

FireGate 10NX



Quick Guide
rev. 1.0 del 09/2006

INDICE

PREMESSA	II
PRECAUZIONI	II
DICHIARAZIONE CE DI CONFORMITA'	II
1. INTRODUZIONE	1.1
1.1. CARATTERISTICHE	1.1
1.2. DESCRIZIONE PORTE, LED E DIP SWITCH	1.3
1.2.1. DESCRIZIONE DEI LED	1.3
1.2.2. POSTERIORE	1.4
2. CONFIGURAZIONE	2.1
2.1. DESCRIZIONE	2.1
2.2. INSTALLAZIONE E CABLAGGI	2.1
2.3. LA CONFIGURAZIONE	2.2
2.3.1. PREPARAZIONE DEL COMPUTER	2.2
2.4. CENNI PRELIMINARI PER LA CONFIGURAZIONE	2.4
2.5. ACCESSO ALLA CONFIGURAZIONE	2.6
2.6. COME CONFIGURARE LE STAZIONI DI RETE	2.14
2.6.1. CONFIGURAZIONE DEL TCP/IP	2.14
2.6.2. NAVIGAZIONE INTERNET TRAMITE ROUTER IN LAN	2.14
2.6.3. IMPOSTAZIONI INTERNET	2.14
2.6.4. ACCESSO INTERNET – LA NAVIGAZIONE	2.14
3. RISOLUZIONE DEI PROBLEMI	3.1

PREMESSA

E' vietata la riproduzione di qualsiasi parte di questo manuale, in qualsiasi forma, senza esplicito consenso scritto della Digicom S.p.A. Il contenuto di questo manuale può essere modificato senza preavviso.

Ogni cura è stata posta nella raccolta e nella verifica della documentazione contenuta in questo manuale, tuttavia la Digicom non può assumersi alcuna responsabilità derivante dall'utilizzo della stessa.

Tutte le altre marche, prodotti e marchi appartengono ai loro rispettivi proprietari.

PRECAUZIONI

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore e il funzionamento dell'apparato, devono essere rispettate le seguenti norme per l'installazione. Il sistema, compresi i cavi, deve venire installato in un luogo privo o distante da:

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

CONDIZIONI AMBIENTALI

Temperatura ambiente da -5 a +45°C Umidità relativa dal 20 a 80% n.c.

Si dovrà evitare ogni cambiamento rapido di temperatura e umidità.

AVVERTENZE GENERALI

Per evitare scosse elettriche, non aprite l'apparecchio o il trasformatore. Rivolgetevi solo a personale qualificato. Scollegate il cavo di alimentazione dalla presa a muro quando non intendete usare l'apparecchio per un lungo periodo di tempo. Per scollegare il cavo tiratelo afferrandolo per la spina. Non tirate mai il cavo stesso.

In caso di penetrazione di oggetti o liquidi all'interno dell'apparecchio, scollegate il cavo di alimentazione e fatelo controllare da personale qualificato prima di utilizzarlo nuovamente.

PULIZIA DELL'APPARATO

Usate un panno soffice asciutto senza l'ausilio di solventi.

VIBRAZIONI O URTI

Attenzione a non causare vibrazioni o urti.

DICHIARAZIONE DI CONFORMITA'

Noi, **Digicom S.p.A. via Volta 39 - 21010 Cardano al Campo (Varese - Italy)**, dichiariamo sotto la nostra esclusiva responsabilità, che il prodotto a nome **Firegate 10NX**, soddisfa la direttiva 89/336/CEE (solo compatibilità elettromagnetica). Le norme sono:

EN 55022 classe B

EN 61000-3-2

EN 61000-3-3

EN 55024

Smaltimento delle apparecchiature obsolete



Tutti i prodotti elettrici ed elettronici devono essere smaltiti separatamente rispetto alla raccolta differenziata municipale, mediante impianti di raccolta specifici designati dal governo o dalle autorità locali. Quando sul prodotto è riportato il simbolo di un bidone della spazzatura barrato da una croce, significa che l'apparato è coperto dalla direttiva europea 2002/96/EC (WEEE).

Sono previste sanzioni in caso di smaltimento abusivo di detti prodotti.

1. INTRODUZIONE

Grazie per la fiducia accordatoci nell'acquistare un prodotto Digicom!

Con Firegate 10NX le sarà possibile collegare il suo ufficio o dipartimento aziendale ad Internet in modo semplice ed efficiente.

Fino a 253 stazioni della sue rete locale LAN e Wireless* avranno la possibilità di accedere ad Internet per la navigazione (WWW, HTTP) o l'accesso alla posta elettronica (e-mail) utilizzando un modem* ADSL, xDSL o Cable Modem ed un abbonamento per singolo utente.

La sua LAN sarà inoltre protetta dai più comuni attacchi di hacker che potenzialmente possono provenire da Internet (Denial Of Service). Firegate 10NX supporta trasparentemente i protocolli L2TP, PPTP e IPSEC per il VPN passthrough oltre che le funzioni native per stabilire connessioni VPN con altri dispositivi su IPSEC e IKE.

Tutte le operazioni di linea saranno gestite in modo completamente automatico e trasparente da Firegate 10NX, senza intervento alcuno da parte degli utilizzatori della rete.

Potrà inoltre sfruttare le funzionalità avanzate di Firegate 10NX per gestire in modo efficiente l'accesso ad Internet dei suoi computer, realizzando esportazioni di servizi, gruppi di utenti a cui permettere/negare l'accesso, bloccare protocolli o applicazioni e molto altro.

In questo manuale troverà tutte le informazioni necessarie per collegare Firegate 10NX alla vostra rete di computer e configurare opportunamente l'insieme in pochi minuti.

Per una configurazione più estesa e completa dei prodotti si faccia riferimento ai manuali della serie FireGate disponibili on-line o su CD-ROM e consultabili da browser o Acrobat® Reader™.

Per comodità, per indicare il modem connesso alla porta WAN, questo verrà convenzionalmente chiamato "Modem xDSL", indipendentemente dalla sua tipologia (ADSL, HDSL, SDSL, Cable o altra tecnologia simile).

1.1. CARATTERISTICHE

LAN

- Switch 10/100 BaseT integrato

Fino a 4 stazioni di rete possono essere collegati direttamente al dispositivo. La velocità e modalità di funzionamento della LAN viene riconosciuta ed impostata automaticamente.

