# Scheda PCI Wireless
# IEEE 802.11n  300Mbps

## MANUALE UTENTE

www.hamletcom.com

Gentile Cliente,
La ringraziamo per la fiducia riposta nei nostri prodotti. La preghiamo di seguire le norme d'uso e manutenzione che seguono. Al termine del funzionamento di questo prodotto La preghiamo di non smaltirlo tra i rifiuti urbani misti, ma di effettuare per detti rifiuti una raccolta separata negli appositi raccoglitori di materiale elettrico/elettronico o di riportare il prodotto dal rivenditore che lo ritirerà gratuitamente.

Informiamo che il prodotto è stato realizzato con materiali e componenti in conformità a quanto previsto dalle seguenti direttive.

ROHS: 2002/95/CE.
RAEE: 2003/96/CE, D.Lgs. 151/2005.

Direttive CE:
EN 62311: 2008
EN 300 328 (2006-10)
EN 301 489-1 (2008-04)
EN 301 489-17 (2008-04)
EN 55022: 2006+A1: 2007, Class B
EN 61000-4-2: 1995+A1: 1998+A2:2001
EN 61000-4-3: 2006+A1: 2008

**CE Mark Warning**
Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

CE

**Marchi commerciali**
Tutti i marchi e i nomi di società citati in questa guida sono utilizzati al solo scopo descrittivo e appartengono ai rispettivi proprietari.

**Variazioni**
La presente guida ha scopo puramente informativo e può essere modificata senza preavviso. Sebbene questo documento sia stato compilato con la massima accuratezza, Hamlet non si assume alcuna responsabilità per eventuali errori od omissioni e all'uso delle informazioni in esso contenute. Hamlet si riserva il diritto di modificare o aggiornare il prodotto e la guida senza alcuna limitazione e senza obbligo di preavviso.

# Sommario

# 1. Introduzione

La scheda PCI wireless HNW300CI di Hamlet è la soluzione più semplice ed economica per utilizzare il proprio computer senza preoccuparsi degli eventuali problemi causati dall'utilizzo di numerosi cavi. Una volta connessi è possibile fare qualsiasi operazione esattamente come se ci si trovasse in una rete cablata.
Questa scheda PCI opera nello spettro di frequenza di 2.4 GHz e supporta gli standard wireless 802.11b, 802.11g, and 802.11n. È la soluzione migliore per aggiungere alla propria rete la funzionalità wireless o anche solo per navigare in rete senza fili.

Per proteggere la connettività wireless, la scheda HNW300CI può criptare tutte le trasmissioni wireless tramite crittografia ed identificazione WEP 64/128-bit, WPA, WPA-PSK e WPA-AES permettendo una connessione senza fili più sicura possibile.

La scheda Wireless PCI di Hamlet implementa la più recente tecnologia 11n draft 2.0 migliorando considerevolmente il segnale wireless rispetto allo standard 802.11g. Essa supporta l'architettura MIMO 1T2R del tutto compatibile con lo standard IEEE 802.11n. L'elevata velocità permette una migliore e più flessibile gestione dell'intenso traffico di rete, offrendo una velocissima connessione wireless per la navigazione Internet senza fili.

L'installazione della scheda HNW300CI nel proprio computer garantisce alte performance e una soluzione efficiente per attività quali la condivisione video, giochi ed aumenta la QoS (WMM) senza nessuna perdita in performance. Triplica la copertura della rete ed aumenta fino a sei volte la capacità di trasmissione rispetto ai precedenti prodotti con tecnologia 11g.

Per applicazioni più avanzate la scheda Wireless PCI di Hamlet supporta anche la cifratura/decifratura hardware IEEE 802.11i, compresi 64/128-bit WEP, TKIP e AES. Supporta inoltre la crittografia WPA e WPA2.

## 1.1 Caratteristiche

| Caratteristiche | Vantaggi |
|---|---|
| Velocità fino a 300Mbps* (2.4GHz tecnologia 11N draft 2.0) | Permette una connessione Internet ad alta velocità senza l'impiego di cavi |
| Gestione avanzata dell'alimentazione | Bassi consumi energetici |
| Supporta WPA/WPA2 (IEEE 802.11i), WEP 64/128-bit | Elevata sicurezza dei dati |
| Supporta lo standard WMM (IEEE 802.11e) | Supporta Quality of Service (QoS) per Wireless Multimedia Enhancements (WMM) / Risparmio energetico più efficiente per il Dynamic Networking |
| PCI 2.2 | Interfaccia PCI standard 2.2 |

** Massima velocità teorica del segnale wireless definita dalle specifiche IEEE 802.11g, 802.11a e 802.11n. La velocità reale dei dati può subire variazioni. Condizioni di rete e fattori ambientali quali volumi di traffico, materiali edili e tipologie di edifici, possono causare un decremento delle velocità di trasmissione e possono incidere negativamente sul raggio operativo del segnale wireless.*

## 1.2 Contenuto della scatola

Aprire con attenzione la confezione ed assicurarsi che gli articoli sotto elencati siano tutti presenti. Non scartare i materiali in caso di sostituzione; il prodotto deve essere riconsegnato con il suo imballo originale

- Scheda PCI Wireless 802.11b/g/n
- Due antenne removibili con attacco SMA
- CD-ROM con Driver e Manuale Utente inclusi
- Guida rapida di Installazione

## 1.3 Descrizione

La scheda HNW300CI è compatibile con l'interfaccia PCI 2.2 e presenta nella staffa posteriore due connettori SMA per le antenne esterne rimovibili e due indicatori LED (LINK e PWR) di colore verde che indicano lo stato di attività della periferica.

## 1.4 Requisiti di sistema

Di seguito indichiamo i requisiti minimi di sistema necessari per l'utilizzo della scheda PCI.

- Computer con uno slot PCI disponibile
- Windows 2000/XP/Vista
- 30 MB di spazio libero sul disco per l'installazione

# 2. Scheda PCI per Windows 2000/XP/Vista

## 2.1 Prima di iniziare

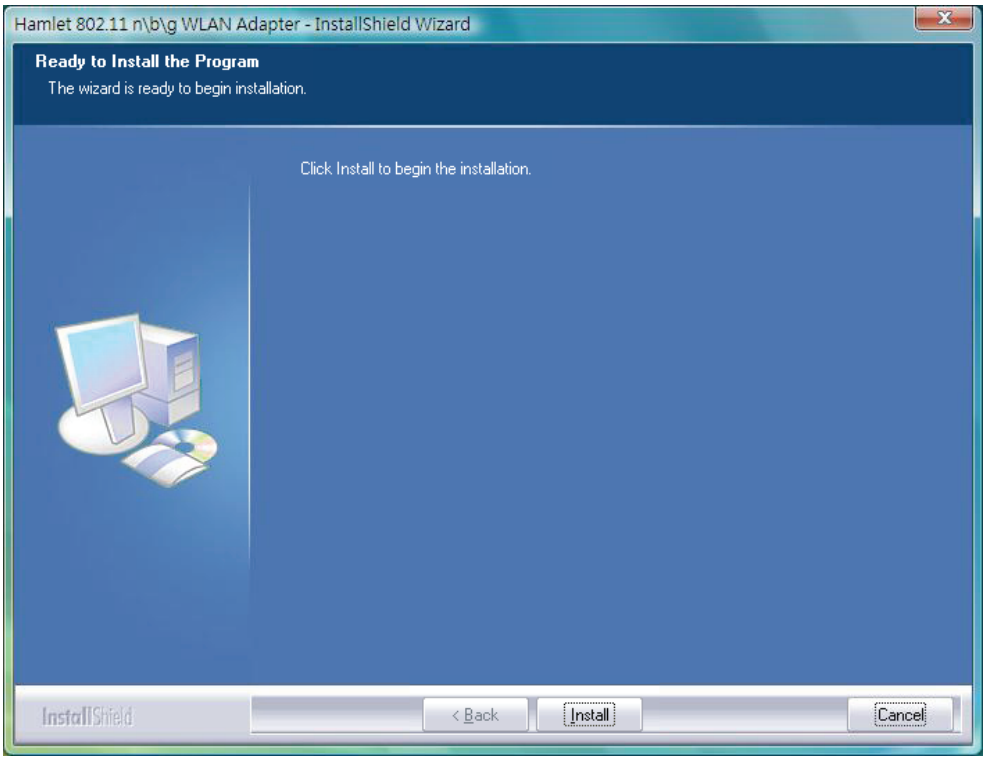
Durante l'installazione, il sistema operativo potrebbe richiedere la copia di alcuni file di sistema dal proprio CD di installazione. Assicurarsi di avere a disposizione una copia del CD di installazione di Windows prima di procedere all'installazione dei driver.

