BELKIN

Modem ADSL2+ con router G+ MIMO wireless

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

Assistenza tecnica Belkin
Europa: 00 800 223 55 460

P75125it

BELKIN

Modem ADSL2+ con router G+ MIMO wireless

Per collegare in rete diversi computer e condividere l'accesso a Internet in ADSL

Manuale d'uso

Connect Wider

802.11g G+ MIMO

F5D9630it4A

Indice

Introduzione

Grazie per aver scelto il Modem ADSL con Router Wireless G High-Speed Mode Belkin (il router). Con questo nuovo router sarà possibile condividere in pochi minuti la stessa connessione a 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".

I vantaggi di una rete domestica

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

- condividere la connessione ad alta velocità a Internet con tutti i computer di casa;
- condividere risorse, quali file e dischi rigidi, tra tutti i computer collegati alla rete domestica;
- Condividere una sola stampante tra tutta la famiglia;
- Condividere documenti, musica, video e fotografie digitali;
- Memorizzare, recuperare e copiare 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 installazione 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 ADSL2+ con Router G+ MIMO Wireless
- Cavo telefonico RJ11 - Grigio
- Cavo di rete RJ45 Ethernet - Giallo
- Microfiltro ADSL*
- Adattatore di corrente
- Manuale d'uso

*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) e un browser web 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

Impostazionidi connessione a Internet

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

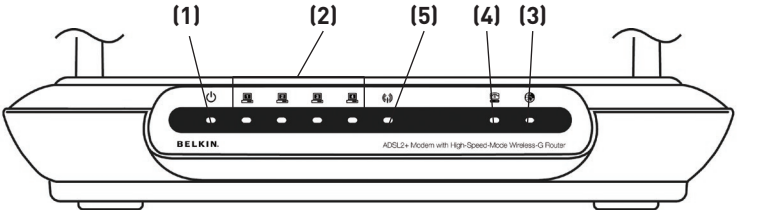
- Protocollo di connessione a Internet: _____ (PPPoE, PPPoA, IP dinamico, IP statico)
- Metodo Multiplexing o incapsulamento: _____ (LLC oppure VC MUX)
- Circuito virtuale: VPI (Virtual Path Identifier) _____ (un numero compreso tra 0 e 255)
- VCI (Virtual Channel Identifier) _____ (un numero compreso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

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

Conoscere il router

Il router è stato progettato per essere posizionato su una 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



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.

	OFF	Il router NON è attivo
	Verde	Il router è ATTIVO
	Rosso	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.

	OFF	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.

	OFF	WLAN è disattivata
	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.

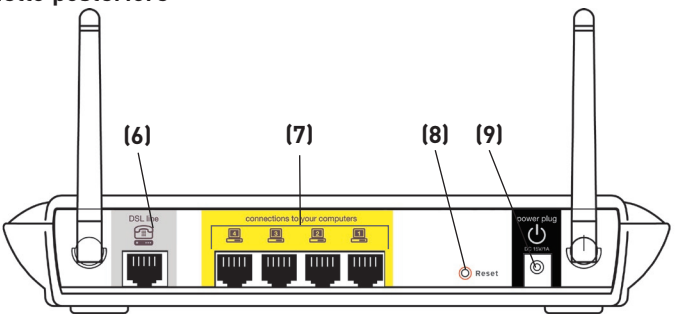
	OFF	Nessuna connessione ADSL
	Verde	Collegamento ADSL attivo
	Verde - lampeggiante	negoziazione della connessione

5. LED Internet

Il LED Internet segnala quando il router è collegato a 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.

	OFF	Nessuna connessione a Internet
	Verde	Connesso a Internet
	Verde - lampeggiante	Durante la trasmissione o la ricezione dei dati
	Rosso	Mancata ricezione dell'IP

Pannello posteriore



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

7. 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.

8. Pulsante di Reset
Il pulsante di Reset viene utilizzato in alcuni casi rari, quando il router non funziona correttamente. 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 alimentazione/pronto è di nuovo fissa, significa che l'operazione di reset è stata completata.

b. Ripristino delle impostazioni predefinite
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. Presa di alimentazione
Il cavo di alimentazione da 15V CC va collegato a questa presa. L'utilizzo di un tipo di adattatore di alimentazione sbagliato può danneggiare il router.

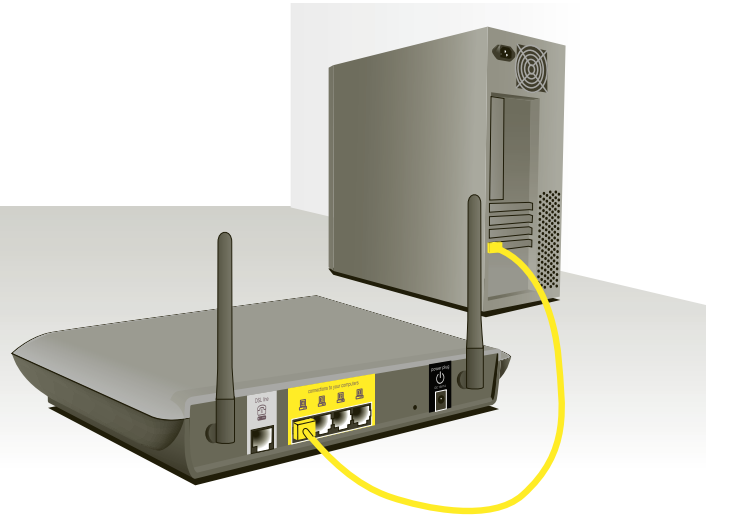
Collocazione del router

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 risoluzione dei problemi.

Collegamento dei computer

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



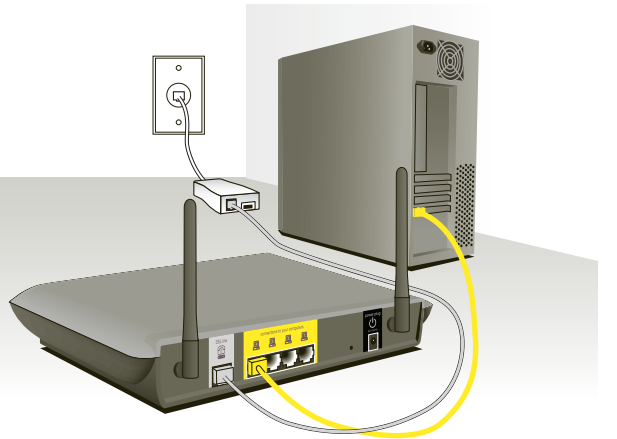
Collegamento della linea ADSL

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 bene: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 bene: un cavo telefonico RJ11 è compreso nella confezione. 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 portagrigia RJ11 etichettata “DSL line” sul retro del router.

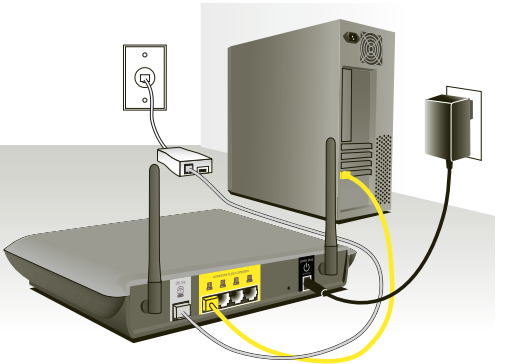
4. Se per il proprio servizio ADSL si dispone di una presa a muro RJ45, collegare un convertitore RJ45-RJ11 alla presa a muro. Quindi collegare un’estremità del cavo telefonico al convertitore e l’altra estremità alla porta grigiaRJ11 etichettata “DSL line” sul retro del router.

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

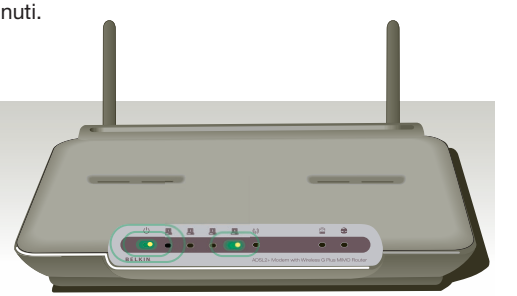
Accensione del router

1. Collegare l'adattatore di alimentazione fornito alla presa di corrente del router etichettata "Power".

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



2. 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.



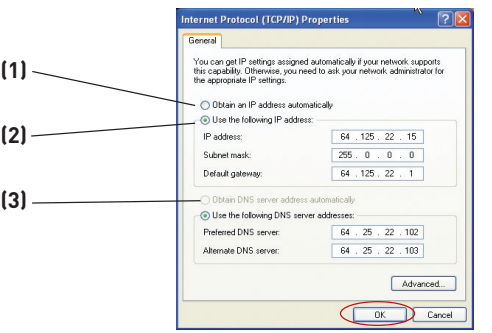
3. Accendere i computer. Dopo aver avviato i computer, si accederà un LED 💻 di indicazione di stato LAN sulla parte frontale del router per ciascuna porta alla quale è connesso un computer cablato. Queste spie servono ad indicare lo stato di connessione e attività. A questo punto si può procedere con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

Per consentire al computer di comunicare correttamente con il Router, è necessario modificare le impostazioni “TCP/IP Ethernet” e impostarle su “Ottieni automaticamente un indirizzo IP/Utilizza 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 stesse operazioni si possono eseguire anche per aggiungere altri computer al router dopo aver impostato il router in modo da collegarlo ad Internet.

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

1. Fare clic su “Start”, “Impostazioni” e quindi su “Pannello di controllo”.
2. Fare doppio clic sull’icona “Connessioni di rete e accesso remoto” (Windows 2000) o sull’icona “Rete e connessioni Internet (Windows XP).
3. Fare clic con il tasto destro del mouse sull’opzione “Connessione alla rete locale (LAN)” associata alla propria scheda di rete e selezionare “Proprietà” dal menu a tendina.
4. Dalla finestra “Proprietà connessione locale” fare clic su “Protocollo Internet (TCP/IP)”, quindi su “Proprietà”. Compare la seguente schermata.



5. Se l’opzione “Usa il seguente indirizzo IP” **(2)**è selezionata, il router deve essere impostato per un tipo di connessione IP statica. Scrivere le informazioni relative all’indirizzo riportate nella tabella in basso. Queste informazioni devono essere inserite nel router.

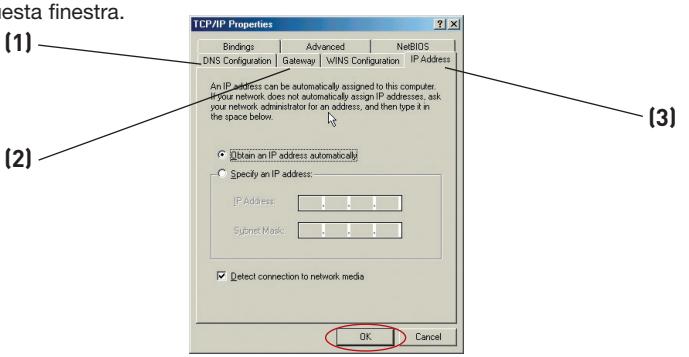
IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

6. Se non fosse già selezionata, selezionare l’opzione “Ottieni automaticamente un indirizzo IP” **(1)** e “Ottieni indirizzo server DNS automaticamente” **(3)**. Fare clic su “OK”.

