

**theremino**  
•the•real•modular•in-out•

**Sistema** theremino

# VPN Help

## Collegamenti attraverso Internet



Alcune applicazioni del sistema theremino (SlotsOverNet, loTHAL e NetHAL) che normalmente si utilizzano in rete locale, possono comunicare anche attraverso Internet.

Il collegamento attraverso Internet richiede un IP fisso, inoltre si deve scegliere una porta e questa porta non deve venire bloccata dai firewall.

In alternativa è possibile utilizzare alcuni tipi di VPN che forniscono un collegamento di tipo "Mesh con connessione diretta".

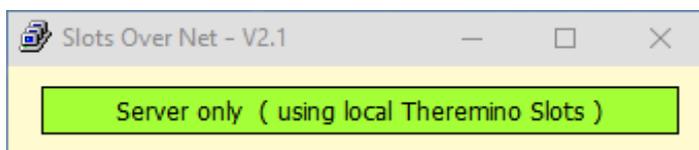
Una VPN comoda e gratuita (fino a cinque collegamenti contemporanei) potrebbe essere Hamachi (di LogMeIn).

Non abbiamo alcun interesse a consigliarvela, non siamo in contatto con loro e non ci pagano, se volete (e riuscite) usatene pure un'altra.

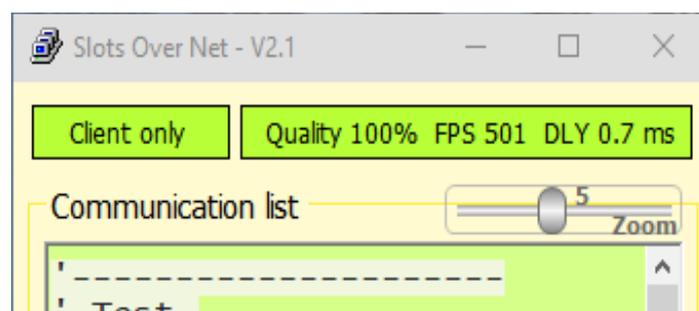
## Utilizzare la VPN con SlotsOverNet

Per far comunicare SlotsOverNet via Internet si procede come se si lavorasse su una rete locale.

Si dovrà avviare un solo server, su uno qualunque dei PC.



Tutte le altre applicazioni SlotsOverNet, una per ogni PC, dovranno essere configurate come "Client only".



Non si dovrà fare altro perché la VPN si occuperà di far vedere tutti i PC come se fossero nella stessa rete locale.

## Utilizzare la VPN con loTHAL e NetHAL

Leggere la documentazione delle applicazioni e procedere come se si lavorasse in rete locale, la VPN si occuperà di tutto il resto.

# Installare la VPN

## Download e installazione della VPN Hamachi

- ◆ Fare il download da qui: <https://www.vpn.net> e lanciare hamachi.msi
- ◆ Scegliere la lingua e premere "Next"
- ◆ Accettare il contratto di licenza e premere "Avanti"
- ◆ Crea collegamento sul Desktop e premere "Avanti"
- ◆ Attenzione a non installare LastPass o altri programmi e premere "Installa"
- ◆ Se Windows chiede il permesso concederlo per "Rete privata"

Quando Hamachi chiede "Crea rete" o "Partecipa" **non creare la rete e non partecipare**. Per creare la rete e per i dettagli della configurazione della VPN si utilizza [questa pagina](#).

## La prima volta

- ◆ Registrare il proprio account su [questa pagina](#).
- ◆ Nella registrazione immettere una mail valida e una password e premere "Crea account"
- ◆ Se Windows chiede il permesso concederlo per "Rete privata"

The screenshot shows the LogMeIn dashboard. On the left is a navigation menu with options: Computer, Utenti, Report (with a sub-option Visualizzatore report), and Reti (with sub-options Reti personali, Distribuzione, and Impostazioni di rete). The main area is titled 'Reti' and contains two buttons: 'Aggiungi client' and 'Aggiungi rete'. Below these is a table of networks. The first row shows a network named 'SlotsOverNet2' with a status of 'Mesh • Free • 2 / 5 Client • 1 in linea'. Below this, two clients are listed: 'DESKTOP-J9DV6E6 [Ospite]' and 'LAB1', both with a status of '24€'.

