Reference Guide

WinRoute Pro 4.1 IT

Per configurazioni 22 di versione 4,1 e successivamente

Tiny Software Inc.

Sommario

Installazione ed esecuzione — Capitolo 2

PRIMA DI COMINCIARE

Gentile Cliente,

grazie per avere acquistato/valutato WinRoute Pro. Tiny Software, leader nella tecnologia firewall per reti di piccole/medie dimensioni, ha dedicato tempo e risorse alla creazione di un router/firewall per i sistemi operativi Windows, che fosse potente e nel contempo facile da usare.

WinRoute Pro è un'applicazione per reti che, eseguita su un PC, sostituisce efficacemente router e firewall hardware ben più costosi. Per funzionare al meglio richiede che la rete sia impostata e configurata correttamente, e che l'utente abbia una certa dimestichezza con gli ambienti di rete.

Sulla base delle statistiche condotte, nel 90 per cento dei casi l'errata configurazione della rete è responsabile delle difficoltà di connessione a Internet. Il presente manuale è ricco di esempi di configurazione di rete, ma è bene ricordare che ogni impostazione può avere caratteristiche proprie.

È molto importante leggere attentamente la presente documentazione. È stata creata per utenti in possesso della conoscenza teorica necessaria per utilizzare le reti e della capacità di installare una LAN (Local Area Network).

Per ulteriori suggerimenti, elenchi di controllo o aggiornamenti, si consiglia di collegarsi al supporto on-line prima di contattare il supporto tecnico.

Rinnoviamo i nostri più sentiti ringraziamenti per avere acquistato/valutato WinRoute.

Cordialmente,

TINY SOFTWARE, INC.

CAPITOLO 1

DESCRIZIONE DI WINROUTE

In questo capitolo

Principali caratteristiche di WinRoute

WinRoute Pro è un **router- firewall software per Internet**e con poche, semplici operazioni di impostazione predispone i computer di una rete a condividere un'unica connessione Internet, utilizzando linee di accesso remoto, DSL, cavo, ISDN, LAN, T1, radio o DirecPC.

Amministrazione remota

L'Amministrazione di WinRoute gestisce la configurazione e le impostazioni di WinRoute. Poiché si tratta di un'applicazione separata (wradmin.exe), può essere eseguita da qualunque computer collegato al PC su cui è installato WinRoute. L'accesso a WinRoute è protetto da crittografia avanzata e password.

Registrazione log

WinRoute Pro fornisce uno strumento completo per il controllo del traffico che passa dal computer host. L'amministratore potrà analizzare i pacchetti TCP, UDP, ICMP, ARP, le richieste DNS, le informazioni sul driver e molto altro. Tutte le operazioni contengono l'indicatore della data e dell'ora.

Router IP NAT

WinRoute include la migliore implementazione della tecnologia NAT (Network Address Translation) disponibile attualmente sul mercato, studiata per offrire funzionalità complete di routing e di protezione della rete. Il driver NAT, scritto esclusivamente per WinRoute, è una soluzione di protezione paragonabile a prodotti molto più costosi.

Routing NAT avanzato

Il protocollo NAT avanzato permette di modificare l'indirizzo IP di origine dei pacchetti in uscita, sulla base di diversi criteri. Ciò garantisce la facile integrazione delle LAN protette da WinRoute nella WAN aziendale con diversi segmenti, zone di delimitazione, reti private virtuali, ecc.

Server host protetti da WinRoute

In base all'impostazione predefinita, WinRoute chiude tutte le porte, a garanzia della massima protezione. Le richieste esterne saranno pertanto rifiutate, a meno che non vengano create mappature specifiche. La tecnologia di mappatura della porta permette di deviare i pacchetti IP che passano attraverso le interfacce gestite da WinRoute. Con WinRoute, gli utenti possono fare in modo che i pacchetti in entrata diretti a una determinata porta vengano indirizzati a un computer interno prescelto. Ciò consente di eseguire all'interno del firewall un server Web, un server di posta elettronica, un server FTP, un server VPN o, di fatto, qualunque altro tipo di server.

Protezione del firewall

Grazie alla combinazione dell'architettura NAT e della capacità di operare a livello basso, WinRoute è in grado di offrire un livello di protezione pari a quello di soluzioni ben più costose. WinRoute opera sia sui pacchetti in uscita sia su quelli in entrata. Funzionalità quali l'anti-spoofing, un add-on per il filtro pacchetto di WinRoute, garantiscono un'ulteriore protezione della LAN dagli attacchi che si avvalgono della strategia di cambiamento dell'indirizzo IP di origine.

Configurazione di rete semplificata

Il server DHCP e il server d'inoltro DNS inclusi in WinRoute Pro semplificano l'amministrazione della configurazione di rete. Entrambi si basano su tecnologie di comprovata efficacia. Il server DHCP di WinRoute può sostituire il server DHCP di Windows NT.

Server di posta elettronica

Il server di posta elettronica di WinRoute, grazie a caratteristiche quali l'assoluta compatibilità con SMTP/POP3, la possibilità di creare alias pressoché infiniti e all'ordinamento automatico della posta, è uno strumento estremamente versatile. Gli utenti possono avere uno o più indirizzi di posta elettronica e lavorare efficacemente in gruppi (ad es. vendite, supporto tecnico, ecc.), e ciascun gruppo può essere assegnato a più utenti. Le funzionalità sono disponibili indipendentemente dal tipo di connessione Internet utilizzata.

Cache HTTP

L'architettura di WinRoute include un'innovativa tecnologia di gestione della cache. A differenza dei server proxy con funzionalità di cache, la memoria cache di WinRoute archivia i dati passanti in un file di lunghezza predefinita invece di utilizzare un file per ciascun oggetto. Ciò consente di risparmiare significative quantità di spazio su disco, soprattutto in ambienti che utilizzano il file system FAT16, ovvero la maggior parte dei sistemi operativi Windows 95.

Supporto avanzato ai protocolli

WinRoute supporta i seguenti protocolli standard di Internet:

IPSEC, H.323, NetMeeting Net2Phone WebPhone UnixTalk RealAudio RealVideo ICA Winframe IRC FTP HTTP Telnet PPTP Traceroute Ping Year 2000 Aol, chargen, cuseeme, daytime, discard, dns, echo, finger, gopher, https, imap3, imap4, ipr, IPX overIP, netstat, nntp, ntp, ping, pop3, radius, wais, rcp, rlogin, rsh, smtp, snmp, ssl, ssh, systat, tacacs, uucpover IP, whois, xtacacs

Router NAT

In questa sezione

Introduzione a NAT

NAT - Network Address Translation

Network Address Translation, o NAT, è una delle funzioni di protezione più potenti di WinRoute. Si tratta di un protocollo standard con il quale è possibile "nascondere" gli indirizzi di reti private dietro un unico indirizzo o indirizzi multipli. La versione NAT denominata "IP Masquerading" è nota da tempo alla comunità di utenti Linux, ma WinRoute è uno dei pochi prodotti per Windows in grado di fornire fu zionalità NAT entry-level.

NAT può essere implementata in molti modi, ma essenzialmente crea un numero quasi illimitato di spazio per indirizzi privati che vengono poi "tradotti" da WinRoute affinché la comunicazione possa transitare su reti pubbliche senza rivelare le informazioni sui sistemi interni. Non essendo noto lo spazio degli indirizzi privati sull'interfaccia interna di un firewall WinRoute, è praticamente impossibile attaccare direttamente un sistema protetto con NAT.

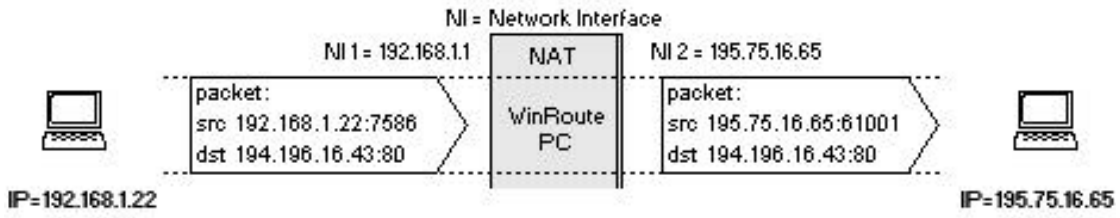
Funzionamento di NAT

Network Address Translation (NAT) è un processo che modifica i pacchetti inviati o ricevuti dalla rete locale a/da Internet o altre reti basate su IP.

Pacchetti in uscita

Dopo essere stati manipolati dal modulo di traduzione degli indirizzi, i pacchetti provenienti **dalla** LAN appaiono come se fossero stati inviati dal computer su cui NAT è in esecuzione (il computer è connesso direttamente a Internet). Quello che realmente accade è che l'indirizzo IP di "origine" dell'intestazione viene sostituito con l'indirizzo IP (pubblico) del computer "NAT".

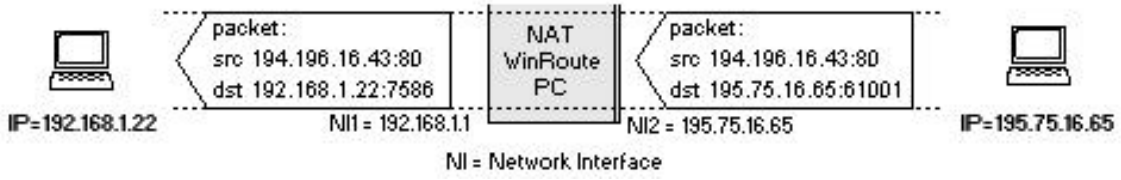
Il modulo NAT crea inoltre una tabella con le informazioni relative a ciascun pacchetto transitato su Internet.



Pacchetti In entrata

I pacchetti che passano per NAT, nel tragitto di ritorno **VERSO** la LAN, sono confrontati con le registrazioni archiviate dal modulo NAT. L'indirizzo IP di "destinazione" viene sostituito (sulla base dei record del database) con lo specifico indirizzo IP interno di classe privata, affinché il pacchetto possa raggiungere il computer di destinazione nella LAN.

Si ricordi che originariamente il pacchetto possedeva l'indirizzo IP pubblico del computer NAT come "destinazione", e che il modulo NAT aveva dovuto modificare tale informazione per poter consegnare il pacchetto al destinatario interno alla rete locale.



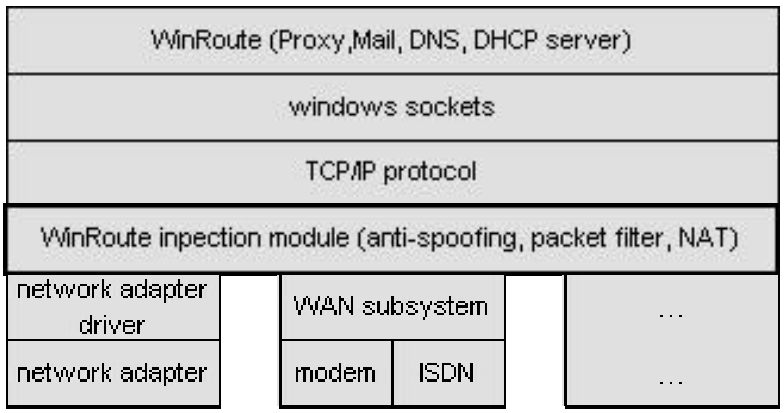
Architettura di WinRoute

Architettura di WinRoute

Per sfruttare a pieno Internet, è importante conoscere le modalità di funzionamento di WinRoute. Come dimostrano le spiegazioni e gli esempi di seguito riportati, WinRoute è una soluzione eccellente per la maggior parte delle configurazioni di rete.

1. **Protezione totale**
   WinRoute opera **al di sotto dello stack TCP/IP**, a livello IPSEC. In altre parole, cattura i pacchetti **in uscita** e **in entrata PRIMA** che raggiungano il computer.

Questa caratteristica avanzata rende la protezione di WinRoute virtualmente **inattaccabile.**



2. **Supporto completo al protocollo**
   WinRoute è un ROUTER software e come tale, a differenza di server proxy quali WinGate o WinProxy, consente il passaggio della maggior parte dei protocolli Internet. Allo stesso tempo WinRoute controlla ogni pacchetto utilizzando funzioni avanzate di protezione e di firewall completamente integrate nel software. Nei sistemi che operano con Windows 95 e 98, WinRoute gestisce l'indirizzamento dei pacchetti, mentre nei sistemi che operano con Windows NT, l'indirizzamento è affidato al sistema operativo e WinRoute gestisce la funzionalità NAT e altri dati.
3. **Flessibilità assoluta**
   WinRoute esegue NAT (Network Address Translation) sulle interfacce scelte dall'utente, ed eventuali altre regole di protezione predefinite per interfacce specifiche. Una tale flessibilità consente all'utente di progettare e configurare le opzioni di protezione nella più assoluta libertà.

Installazione di NAT su entrambe le interfacce

Qualora sia stata già adottata una soluzione per l'accesso condiviso a Internet, è possibile utilizzare WinRoute anche solo come **router di accesso neutro** per il traffico (pacchetti) proveniente da **Internet** e diretto a una **rete locale**; se la soluzione in uso non consente di utilizzare server e applicazioni per la connessione a Internet da una rete privata, WinRoute potrebbe essere la soluzione giusta.

I servizi tipici a cui è possibile accedere tramite Internet sono:

- Server Telnet (ad es. AS400)
- Server WWW
- Server di posta elettronica
- PC Anywhere
- Server FTP
- … e qualunque altro server (servizio) accessibile su una data porta.

WinRoute mette a disposizione di utenti e clienti un accesso affidabile e sicuro per tali servizi. La configurazione di WinRoute per questi servizi è descritta in altri capitoli. Le impostazioni seguenti saranno eseguite diversamente:

Funzionalità	Impostazione consigliata	In questo scenario
NAT su interfaccia Internet	ABILITATA	ABILITATA
NAT su interfaccia interna (LAN)	DISABILITATA	ABILITATA
Indirizzo IP dell'interfaccia interna di WinRoute, come gateway predefinito per gli altri computer della rete	SÌ (OBBLIGATORIO)	NO (non necessario)

In altre parole, utilizzando WinRoute è possibile rendere accessibili determinati servizi di Internet SENZA modificare la configurazione della rete.

✍✍ ***Nota! Se si installa NAT su entrambe le interfacce NON sarà possibile utilizzare WinRoute per la condivisione di Internet!***

Le impostazioni predefinite del gateway utilizzate per l'esempio consentono ampia libertà e non richiedono la modifica degli ambienti esistenti. È possibile mantenere attivi i router e le route già impostati e aggiungere nuovi computer, per consentire agli utenti esterni di accedere ai server della rete locale, quali l'AS400 (server Telnet) di una rete WAN esistente, o a una rete interna tramite PPTP.

Per ottenere questi risultati è necessario procedere come di seguito indicato:

1. Collegare in rete un computer con due interfacce: una (interfaccia esterna) per la connessione a Internet, l'altra per la connessione alla rete esistente.
2. Assegnare ai servizi/server che si desidera rendere accessibili da Internet l'interfaccia esterna con l'indirizzo IP.
3. Assegnare l'indirizzo IP interno manualmente o tramite il server DHCP.
4. Impostare WinRoute in modo che NAT venga eseguita su entrambe le interfacce.
5. Mappare la porta per i servizi che si desidera utilizzare all'interno della rete

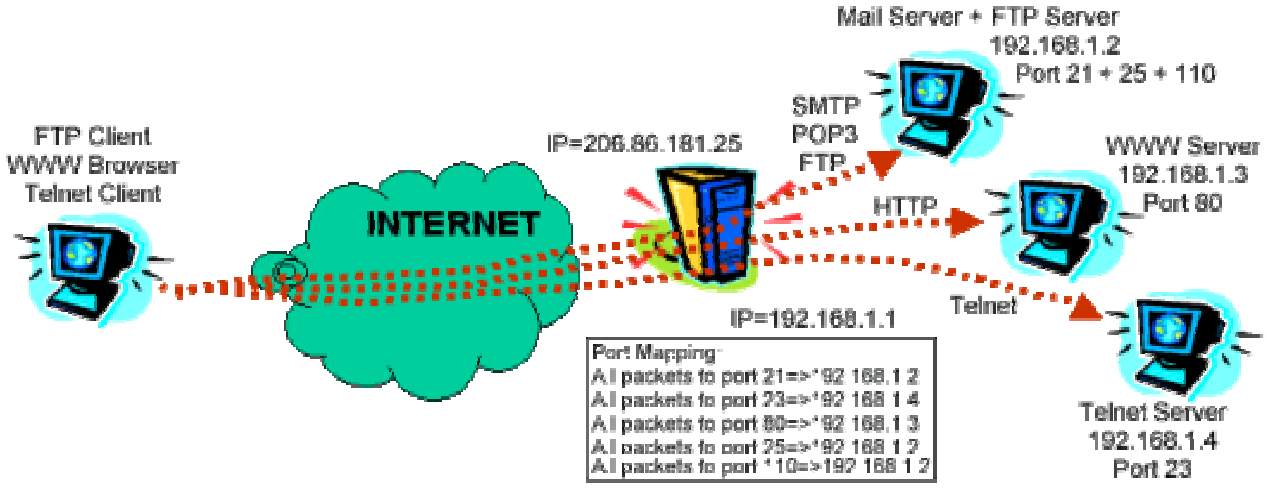
Terminate le impostazioni, gli utenti esterni potranno accedere da Internet ai servizi interni della rete eseguiti su porte specifiche. La protezione dell'accesso è garantita dal firewall di WinRoute.

Mappatura della portainoltro dei pacchetti

Utilizzando la mappatura della porta (o PAT - Port Address Translation), i server WWW o FTP e gli altri servizi pubblici eseguiti su una rete privata diventano accessibili da Internet anche se WinRoute esegue NAT, il protocollo che rende inattaccabile dall'esterno la rete protetta.

Come funziona la mappatura della porta

Tutti i pacchetti ricevuti da una rete esterna (Internet) sono sottoposti a controllo, per verificare se gli attributi (è cioè il protocollo, la porta di destinazione e l'indirizzo IP di destinazione) siano conformi alle voci della tabella di mappatura della porta (protocollo, porta in ascolto, IP in ascolto). Se il pacchetto in arrivo soddisfa i criteri desiderati, verrà modificato e inviato all'indirizzo IP della rete protetta, definita nella tabella come "IP di destinazione", e alla porta definita "Porta di destinazione".

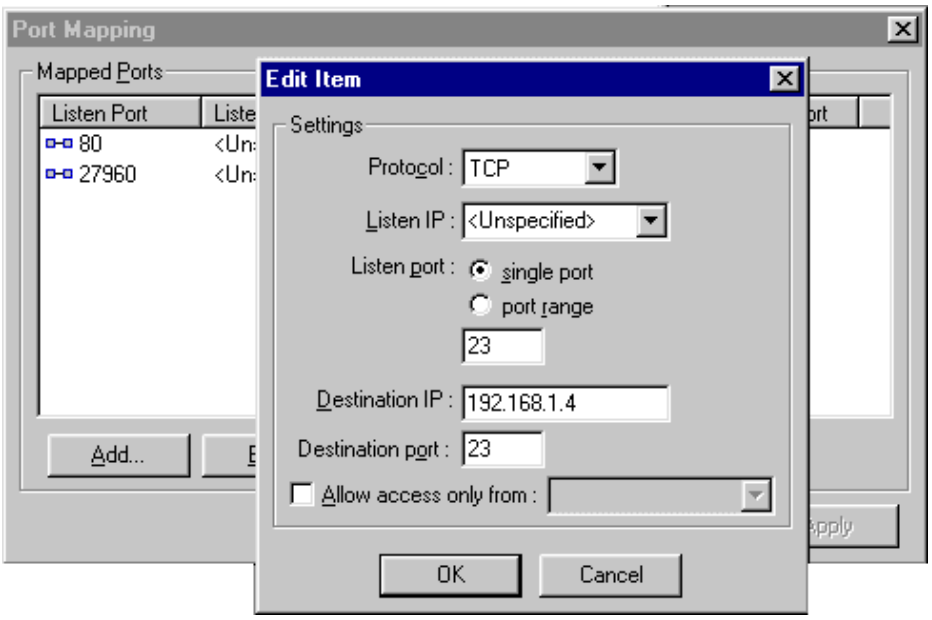


A titolo esemplificativo, si supponga che l'indirizzo interno IP di un server Web sia 192.168.1.3 e che si desideri consentirne l'accesso da Internet. L'indirizzo IP esterno delle richieste degli utenti Internet inoltrate al computer WinRoute sarà uguale al record DNS relativo al server Web www.tuodominio.com. Poiché tutte le richieste indirizzate al server Web arrivano alla porta 80, sarà sufficiente mappare la porta in modo che le comunicazioni TCP in arrivo sulla porta 80 siano deviate all'indirizzo IP interno 192.168.1.3.

Mappatura della porta

Per impostare la mappatura della porta

1. Scegliere il menu *Impostazioni->Avanzate->Mappatura porte*
2. Aggiungere la nuova mappatura:



Protocollo

Selezionare il protocollo utilizzato dall'applicazione/servizio. Alcune applicazioni/servizi, quali ad esempio Amministrazione di WinRoute, utilizzano insieme i protocolli TCP e UDP.

IP in ascolto

L'indirizzo IP a cui pervengono i pacchetti in entrata. Generalmente è l'indirizzo IP associato all'interfaccia Internet dell'utente. Nota: all'interfaccia possono essere associate più indirizzi IP (qualora si abbiano più server Web, ecc.).

Porta in ascolto

Il numero della porta a cui pervengono i pacchetti.

IP di destinazione

L'indirizzo IP interno alla rete locale su cui viene eseguito il server (servizio) che risponde ai pacchetti in entrata (server Web, server FTP, ecc.).

Porta di destinazione

La porta su cui è in ascolto l'applicazione di destinazione. Solitamente è uguale al numero della porta in ascolto.

Consenti accesso solo da

È possibile specificare l'indirizzo IP attraverso cui si desidera consentire l'accesso. Questa opzione è molto importante ai fini della sicurezza, nel caso in cui si mappi la porta per applicazioni di gestione remota quali Amministrazione di WinRoute, PC Anywhere ecc. È possibile specificare un gruppo di indirizzi IP, a condizione che il gruppo sia stato creato nella finestra di dialogo "Gruppi di indirizzi".

Mappatura della porta con i sistemi multihomed (indirizzi IP multipli)

È possibile che siano assegnati più indirizzi IP all'interfaccia Internet, e che si desideri rendere accessibili da Internet i servizi multipli di una rete.

Scenario con cinque server WWW

A titolo esemplificativo, si supponga di voler eseguire cinque server Web, ciascuno dei quali con proprio dominio associato a indirizzi IP differenti.

In questo scenario si dovranno assegnare cinque indirizzi IP alle interfacce esterne (collegamento a Internet) ed eseguire i server Web sugli altri computer della rete interna.

È possibile eseguire ogni server Web su un diverso computer, oppure assegnare più indirizzi IP a un computer della rete interna ed eseguire i server Web su di esso.

Si dovranno quindi definire cinque mappature di porte nella finestra di dialogo Mappatura porte. Per ciascuno dei server Web (dominio) definire:

- L'indirizzo IP in ascolto (indirizzo IP pubblico associato al dominio).
- La porta in ascolto: nello scenario ipotizzato dall'esempio è 80.
- L'indirizzo IP di destinazione: l'indirizzo IP a cui viene eseguito il server Web.
- La porta di destinazione: 80 (per WWW)

Per ulteriori esempi sulla mappatura avanzata delle porte, vedere il capitolo "Internetworking avanzato".

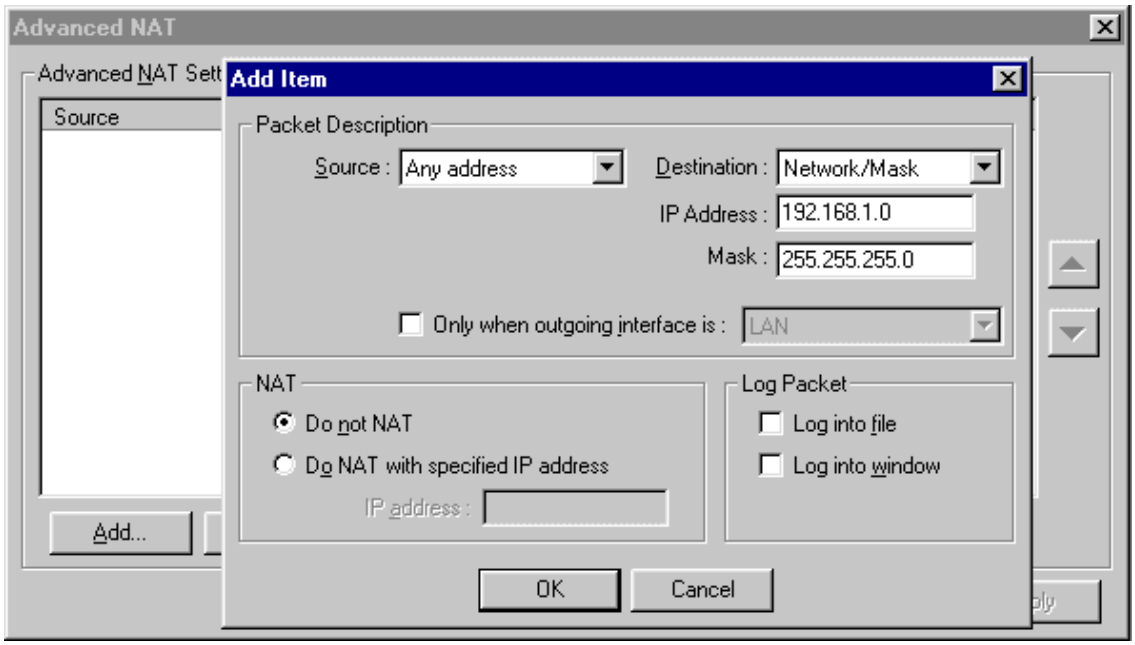
NAT multipli

WinRoute permette di utilizzare impostazioni **NAT** (Network Address Translation) semplici o complesse. In base all'indirizzo IP di **origine** o di **destinazione** del pacchetto, è possibile specificare se NAT verrà eseguita su alcuni **indirizzi IP** (nel quale caso i pacchetti apparirebbero come se fossero stati originati da un altro indirizzo IP) o se non verrà eseguita affatto.