- Porta DMZ 10/100 per la connessione di stazioni server
- Supporto DHCP Server

Un server DHCP (Dynamic Host Configuration Protocol) interno è in grado di assegnare gli indirizzi IP ai computer della rete che ne fanno richiesta.

- Supporto RIP e Tabelle di Routing statiche

E' supportato il protocollo RIP ed è possibile configurare le tabelle di routing statiche per interagire con altri router connessi in LAN.

WAN

- Porta WAN 10/100BaseT

A questa porta è possibile connettere il Modem xDSL.

- Supporto protocollo PPPoE e PPTP

Firegate è in grado di generare una chiamata automatica verso il provider Internet (se necessario), utilizzando il protocollo PPP over Ethernet integrato e supportare il protocollo PPTP.

- Connessione diretta al provider Internet

Firegate 10NX può effettuare una "connessione diretta", senza protocollo PPPoE, se il provider Internet richiede questo tipo di funzionamento o se si collega il dispositivo ad un router intermedio.

Accesso ad Internet

- Accesso condiviso ad Internet
Fino a 253 computer connessi alla rete LAN (opportunamente configurati) possono usufruire dell'accesso Internet contemporaneamente e in modo trasparente.
- Abbonamento per singolo utente
Tramite un abbonamento Internet per singolo utente, gli utenti della LAN hanno l'accesso simultaneo ad Internet.

Funzioni Internet Avanzate

- Virtual Servers. Permette a utenti Internet di accedere a computer presenti sulla propria LAN
- User-Defined Virtual Servers. Permette a utenti Internet di accedere a servizi speciali messi a disposizione sulla propria LAN.
- Special Internet Applications. Permette di utilizzare applicazioni Internet speciali come Internet Videoconferencing*, Telephony, Games Servers ecc.
- Exposed Computer. Un solo (1) computer della LAN può essere reso visibile (esposto) agli utenti Internet in modo completo, senza applicare alcuna restrizione o sicurezza.
* Alcune applicazioni potrebbero non essere supportate.

Configurazione e Monitor

- Configurazione semplice ed immediata attraverso un comune browser (Explorer, Netscape, ecc.)
- Gestione e monitoraggio da una qualsiasi stazione di LAN locale o remota
- Supporto protocollo UpnP (Universal Plug and Play) per Windows XP, 2000 e Me.

Sicurezza e protezione dei dati

- Accesso alla configurazione protetto da password
- Access List. Creazione di gruppi di utenti ai quali restringere o negare l'utilizzo di Internet con log visualizzabili. Filtro su URL in uscita.
- Tutti i pacchetti di dati provenienti dal link WAN vengono controllati e verificati.
- Tutte le richieste di accesso a stazioni presenti in LAN, WAN o DMZ sono controllati da regole di Firewall definibili dall'utente.
- Protezione automatica da attacchi di tipo Denial of Service.
- Log delle operazioni ed eventi diretto, via e-mail o Syslog.

Funzioni di VPN Gateway

- Supporto IPSec standards, incluso IKE e Certificati, DES, 3DES, AES
- Supporto fino a 10 Tunnel VPN.

Prerequisiti

- Computer con schede di rete Ethernet 10/100 Megabit/s, connettori UTP
- Driver software per le schede di rete installati su ogni computer
- Cavi di rete diritti, connettori RJ45 su entrambe le estremità
- Modem xDSL per l'accesso ad Internet dotato di porta LAN 10Mbit/s e connettore UTP RJ45
- Abbonamento Internet per singolo utente stipulato con un ISP (Internet Service Provider)

Contenuto della confezione

- 1 Firegate 10NX
- 1 Alimentatore
- 1 CD-ROM contenente il Manuale
- 1 Manuale di configurazione rapida

1.2. DESCRIZIONE PORTE, LED E DIP SWITCH

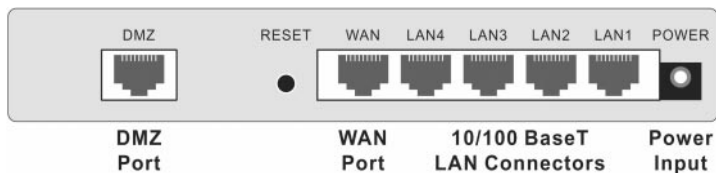


Fig. 1.1. Vista dei Led

1.2.1. DESCRIZIONE DEI LED

Power	<p>Acceso – Dispositivo Acceso</p> <p>Spento – Dispositivo Spento</p>
Status (Rosso)	<p>Acceso – Condizione di errore</p> <p>Spento – Stato normale</p>
LAN	<p>Lampeggiante - Durante il selftest di accensione</p> <p>2 led per ogni porta</p> <ul style="list-style-type: none"> ● Link/Act <ul style="list-style-type: none"> ● Acceso – Porta LAN attiva ● Spento – Porta Lan non attiva ● Lampeggiante - Attività dati sulla porta ● 100 <ul style="list-style-type: none"> ● Acceso - La porta sta operando a 100Mbit/s ● Spento - La porta sta operando a 10Mbit/s (se Link/Act acceso)
WAN	<p>Acceso - connessione con il modem xDSL sulla porta WAN stabilita e attiva</p> <p>Lampeggiante - Attività dati sulla porta WAN</p>
PPPoE	<p>Acceso - Connessione PPPoE stabilita</p> <p>Spento – Nessuna Connessione PPPoE</p>
DMZ	<ul style="list-style-type: none"> ● Link/Act <ul style="list-style-type: none"> ● Lampeggiante – Attività dati sulla porta ● 100 <ul style="list-style-type: none"> ● Acceso - La porta sta operando a 100Mbit/s ● Spento - La porta sta operando a 10Mbit/s (se Link/Act acceso)

1.2.2. POSTERIORE



DMZ Reset

Usare un normale cavo per collegare la porta ad un HUB o Switch

Pulsante di Reset. Ha due funzioni:

- Reboot. Premendo e rilasciando il pulsante si effettua un riavvio del dispositivo.
- Reset di tutte le impostazioni. Per riportare tutte le impostazioni al default di fabbrica:
 1. Spegner il dispositivo.
 2. Tenere premuto il pulsante e riaccendere il dispositivo.
 3. Mantenere il pulsante premuto per circa 10 secondi o finché il led di status sarà acceso per 2 volte.
 4. Rilasciare il pulsante. Il dispositivo è ora tornato alle impostazioni di fabbrica.