Client	ID c
SlotsOverNet2	Mesh • Free • 2 / 5 Client • 1 in linea
DESKTOP-J9DV6E6 [Ospite]	24€
LAB1	24€

## Collegare i PC attraverso la VPN Hamachi

Dopo aver installato la VPN e aver creato l'account LogMeIn e aver creato una nuova rete, si deve partecipare alla rete.



- ◆ Una volta creata la rete andare sul programma Amachi e premere "Partecipa alla rete".
- ◆ Se Windows chiede il permesso concederlo per "Rete privata".
- ◆ Andare sulla pagina web della configurazione e dare il consenso alla partecipazione (per evitare questo si potrebbe modificare la rete per non farle chiedere il consenso).
- ◆ Quando il programma Hamachi chiede "ID-Rete" non dare il nome della rete ma il suo "ID" (altrimenti avviene un errore password rejected).
- ◆ L'ID è nella pagina web della configurazione, menu a sinistra, reti / Reti personali / Cliccare sul primo modifica in alto / Il primo numero in alto a sinistra è l'ID della rete.
- ◆ Dopo l'ID si deve scrivere anche la password.

## Se la VPN diventa "Rete pubblica"

Se non si risponde alla richiesta di Windows la rete VPN diventa "Rete pubblica" e la applicazione SlotsOverNet non potrà comunicare. In questo caso è difficile modificare la rete VPN e farla diventare "Rete privata", non abbiamo trovato altro modo che modificare il Registry e riavviare Windows.

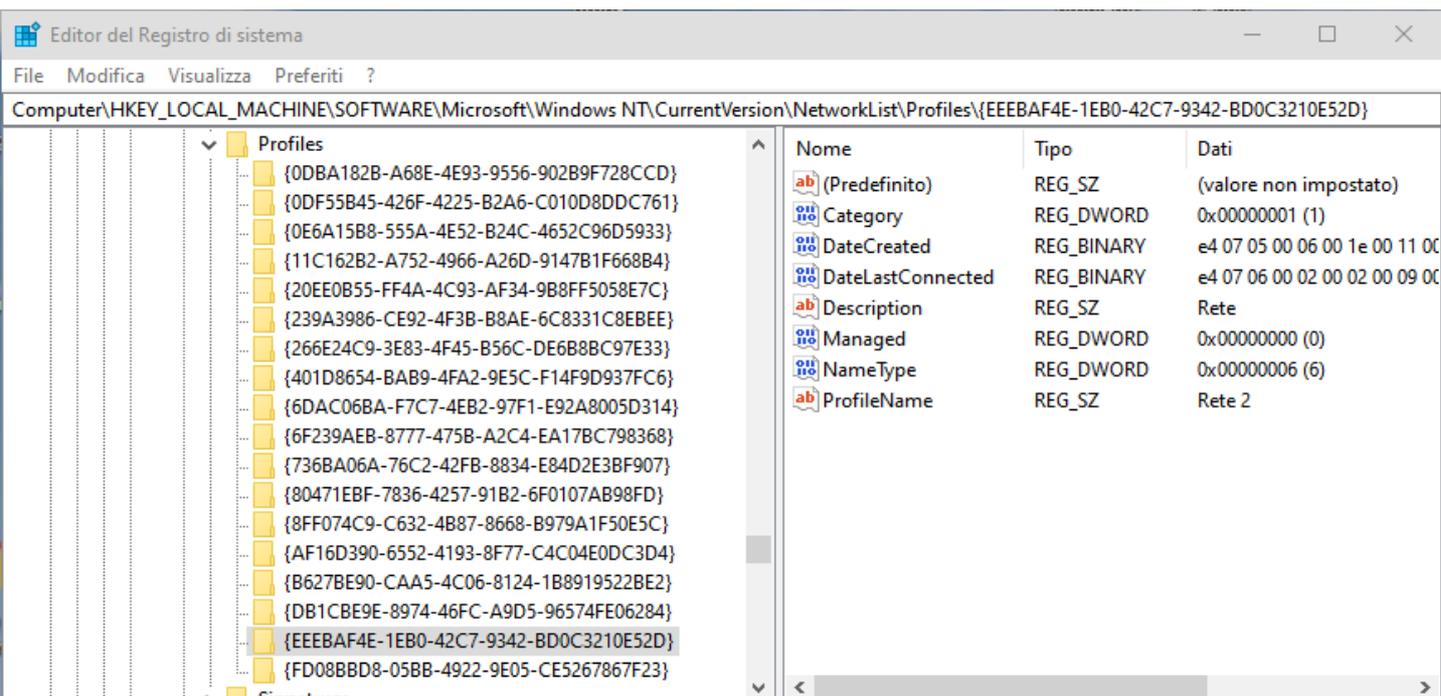
Prima di tutto si deve Individuare il nome della rete relativa alla connessione VPN