Queste impostazioni sono molto importanti, soprattutto nel caso di reti complesse dove:

- Alcuni computer devono avere un indirizzo IP apparentemente **diverso** da quello del computer principale, utilizzato dal **resto** della rete.
- Esistono succursali connesse tramite **WAN** a uno spazio di indirizzo privato, e le succursali devono condividere **un solo** accesso Internet
- Esistono segmenti multipli gestiti da WinRoute, e uno o più segmenti costituiscono una zona DMZ con indirizzi IP pubblici
- Si desidera avere indirizzi IP pubblici in una rete privata (importante! Verificare con il proprio provider Internet che le route di questi indirizzi IP transitino dall'indirizzo IP principale).

Il capitolo "Internetworking avanzato" contiene molti esempi che illustrano le impostazioni avanzate di NAT.



Indirizzo IP di origine, indirizzo IP di destinazione

È possibile eseguire impostazioni NAT avanzate sulla base dell'indirizzo IP di origine o di destinazione. Come indirizzo di origine è possibile specificare l'IP dell'host, l'intera rete (limitata dalla maschera di rete) o il gruppo di indirizzi IP precedentemente creati nel menu Impostazioni->Avanzate->Gruppi di indirizzi.

Non eseguire NAT

I pacchetti selezionati in transito dall'interfaccia Internet non verranno modificati.

Esegui NAT con l'indirizzo IP specificato

I pacchetti selezionati in transito dall'interfaccia Internet verranno modificati, come se fossero stati originati dall'indirizzo IP desiderato.

Tabella interfaccia

La Tabella interfaccia è una finestra di dialogo in cui vengono visualizzate le interfacce riconosciute da WinRoute nel computer. Se il numero delle interfacce installate sul computer è superiore a quello riportato da WinRoute, è possibile che il driver delle interfacce non riconosciute non sia stato caricato correttamente dal sistema operativo, e che pertanto WinRoute non sia riuscito a leggerlo.

La tabella riporta:

Nome dell'interfaccia

Per modificare il nome visualizzato, selezionare “proprietà” e modificare il nome.

Indirizzo IP

Il valore impostato nelle proprietà TCP/IP dell'interfaccia. Se l'interfaccia è stata impostata per ottenere l'indirizzo IP dal server DHCP, verrà visualizzato l'indirizzo IP assegnato all'interfaccia.

NAT “On” o “Off”

Se NAT è stato è stato impostato per essere eseguito sull'interfaccia, in questa colonna verrà visualizzata l'indicazione “On”.

Supporto VPN

Come ricordato in precedenza, WinRoute può utilizzare i due protocolli VPN più diffusi per lo smistamento del traffico: IPSec (IP Security protocol) proposto da IETF, e il protocollo di tunnelling point-to-point, molto utilizzato in questi ultimi anni perché è stato incluso nel software del sistema operativo client di Microsoft Windows.

Firewall con filtro pacchetti

In questa sezione

Informazioni generali sui filtri pacchetto

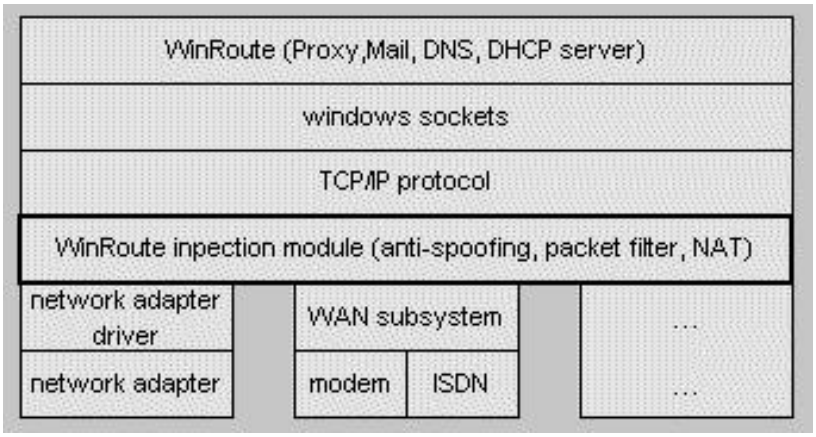
Il cuore di tutti i meccanismi che controllano l'accesso a un firewall è la tecnologia che permette o rifiuta l'accesso dei pacchetti alle reti protette. WinRoute implementa quella che, fra tutte, è forse la più utilizzata: il filtro pacchetti. Sebbene WinRoute implementi anche altri meccanismi di controllo sull'accesso, quali un server proxy cache integrato per i protocolli HTTP, FTP e Gopher, si tratta in questo caso di un elemento atto a migliorare le prestazioni, non di una funzione di protezione.

Il filtro pacchetti vanta una lunga tradizione in termini di efficacia, e viene ancora ampiamente utilizzato in prodotti quali il sistema operativo dei dispositivi di rete IOS di Cisco. Se configurati correttamente, i filtri pacchetti offrono una protezione affidabile, indicata specialmente per i siti Internet con grande volume di traffico.

Architettura

Generalmente i firewall sono costituiti da una componente hardware, integrata nella piattaforma, e da una componente software, difficile da eludere. Molti dispositivi di protezione delle reti soffrono di un difetto comune: nell'intervallo che intercorre tra il momento in cui l'hardware è in grado di instradare il traffico e il momento in cui il software assume il controllo delle interfacce di rete, la protezione può risultare completamente compromessa.

Il driver (o modulo di gestione) di WinRoute si attiva subito dopo il caricamento in memoria dei file principali del sistema operativo Windows (kernel); in particolare, viene caricato prima dei moduli NDIS (Network Device Interface Specification), per impedire che la connessione avvenga quando WinRoute non è ancora attivo. In questo modo tutte le interfacce sono protette prima che il traffico dannoso o altri tipo di attacchi possano danneggiare il sistema. Questo meccanismo è più affidabile dei prodotti autonomi per il rilevamento delle intrusioni che, essendo eseguiti come servizi, entrano in funzione solo dopo l'avvio del sistema.



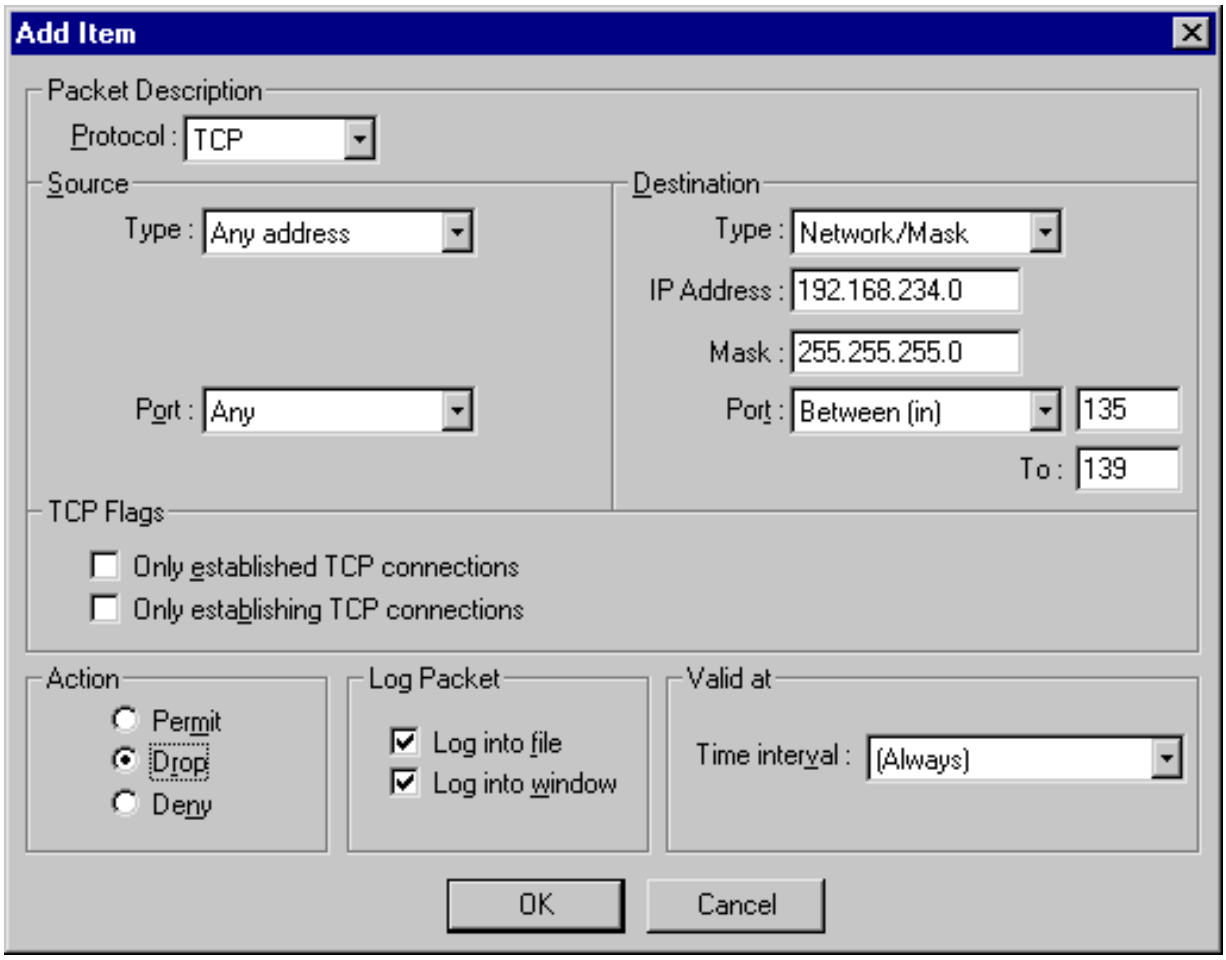
WinRoute "raccoglie" le NDIS in modo proprietario, cosicché tutto il traffico TCP/IP viene deviato dal driver della scheda di interfaccia di rete (NIC) verso il modulo di gestione, prima che esso passi lo stack delle comunicazioni di rete al sistema operativo.

L'inserimento a livello basso nel sistema operativo consente di sfruttare una prospettiva particolare sul traffico di rete in arrivo sulle interfacce (in entrata o in uscita). Come per molti altri firewall destinati alle aziende, quali ad esempio Check Point's Firewall-1, WinRoute ha diritto di decidere per primo se autorizzare o negare l'accesso a un dato pacchetto. Ancora una volta, ciò impedisce attacchi pericolosi contro altri aspetti del sistema operativo o altri software, nel caso in cui fosse stata aggirata la protezione offerta dal firewall. Si tratta certamente di un'opzione auspicabile per i gateway Internet rivolti all'esterno, ma offre grandi vantaggi anche per gli host autonomi con requisiti elevati di protezione o di anonimato, quali i sistemi incaricati del rilevamento di intrusioni. Un software di rilevamento delle intrusioni, quale ad esempio Real Secure, prodotto da Internet Security Systems (ISS), sarebbe praticamente invisibile a un host protetto da WinRoute.

Infine, il modulo di gestione di WinRoute si fa carico di tutte le funzionalità di instradamento delle comunicazioni svolte dal sistema operativo Windows (Windows 9x, NT, o 2000). Ciò garantisce che, qualora il modulo di gestione di WinRoute non funzionasse correttamente, il traffico tra le reti non verrebbe instradato. Questa opzione di interdizione del traffico in caso di errore è stata adottata da molti anni come impostazione predefinita per le configurazioni di firewall, e serve a proteggere le reti private nel caso di guasti di sistema.

Regole

Indipendentemente dalle teorie sui filtri pacchetti, la principale debolezza di un firewall è l'errata configurazione, soprattutto se eseguita da personale poco esperto. In WinRoute la configurazione dei filtri è un'operazione semplice e flessibile, tanto da permettere anche agli amministratori di rete sprovvisti di particolari conoscenze dei protocolli TCP/IP di implementare una configurazione protetta con pochi clic del mouse, come illustra la schermata riprodotta di seguito



Le regole di filtro possono essere applicate, in base all'interfaccia, a tutte le seguenti entità:

✍ Singolo indirizzo IP

✍ Elenco di indirizzi IP definito dall'amministratore

✍ Intera rete o sottorete

È importante ricordare che i filtri possono essere impostati sia per il traffico in entrata sia per quello in uscita.

Questa funzionalità permette di personalizzare in modo granulare le regole di accesso, in funzione di specifici requisiti di protezione. È possibile, ad esempio, autorizzare l'accesso di un gruppo di sviluppatori Web a specifiche risorse esterne, quali server temporanei FTP anonimi, o rendere accessibile a reti esterne un elenco specificato di indirizzi interni, per la consegna di file elettronici. La capacità di configurare sia il traffico in entrata sia quello in uscita permette di proteggersi anche da pericolosi "cavalli di Troia" quali Back Orifice (BO) o dai servlet DDOS (Distributed Denial Of Service) che cercano di aprire la porta ad attacchi esterni tramite protocolli non affidabili o attraverso il firewall.

In base alle impostazioni prescelte, è possibile permettere, ignorare o rifiutare il traffico specificato; l'opzione "Ignora" è quella che maggiormente protegge le informazioni sul firewall in caso di potenziali attacchi, perché non invia la risposta ICMP Administrative Prohobited Filter o TCP Reset/Acknowledge a un pacchetto TCP SYN (l'invio rappresenta il primo passaggio di una procedura di handshake standard a tre vie TCP).

Le regole possono essere ordinate secondo la priorità specificata dall'utente nei confronti dei pacchetti in entrata o in uscita. L'utilizzo più comune di questa di funzionalità è quello di aggiungere le cosiddette "regole di pulizia" agli elenchi filtro, per bloccare il traffico privo dell'autorizzazione rilasciata da regole la cui priorità è più alta rispetto a quelle dell'elenco (per un esempio di regola di pulizia, vedere "Regole filtro del pacchetto campione di base", più avanti in questo documento).

Protocolli

I protocolli supportati dai filtri pacchetto di WinRoute sono:

✍ IP

- Sette tipi di ICMP (o tutti)
- TCP
- UDP
- PPTP.

La possibilità di autorizzare o bloccare tipi specifici di ICMP o di protocolli IP non elaborati è di grande importanza per gli amministratori di rete, che si trovano a dover gestire elenchi sempre più complessi di requisiti da supportare. Ad esempio, i recenti protocolli VPN, quali IPSec, utilizzano i protocolli IP non elaborati 51 e 52, e non potrebbero essere filtrati dai comuni firewall commerciali, che sono in grado di controllare solo i protocolli basati su TCP o UDP.

Anti-spoofing

WinRoute è fornito inoltre di funzionalità anti-spoofing, che impediscono la creazione di pacchetti con indirizzi di origine non validi all'interno della rete. L'anti-spoofing avrebbe potuto impedire gli attacchi ICMP riportati nel febbraio 2000, attuando la negazione distribuita degli attacchi ai servizi di importanti siti Web quali Yahoo e Buy.com. Gli utenti di WinRoute sanno che, grazie a questa funzionalità, le loro reti non saranno mai oggetto di tali attacchi.

Analisi dei registri e dei pacchetti

In questa sezione

Informazioni su registri e analisi

Una funzione fondamentale di qualsiasi prodotto di protezione è rappresentata dalla capacità di fornire registrazioni continue e particolareggiate degli eventi. WinRoute utilizza sei diversi registri di traffico, per raccogliere informazioni quali i pacchetti che attraversano il firewall, le attività utente, l'applicazione dei filtri e così via. La tabella di seguito riportata contiene una breve descrizione di ciascun registro:

Registro HTTP	Visualizza solo i dati che transitano dal server proxy di WinRoute; include gli indirizzi IP di origine e il nome utente, l'indicatore data e ora, le richieste HTTP e le relative risposte.
Registro di posta elettronica	Memorizza le operazioni eseguite dal server di posta elettronica integrato in WinRoute; registra le attività di invio e ricezione POP3.
Registro di protezione	Mostra tutte le attività definite come "Accedi alla finestra/file" nelle regole che governano i filtri pacchetto (vedere qui sotto per la descrizione dettagliata delle voci registrate).
Registro chiamate	Registra l'utilizzo delle informazioni per le interfacce di accesso remoto controllate da WinRoute.
Registro di debug	Contiene le impostazioni personalizzate per la registrazione di tutti i pacchetti ARP, ICMP, UDP, TCP e/o DNS che attraversano fisicamente un'interfaccia del router WinRoute; per la configurazione granulare scegliere Impostazioni | Avanzate | Informazioni di debug, scheda Debug.
Registro errori	Visualizza le operazioni non riuscite dei moduli WinRoute in esecuzione.

Le registrazioni possono essere visualizzate sulla console di Amministrazione di WinRoute, scritte su un file, o entrambe le cose. I file di registro sono archiviati in \%directory di installazione%\Logs, e sono accessibili solo agli account NT/2000 Amministratori, Operatori di server, SISTEMA e al PROPRIETARIO AUTORE che ha installato WinRoute.

Le informazioni archiviate nei registri di protezione di WinRoute contengono tutti i dati necessari per avviare una ricerca sulle attività potenzialmente pericolose:

- Data
- Ora
- Regola di filtro pacchetto utilizzata
- Interfaccia
- Azione (se autorizzata, ignorata o rifiutata)
- Protocollo
- Indirizzo IP di origine e porta TCP
- Indirizzo IP di destinazione e porta TCP

I test eseguiti in condizioni di traffico gravoso non alterano le capacità di registrazione di WinRoute. Ciò consente di non perdere dati preziosi, che potrebbero venire utilizzati come prove legali, e consente altresì di risolvere potenziali situazioni di "negazione di servizio", ovvero le interruzioni di funzionalità del firewall che si verificano quando il sistema è oppresso.

Registro di debug

Il **registro di debug** è il registro più importante di WinRoute. Permette di vedere **tutti i pacchetti IP** (TCP, UDP, ICMP, ARP, DNS) che transitano fisicamente dalle interfacce del computer WinRoute.

La finestra **Eventi di debug** mostra gli eventi che si desidera visualizzare.

Lettura del registro

Da sinistra a destra, il registro presenta i seguenti elementi:

Indicatore data e ora la data e l'ora specificano con esattezza il momento in cui l'evento si è verificato o il pacchetto è transitato dall'interfaccia.

Protocollo - il tipo di protocollo utilizzato dal pacchetto

Nome dell'interfaccia da/a indica quale sia il nome dell'interfaccia e se il pacchetto provenga o sia destinato all'interfaccia (le interfacce del PC WinRoute sono le porte di comunicazione tra il computer e la rete).

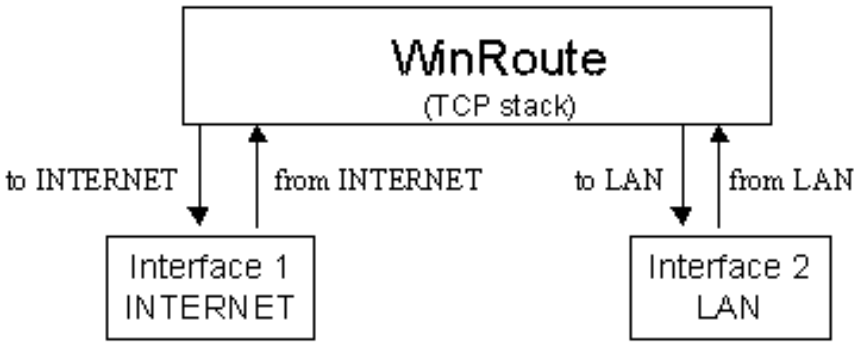
Indirizzo IP di origine -> indirizzo IP di destinazione l'origine e la destinazione degli indirizzi IP presenti nel pacchetto.

Flag - elemento di ulteriore identificazione dell'azione.

Esempio:

```
[10/Nov/1999 09:32:38] TCP: packet 511464, from lan,
length 1514, 192.168.1.7:2442 -> 192.168.1.1:25,
flags: ACK

[10/Nov/1999 09:32:38] TCP: packet 511465, to lan,
length 54, 192.168.1.1:25 -> 192.168.1.7:2442, flags:
ACK
```


WinRoute
(TCP stack)
to INTERNET
from INTERNET
to LAN
from LAN
Interface 1
INTERNET
Interface 2
LAN

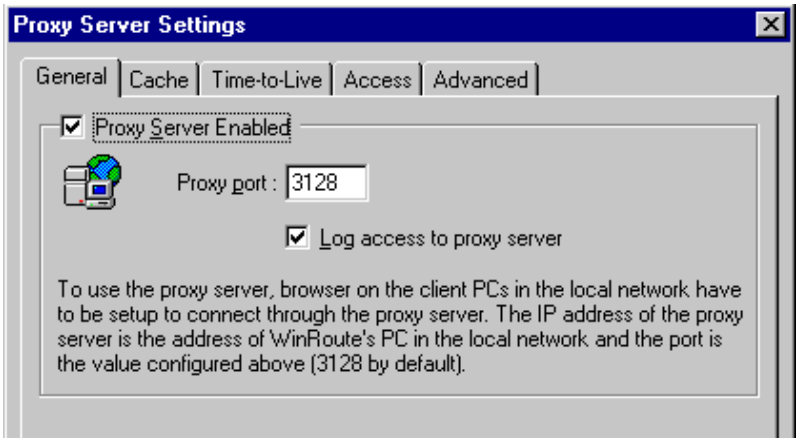
RegistroHTTP (proxy)

Il registro HTTP (proxy) è uno strumento potente che facilita il controllo delle attività degli utenti su Internet. Fornisce informazioni di più facile comprensione rispetto a quelle messe a disposizione dal registro di debug.

Funzionamentodel registro

Il registro HTTP (proxy) visualizza solo i dati che passano attraverso il server proxy di WinRoute. Ciò significa che, per ottenere tali dati, è necessario obbligare gli utenti a utilizzare il server proxy. Fare riferimento agli esempi nei capitoli sul firewall e sul server proxy.

Inoltre, è necessario abilitare l'accesso alla configurazione del server proxy.



Lettura del registro HTTP (proxy)

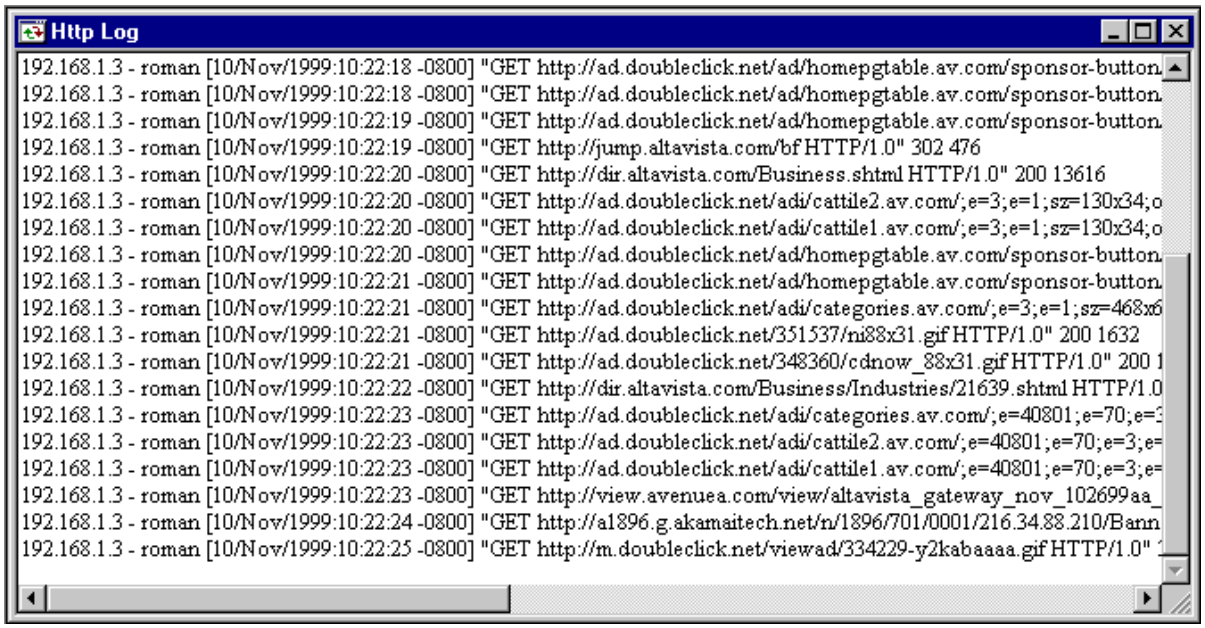
```
192.168.1.3 - roman [10/Nov/1999:10:22:20 -0800] "GET
http://dir.altavista.com/Business.shtml HTTP/1.0" 200
13616
```

Da sinistra a destra:

Indirizzo IP - nome - il nome e l'indirizzo IP corrente dell'utente che accede a Internet

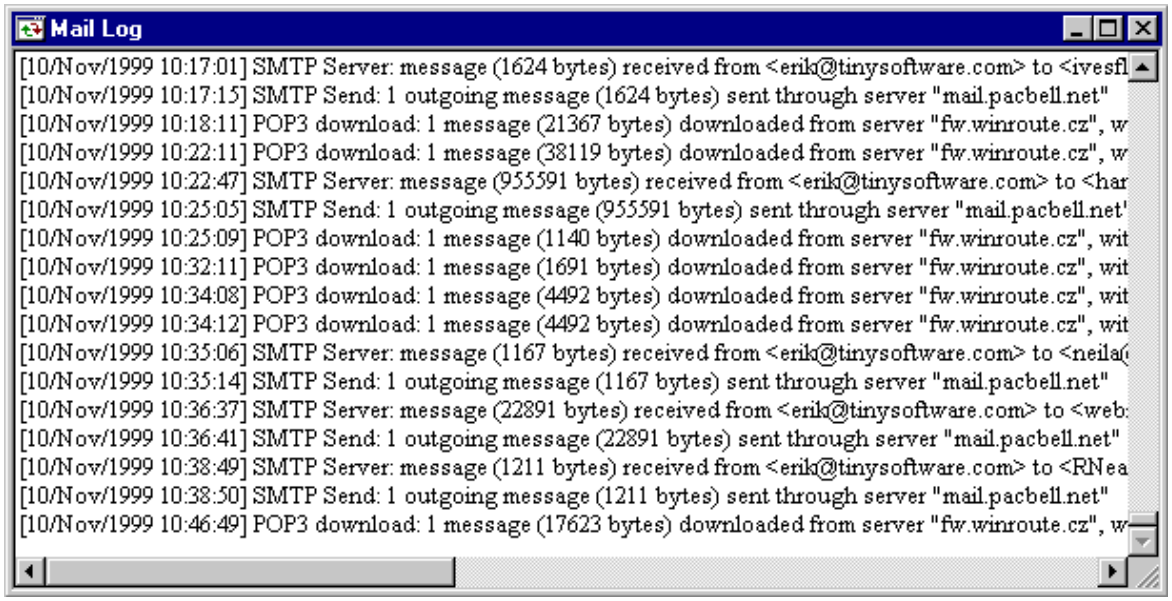
indicatore data e ora - la data e l'ora dell'accesso

GET "http..." - l'obiettivo dell'accesso



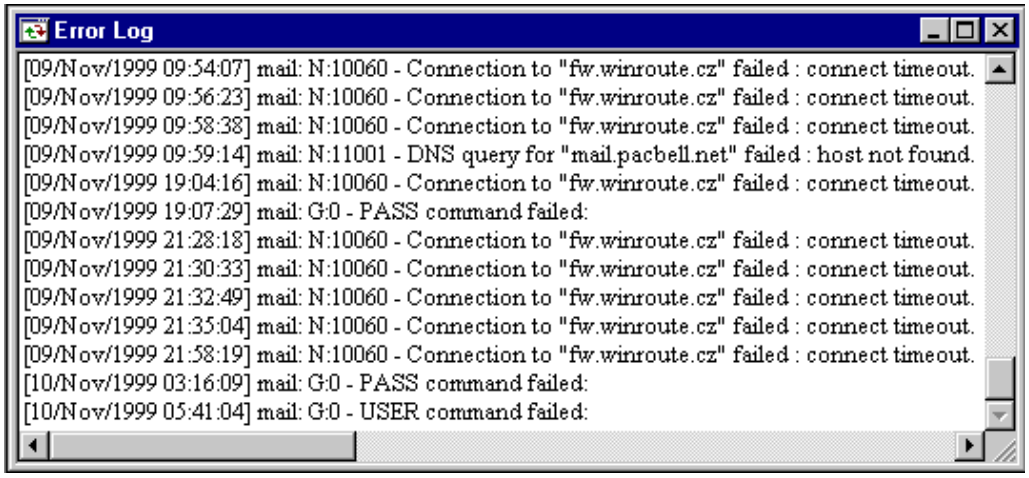
Registro di posta elettronica

Il registro di posta elettronica memorizza tutte le operazioni del server di posta elettronica integrato in WinRoute, permettendo di vedere il numero di messaggi inviati e ricevuti, la loro destinazione, ecc. Tutte le operazioni sono accompagnate dall'indicazione della data e dell'ora.



