà rilevata. Naturalmente, disattivando la trasmissione SSID, la protezione aumenta.

Crittografia

Utilizzando la funzione di crittografia, la rete viene resa più sicura. Per proteggere i vostri dati, il router sfrutta la crittografia Wired Equivalent Privacy (WEP) e prevede due gradi di crittografia: a 64 bit e a 128 bit. La crittografia si basa su un sistema di chiavi. La chiave inserita nel computer deve corrispondere alla chiave del router ed esistono due modi per creare una chiave. Il più semplice consiste nel consentire al software del router di convertire una frase di accesso creata dall’utente in una chiave. Il metodo avanzato prevede l’inserimento manuale delle chiavi.

Server virtuali

Questa funzione consente di instradare eventuali richieste di servizio esterne (di Internet), tra cui quelli di server web (porta 80), server FTP (porta 21) o altre applicazioni attraverso il proprio router nella rete interna. Poiché i computer interni sono protetti da una protezione firewall, i computer di Internet non possono accedervi perché non li “vedono”. Se fosse necessario configurare una funzione di server virtuale per una specifica applicazione, si dovrà contattare il fornitore dell’applicazione per conoscere le impostazioni delle porte necessarie.

Per digitare manualmente le impostazioni, inserire l’indirizzo IP nello spazio previsto per la macchina interna, il tipo di porta (TCP o UDP) e la(e) porta(e) pubbliche da superare. Quindi selezionare “Enable” (Abilita) e fare clic su “Set” (Imposta). È possibile passare soltanto attraverso una porta per ciascun indirizzo IP interno. L’apertura delle porte nella protezione firewall può comportare un rischio per la sicurezza. Le impostazioni possono essere attivate e disattivate molto rapidamente. È consigliabile disattivare le impostazioni quando non si utilizza un’applicazione specifica.

Filtri IP Client

Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti. Il limite può essere impostato per un solo computer, una serie di computer o numerosi computer.

Blocco di URL

Per poter configurare il blocco URL, specificare i siti web (www.sitoweb.com) e/o le parole che si vuole filtrare dalla rete. Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica. Per completare la configurazione bisognerà creare o modificare la regola dell'accesso nella sezione "Client IP filters" (Filtri IP Client). Per modificare una regola esistente, fare clic sull'opzione "Edit" vicina alla regola che si vuol modificare. Per creare una nuova regola, fare clic su "Add PC"(Aggiungi PC). Dalla sezione "Access Control > Add PC" , apporre il segno di spunta accanto all'opzione "WWW with URL Blocking" (www con blocco URL) nella scheda "Client PC Service" per eliminare i siti web e le parole specificate.

Regola di pianificazione

Per configurare la regola di pianificazione, specificare il nome, il commento, l'orario di inizio e di fine del filtraggio della rete. Questa pagina definisce i nomi delle regole di pianificazione e attiva la pianificazione dell'accesso della pagina "Access Control".

Il filtro indirizzi MAC

Il filtro indirizzi MAC è un potente mezzo per specificare quali sono i computer che possono accedere alla rete. Sarà negato l'accesso a qualsiasi computer che dovesse tentare di accedere alla rete e che non fosse specificato nell'elenco dei filtri. Attivando questa funzione, è necessario inserire l'indirizzo MAC per ciascun client nella propria rete per consentire l'accesso della rete ad ognuno oppure copiare l'indirizzo MAC selezionando il nome del computer dal "DHCP Client List" (Elenco Client DHCP). Per attivare questa funzione, selezionare "Enable" (Abilita). Quindi, fare clic su "Apply Changes" (Esegui modifiche) per salvare le impostazioni.

DMZ

Se si ha un PC client che non è in grado di gestire adeguatamente un'applicazione Internet da dietro una protezione firewall, per il client è possibile aprire un accesso a Internet illimitato a due vie. Questa operazione potrebbe rivelarsi necessaria nel caso l'opzione NAT stesse causando problemi con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Questa opzione va sfruttata solo provvisoriamente. Il computer nella DMZ non è protetto dagli attacchi degli hacker. Per collocare il computer nella DMZ, digitare le ultime cifre del rispettivo indirizzo IP LAN

nel campo “Static IP” (IP Statico) e fare clic su “Apply Changes” (Esegui modifiche) affinché la modifica venga attivata. Se si dispone di un unico indirizzo IP pubblico (WAN), l’IP pubblico può essere lasciato su “0.0.0.0”. Se si stessero utilizzando diversi indirizzi pubblici (WAN) IP, è possibile selezionare a quale indirizzo pubblico (WAN) IP dirigere l’host DMZ. Digitare l’indirizzo pubblico (WAN) IP al quale si desidera indirizzare l’host DMZ, digitare le ultime due cifre dell’indirizzo IP del computer host DMZ e fare clic su “Apply Changes” (Esegui modifiche).