## 2.2 Installazione dei Driver

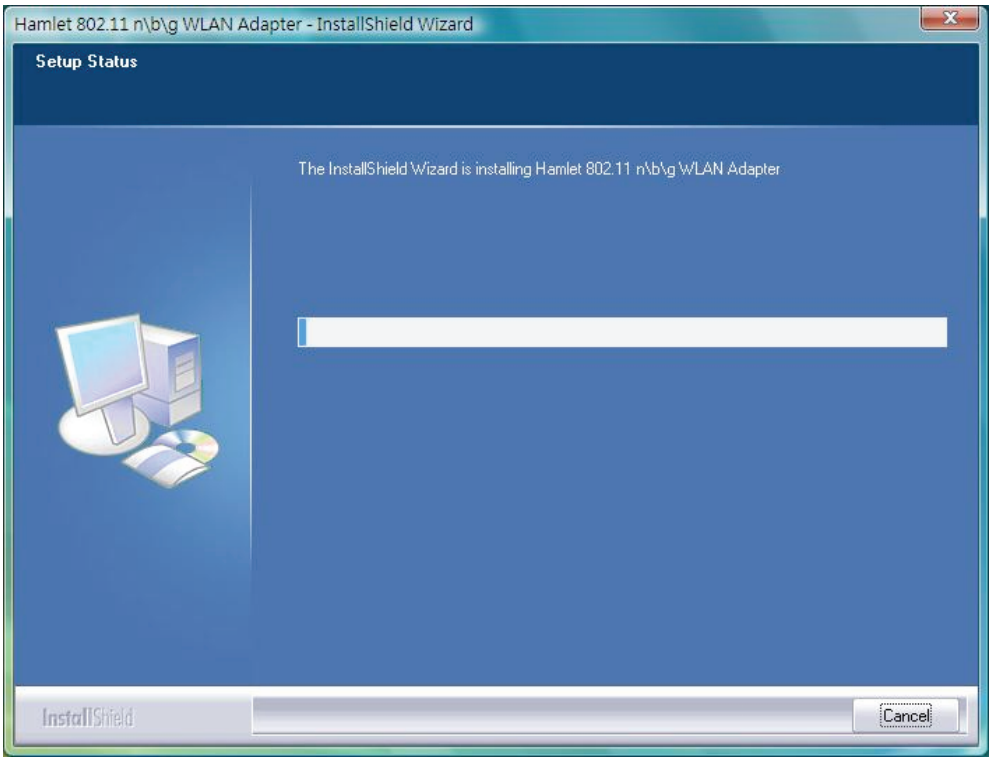
Seguire la procedura descritta di seguito per installare i driver:

1. Inserire il CD presente nella confezione. La procedura di setup dovrebbe iniziare automaticamente. In caso contrario selezionare manualmente il file **setup.exe** dalla directory principale del CD-ROM.

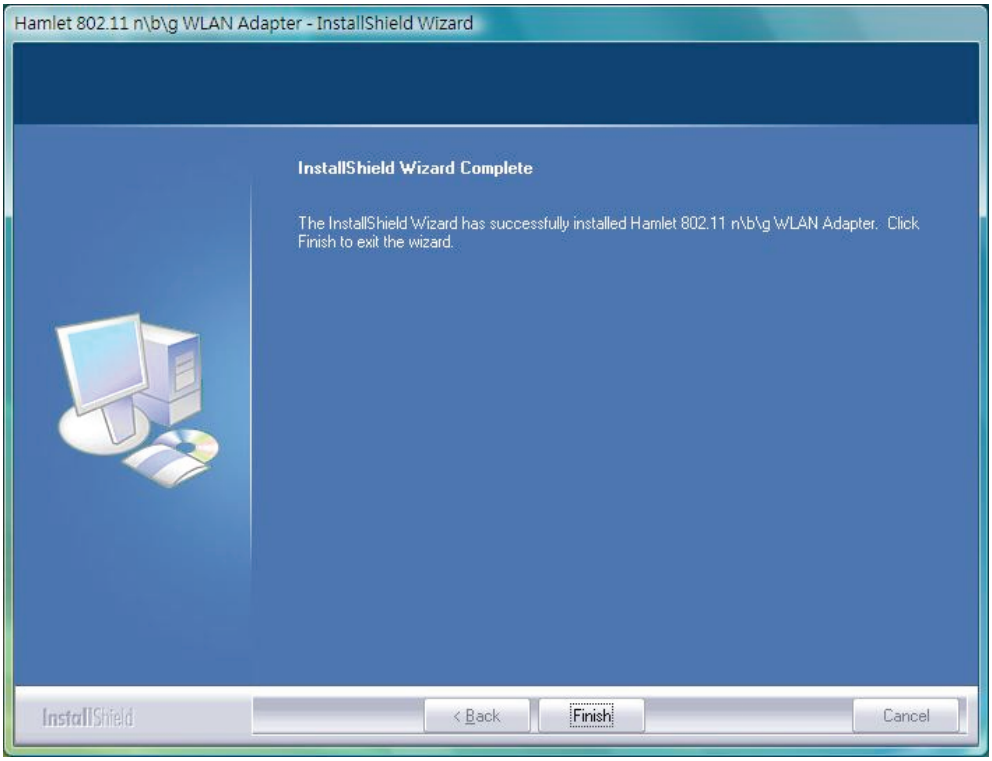
2. Una volta che il setup è iniziato comparirà la maschera di installazione guidata - **InstallShield Wizard**.




3. Cliccare su **Install** per avviare l'installazione.



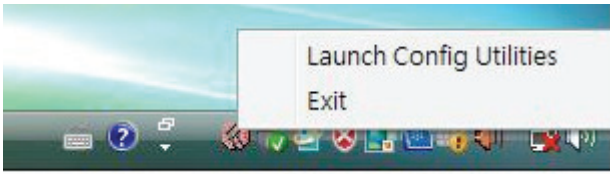

4. Attendere qualche minuto affinché il software porti a termine l'installazione.



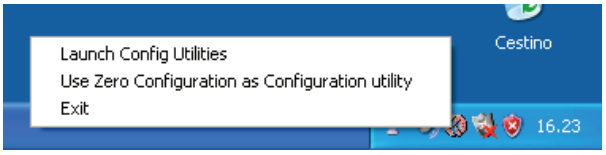

5. Quando l'installazione è completata cliccare su **Finish.**

6. Inserire la scheda PCI nello slot del computer. Windows rileverà e installerà il nuovo hardware automaticamente.

7. Nell'area di notifica della barra delle applicazioni comparirà l'icona Hamlet. Fare clic su di essa con il pulsante destro del mouse e selezionare **Launch Config Utilities.**

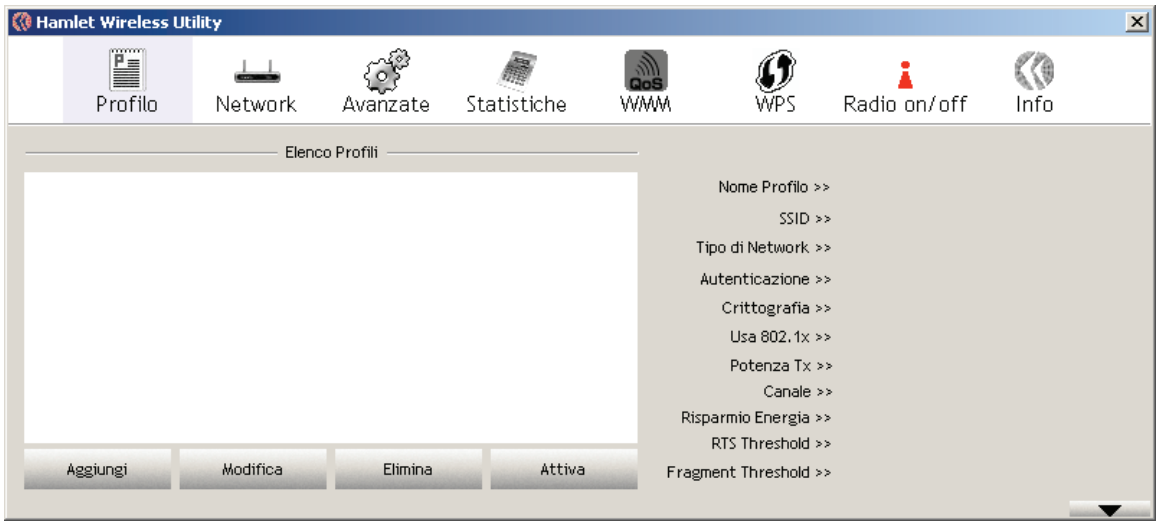



**Attenzione:** in Windows XP è disponibile anche l'opzione **Use Zero Configuration as Configuration Utility** se si desidera utilizzare Windows Zero Config.



## 2.3 Profili

La schermata **Profilo** serve per impostare più Access Point. Quando si aggiunge un nuovo profilo viene richiesto un Nome Profilo, un SSID e la modalità di risparmio energetico, il Tipo di Network, la soglia RTS/Frammentazione e le impostazioni per Crittografia/Autenticazione. Un profilo può essere configurato nella modalità **Infrastructure** o **Ad-Hoc**. Di seguito viene descritto come configurare entrambe le soluzioni.