Registroerrori

Il registro errori visualizza le operazioni non riuscite nei moduli di WinRoute abilitati. Contiene gli errori intervenuti nelle operazioni di scambio della posta, del server DNS, ecc.



Server DHCP

In questa sezione

✍✍

Informazioni generali su DHCP

In una rete è necessario configurare correttamente il protocollo TCP/IP di ciascun computer. Ciò significa che l'indirizzo IP, la maschera di rete, l'indirizzo del gateway predefinito, l'indirizzo del server DNS e così via dovranno essere configurati su ogni computer. Se chi si occupa della manutenzione della rete deve configurare manualmente i parametri su un numero cospicuo di computer, sarà difficile evitare quegli errori, quali ad esempio il riutilizzo di un utilizzo, che potrebbero dare adito a collisioni o all'errato funzionamento dell'intera rete.

DHCP (Dynamic Host Configuration Protocol) è un'implementazione di WinRoute studiata per semplificare il compito degli amministratori di rete. Esso viene utilizzato per la configurazione dinamica del protocollo TCP/IP sui computer. Al momento dell'avvio, il computer client DHCP invia una richiesta. Quando il server DHCP riceve la richiesta, sceglie i parametri di configurazione TCP/IP per il client. Tali parametri sono l'indirizzo IP, la maschera di rete, il gateway predefinito, l'indirizzo del server DNS, il nome del dominio del client, e così via. Utilizzando questi parametri, il server crea una risposta e la invia al client.

Il server può anche assegnare una data configurazione al client solo per un periodo di tempo limitato (il cosiddetto "lease"). Il server assegna sempre un indirizzo IP che non entra in collisione con gli altri indirizzi assegnati tramite DHCP a un altro client.

Se il server DHCP è disponibile, è sufficiente abilitare l'opzione "Ottieni l'indirizzo IP dal server DHCP" e il server DHCP si assumerà il compito di configurare correttamente il protocollo TCP/IP sulle workstation. Questa funzionalità riduce significativamente i costi di manutenzione e di gestione della rete.

✍✍ ***Se alcuni computer della rete non vengono configurati dinamicamente da DHCP, ma dispongono di una configurazione fissa, è necessario accertarsi che i parametri utilizzati da DHCP non entrino in conflitto con quelli utilizzati dalle configurazioni fisse.***

Server d'inoltro DNS

In questa sezione

Informazioni sul server d'inoltro DNS

Ogni computer connesso a Internet è identificato da un indirizzo IP univoco, che deve essere noto al computer che crea la connessione. Poiché gli indirizzi IP sono difficili da ricordare, è stato creato il servizio DNS (Domain Name Service).

Il DNS è un database di nomi descrittivi che si suppone siano facili da ricordare, grazie al quale gli utenti non hanno necessità di conoscere l'indirizzo IP del server con il quale desiderano comunicare. È sufficiente immettere il nome appropriato (ad es. www.yahoo.com) e il DNS troverà l'indirizzo IP corrispondente.

Server d'inoltro DNS di WinRoute

WinRoute contiene un modulo DNS che è in grado di inoltrare le richieste DNS a un server DNS scelto su Internet. Il modulo DNS raccoglie i risultati della ricerca nella memoria cache interna, dove rimangono archiviati per un certo periodo di tempo. Le successive richieste di uno stesso indirizzo verranno risolte ricorrendo ai dati memorizzati nella cache, evitando sprechi di tempo dovuti all'attesa della risposta da Internet.

Il server d'inoltro DNS di WinRoute è in grado di rispondere alle richieste DNS sulla base delle informazioni contenute nel file HOSTS, definito dall'utente. Dopo ogni richiesta DNS, WinRoute esegue per prima cosa una ricerca nel file HOSTS. Solo in un secondo momento, se non esistono record corrispondenti, la richiesta verrà inoltrata al server DNS di Internet.

Server proxy

In questa sezione

Informazioni generali sul server proxy

L'**obiettivo principale** di un server proxy è quello di **risparmiare** la **larghezza di banda** della connessione Internet dell'utente. Se l'accesso a Internet avviene tramite un server proxy, sarà possibile **memorizzare** gli oggetti richiesti (pagine HTML, immagini e altri tipi di file) nella sua **cache**.

Se le medesime pagine o immagini verranno richieste nuovamente, dallo stesso o da un altro utente, il server proxy fornirà gli elementi richiesti prelevandoli dalla propria cache. In questo modo **diminuisce** il carico sulla connessione Internet e l'intera operazione diventa molto più semplice e rapida di quanto non sarebbe se fosse necessario scaricare nuovamente le immagini da Internet.

Gli oggetti memorizzati nella cache di un server proxy diventano però obsoleti. È necessario pertanto regolare con cura la durata della vita pacchetto, o **TTL** (Time-To-Live), dei documenti archiviati, per evitare l'insorgere di incomprensioni dovute al fatto, ad esempio, di leggere il notiziario CNN di ieri.

Impostazione rapida

Per prima cosa occorre ricordare che con WinRoute **non è necessario** utilizzare il server proxy per accedere a Internet. La connessione Internet viene mantenuta dal **router NAT,** incluso in WinRoute. NAT è molto più indicato della tecnologia proxy per la condivisione di Internet. WinRoute include tuttavia anche un server proxy per poter offrire funzionalità cache quando la situazione lo richieda.

Per iniziare a utilizzare il server proxy di WinRoute, seguire questi semplici passaggi:

1 In Amministrazione di WinRoute selezionare *Impostazioni -> Impostazioni proxy ->* scheda *Generale*. Selezionare l'opzione "Server proxy abilitato". Mantenere il numero originale di porta 3128.

2 Nel browser di Internet (Explorer, Netscape, Opera...), passare alle impostazioni proxy, scegliere la configurazione manuale e immettere l'indirizzo del PC WinRoute come indirizzo del server proxy per i protocolli HTTP, FTP e Gopher. Immettere 3128 come numero di porta proxy per tutti i protocolli.

3 Controllare la correttezza dell'impostazione accedendo con il browser ad alcune pagine Web.

Scheda Proprietà generali

Server proxy abilitato

Utilizzare questa opzione per attivare o disattivare il server proxy.

Numero porta

Il numero della porta utilizzata per l'ascolto delle richieste dal server proxy. Generalmente non è necessario modificare il numero, che in base all'impostazione predefinita è 3128.

Registra accesso al server proxy

Se questa opzione è selezionata, tutte le richieste di URL avanzate dai browser tramite il server proxy vengono registrate su un registro log.

Controlloaccessi utente

Il server proxy di WinRoute permette all'amministratore di controllare l'accesso alle pagine Web. L'amministratore può decidere di autorizzare l'accesso a determinate pagine o domini solo a utenti e/o gruppi di utenti specifici.

Utilizzo obbligatorio del server proxy

Se si decide di utilizzare il controllo di accesso del server proxy, è necessario bloccare l'accesso diretto alle pagine Web, in modo che l'accesso al server proxy sia l'unica alternativa possibile per connettersi a Internet. Per bloccare l'accesso diretto, definire una regola di filtro pacchetti. Per ulteriori informazioni, fare riferimento alla sezione ***Filtro di pacchetto*** (see "Forzare gli utenti a utilizzare il server proxy" on page 124) della guida utente di WinRoute.

Configurazione del controllo di accesso proxy

Per configurare il controllo di accesso proxy di WinRoute, selezionare la scheda "Accesso" in Impostazioni del server proxy.

Elenco accessi

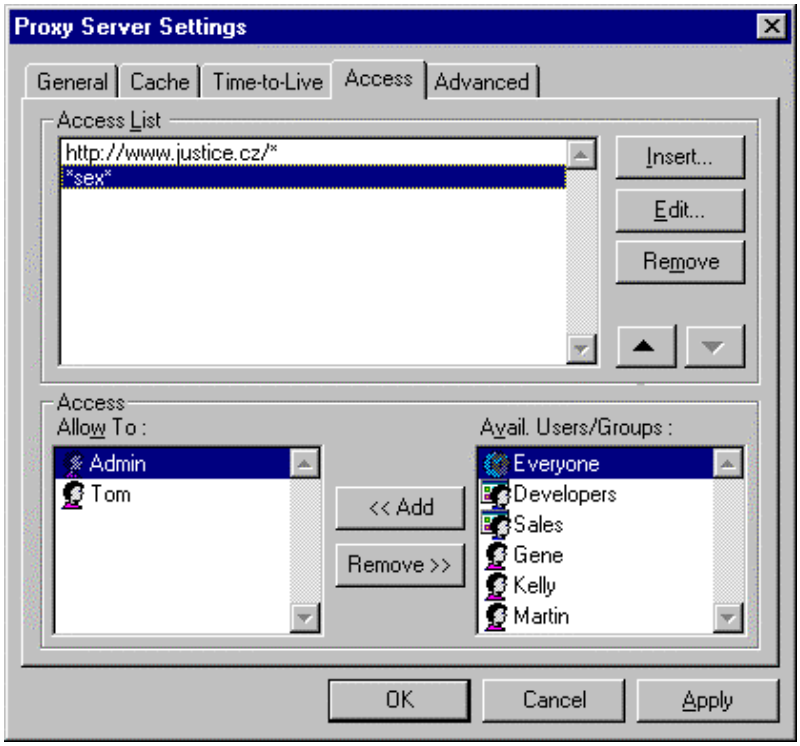
L'elenco degli URL con restrizioni. Il nome degli URL consente l'utilizzo dell'asterisco con funzione di carattere jolly. Per comprendere tutti i computer di nomedominio.com, si potrà utilizzare la stringa "*.nomedominio.com". WinRoute 4.0 si serve anche di sottostringhe per corrispondere agli URL, pertanto la stringa "sex", ad esempio, corrisponderà allo stesso gruppo URL della stringa "*sex*" (solo quest'ultima variante era supportata nelle versioni precedenti di WinRoute)

Consenti a

L'elenco degli utenti e/o dei gruppi utenti a cui è consentito l'accesso a un determinato URL.

Utenti/gruppi disponibili

L'elenco degli utenti e dei gruppi definiti in WinRoute.



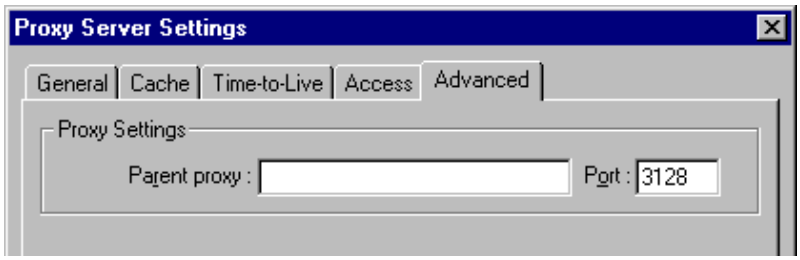
Se la pagina Web cui l'utente cerca di accedere rientra nella categoria delle pagine con restrizioni, il browser richiederà all'utente di specificare l'autorizzazione di accesso. WinRoute controllerà l'esattezza del nome utente e della password e verificherà che l'utente disponga dell'autorizzazione necessaria per accedere alla pagina Web richiesta.

Il browser archivia nella propria memoria il nome utente e la password e può pertanto rispondere automaticamente alle successive richieste di autenticazione, evitando all'utente di immettere ripetutamente il nome utente e la password.

È bene che chiunque utilizzi questa funzione si ricordi di terminare il browser al momento di lasciare il computer. In caso contrario il nome utente e la password rimarrebbero memorizzate e potrebbero essere utilizzate senza l'autorizzazione dell'utente.

Proprietà avanzate

Nella scheda "Avanzate" di Impostazioni del server proxy è possibile configurare WinRoute in modo che venga utilizzato un server proxy superiore.



Talvolta è possibile accedere a un server proxy provvisto di una **memoria cache di considerevoli dimensioni** di una **connessione veloce** a Internet, e anche la connessione utilizzata per quel server è abbastanza rapida, grazie all'utilizzo di collegamenti supplementari oltre a quello utilizzato per Internet.

Per migliorare la velocità di trasmissione dei dati, è possibile decidere che il server proxy di WinRoute inoltri tutte le richieste al server proxy superiore. Per ottenere questo risultato, è sufficiente immettere il nome del **server proxy superiore** e il numero di porta negli appositi campi della scheda "**Avanzate**".

Informazioni sulla cache

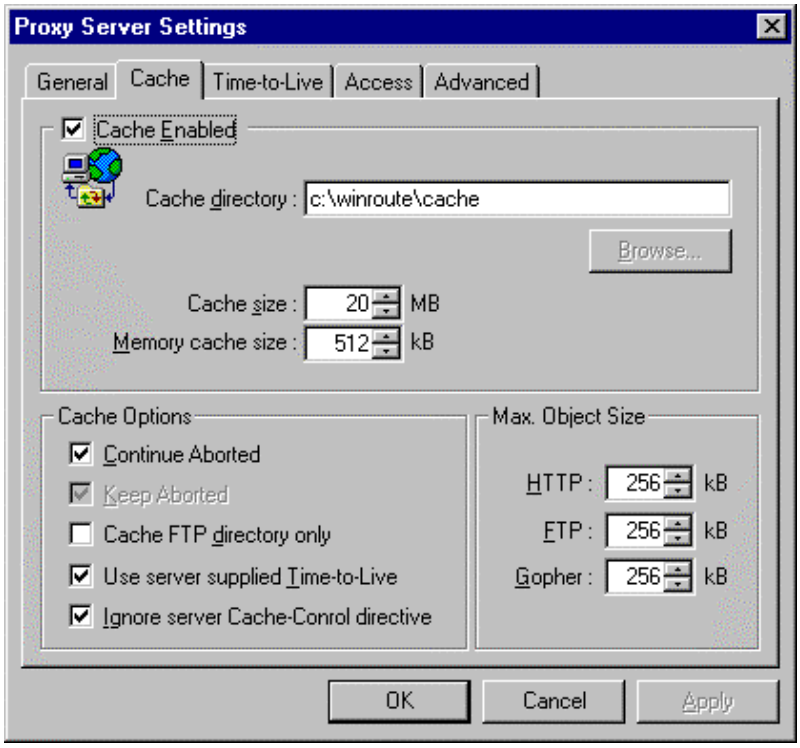
Il server proxy di WinRoute utilizza un metodo **molto razionale** di archiviazione dei dati, in base al quale gli oggetti memorizzati nella cache vengono conservati in un **unico file di dimensioni predefinite**, laddove un server proxy tradizionale genererebbe un file per ogni oggetto.

Se il disco utilizza **unità di allocazione di grandi dimensioni** (ad es. FAT 16), si verifica uno **spreco significativo** di memoria, perché spesso i componenti delle pagine Web hanno dimensioni ridotte e occupano quindi poco spazio. Generalmente il 50% degli oggetti occupa meno di 6 kilobyte, mentre la dimensione delle unità di allocazione di un disco fisso di grandi dimensioni è di 32 KB (con un file system FAT).

Il fatto che la cache di WinRoute sia capace di memorizzare i dati in un unico file permette di risparmiare fino a 10 volte lo spazio richiesto dall'approccio standard, con evidenti benefici in termini di efficienza e di ottimizzazione del disco fisso.

Il file con dimensioni predefinite permette inoltre a WinRoute di utilizzare sofisticate tecniche di indicizzazione, che garantiscono un utilizzo molto veloce della cache.

Impostazioni della cache



Cache abilitata

Abilita e disabilita la memoria cache. Se l'opzione è deselezionata, le pagine Web saranno sempre recuperate da Internet.

Directory cache

La directory in cui verrà memorizzato il contenuto della cache.

Dimensione cache

La quantità di spazio su disco a disposizione della cache del server proxy. Prima di decidere la quantità di memoria da destinare alla cache, è necessario considerare il numero di utenti, il traffico previsto, e così via. Se lo spazio a disposizione lo consente, si potrà specificare una dimensione maggiore di cache. La dimensione massima è di 3072 megabyte (3 GB).

Continuaanche se annullata

Se l'opzione è selezionata, il server proxy completerà sempre lo scaricamento degli oggetti da Internet, anche nel caso in cui il browser dell'utente avesse interrotto la richiesta (perché l'utente ha scelto il pulsante Termina, o si è spostato su una nuova pagina senza attendere il completamento dello scaricamento della pagina precedente). Le successive visite alla stessa pagina saranno molto più veloci.

Mantieni anche se annullata

Questa opzione istruisce il server proxy di WinRoute a memorizzare nella cache anche gli oggetti incompleti (pagine Web, immagini). In questo modo si velocizza il processo di visualizzazione delle pagine già visitate. Se l'opzione "Continua anche se annullata" è selezionata, verrà ignorata l'opzione "Mantieni anche se annullata".

Solo directory cache FTP

Durante l'esplorazione dei server FTP, utilizzando questa opzione è possibile memorizzare nella cache solo gli elenchi delle directory. Se si desidera memorizzare anche i file scaricati dai server FTP, deselezionare l'opzione. La decisione di memorizzare nella cache un determinato file dipende inoltre dalla sua dimensione. Fare riferimento a "Dimensione max. oggetto" qui sotto.

Usa vita pacchetto fornita dal server

Per vita del pacchetto si intende il periodo di tempo trascorso il quale una pagina Web verrà considerata obsoleta e il suo contenuto dovrà essere nuovamente recuperato dal server. Questa opzione istruisce il server proxy di WinRoute a rispettare la vita pacchetto (TTL) ricevuta con le singole pagine. Se le pagine sono prive di TTL, verrà utilizzata la TTL predefinita del server.

Ignora istruzione di controllo cache del server

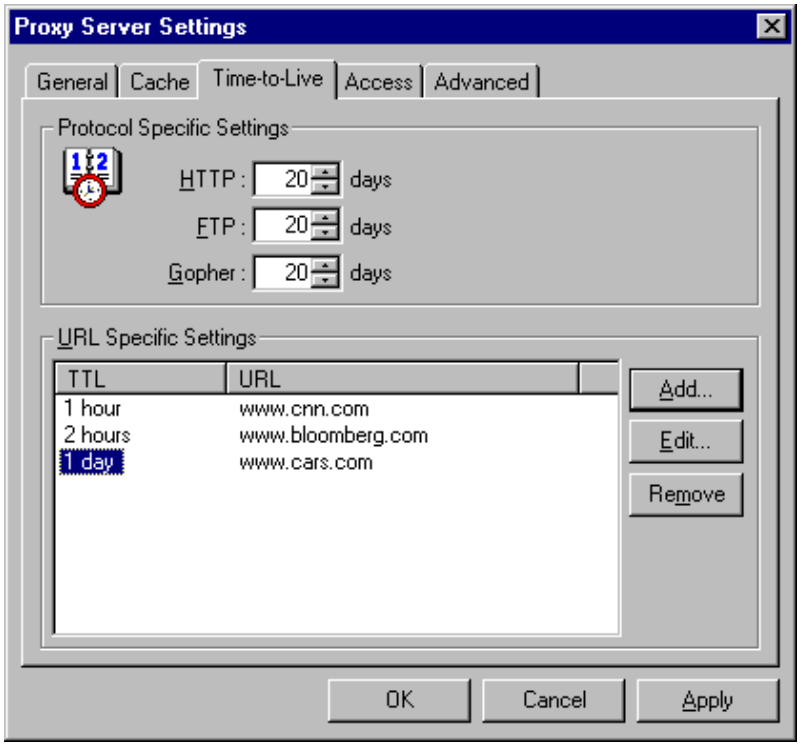
Se il contenuto di una pagina Web è soggetto a continui cambiamenti, l'autore della pagina potrebbe decidere di impostare l'istruzione "nessuna cache". Sebbene si tratti di una funzionalità molto utile, alcuni server Web ne fanno un uso estremo, a volte anche per tutte le pagine, annullando di fatto i vantaggi derivanti dall'utilizzo di un server proxy. Per proteggersi da un simile comportamento, selezionare questa opzione.

Dimensione max. oggetto

La dimensione massima degli oggetti memorizzati nella cache. Gli oggetti di dimensioni maggiori di quelle specificate verranno passati al browser dell'utente, ma non saranno registrati nella memoria cache. Generalmente non è necessario memorizzare gli oggetti di grandi dimensioni (come i file archivio di un programma), perché non vengono scaricati di frequente.

Vita pacchetto

È possibile definire il valore della vita pacchetto (TTL) utilizzata dalle pagine Web prive di una propria TTL definita, oppure decidere di ignorare tutti i valori TTL forniti dal server (vedere l'opzione "Usa vita pacchetto fornita dal server" nella scheda Cache).



Impostazioni specifiche protocollo

Le caselle di questo riquadro permettono di impostare la durata in giorni della vita pacchetto per i protocolli HTTP, FTP e Gopher.

Impostazioni specifiche URL

Se si desidera impostare individualmente la vita pacchetto per specifici domini, server Web o pagine singole, immettere qui i valori dei singoli URL. Il valore TTL può essere espresso in giorni e/o ore.

Il nome degli URL consente l'utilizzo dell'asterisco con funzione di carattere jolly. WinRoute 4.0 si serve anche di sottostringhe per corrispondere agli URL. Immettendo, ad esempio "ftp", sarà possibile trovare tutti gli URL che contengono la parola "ftp" nel proprio nome. Nelle versioni precedenti di WinRoute, per ottenere lo stesso risultato era necessario immettere "*ftp*").

Se l'opzione "Usa vita pacchetto fornita dal server" della scheda Cache è selezionata, la TTL fornita dal server avrà una priorità di esecuzione superiore a quella dell'opzione "Impostazioni specifiche URL".

Impostazioni per l'utilizzo obbligatorio del server proxy al posto di NAT

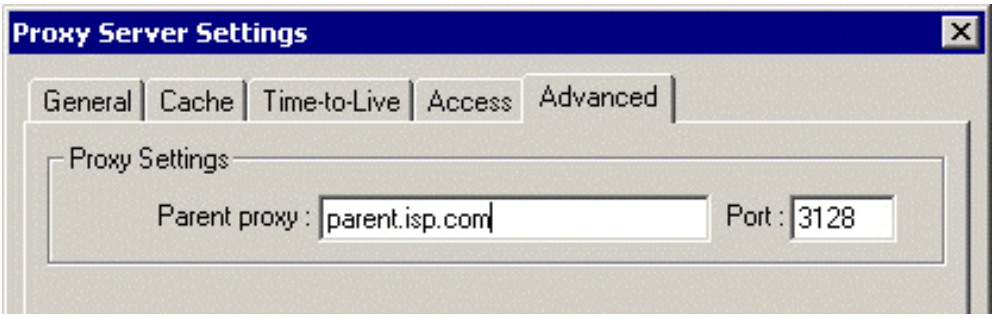
Anche se **NAT** è un eccellente protocollo di connessione a Internet, a volte potrebbe essere preferibile obbligare gli utenti a utilizzare il **server proxy** per accedere al **Web,** come nel caso in cui si disponga di un'unica connessione tramite modem a 56 K per l'intera azienda. Il server proxy permette di utilizzare la funzione cache o di impostare **filtri URL** per controllare gli **accessi utente**

Per accedere a Internet tramite il server proxy è necessario predisporre tutti i browser in modo specifico. L'impostazione predefinita della porta del server proxy di WinRoute è **3128,** ma può essere modificata. Gli utenti possono ignorare il server proxy e accedere direttamente a Internet tramite il protocollo NAT. Per evitare che ciò avvenga, sarà necessario impostare un firewall. Fare riferimento all'esempio ***Impostazioni del firewall*** (see "Forzare gli utenti a utilizzare il server proxy" on page 124).

Utilizzo di un server proxy superiore

Server proxy superiore

In alcuni casi, il server proxy di WinRoute deve potersi collegare a un server proxy di "livello superiore", chiamato appunto **server proxy superiore**. Scegliere *Impostazioni / Server proxy*, selezionare la scheda *Avanzate* e immettere l'indirizzo IP del server proxy superiore e la porta.