Password Amministratore

Il router viene fornito senza alcuna password. Se si desidera aggiungere una password per maggiore sicurezza, la password può essere impostata dall’interfaccia utente basata sul server del router. Conservare la password in un posto sicuro, in quanto sarà necessaria per accedere al router in futuro. È anche **VIVAMENTE CONSIGLIATO** inserire una password nel caso si intenda utilizzare l’opzione di gestione a distanza. L’opzione di durata della connessione consente di impostare un intervallo di tempo di connessione all’interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all’interfaccia di impostazione avanzata, il computer si gestirà da solo senza dover fare clic su “Logout”.

Supponendo che la durata di connessione sia stata impostata su 10 minuti, dopo 10 minuti di mancato utilizzo del computer, la sessione di connessione verrà interrotta. Per apportare ulteriori modifiche sarà quindi necessario connettersi di nuovo al router. L’opzione di durata della connessione è prevista a scopo cautelativo ed è preimpostata su 10 minuti. Va ricordato che è possibile connettere all’interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Orario e fuso orario

Il router mantiene l’orario collegandosi ad un server SNTP (Simple Network Time Protocol). In questo modo il router è in grado di sincronizzare l’orologio del sistema con la rete Internet mondiale. L’orologio sincronizzato presente nel router viene utilizzato per registrare l’elenco di protezione e controllare il filtro client. Selezionare il proprio fuso orario. Se si vive in una zona che osserva l’ora legale, inserire un segno di spunta nella casella accanto a “Enable Daylight Saving” (Attiva ora legale). L’orologio del sistema potrebbe non aggiornarsi immediatamente. Attendere almeno 15 minuti perché il router contatti i server dell’orario su Internet e riceva una risposta. L’utente non può impostare autonomamente l’orologio.

Gestione a distanza

Prima di abilitare questa funzione, **ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE.** La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

UPnP

Quella UPnP (Universal Plug-and-Play) è una tecnologia in grado di offrire un funzionamento diretto delle opzioni di trasmissione di messaggi vocali, video, giochi ed altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. Per farlo è generalmente necessario aprire le porte TCP e UDP e, in alcuni casi, impostare le porte trigger. Un'applicazione conforme al servizio UPnP ha la capacità di comunicare con il router, fondamentalmente "dicendo" al router come configurare la protezione firewall. Il router viene fornito con l'opzione UPnP disabilitata. Se si sta utilizzando una qualsiasi applicazione conforme al servizio UPnP, e si desidera utilizzare le opzioni UPnP, queste si possono attivare. È sufficiente selezionare "Enable" (Abilita) nella sezione "UPnP Enabling" (Abilitazione UpnP) della pagina "Utilities" (Utility). Fare clic su "Apply Changes" (Esegui modifiche) per salvare la modifica.

Allegato B: Considerazioni importanti per il posizionamento e l'installazione

Nota: alcuni dei fattori elencati di seguito possono pregiudicare le prestazioni della rete, tuttavia non ne impediscono il funzionamento. Se si dovessero avere dubbi circa l'efficienza della propria rete, il seguente elenco di controllo potrebbe rivelarsi utile.

1. Collocazione del router o dell'access point wireless

Posizionare il Router (or Access Point) Wireless, il punto di collegamento centrale della rete wireless, il più vicino possibile al centro della copertura dei dispositivi wireless.

Per ottenere la migliore connessione per i "client wireless"(ovvero, computer provvisti delle Schede di Rete Wireless per computer notebook, Schede di Rete per computer Desktop ed adattatori USB wireless Belkin):

- Assicurarsi che le antenne di rete del router wireless (o dell'access point) siano parallele e verticali (rivolte verso il soffitto). Se il router wireless (o l'access point) è in posizione verticale, puntare le antenne il più possibile verso l'alto.

- Negli edifici a più piani, posizionare il Router Wireless (o l'Access Point) su un pavimento che sia il più vicino possibile al centro dell'edificio. Ad esempio sul pavimento di un piano superiore.
- Non mettere il Router Wireless (o l'Access Point) vicino a telefoni senza filo da 2,4 GHz.