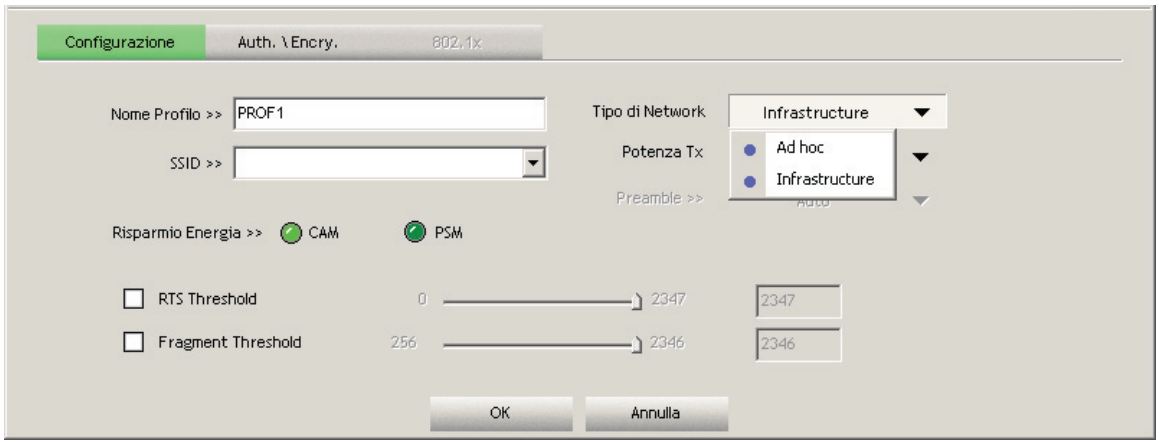



- **Elenco Profili:** in questo riquadro sono mostrati i profili configurati.
- **Nome Profilo:** indica il nome del profilo selezionato.
- **SSID**: mostra il nome dell'SSID relativo al profilo selezionato.
- **Tipo di Network:** indica il tipo di network associato al profilo.
- **Autenticazione:** mostra il tipo di autenticazione utilizzato.
- **Crittografia:** indica il tipo di crittografia impostato.
- **Usa 802.x**: indica se è utilizzato 802.x.
- **Potenza TX:** mostra la potenza di trasmissione del segnale radio.
- **Canale:** indica il canale radio utilizzato.
- **Risparmio Energia:** indica l'opzione di Risparmio Energetico attivata.
- **RTS Threshold:** indica la Soglia RTS.
- **Fragment Threshold:** indica la soglia di frammentazione dei pacchetti.

I pulsanti **Aggiungi**, **Modifica**, **Elimina** e **Attiva** permettono di inserire un nuovo profilo, modificarne uno esistente, nonchè eliminare o attivare uno dei profili presenti.

### 2.3.1. Modalità "Infrastructure"

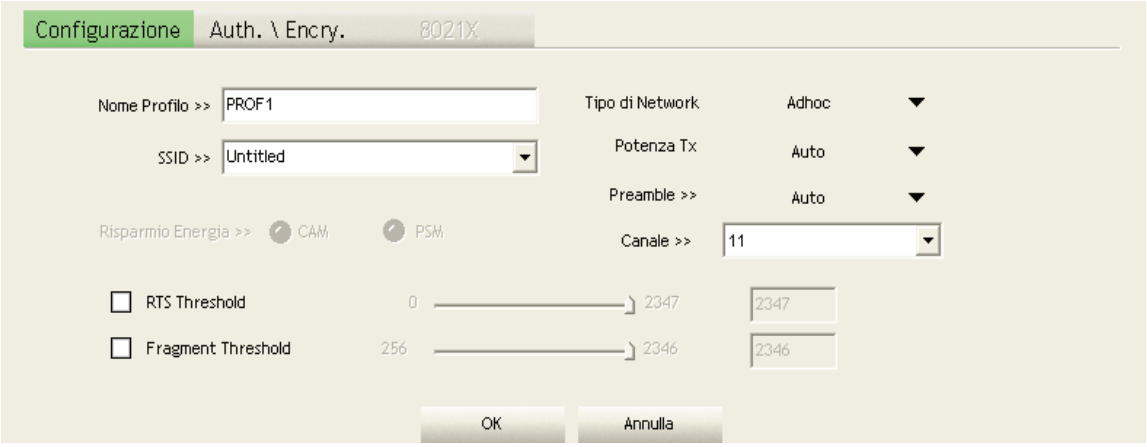
La modalità Infrastructure richiede l'utilizzo di un Access Point (AP) attraverso il quale avvengono tutte le comunicazioni di tipo wireless. L'AP può essere collegato ad una rete Ethernet o stand-alone, in quest'ultimo caso può aumentare il raggio di azione della rete wireless fungendo da repeater raddoppiando così la distanza tra le postazioni wireless.




- **Nome Profilo:** Inserire un nome per il profilo che si vuole aggiungere. Non deve essere necessariamente uguale all' SSID.
- **SSID**: Inserire l'SSID della rete o selezionarne uno dalla lista a tendina. L'SSID è un nome univoco condiviso tra tutti i punti di accesso della rete ed è case-sensitive, attribuisce cioè un diverso valore alle stringhe di caratteri identici se scritte in maiuscolo o minuscolo.
- **Risparmio Energia:** Selezionare l'opzione di Risparmio Energetico.
  - **CAM (Continuously Awake Mode)**: Selezionare questa opzione se il vostro notebook è collegato ad un alimentatore.
  - **PSM (Power Saving Mode)**: Selezionare questa opzione se il vostro notebook utilizza la propria batteria. Questa opzione ridurrà al minimo l'utilizzo della batteria mentre la rete non è in funzione.
- **Tipo di Network:** Selezionare **Infrastructure** dal menu a tendina.
- **Potenza TX:** Selezionare la potenza di trasmissione dal menu a tendina. Se il notebook è connesso ad una porta esterna allora selezionare **100**% o **auto**, in caso contrario selezionare uno dei valori più bassi per risparmiare energia.
- **RTS Threshold:** casella di controllo per attivare la Soglia RTS. Tutti I pacchetti più grandi del valore specificato (byte) saranno scartati.
- **Fragment Threshold:** casella di controllo per attivare la soglia di frammentazione. Tutti I pacchetti più grandi del valore specificato (byte) saranno scartati.
- Cliccare **OK** per salvare le modifiche.

### 2.3.2. Modalità "Ad-Hoc"

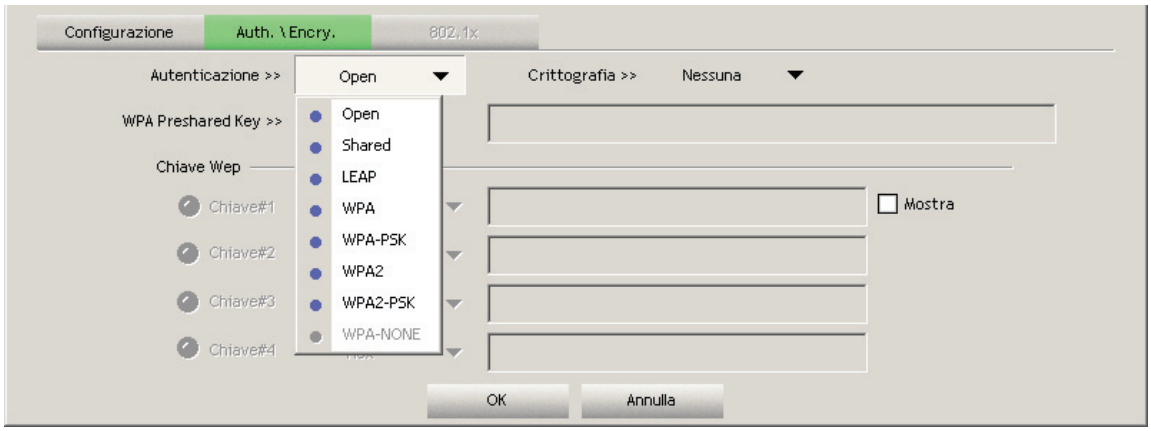
Questa è la configurazione di rete più semplice tra più computer che formano tra loro una rete wireless. Nella modalità Ad-Hoc ogni client ha solo accesso alle risorse condivise dagli altri client e non necessita l'utilizzo di un AP. Questa è la soluzione ideale e meno costosa per realizzare una rete wireless per piccoli uffici o uffici domestici.




- **Nome Profilo:** Inserire un nome per il profilo che si vuole aggiungere. Non deve essere necessariamente uguale all'SSID.
- **SSID**: Inserire l' SSID della rete o selezionarne uno dalla lista a tendina. L'SSID è un nome univoco condiviso tra tutti i punti di accesso della rete ed è case-sensitive, attribuisce cioè un diverso valore alle stringhe di caratteri identici se scritte in maiuscolo o minuscolo.
- **Tipo di Network:** Selezionare **Ad-Hoc** dal menu a tendina.
- **Potenza TX:** Selezionare una fonte di trasmissione dalla lista a tendina. Se il vostro notebook ha una alimentazione esterna selezionare 100% oppure auto, in caso contrario selezionare trai valori più bassi per migliorare il risparmio energetico.
- **Preamble:** Selezionare Auto da menu a discesa, a meno che non sappiate il tipo di preamble (long o short) utilizzato in ogni stazione.
- **Channel:** Mostra il canale radio utilizzato dall'Access Point.
- Fare click su **OK** per salvare le modifiche.