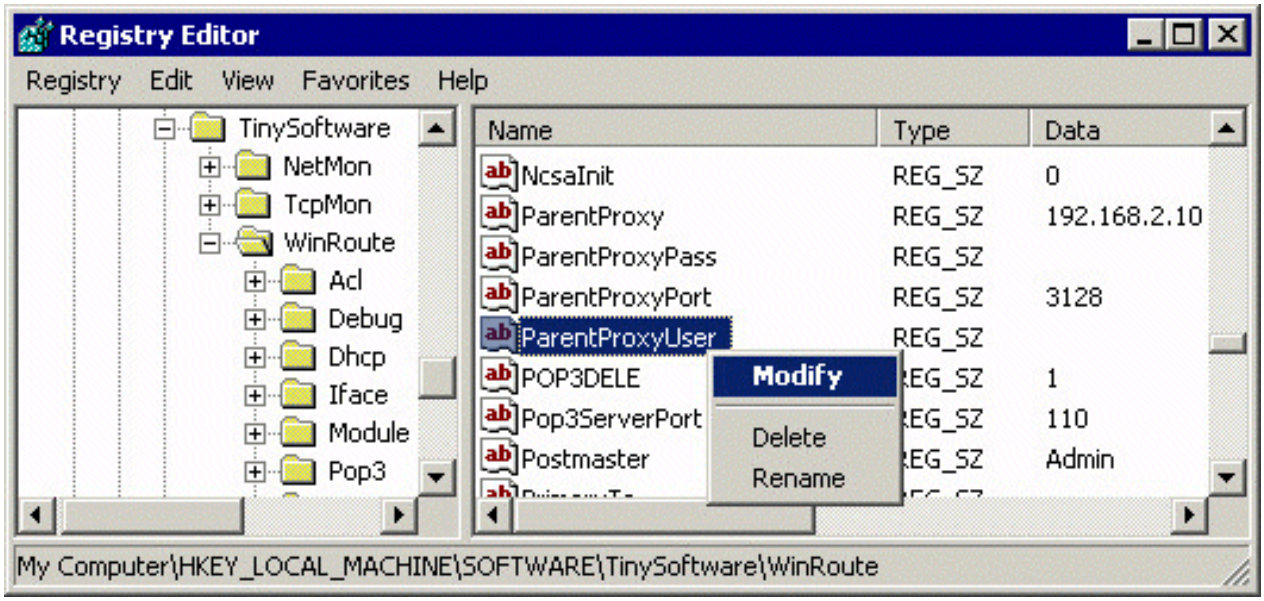
Nome utente e password del server proxy superiore

Il server proxy superiore può richiedere l'autenticazione dell'utente per consentire l'accesso ad alcuni (o a tutti) i siti Web, seguendo una procedura analoga a quella messa in atto da WinRoute (per ulteriori informazioni, vedere il capitolo *Controllo accessi proxy*). WinRoute Pro 4.1 include la funzione di autenticazione a partire dalla build 22.

Per impostare l'autenticazione:

- Arrestare il modulo di gestione di WinRoute (da Servizi di Windows o utilizzando il programma Monitor di stato di WinRoute)
- Avviare l'editor del registro di sistema di Windows (regedit.exe)
- Trovare la chiave *HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute*
- Nel campo a destra, trovare le voci **ParentProxyUser** e **ParentProxyPass** e modificarne il contenuto digitando il nome utente e la password corretti.
- Chiudere l'editor di registro e avviare WinRoute Engine.

Terminata la procedura, il server proxy di WinRoute sarà in grado di auto-autenticarsi per il server proxy superiore.



Server di posta elettronica

In questa sezione

Informazioni sul server di posta elettronica di WR

WinRoute include un server completo di posta elettronica SMTP/POP3, che può essere utilizzato al posto di quello del provider Internet per inviare messaggi su Internet e agli utenti della LAN, o per ricevere la posta elettronica e conservarla nelle cassette postali degli utenti di WinRoute. Il server dispone inoltre uno strumento di pianificazione che permette di programmare gli scambi di posta elettronica.

Se non si utilizza il server di posta elettronica

L'utilizzo del server di posta elettronica di WinRoute non è obbligatorio. È sempre possibile continuare a utilizzare il server del proprio provider Internet o qualunque altro server di posta elettronica, nel quale caso WinRoute funzionerà da router/firewall, per consentire al software client di comunicare con il server di posta elettronica del provider Internet.

✍✍ ***Nota! non impostare il software client di posta elettronica all'utilizzo del proxy! L'accesso a Internet deve obbligatoriamente avvenire tramite il NAT di WinRoute, mentre il software client deve poter accedere direttamente a Internet. L'eventuale impossibilità di stabilire un corretto scambio di posta elettronica significherà che NAT non è stato configurato propriamente. Per la configurazione corretta, vedere il successivo*** Elenco di controllo .

Utenti e gruppi

In questa sezione

Informazioni su utenti e gruppi

WinRoute- utenti e gruppi

WinRoute può essere programmato con utenti individuali, che possono essere raccolti in gruppi (scegliere Impostazioni | Utenti e gruppi… | scheda Utenti). Gli utenti di Windows NT/2000 possono essere importati per mezzo della scheda Avanzate, nel menu Impostazioni | Utenti e gruppi…

Definizione di utente

In qualità di utente di WinRoute è possibile prendere parte all'amministrazione di WinRoute, avere una propria cassetta postale ed essere incluso nelle politiche di accesso ristretto del server proxy di WinRoute.

Gli utenti possono creare gruppi e applicarvi privilegi o restrizioni di accesso.

Aggiunta di un utente

Per aggiungere un utente:

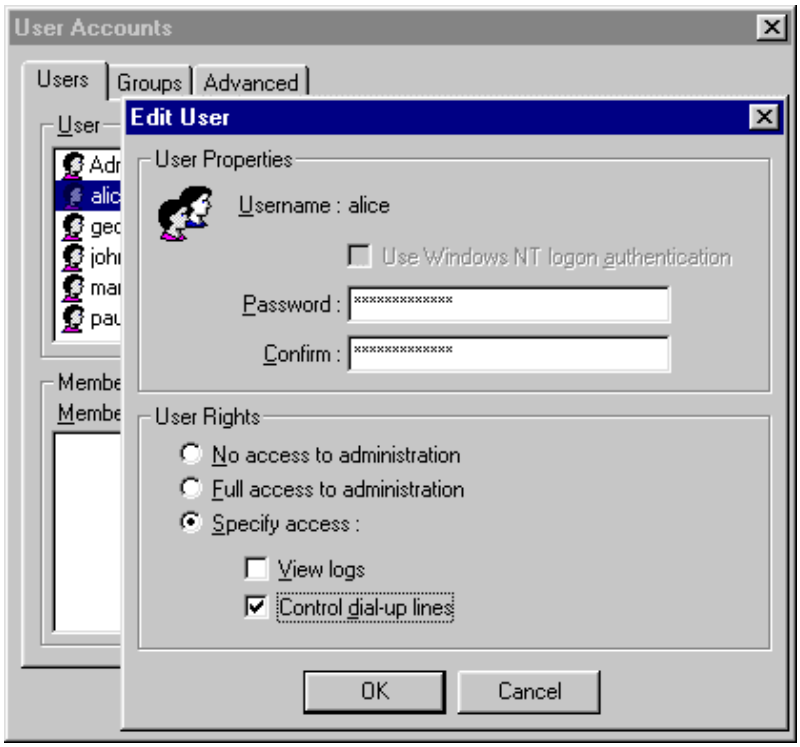
1. Selezionare il menu **Impostazioni>Utenti e gruppi**
2. Scegliere **Aggiungi**
3. Definire il **nome utente** e la **password**
4. Assegnare i **diritti** all'utente:

   L'utente non ha diritto di amministrare WinRoute.

   L'utente ha accesso completo all'amministrazione

   ✍ **Visualizza registri**: l'utente ha diritto di accedere all'amministrazione di WinRoute e vedere solo le finestre dei registri (informazioni di debug, registro del server proxy, registro di posta elettronica, ecc.), ma non è autorizzato a modificare le altre impostazioni.

✍ **Controlla le linee di accesso remoto:** l'utente ha diritto di accedere all'amministrazione e stabilire o disconnettere le connessioni a Internet, ma non è autorizzato a modificare le altre impostazioni.



Gruppi di utenti

WinRoute permette di raggruppare gli utenti in diversi gruppi. Un utente può essere contemporaneamente membro di più gruppi.

È possibile assegnare **diritti** al gruppo.

✍✍ ***Nota: i diritti assegnati al gruppo si sovrappongono a quelli assegnati all'utente.***

I membri di un gruppo possono avere i seguenti **diritti**:

L'utente non ha diritto di amministrare WinRoute.

L'utente ha accesso completo all'amministrazione.

- **Visualizza registri** l'utente ha diritto di accedere all'amministrazione di WinRoute e a vedere solo le finestre dei registri (informazioni di debug, registro del server proxy, registro di posta elettronica, ecc.), ma non è autorizzato a modificare le altre impostazioni.
- **Controlla le linee di accesso remoto** l'utente ha diritto di accedere all'amministrazione e a stabilire o disconnettere le connessioni a Internet, ma non è autorizzato a modificare le altre impostazioni.

Amministrazione remota

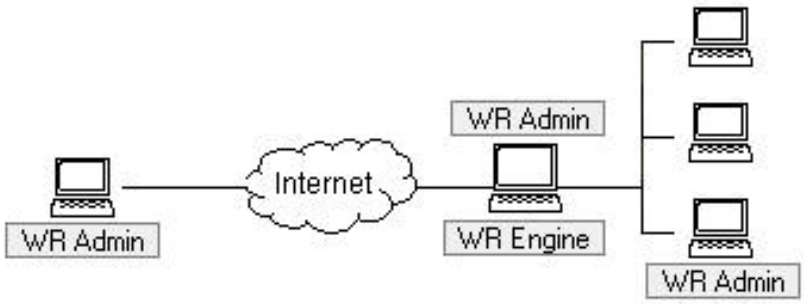
WinRoute Pro consente di eseguire l'amministrazione remota del sistema. Dopo avere impostato correttamente i parametri e i diritti, sarà possibile gestire il firewall da qualunque postazione, anche dall'altra parte del mondo. L'accesso al modulo di gestione è garantito da un complesso sistema di crittografia e dalla password.

Componenti di WinRoute Pro

WinRoute Pro 4.x si compone di tre moduli:

Gestione di WinRoute esegue tutte le operazioni di analisi e di routing (NAT, filtro pacchetti, mappatura porta, ecc.). È possibile avviare/interrompere il modulo di gestione di WinRoute da Monitor di stato di WinRoute o, se si utilizza Windows NT, direttamente dall'opzione Servizi di NT. Gestione di WinRoute viene eseguito, in maniera assolutamente trasparente, come servizio con i sistemi operativi Windows 2000/NT/98 o 95.

Monitordi stato di WinRoute è l'applicazione di controllo che segnala quando il modulo di gestione di WinRoute è in esecuzione, grazie a una piccola icona blu visualizzata nell'angolo inferiore destro del desktop.



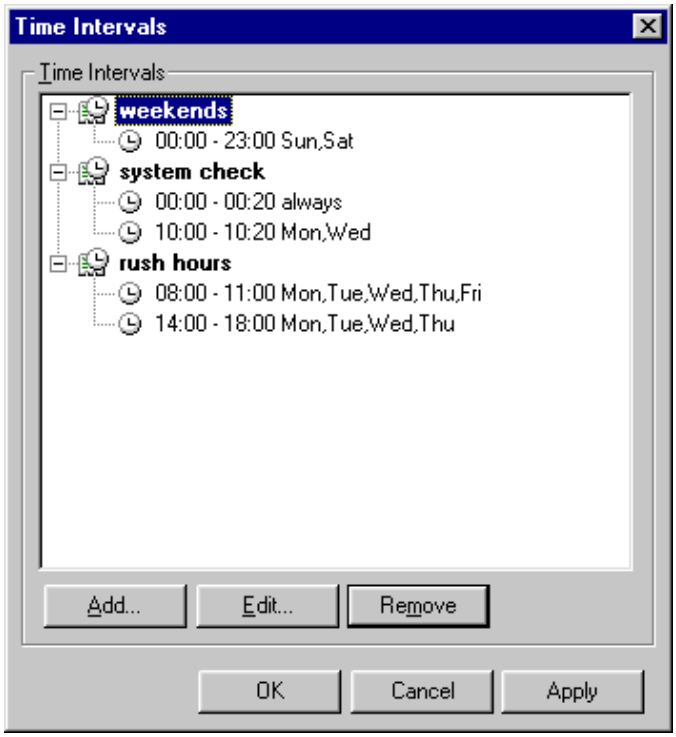
Amministrazione di WinRoute fornisce la configurazione e le impostazioni per il modulo di gestione di WinRoute. Amministrazione di WinRoute è un'applicazione separata, (wradmin.exe) che può essere eseguita da qualunque computer e collegata al computer del modulo di gestione di WinRoute tramite una connessione TCP/IP. Per conoscere le impostazioni necessarie a eseguire la connessione remota, fare riferimento agli altri capitoli di questa sezione.

Intervalli di tempo

È possibile definire delle fasce orarie – intervalli di tempo predefiniti – in cui eseguire determinate azioni. Tali azioni possono essere:

- Filtro di pacchetto
- Scambio di posta elettronica (invio e ricezione)
- Connessione a Internet
- Impostazioni NAT avanzate

La fascia oraria si compone di più intervalli di tempo, non necessariamente contigui.



✍✍ ***Esempio: è possibile creare una fascia oraria denominata "Festivi e pomeriggi" che coprirà i giorni di sabato, domenica e lunedì dalle ore 16.00 alle ore 18.00, e giovedì dalle 17.00 alle 19.00***

Per definire una fascia oraria:

1 Scegliere il menu *Impostazioni=>Avanzate=>Intervalli di tempo.*

2 Denominare la fascia oraria.

3 Aggiungere un nuovo intervallo di tempo.

CAPITOLO 2

INSTALLAZIONE ED ESECUZIONE

In questo capitolo

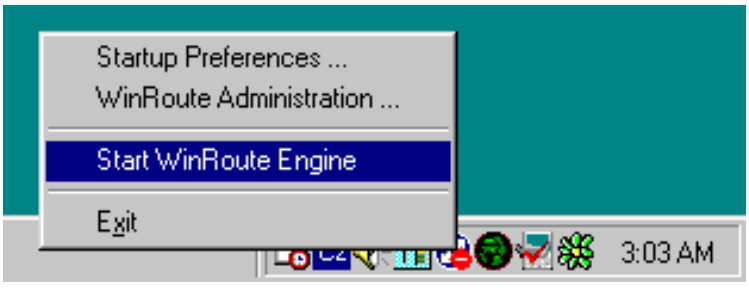
Amministrazione in WinRoute

In questa sezione

Amministrazione tramite rete locale

Per amministrare WinRoute dalla rete locale o da un computer su cui sia stato installato WinRoute, è necessario procedere come di seguito indicato:

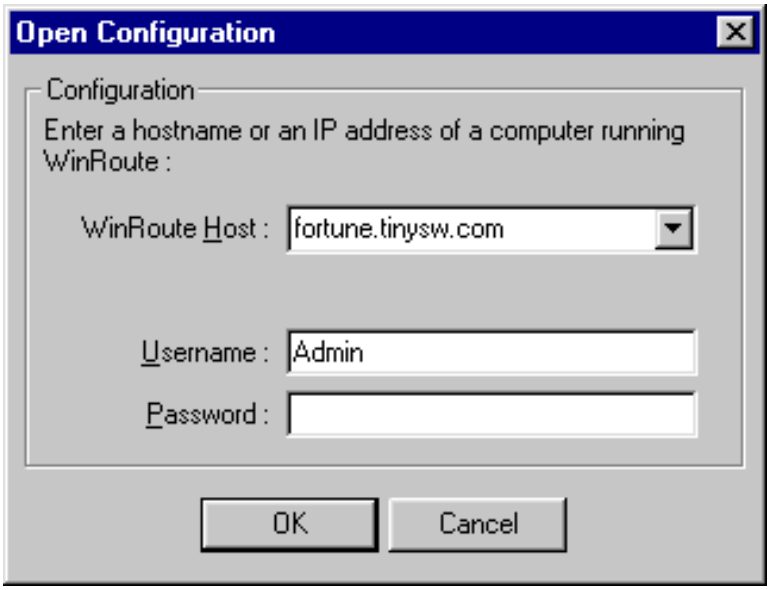
1. **Verificare che il modulo di gestione di WinRoute sia in esecuzione**
   Per controllare se WinRoute sia stato avviato, eseguire Monitor di stato di WinRoute dal gruppo di programmi WinRoute 4.0. Sulla barra delle applicazioni verrà visualizzata una piccola icona blu e bianca di forma circolare (angolo inferiore destro del desktop). L'icona indica che l'applicazione è in esecuzione. Se l'icona è sbarrata da una croce rossa, significa che WinRoute è stato arrestato. Per avviare il modulo di gestione di WinRoute è sufficiente fare **clic con il pulsante destro del mouse** sull'icona e scegliere modulo di gestione di WinRoute dal menu popup.



2. Avviare Amministrazione di WinRoute

Per avviare il modulo Amministrazione di WinRoute, scegliere Avvio=>Programmi=>WinRoute 4.0 o fare clic con il pulsante destro del mouse sull'icona del Monitor di stato di WinRoute e scegliere *Amministrazione di WinRoute* dal menu popup. È inoltre possibile copiare ed eseguire il file *WRAdmin.exe* su qualunque computer della rete.

Dopo la visualizzazione della finestra popup Admin, è possibile lasciare l'host locale preimpostato o immettere l'indirizzo IP del computer su cui è in esecuzione WinRoute. Immettere il nome utente e la password utilizzata per l'amministrazione.



Nota: se ci si connette per la prima volta, è possibile utilizzare "Admin" come nome utente e lasciare vuoto lo spazio per la password. Per ulteriori dettagli sulla politica relativa al nome utente e alla password di amministrazione, vedere Configurazione utente.

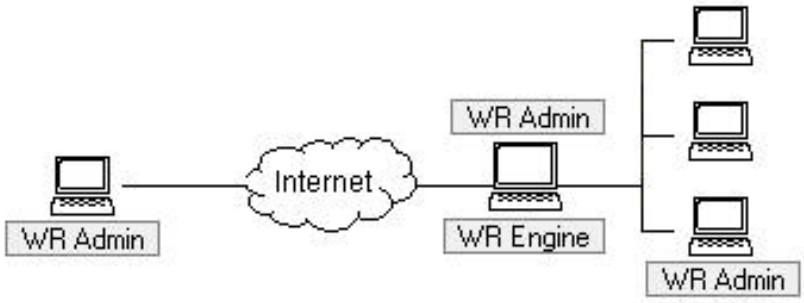
Per eseguire le impostazioni è necessario accedere al modulo gestione di WinRoute come amministratore.

Di seguito sono elencati le possibili cause di accesso errato da una rete locale:

- Il modulo di gestione di WinRoute non è in esecuzione
- Nome utente o password errati
- Indirizzo IP errato immesso al momento dell'accesso a WinRoute Engine
- Non si dispone dell'autorizzazione necessaria per amministrare WinRoute
- Protocollo NAT abilitato sull'interfaccia di collegamento alla rete – vedere i capitoli sull'elenco di controllo e sulle impostazioni della rete della Guida

Amministrazione tramite Internet

È possibile amministrare il modulo di gestione di WinRoute Pro da un qualunque computer nel mondo, a condizione che si disponga di una connessione TCP/IP attiva. L'amministrazione è protetta (crittografata) e controllata tramite nome utente e password.



Per poter amministrare il computer WinRoute dall'esterno di una LAN (da Internet) occorre mappare correttamente la porta sul computer WinRoute. Quando il protocollo NAT è abilitato sull'interfaccia di collegamento a Internet (impostazione necessaria per la condivisione di Internet), l'intera rete, incluso il computer WinRoute, è completamente protetta e nessuno può accedervi.

Per mappare la porta per l'amministrazione remota, selezionare *Impostazioni=>Avanzate=>Mappatura porte*, scegliere Aggiungi e impostare:

Protocollo: TCP/UDP

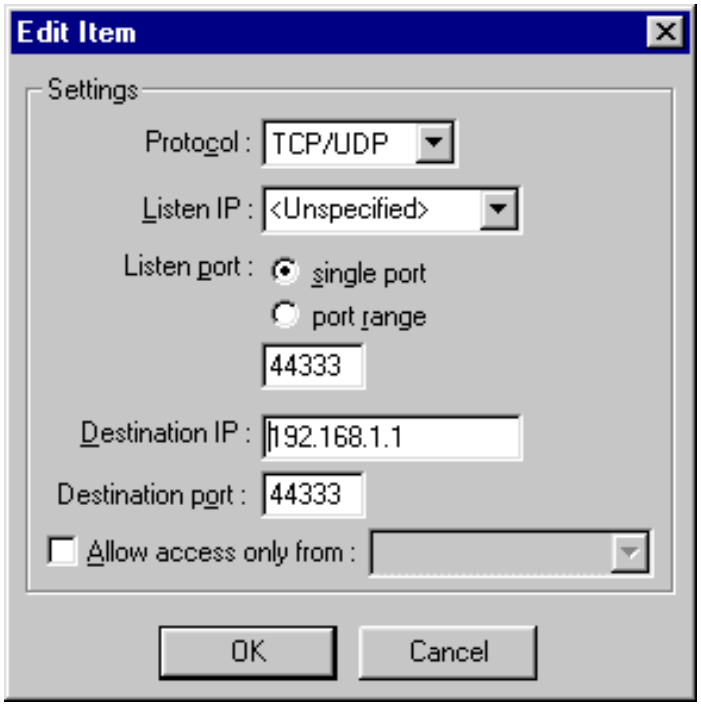
IP in ascolto: <Non specificato> (raccomandato) o l'indirizzo IP dell'interfaccia.

Porta in ascolto: 4333

IP di destinazione: l'indirizzo IP dell'interfaccia che collega il computer WinRoute alla rete locale (indirizzo IP di classe privata)

Porta di destinazione: 4333

Consenti accesso solo da: selezionando questa opzione è possibile limitare ulteriormente l'accesso al modulo di gestione di WinRoute. È necessario però aver definito in precedenza gli indirizzi IP a cui WinRoute potrà accedere da Internet, tramite il menu *Impostazioni=>Avanzate=>Gruppi di indirizzi*. Si possono raggruppare indirizzi IP separati, intervalli di indirizzi IP e reti.



Per ulteriori informazioni sulla mappatura della porta, fare riferimento agli esempi. Se tutte le impostazioni sono selezionate correttamente, sarà possibile eseguire Amministrazione di WinRoute da qualunque computer e immettere l'indirizzo IP registrato (ad es. 206.86.181.25) del computer su cui viene seguito WinRoute, nonché il nome utente e la password utilizzati per l'amministrazione. Per ulteriori dettagli sulla politica relativa al nome utente e alla password di amministrazione, vedere Configurazione utente.

Possibili cause di accesso errato da Internet:

- Il modulo di gestione di WinRoute non è in esecuzione
- Nome utente e password errati
- Indirizzo IP errato immesso al momento dell'accesso al modulo di gestione di WinRoute
- Non si dispone dell'autorizzazione necessaria per amministrare WinRoute

- La mappatura della porta del computer su cui è in esecuzione il modulo di gestione di WinRoute è assente o errata

Perdita della password di amministrazione

In caso di perdita della password di amministrazione, inviare un messaggio di posta elettronica a support@tinysoftware.com per ricevere istruzioni sul da farsi. Per motivi di sicurezza, la soluzione non viene pubblicata su queste pagine.

Requisiti di sistema

I requisiti minimi per installare ed eseguire WinRoute Pro 4.1 sono i seguenti:

- PC Pentium (con processore singolo o doppio)
- Windows 95/98/NT4.0/2000
- 32 MB di memoria
- 1 MB di spazio libero su disco
- Almeno due interfacce libere, che potranno essere: Ethernet, RAS, TokenRing o DirecPC

Elenco di controllo rapido

L'elenco delle impostazioni e delle regole di base permette a tutti gli utenti di WinRoute di collegare in modo corretto una rete locale a Internet, a condizione che esista un presupposto imprescindibile, ovvero una connessione a Internet funzionante.

Le impostazioni di seguito descritte consentono di utilizzare al meglio NAT per la condivisione di un accesso Internet. Se si desidera utilizzare un server proxy (integrato in WinRoute), le impostazioni non andranno eseguite. Sarà infatti necessario indirizzare i browser e le applicazioni al server proxy di WinRoute. Ove possibile, è sempre preferibile utilizzare NAT (Network Address Translation) perché è più rapido, sicuro e affidabile.

Impostazioni e regole

1 **PC WinRoute - due interfacce (NIC)**
Controllare che il computer WinRoute abbia almeno due interfacce, una per la connessione a Internet e una per la connessione locale/client. Le interfacce possono essere schede di rete o linee RAS. Una delle interfacce (Ethernet o RAS/Accesso remoto) viene utilizzata per la connessione a Internet, mentre le altre interfacce (Ethernet, token ring…) servono per la connessione alla rete dell'utente.

2 **Accertarsi che tutti gli indirizzi IP consentano di eseguire il ping!**
Affinché WinRoute possa funzionare correttamente, i computer client devono essere in grado di eseguire il ping sugli indirizzi IP pubblici e privati del PC host WinRoute.

3 **PC WinRoute - abilitare NAT sull'interfaccia Internet!**
Accertarsi che sia stata selezionata l'opzione NAT per l'interfaccia di connessione a Internet (Ethernet, linea RAS). Per selezionare l'opzione, selezionare **Impostazioni=>Tabella interfaccia** e scegliere le proprietà dell'interfaccia desiderata.

4 PC WinRoute - disabilitare NAT sull'interfaccia interna!

Accertarsi che NAT **NON SIA SELEZIONATO** sulle interfacce di connessione alla rete interna.

Nota! In alcune particolari impostazioni, NAT può essere selezionata anche sull'interfaccia interna, come dimostra l'esempio (quando disponibile).