2. Evitare ostacoli e interferenze

Evitare di posizionare il router wireless (o l'acces point) vicino a dispositivi che possono trasmettere "interferenze", come nel caso dei forni a microonde. Tra gli oggetti che possono impedire la comunicazione wireless sono compresi:

- Frigoriferi
- Lavatrici e/o asciugabiancheria
- Armadietti metallici
- Acquari grandi
- Finestre verniciate con vernice a base metallica di protezione dai raggi UV

Se il segnale wireless dovesse sembrare più debole in alcuni punti, assicurarsi che oggetti di questo tipo non ostacolino il segnale tra i computer e il router (o l'access point) wireless.

3. Telefoni cordless

Se, dopo aver verificato i punti sopra riportati, la prestazione della rete wireless dovesse essere ancora scarsa e si ha un telefono cordless:

- Allontanare il telefono cordless dal Router (o dall'Access Point) Wireless e dai computer provvisti di tecnologia wireless.
- Staccare la spina e rimuovere la batteria da eventuali telefoni cordless che utilizzano la banda 2,4 GHz (consultare le informazioni del produttore). Se il problema si risolve, ciò era probabilmente dovuto ad un'interferenza del telefono.
- Se il telefono supporta la selezione dei canali, e se possibile, cambiare il canale sul telefono e scegliere il canale più lontano dalla rete wireless. Per esempio, spostare il telefono sul canale 1 e il Router Wireless (o Access Point) sull'11. Vedere il manuale utente per maggiori informazioni.
- Se necessario, passare ad un telefono cordless a 900 MHz o 5 GHz.

4. Scegliere il canale “più tranquillo” della propria rete wireless

Nei luoghi dove case e uffici sono vicini, quali palazzi o edifici con uffici, potrebbe esservi vicino una rete che entra in conflitto con la vostra.

Usare le capacità Site Survey (Analisi sito) della utility LAN wireless del proprio adattatore wireless per localizzare eventuali reti wireless disponibili (vedere il manuale di istruzioni dell’adattatore wireless) e spostare il router wireless (o access point) ed i computer su un canale che sia il più lontano possibile da altre reti.

Provare con più canali, in modo da individuare la connessione più chiara ed evitare in questo modo interferenze da altri telefoni cordless o da altri dispositivi di rete wireless.

Per i prodotti wireless Belkin, consultare l’opzione Site Survey e le informazioni sui canali wireless riportate nel manuale utente. Queste indicazioni dovrebbero consentire di ottenere la migliore copertura possibile con il router wireless (o l’access point). Per coprire un’area più estesa, si consiglia di usare il Range Extender/Access Point Wireless Belkin.

5. Connessioni sicure, VPN e AOL

Le connessioni sicure generalmente richiedono un nome utente ed una password e sono usate quando la sicurezza è importante. Le connessioni sicure comprendono:

- Le connessioni Virtual Private Network (VPN), spesso usate per il collegamento remoto ad una rete di un ufficio
- Il programma di America Online (AOL) “Bring Your Own Access” , che permette di usare AOL mediante la banda larga fornita da un altro servizio via cavo o DSL
- La maggior parte dei servizi bancari online
- Molti siti commerciali che richiedono un nome utente ed una password per accedere all’account

Le connessioni sicure si possono interrompere con la configurazione della gestione dell’alimentazione del computer, che le fa “addormentare”. La soluzione più semplice per evitare che questo accada consiste nell’effettuare nuovamente il collegamento riavviando il software VPN o AOL o eseguendo di nuovo il login nel sito protetto.

Un’alternativa è cambiare le configurazioni della gestione dell’alimentazione del computer, in modo da non farlo addormentare; tuttavia, ciò potrebbe non essere raccomandabile per i portatili. Per modificare le configurazioni della gestione dell’alimentazione in Windows, vedere in “Power Options” (Opzioni risparmio energia) nel pannello di controllo.

Se si dovessero ancora avere difficoltà con la connessione sicura, con VPN e AOL, rivedere i passi sopra riportati per assicurarsi di aver identificato il problema.

Allegato C: Tabella delle impostazioni per la connessione a Internet

La tabella della pagina successiva fornisce alcuni valori di riferimento per selezionare e configurare la connessione a Internet con la propria linea ADSL. Molti ISP utilizzano impostazioni diverse, a seconda della regione e dell'attrezzatura utilizzata. Si possono provare le impostazioni suggerite per gli ISP della propria regione, se non dovessero funzionare, rivolgersi al proprio ISP per ricevere i parametri specifici.