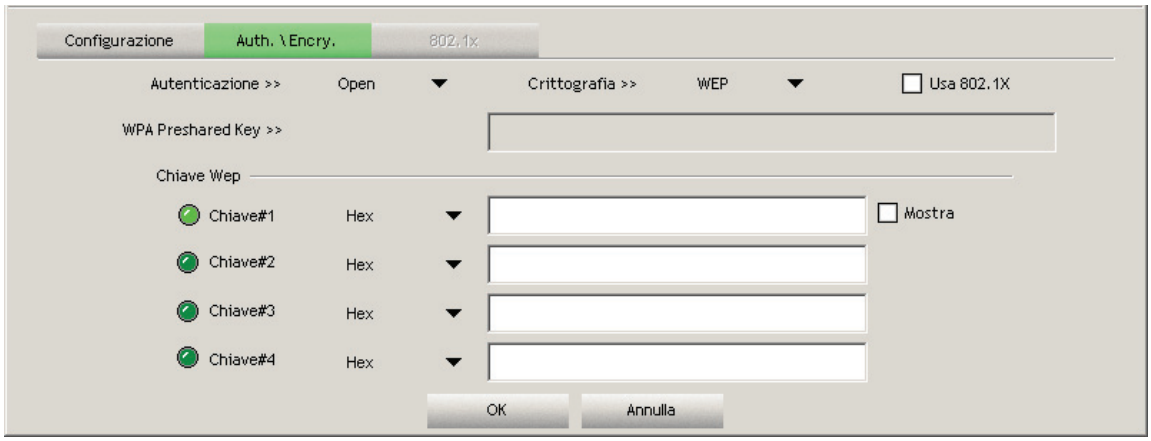
## 2.4 Autenticazione e Sicurezza

La schermata **Auth\Encry.** consente di configurare le impostazioni di autenticazione e la crittografia per: WEP, WPA, WPA-PSK. Ogni opzione è illustrata in dettaglio di seguito.




### 2.4.1. Crittografia WEP

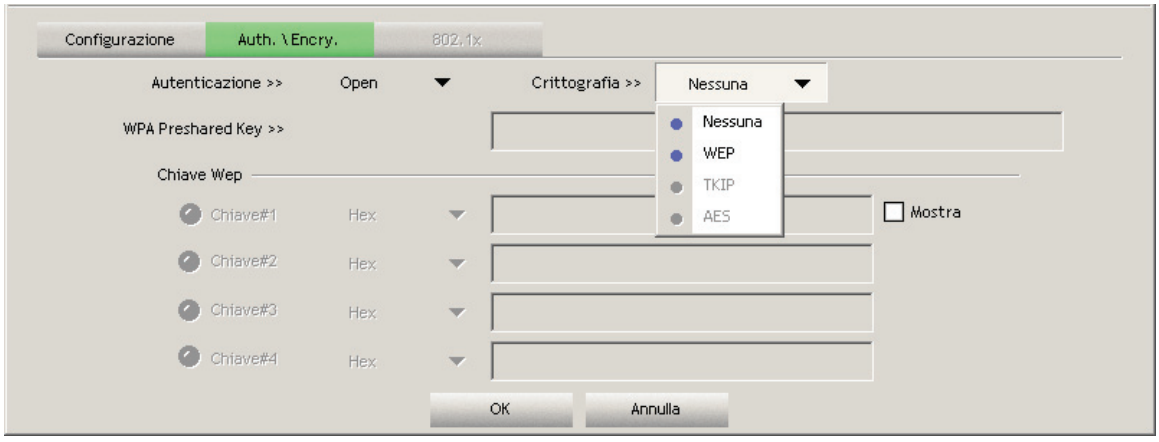
La schermata **WEP** mostra le impostazioni WEP. La crittografia è studiata per rendere la trasmissione dei dati sicura. È possibile scegliere tra 64 o 128-bit WEP (Wired Equivalent Privacy) per criptare i dati ( tale funzione è disabilitata di default). Il WEP cripterà ogni frame trasmesso via radio utilizzando una delle chiavi inserite nella schermata. Quando si utilizza il WEP per comunicare con uno dei client wireless, tutte le periferiche wireless della rete devono avere la stessa chiave di criptazione o frase d'accesso. Tutte queste informazioni sono rappresentate nell'immagine seguente.




- **Autenticazione:** Selezionare **Open** o **Shared** dal menu a tendina.
- **Crittografia:** Selezionare WEP dal menu a tendina.
- **Chiave WEP:** digitare la stringa di caratteri nel campo. Per 64-bit inserire 5 caratteri alfanumerici o 10 caratteri esadecimali. Per 128-bit inserire 13 caratteri alfanumerici o 26 caratteri esadecimali.
- Fare click su **OK** per salvare le modifiche.
- **Mostra:** per verificare la password digitata, selezionare la casella **Mostra**.

### 2.4.2. Autenticazione WPA, WPA2 & Crittografia TKIP, AES

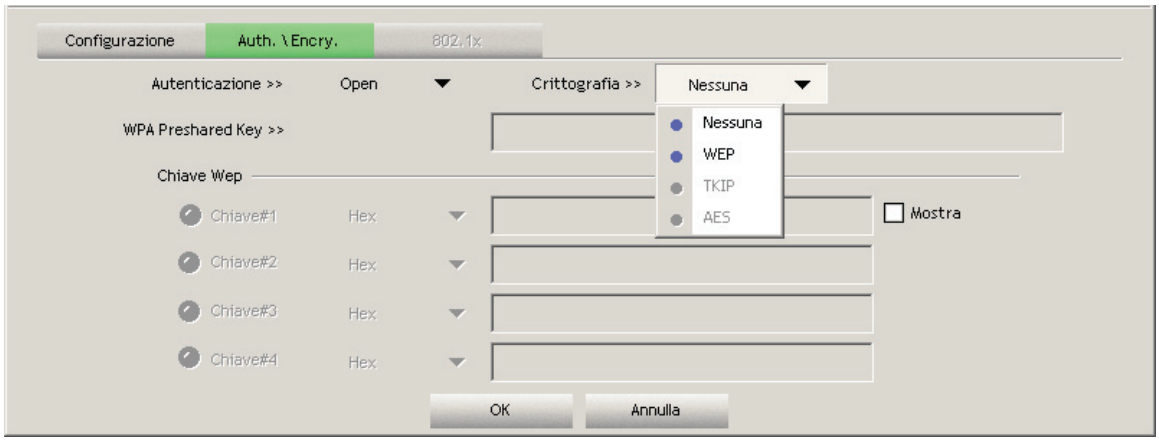
Il WPA (Wi-Fi Protected Access) è stato pensato per aumentare le caratteristiche di sicurezza del WEP (Wired Equivalent Privacy). Il WPA fornisce una ulteriore crittografia dei dati grazie al Temporal Integrity Protocol (TKIP) mescolando alla rinfusa le chiavi basandosi su un algoritmo hashing e aggiungendo una funzionalità di integrity-checking per verificare che le chiavi non siano state manomesse. EAP (Extensible Authentication Protocol) è un'estensione del protocollo PPP che consente l'utilizzo di un certo numero di protocolli di autenticazione. Esso passa attraverso lo scambio di messaggi di autenticazione autorizzando il software presente nel server ad interagire con la sua controparte lato client.




- **Autenticazione**: Selezionare **WPA** o **WPA2** dalla lista a tendina.
- **Crittografia:** Selezionare **TKIP** o **AES** dalla lista a tendina.
- Fare click su **OK** per salvare le modifiche.
- **Mostra:** per verificare che la password digitata sia corretta selezionare la casella di controllo **Mostra**.

### 2.4.3. Autenticazione WPA-PSK & Crittografia TKIP, AES

Il WPA – PSK (Pre-shared Key) è usato nella modalità Pre-shared Key e non richiede un server di autenticazione. L'accesso alla rete e a tutti i servizi di rete wireless sono possibili solo se la PSK del computer coincide con quella dell'AP garantendo così una maggiore crittografia TKIP.
L'EAP (Extensible Authentication Protocol) è una estensione del protocollo PPP che abilita l'utilizzo di diversi protocolli di autenticazione. Esso passa attraverso lo scambio di messaggi di autenticazione autorizzando il software presente nel server ad interagire con la sua controparte lato client.




- **Autenticazione**: Selezionare **WPA** or **WPA2** dalla lista a tendina.
- **Crittografia:** Selezionare **TKIP** o **AES** dalla lista a tendina.
- **WPA Preshared key:** Inserire una frase di accesso la cui lunghezza deve essere compresa tra 8 e 32 caratteri.
- Fare click su **OK** per salvare le modifiche.
- **Mostra:** per verificare che la password sia digitata correttamente selezionare la casella **Mostra**.