5 PC WinRoute - deselezionare i gateway sull'interfaccia interna!

Accertarsi che non siano stati impostati gateway predefiniti nelle proprietà dell'interfaccia (scheda di rete) che collega alla rete interna. Impostare il gateway predefinito sull'interfaccia che collega a Internet in base ai dettagli forniti dal provider Internet.

6 PC WinRoute - immettere le opzioni per la configurazione DHCP!

Nella maggior parte dei casi la configurazione automatica della rete verrà eseguita dal server DHCP di WinRoute. Ricontrollare che siano stati definiti gli ambiti degli indirizzi IP che il server DHCP dovrà assegnare e le opzioni. In Opzioni è possibile specificare altre informazioni relative alle workstation, quali il server DNS, il gateway predefinito, ecc.

7 PC client - l'indirizzo IP interno del PC WinRoute è il gateway predefinito!

Il PC WinRoute funge da GATEWAY PREDEFINITO per tutti i computer della LAN. È necessario pertanto utilizzare l'indirizzo IP della scheda d'interfaccia di rete interna sull'host WinRoute (ad es. 192.168.1.1) come gateway per tutti i computer interni/client. Impostare il valore di ciascun computer "client" O impostare una sola volta il valore sul server DHCP di WinRoute, che provvederà ad assegnarlo automaticamente alle workstation! Se si desidera utilizzare un differente gateway predefinito, fare riferimento agli esempi di internetworking avanzato!

8 PC client - controllare il server DNS!

Nella maggior parte dei casi verrà utilizzato il server d'inoltro DNS integrato in WinRoute per tutti i computer della rete. Accertarsi quindi che sia stato selezionato e configurato. È possibile utilizzare l'indirizzo del server DNS del proprio provider Internet, immettendolo direttamente negli appositi campi di configurazione TCP/IP relativi a ogni computer della rete.

✍✍ ***Se WinRoute viene utilizzato esclusivamente come firewall o server di posta elettronica, e non per richieste di condivisione Internet, NON è necessario abilitare il protocollo NAT su alcuna interfaccia.***

✍✍ ***Le interfacce sul computer WinRoute devono avere indirizzi IP diversi per le diverse reti. Non è possibile assegnare indirizzi IP ottenuti dalla stessa rete (e cioè non è possibile, ad esempio, che un indirizzo sia 207.181.216.23 e l'altro 207.181.216.24). Se si hanno due sole interfacce, come nella maggior parte dei casi, una sarà destinata alla rete locale (LAN) e l'altra a Internet. Se le interfacce fossero tre (due locali e una Internet), gli indirizzi IP assegnati alle interfacce locali dovranno provenire da reti diverse (ad es. 192.168.1.1 e 192.168.2.1).***

Prodotti software in conflitto

Di seguito sono elencati i problemi noti di incompatibiltà software:

Norton Antivirus

Per eseguire il server di posta elettronica di WinRoute è necessario disabilitare la porta 110 nella configurazione di Norton Antivirus. In caso contrario non sarà possibile avviare il computer.

WinGate

Disinstallare WinGate prima dell'installazione. Disinstallare sia il software per il server sia quello per il client.

SyGate

Disinstallare SyGate prima dell'installazione. Disinstallare sia il software per il server sia quello per il client.

Server proxy MS

Disinstallare il server proxy MS prima dell'installazione. Disinstallare sia il software per il server sia quello per il client. Rimuovere TCP/IP, riavviare il computer e reinstallare TCP/IP.

Condivisione di connessione Internet di Microsoft

Disinstallare MS ICS prima dell'installazione, rimuovere TCP/IP, riavviare il computer e reinstallare TCP/IP.

WinProxy di Ositis

Disinstallare WinProxy prima dell'installazione, rimuovere TCP/IP, riavviare il computer e reinstallare TCP/IP.

Tutti i software qui menzionati utilizzano driver che lavorano in modo non corretto con le porzioni inferiori del protocollo di rete controllato da WinRoute.

Problemicon la tabella di routing

Potrebbero accadere che, nonostante i componenti siano stati installati e configurati correttamente, si verifichino casi di funzionamento errato. Sfortunatamente i sistemi operativi Windows 95/98/NT non sono stati progettati specificatamente per le reti. Anche dopo la corretta impostazione di WinRoute e della rete è possibile che insorgano problemi di funzionalità. In questo caso occorrerà controllare la tabella di routing e scegliere una delle seguenti possibilità:

✍ cancellare le route e inserirle nuovamente - solo per utenti esperti;

o

✍ rimuovere completamente il protocollo TCP/IP, riavviare il computer e aggiungere nuovamente il protocollo. La risoluzione del problema è garantita.

Problemi con il software proxy client

Alcuni server proxy richiedono che il software sia installato su tutti i computer client. Il software client fa sì che tutte le applicazioni interroghino il server proxy. Se il software proxy client non è stato rimosso, il computer potrebbe non connettersi a Internet perché WinRoute non è stato impostato come server proxy. Se nonostante l'intervento correttivo il client non riuscisse a connettersi a Internet, reinstallare TCP/IP, reimpostarlo e riavviare il computer.

Problemi con i driver delle schede di rete

È sempre consigliabile utilizzare schede di interfaccia di rete standard. Se la scheda è di un modello particolare, di vecchia manifattura o molto recente, potrebbe darsi che il relativo driver comprenda istruzioni specifiche che impediscono la comunicazione con WinRoute. Una soluzione possibile è scambiare la posizione della scheda in questione con quella di una scheda Ethernet standard installata sulla stessa rete. Spesso è sufficiente questo piccolo stratagemma, o l'aggiornamento del driver, per risolvere problemi di incompatibilità.

WinRoute è un software router/firewall assolutamente neutro, che non richiede l'esecuzione di software sui computer client , a meno che non sia utilizzato per l'amministrazione remota. In questo caso sul PC esterno, o client, dovrà essere installato il programma di Amministrazione di WinRoute "wradmin.exe".

Impostazione della rete (DHCP)

In questa sezione

Informazioni su DHCP

Il server DHCP semplifica notevolmente la configurazione delle workstation della LAN. Se si utilizza un server DHCP, la sola impostazione richiesta sulle workstation è quella che permette di ottenere gli indirizzi IP in maniera dinamica dal server DHCP (questa impostazione viene eseguita automaticamente come predefinita quando si aggiunge il protocollo TCP/IP nelle proprietà della rete).

✍✍ ***È possibile usare il server DHCP integrato WinRoute o qualunque altro server DHCP della rete. Accertarsi che venga eseguito un solo server DHCP per volta!***

Informazioni generali sul gateway predefinito

Poiché WinRoute funziona come un router, necessita di due impostazioni TCP/IP di base su ciascun computer della rete:

✍ Assegnazione dell'indirizzo IP, manualmente o tramite il server DHCP (ad es. il server DHCP di WinRoute)

✍ Impostazione del gateway predefinito

Il gateway predefinito dei computer che accedono a Internet tramite WinRoute deve essere impostato sull'**indirizzo IP** dell'interfaccia Ethernet del computer WinRoute utilizzato per il collegamento alla LAN.

Esempio:

si supponga che l'indirizzo IP del computer client sia 10.10.10.23 e che il PC WinRoute abbia due interfacce, una per il collegamento al modem via cavo, che ottiene l'indirizzo IP dal provider Internet (ad es. 203.23.14.232) e l'altra per il collegamento alla rete privata (10.10.10.1). L'impostazione del gateway predefinito sul computer 10.10.10.23 sarà 10.10.10.1.

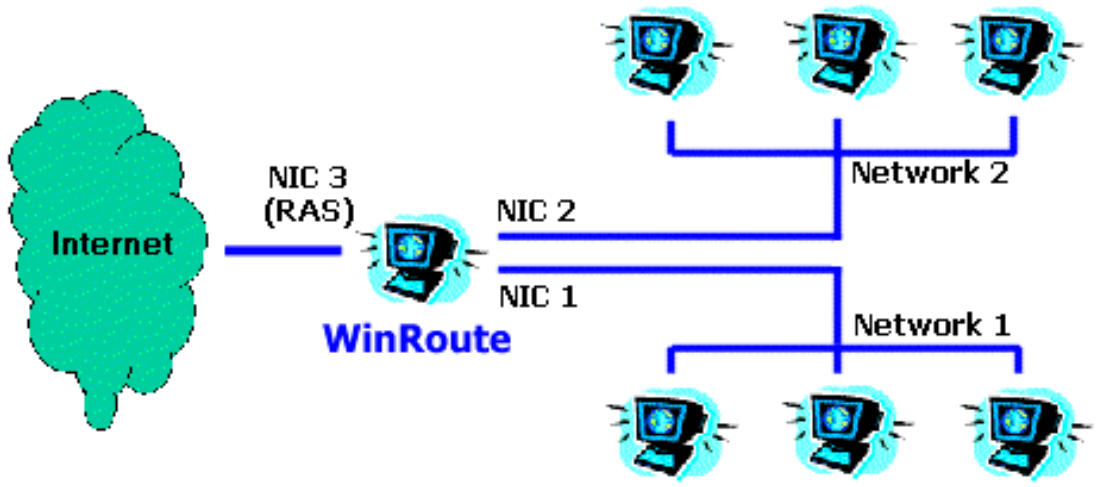
✍✍ ***Nota 1: quando si crea uno spazio per l'indirizzo IP nella rete locale, è necessario utilizzare un indirizzo IP proveniente dalla stessa sottorete: supponendo che la maschera di sottorete utilizzata sia 255.255.255.0, gli indirizzi dovranno essere compresi tra 10.10.10.1 e 10.10.10.255.***

✍✍ ***Nota 2: è possibile connettere più reti a Internet tramite WinRoute. Il computer WinRoute può avere più interfacce, una per ogni rete. Ciascuna delle interfacce (i loro indirizzi IP) rappresenterà il gateway predefinito per il resto della rete.***

Scelta del computer WinRoute

WinRoute **DEVE ESSERE SEMPRE** eseguito sul computer connesso a Internet, indipendentemente dal metodo di connessione (scheda di rete, cavo, modem DSL, connessione di accesso remoto o router).

WinRoute agisce sempre da gateway tra due o più reti, e a ciascuna rete corrisponde un'interfaccia. Le interfacce possono essere schede Ethernet, schede RAS, schede USB-to-Ethernet, schede PPPoE , ecc.


Internet
NIC 3
(RAS)
NIC 2
NIC 1
WinRoute
Network 2
Network 1

Configurazione IP con il server DHCP

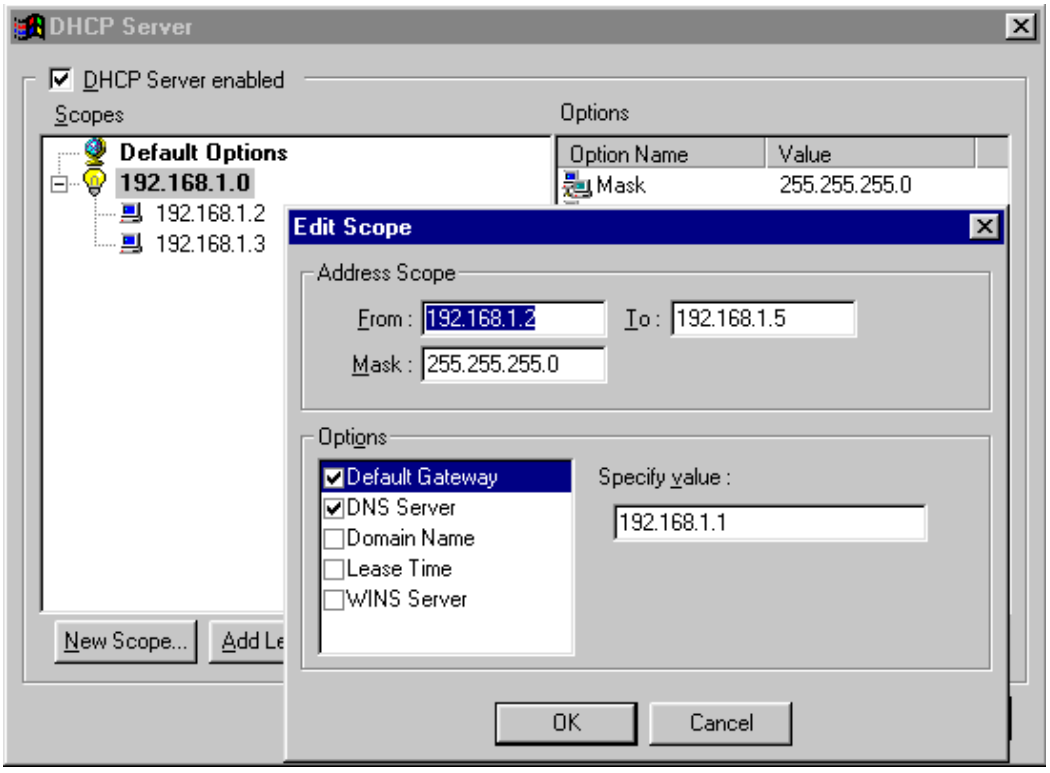
Accertarsi che le workstation siano impostate in modo da ottenere l'indirizzo IP dal server DHCP (vedere le proprietà *TCP/IP->interfaccia di rete* di ciascun computer) e che tutte le altre proprietà TCP/IP siano vuote, incluse le informazioni sul server DNS.

Eseguire quindi Amministrazione di WinRoute:

1. Passare al menu *Impostazioni=>Server DHCP*.
2. Abilitare il server DHCP (selezionare l'opzione) e scegliere **Nuovo ambito**.

3. Aggiungi ambito
Qui è possibile specificare l'ambito degli indirizzi IP assegnati alle workstation, che saranno utilizzati dal server DHCP. Si ricordi che un indirizzo IP è già utilizzato dal computer WinRoute e non può quindi essere riusato. Tutti gli indirizzi IP dell'intervallo devono provenire dalla stessa sottorete. Vedere l'esempio della figura.

4. Specifica opzioni (importante!)
In Opzioni è possibile specificare le altre informazioni fornite alle workstation (ad es. il gateway predefinito, il server DNS, ecc.). Selezionare il pulsante a fianco dei componenti desiderati nella finestra di dialogo. Immmettere le informazioni relative al gateway predefinito e al server DNS (generalmente si utilizza WinRoute come server DNS) e utilizzare l'indirizzo IP del computer WinRoute (ad es. 192.168.1.1). Le altre opzioni possono essere lasciate vuote.


DHCP Server
DHCP Server enabled
Scopes
Options
Default Options
192.168.1.0
192.168.1.2
192.168.1.3
Option Name
Value
Mask
255.255.255.0
Edit Scope
Address Scope
From : 192.168.1.2
To : 192.168.1.5
Mask : 255.255.255.0
Options
Default Gateway
DNS Server
Domain Name
Lease Time
WINS Server
Specify value :
192.168.1.1
New Scope...
Add Le
OK
Cancel

✍✍ ***Nota: è necessario assegnare l'indirizzo IP dell'interfaccia Ethernet (utilizzata per il collegamento alla LAN) sul computer WinRoute. L'indirizzo IP sarà utilizzato dagli altri computer come gateway predefinito e, facoltativamente, come server DNS! Tuttavia, il gateway predefinito sull'interfaccia sarà vuoto.***

Configurazione IP con un terzo server DHCP

Se si utilizza un terzo server DHCP con la propria configurazione di rete, è necessario valutare con attenzione i valori trasmessi da tale server alle workstation della rete.

Accertarsi che le informazioni rilasciate dal server DHCP alle workstation client siano corrette! Il server DHCP deve essere impostato in modo da assegnare agli altri computer della rete l'indirizzo IP della scheda LAN del computer WinRoute come gateway predefinito e (facoltativamente) come server DNS.

L'indirizzo IP rilasciato alla workstation client deve appartenere alla stessa sottorete del computer WinRoute.

ACCERTARSI (!!!) che alla scheda di rete interna sul computer WinRoute **sia assegnato** un indirizzo IP fisso (ad es. 192.168.1.1), e che lo stesso indirizzo sia stato rilasciato come gateway predefinito al resto della rete. Il server DHCP potrebbe non assegnare l'indirizzo IP all'host di WinRoute!

Esempio:

supponendo che l'indirizzo su cui viene eseguito un server NT con DHCP è 192.168.1.1, e quello su cui viene eseguito WinRoute sia 192.168.1.5, l'indirizzo del gateway predefinito (e del DNS, qualora si utilizzi il DNS di WinRoute) rilasciato alle workstation sarà 192.168.1.5.

Configurazione IP assegnazione manuale

In alcuni casi è necessario assegnare manualmente gli indirizzi IP alle workstation. Prima di procedere, è bene ricordare le seguenti regole:

Assegnazione dell'indirizzo IP

Assegnare ad ogni computer un indirizzo IP di "tipo interno". Generalmente 192.168.x.x o 10.x.x.x. Assegnare ai sistemi solo indirizzi IP della stessa sottorete. Supponendo che l'indirizzo IP dell'host WinRoute sia 192.168.1.1, sarà necessario continuare con lo stesso schema numerico (ad es. 192.168.1.2., 192.168.1.3 ecc.).

Impostazione del gateway predefinito

Utilizzare l'indirizzo IP del computer host di WinRoute come gateway predefinito per tutti i computer client. In altre parole, ciascun computer client utilizzerà l'indirizzo IP dell'host WinRoute (indirizzo IP interno) come gateway predefinito. L'indirizzo va immesso nella scheda TCP/IP=>Scheda Ethernet di Proprietà di rete del computer.

Impostazione del DNS

Utilizzare l'indirizzo IP dei computer WinRoute come server d'inoltro DNS per tutti i computer (che corrisponderà all'indirizzo IP interno qualora si stia utilizzando il server DHCP di WinRoute). Qualora si utilizzi l'indirizzo DNS del provider Internet o di un altro server DNS, i dettagli sul DNS saranno forniti dal provider Internet (nelle proprietà TCP/IP->NIC di ciascuna workstation).

Importante! Si raccomanda di fare riferimento al capitolo sulle impostazioni DNS avanzate!

Impostazione del server d'inoltro DNS

Per configurare il server DNS, utilizzare il menu: *Impostazioni => Server DNS*.

"Abilita inoltro DNS"

Questa opzione consente di abilitare e disabilitare il server DNS.

"Inoltra richieste DNS al server selezionato automaticamente tra i server DNS noti al sistema operativo"

Se l'opzione è selezionata, tutte le richieste DNS verranno inoltrate al server DNS scelto dalla configurazione TCP/IP dell'interfaccia Internet o della connessione di accesso remoto.

"Abilita ricerca nel file HOST"

Se l'opzione è selezionata, il server DNS potrà utilizzare i dati archiviati nel file HOSTS per rispondere alle richieste.

"Modifica file HOST..."

Il pulsante avvia un editor di testo esterno per modificare il file HOSTS.

"Dominio DNS"

Immettere qui il nome del dominio (ad es. "acme.com"). Nelle risposte alle richieste DNS, il nome di dominio viene aggiunto al nome host ottenuto dal file HOSTS o dalla tabella di lease DHCP.

"inoltra le richieste del server DNS a"

Immettere l'indirizzo IP numerico del server DNS a cui si desidera inoltrare le richieste DNS. Scegliere un indirizzo del server DNS del proprio provider Internet o di un server a cui ci si possa connettere rapidamente.

"Abilita cache DNS"

Permette di archiviare nella cache interna le risposte alle richieste DNS. Le successive richieste verranno elaborate in base al contenuto della cache, senza attendere la risposta del server DNS esterno alla rete.

"Durante la risoluzione del nome ricavato dal file HOST o dalla tabella di lease, unire il nome con il dominio DNS sotto indicato"

✍✍ ***Questa funzione può essere compresa più facilmente con un esempio: si supponga di voler risolvere la richiesta DNS per il computer CARLO. Nel file HOST si è specificato che il dominio UFFICIO è associato a un indirizzo IP specifico. La richiesta CARLO.UFFICIO potrà essere risolta correttamente.***

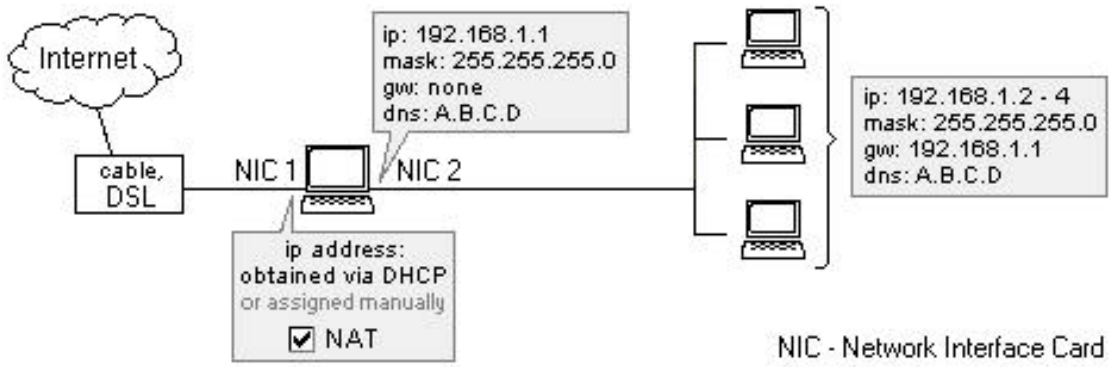
La cache archivia solo le risposte di tipo "Nome => Indirizzo IP". Le risposte rimangono in memoria fino al momento della scadenza. La data di scadenza viene fornita dai server DNS insieme alle risposte.

Connessione della rete a Internet

In questa sezione

Connessione DSL

La connessione DSL (ADSL, SDSL) richiede l'installazione di due schede NIC (Network Interface Card) sul computer WinRoute. Una delle schede servirà per il collegamento a Internet (modem DSL), l'altra per il collegamento all'interfaccia interna.



Configurazione di WinRoute

Per connettersi a Internet:

1. Selezionare Impostazioni->Tabella interfacce
2. Scegliere la scheda NIC per il collegamento a Internet, fare clic su Proprietà e selezionare "Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti". Quando si aprirà la finestra di dialogo Tabella interfacce, la linea esterna sarà affiancata dall'indicazione NAT ON.
3. Verificare che l'indicazione NAT ON non compaia a fianco dell'interfaccia utilizzata per il collegamento alla rete interna (passare alle proprietà dell'interfaccia nella Tabella interfacce)
4. Accertarsi che non sia stato impostato alcun gateway nelle proprietà TCP/IP della scheda NIC interna (passare alle impostazioni di rete) e che la NIC possieda un indirizzo IP interno.
5. Controllare la correttezza dei dati rilasciati dal provider relativamente alla NIC utilizzata per il collegamento a Internet. Qualora gli indirizzi IP vengano assegnati in modo dinamico, lasciare vuoto lo spazio destinato all'indirizzo IP.

Per le altre impostazioni di rete, fare riferimento ai capitoli appropriati, in particolare a ***Elenco di controllo*** .

Connessione DSL con scheda PPPoE

PPPoE è una tecnologia adottata di recente da molti sottoscrittori DSL. Sebbene abbia larga diffusione tra i provider Internet, non è attualmente la soluzione più indicata per connettere una rete privata a Internet, per via delle prestazioni troppo spesso insoddisfacenti. È sempre consigliabile richiedere la soluzione DSL standard.

L'utilizzo di PPPoE con WinRoute è analogo, in termini di impostazioni TCP/IP, a quello del DSL standard. Installare WinRoute Pro sullo stesso computer su cui è installata la scheda PPPoE utilizzata come interfaccia di rete. Abilitare NAT sull'interfaccia. La tabella interfacce di WinRoute Pro riporterà anche la scheda Ethernet (collegata al modem via cavo). Non abilitare NAT per questa interfaccia.

Anche se WinRoute Pro funziona egregiamente con tutte le schede PPPoE attualmente in commercio, sono stati riscontrati alcuni problemi di prestazioni:

Enternet 100, 300, 500 PPPoE client

WinRoute Pro 4.1 funziona bene con Enternet PPPoE client di NTS se si ha l'accortezza di selezionare il driver del protocollo invece del driver del filtro. Per eseguire l'operazione, avviare Enternet PPPoE client, passare al menu Impostazioni->Avanzate e modificare i valori desiderati.

Per evitare il problema delle prestazioni insoddisfacenti, potrebbe essere necessario ridurre a 800 la dimensione MTU sui computer client.

WinPoet d Ivasion

WinRoute Pro 4.1 funziona bene con WinPoet, a condizione che la compressione dell'intestazione IP (impostazioni di rete RAS/Accesso remoto) sia disattivata.

Riduzione della dimensione MTU:

la scheda PPPoE aggiunge informazioni supplementari alle intestazioni dei pacchetti in uscita. In base all'impostazione predefinita, Windows utilizza la dimensione massima consentita dei pacchetti. La scheda PPPoE compensa questa impostazione riducendo leggermente la MTU del computer locale. Sfortunatamente tutti gli altri PC continuano a utilizzare la dimensione massima per la trasmissione, e ciò porta alla perdita di pacchetti. I due collegamenti di seguito indicati mostrano come procedere per ridurre la MTU di tutti i client.

Per gli utenti di Windows 95/98:

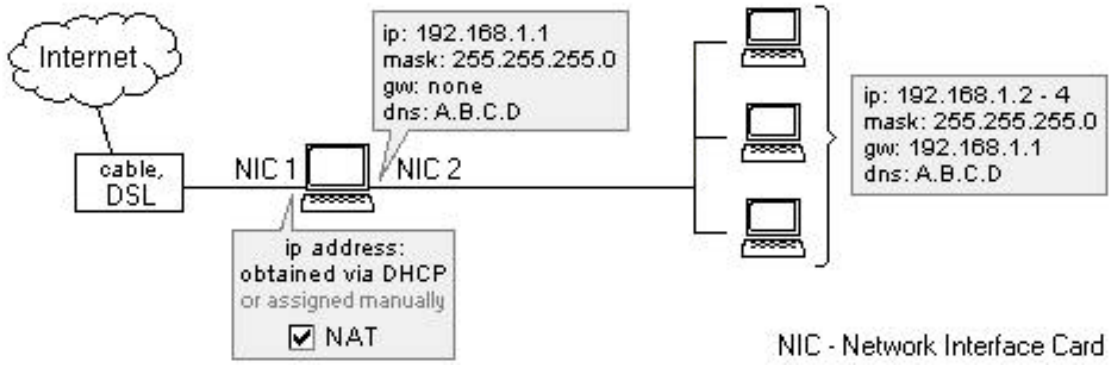
http://www.microsoft.com/support/kb/articles/Q158/4/74.asp

Per gli utenti di Windows NT4/2000:

http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnbd/cnbd_trb_vcfx.asp

Connessione con modem via cavo (bidirezionale)

La connessione con modem via cavo richiede l'installazione di due schede NIC (Network Interface Card), incluse in WinRoute. Una delle schede servirà per il collegamento a Internet (modem via cavo), l'altra per il collegamento alla rete interna. Per i modem via cavo unidirezionali, (modem all'andata, cavo al ritorno) passare al capitolo appropriato.