- ◆ Cliccare l'Icona delle reti, nella parte in basso a destra del desktop.
- ◆ Scegliere "Impostazioni rete e internet".
- ◆ Scegliere "Centro connessione di rete".
- ◆ Individuare il nome della rete (a sinistra) della connessione Hamachi (a destra).

Poi si deve avviare l'editor del registro di sistema, scrivendo "RegEdit" nella casella di ricerca di Windows.

Una volta aperto il RegEdit si va alla chiave seguente:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles**



- ◆ Appare un lista di numeri simili a questo: {0DBA182A-A68E-4E93-9556-703A9F728EEF}
- ◆ Si selezionano fino a trovare quello che come "Profile name" ha il nome della rete VPN.
- ◆ Si fa doppio click su "Category" e si cambia il numero "Dati valore" da "0" a "1".
- ◆ Si preme OK e si riavvia il PC.
- ◆ La rete VPN dovrebbe essere diventata "privata" e lo SlotsOverNet dovrebbe comunicare.

# Sicurezza delle comunicazioni UDP



Premessa.

Non controllate mai apparecchiature essenziali o pericolose.

Il nostro sistema non è progettato per questo.

## Rete locale o Internet

Internet è più vulnerabile rispetto al WiFi e alla rete locale cablata. Per aumentare la sicurezza in Internet potremmo utilizzare una VPN.

In ogni caso i maggiori pericoli non vengono dai pirati informatici, ma da interruzioni della comunicazione, errori umani o guasti, sia hardware che software. Quindi, come già scritto, non utilizzate mai il nostro sistema per controllare apparecchiature pericolose o essenziali.

## Attacchi informatici

Utilizzare questa applicazione per installare virus, o spiare i dati che sono nel computer, è del tutto impossibile. Il massimo che un malintenzionato potrebbe ottenere è di modificare un valore numerico. Valore che verrà prontamente corretto entro pochi millisecondi.

In ogni caso il massimo danno potrebbe essere di accendervi l'irrigazione per un breve istante, oppure di conoscere la temperatura o l'umidità dell'orto. Nessuno è interessato a conoscere o modificare questo tipo di dati, quindi normalmente potete stare del tutto tranquilli.

Ci sarebbe da preoccuparsi solo nel caso si controllassero apparecchi che possono rompersi, esplodere, fare danni o essere pericolosi per la sicurezza delle persone.

In questi casi i rischi sarebbero molteplici, dal PC che impazzisce agli errori umani, alla mancanza di corrente, ai difetti del software... pericoli ben più comuni e probabili di un attacco informatico.

## Perdita di pacchetti e interruzioni della comunicazione

Per trasferire i dati alla massima velocità possibile utilizziamo il protocollo UDP e questo protocollo non garantisce che i pacchetti arrivino.

Il protocollo TCP potrebbe rispondere con una conferma, e in caso di errore si potrebbe ripetere la trasmissione. Questo nel nostro caso sarebbe del tutto inutile, perché ripetiamo sempre la trasmissione ogni pochi millisecondi. E questo tempo è minore del tempo che impiegherebbe il TCP a dare la conferma, sommato alla eventuale ritrasmissione.

In caso di interruzioni nella comunicazione, anche il protocollo TCP smetterebbe di trasferire i dati. Inoltre sarebbe più lento a riprendere la comunicazione, perché dovrebbe uscire da uno stato di errore, rimandare i pacchetti perduti e infine riprendere la comunicazione a tempi regolari.