L’adattatore di rete è ora configurato 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 “Risorse di rete” e selezionare “Proprietà”.
2. Selezionare “Impostazioni TCP/IP” per l’adattatore di rete installato. Si apre questa finestra.



3. Se l’opzione “Specifica l’indirizzo IP” 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.

IP address:	
Subnet Mask:	
Default gateway:	
Preferred DNS server:	
Alternate DNS server:	

4. Compilare i dati per l’indirizzo IP e la scheda di sottorete dalla scheda “Indirizzo IP” **(3)**.
5. Fare clic sulla scheda “Gateway” **(2)**. Trascrivere l’indirizzo gateway nella tabella.
6. Fare clic sulla scheda “Configurazione DNS” **(1)**. Trascrivere l’indirizzo (o gli indirizzi) DNS nella tabella.
7. Se non fosse già selezionata, selezionare l’opzione “Ottieni automaticamente un indirizzo IP” (1) dalla scheda di indirizzo IP. Fare clic su “OK”.
8. Per una corretta configurazione di connessione al router Belkin è necessario cancellare l’indirizzo gateway dalla scheda Gateway e i dati di configurazione DNS.

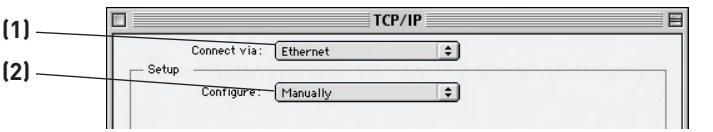
Riavviare il computer. Una volta riavviato il computer, gli adattatori di rete saranno configurati per essere utilizzati con il router.

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.

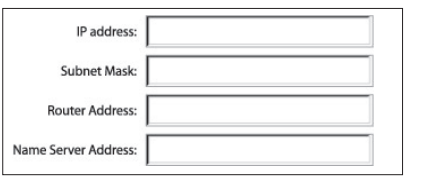
Configurazione manuale delle impostazioni degli adattatori nei sistemi operativi Mac OS fino alla versione 9.x

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

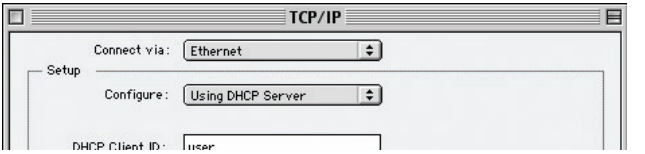
1. Aprire il menu “Apple”. Selezionare dapprima “Pannelli di controllo”, e quindi “TCP/IP”.
2. Compare il pannello di controllo TCP/IP. +Selezionare “Ethernet Built-In” (Ethernet Integrato) o “Ethernet” dal menu a tendina “Connetti tramite”. **(1)**.



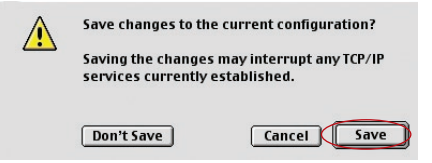
3. Accanto a “Configura” **(2)**, se è stato selezionato “Manualmente”, il router deve essere impostato per consentire una connessione IP statica. Scrivere le informazioni relative all’indirizzo nella tabella in basso. Queste informazioni devono essere inserite nel router.



4. Se non fosse già impostato, nella scheda “Configura”, selezionare “Utilizza 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).

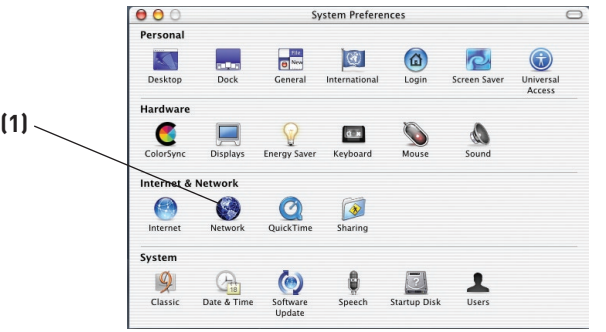


Riavviare il computer. Quando il computer verrà riavviato, le impostazioni di rete saranno configurate per essere utilizzate con il router.

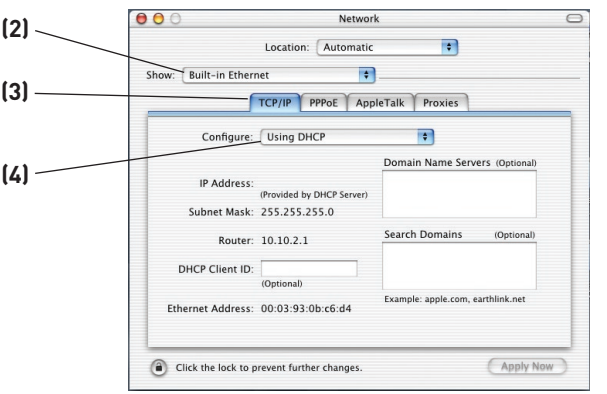
Configurazione manuale degli adattatori di rete nei sistemi operativi Mac

1. Fare clic sull'icona "Preferenze del sistema".

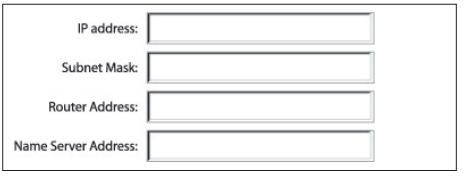
2.Selezionare "Rete" **(1)** dal menu "Preferenze del sistema".



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



4. Selezionare la scheda “TCP/IP” **(3)**. Accanto a “Configura” **(4)**, dovrebbero comparire “Manualmente” o “Utilizza DHCP”. In caso contrario, verificare nella scheda PPPoE **(5)** che l’opzione “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 “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.



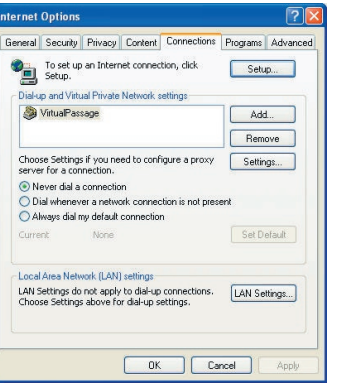
6. Se non fosse già selezionato, selezionare “Utilizza server DHCP” accanto a “Configura” **(4)**, quindi fare clic su “Applica ora”.

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

Impostazioni consigliate del browser web

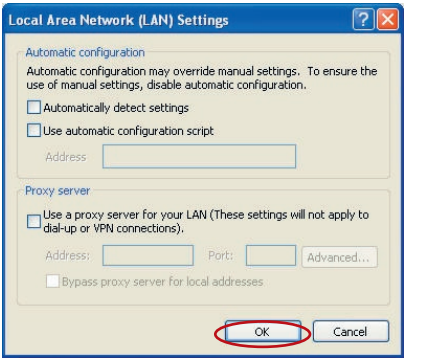
Nella maggior parte dei casi non è necessario eseguire molte modifiche alle impostazioni del browser web. Nel caso l'accesso ad Internet o l'utilizzo dell'interfaccia utente avanzata basata sul web creassero qualche problema, modificare le impostazioni del browser in base alle impostazioni consigliate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

Internet Explorer versione 4.0 o successive



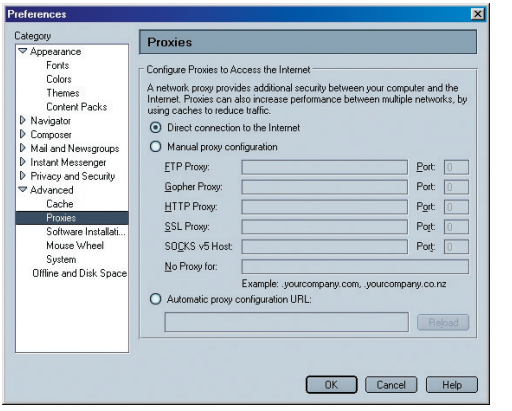
1. Avviare il browser Web. Selezionare "Strumenti" e "Opzioni Internet".
2. Nella schermata "Opzioni Internet" compaiono tre opzioni: "Non utilizzare mai connessioni remote", "Usa connessione remota se non è disponibile una connessione di rete" e "Utilizza sempre la connessione remota predefinita". Se è possibile, selezionare "Non utilizzare mai connessioni remote". Nel caso non fosse possibile eseguire una selezione, passare alla fase successiva.
3. Nella finestra "Opzioni Internet", cliccare su "Connessioni" e selezionare "Impostazioni LAN".

4. Accertarsi che non vi siano segni di spunta vicino a nessuna delle opzioni visualizzate: “Rileva automaticamente impostazioni” e “Utilizza un server proxy”. Fare clic su “OK”. Cliccare ancora su “OK” nella pagina delle “Opzioni Internet”.



Netscape Navigator versione 4.0 o successive

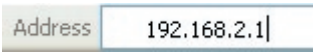
1. Avviare Netscape. Clic su “Modifica”, quindi su “Preferenze”.
2. Nella finestra delle preferenze, cliccare su “Avanzate”, quindi selezionare “Proxy”. Nella finestra “Proxy”, selezionare “Connessione diretta a Internet”.



Configurazione del router con il programma di installazione guidata

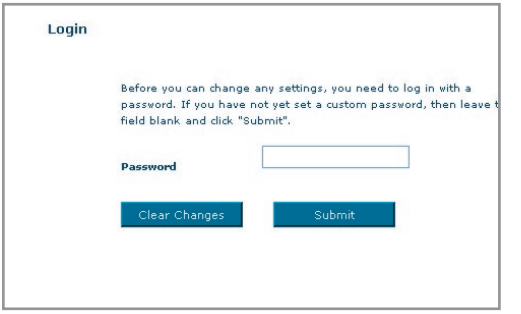
Esecuzione del programma di installazione guidata

1. Per accedere all'interfaccia utente di gestione del router basata sul web, utilizzare il browser web 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).



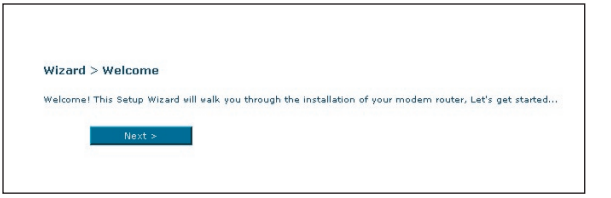
Nota bene: per la configurazione iniziale, si consiglia vivamente di utilizzare un computer fisicamente collegato al router tramite un cavo RJ45. Non è consigliabile utilizzare per la configurazione iniziale un computer collegato in modalità wireless.

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 connettersi.

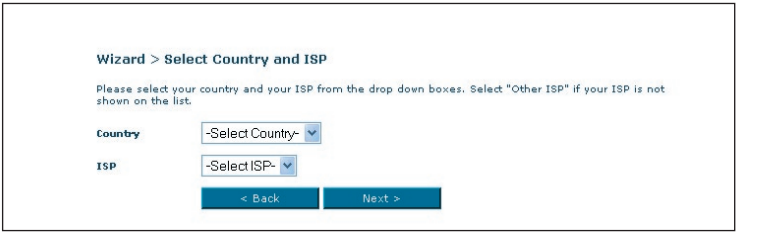


Nota bene:per maggiore sicurezza, si consiglia vivamente di cambiare la password. Per ulteriori informazioni su come cambiare la password e sulle altre opzioni di protezione, leggere la sezione intitolata "Configurazione manuale del router".