Configurazione di WinRoute

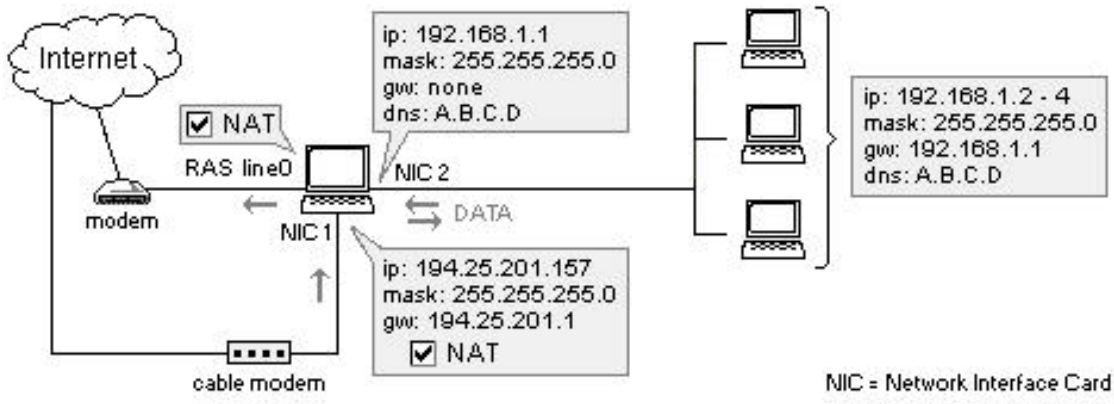
1. Selezionare il menu Impostazioni->Tabella interfacce
2. Scegliere il collegamento NIC per Internet, fare clic su Proprietà e selezionare "Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti". Nella finestra di dialogo Tabella interfacce, la linea esterna sarà affiancata dall'indicazione NAT ON.
3. Verificare che l'indicazione NAT ON non compaia a fianco dell'interfaccia utilizzata per il collegamento alla rete interna (passare alle proprietà dell'interfaccia nella Tabella interfacce).
4. Accertarsi che non sia stato impostato alcun gateway nelle proprietà TCP/IP della scheda NIC interna (passare alle impostazioni di rete) e che la NIC possieda un indirizzo IP interno.
5. Controllare la correttezza dei dati rilasciati dal provider Internet relativamente alla NIC utilizzata per il collegamento a Internet. Qualora gli indirizzi IP vengano assegnati in modo dinamico, lasciare vuoto lo spazio destinato all'indirizzo IP.

Per le altre impostazioni di rete, fare riferimento ai capitoli appropriati (ad es. ***Elenco di controllo*** , ***Configurazione IP*** ecc.).

Modem via cavo unidirezionali (modem all'andata, cavo al ritorno)

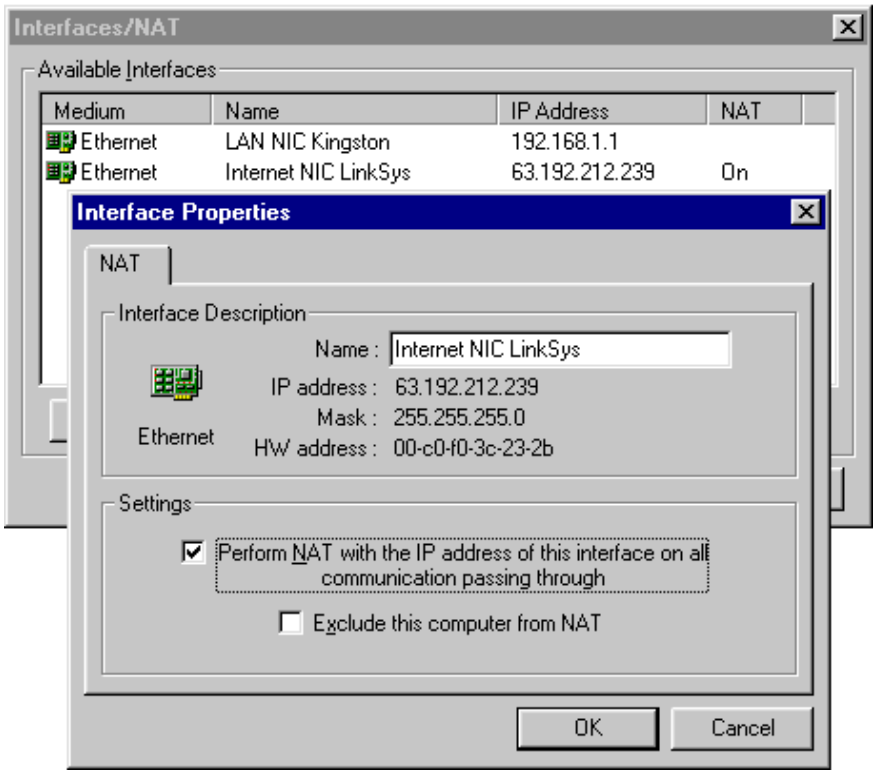
NOTA: questo tipo di connessione Internet **non è una "configurazione supportata ufficialmente"** perché le impostazioni possono variare da un provider Internet all'altro. Tuttavia, la tendenza è quella di supplire il maggior numero di soluzioni d'accesso possibili. Molti utenti sono riusciti a configurare la connessione applicando le impostazioni di seguito indicate.

In generale, il flusso dei dati è **simile a quello di Direc P.Q** pacchetti in uscita passano attraverso l'interfaccia di **accesso remoto** Sulla via del ritorno, i pacchetti vengono instradati **via cavo** Di fatto il provider Internet deve sempre associare l'utente a due interfacce. Anche se ciò può sembrare macchinoso, è l'unica soluzione che consenta di stabilire una connessione. Pertanto, prima di acquistare WinRoute è consigliabile verificare che il proprio provider Internet offra questo tipo di soluzione.



1. Scegliere il menu *Impostazioni->Tabella interfacce*. Verranno visualizzati un'interfaccia di **linea RAS** (il modem dell'utente) e due interfacce con **schede di rete** - una per il collegamento a Internet e una per il collegamento alla rete locale.

2. Fare clic sull'interfaccia della scheda di rete utilizzata per il collegamento a Internet e passare a *"Proprietà"*. Selezionare *"Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti"*.



3. Fare clic su **Interfaccia RAS** e passare a *"Proprietà"*. Selezionare *"Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti"*. Nella **scheda RAS** specificare il collegamento che verrà utilizzato per la connessione al provider Internet, quindi immettere il nome utente e la password.

4. Accertarsi che il protocollo NAT **NON SIA SELEZIONATO** per il collegamento di interfaccia alla rete interna (andare alle proprietà dell'interfaccia).

5. Controllare che **NON SIA SELEZIONATO alcun gateway** nelle proprietà TCP/IP della NIC interna (andare alle impostazioni di rete) e che alla NIC sia stato assegnato un **indirizzo IP** di classe privata (ad es.10.10.1.1).

6. Verificare la correttezza dei dati rilasciati dal provider Internet relativamente alla NIC utilizzata per il collegamento a Internet (proprietà TCP/IP). Nota: qualora gli indirizzi IP vengano assegnati in modo dinamico, lasciare vuoto lo spazio destinato all'indirizzo IP.

✍✍ ***Come regola generale, NAT dovrebbe essere abilitato su entrambe le interfacce utilizzate per il collegamento a Internet RAS e Accesso remoto.***

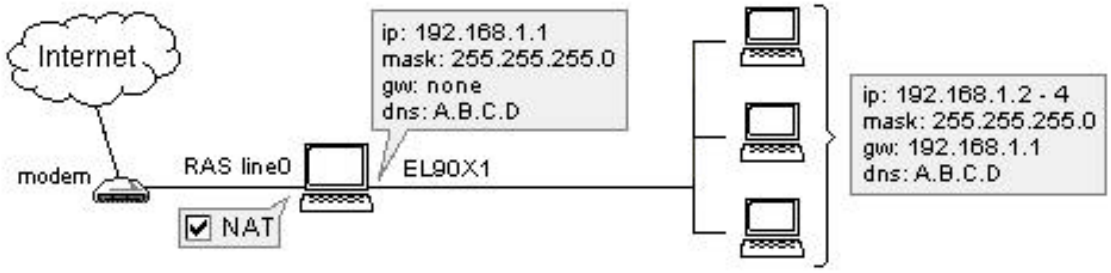
Connessione tramite Accesso remoto o ISDN

Connessione tramite Accesso remoto o ISDN

Se si è connessi a Internet tramite una linea di accesso remoto (con modem a 56 K o ISDN) e un PC con sistema operativo Win 95, Win 98 o NT 4.0 , si dispone di tutto ciò che occorre per eseguire WinRoute. I requisiti fondamentali per eseguire WinRoute sono:

✍✍ Modem collegato a una linea telefonica o ISDN.

✍ Scheda NIC (Network Interface Card) collegata alla rete interna.



Qualora il modem ISDN sia collegato al computer tramite scheda Ethernet, fare riferimento al capitolo Connessione tramite DSL; WinRoute dovrà essere configurato appositamente per funzionare con due schede Ethernet.

Prima della onnessione

Prima di connettersi Internet, controllare che:

✍ · Il protocollo TCP/IP sia stato installato e configurato correttamente (vedere i capitoli sull'elenco di controllo o sulle impostazioni di rete).

✍ · Accesso remoto (Windows 95/98) o RAS (Windows NT) sia stato installato e configurato correttamente.

✍ · Il modem sia collegato al PC host di WinRoute.

Per la connessione a Internet, WinRoute utilizza i servizi di Accesso remoto o RAS del sistema operativo.

Installare ed eseguire WinRoute PRIMA di connettersi a Internet; in questo modo sarà possibile verificare se la connessione sia stata configurata correttamente e se Accesso remoto o RAS funzionino correttamente.

Configurazione di WinRoute

Dopo avere completato le configurazioni descritte qui sopra:

1. Scegliere il menu Impostazioni->Tabella interfacce. La tabella dovrebbe mostrare tutte le interfacce disponibili per il computer. Le interfacce di Accesso remoto sono denominate RAS nei sistemi operativi di WinRoute (Windows 95/98/NT).
2. Andare alle proprietà dell'interfaccia RAS selezionata.
3. Selezionare l'opzione "Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti".
4. Andare alla tabella RAS, nella finestra di dialogo Proprietà, scegliere o creare la connessione e impostare le opzioni in conformità alle proprie esigenze. Per ulteriori informazioni, vedere la tabella RAS.

✍✍ ***Importante! Il protocollo NAT deve essere SELEZIONATO sull'interfaccia RAS e DESELEZIONATO sulle interfacce che collegano alla rete interna.***

Configurazione dell'interfaccia Ethernet

1. La scheda NIC utilizzata come interfaccia per la rete interna deve avere un indirizzo IP assegnato (classe privata) ma NON DEVE AVERE un gateway assegnato!
2. I dati DNS utilizzati per questa interfaccia sono ricavati dalle informazioni rilasciate dal provider Internet. Se non si dispone di tali dati, richiederli al proprio provider.

È possibile impostare WinRoute in modo che esegua la funzione di composizione su richiesta, in base alla quale la connessione viene stabilita automaticamente a seconda del traffico (dati) in uscita dalla rete locale. Per ulteriori informazioni, fare clic qui.

Connessione AOL

Tramite WinRoute Pro è possibile connettere una rete privata a Internet utilizzando un singolo account di accesso remoto AOL. Nota - AOL supporta solo i computer con Windows 95/98. Per connettersi tramite AOL procedere come di seguito indicato:

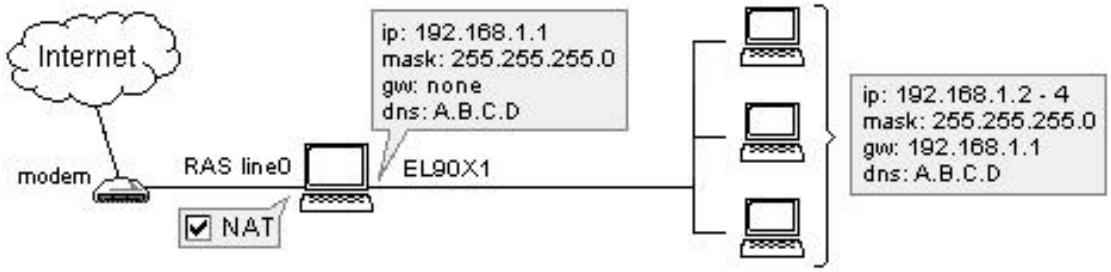
1. Installare il client AOL (AOL 5.0 o superiore)
2. Connettersi a Internet per verificare che le impostazioni siano corrette.
3. Installare WinRoute Pro.
4. In Amministrazione di WinRoute scegliere il menu *Impostazioni->Tabella interfacce*
5. Nell'elenco delle interfacce disponibili dovrebbe comparire la scheda AOL. Fare clic sulle proprietà dell'interfaccia e scegliere "Esegui NAT".

Impostare il computer WinRoute e i computer client in funzione dell'elenco di controllo (vedere l'altro capitolo).

✍✍ ***Nota! La funzione di connessione su richiesta non è disponibile. È necessario iniziar connessione ad AOL manualmente.***

Connessione T1 o LAN

La connessione T1 o LAN richiede l'installazione di due schede NIC (Network Interface Card) sul computer WinRoute. Una delle schede servirà per il collegamento a Internet (ad es. router), l'altra per il collegamento all'interfaccia interna.



Per connettersi a Internet :

1. Scegliere il menu Impostazioni->Tabella interfacce.
2. Scegliere la scheda NIC per il collegamento a Internet, fare clic su Proprietà e selezionare "Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti". Nella finestra di dialogo Tabella interfacce, la linea esterna sarà affiancata dall'indicazione NAT ON.
3. Verificare che l'indicazione NAT ON non compaia a fianco dell'interfaccia utilizzata per il collegamento alla rete interna (passare alle proprietà dell'interfaccia nella Tabella interfacce).
4. Accertarsi che non sia stato impostato alcun gateway nelle proprietà TCP/IP della scheda NIC interna (passare alle impostazioni di rete) e che la NIC possieda un indirizzo IP interno.

5 Controllare la correttezza dei dati rilasciati dal provider Internet relativamente alla NIC utilizzata per il collegamento a Internet. Qualora gli indirizzi IP vengano assegnati in modo dinamico, lasciare vuoto lo spazio destinato all'indirizzo IP.

Per le altre impostazioni di rete, fare riferimento ai capitoli appropriati, in particolare a ***Elenco di controllo*** .

Connessione DirecPC

DirecPC utilizza un modem (analogico, ISDN, ...) o una scheda NIC (Ethernet, Token Ring) per l'uplink, mentre si serve di un'antenna satellitare per lo scaricamento dei dati. Per la connessione a Internet è possibile utilizzare DirecPC o, in alternativa, la connessione di accesso remoto del provider Internet.

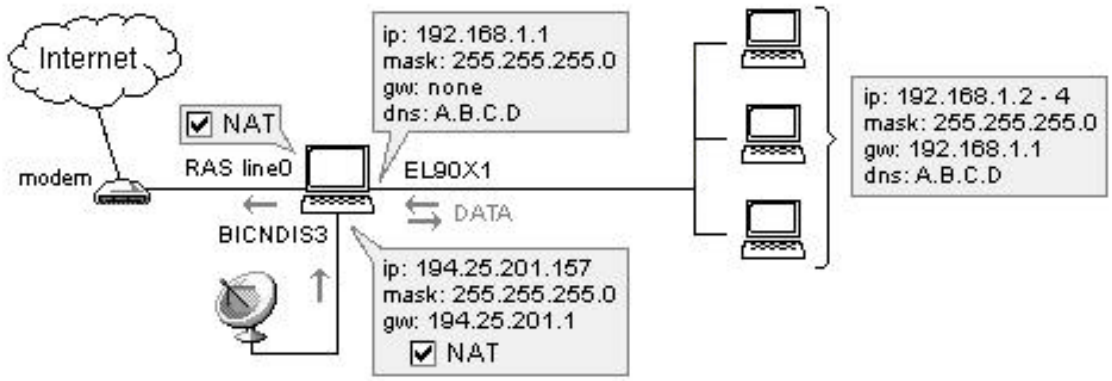
Tramite il modem, i dati passano dal computer di origine al servizio Internet di DirecPC, da dove vengono instradati verso la destinazione finale. Nel percorso di ritorno, i pacchetti (dati) diretti al computer dell'utente vengono associati a dati diversi, per poterli instradare tramite l'antenna satellitare.

Configurazione di WinRoute

Per prima cosa occorre controllare che il software DirecPC e i componenti necessari siano stati installati correttamente. Dopodiché sarà possibile configurare WinRoute in funzione delle proprie esigenze.

Per l'uplink è possibile scegliere tra DirecPC o RAS di WinRoute. Nel secondo caso si disporrà anche della funzione di composizione su richiesta, che consente di risparmiare sulla bolletta telefonica.

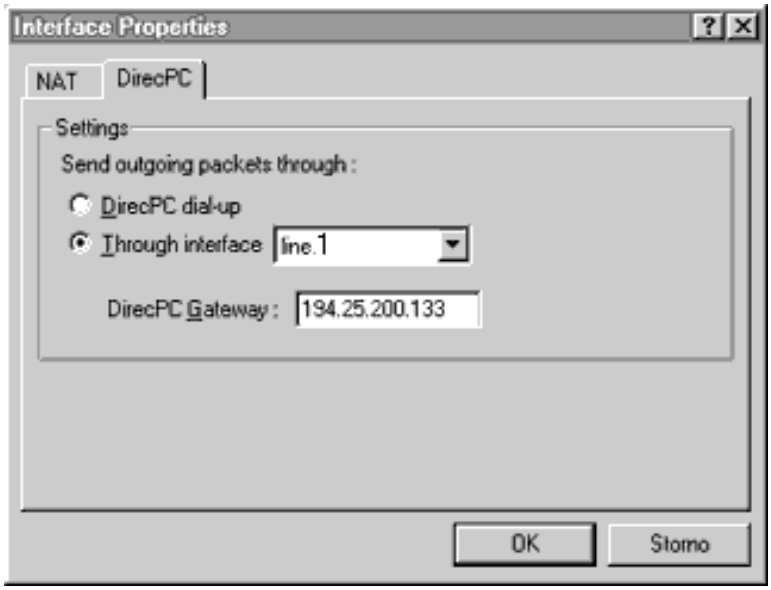
1. Utilizzo di linee RAS per l'uplink



Scegliere il menu *Impostazioni->Tabella interfacce*. Verranno visualizzate l'interfaccia della linea RAS (il modem in uso) e la scheda d'interfaccia DirecPC.

Fare clic sulla scheda d'interfaccia DirecPC e scegliere "Proprietà". Verranno visualizzate due schede - **NAT** e **DirecPC**.

- Nella scheda NAT selezionare l'opzione *"Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti"*.
- Nella scheda DirecPC specificare che verrà utilizzata la *linea 0* per l'uplink. Immettere l'*indirizzo IP del gateway* ottenuto da DirecPC.

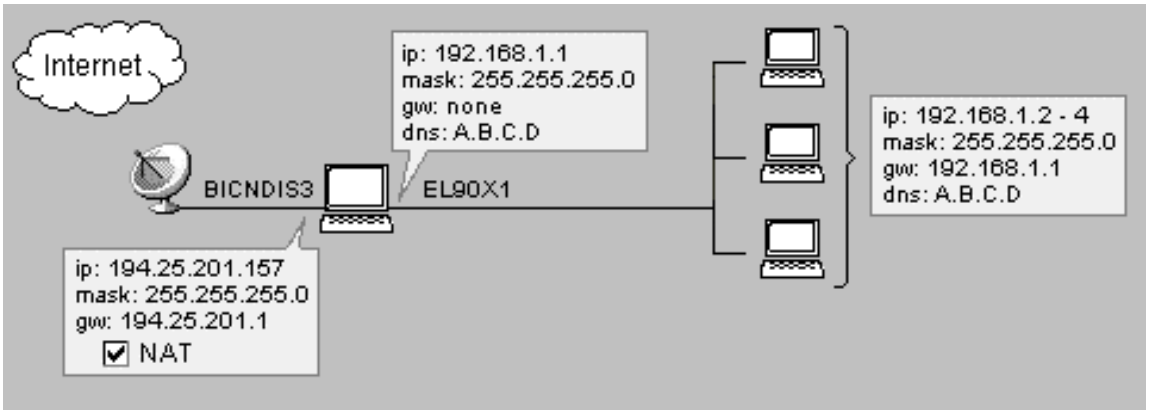


3. Fare clic sull'interfaccia RAS e scegliere "Proprietà". Selezionare l'opzione "Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti". Nella scheda RAS, selezionare la connessione che verrà utilizzata per il collegamento al proprio provider Internet, quindi immettere il nome utente e la password.

✍✍ ***Nota! DESELEZIONARE l'opzione "Utilizza gateway predefinito sulla rete remota" nelle proprietà dell'account di accesso remoto creato per connettersi al provider Internet e selezionare l'opzione nelle proprietà TCP/IP dell'interfaccia di accesso remoto.***

2. Utilizzo della composizione automatica di DirecPC per l'uplink

Ove disponibile, è possibile utilizzare la funzione di composizione automatica di DirecPC, ma è sempre preferibile utilizzare la linea RAS di WinRoute.



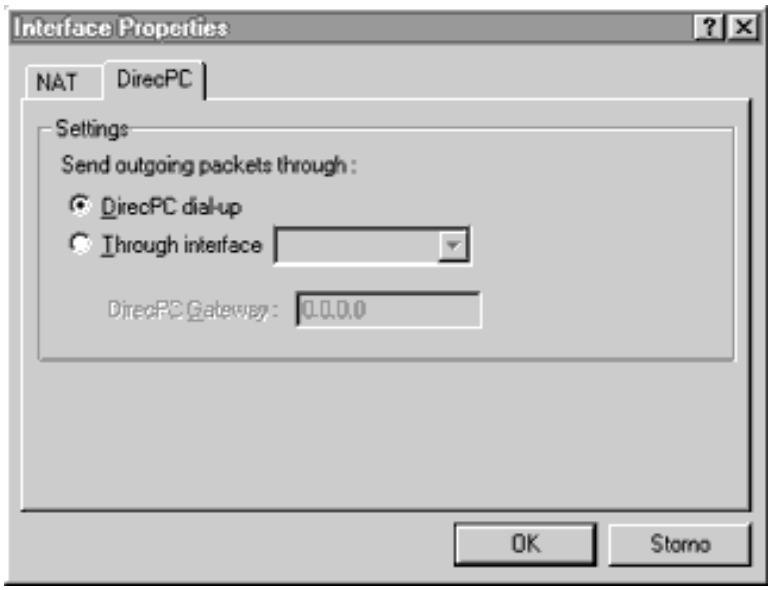
Per utilizzare la composizione automatica di DirecPC:

Scegliere il menu *Impostazioni->Tabella interfacce*. Verranno visualizzate l'interfaccia della linea RAS (il modem in uso) e la scheda d'interfaccia DirecPC.

Fare clic sulla scheda d'interfaccia DirecPC e scegliere "*Proprietà*". Verranno visualizzate due schede - NAT e DirecPC.

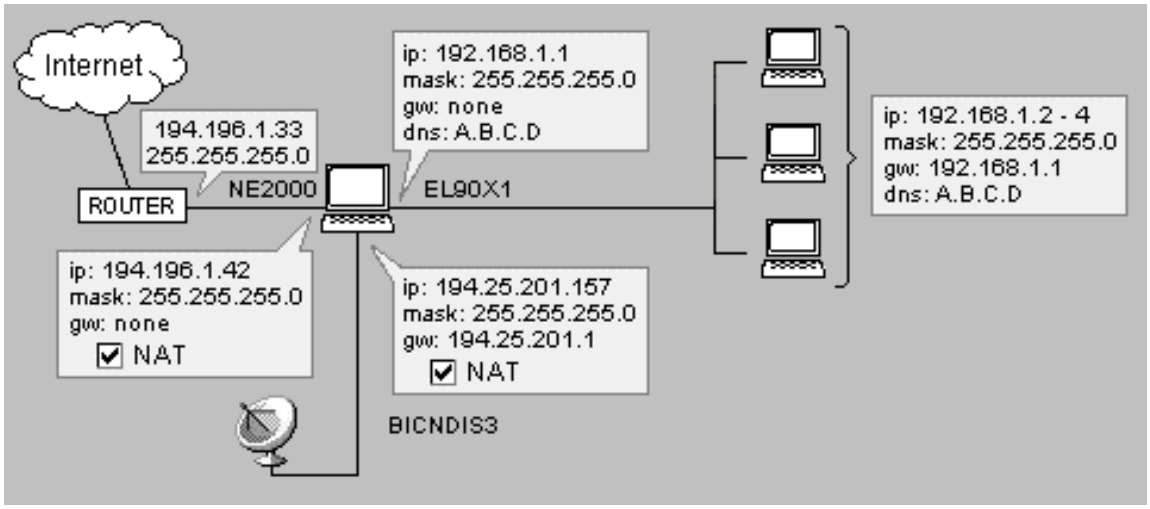
✍ Nella scheda NAT, selezionare l'opzione "*Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti*".

✍ Nella scheda DirecPC, selezionare l'opzione "*Utilizzare la connessione DirecPC per l'uplink*".