### 2.4.4. Autenticazione LEAP

LEAP (Lightweight Extensible Authentication Protocol) anche conosciuto come Cisco-Wireless EAP fornisce username/password basati sull'autentificazione tra un client wireless e un server RADIUS. L'LEAP è uno dei protocolli utilizzati con lo standard IEEE 802.1X per il controllo d'accesso alle porte LAN. Inoltre rilascia una session key (chiave di sessione) alla stazione autentificata cosicché i frame successivi possono essere criptati con una chiave diversa da quelle utilizzate nelle altre sessioni. Il rilascio di una chiave dinamica elimina un grosso problema di vulnerabilità: la cifratura delle chiavi statiche condivise da tutte le stazioni della rete wireless WLAN. L'EAP (Extensible Authentication Protocol) è un'estensione del protocollo PPP che abilita l'utilizzo di molteplici protocolli di autenticazione. Esso passa attraverso lo scambio di messaggi di autenticazione autorizzando il software presente nel server ad interagire con la sua controparte nel client.

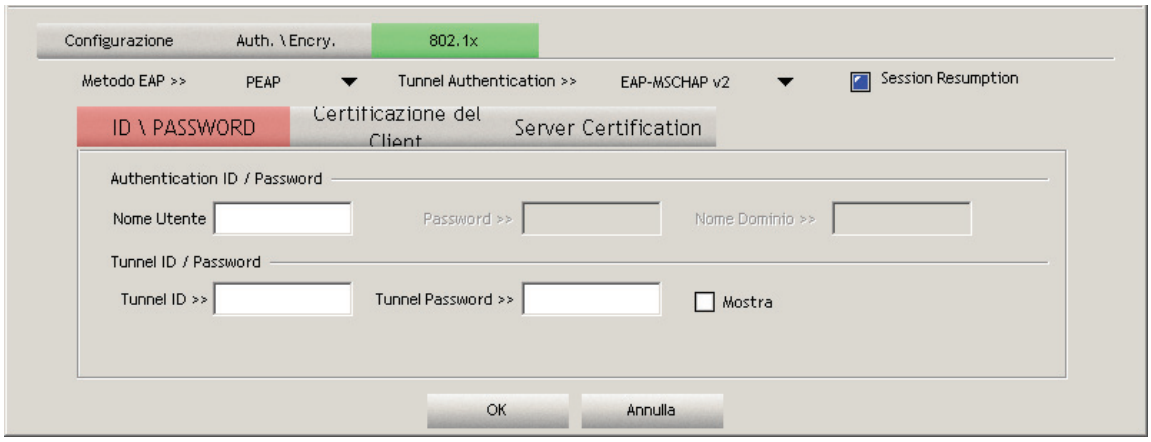

- **Autenticazione**: Selezionare **LEAP** dal menu a tendina.
- **Identity:** Inserire il nome utente.
- **Password**: Inserire la password.
- **Dominio**: Inserire il nome del dominio.
- **Crittografia**: Selezionare **WEP**, **WPA-TKIP** o **WPA2-AES** encryption.
- Cliccare **OK** per salvare le modifiche.

## 2.4.5. 802.1x con PEAP

La scheda 802.1X fornisce una piattaforma di autenticazione per le reti wireless permettendo l'autenticazione dell'utente da parte di una authority.
802.1X utilizza il protocollo EAP (Extensible Authentication Protocol) che è una estensione del protocollo PPP che abilita l'utilizzo di molteplici protocolli di autenticazione. Esso passa attraverso lo scambio di messaggi di autenticazione autorizzando il software presente nel server ad interagire con la sua controparte nel client.

### 2.4.5.1. PEAP Authentication with EAP/TLS Smartcard

EAP/TLS Smartcard permette la reciproca autenticazione basata su certificato del client e della rete. Essa si basa su certificati lato client e lato server per eseguire l'autenticazione e può essere utilizzata per generare dinamicamente chiavi WEP basate sull'utente e sulla sessione per consentire una successiva comunicazione protetta tra il client wireless e l'access point.




- **Metodo EAP**: Selezionare **PEAP** dal menu a tendina.
- **Tunnel Authentication**: se la vostra rete utilizza un TLS o una Smart Card per autentificare gli utenti, selezionare **TLS/Smartcard** dalla lista. **TLS** (Transport Layer Security) è un protocollo di autenticazione standard IETF che utilizza l'autenticazione PKI (Public Key Infrastructure) basata su certificato sia per il server di autenticazione che per il client.
- **Nome Utente**: Inserire user name.
- Cliccare **OK** per salvare le modifiche.

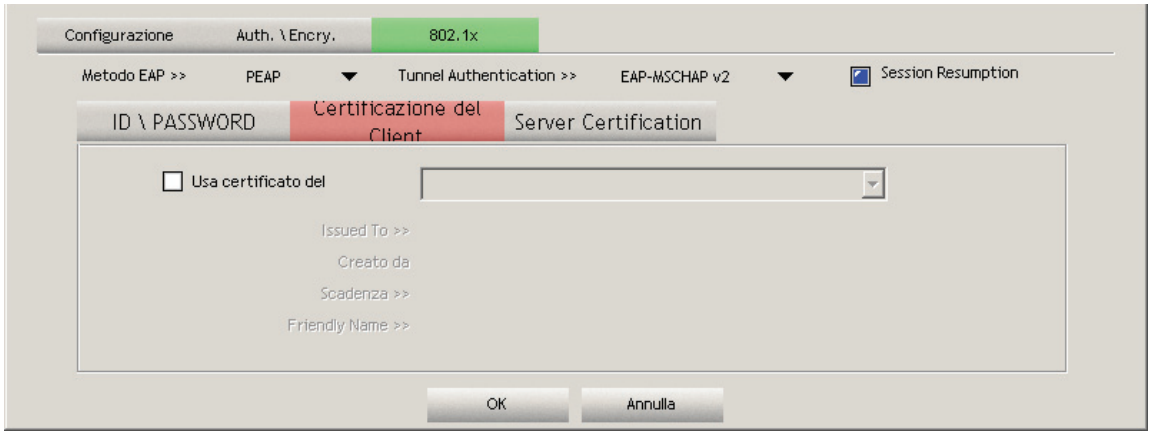
### 2.4.6. 802.1x with TTLS with EAP-MD5, MS-CHAP, MS-CHAPv2

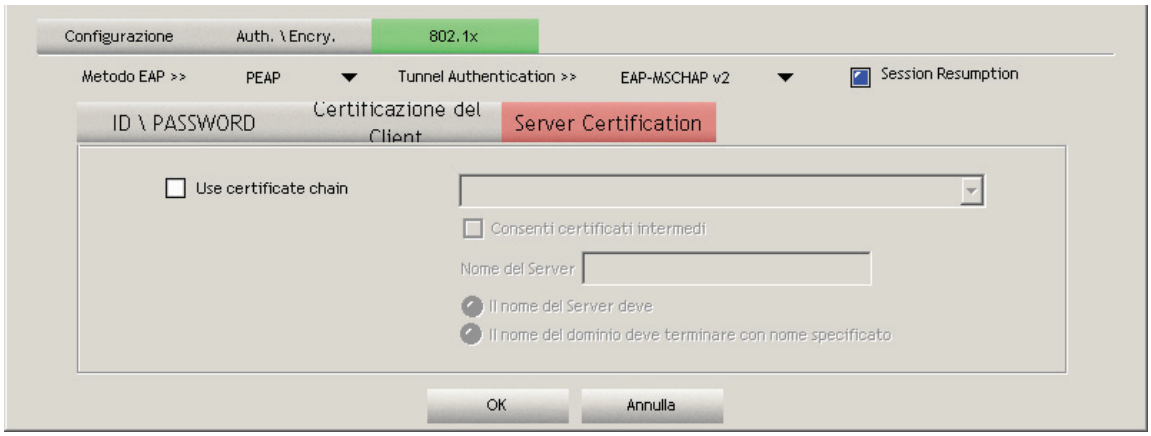
802.1X fornisce un framework di autenticazione per le reti wireless permettendo l'autenticazione dell'utente da parte di una authority.
802.1X utilizza il protocollo EAP (Extensible Authentication Protocol) che è una estensione del protocollo PPP che abilita l'utilizzo di molteplici protocolli di autenticazione. Esso passa attraverso lo scambio di messaggi di autenticazione autorizzando il software presente nel server ad interagire con la sua controparte nel client.
TLS (Transport Layer Security) è un protocollo di autenticazione sntandardizzato IETF ed utilizza un sistema di autenticazione basato su certificati PKI (Public Key Infrastructure) per l'autentificazione del server e del client.


- **Metodo EAP**: Selezionare **TTLS** dalla lista a tendina.
- **Tunnel Authentication**: Selezionare EAP-MSCHAP v2, MS-CHAP, o CHAP dal menu a tendina.
- **Identity**: Inserire il Nome Utente.
- **Password**: Inserire la password.
- Cliccare **OK** per salvare le modifiche.