WAN (10/100BaseT)

Porta per la connessione del modem xDSL. Usare il cavo fornito con il modem o un normale cavo di LAN.

LAN1-4 (10/100BaseT)

Porte LAN (MDI-X/MDI automatiche). Usare normali cavi LAN (CAT5 per 100Mbit/s).

Power port

Tutte le porte si tramutano, se necessario, in "Uplink" (MDI) in modo automatico
Ingresso per il cavo proveniente dall'alimentatore. Utilizzare unicamente l'alimentatore fornito nella confezione. L'utilizzo di alimentatori diversi può comportare il danneggiamento del dispositivo con conseguente invalidazione delle condizioni di garanzia.

2. CONFIGURAZIONE

2

2.1. DESCRIZIONE

La configurazione dell'intero sistema comprende:

- Installazione e cablaggi
- Configurazione Firegate 10NX
- Configurazione stazioni di rete

2.2. INSTALLAZIONE E CABLAGGI

1. Scelta della locazione di installazione

Scegliete una locazione che sia vicina:

- Al modem xDSL.
- Alla presa di alimentazione 220V.
- Ad un hub o presa di rete 10BaseT o 100BaseT.

2. Connessione del router alla rete LAN

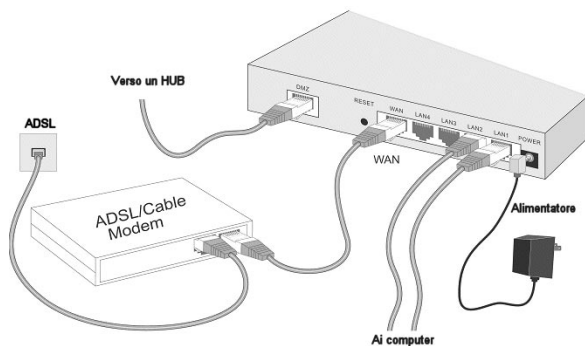
Utilizzate un normale cavo LAN.

- Collegate un'estremità del cavo alla porta LAN1 presente sul posteriore del dispositivo.
- Collegate l'altra estremità del cavo ad una porta 10BaseT o 100BaseT di un Hub o alla presa di rete LAN.
- Il router rileverà e imposterà la velocità di funzionamento 10/100 e la modalità half/full duplex in modo automatico. Il router imposterà anche la porta in modalità MDI (Uplink) se necessario
- Se preferite potete collegare il dispositivo direttamente ad un PC.

3. Connessione computer sulla porta DMZ

Utilizzate un normale cavo LAN per collegare la porta DMZ ad una normale porta Hub o Switch.

Nota: I computer connessi "in DMZ" hanno accesso ad Internet ma nessun accesso alla LAN



4. Connessione del router al modem xDSL

Utilizzate il cavo RJ45-RJ45 fornito con il modem oppure un normale cavo di LAN.

Collegate un'estremità del cavo alla porta Ethernet del modem xDSL.

Collegate l'altra estremità del cavo alla porta WAN di Firegate 10NX.

5. Accensione del router

Collegate il cavetto di alimentazione alla presa Power.

Inserite l'alimentatore fornito nella confezione nella presa di alimentazione 220V.

Non utilizzate alimentatori diversi da quello fornito nella confezione, pena il possibile danneggiamento del dispositivo e conseguente invalidazione delle condizioni di garanzia.

6. Verifica stato led

Una volta acceso il dispositivo i led WAN e LAN (per le porte attive) accesi di colore verde.

Il led Status deve spegnersi dopo qualche secondo dall'accensione.

Nota: La lunghezza di ogni cavo deve essere inferiore a 100mt. Se la rete LAN opera a 100Mbit/s è necessario l'uso di cavi di rete in categoria 5.

Uso della porta DMZ

Quando si utilizza la porta DMZ tenere presente i seguenti punti:

- La porta DMZ è una porta "normale" (MDI-X), non una porta di Uplink.
- I PC connessi alla porta DMZ sono sullo stesso segmento logico di LAN dei PC connessi alle porte LAN1-3, e pertanto devono appartenere allo stesso range di indirizzi IP.
- I PC connessi alla porta DMZ NON sono visibili dai PC connessi alle porte LAN1-3. Non sarà possibile accedere a questi PC con protocolli di rete Microsoft o similari.
- I PC connessi alla porta DMZ possono comunque condividere l'indirizzo IP di WAN per l'accesso a/dal Internet.

Vantaggi della porta DMZ

I server di Lan dovrebbero essere connessi alla porta DMZ per i seguenti motivi:

- Il traffico dati tra DMZ e LAN passa attraverso il Firewall, Il Firewall proteggerà la rete LAN nel caso i server fossero stati compromessi ed usati per attaccare la LAN.
- Se si utilizza la funzione di Virtual Server, il dispositivo crea automaticamente una regola di Firewall "WAN -> DMZ". Se il PC Virtual Server è connesso alla porta LAN1-3 la regola va inserita manualmente.

2.3. LA CONFIGURAZIONE

Firegate 10NX supporta il servizio HTTP server permettendovi di accedere alla sua configurazione tramite un comune browser (tipo Explorer o Netscape) che supporti tabelle e form HTML. Il vostro browser deve supportare i Javascript (Netscape 4.08 o superiore, Internet Explorer 4 o superiore).

In alternativa potete utilizzare il protocollo UpnP se il vostro sistema operativo lo supporta.

2.3.1. PREPARAZIONE DEL COMPUTER

Per accedere alla configurazione di FireGate 10NX è indispensabile che il vostro computer utilizzi il protocollo TCP/IP dopodiché il metodo più semplice è quello di utilizzare il servizio di DHCP server di Firegate 10NX; l'alternativa è quella di modificare manualmente l'indirizzo IP del vostro computer.

Di seguito sono riportate le indicazioni per entrambe le modalità.