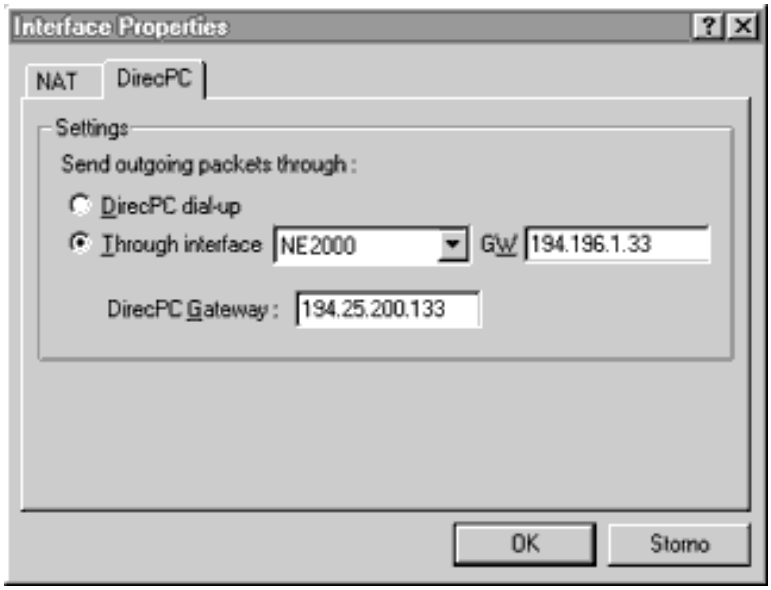


3. Utilizzo dell'interfaccia Ethernet per l'uplink

A volte è auspicabile utilizzare la scheda d'interfaccia Ethernet per l'uplink, soprattutto se si utilizza una connessione ISDN (con modem o router ISDN) o una connessione V-SAT (parabola con scheda Ethernet).



Andare alla finestra di dialogo delle proprietà dell'interfaccia DirecPC.



✍ Nella scheda NAT, selezionare l'opzione "*Esegui NAT con l'indirizzo IP di questa interfaccia su tutte le comunicazioni passanti*".

✍ Nella scheda DirecPC selezionare l'opzione "*Interfaccia passante*" e scegliere l'interfaccia utilizzata per i collegamento a Internet. Immettere quindi il gateway predefinito del provider Internet nel campo "GW" (ad es. 194.196.1.33).

Aumento della velocità di trasmissione

Per massimizzare la velocità di trasmissione dei dati quando ci si connette a Internet tramite DirecPC, ridurre la **finestra di ricezione TCP** su tutti i computer che utilizzeranno DirecPC:

In Windows NT:

1. Andare a Registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servizi\Tcpip\Parametri
2. Aggiungere (o modificare, se già esistente) la voce "TcpWindowSize" (del tipo DWORD) nel registro di sistema. Impostare i valore a 0xBB80.

In Windows 95:

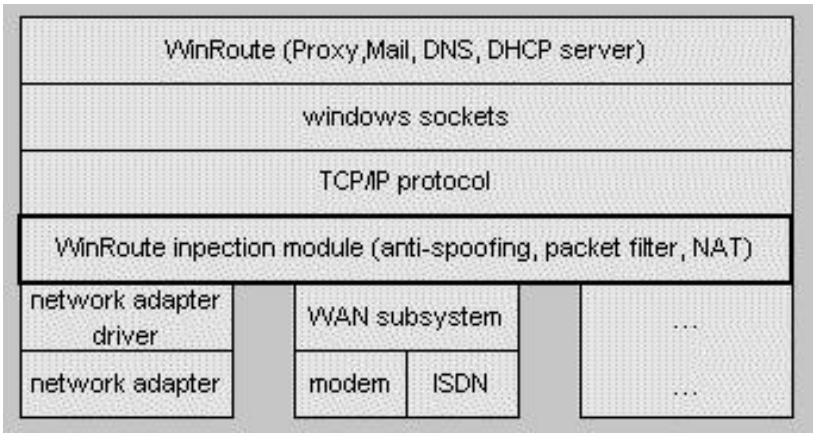
1. Andare a Registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Servizi\VxD\MSTCP.
2. Aggiungere (o modificare, se già esistente) la voce "DefaultRcvWindow" (del tipo stringa) nel registro di sistema. Impostare il valore a "0xBB80".

Impostazione della protezione

In questa sezione

ProtezioneNAT

WinRoute esegue NAT al livello più basso possibile del protocollo di rete, e controlla il traffico tra il driver della scheda NIC (Network Interface Card) e lo stack TCP. Poiché gestisce l'intero traffico Internet, catturando sia i pacchetti in uscita sia quelli in entrata, si riduce drasticamente il pericolo di guasti. Questa funzione è disponibile solo con l'implementazione del protocollo NAT di WinRoute. Un'ulteriore caratteristica di protezione è il firewall basato su filtri pacchetto, o anti-spoofing. Grazie a NAT l'intera rete è completamente protetta, incluso il computer WinRoute.



Opzioni di protezione NAT

A partire dalla build 20, WinRoute è stato arricchito di un menu di protezione NAT che, tra le altre opzioni, permette di operare in **modalità silenziosa**. Ciò significa che, con particolari tipi di richieste, WinRoute può "ignorare" i pacchetti, affinché la rete appaia invisibile dall'esterno.

Richiesta diecho ICMP:

ICMP (Internet Control Message Protocol) è il protocollo che consente di iniziare una richiesta di informazioni (esecuzione di ping, ad es. - ping 206.86.211.32). Se un computer cerca di eseguire il **ping** sull'host di WinRoute, le **Opzioni di protezione NAT** prevedono due reazioni:

- Se si seleziona *"Rispondi alla richiesta"* il computer che ha inoltrato la richiesta riceverà una risposta.
- Se si seleziona *"Ignora la richiesta (modalità silenziosa)"* il datagramma verrà ignorato, e il computer che ha inoltrato la richiesta riceverà in risposta il messaggio *"host di destinazione irraggiungibile"*.

Pacchetti in entrata non indicati nella tabella NAT:

WinRoute ispeziona tutto il traffico in entrata e in uscita sulla LAN e confronta sempre il numero di porta e l'indirizzo IP del pacchetto o del record con le informazioni registrate nella tabella NAT, anche nel caso in cui non venga eseguita la NAT. In questo modo, il pacchetto di ritorno potrà essere confrontato con la tabella NAT, per stabilire a chi debba essere instradato. Se il pacchetto non è stato iniziato, e quindi non è un pacchetto di ritorno, WinRoute lo confronterà con i dati della tabella NAT, per confermare che si tratta di un pacchetto non iniziato. Se le porte non sono state mappate, non sarà possibile inviare il pacchetto a nessun componente della LAN.

- L'opzione "Invia pacchetto di rifiuto" restituirà il pacchetto al mittente, informandolo che non è stato possibile stabilire la connessione.
- L'opzione "Ignora la richiesta (modalità silenziosa)" eliminerà il pacchetto e non invierà alcun pacchetto di ritorno. In questo modo l'host di WinRoute, e la LAN a cui esso appartiene, sembreranno non esistere.

Pacchetti in entrata UDP:

Alcune applicazioni che utilizzano l'UDP (**User Datagram Protocol**) richiedono l'invio dei pacchetti UDP a un server centrale. WinRoute registra l'origine e la destinazione di tutti i pacchetti UDP diretti al server assegnato dall'applicazione che invia il pacchetto. In alcuni casi, il server potrà passare l'indirizzo IP e la porta dell'utente a un altro computer, che risponderà all'utente con un pacchetto UDP contenente le informazioni richieste. Anche se quest'ultimo computer scelto a caso avrà un indirizzo IP diverso da quello del server, potrà comunque inviare pacchetti UDP al server, perché conosce l'IP e la porta da utilizzare.

- Sulla base di quanto detto, se si scegliesse "*Smista via NAT indipendentemente dall'indirizzo IP di origine*" il pacchetto UDP passerebbe da WinRoute.
- Per migliorare la protezione, è possibile scegliere "*Smista via NAT solo se l'indirizzo IP di origine è stato registrato dopo l'invio del primo pacchetto in uscita da LAN*". In questo modo solo i pacchetti UDP provenienti dal server centrale passeranno da WinRoute.

Opzioni di registrazione log NAT:

Tra le opzioni avanzate di protezione, esiste la possibilità di registrare le informazioni dei pacchetti in arrivo non richiesti da nessuno all'interno della LAN. Questa opzione viene in genere selezionata per le reti con server Web, FTP, DNS o di altro tipo interni a WinRoute, perché consente di rintracciare l'origine di eventuali problemi.

Registrazione log pacchetti non indicati nella tabella NAT:

WinRoute offre due opzioni per la registrazione log dei pacchetti TCP non indicati nella tabella NAT.

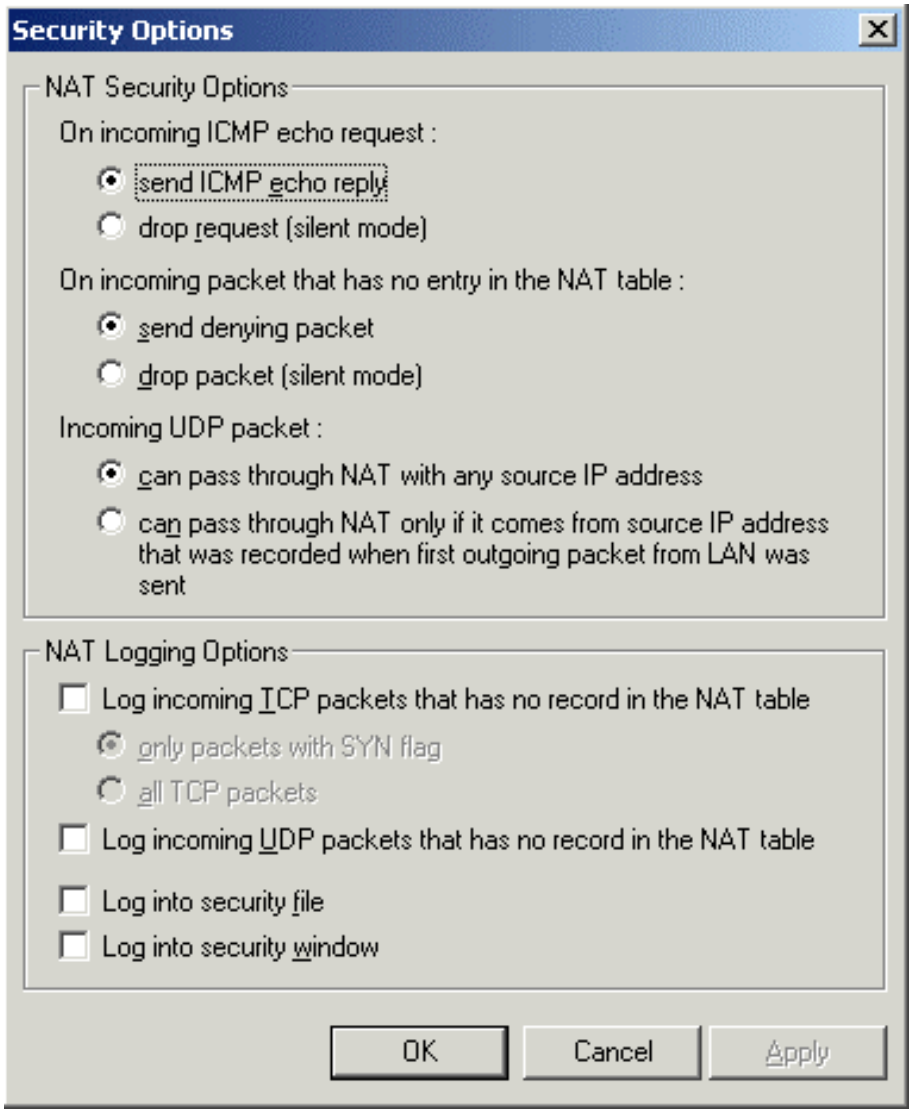
- Se si sceglie "*Solo pacchetti con flag SYN*" (sincronizza), il pacchetto TCP verrà registrato solo se la connessione tra mittente e destinatario sarà stata stabilita.

✍ L'opzione "*Tutti i pacchetti TCP*" registra tutti i pacchetti TCP in arrivo, indipendentemente dal fatto che la connessione sia stata stabilita. Poiché i pacchetti UDP non fanno uso di flag, tutti i pacchetti UDP non iniziati verranno registrati se si sceglie la registrazione log dei pacchetti UDP.

Registrazione log su file o finestra:

✍ Se si seleziona l'opzione "*Registra log pacchetti in finestra di protezione*" è possibile scegliere di visualizzare le informazioni di log dall'applicazione di amministrazione di WinRoute, scegliendo Visualizza>Registri>Registro di protezione.

✍ Se si sceglie "*Registra log su file*", WinRoute salverà le informazioni di log sul log di protezione, nella cartella Logs di WinRoute Pro (generalmente c:/Program Files/WinRoute Pro/Logs)


Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Impostazioni del filtro pacchetto

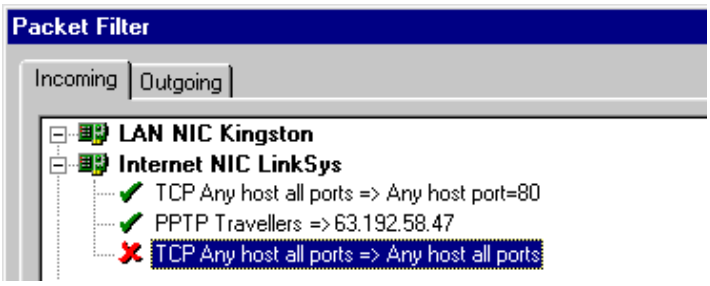
La configurazione del filtro pacchetto di WinRoute Pro per il firewall è piuttosto semplice, ma richiede una buona comprensione della logica adottata da WinRoute per il filtro del pacchetto .

Insieme di regole per l'interfaccia

Gli utenti possono definire specifiche regole di protezione per le singole interfacce del computer. Questa caratteristica è molto utile per l'amministrazione di reti multi-segmento.

Esempio: la figura seguente mostra una rete che:

- *Consente a tutti coloro che navigano in Internet di accedere al server Web interno alla rete.*
- *Consente solo ad alcuni individui prescelti dai gruppi di indirizzi predefiniti, chiamati "Viaggiatori", di accedere al server PPTP interno alla rete, che apre l'accesso alla rete stessa.*



Regole separate per i pacchetti in uscita e in entrata

WinRoute applica regole separate ai pacchetti in uscita e in entrata. Per ogni interfaccia WinRoute crea a una tabella specifica, nella quale viene registrato il traffico dei pacchetti in entrata e in uscita. In altre parole, ad ogni pacchetto corrispondono due voci, una per l'uscita e l'altra per l'entrata.

Pacchetti IN USCITA e pacchetti IN ENTRATA

WinRoute considera il proprio modulo di gestione come il componente centrale dell'intero sistema. Ciò significa che tutti i pacchetti che lasciano WinRoute sono classificati come IN USCITA, indipendentemente dal fatto che la loro destinazione sia Internet o la LAN. Allo stesso modo, tutti i pacchetti diretti AL PC WinRoute sono considerati IN ENTRATA, indipendentemente dalla loro origine. È opportuno ricordare questa logica quando si determinato le regole di protezione.

APPLICAZIONEDELLE REGOLE:

Dall'ALTO al BASSO

Le regole, definite in un apposito elenco, vengono applicate a partire dalla prima in alto e proseguendo in ordine discendente. Quando un pacchetto raggiunge l'interfaccia, viene confrontato con i criteri definiti nell'elenco. La verifica inizia dal primo criterio dell'elenco (quello più in alto) e prosegue in direzione della regola che occupa la posizione più bassa. Non appena il pacchetto corrisponda ai criteri di confronto, la regola appropriata verrà applicata e le regole restanti omesse.

Le regole possono essere applicate a:

- utenti indipendenti

- intervallo di indirizzi IP
- gruppi di indirizzi IP definiti dall'utente (per definire un gruppo di utenti, fare riferimento al presente manuale)
- l'intera sottorete o rete

Le regole possono essere applicate a fasce orarie predefinite

In alcuni casi, potrebbe essere utile applicare regole specifiche durante l'orario d'ufficio e altri criteri per l'orario di chiusura dell'ufficio. Oppure, si potrebbe voler consentire l'accesso durante la pausa pranzo e limitare l'accesso a risorse specifiche durante l'orario di lavoro.

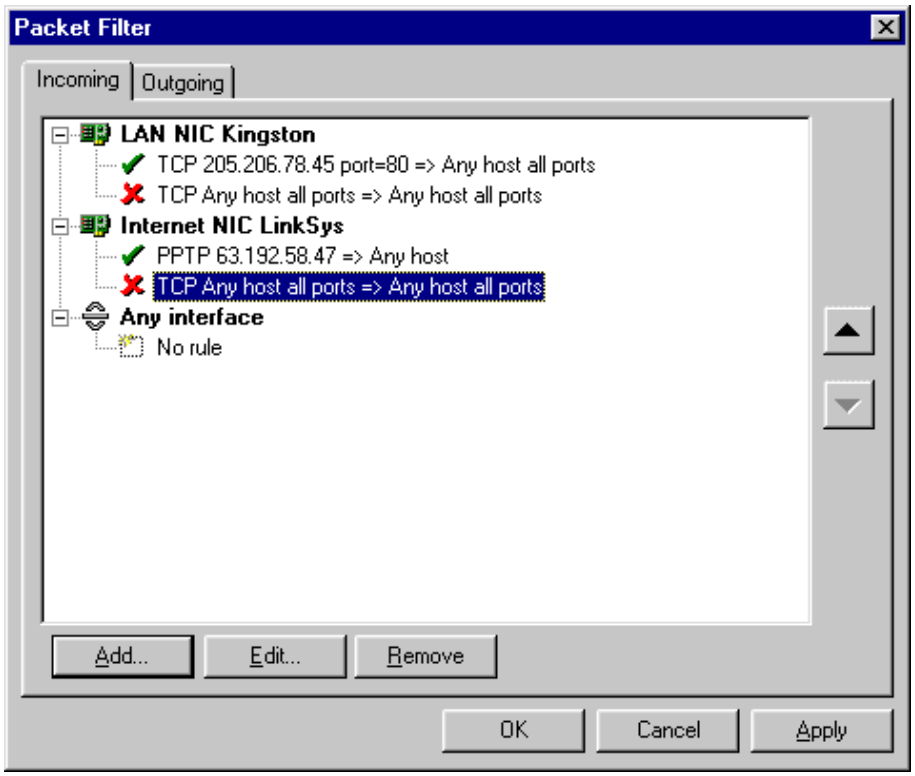
Esempio:

controllo totale sull'accesso degli utenti: l'amministratore di rete desidera che l'accesso alla rete sia soggetto ad autorizzazione. Tuttavia, l'impostazione di molte reti prevede che i server Web o FTP siano a monte di WinRoute, che necessita invece di un accesso pubblico.

Nel caso descritto dall'esempio, la regola vigente sui pacchetti in entrata sarebbe la seguente.

1. Consentire l'accesso ai pacchetti diretti alla porta 80, indipendentemente dall'host di provenienza.
2. Consentire l'accesso ai pacchetti diretti alla porta 21, indipendentemente dall'host di provenienza.
3. Rifiutare tutti gli altri pacchetti.

I pacchetti in arrivo che soddisfino le regole 1 o 2 potranno passare e non verrà applicata la regola 3. In caso contrario saranno rifiutati.



Esempio di gruppo di regole di base per il filtro pacchetto

Regole per i pacchetti in entrata (rispettare l'ordine seguente)

Protocollo	Origine	Destinazione	Tipi ICMP	Azione	Log
UDP	Indirizzo qualsiasi, porta = 53	Indirizzo qualsiasi, porta > 1023		Permesso	
TCP	Indirizzo qualsiasi, tutte le porte	Indirizzo qualsiasi, porta > 1023		Permesso stabilito TCP	
ICMP	Indirizzo qualsiasi	Indirizzo qualsiasi	Risposta echo	Permesso	
IP	Indirizzo qualsiasi	Indirizzo qualsiasi		Ignorare	In finestra

Nota: l'ultima "regola di pulizia" interferirà con gli strumenti per la cattura dei pacchetti di rete utilizzati su questo host.

Esempio di gruppo di regole di base per il filtro pacchetti inentrata HTTP e FTP

Protocollo	Origine	Destinazione	Tipi ICMP	Azione	Log	De
TCP	Indirizzo qualsiasi, tutte le porte	[questo host], porta = 80		Permettere	(Facoltativo)	Au ent acc
TCP	Indirizzo qualsiasi, tutte le porte	[questo host], porta = 21		Permettere	(Facoltativo)	Au cor ent
TCP	Indirizzo qualsiasi, tutte le porte	[questo host], porta = 20		Permettere	(Facoltativo)	Au cor ent (sc pas tut scc

Autorizzazione alla comunicazione su porte specifiche

Applicare le regole seguenti:

- Massima protezione
- Consentire l'accesso al proprio server Web
- Consentire la comunicazione con il proprio server SMTP
- Consentire il prelievo della posta elettronica da Internet tramite il proprio server di posta elettronica

✍ Consentire l'accesso al proprio server FTP

Massima protezione:

Scheda In entrata

Protocollo: TCP, rifiuta tutti i pacchetti in entrata

IP di origine - qualsiasi	IP di destinazione - qualsiasi
Porta di origine - qualsiasi	Porta di destinazione - qualsiasi

Questa regola sarà sempre l'ultima (posizione più bassa) tra tutte le regole disponibili per l'interfaccia.

Per consentire l'accesso da Internet al proprio server Web:

Scheda In entrata

Protocollo: TCP

IP di origine - qualsiasi	IP di destinazione - indirizzo IP del server Web
Porta di origine - qualsiasi	Porta di destinazione - 80

Per consentire l'accesso ad alcuni indirizzi da Internet al proprio server FTP:

Scheda In entrata

Protocollo: TCP

IP di origine - qualsiasi	IP di destinazione - indirizzo IP del server FTP
Porta di origine - qualsiasi	Porta di destinazione - 21

IP di origine - qualsiasi	IP di destinazione - indirizzo IP del server FTP
Porta di origine - qualsiasi	Porta di destinazione - 20

Per consentire al proprio server SMTP di comunicare solo tramite il server d'inoltro SMTP del provider Internet:

Scheda In entrata

Protocollo: TCP

IP di origine - server d'inoltro SMTP del provider	IP di destinazione - indirizzo IP del server SMTP della LAN utente
Porta di origine - qualsiasi	Porta di destinazione - 25

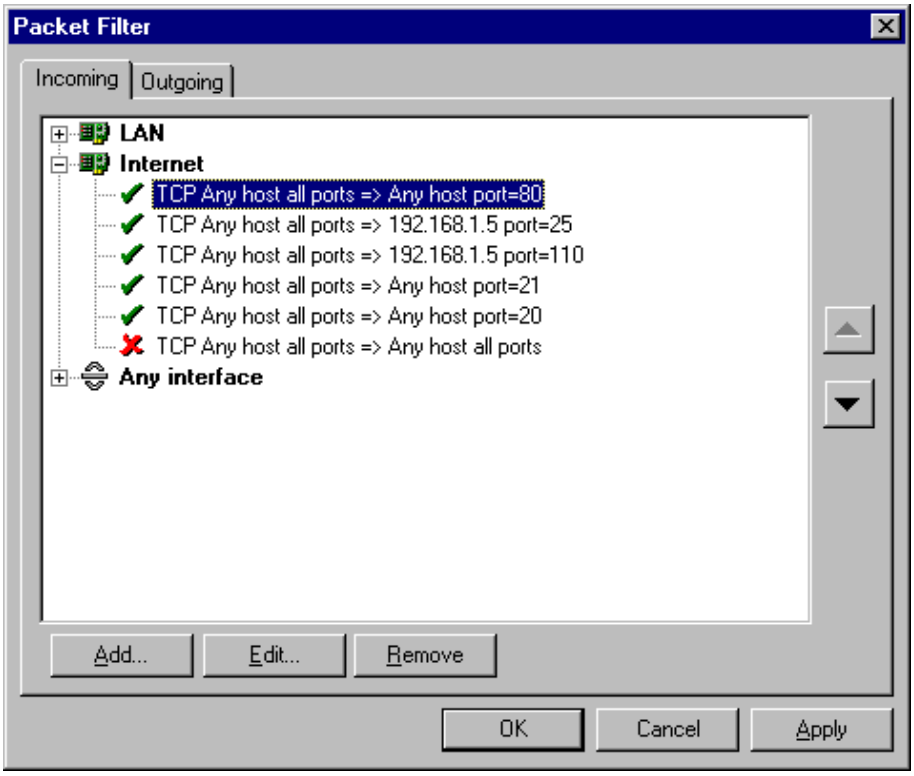
Scheda In uscita

IP di origine - server SMTP dell'utente	IP di destinazione - indirizzo IP del server SMTP del provider
Porta di origine - qualsiasi	Porta di destinazione - 25

Per consentire il prelievo della posta elettronica da Internet tramite il proprio server di posta elettronica

Scheda In entrata

IP di origine - server SMTP dell'utente	IP i destinazione - indirizzo IP del server SMTP della LAN utente
Porta di origine - qualsiasi	Porta di destinazione - 110


Packet Filter
Incoming
Outgoing
LAN
Internet
TCP Any host all ports => Any host port=80
TCP Any host all ports => 192.168.1.5 port=25
TCP Any host all ports => 192.168.1.5 port=110
TCP Any host all ports => Any host port=21
TCP Any host all ports => Any host port=20
TCP Any host all ports => Any host all ports
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

Forzare gli utenti a utilizzare il server proxy

A volte è auspicabile poter utilizzare il **server proxy integrat**di WinRoute, per **controllare**l'attività degli utenti che accedono alle pagine Web, per **imporre restrizioni**di accesso ad alcuni siti Web o per far sì che i client utilizzino la **cache**.