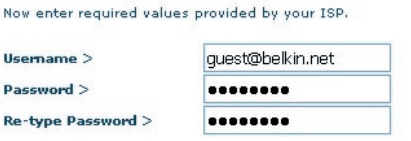
3. La procedura di installazione guidata sarà avviata automaticamente per eseguire la configurazione rapida (consigliata). Fare clic su “Next” (Avanti) per continuare.



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 A questo punto digitare negli spazi vuoti il nome utente e la password forniti dal proprio provider Internet (ISP). Per eseguire la connessione, il nome utente e la password devono essere inseriti con esattezza. Il provider Internet confermerà il nome utente e la password.



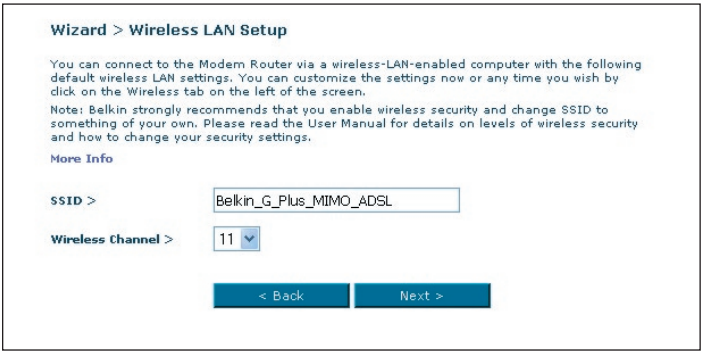
Nota bene: per istruzioni più dettagliate relative ad altri tipi di connessione, fare riferimento alla sezione intitolata “Configurazione manuale del router” di questo manuale.

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 = Belkin G+ MIMO ADSL

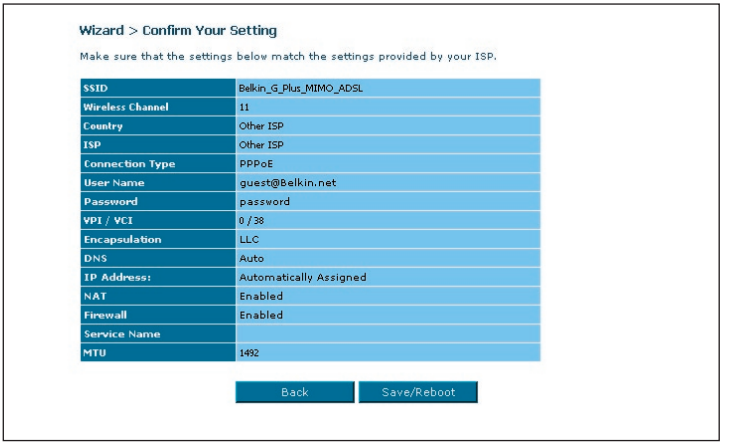
Canale Wireless = Auto

Protezione = disattivata



Nota bene: 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.

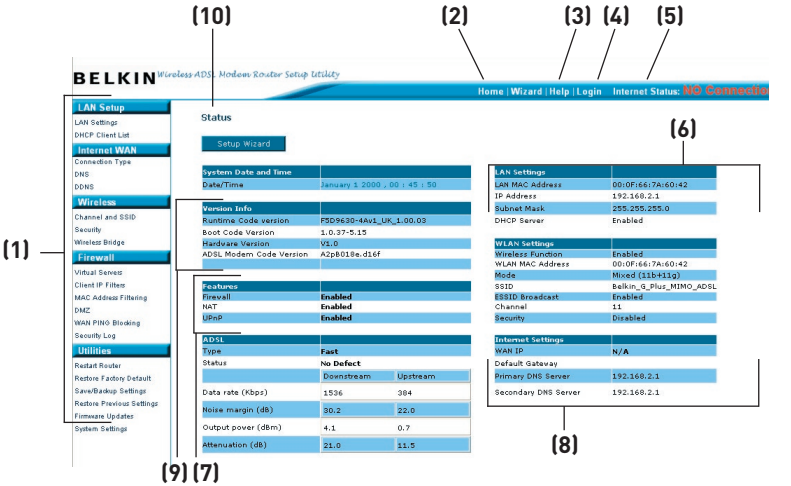
7. Controllare con attenzione le impostazioni riportate nella schermata successiva. Per modificare le impostazioni, fare clic su “Back” (Indietro) o fare clic su “Next” (Avanti) per confermarle.



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

Per una migliore comprensione dell'interfaccia utente avanzata 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. 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. Funzioni

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. Impostazioni Internet

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

9. Informazioni sulla versione

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

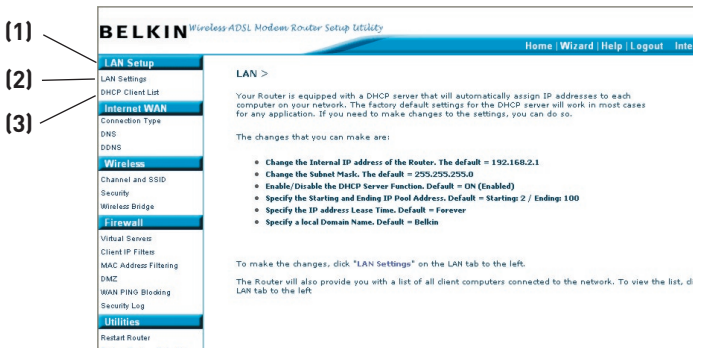
10. Nome della pagina

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 “Impostazioni LAN”.

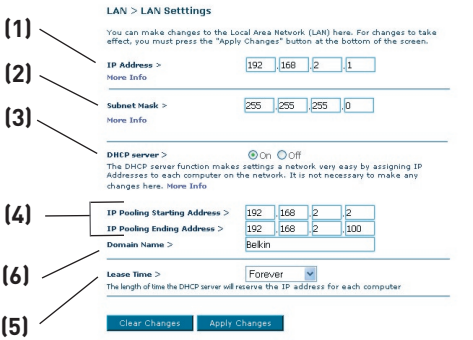
Modifica delle impostazioni LAN

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

Facendo clic sul titolo della scheda LAN **(1)** 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” **(2)** (Impostazioni LAN), o per visualizzare l’elenco dei computer collegati, fare clic su “DHCP client list” (Elenco client DHCP) **(3)**.



LAN Settings (Impostazioni LAN)



1. **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” (Applica 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. **Maschera di sottorete**

   Non è necessario modificare la subnet mask, in quanto il router imposterà automaticamente la lunghezza in base al tipo di indirizzo IP.

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” (disattivato) e fare clic su “Apply Changes” (Applica 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” (Applica 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

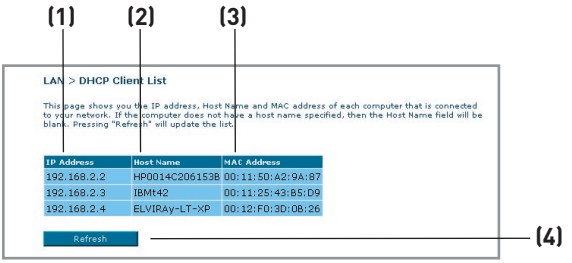
Per “lease time” si intende la durata dell’intervallo durante il quale il server DHCP mantiene riservato l’indirizzo IP per ogni computer. È consigliabile lasciare questo intervallo impostato su “Forever” (Per sempre). L’impostazione predefinita “Forever” (Per sempre) sta ad indicare che ogni volta che ad un computer verrà assegnato un indirizzo IP dal server DHCP, l’indirizzo IP per quel particolare computer non cambierà più. Impostando 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

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).

Elenco dei client DHCP

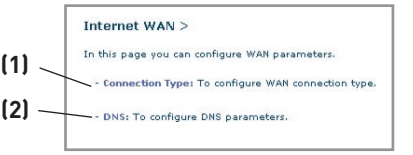
È possibile visualizzare un elenco dei computer (conosciuti come client) collegati alla rete. È possibile visualizzare l'indirizzo IP **(1)** del computer, il nome di host **(2)** (se al computer ne è stato assegnato uno), e l'indirizzo MAC **(3)** della scheda NIC (Network Interface Card). Premendo 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 "connection OK" (connessione OK).



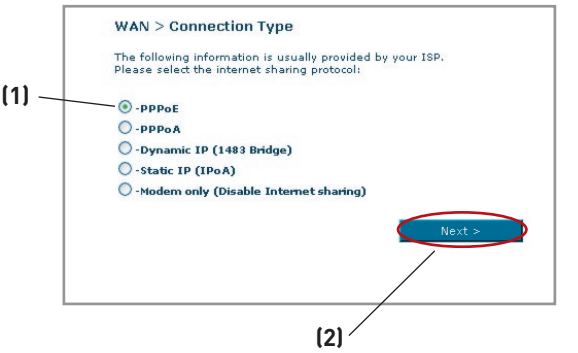
Tipo di connessione

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 (con bridging 1483)
- IP statico (IPOA)
- Soltanto modem (disattivare la condivisione Internet)

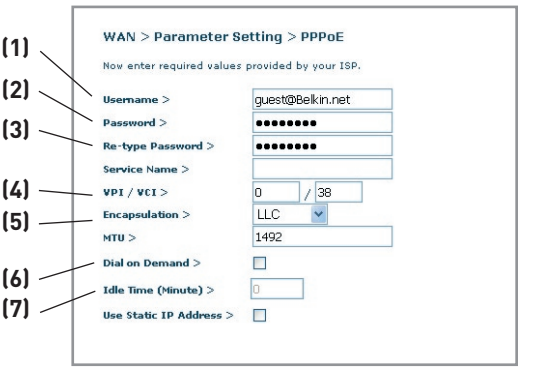
Nota bene: per conoscere alcuni dei parametri di impostazione Internet DSL comuni, vedere l’Appendice C di questo manuale. Nel dubbio, contattare il proprio ISP.

Selezionare il tipo di connessione utilizzata facendo clic sul pulsante di opzione**(1)** accanto al tipo di connessione e facendo quindi clic su “Next” (Avanti) **(2)**.



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" (Applica modifiche) per attivare le impostazioni.



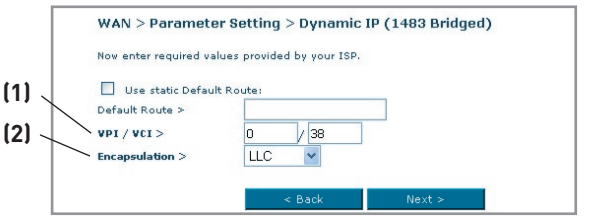
1. **User Name -** digitare il nome utente. (forniti dal proprio ISP).
2. **Password -** Digitare la password. (forniti dal proprio ISP).
3. **Retype Password (Ridigita password) -** Confermare la password (fornita dal proprio ISP).
4. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI) (forniti dal proprio ISP).
5. **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).
6. **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
7. **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.