IMPOSTAZIONE COME CLIENT DHCP

Windows® XP

1. Dal menù Start selezionate -> **Pannello di Controllo -> Rete e Connessioni Internet**, Risorse di rete e selezionate **Visualizza risorse di rete**.
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/ IP)** e premete sul pulsante **Proprietà**.
3. Per impostare il Computer come client DHCP dovete selezionare **Ottieni automaticamente un Indirizzo IP**, a questo punto potete chiudere le finestre confermando con **OK**.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

Macintosh®

1. Dal Pannello di controllo selezionate **Preferenze di Sistema** (System Preferences).
2. Cliccate sull'icona **Network**.
3. Selezionate Mostra: **Ethernet Integrata** (Built-in Ethernet).
4. Cliccate sul pulsante **TCP/IP**.
5. Selezionate **Utilizzo di DHCP** (Using DHCP).
6. Chiudete il pannello **Network**.

Linux

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.
3. Selezionate Assegnazione automatica degli indirizzi (via DHCP) .
4. Confermate con **Termina**.

INDIRIZZI IP STATICI**Windows® XP**

1. Dal menù Start selezionate -> **Pannello di Controllo -> Rete e Connessioni Internet , Risorse di rete e** selezionate **Visualizza risorse di rete**.
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/ IP)** e premete sul pulsante **Proprietà**.
3. Per impostare un indirizzo IP dovete selezionare **Utilizza il seguente indirizzo IP**: ed inserite Indirizzo IP 192.168.0.2, la Subnet mask 255.255.255.0 ed il Gateway 192.168.0.1. Confermate con **OK** le nuove impostazioni.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

Macintosh®

1. Dal Pannello di controllo selezionate **Preferenze di Sistema** (System Preferences).
2. Cliccate sull'icona **Network**.
3. Selezionate Mostra: **Ethernet Integrata** (Built-in Ethernet).
4. Cliccate sul pulsante **TCP/IP**.
5. Selezionate **Manualmente** (Manually).
6. Inserite i valori per **IP** 192.168.0.2, **Maschera di sottorete** (Subnet Mask) 255.255.255.0 e **Router** 192.168.0.1.
7. Chiudete il pannello **Network**.

Linux

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.
3. Selezionate Impostazione degli indirizzi statici, ed inserite Indirizzo IP 192.168.0.2, la Subnet mask 255.255.255.0.
4. Per impostare il gateway, cliccate su Routing e inserite l'indirizzo 192.168.0.1 nel campo Gateway predefinito.

2.4. CENNI PRELIMINARI PER LA CONFIGURAZIONE

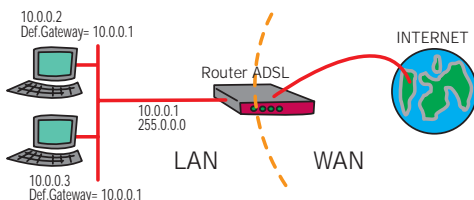
CONFIGURAZIONE FIREWALL

Questa sezione descrive gli scenari della vostra rete LAN, prima e dopo l'inserimento del Firewall, fornendovi le indicazioni principali necessarie alla corretta impostazione dell'intero sistema.

Nota: Nel nostro esempio assumiamo che gli indirizzi IP siano stati configurati in modalità fissa e non tramite DHCP (Indirizzi assegnati automaticamente, solitamente dal router ADSL). La descrizione generale è comunque valida. Fate riferimento alle sezioni DHCP e DNS per le descrizioni specifiche.

PRIMA

Ipotizziamo la tipica situazione di una rete LAN che accede ad Internet tramite un router ADSL. Tutto il sistema è già installato, configurato e funzionante.



Gli indirizzi IP e la Subnet Mask

Nell'esempio illustrato, tutti i computer della rete LAN hanno un indirizzo IP appartenente alla stessa classe 10.0.0.x con Subnet Mask 255.0.0.0.

Affinchè i computer possano comunicare tra di loro tramite il protocollo TCP/IP, gli indirizzi e Subnet Mask assegnati alle stazioni di rete devono necessariamente appartenere alla stessa classe.

In questo contesto anche il Router ADSL fa parte della rete LAN e pertanto ha anch'esso un indirizzo appropriato.

Il Default Gateway

Il **Router ADSL** svolge la funzione fondamentale di fornire l'accesso ad Internet a tutti i componenti della rete LAN, pertanto ne è la "porta di uscita" verso il mondo esterno, in altre parole, il **Gateway** della rete.

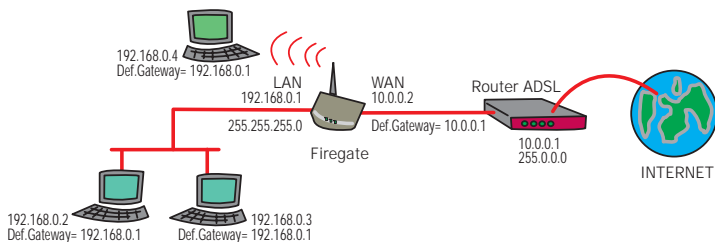
Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere l'**indirizzo IP del Router ADSL** impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

DOPO

La caratteristica principale del Firewall è quella di interporre una "barriera" a protezione della rete locale, tra la LAN (Local Area Network) ed il mondo esterno, convenzionalmente chiamato "WAN" (Wide Area Network).

Il Firewall considera i due network LAN e WAN come due reti separate e distinte aventi indirizzi diversi.

Per questo motivo, inserendo il Firewall nella nostra rete sarà necessario modificare gli indirizzi IP della parte LAN come di seguito descritto (1).



Gli indirizzi IP di LAN

Nell'esempio illustrato, tutti i computer della rete LAN dovranno modificare le proprie impostazioni per "passare" alla nuova classe di indirizzi 192.168.0.x e Subnet Mask 255.255.255.0.

Il Default Gateway

Il **Firewall** svolgerà ora la funzione di punto di accesso verso il mondo esterno e pertanto diventerà il nuovo **Gateway** della rete.

Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere l'indirizzo IP del Firewall impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

Resta ora da configurare il **"lato WAN" del Firewall** per farlo comunicare con il Router ADSL.

Lasciando invariata la configurazione del router ADSL, l'impostazione della porta WAN del Firewall andrà a "sostituire" quella che era l'impostazione di una stazione di rete LAN, prima dell'inserimento del Firewall stesso.

Essendo 10.0.0.1 l'indirizzo IP del Router ADSL assegneremo alla porta WAN del Firewall un indirizzo IP appartenente alla stessa classe, ad esempio 10.0.0.2 e Subnet mask 255.0.0.0.

Dovremo anche specificare un indirizzo per il **Default Gateway** della porta **WAN**. In questo caso sarà ancora l'indirizzo IP 10.0.0.1 del Router ADSL che è di fatto il Gateway di accesso ad Internet per il Firewall.