Nazione	Protocollo di connessione	VPI/VCI	Incapsulamento	ISP
Europa				
Francia	PPPoE	8/35	LLC	Vari
Germania	PPPoE	1/32	LLC	T-Online, vari
Olanda	1483 Bridged	0/35 0/32 0/34	LLC LLC LLC	BBNed, XS4all Versatel DHCP Baby XL, Tiscali (start/ Surf/ Family/ Live)
	PPPoA	8/48	VC MUX	KPN, Hetnet, HCCNet, Tiscali (lite/ Basis/Plus) Wanadoo
	PPPoA	0/32	VC MUX	Versatel PPP, Zonnet
	PPPoE	8/35	LLC	Vari
Belgio	PPPoA	8/35	LLC	Belgacom, Tiscali, Scarlet
Italia	PPPoE o PPPoA	8/35	VC MUX	TIN
Spagna	PPPoE oppure 1483 Bridged	8/32	LLC	Telefonica
Svezia	1483 Bridged	3/35	LLC	Telia
GB	PPPoA	0/38	VC MUX	BT, Freeserve, Tiscali, AOL*
Asia				
Australia	PPPoE o PPPoA	8/35	LLC	Vari
Nuova Zelanda	PPPoE o PPPoA	0/100	VC MUX	Vari
Singapore	PPPoE	0/100	LLC	SingNet, Pacific Internet

Dichiarazione FCC

DICHIARAZIONE DI CONFORMITÀ CON LE LEGGI FCC PER LA COMPATIBILITA' ELETTROMAGNETICA

Noi sottoscritti, Belkin Corporation, con sede al 501 West Walnut Street, Compton, CA 90220, dichiariamo sotto la nostra piena responsabilità che il prodotto,

F5D7632-4

, cui questa dichiarazione fa riferimento, è conforme alla sez.15 delle norme FCC. Le due condizioni fondamentali per il funzionamento sono le seguenti: (1) il dispositivo non deve causare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, comprese eventuali interferenze che possano causare un funzionamento anomalo.

Attenzione: esposizione a radiazioni in radiofrequenza

La potenza in uscita irradiata da questa periferica è molto inferiore rispetto ai limiti stabiliti dalla FCC riguardo l'esposizione alla radiofrequenza. Tuttavia, la periferica dovrà essere utilizzata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento.

Se il dispositivo viene collegato ad un'antenna esterna, questa deve essere posizionata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento. Per evitare la possibilità di un eventuale superamento dei limiti di esposizione alle radiofrequenze FCC, non è consentito avvicinarsi all'antenna di oltre 20 cm nel corso del suo normale funzionamento.

Informazione della Commissione Federale per le Comunicazioni

Questa attrezzatura è stata testata ed è risultata conforme ai limiti previsti per le periferiche digitali di classe B, in conformità alla Sezione 15 delle Regole FCC. Questi limiti hanno lo scopo di offrire una protezione ragionevole dalle interferenze dannose in un'installazione domestica. Questo dispositivo genera, utilizza e può emettere energia in radiofrequenza. Se questo dispositivo causasse interferenze dannose per la ricezione delle trasmissioni radiotelevisive determinabili spegnendo o riaccendendo l'apparecchio stesso, si suggerisce all'utente di cercare di rimediare all'interferenza ricorrendo ad uno o più dei seguenti provvedimenti:

- Cambiare l'orientamento o la posizione dell'antenna ricevente.
- Aumentando la distanza tra il dispositivo ed il ricevitore.
- Collegare il dispositivo ad una presa di un circuito diversa da quella cui è collegato il ricevitore.

- Consultare il rivenditore o un tecnico radio/TV specializzato.

Modifiche

Le indicazioni FCC prevedono che l'utente venga informato del fatto che eventuali variazioni o modifiche apportate a questo dispositivo non espressamente approvate da Belkin Corporation potrebbero annullare la facoltà dell'utente di utilizzare il dispositivo.