Configurazione del tipo di connessione su IP dinamico (con bridging 1483)

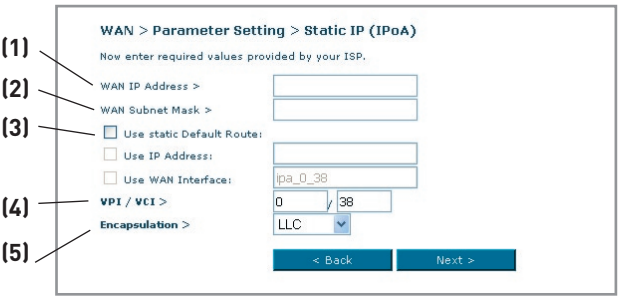
Questo metodo di connessione consente di creare un ponte di collegamento tra la propria rete e quella dell'ISP. Il router riceve l'indirizzo IP automaticamente dal server DHCP dell'ISP.



1. **VPI/VCI -** Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). Questi parametri di identificazione vengono assegnati dall'ISP.
2. **Encapsulation (Incapsulamento)** Selezionare i parametri LLC o VC MUX utilizzati dall'ISP.

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

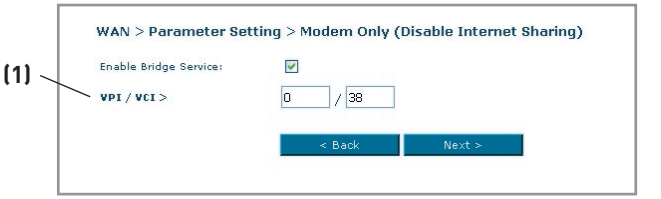
Questo tipo di connessione viene anche chiamato "Classical IP over ATM" o "CLIP", ed è quello fornito dall'ISP come IP fisso del router da collegare ad Internet.



1. **WAN IP Address (Indirizzo IP WAN) –** Digitare un indirizzo IP assegnato dal proprio ISP per l'interfaccia WAN del router.
2. **WAN Subnet Mask -** Digitare una maschera di sottorete 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.

Impostare il tipo di connessione su Modem Only (Soltanto modem) disattivando la condivisione Internet

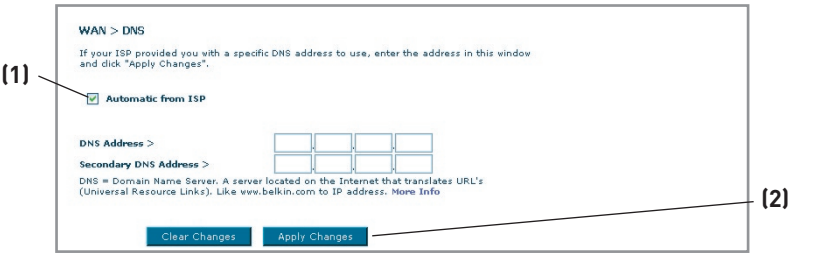
In questa modalità, il router agisce semplicemente come ponte per trasferire i pacchetti attraverso la porta DSL. Per accedere ad Internet è necessario disporre di altro software supplementare installato nei propri computer.



1. VPI/VCI - Digitare i propri parametri Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI). (forniti dal proprio ISP).

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” **(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” (Applica modifiche) **(2)** per salvare le impostazioni.



Utilizzo del DNS dinamico

Il servizio Dynamic DNS (DNS dinamico) vi 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.

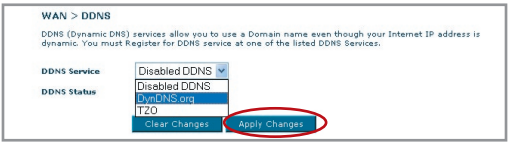
Il servizio “Dynamic DNSSM” è ideale per i siti web domestici, file server o per semplificare l’accesso ai file archiviati ed al PC in casa. Con questo servizio si può essere certi che il proprio nome host porti sempre al proprio indirizzo IP, anche se l’ISP lo cambia. Quando l’indirizzo IP cambia, rimanete localizzabili attraverso il sito dyndns.org.

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

Impostazione dell’aggiornamento client del DNS dinamico del router

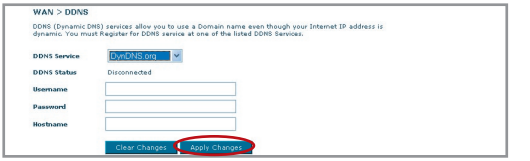
Prima di poter usufruire del servizio di aggiornamento gratuito, bisogna registrarsi con DynDNS.org. Una volta effettuata la registrazione, seguire le seguenti istruzioni:

1. Selezionare “DynDNS.org” dal menu a tendina. Fare clic su “Apply Changes” (Applica modifiche).



2. Inserire il proprio nome utente DynDNS.org nel campo “User Name” **(1)**.
3. Inserire la propria password DynDNS.org nel campo “Password / Key” **(2)**.
4. Nel campo “Domain Name”(Nome dominio) (3), digitare il nome del dominio DynDNS.org creato con DynDNS.org. **(3)**.
5. Fare clic su “Apply Changes” (Applica modifiche) per aggiornare l’indirizzo IP.

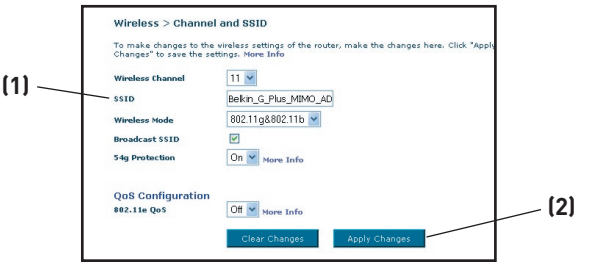
Ogni volta che l’indirizzo IP fornito dall’ISP cambia, il router aggiornerà automaticamente i server di DynDNS.org con il nuovo indirizzo IP. È possibile effettuare questa operazione anche manualmente, facendo clic sul pulsante “Apply Changes” (Applica modifiche) **(4)**.



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.

Channel and SSID (Canale e SSID)



1. 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 vostro router è stato configurato per funzionare sui canali adatti al paese in cui vivete. Il canale predefinito è 11. (Salvo che vi troviate in un paese che non consente l’impiego del canale 11). 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 dalle altre reti 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 dal menu a tendina. Fare clic su “Apply Changes” (Applica modifiche). La modifica è immediata.

2. Modifica del nome della rete wireless (SSID)

Per identificare la propria rete wireless, si utilizza 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 cambiare l’SSID, digitare nel campo SSID il nome desiderato **(1)** e fare clic su “Apply Changes” (Applica 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.

3. 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 il servizio di trasmissione SSID, togliere il segno di spunta dalla casella accanto all'opzione Broadcast SSID. 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 bene: questa funzione avanzata dovrebbe essere scelta soltanto dagli utenti esperti.

4. Utilizzo dello switch di modalità wireless

Il router può funzionare in due diverse modalità wireless:

- **802.11b & 802.11g-** Scegliere questa opzione se si pensa di connettere alla propria rete dei client wireless 802.11b e 802.11g
- **802.11g -** Usare questa modalità se non vi sono clienti 802.11b all'interno della rete. Questa opzione offre le migliori prestazioni, tuttavia non permette il collegamento ai clienti 802.11b.

5. Commutazione in modalità protetta

Una parte della specifica 802.11g prevede che la modalità protetta garantisca il corretto funzionamento dei client e punti di accesso 802.11g in presenza di un pesante traffico 802.11b nell'ambiente operativo. Quando la modalità protetta è ATTIVA, il dispositivo 802.11 verifica la presenza di altro traffico di rete prima di provvedere alla trasmissione dei dati. Pertanto, utilizzata negli ambienti con un PESANTE traffico 802.11b o in presenza di interferenze, questa modalità garantisce prestazioni migliori. In un ambiente dove il traffico di rete wireless è molto ridotto o assente, le prestazioni migliori si ottengono con la modalità protetta DISATTIVATA.

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	Wi-Fi Protected Access 2
Acronimo	64-bit WEP	128-bit WEP	WPA-TKIP/AES (oppure soltanto WPA)	WPA2-AES (oppure soltanto WPA2)
Protezione	Buona	Migliore	Ottima	Ottima
Caratteristiche	Chiavi statiche	Chiavi statiche	Crittografia a chiavi dinamiche e autenticazione reciproca	Crittografia a chiavi dinamiche 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 per permettere la rotazione delle chiavi e il potenziamento della crittografia	La crittografia AES (Advanced Encryption Standard) non provoca alcuna perdita di trasferimento dati

WEP (Wired Equivalent Privacy)

Il protocollo WEP (Wired Equivalent Privacy) potenzia la protezione di 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 protezione 64-bit WEP fu introdotta per la prima volta con la crittografia da 64 bit, che prevedeva una lunghezza di chiave di 40 bit più altri 24 bit supplementari di dati generati dal sistema (per un totale di 64 bit). Alcuni produttori di hardware chiamarono la protezione a 64 bit 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 WEP a 64 bit, fu quindi progettato un metodo più sicuro 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 chiamarono la protezione a 128 bit 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.

Chiavi 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, vanno inseriti 26 caratteri esadecimali.

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.

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.

Ad 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.

Nota per gli utenti Mac: i prodotti originali Apple AirPort supportano soltanto la crittografia a 64 bit. I prodotti Apple Airport 2 supportano sia la modalità di crittografia a 64 che a 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.

WPA (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access) è un nuovo standard Wi-Fi che offre maggiore sicurezza rispetto alle caratteristiche di crittografia 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-Personal (PSK) e WPA-Enterprise (RADIUS).

WPA-Personal (PSK)

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 utilizzata in un ambiente domestico.

WPA-Enterprise (RADIUS)

Questo sistema consente ad un radius server di distribuire automaticamente la chiave di rete ai client. Generalmente, questa modalità viene utilizzata in un ambiente di lavoro. Un elenco dei prodotti wireless Belkin che supportano la protezione WPA è riportato al sito web **www.belkin.com/networking**.

WPA2 (WiFi Protected Access)

WPA2 è la seconda generazione dello standard 802.11i basato su WPA. Offre un maggiore livello di protezione combinando un'autenticazione di rete avanzata ed un metodo di crittografia AES rafforzato. Come per la protezione WPA, la protezione WPA2 è disponibile sia nella modalità Personal (PSK) sia nella modalità Enterprise (RADIUS). Solitamente, la modalità WPA2-Personal è quella più diffuso nelle reti domestiche, mentre la modalità WPA-Enterprise viene utilizzata più spesso in aziende dove un server radius distribuisce automaticamente la chiave di rete ai client.

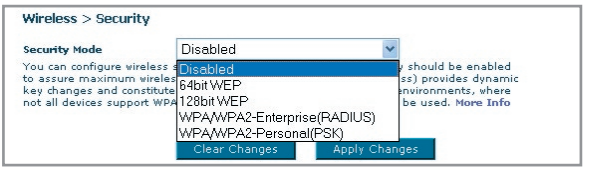
Condivisione dei codici di rete

Nella maggior parte dei prodotti Wi-Fi la sicurezza è disattivata. Una volta messa in funzione la rete, sarà necessario attivare la protezione WEP o WPA2 ed assicurarsi che tutti i dispositivi wireless usino la stessa chiave di rete.