A questo punto le stazioni della rete rete LAN saranno in grado di navigare in Internet in virtù del fatto che, di default, il Firewall non limiterà alcun accesso dalla LAN verso l'esterno mentre qualsiasi tentativo di intrusione, proveniente dall'esterno ed indirizzato verso la LAN del Firewall, verrà automaticamente impedito e bloccato.

DNS

Una volta che una stazione di rete ha la possibilità di accedere ad Internet, un'altra impostazione fondamentale è quella relativa ai DNS (Domain Name Server). In una rete TCP/IP il servizio DNS svolge la funzione di **tradurre gli URL** (ad esempio www.digicom.it) nei corrispondenti **indirizzi IP globali** (ad esempio 195.103.9.66).

Se le impostazioni DNS sono assenti o incorrette, di fatto le stazioni di rete non possono navigare in Internet.

Tutte le stazioni di rete dovranno avere **almeno un indirizzo IP configurato nel campo DNS** delle impostazioni di rete TCP/IP. Questo indirizzo è solitamente fornito dal provider Internet.

Nota: Se il router ADSL supporta la funzione di **DNS Autodiscovery/Proxy**, l'impostazione del server DNS sulle stazioni di LAN può essere l'indirizzo IP del router ADSL stesso (10.0.0.1 nel nostro esempio); sarà il router ad occuparsi di svolgere il servizio di risoluzione dei nomi DNS per la rete LAN.

DHCP

La descrizione fin qui fornita fa riferimento alle impostazioni degli indirizzi in modo "fisso" o statico.

E' possibile che una rete LAN si avvalga del servizio DHCP (Domain Host Control Protocol) per la configurazione automatica degli indirizzi. Questo servizio è svolto da un **DHCP server**, solitamente attivato sul Router ADSL, ed ha il compito di assegnare in modo automatico gli indirizzi IP, Subnet Mask, Default Gateway e DNS alle stazioni di LAN che ne fanno esplicita richiesta.

Una stazione di rete Microsoft Windows opera in **modalità DHCP** quando nelle impostazioni del protocollo TCP/IP della scheda di rete ha selezionato la voce "Ottieni automaticamente un indirizzo IP"; opera invece in modalità **fissa o statica** quando ha selezionato la voce "Utilizza il seguente indirizzo IP". La stessa cosa vale per le impostazioni dei server DNS.

Detto ciò, se la nostra rete LAN utilizzava il **servizio DHCP prima dell'inserimento del Firewall**, affinché si possano lasciare invariate le impostazioni delle stazioni di LAN sarà necessario attivare il servizio DHCP anche nel Firewall. Si dovranno configurare un numero sufficientemente grande di indirizzi disponibili ma anche gli indirizzi dei server DNS da utilizzare in modo che, quando le stazioni di LAN ne faranno richiesta, il Firewall possa soddisfare tali richieste assegnando tutti i parametri necessari alla navigazione.

(1) Se avete libero accesso alla configurazione del Router ADSL ed avete ben compreso la descrizione della sezione "DOPO", potete anche optare per l'alternativa di lasciare invariata la configurazione dell'intera LAN ma modificare opportunamente l'indirizzo IP del Router ADSL.

2.5. ACCESSO ALLA CONFIGURAZIONE

Configurazione via Browser

1. Avviate il vostro Browser (Explorer, Netscape, ecc.)
2. Nel campo Indirizzo URL inserite "HTTP://" e l'indirizzo IP (usando l'indirizzo impostato di fabbrica: HTTP://192.168.0.1)

Se non vedete apparire la schermata iniziale verificate che:

- Il dispositivo sia acceso ed il cavo di LAN è correttamente collegato.
- Il dispositivo ed il computer dal quale state tentando di accedere alla configurazione si trovino sullo stesso segmento di rete
- Nessun altro computer o dispositivo di rete stia utilizzando l'indirizzo 192.168.0.1. Se così fosse, scollegate la stazione dalla rete e modificate l'indirizzo IP prima di ricollegarla alla rete oppure spegnetela finché non avrete assegnato un diverso indirizzo IP al dispositivo.
- Il vostro computer abbia un indirizzo IP compatibile. Per verificare quale sia l'indirizzo IP attualmente utilizzato dal vostro computer, dalla barra di Avvio di Windows® selezionate Esegui, inserite winipcfg (Win98) o ipconfig (WinMe/2000/XP) e cliccate OK.

Verificate che sia selezionata la vostra scheda di rete. Verificate che l'indirizzo IP sia compreso tra 192.168.0.2 e 192.168.0.254 e il Subnet Mask sia uguale a 255.255.255.0

- Il vostro browser non sia configurato per utilizzare un Proxy server.

Se utilizzate Internet Explorer verificate il menu Visualizza -> Opzioni -> Connessione.

Se utilizzate Netscape verificate Opzioni -> Preferenze di rete -> Proxy.

Configurazione via UPnP

Se il vostro sistema operativo supporta UPnP, una icona per il vostro Router apparirà nel system tray notificandovi che un nuovo dispositivo di rete è stato trovato e proponendovi un collegamento.

- Se non intendete cambiare l'indirizzo IP potete accettare di creare il collegamento.
- Che accettiate o meno di creare il collegamento il router sarà raggiungibile dalle Risorse di Rete.
- Fate doppio click sull'icona del Router (Collegamento o Risorse di Rete) per iniziare la configurazione.

Se è stata impostata una password vedrete la seguente schermata:



- Lasciate il campo "User Name" vuoto ed inserite la password per il router.

Se si tratta della prima configurazione apparirà la finestra principale, il **Setup Wizard**, tramite il quale potrete effettuare le **impostazioni principali di WAN**.

Dovete avere a disposizione i dati relativi al tipo di connessione Internet con il vostro ISP.

Di seguito un riassunto delle tipologie più comuni:

Modem xDSL (ADSL, HDSL, SDSL, ecc)

Tipo	Dettagli	Dati ISP richiesti
Dynamic IP address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Nessuno
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate.
PPPoE	Connessione all'ISP in modalità PPP over Ethernet. L'assegnazione dell'indirizzo è automatica.	User name e password.
PPTP	Connessione all'ISP in modalità Point to Point Tunneling. L'assegnazione dell'indirizzo è solitamente dinamica ma può essere statica.	- Indirizzo IP del PPTP Server - User name e password - Indirizzi e Subnet mask a voi assegnate (se statico)

Other Modems (Altri modem, Router o Wireless)

Tipo	Dettagli	Dati ISP richiesti
Dynamic IP Address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Nessuno
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate.