### 2.4.7. 802.1x CA Server

A seconda dell'EAP utilizzato possono essere autentificati solo il server o server e client e può essere richiesto un certificato. I certificati Server identificano un server, solitamente un server di autenticazione o RADIUS ai client. La maggior parte degli EAPs richiedono un certificato fornito da un'autorità principale o un'autorità di certificazione commerciale autorizzata.

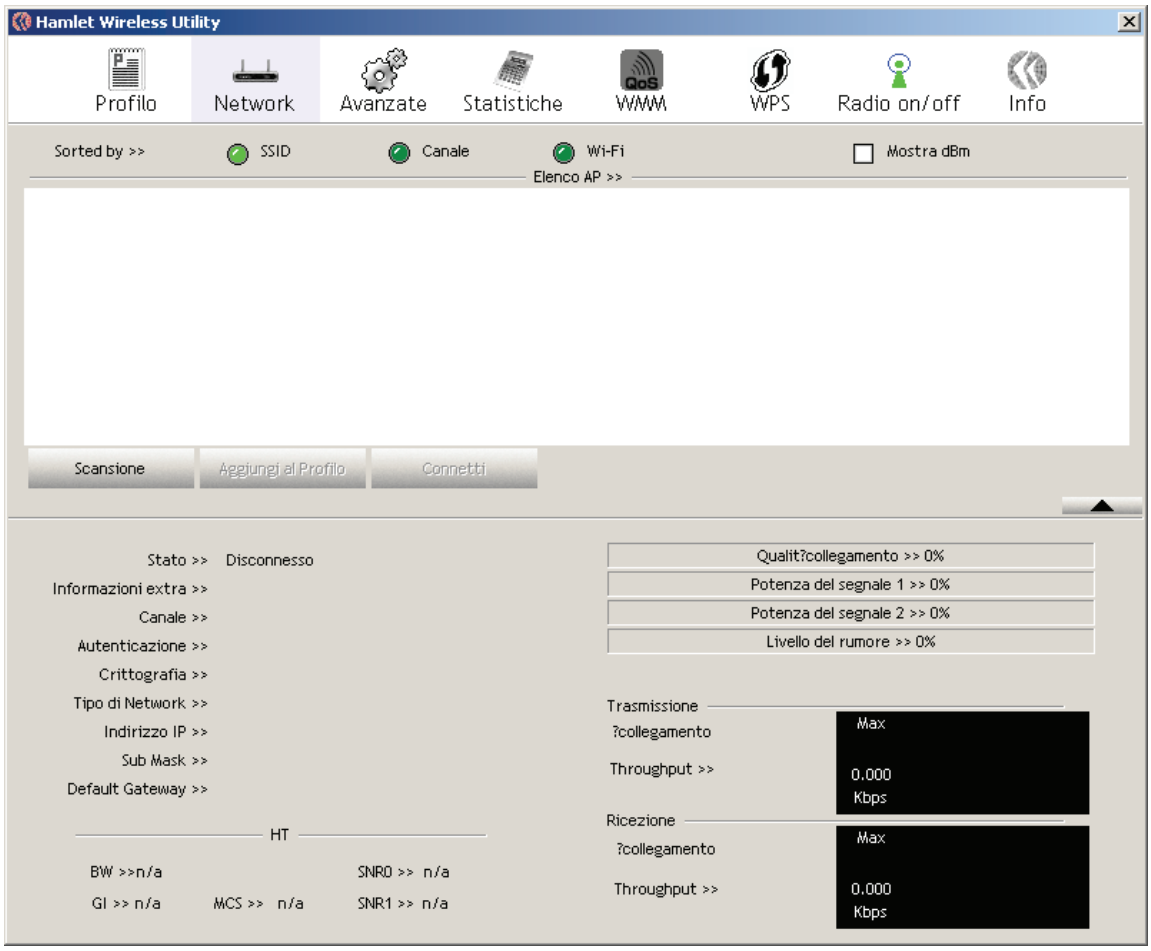



- **Use certificate chain**: Selezionare questa casella di controllo per utilizzare un certificato.
- **Fornitore del certificato**: Selezionare una Certification Authority dalla lista.
- **Consenti certificati intermedi:** Durante la creazione del tunnel di comunicazione il client deve verificare il certificato del server. Durante questa verifica la firma viene verificata confrontandola con una lista di autorità certificate affidabili. Se il parametro riportato risulta vero allora il client utilizzerà anche la firma di un'autorità certificata intermedia, in caso contrario non lo farà.
- **Nome del Server:** Inserire il nome del server se non selezionato in precedenza dalla lista a tendina.
- Cliccare **OK** per salvare le modifiche.

## 2.5 Network (Rete)

La schermata **Network** mostra lo stato attuale della rete wireless.

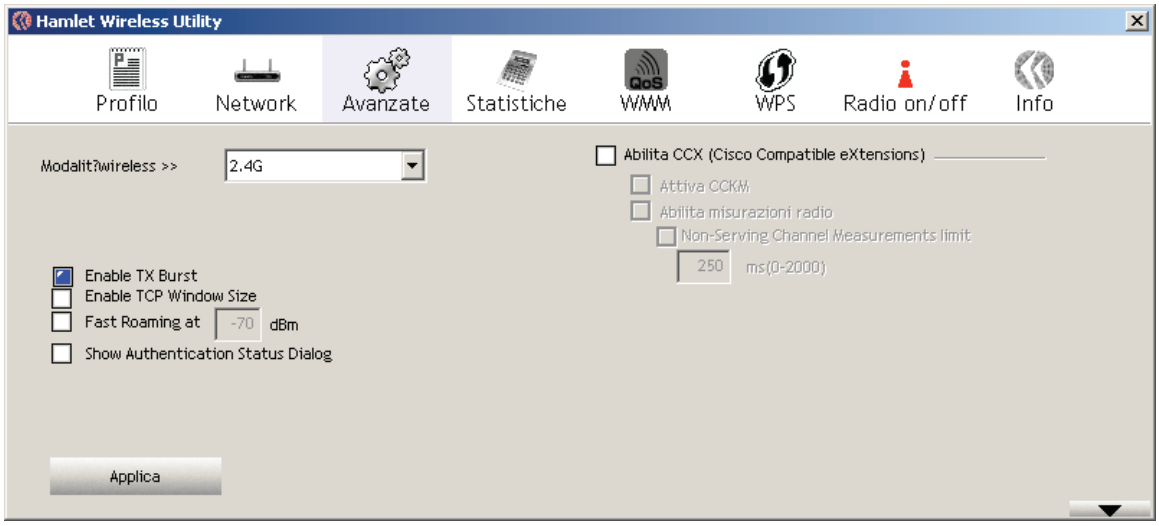



- **SSID**: Mostra l'SSID dell'Access Point. L'SSID è un nome univoco condiviso tra tutti i punti di accesso della rete ed è case-sensitive, attribuisce cioè un diverso valore alle stringhe di caratteri identici se scritte in maiuscolo o minuscolo.
- **MAC**: Indirizzo MAC dell'Access Point.
- **Canale**: Mostra il numero del canale dell'Access Point.
- **Crittografia**: Mostra la crittografia dell'Access Point, compresi WEP, TKIP, AES o Nessuno.
- **Segnale**: Mostra la forza del segnale ricevuto dall'AP.
- **Scansione:** fare click qui per aggiornare l'elenco di Access Points presenti nell'area.
- **Connetti**: per connettersi ad uno specifico Access Point, selezionare l'SSID dalla lista, poi fare click su **Connetti**.
- **Attiva**: imposta l'AP selezionato come AP predefinito.
- **Aggiungi al Profilo**: fare click qui per aggiungere l'SSID e le relative impostazioni nel profilo.

- **Stato:** Indica lo stato del client. Esistono 3 opzioni:
  - **Connesso:** Indica che il client wireless è connesso a un Access Point (AP). Il BSSID è sotto forma di cifra a 12 caratteri esadecimali ed è l'indirizzo MAC dell'AP.
  - **Scansione:** Indica che il client wireless sta cercando un AP nell'area.
  - **Disconnesso:** non ci sono AP o client nell'area.
- **Informazioni extra:** qui vengono fornite le informazioni relative al link status e alla percentuale di potenza in uscita.
- **Canale:** Mostra la frequenza del Canale utilizzato dal client (infrastructure mode).
- **Autenticazione:** Mostra il tipo di Autenticazione in uso.
- **Crittografia:** Mostra il tipo di Crittografia.
- **Tipo di Network:** Mostra il tipo di rete; infrastructure o ad-hoc.
- **Indirizzo IP:** Mostra l'indirizzo IP.
- **Sub Mask:** Mostra la subnet mask dell'indirizzo IP.
- **Default Gateway:** Mostra l'indirizzo IP del gateway predefinito.
- **Velocità**: attuale valore di trasmissione e ricezione del client.
- **Throughput:** Mostra i kilo-bytes trasmessi e ricevuti per secondo Tx (trasmessi) e Rx (ricevuti).
- **Qualità collegamento:** Nella modalità infrastructure, questa barra mostra la qualità di trasmissione tra l'AP e il client. Nella modalità Ad-Hoc mostra la qualità di trasmissione tra un client e l'altro.
- **Potenza del segnale:** Questa barra mostra la forza del segnale ricevuto dall'AP o dal client.
- **Livello del rumore:** Mostra il livello di rumore; minore è il livello minori sono le interferenze.
- **HT: High Through-Put / 802.11 n Section**
  - **BW: Channel Bandwidth**.
  - **GI:** Guard Interval.
  - **MCS:** Modulation Coding Scheme.
  - **SNR:** Signal Noise Rate.