La scheda di rete wireless G+ MIMO per desktop non può accedere alla rete perché usa una chiave di rete diversa da quella configurata nel router G+ MIMO 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 WEP

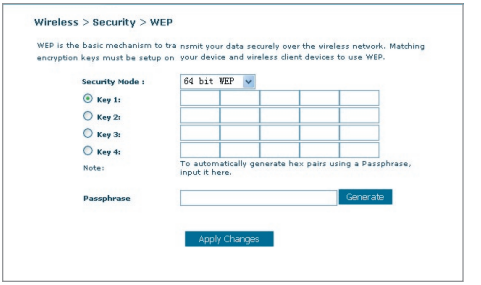
Crittografia WEP a 64 bit

1. Selezionare “64-bit WEP” dal menu a tendina.
2. 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.

Ad esempio:

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



3. Fare clic su “Apply Changes” (Applica 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 dell’access point wireless da un computer con un client wireless, si perderà il collegamento fino a quando la protezione del client wireless non sarà stata attivata. Accertarsi di annotare la propria chiave prima di eseguire le modifiche

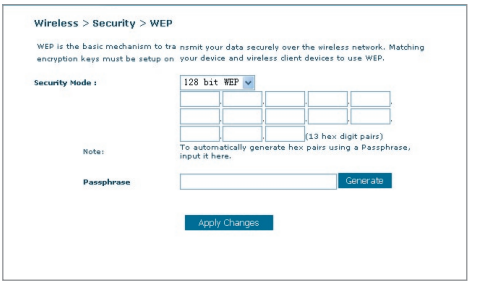
Crittografia WEP a 128 bit

1. Selezionare “128-bit WEP” dal menu a tendina.
2. 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 128 bit è necessario inserire una chiave composta da 26 caratteri esadecimali.

   Ad esempio:

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



3. Fare clic su “Apply Changes” (Applica 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 dell’access point wireless da un computer con un client wireless, si perderà il collegamento fino a quando la protezione del client wireless non sarà stata attivata. Accertarsi di annotare la propria chiave prima di eseguire le modifiche.

Configurazione WPA

Nota bene: 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. È necessario inoltre scaricare dal sito di supporto Belkin il driver più recente per la propria scheda di rete wireless G per computer desktop o

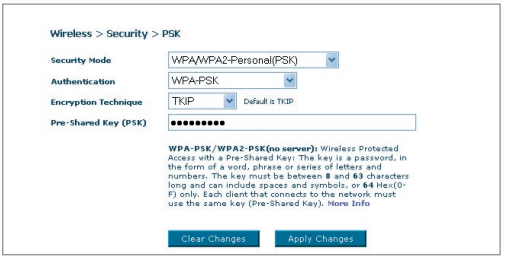
notebook Belkin. Attualmente gli altri sistemi operativi non sono supportati. Il patch Microsoft supporta esclusivamente i dispositivi che prevedono driver con la funzione WPA abilitata, tra cui i prodotti 802.11g Belkin.

Esistono due tipi di protezione WPA: WPA-Personal (PSK) e WPA-Enterprise (RADIUS). La protezione WPA-Personal (PSK) sfrutta la cosiddetta chiave precondivisa 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-Enterprise (RADIUS) è una configurazione nell'ambito della quale un radius server distribuisce automaticamente le chiavi ai client. Questa soluzione viene generalmente utilizzata nell'ambiente lavorativo.

Impostazione della protezione WPA-Personal (PSK)

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-PSK.
2. Selezionare "WPA-PSK" per l'autenticazione.
3. Come "Encryption Technique" (tecnica di crittografia), scegliere "TKIP". Questa impostazione dovrà essere identica per tutti i client configurati.
4. Inserire la propria chiave precondivisa Questo codice può essere composto 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: "Codice rete famiglia Rossi".



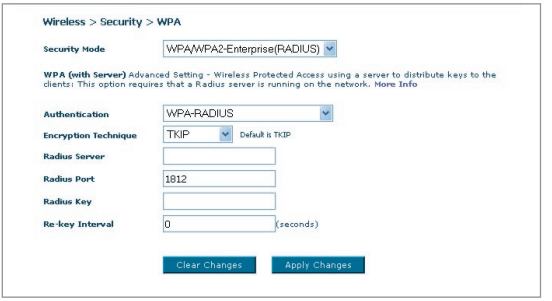
5. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Impostazione WPA-Enterprise (RADIUS)

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

1. Dal menu a tendina "Security mode" (Modalità di protezione), selezionare "WPA/WPA2-Enterprise (RADIUS).

2. Selezionare “WPA-RADIUS” per l’autenticazione
3. Come “Encryption Technique” (tecnica di crittografia), scegliere “TKIP”. Questa impostazione dovrà essere identica sui client configurati
4. Digitare l’indirizzo IP del radius server nei campi “Radius Server”.
5. Digitare la chiave radio nel campo “Radius Key”.
6. Digitare l’intervallo chiave. L’intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
7. Fare clic su “Apply Changes” (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.



Requisiti WPA2

IMPORTANTE: Per utilizzare la protezione WPA2, tutti i computer e gli adattatori di rete devono essere aggiornati con patch, driver e programmi di utilità 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.

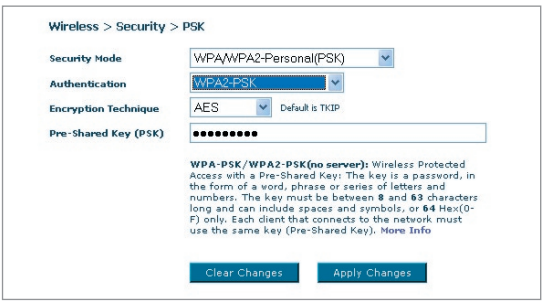
Per i computer con Windows XP che non hanno Service Pack 2 (SP2), è possibile scaricare gratuitamente un file da Microsoft chiamato “Windows XP Support Patch for Wireless Protected Access (KB 826942)”.

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

Impostazione della protezione WPA2-Personal (PSK)

1. Dal menu a tendina “Security mode” (Modalità di protezione), selezionare “WPA/WPA2-PSK (PSK)”.
2. Selezionare “WPA2-Personal (PSK)” per l’autenticazione.
3. Come “Encryption Technique” (tecnica di crittografia), scegliere “AES”. Questa impostazione dovrà essere identica per tutti i client configurati.
4. Digitare la propria chiave precondivisa, Questo codice può essere composto 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: “Codice rete famiglia Rossi”.



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

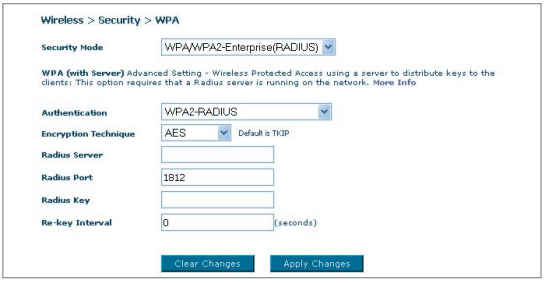
Impostazione WPA2-Enterprise (RADIUS)

Se la vostra rete utilizza un radius server per distribuire le chiavi ai client,

utilizzare questa impostazione.

1. Dal menu a tendina “Security mode” (Modalità di protezione), selezionare “WPA/WPA2-Enterprise (RADIUS)”.
2. Selezionare “WPA2-RADIUS” per l’autenticazione
3. Come “Encryption Technique” (tecnica di crittografia), scegliere “AES”. Questa impostazione dovrà essere identica sui client configurati

4. Digitare l'indirizzo IP del radius server nei campi "Radius Server".
5. Digitare la chiave radio nel campo "Radius Key".
6. Digitare l'intervallo chiave. L'intervallo chiave indica la frequenza di distribuzione delle chiavi (in pacchetti).
7. Fare clic su "Apply Changes" (Applica modifiche) per terminare. Ora devono essere configurati tutti i client in modo da essere adattati a queste impostazioni.



IMPORTANTE: 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 dell'adattatore di rete per l'utilizzo della protezione

Nota bene: questa sezione contiene le informazioni su come configurare un adattatore di rete per utilizzare la protezione. A questo punto il router e l'access point wireless dovrebbero essere stati già configurati per l'utilizzo della crittografia WPA2, WPA o WEP. Per ottenere una connessione wireless, bisognerà configurare le schede di rete wireless notebook e desktop con le medesime impostazioni di protezione.

Le schede di rete wireless G+ MIMO Belkin dispongono di un programma di utilità di rete wireless. Cliccare sul nome della rete wireless (SSID) dall'elenco delle reti disponibili e digitare la chiave pre-condivisa (PSK). Per maggiori informazioni, vi preghiamo di consultare il manuale d'uso della scheda di rete Belkin.

Sulla maggior parte dei computer è possibile configurare il router dalla finestra "Proprietà di rete wireless" presente nel sistema operativo di Windows. Qui di seguito mostriamo due esempi:

Collegamento del computer a una rete wireless che richiede una chiave WEP a 64 o 128 bit

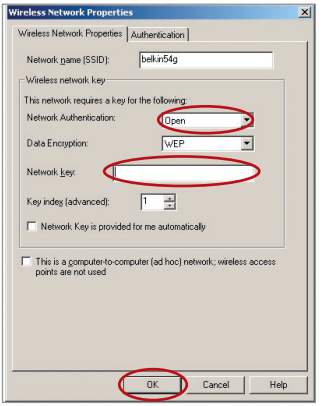
1. Fare doppio clic sull' icona "Signal Indicator" per aprire la schermata "Wireless Network" (Rete wireless). Il pulsante "Advanced" (Avanzate) consente di visualizzare e configurare diverse opzioni della scheda wireless.

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).

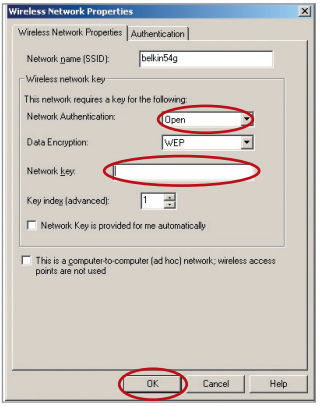


Importante: una chiave WEP è composta da numeri e lettere, da 0 a 9 e dalla A alla F. Per la protezione WEP a 128 bit, bisogna inserire 26 caratteri. Per la protezione WEP a 64 bit, bisogna inserire 10 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access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

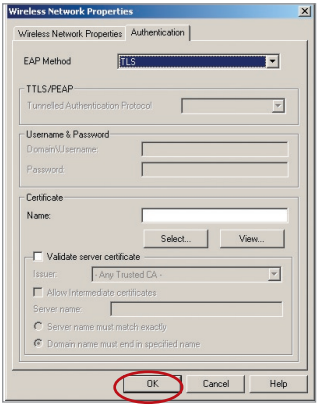


Importante: una chiave WPA-PSK è composta da numeri e lettere, da 0 a 9 e dalla A alla Z. Per la protezione WPA-PSK, si possono inserire da 8 a 63 chiavi. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

5. Fare clic su "OK" per salvare le impostazioni.

Collegamento del computer ad una rete wireless che usa la protezione WPA (con radius 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”.
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/WPA2 per schede wireless di altre marche

Per le schede di rete wireless WPA desktop e notebook di altre marche sprovviste del software WPA/WPA2, 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/WPA2 e di aver scaricato e installato il driver più recente dal suo sito.