Cable Modems

Tipo	Dettagli	Dati ISP richiesti
Dynamic IP Address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Generalmente nessuno. L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address.
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate. L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address.

Big Pond (Australia) e SingTel RAS

- Non utilizzati in Europa

Selezionate la modalità in base alla vostra tipologia di collegamento e proseguite nella configurazione cliccando su Next. Inserite i dati nelle apposite caselle.

Esempi di configurazione:

- **Accesso Internet tramite modem (Bridge) ADSL* e protocollo PPPoE:**

Selezionate DSL/ADSL modem, selezionate PPPoE, inserite User name e password, deselectionate le voci "Connect automatically..." e "Disconnect after idle...", selezionate "Dynamic" per gli accessi con IP dinamico, selezionate "Static" se l'indirizzo IP è statico, inserite l'IP di WAN e l'indirizzo del DNS (fornito dall'ISP) in DNS.

- **Accesso ad Internet tramite Router ADSL* con NAT e IP dinamico:**

Se la vostra LAN (e di conseguenza il Router ADSL) sta utilizzando gli indirizzi IP del range 192.168.0.x, modificate l'IP del router ADSL (ad esempio 10.0.0.1/255.0.0.0).

Selezionate Other, selezionate "Static" IP address, inserite un indirizzo IP libero appartenente al range assegnato al router ADSL, Subnet mask e Gateway (ad esempio rispettivamente 10.0.0.2, 255.0.0.0 e 10.0.0.1. Inserite l'indirizzo del DNS (fornito dall'ISP) in DNS.

- **Accesso ad Internet tramite Router ADSL* con IP pubblico:**

Selezionate Other, selezionate "Static" IP address, inserite uno degli indirizzi IP pubblici disponibili in IP address, inserite la Subnet mask, inserite l'indirizzo IP del router ADSL in Gateway, inserite l'indirizzo del DNS (fornito dall'ISP) in DNS.

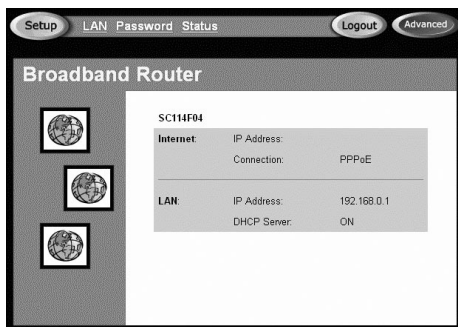
*** La porta LAN del Bridge o Router ADSL deve essere collegata alla porta WAN del dispositivo**

Al termine cliccate su **Finish**. Se avete selezionato "Test Internet connection" verrà verificata la raggiungibilità della parte WAN.

Cliccate su **Close** per chiudere il Wizard.

Home Screen

Una volta terminata la configurazione con il Wizard apparirà la seguente schermata.



Navigazione nei menu e inserimento dati

- Utilizzate i "bottoni" e i menu visualizzati per accedere alle varie pagine di configurazione. Utilizzate il bottone "Indietro" del browser per tornare alla pagina precedente.
- Ogni modifica effettuata va convalidata cliccando su "Save" prima di cambiare pagina. Modifiche non convalidate da Save verranno ignorate.

In ogni pagina è disponibile un Aiuto Online completo di indice cliccando su Help.

Di seguito la descrizione delle pagine di configurazione LAN, Password e Status

LAN

Cliccate su LAN per accedere ai parametri della sezione LAN.

TCP/IP IP Address Network Mask

Queste impostazioni dipendono dalle impostazioni della vostra LAN:

Se utilizzate il DHCP server (consigliato):

Generalmente nessun cambiamento è richiesto per queste impostazioni.

Comunque tutti i dispositivi in rete devono essere impostati come DHCP Client oppure utilizzare un indirizzo IP e Subnet mask compatibile.

Se in LAN è già presente un DHCP server:

Deselezionate il DHCP server interno per non incorrere in conflitti

Se la LAN utilizza indirizzi IP statici:

Impostate per il router un indirizzo IP tra quelli non utilizzati della LAN.

La Network Mask deve essere la stessa utilizzata per i PC in rete.

DHCP Server

Se abilitato (default), il router fornirà gli indirizzi IP e dati relativi ai computer DHCP client che ne faranno richiesta.

Se necessario modificate i campi Start IP Address e Finish IP Address per adattarli alla vostra LAN. Queste impostazioni determinano anche quanti client saranno gestiti.

Save Cancel

Salva nel dispositivo le modifiche apportate

Ignora le modifiche apportate e ricarica i parametri dal dispositivo

Password

Questa pagina permette di assegnare una password per l'accesso alla configurazione del dispositivo.

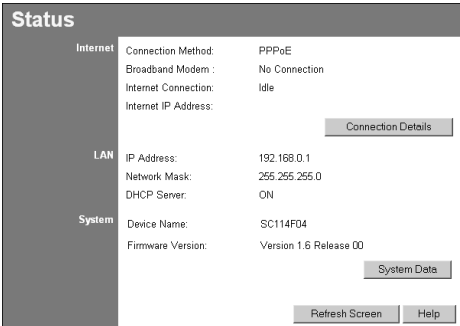
Una volta assegnata una password nella finestra sopra indicata, ogni volta che vorrete accedere alla configurazione del dispositivo, verrà visualizzata una finestra simile alla seguente:



- Lasciate vuoto il campo "User Name"
- Inserite la password e cliccate OK.

Status

La finestra di Status permette di verificare lo stato della connessione WAN, della sezione LAN e del Sistema.



Internet

Connection Method	Indica il metodo di connessione, come impostato nel Wizard
Broadband Modem	Stato della connessione (WAN)
Internet Connection	Stato della connessione Internet: <ul style="list-style-type: none">- Active (attivo)- Idle (a riposo)- Unknown (sconosciuto)- Failed (fallito)
Internet IP Address	In caso di errori potete cliccare "Connection Details" per maggiori dettagli. L'indirizzo IP assegnato dall'ISP (Internet Service Provider).
"Connection Details"	Descrizione dettagliata della connessione corrente

LAN

IP Address	Indirizzo IP del dispositivo
Network Mask	Network Mask (Subnet Mask) associata all'indirizzo IP
DHCP Server	Stato del DHCP Server interno: "Enabled" (abilitato) o "Disabled" (disabilitato).