## 2.6 Configurazione Avanzata

La schermata **Avanzate** è utilizzata per configurare la modalità wireless (802.11g, 802.11b/g-mixed, o 802.11b/g/n-mixed), Tx burst, e CCX.

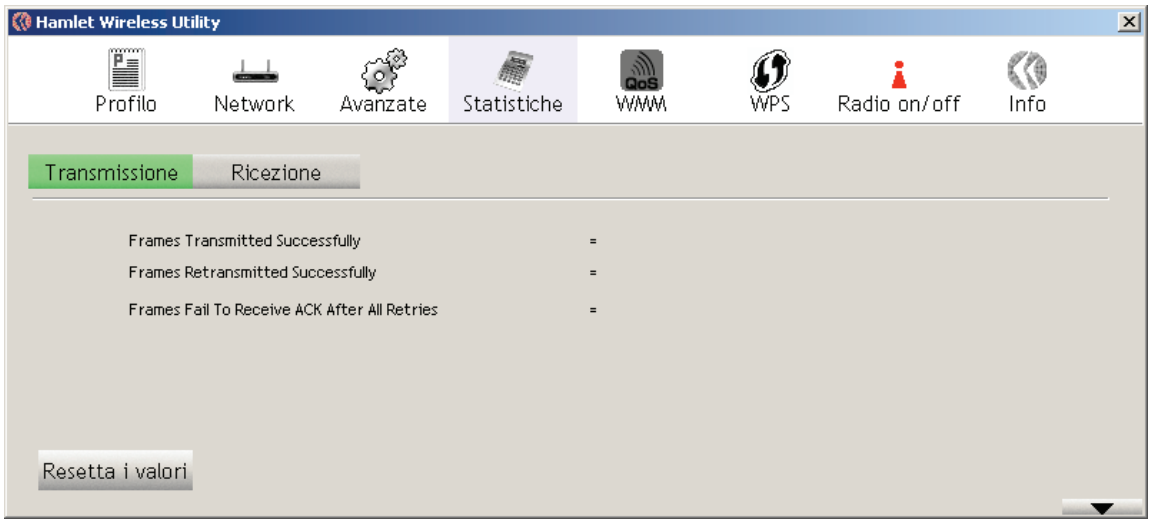


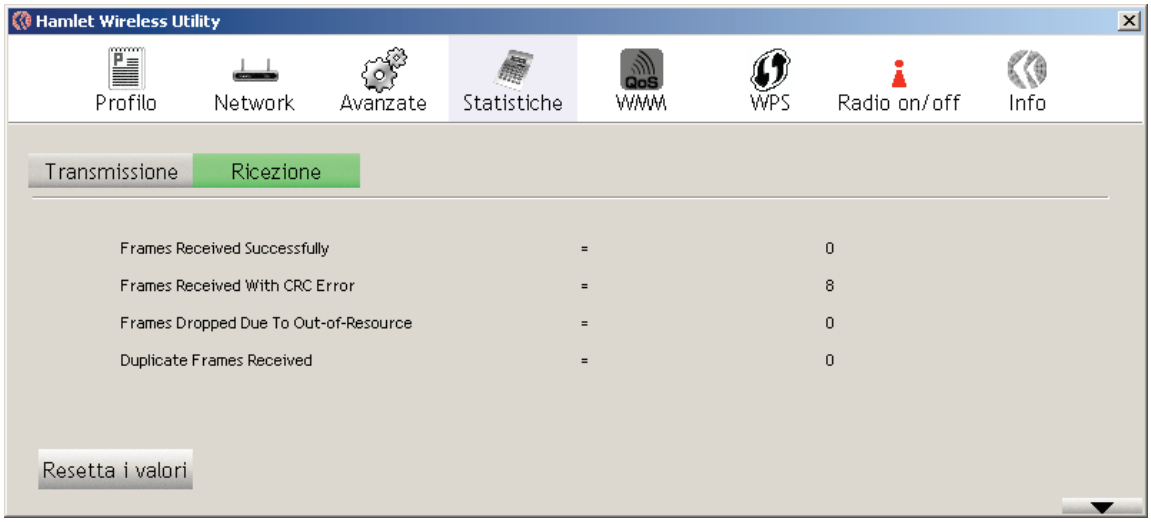

- **Modalità wireless**: Selezionare **802.11 b/g/n mix** se la rete wireless utilizza entrambe le stazioni 11b, 11g, e 11n e gli AP. **B/G Protection**: è la modalità di protezione ERP del 802.11g. Selezionando **auto** invierà frame con e senza protezione. Selezionare **On** per inviare un frame senza protezione, e **Off** per inviarlo con la protezione.
- **Enable Tx BURST**: selezionare questa casella per abilitare il TX Burst.
- **Enable TCP Window Size**: abilitare questa opzione per milgiorare la capacità della banda dati.
- **Abilita CCX**: Abilitare questa opzione se la rete supporta Cisco Compatible Extensions.
- Cliccare **Applica** per salvare le impostazioni.

**NOTA**
Alcune impostazioni della scheda di configurazione avanzata sono disponibili e selezionabili solo in Windows XP.

## 2.7 Statistiche

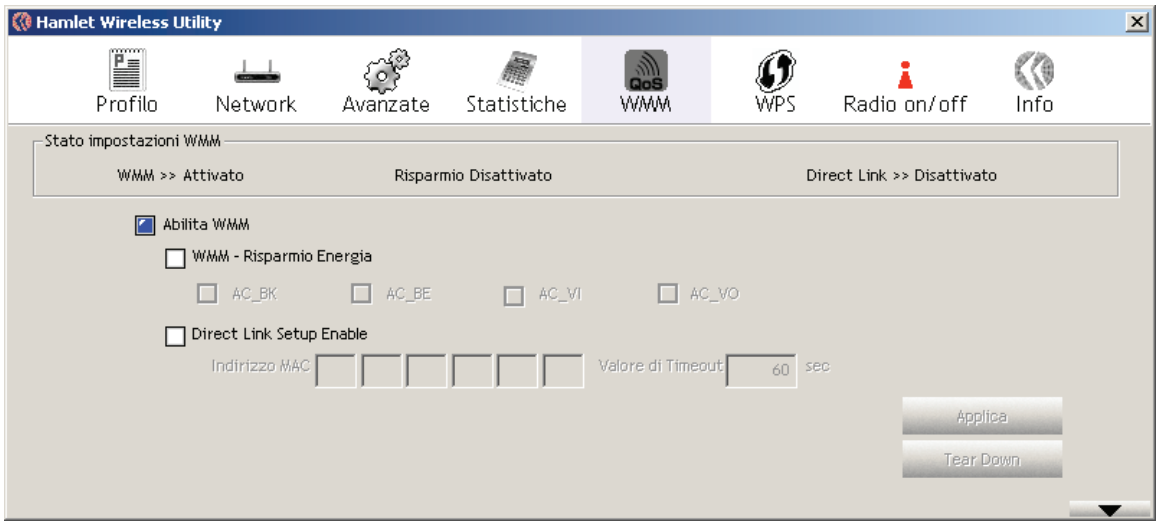
La schermata **Statistiche** mostra le statistiche in tempo reale dei pacchetti inviati e ricevuti. Le informazioni visualizzate riguardano frame trasmessi/ricevuti con successo, trasmessi con successo senza riprovare o dopo alcuni tentativi, ricevuti con errore CRC, frame duplicati, etc.