Sistemi operativi supportati: • Windows XP Professional

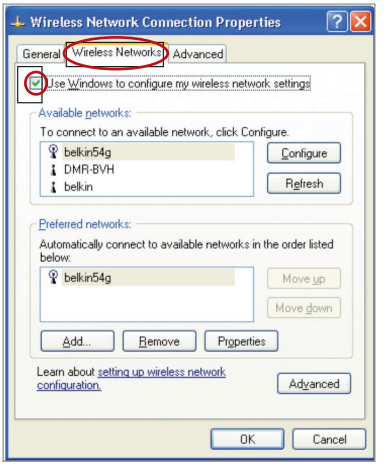
• Windows XP Home Edition

Impostazione della utility wireless Windows XP per utilizzare la protezione WPA/WPA2-PSK

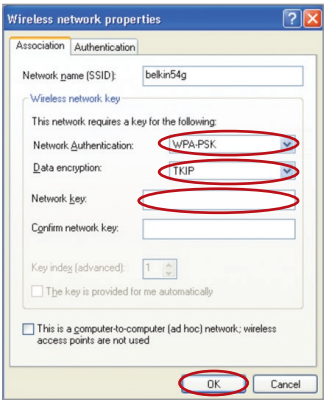
Per utilizzare la protezione WPA-PSK, accertarsi di utilizzare la utility di rete wireless Windows nel seguente modo:

1. In Windows XP, fare clic su “Start > Pannello di controllo > Connessioni di rete.

2. Con il tasto destro del mouse, fare clic sull’opzione “Connessione rete wireless”, e selezionare “Proprietà”.



3. Cliccando sulla scheda “Reti wireless” si aprirà la seguente schermata. Accertarsi che l’opzione “Utilizza Windows per configurare le impostazioni di rete wireless” sia selezionata.



4. Nella scheda “Reti wireless”, cliccare il pulsante “Configura” e si visualizzerà la seguente schermata.

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

Nota bene: 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 “Crittografia dati”. Questa impostazione dovrà essere identica a quella del router configurato.

7. Digitare la propria chiave di crittografia nella casella “Chiave di rete”.

Importante: inserire la propria chiave precondivisa Questo codice può essere composto da 8 a 63 caratteri tra lettere, numeri o simboli. Questa stessa chiave dovrà essere utilizzata su tutti i client configurati.

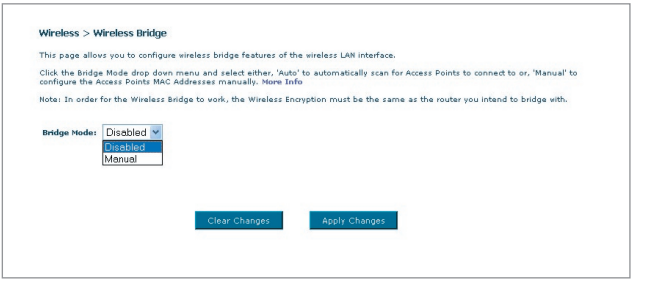
8. Fare clic su “OK” per confermare le impostazioni.

Bridge wireless

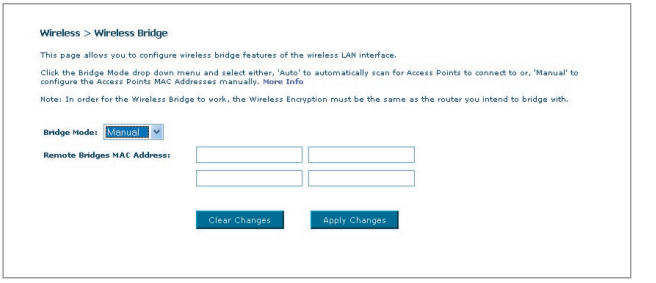
Le soluzioni Wireless Bridging o Wireless Distribution System (WDS) servono a collegare i router e gli access point wireless tra loro per ampliare una rete.

Fare clic sul menu a tendina accanto alla didascalia ‘Bridge Mode’ per scegliere tra:

Disabled (Disattivato): per disattivare la modalità Wireless Bridging (predefinita)



Manuale: per inserire manualmente l’indirizzo(i) MAC wireless degli access point ai quali collegarsi.



1 I canali wireless del router devono corrispondere a quelli dell'AP.

2 Le impostazioni di protezione (WEP) del router devono corrispondere a quelle dell'AP.

3 Se la filtrazione MAC è attiva, è necessario accertarsi di aggiungere l' indirizzo/i WLAN MAC del router/AP per consentire la comunicazione tra i due.

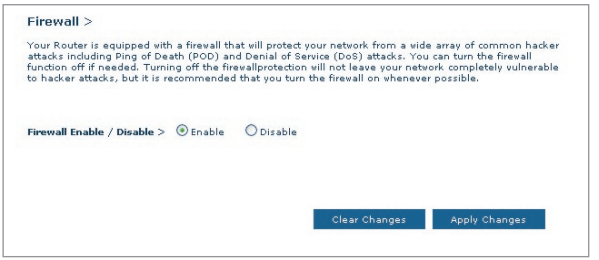
4 Se si utilizza una rete con protezione WPA, entrambi gli access point devono avere lo stesso SSID.

Firewall

Il router è dotato di una protezione firewall che salvaguarda la rete da una vasta gamma di comuni attacchi degli hacker, tra cui:

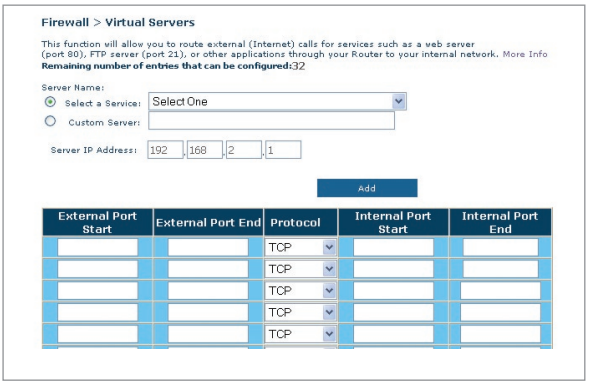
- IP Spoofing
- Land Attack
- Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

La protezione firewall inoltre maschera le porte comuni generalmente 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. Le informazioni relative a queste porte si possono inserire nel router manualmente.



Scelta di un’applicazione

Sono previste diverse applicazioni comuni tra cui scegliere. Fare clic su “Select a Service” (Seleziona un servizio) e scegliere l’applicazione desiderata dall’elenco a tendina. Le impostazioni saranno trasferite alla riga specificata. Fare clic su “Add” (Aggiungi) per salvare le impostazioni per quella specifica applicazione.

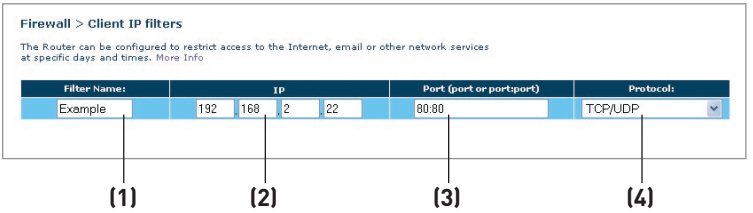
Immissione manuale delle impostazioni nel server virtuale

Per inserire manualmente le impostazioni, fare clic su “Custom Server” (Server personalizzato) ed inserire il nome per il server. Digitare l’indirizzo IP del server nello spazio previsto per la macchina interna e la(e) porta(e) da superare. Quindi selezionare il tipo di protocollo (TCP o UDP), quindi fare clic su “Add” (Aggiungi).

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

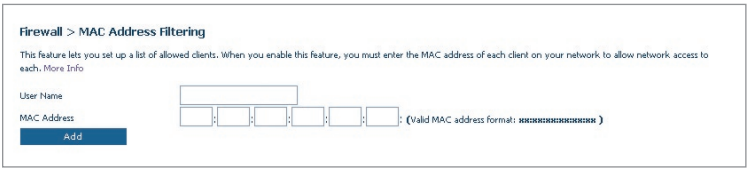
Il router può essere configurato in modo da limitare l'accesso ad Internet, alla posta elettronica o ad altri servizi di rete in particolari giorni o momenti.



Per limitare l'accesso ad Internet ad un solo computer ad esempio, inserire un nome del filtro nella casella "Filter Name" (Nome filtro) **(1)** e l'indirizzo IP del computer per il quale si desidera limitare l'accesso nel campo IP **(2)**. Quindi, digitare "80:80" nel campo Port (Porta) **(3)**. Selezionare il protocollo dalla casella a tendina "Protocol"
(4). Fare clic su "Apply Changes" (Applica modifiche). Al computer corrispondente all'indirizzo IP specificato sarà ora impedito l'accesso ad Internet.

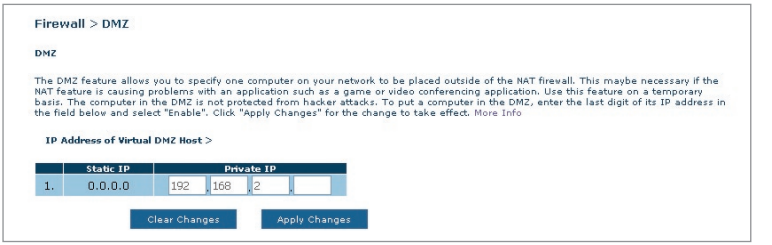
Il filtro indirizzi MAC

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. Quando questa opzione viene attivata, per consentire l'accesso alla rete ad ogni client, è necessario digitare un nome per l'utente e l'indirizzo MAC. Fare clic su "Add" (Aggiungi) per salvare le impostazioni.



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 essere necessaria qualora la funzione NAT entrasse in conflitto con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Utilizzare questa funzione solo provvisoriamente. **Il computer nella DMZ non è protetto dagli attacchi degli hacker.**

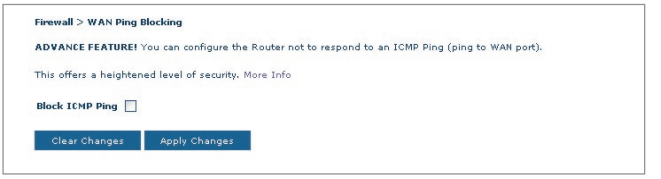


Per collocare il computer nella DMZ, digitare il rispettivo indirizzo IP LAN nel campo "Private IP" (IP Privato) e fare clic su "Apply Changes" (Applica modifiche) affinché la modifica venga attivata.