System

Device Name	Identificativo del dispositivo
Firmware Version	Versione del firmware attualmente a bordo del dispositivo.
System Data	Informazioni varie di sistema.

Bottoni	
Connection Details	Finestra dei dettagli relativi alla connessione
System Data	Visualizza ulteriori informazioni varie di sistema
Refresh Screen	Aggiorna le informazioni visualizzate.

Connection Status - PPPoE	
Log di connessione quando si utilizza PPPoE (PPP over Ethernet).	

Connection Status - PPPoE

Connection

Physical Address: 00-c0-02-11-4f05
IP Address:
Network Mask:
PPPoE Link Status: OFF

Connection Log

005:Reset physical connection
004:stop PPP
003:try to hang up
002:sub_wait:timeout
001:wait 100 msec "WAN start... "
000:stop PPP

Clear Log

Connect and Disconnect buttons should only be needed if the setting "Connect automatically, as required" is Disabled.

Connect

Disconnect

Refresh

Help

Close

PPPoE	
Connection	
Physical Address	Il Mac address (lato WAN) del dispositivo
IP Address	L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo)
Network Mask	La Network Mask (Subnet Mask) per l'indirizzo sopra
PPPoE Link Status	Indica lo stato attuale della connessione Se la connessione non è attiva, il pulsante Connect permette di iniziarne una - Se la connessione è attiva il pulsante Disconnect termina la connessione in corso

Connection Log	
Connection Log	Fornisce una serie di messaggi inerenti l'attività di connessione/negoziazione del protocollo PPPoE e del dispositivo sulla porta WAN.

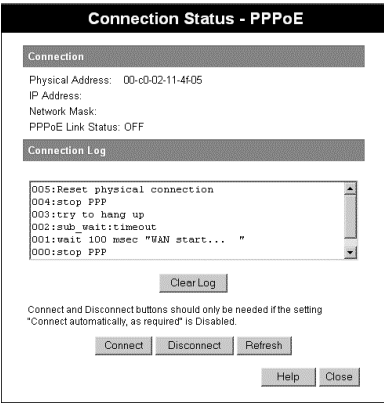
Bottoni	
Connect	Se non collegato, attiva una connessione verso l'ISP.
Disconnect	Se connesso, termina la connessione.
Clear Log	Cancella il contenuto del log di connessione
Refresh	Aggiorna le informazioni visualizzate.

Descrizione messaggi di Log:

Messaggio	Descrizione
Connect on Demand	La connessione è stata attivata per "Connect on Demand"
Manual connection	La connessione è stata attivata premendo il pulsante "Connect"
Reset physical connection	Preparazione per la connessione
Connecting to remote server	Inizio connessione verso il remoto (provider o LAN)
Remote Server located	Il server remoto ha risposto alla richiesta di connessione
Start PPP	Inizio della negoziazione PPP con il server remoto
PPP up successfully	Negoziazione PPP completata con successo
Idle time-out reached	La connessione viene terminata per inattività dati superiore al valore impostato in "Idle Time-out".
Disconnecting	La connessione viene terminata per inattività o sconnessione manuale
Error: Remote Server not found	Il server remoto non ha risposto. Può dipendere dal server remoto stesso o da problemi sul link di connessione
Error: PPP Connection failed	Impossibile stabilire una corretta negoziazione PPP con il server remoto. Può dipendere dal server stesso o da errata impostazione di user id e password.
Error: Connection to Server lost	La connessione con il server remoto è stata persa. Potrebbe essere stata causata da caduta accidentale del link, mancanza di alimentazione o blocco del server remoto.
Error: Invalid or unknown packet type	I dati ricevuti dal server remoto sono incompatibili, incomprensibili o sconosciuti. Potrebbe essere causato da dati corrotti a causa di una connessione inaffidabile o instabile oppure il server remoto utilizza un protocollo non supportato dal dispositivo.

Connection Status - PPTP

Log di connessione quando si utilizza PPTP (Peer-to-Peer Tunneling Protocol).



PPTP

Connection

Physical Address	Il Mac address (lato WAN) del dispositivo
IP Address	L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo)
PPTP Status	Indica lo stato attuale della connessione - Se la connessione non è attiva, il pulsante Connect permette di iniziarne una - Se la connessione è attiva il pulsante Disconnect termina la connessione in corso

Connection Log	
Connection Log	Fornisce una serie di messaggi inerenti l'attività di connessione/negoziazione del protocollo PPTP.
Bottoni	
Connect	Se non collegato, attiva una connessione verso l'ISP.
Disconnect	Se connesso, termina la connessione.
Clear Log	Cancella il contenuto del log di connessione
Refresh	Aggiorna le informazioni visualizzate.

Connection Details - Fixed/Dynamic IP Address	
Log di connessione quando si utilizza il metP ⁰ "Direct" (senza login).	



Fixed/Dynamic IP address	
Internet	
Physical Address	Il Mac address (lato WAN) del dispositivo
IP Address	L'indirizzo IP con il quale il dispositivo viene identificato sulla WAN (Attenzione, non è l'indirizzo IP lato LAN del dispositivo).
Network Mask	La Network Mask (Subnet Mask) per l'indirizzo sopra
Default Gateway	L'indirizzo IP del Gateway o Router associato con l'indirizzo sopra.
DNS IP Address	L'indirizzo IP del Domain Name Server attualmente in uso.
DHCP Client	Mostra "Enabled" (attivo) o "Disabled" (disattivo) a seconda dell'impostazione DHCP client. Se "Enabled" il tempo mostrato da "Remaining lease time" indica quando l'indirizzo IP allocato dal DHCP Server non sarà più valido. Allo scadere del tempo l'indirizzo sarà automaticamente rinnovato. Usare il bottone "Renew" per rinnovarlo manualmente.
Bottoni	
Release/Renew	- Premendo questo bottone l'indirizzo IP viene rinnovato o rilasciato. Non attivo se l'impostazione è Fixed (Static) IP address..
Refresh	Aggiorna le informazioni visualizzate.