## 2.8 WMM (Wireless MultiMedia)

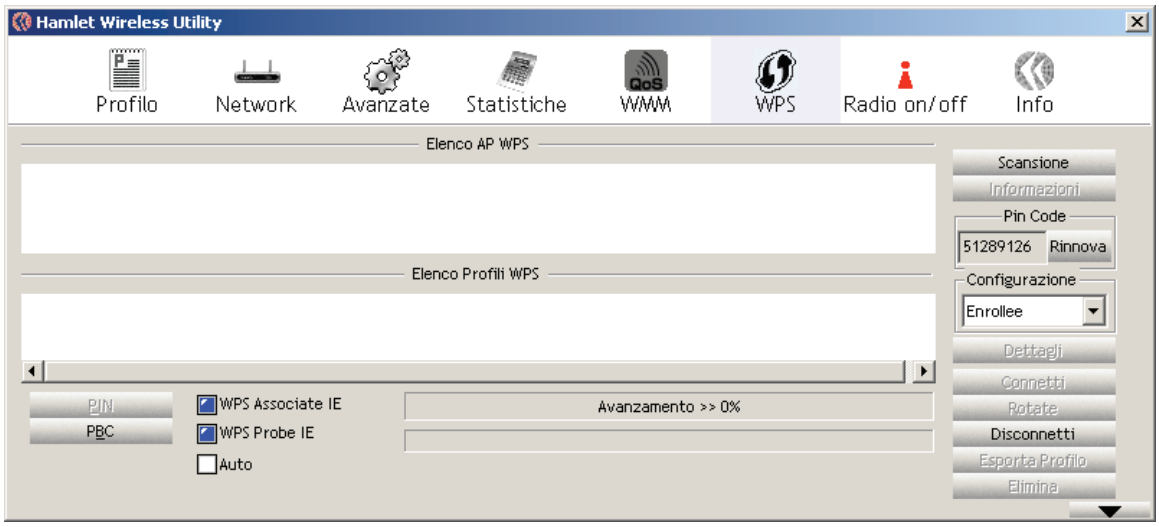
Il menu **WMM** (Wireless Multimedia), anche conosciuto come WME (Wireless Multimedia Extensions) è una funzione Wi-Fi basata sullo standard IEEE 802.11e. Essa fornisce caratteristiche di base quali il Quality of Service (QoS) alla rete IEEE 801.11. Inoltre il WMM assegna al traffico di rete diverse priorità basandosi su quattro categorie di accesso. L'utilizzo di questa funzione è consigliabile per applicazioni che richiedono il QoS quali telefoni Voip o giochi on line.




- **Abilita WMM**: Selezionare per abilitare/disabilitare WMM.
- **WMM – Risparmio Energia**: Selezionare per abilitare la modalità risparmio energetico in WMM.
- **Direct Link Setup Enable**: specificare un indirizzo MAC ed un valore di timeout.
- Cliccare su **Applica** per salvare le impostazioni e chiudere la finestra.

## 2.9 WPS

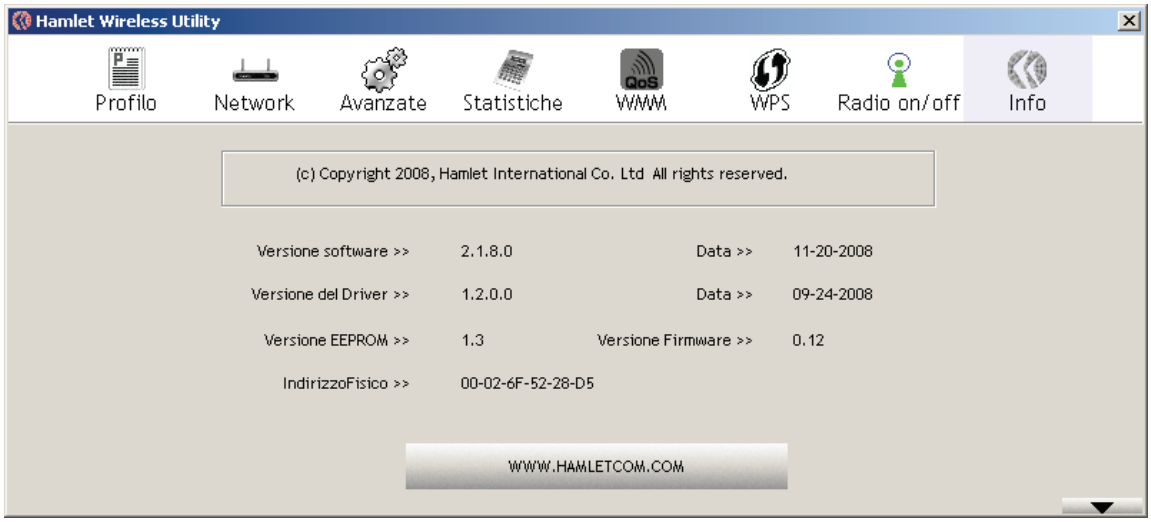
Il WPS (Wireless Push Button) è usato per abilitare le protezioni sulla rete Wi-Fi. Premendo questo pulsante le impostazioni di sicurezza della periferica saranno automaticamente sincronizzate con le altre periferiche della propria rete che supportano Il WPS.




- **Scansione:** Premere il pulsante per vedere gli Access Point presenti nell'area.
- **Informazioni:** visualizza le informazioni relative al WPS della rete selezionata. La lista delle informazioni include il tipo di autenticazione, la crittografia, i metodi di configurazione, la password, I registri, lo stato, la versione…
- **Pin Code:** è un numero a 8 cifre. È necessario registrare un PIN Code utilizzando il metodo PIN. Quando il terminale wireless è registrato (**Enrollee**), potete utilizzare il pulsante **Rinnova** per generare un nuovo PIN Code.
- **Dettagli:** informazioni sulla Sicurezza e le Chiavi.
- **Connetti:** comando da usare per connettersi alla rete selezionata nelle credenziali. Le credenziali attive selezionate sono come i profili selezionati attivi.
- **Rotate:** comando che serve a cambiare la connessione dalla rete attuale verso quella successive nelle credenziali.
- **Disconnetti: :** interrompe la funzione WPS e disconnette il collegamento attivo. A quel punto sarà selezionato l'ultimo profilo nella pagina dei profili. Se la pagina è vuota i driver selezioneranno una connessione non protetta.
- **Esporta Profilo:** esporta tutte le credenziali verso il profilo.
- **PBC:** aggiunge AP usando il metodo preconfigurato da PCB.
- Cliccare su **OK** nel caso abbiate modificato delle impostazioni.

## 2.10 Info

Il pannello **Info** mostra informazioni relative alla periferica, come: la data di rilascio e la versione driver e dell'utility di configurazione, la versione del firmware del NIC (Network Interface Card).




## 2.11 Radio On/Off

Il pulsante **Radio On/Off** permette semplicemente di abilitare o disabilitare la trasmissione del segnale wireless.

## 2.12 Rimozione dei Driver e del Software

Se l'installazione della scheda PCI non fosse avvenuta correttamente, il modo migliore per risolvere il problema è rimuovere la scheda PCI stessa e il relativo software quindi procedere a una nuova installazione.

Per disinstallare i driver, seguire la procedura descritta di seguito:

1. Fare click su **Start** > **Hamlet Wireless** > **Unistall Hamlet Wireless PCI Adapter**.

2. Inizierà così la procedura di rimozione dei driver e del software.

3. Nella schermata successiva fate click su **Yes** per confermare.

4. Una volta terminato il processo di disinstallazione, premete il pulsante **Finish**. Ora potete rimuovere la scheda PCI dal computer.

# 3. Specifiche

| | |
|---|---|
| **HARDWARE** | |
| Standard IEEE | 802.11b, 802.11g, 802.11n (draft 2.0) |
| Interfaccia | PCI 2.2 slot |
| Voltaggio | 3.3V |
| LED | Link/Activity |
| Antenna | 2 antenne esterne da 2dBi (2,4GHz) |
| Attacco antenna | SMA Female-Reverse |
| **RADIO** | |
| Banda di frequenza | 2.400~2.484 GHz |
| Modulazione | OFDM: BPSK, QPSK, 16-QAM, 64-QAM<br>DSS: DBPSK, DQPSK, CCK |
| Canali operativi | 11 in Nord America, 13 in Europe, 14 in Giappone |
| Impostazioni Wireless | Modalità Wireless – 11b/11g/11n<br>Selezione Canale (dipende dalla nazione)<br>Banda Canale (Auto, 20MHz, 40MHz)<br>Velocità di trasmissione: 150, 84, 72, 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps |
| Sensibilità in ricezione (Tipica) | 2.412~2.472G (IEEE802.11b) (1Rx)<br>-91 dBm @ 1Mbps<br>-87 dBm @ 11Mbps<br>2.412~2.472G (IEEE802.11g) (2Rx)<br>-90 dBm @ 6Mbps<br>-75 dBm @ 54Mbps<br>2.412~2.472G(IEEE802.11n) (2Rx)<br>-88 dBm MCS 8<br>-65 dBm MCS 15 |
| Potenza di trasmissione | 2.412~2.472G (IEEE802.11b)<br>18 dBm @1~11Mbps<br>2.412~2.472G (IEEE802.11g)<br>15 dBm @6Mbps<br>14 dBm @54Mbps<br>2.412~2.472G (IEEE802.11n)<br>15 dBm |
| Certificazioni | FCC Part 15, ETSI 300/328/CE |
| **SOFTWARE** | |
| Wireless | WPA/WPA2 (AES, 64,128-WEP con autenticazione tramite chiave condivisa)<br>WPS (WiFi Protected Setup) tramite software<br>QoS-WMM |
| Sistemi operativi supportati | Windows 2000/XP/Vista |
| **CONDIZIONI AMBIENTALI** | |
| Temperatura | 0 ~ 45° C – In uso<br>-10 ~ 70 ° C – In magazzino |
| Umidità (senza condensa) | 15% ~ 95% tipica |