Blocco del ping ICMP

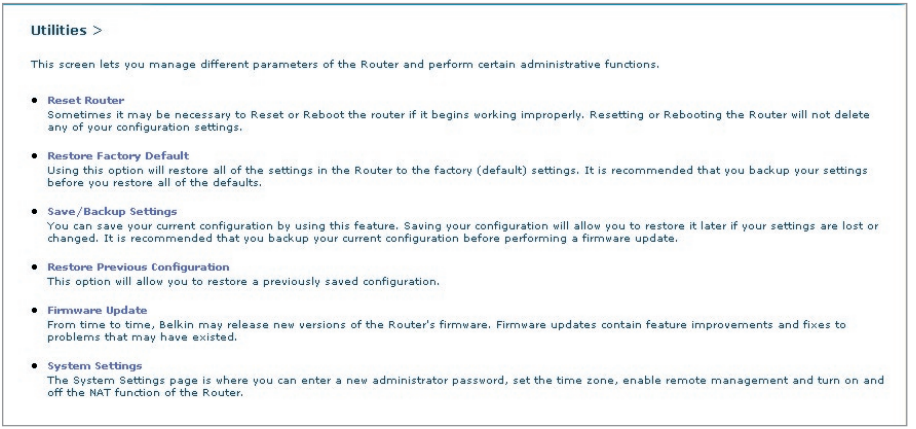
Gli hacker informatici utilizzano quello che è noto come "pinging" per scoprire le potenziali vittime in Internet. Colpendo uno specifico indirizzo IP e ricevendo una risposta da detto indirizzo IP, un hacker è in grado di stabilire se ci sia qualcosa di interessante o meno. Il router può essere impostato 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" (Applica modifiche). Il router in questo modo non reagirà se colpito da un ping ICMP.



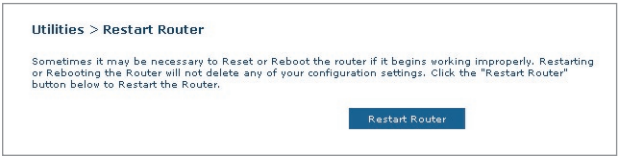
Utility

La schermata “Utility” 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, il router deve essere riavviato. Se il router dovesse essere riavviato, le impostazioni di configurazione NON saranno cancellate.



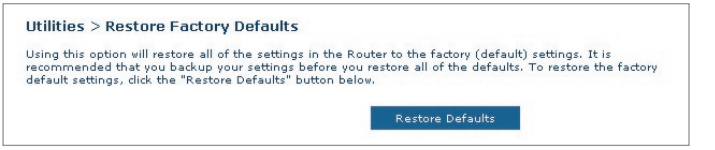
Riavvio del router per ripristinare il normale funzionamento

1. Fare clic sul pulsante “Restart Router” (Riavvia il router).

2. Compare il seguente messaggio. Fare clic su “OK” per riavviare il router.

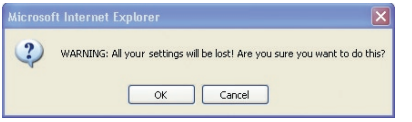
Ripristino delle impostazioni predefinite

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



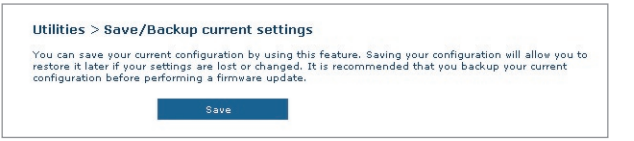
1. Fare clic sul pulsante “Restore Default” (Ripristina impostazioni predefinite).

2. Compare il seguente messaggio. Fare clic su “OK” per ripristinare le impostazioni predefinite.

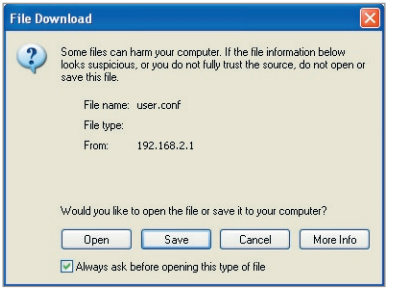


Salvataggio/Creazione di un copia di backup delle impostazioni correnti

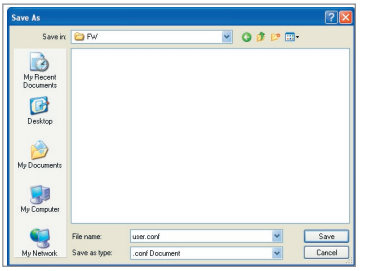
Questa opzione consente di salvare la configurazione attuale. Salvando la configurazione corrente è possibile ripristinarla in un momento successivo nel caso le impostazioni andassero perdute o venissero modificate. È consigliabile fare una copia della configurazione corrente prima di eseguire un aggiornamento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



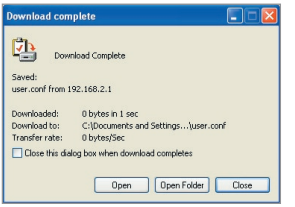
1. Fare clic su “Save” (Salva). Compare una finestra chiamata “File Download”. Fare clic su “Save” (Salva).



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. Fare clic su “Close” (Chiudi).

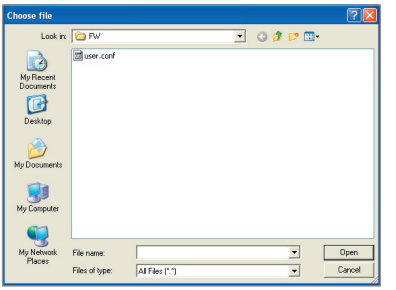


La configurazione è stata salvata.

Ripristino delle impostazioni precedenti

Questa opzione consente di ripristinare qualsiasi configurazione salvata in precedenza.

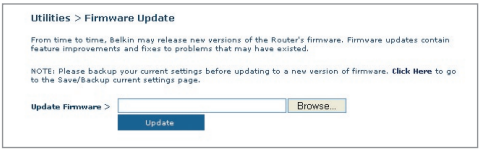
1. Fare clic su “Browse” (Sfoglia). Si apre una finestra che consente di selezionare la posizione del file di configurazione. Tutti i file di configurazione terminano con “.conf”. Trovare il file di configurazione che si desidera ripristinare e fare doppio clic su di esso.



2. Quindi, fare clic su “Open” (Apri).

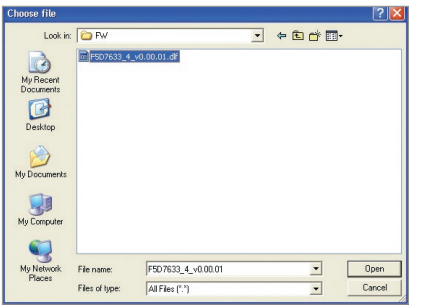
Aggiornamenti del firmware

Di tanto in tanto, Belkin potrebbe pubblicare 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.



Aggiornamento del firmware del router

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



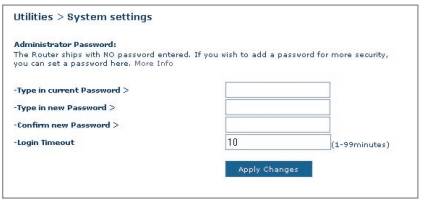
2. Andare al file di firmware scaricato. Selezionarlo facendo doppio clic sul nome del file.
3. Fare clic su “Update” (Aggiorna) per ottenere la più recente versione del firmware.

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 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

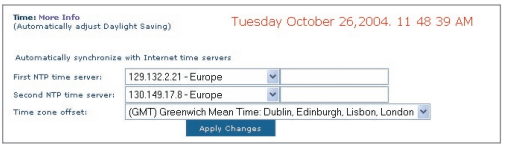
L’opzione di durata connessione consente di impostare un intervallo di tempo di connessione all’interfaccia avanzata di impostazione del router. Il timer parte dal momento in cui non si rileva alcuna attività. Ad esempio, se fosse stata apportata qualche modifica all’interfaccia di impostazione avanzata, 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 bene: è possibile connettere all’interfaccia avanzata di impostazione del router soltanto un computer alla volta.

Impostazione dell'ora e del fuso orario

Il router aggiorna 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 i server di orario NTP desiderati ed il proprio fuso orario, quindi fare clic su " Apply Changes" (Applica modifiche). 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.



Attivazione della gestione a distanza

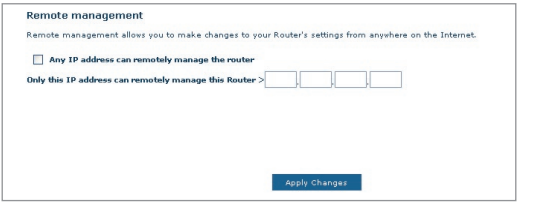
Prima di attivare questa funzione avanzata del router Belkin, **ACCERTARSI DI AVER IMPOSTATO LA PASSWORD AMMINISTRATORE.**. La gestione a distanza consente di modificare le impostazioni del router da qualsiasi punto di Internet.

Fare clic sul pulsante "Change Settings" (Modifica impostazioni) per visualizzare la pagina "Remote Management" (Gestione a distanza).

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 soltanto ad uno specifico indirizzo IP di gestire 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, si apre potenzialmente il router ad eventuali intrusioni esterne.

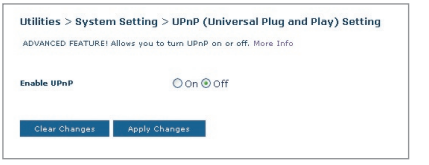
Fare clic su “Apply Changes” (Applica modifiche) per salvare le proprie impostazioni.



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.

Fare clic sul pulsante “Change Settings” (Modifica impostazioni) per visualizzare la pagina “UPnP Setting” (Impostazione UPnP). Quindi selezionare “On” per “Enable UPnP” (Abilita UPnP). Fare clic su “Apply Changes” (Applica modifiche) per salvare le proprie impostazioni.



Risoluzione dei problemi

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 è “un indirizzo IP statico”. Non riesco a collegarmi ad 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 10 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 si riesce ad impostare un collegamento a Internet in modalità wireless.

Soluzione:

Nell'impossibilità di collegarsi ad Internet da un computer wireless, eseguire le seguenti verifiche:

1. Controllare lespie luminose sul router. Se si utilizza un router Belkin, le spie dovrebbero essere illuminate come segue:
   - La spia "Power" (Alimentazione) dovrebbe essere accesa.
   - Il LED "DSL" dovrebbe essere acceso, non lampeggiante.
   - Il LED "Internet LED" dovrebbe essere acceso o lampeggiante.
2. Aprire il software della utility wireless facendo clic sull'icona nel desktop di sistema nell'angolo in basso a destra dello schermo. Se si sta usando una scheda wireless Belkin, l'icona nel desktop del sistema dovrebbe apparire così  (l'icona può essere rossa o verde).
3. La finestra precisa che si apre varia in base al modello della scheda wireless in vostro possesso, tuttavia, qualsiasi utility dovrebbe prevedere un elenco delle reti disponibili (Available Networks), ovvero delle reti alle quali si può collegare .

Il nome della propria rete wireless appare nei risultati?

Sì, il nome della mia rete è in elenco passare alla soluzione per la risoluzione delle anomalie 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 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”.
2. Se la protezione (crittografia) della rete è stata attivata, bisognerà digitare la chiave di rete. Per ulteriori informazioni sulla protezione, vedere: “Modifica delle impostazioni di protezione della rete wireless”.
3. 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 le prestazioni di trasmissione tra i dispositivi diminuiscono all’aumentare della distanza. 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 metri e 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 manuale a pagina 37 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 dettagli consultare il manuale della scheda wireless.