2.6. COME CONFIGURARE LE STAZIONI DI RETE

2.6.1. CONFIGURAZIONE DEL TCP/IP

Se utilizzate il servizio DHCP Server:

- Configurate ogni computer come DHCP client, cioè per ottenere automaticamente un indirizzo IP dalla rete.

Se sulla vostra rete è già presente un DHCP server:

- Configurate il vostro DHCP server per assegnare alle stazioni l'indirizzo IP di Firegate 10NX come "Default Gateway" o "Router".
- Riportate il computer utilizzato per la configurazione al suo stato originale.

Se sulla vostra rete è già presente uno o più Router:

- Non modificate le impostazioni delle stazioni di rete
- Fate riferimento al capitolo Routing del manuale completo.

Se sulla vostra utilizzate indirizzi IP statici:

Su tutte le stazioni di rete:

- Inserite l'indirizzo IP di Firegate 10NX nel campo Default Gateway
- Inserite lo stesso indirizzo IP del DNS inserito nella configurazione di FireGate 10NX nel campo DNS.

2.6.2. NAVIGAZIONE INTERNET TRAMITE ROUTER IN LAN

Fate riferimento alla voce Routing Table del manuale completo.

2.6.3. IMPOSTAZIONI INTERNET

Ogni stazione di rete deve essere configurata per accedere ad Internet tramite la LAN (non attraverso una connessione modem).

In Windows® 95/98/Me/2000/XP:

- Dal menu di Avvio – Programmi – Accessori, (Comunicazioni) oppure Internet Explorer.
- Selezionate Connessione guidata (Internet Connection Wizard).
- Selezionate "rete locale (LAN)" quando richiesto.

2.6.4. ACCESSO INTERNET – LA NAVIGAZIONE

Una volta terminata la configurazione della stazione di rete per accedere ad Internet tramite la LAN, è sufficiente utilizzare il vostro browser per accedere ad un sito Internet, ad esempio www.digicom.it.

Le Funzioni Avanzate

FireGate 10NX mette a disposizione una serie di funzioni Avanzate per permettere una più completa e sofisticata configurazione del sistema, le più importanti di seguito elencate :

- Advanced Internet
 - Communication Applications, per dirigere delle "sessioni" di comunicazione entranti, quando la destinazione non è conosciuta, verso specifici PC di LAN
 - Special Applications, per mappare in modo specifico "porte UDP/TCP" interne ed esterne in uso da applicazioni particolari
 - DMZ, per permettere l'accesso "trasparente" ad un singolo PC di LAN dall'esterno
 - URL filter, per bloccare la navigazione e accesso a siti internet "non autorizzati"
- Access Control, per restringere l'uso di Internet e di applicazioni a singoli o gruppi di PC
- DoS attack Firewall, per essere protetti dai più comuni attacchi di hacker e buontemponi.
- Policy based Firewall, per creare regole di tipo blocca/permitti sui pacchetti in transito tra LAN, WAN e DMZ
- VPN Policy, per creare connessioni protette attraverso Internet tramite i protocolli VPN, IPSEC, IKE e certificati.
- VPN passthrough, per realizzare connessioni protette attraverso Internet

- Remote Management, per accedere alla configurazione del dispositivo da remoto
- Virtual Servers, per “esportare” dei servizi presenti sui computer di LAN e renderli accessibili da Internet (Web server, FTP server, ecc)
- Dynamic DNS, per associare l'IP dinamico ad un URL (nome di dominio) virtuale, anche se l'IP cambia da connessione a connessione
- Firmware Upgrade, per aggiornare il firmware e le funzioni del dispositivo

Fate riferimento ai manuali completi relativi ai vari modelli FireGate 10NX per la descrizione dettagliata delle suddette funzioni.

3. RISOLUZIONE DEI PROBLEMI

3

In questa sezione troverete le soluzioni ai problemi più comuni e le indicazioni per individuare le cause dei malfunzionamenti, nel caso si verificassero.

Problema 1: Non riesco ad accedere alla configurazione del dispositivo

Soluzione 1: Verificare che:

- Il dispositivo sia acceso e le connessioni LAN siano corrette.
- Che il PC utilizzato abbia il protocollo di rete TCP/IP installato, e che sia associato alla scheda di rete. Se mancante cliccate su Aggiungi, protocollo, Microsoft, TCP/IP, OK. Potrebbe essere necessario riavviare il PC.
- Che il PC e il dispositivo siano connessi allo stesso segmento di rete.
- Che gli indirizzi IP siano corretti, come definiti nella parte di configurazione di questo manuale.

Problema 2: Inserendo un indirizzo URL o indirizzo IP ricevo un errore di time out

Soluzione 2: Verificate che le impostazioni TCP/IP del computer siano corrette (indirizzo IP, Default gateway e DNS).

Effettuate un Ping verso il dispositivo. Da prompt di DOS digitare

Ping xxx.xxx.xxx.xxx

dove xxx.xxx.xxx.xxx è l'indirizzo IP del dispositivo.

In caso di risposta negativa verificare che il router sia connesso alla LAN e acceso. Se cos'è, il problema è dovuto alla rete LAN.

Nelle finestre di Status esaminate il log. Fate riferimento alla sezione Connection Log.

Verificate che il modem xDSL sia acceso e correttamente connesso.

Verificate le impostazioni "Proxy Server" del PC.

Il dispositivo non è un Proxy Server e il PC non necessita di un "Proxy Server" per utilizzarlo.

Se è presente un Proxy Server in LAN, disabilitatelo e disabilitate le impostazioni "Proxy Server" del PC.

Se il provider ha un Proxy Server seguite le istruzioni da esso fornite.

Problema 3: Alcune applicazioni non funzionano correttamente quando utilizzano il dispositivo

Soluzione 3: Il dispositivo processa i dati che lo attraversano e non è trasparente.

La finestra Advanced Internet mette a disposizione alcune funzionalità per le applicazioni non standard:

Special Internet Applications

Exposed Computer

Utilizzare Special Internet Applications quando possibile.

Ricordare che ad ogni modo un solo utente alla volta può usare un'applicazione speciale.

Se non si riesce ad ottenere un buon funzionamento utilizzare la funzione Exposed Computer.

Attenzione, questa funzione scavalca qualsiasi sicurezza ed espone la LAN ad accessi indiscriminati dall'esterno.

21010 Cardano al Campo VA
via A. Volta 39