Canada- Industry Canada (IC)

L'apparecchio radio wireless di questo dispositivo è conforme alle indicazioni RSS 139 & RSS 210 Industry Canada. Questo apparecchio digitale di classe B è conforme allo standard canadese ICES-003. Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

Europa -Comunicato dell'Unione Europea

I prodotti radio con la sigla di avvertenza CE 0682 o CE sono conformi alla direttiva R&TTE (1995/5/EC) emessa dalla Commissione della Comunità Europea. La conformità a tale direttiva implica la conformità alle seguenti norme europee (tra parentesi sono indicati i rispettivi standard internazionali).

- EN 60950 (IEC60950) - Sulla sicurezza del prodotto
- EN 300 328 Requisiti tecnici per gli apparecchi radio
- ETS 300 826 - Esigenze generali EMC per dispositivi radio

Per stabilire il tipo di trasmettitore utilizzato, vedere la targhetta di identificazione del proprio prodotto Belkin. I prodotti con il marchio CE sono conformi alla Direttiva EMC (89/336/CEE) e alla Direttiva per la Bassa Tensione (72/23/CEE) emesse dalla Commissione della Comunità Europea. La conformità a tale direttiva implica la conformità alle seguenti norme europee (tra parentesi sono indicati i rispettivi standard internazionali).

- EN 55022 (CISPR 22) – Interferenze elettromagnetiche
- EN 55024 (IEC61000-4-2,3,4,5,6,8,11) – Immunità elettromagnetica
- EN 61000-3-2 (IEC610000-3-2) – Armoniche della linea di alimentazione
- EN 61000-3-3 (IEC610000) – Sfarfallio della linea di alimentazione
- EN 60950 (IEC60950) - Sicurezza del prodotto

I prodotti che contengono un trasmettitore radio presentano le etichette di avvertimento CE 0682 o CE,

e possono anche esibire il logotipo CE.

Garanzia limitata a vita sul prodotto di Belkin Corporation

Belkin Corporation garantisce a vita questo prodotto da eventuali difetti di materiale e lavorazione. Qualora venisse rilevata un'anomalia, Belkin provvederà, a propria discrezione, a riparare o sostituire il prodotto gratuitamente, a condizione che esso sia restituito entro il periodo di garanzia, con le spese di trasporto prepagate, al rivenditore Belkin autorizzato da cui è stato acquistato. Potrebbe venire richiesta la prova di acquisto.

Questa garanzia non sarà valida nel caso il prodotto fosse stato danneggiato accidentalmente, per abuso, uso inadeguato o non conforme, qualora fosse stato modificato senza il permesso scritto di Belkin, o nel caso il numero di serie Belkin fosse stato cancellato o reso illeggibile.

LA GARANZIA ED I RIMEDI DI CUI SOPRA PREVALGONO SU QUALSIASI ALTRO ACCORDO, SIA ORALE CHE SCRITTO, ESPRESSO O IMPLICITO. BELKIN DECLINA SPECIFICATAMENTE QUALSIASI OBBLIGO DI GARANZIA IMPLICITO COMPRESE, SENZA LIMITI, LE GARANZIE DI COMMERCIABILITÀ O IDONEITÀ AD UN PARTICOLARE SCOPO.

Nessun rivenditore, agente o dipendente Belkin è autorizzato ad apportare modifiche, ampliamenti o aggiunte alla presente garanzia.

BELKIN DECLINA QUALSIASI RESPONSABILITÀ PER EVENTUALI DANNI SPECIALI, ACCIDENTALI, DIRETTI O INDIRETTI IMPUTABILI AD UN'EVENTUALE VIOLAZIONE DELLA GARANZIA O IN BASE A QUALSIASI ALTRA TEORIA LEGALE, COMPRESI, MA NON SOLO, I CASI DI MANCATO GUADAGNO, INATTIVITÀ, DANNI O RIPROGRAMMAZIONE O RIPRODUZIONE DI PROGRAMMI O DATI MEMORIZZATI O UTILIZZATI CON I PRODOTTI BELKIN.

Alcuni Stati non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non fare al caso vostro. Questa garanzia consente di godere di diritti legali specifici ed eventuali altri diritti che possono variare di stato in stato.

BELKIN

Modem ADSL con Router Wireless G

Progettato per soddisfare le specifiche ADSL2+

BELKIN

www.belkin.com

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL,
Regno Unito
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin GmbH
Hanebergstrasse 2
80637 Monaco di Baviera,
Germania
+49 (0) 89 143405 0
+49 (0) 89 143405 100 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk,
Paesi Bassi
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt
Francia
+33 (0) 1 41 03 14 40
+33 (0) 1 41 31 01 72 fax

P74725it-A