Problema:

Si incontrano alcune 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.
2. Aprire il browser web e digitare l'indirizzo IP del router wireless o dell'access point. (Il router è preimpostato su 192.168.2.1, l'access point 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 (Applica 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 sicurezza WEP a 128 bit, bisogna inserire una chiave di 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” (Applica 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 dell’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 la 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:

Si incontrano 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. FAd esempio, se il router wireless o l’access point utilizza la chiave 00112233445566778899AABBCC, la scheda wireless 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 = chiave a 128 bit

8. Fare clic su “OK” e, quindi, su “Apply” (Applica) 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 bene: 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 al 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 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.

I driver più recenti si possono scaricare al sito: http://web.belkin.com/support/networkingsupport.asp.

Il supporto WPA sarà installato automaticamente nel caso si aggiornasse il proprio sistema alla versione Windows XP Service pack 2. Dettagli in merito sono riportati al sito http://support.microsoft.com

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 "Encryption Technique" (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: "Chiave di rete famiglia Rossi".

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

Problema:

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

Soluzione:

Se la vostra rete utilizza un radius server 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 "Encryption Technique" (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" (Applica modifiche) per terminare. Ora si devono configurare tutti i client adattandoli a queste impostazioni.

Problema:

Si incontrano 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 è "Smith Family Network Key" nel router wireless router o nell'access point, 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. Una volta selezionato il pulsante "Advanced" (Opzioni avanzate), la utility wireless LAN Belkin appare automaticamente. 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 il codice WPA nella casella "Network key" (Codice 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 chiavi da 8 a 63 caratteri. Questa chiave di rete deve essere uguale a quella assegnata al router wireless o all'access point.

7. Fare clic su "OK" e, quindi, su "Apply" (Applica) per salvare le impostazioni.

Problema:

Si incontrano 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. Una volta selezionato il pulsante “Advanced” (Opzioni avanzate), la utility wireless LAN Belkin appare automaticamente. 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” (Applica) per salvare le impostazioni.

Problema:

Si incontrano 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 WPA desktop e notebook **NON** Belkin e sprovviste del software WPA, è possibile 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 bene: 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 > Pannello di controllo > Connessioni di rete”.
2. Cliccando con il tasto destro del mouse sulla scheda “Reti wireless si aprirà la seguente schermata. Accertarsi che l’opzione “Utilizza Windows per configurare le impostazioni di rete wireless” sia attivata.

3. Nella scheda “Reti wireless”, cliccare il pulsante “Configura” e si visualizzerà la seguente schermata.
4. Nel caso di una rete domestica o simile, selezionare “WPA-PSK” da “Amministrazione rete”.

Nota bene: selezionare “WPA (con radius server)” 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.

5. Selezionare “TKIP” o “AES” da “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 “Chiave di rete”.

Importante: Inserire la propria chiave precondivisa Questo codice può essere composto 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, G+ MIMO e Pre-N?

Attualmente esistono quattro livelli 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 wireless più comune, il 802.11b, trasferisce dati a 11 Mbps; l’802.11a e l’802.11g a 54 a 108 Mbps; G+ MIMO ha una velocità di 54 Mbps.

Tabella di confronto wireless

Tecnologia wireless	802.11b	G (802.11g)	G+ (802.11g con HSM)	G+ MIMO(802.11g con MIMO MRC)	Belkin Pre-N (802.11g con True MIMO)
Velocità*	11Mbps link rate / Baseline	5 volte più veloce dello standard 802.11b*	10 volte più veloce dello standard 802.11b*	10 volte più veloce dello standard 802.11b*	15 volte più veloce dello standard 802.11b*
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	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	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/g	Compatibile con 802.11b/g	Compatibile con 802.11b/g	Compatibile con 802.11g o 802.11b
Copertura*	Normalmente 30 - 60m in ambienti chiusi	Fino a 120 metri*	Fino a 200 metri*	Fino a 300 metri*	Fino a 400 metri*
Vantaggi	Tecnologia legacy lungamente testata	Comune - ampio utilizzo della condivisione Internet	Velocità e copertura maggiori	Copertura maggiore e velocità costante	Leader nel settore - ottima copertura ed efficienza

*La distanza e le velocità di connessione variano in funzione dell'ambiente di rete.

Informazioni di assistenza tecnica

Assistenza tecnica

Per i più recenti aggiornamenti software o per qualsiasi dubbio riguardante l'installazione di questo prodotto, visitare il sito **www.belkin.com/networking** o chiamare il numero:

USA:	**877-736-5771 oppure 310-898-1100 int. 2263**
Europa:	**00 800 223 55 460**
Australia:	**1800 235 546**
Nuova Zelanda:	**0800 235 546**
Singapore:	**800 616 1790**

Allegato A: Glossario

IP Address (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” (Applica 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

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

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 alnternet.
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" (Applica modifiche).

Una volta eseguite le modifiche, l'indicatore "Internet Status" (Stato Internet) visualizzerà il messaggio "Connection OK", se il router è stato impostato correttamente.

PPPoA

Digitare le informazioni PPPoA negli appositi spazi e fare clic su "Next" (Avanti). Fare clic su "Apply" (Applica) per attivare le impostazioni.

1. User name (Nome utente) - Digitare il nome utente. (forniti dal proprio ISP).
2. Password - Digitare la propria password (forniti 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.

Channel and SSID (Canale e SSID)

Per cambiare canale, selezionare il canale di funzionamento del router dal menu a discesa e selezionare il proprio canale. Fare clic su "Apply Changes" (Applica 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" (Applica modifiche) per salvare la modifica.

Trasmissione ESSID

Molte schede di rete wireless attualmente sul mercato prevedono una funzione detta “site survey”. 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 WIFI protested Access (WPA) e prevede due gradi di protezione: 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 le richieste di vari servizi 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. La limitazione di accesso ai servizi può essere impostata per uno o più computer.

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" (Applica modifiche) per salvare.

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 essere necessaria qualora la funzione NAT entrasse in conflitto con un'applicazione, come ad esempio un gioco o un'applicazione di videoconferenza. Utilizzare questa funzione 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" (Applica 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" (Applica modifiche).

Password Amministratore

Il router viene fornito SENZA 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 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 aggiorna 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.

Gestione a distanza

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

UPnP

La tecnologia UPnP (Universal Plug-and-Play) è in grado di offrire un funzionamento continuo delle opzioni di trasmissione di messaggi vocali, video, giochi e di altre applicazioni conformi agli standard UPnP. Per funzionare correttamente, alcune applicazioni richiedono che la protezione firewall del router sia configurata in maniera specifica. In genere, questo richiede che si aprano le porte TCP e UDP e, in alcuni casi, che si impostino 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" (Applica modifiche) per salvare la modifica.

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

Nota bene: Sebbene alcuni dei fattori elencati di seguito possano compromettere le prestazioni della rete, non ne impediscono il funzionamento. Se ritenete che la rete non funzioni efficientemente, la seguente lista di controllo potrebbe rivelarsi utile.

1. Collocazione del router o dell'access point

Posizionare il router wireless (o l'access point), che rappresenta il punto di connessione centrale della rete, il più vicino possibile al centro della copertura dei dispositivi wireless.

Per ottenere la migliore connessione per i "clienti wireless"(computer provvisti delle schede di rete wireless per 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 piano 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 cordless 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 in metallo
- 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 le prestazioni della rete wireless dovessero continuare ad essere inadeguate, dopo aver verificato i punti sopra riportati, e se si ha un telefono cordless:

- allontanare il telefono cordless dal router wireless (o access point) 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, la causa era probabilmente 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

Negli edifici dove sono presenti sia abitazioni che uffici, una rete vicina potrebbe entrare in conflitto con la vostra.

Usare le capacità Site Survey 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 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 protette, VPN e AOL

Le connessioni protette generalmente richiedono un nome utente e una password e sono usate quando sono richieste condizioni di sicurezza. Le connessioni protette 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 siti web di home banking
- Molti siti commerciali che richiedono un nome utente e una password per accedere all’account

Le connessioni protette si possono interrompere configurando la gestione dell’alimentazione del computer, facendole “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 “Opzioni risparmio energia” nel pannello di controllo.

Se le difficoltà con la connessione protetta VPN o AOL dovessero persistere, rivedere i passaggi nelle pagine precedenti per assicurarsi di aver individuato 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 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
UK	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 ALLE NORMATIVE FCC PER LA COMPATIBILITÀ' ELETTROMAGNETICA

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

F5D9630-4

al quale questa dichiarazione fa riferimento,
è conforme alla Parte 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 alle radiazioni di radiofrequenza.
La potenza in uscita irradiata da questo dispositivo è molto inferiore ai limiti di esposizione alla radiofrequenza FCC. Tuttavia, il dispositivo dovrà essere utilizzato in modo da ridurre al minimo i potenziali rischi di contatto umano nel corso del suo funzionamento.

Se il dispositivo venisse collegato ad un'antenna esterna, l'antenna dovrà essere posizionata in modo da ridurre al minimo il potenziale rischio di contatto umano nel corso del suo funzionamento. Per evitare un eventuale superamento dei limiti di esposizione alle radiofrequenze FCC, non è consentito avvicinarsi all'antenna di oltre 20 cm nel corso del 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 normative FCC. Questi limiti hanno lo scopo di fornire 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:

- Modificando la direzione o la posizione dell' antenna ricevente.
- Aumentando la distanza tra il dispositivo ed il ricevitore.
- Collegando il dispositivo ad una presa di un circuito diversa da quella cui è collegato il ricevitore.
- Rivolgendosi al rivenditore o ad 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) – Sicurezza del prodotto
- EN 300 328 Esigenze tecniche per i dispositivi radio
- ETS 300 826 - Esigenze generali EMC per dispositivi radio

Per stabilire il tipo di trasmettitore utilizzato, verificare la targhetta di identificazione del proprio prodotto Belkin.

I prodotti con il marchio CE sono conformi alla Direttiva sulla compatibilità elettromagnetica (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.

Questo simbolo posto sul prodotto o sulla sua confezione indica che tale prodotto non deve essere gettato via insieme ai rifiuti domestici. L'utente ha la responsabilità di liberarsi dell'apparecchiatura portandola in un punto di raccolta deputato al riciclaggio di rifiuti di apparecchi elettrici ed elettronici. La raccolta separata e il riciclaggio degli apparecchi da smaltire contribuiranno alla salvaguardia delle risorse naturali e garantiranno che il prodotto sia riciclato in modo da non mettere in pericolo la salute umana. Per maggiori informazioni sui punti di smaltimento e riciclaggio per le apparecchiature elettroniche, vi preghiamo di contattare il vostro comune, il servizio di smaltimento rifiuti domestici o il negozio in cui avete acquistato.

Prodotto garantito a vita da Belkin Corporation Limited

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 sia stato danneggiato accidentalmente, per abuso, uso non corretto o non conforme, qualora sia stato modificato senza il permesso scritto di Belkin, o nel caso il numero di serie Belkin fosse stato cancellato o reso illeggibile.

LA GARANZIA E I RIMEDI DI CUI SOPRA PREVALGONO SU QUALSIASI ALTRO ACCORDO, SIA ESSO ORALE, 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 impiegato di 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."

Poiché alcuni Stati non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, 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.