✍✍ ***Nota! Per controllare il traffico Web è anche possibile utilizzare il****filtro pacchetto, **ma il** filtro URL proxy integrato **semplifica le operazioni, perché risolve i nomi dei domini, lasciando all'utente il solo compito di immettere l'URL, senza l'indirizzo IP associato.***

Impostazioni:

è necessari creare due regole di protezione per i pacchetti **in uscita**

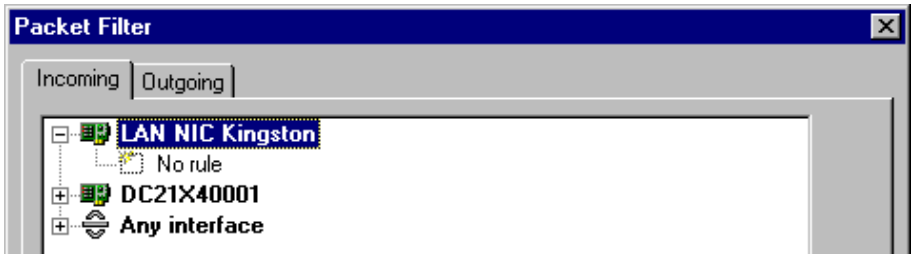
1. **Permettere**i pacchetti in uscita con *destinazione porta 80 e IP di origine* dell'host WinRoute
2. **Rifiutare**tutti i pacchetti in uscita con *destinazione porta 80*

Le regole devono essere applicate secondo l'ordine esatto sopra indicato. WinRoute applica le regole procedendo **dall'alto verso il basso**. Le regole vengono applicate sulla base del metodo "Il primo a entrare è il primo a essere trattato", ovvero: i pacchetti in entrata vengono confrontati con le regole a partire dall'alto e procedendo verso il basso. Viene applicata la prima regola che soddisfa le descrizioni del pacchetto e vengono ignorate le regole successive.

Per configurare le regole:

1. In Amministrazione di WinRoute, scegliere il menu *Impostazioni=>Avanzate=>Filtro pacchetto* e selezionare la scheda *In uscita*.

2. Fare doppio clic sull'interfaccia esterna (Internet). Verrà visualizzato l'elenco delle regole o il messaggio "Nessuna regola".



3. Scegliere *Aggiungi* per aggiungere la nuova regola, che consentirà all'host di WinRoute di stabilire le connessioni con i server Web sulla porta 80.

Protocollo: TCP

Tipo di origine: host

Indirizzo IP: indirizzo esterno del firewall WinRoute (ad es. 204.23.43.26)

Porta di destinazione: uguale a (=) 80, nel riquadro Azione: scegliere Permetti.

4. Fare nuovamente clic su *Aggiungi* per aggiungere una seconda regola, che rifiuterà tutte le altre connessioni TCP alla porta 80.

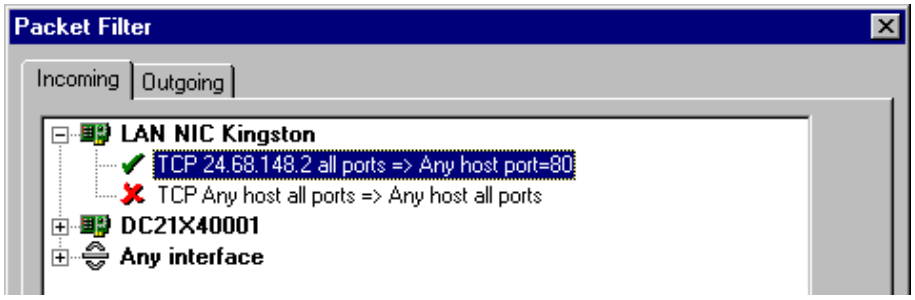
Protocollo: TCP

Tipo di origine: qualsiasi

Porta di destinazione: uguale a (=) 80

Azione: rifiuta.

Se si desidera registrare anche i tentativi, selezionare la casella di spunta "Registra log su file".



✍✍ ***NOTA: se si configurano regole supplementari, procedere sempre dall'ALTO verso il BASSO.***

Impostazione del server di posta elettronica

In questa sezione

Utenti di posta elettronica

Esistono diverse regole di base sugli utenti, sugli indirizzi di posta elettronica e sulle cassette postali di WinRoute.

Un utente = una cassetta postale...

Per ogni utente WinRoute crea una **cassetta postale**, il cui nome corrisponde a quello dell'utente. Se si possiede un dominio Internet registrato e lo si immette in WinRoute, si otterrà automaticamente l'indirizzo di posta elettronica utente@dominio.com.

Un utente = più indirizzi

Per utilizzare più indirizzi di posta elettronica e creare cassette postali generiche quali vendite@..., supporto@...., informazioni@... è possibile ricorrere agli alias. Il numero di combinazioni a disposizione è di fatto illimitato.

Per aggiungere utenti:

1. Scegliere il menu **Impostazioni=>Utenti e gruppi.**
2. Aggiungere gli **utenti.**
3. Se necessario, raccogliere gli utenti in **gruppi.**

Esempio:

supponendo che il dominio di un'azienda sia brutus.com, l'indirizzo di posta elettronica dell'utente di nome Giovanni sarà giovanni@brutus.com. Per le altre opzioni di indirizzo, vedere Alias.

✍✍ ***Nota: le cassette postali sono archiviate in una directory separata, denominata generalmente c:/Program files/WinRoute/Email. le cassette postali vengono create solo DOPO la ricezione del primo messaggio di posta elettronica.***

Invio di posta elettronica agli altri utenti di WinRoute interni alla propria rete

Per inviare messaggi di posta elettronica ad altri utenti **all'interno** della LAN, utilizzare il **nome utente di WinRoute** del destinatario e non l'indirizzo completo di **posta elettronica di Internet**

Esempio: supponendo che il nome utente del destinatario sia Giovanni, e che l'indirizzo completo di posta elettronica sia giovanni@azienda.com, è sufficiente immettere solo *giovanni* nel campo *A:* del messaggio di posta elettronica.

Alias

Se si utilizza l'**indirizzo completo di posta elettronica** di un utente locale, il messaggio verrà inoltrato **tramite** Internet, ovvero al server d'inoltro SMTP di WinRoute e quindi nuovamente a WinRoute. Per evitare inutili passaggi è necessario specificare degli alias.

✍✍ ***Importante! Impostare il PC WinRoute come server di posta elelttronica in uscita (SMTP).***

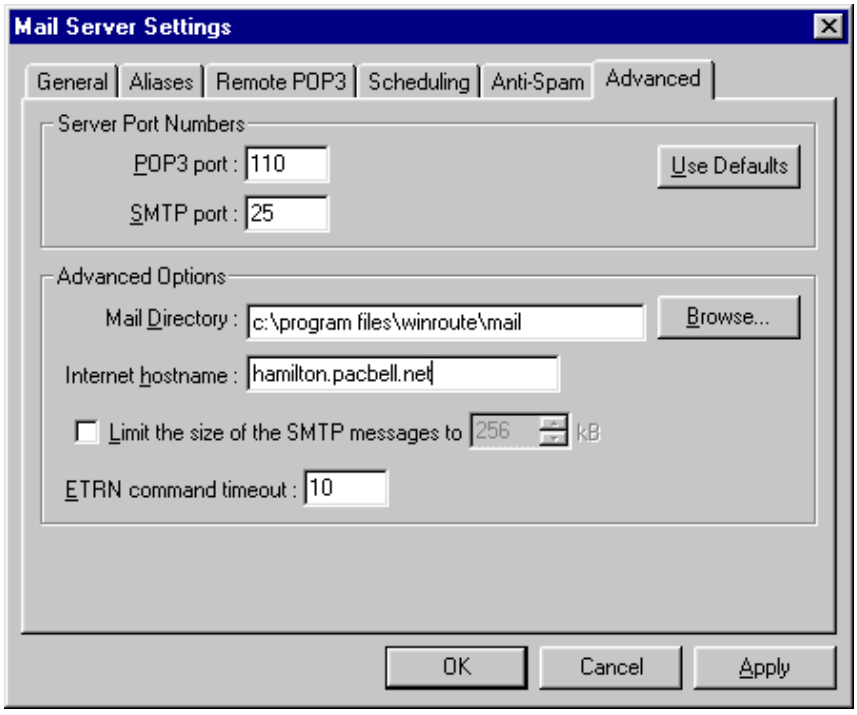
Autenticazione

Autenticazione

Alcuni fornitori di servizi Internet eseguono l'autentic azione della posta elettronica in arrivo per bloccare eventuali messaggi indesiderati. Se questo è il caso, l'utente dovrà supplire loro le necessarie informazioni.

1. Selezionare *Server di posta elettronica->Avanzate.*

2. Immettere il **nome host desiderato** nel campo Nome host Internet. Generalmente è il nome del computer connesso a Internet: ad es. *host.isp.com.*

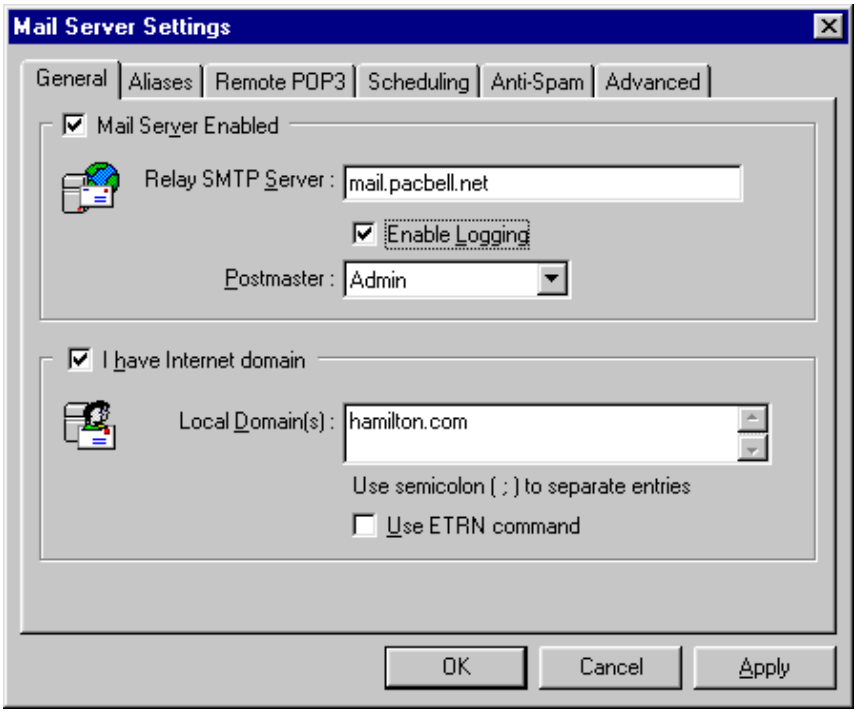


Invio di posta elettronica su Internet

È possibile utilizzare WinRoute come **server SMTP** per la posta in uscita. Per l'invio della posta elettronica WinRoute utilizza il **server d'inoltro SMTP** del provider Internet al posto dei record MX. In altre parole, tutta la posta in uscita transita attraverso l'altro server di posta elettronica specificato dall'utente, che generalmente è il server di posta elettronica del provider Internet. Tutti i client di posta elettronica potranno essere assoggettati alle stesse regole e il server di posta elettronica di WinRoute potrebbe diventare il loro server d'inoltro SMTP.

Per impostare il server d'inoltro SMTP per la posta in uscita:

1. Scegliere il menu *Impostazioni=>Server di posta elettronica.*
2. Immettere il nome del server di posta in uscita del provider Internet nel campo *Server d'inoltro SMTP.*

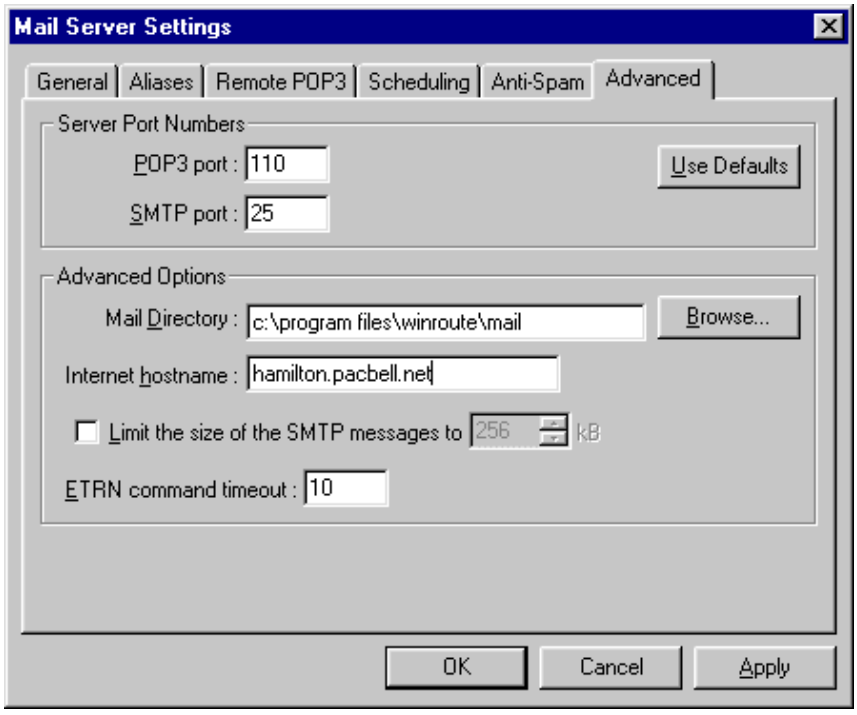


Autenticazione

Alcuni fornitori di servizi Internet eseguono l'autenticazione della posta elettronica in arrivo per bloccare eventuali messaggi indesiderati. Se questo è il caso, l'utente dovrà supplire loro le necessarie informazioni.

1. Selezionare *Server di posta elettronica->Avanzate.*

2. Immettere il **nome host desiderato** nel campo Nome host Internet. Generalmente è il nome del computer connesso a Internet: ad es. *host.isp.com.*



Alias

in **WinRoute** gli **alias** vengono utilizzati per la creazione di indirizzi di posta elettronica supplementari o per la **sostituzione** di indirizzi esistenti.

Tramite l'utilizzo di **alias** è possibile:

- assegnare più indirizzi allo stesso utente
- assegnare un unico indirizzo di posta elettronica a più utenti
- assegnare un unico indirizzo di posta elettronica a un gruppo di utenti
- assegnare più indirizzi allo stesso gruppo.

Esempio:

l'esempio mostra come, di fatto, le combinazioni possibili siano illimitate.

Un'azienda ha due domini:

- azienda.com
- azienda2.com

L'utente *Giovanni* deve poter ricevere la posta ai seguenti indirizzi:

giovanni_oratore@azienda.com

giovanni@azienda2.com

vendite@azienda.com

supporto@azienda.com

La posta indirizzata a *vendite@azienda.com* deve essere recapitata anche al gruppo *[Vendite]*.

Soluzione:

1. Scegliere il menu *Impostazioni=>Server di posta elettronica=>*scheda *Alias*.

2. Aggiungere i seguenti alias:

*giovanni** recapita a *Giovanni* -

In questo modo, tutta la posta proveniente da Internet in cui appaia "giovanni" nel nome del destinatario (*giovanni_oratore@azienda.com* e *giovanni@azienda2.com*) verrà consegnata all'utente *Giovanni.* Ciò servirà inoltre a impedire che la posta inviata dagli utenti locali al destinatario *giovanni@azienda.com* venga smistata attraverso Internet, perché verrà consegnata direttamente nella cassetta postale di Giovanni su WinRoute.

Vendite recapita a *Giovanni* -

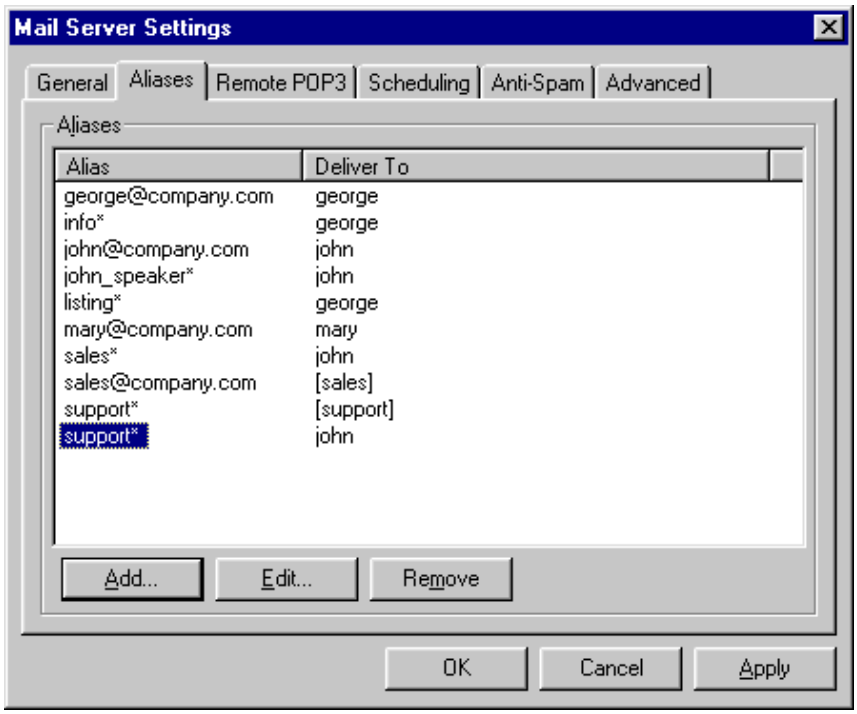
la posta elettronica indirizzata a *vendite@.....* verrà recapitata all'utente *Giovanni*

Supporto recapita a *Giovanni* -

la posta elettronica indirizzata a *supporto@……* verrà recapitata a *Giovanni*

Vendite recapita a *[Vendite]* -

la posta elettronica indirizzata a *vendite@….* verrà recapitata a tutti i membri del gruppo *[Vendite]*



Pianificazione dello scambio di posta elettronica

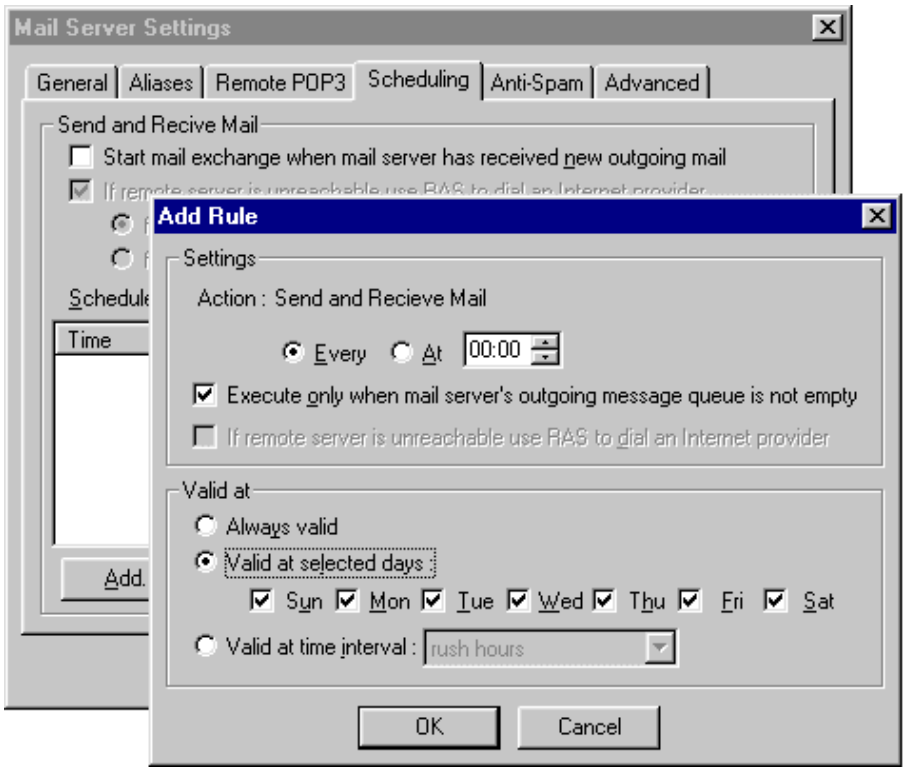
La finestra di dialogo Pianificazione, nelle impostazioni del server di posta elettronica , permette di definire:

- la frequenza con cui controllare la posta presso il provider Internet (POP3 o SMTP che utilizzino ETRN)
- le regole per l'invio della posta elettronica

✍ gli intervalli di tempo durante i quali verranno applicate determinate regole. Per definire gli intervalli di tempo, selezionare il menu *Impostazioni->Avanzate->Intervalli di tempo.*

È possibile scegliere se inviare la nuova posta in uscita non appena abbia raggiunto il server di posta elettronica o se inviarla a intervalli di tempo predefiniti.

È inoltre possibile specificare se il server di posta elettronica debba eseguire chiamate in uscita per ogni nuovo messaggio. Se si seleziona questa opzione, il server di posta di WinRoute stabilirà la connessione ogni volta che gli utenti invieranno nuovi messaggi.



Se si definisce un calendario delle ricezioni, la posta verrà prelevata solo quando specificato. Combinando più regole, il recupero della posta elettronica diventerà un'operazione assolutamente efficiente.

1 Scegliere il menu *Impostazioni->Server di posta elettronica->Pianificazione*

2 Specificare le opzioni desiderate e aggiungere le nuove regole per il controllo della posta.

✍✍ ***Nota! Gli "intervalli di tempo" devono essere impostati nel menu Impostazioni >Avanzate>Intervalli di tempo***

Ricezione della posta elettronica

In questa sezione

Utenti con proprio dominio (SMTP)

Il server di posta elettronica di WinRoute è pienamente compatibile con ***SMTP***[1] e ***POP3***[2]. Se l'utente ha registrato un **dominio Internet** a proprio nome e riceve la posta tramite SMTP e/o WinRoute potrà prelevare la corrispondenza automaticamente anche dall'account presso il proprio provider Internet.

---

[1] Il protocollo **SMTP** (Simple Mail Transfer Protocol) viene utilizzato per la comunicazione diretta tra i server di posta elettronica (quali il server di posta di WinRoute e quello del provider Internet) e per l'invio dei messaggi dal software client di posta elettronica. SMTP è un protocollo "a senso unico", ovvero consente l'invio e la ricezione dei messaggi dal server di posta elettronica, ma non permette di prelevare la posta da altri server.

Il protocollo SMTP funziona sulla **porta 25**. Se si desidera accedere a questo protocollo quando il server di posta elettronica è in esecuzione a valle o sul PC WinRoute (per consentire ad altri server di posta di inviare messaggi o per utilizzare il server per la posta in uscita all'interno della LAN) è necessario eseguire la **mappatura della porta** per il protocollo TCP, con la porta 25 inviata a un indirizzo IP **di classe privata** del PC su cui viene seguito il server di posta elettronica.

[2] Il protocollo **POP3** viene utilizzato principalmente dal software client di posta elettronica per prelevare i messaggi dalle cassette postali di un server di posta conforme a POP3. Il server di posta di WinRoute possiede tale funzionalità, e può pertanto prelevare automaticamente i messaggi da qualunque server di posta conforme a POP3 e distribuirli nelle cassette di posta dei destinatari locali.

POP3 è un protocollo di tipo **TCP** e utilizza la **porta 110** Se si desidera accedere al server di posta in esecuzione a valle o sul computer WinRoute (per prelevare i messaggi provenienti DA Internet) è necessario eseguire la **mappatura alla porta** 110 per inviare i messaggi all'indirizzo IP di **classe privata** del PC su cui viene eseguito il server di posta elettronica.

Se l'utente ha un dominio Internet registrato sul proprio indirizzo IP esterno (pubblico) , WinRoute potrà ricevere la posta elettronica tramite il protocollo SMTP. Immettere il nome del dominio registrato nella scheda Generale della finestra di dialogo Server di posta elettronica.

✍✍ ***Non dimenticare di mappare la porta 25 del protocollo TCP all'indirizzo IP di classe privata della propria cassetta postale in WinRoute! In caso contrario, il protocollo SMTP non consentirà il passaggio della posta dal NAT di WinRoute!***

In base al tipo di connessione Internet, valutare quanto segue:

1 Se si dispone di una connessione permanente

Non sono richieste altre impostazioni oltre all'immissione del nome del dominio.

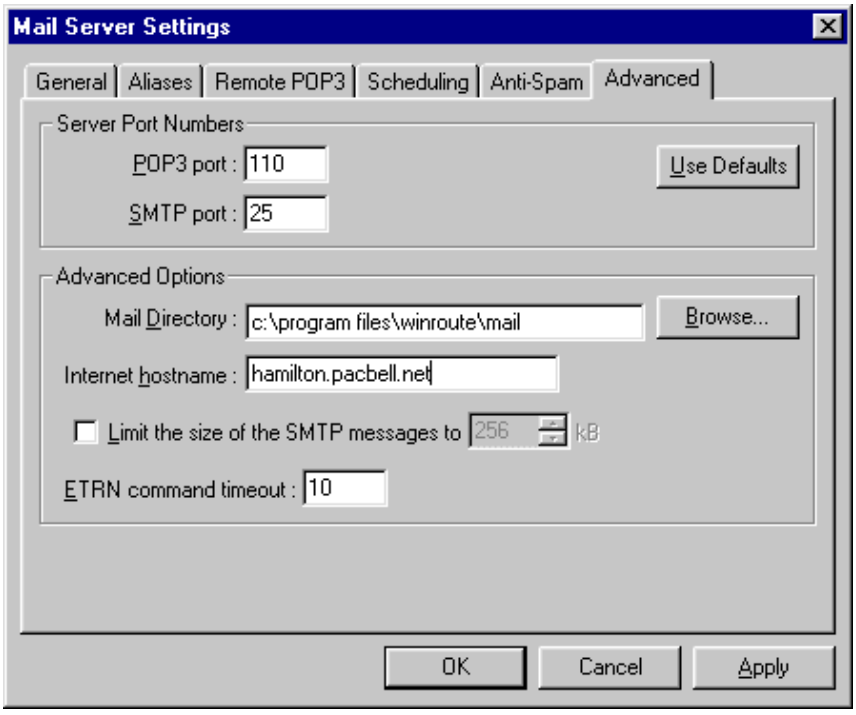
2 Se si dispone di una connessione di Accesso remoto o ISDN (comando ETRN)

Qualora non si disponga di una connessione permanente, la posta elettronica sarà conservata temporaneamente presso il fornitore di servizi Internet. Il trasferimento avverrà durante la connessione. Alcuni fornitori richiedono l'utilizzo del comando ***ETRN***[3] per interrogare la posta. Tale comando è supportato dal server di posta elettronica di WinRoute. Per utilizzarlo, selezionare l'opzione "Utilizza comando ETRN" nella scheda *Generale* della finestra di dialogo **Server di posta elettronica**

[3] Il comando ETRN è utilizzato dai server SMTP per prolungare il periodo di attesa successivo alla connessione, trascorso il quale il server SMTP inizierà la ricerca di nuovi messaggi.

Il comando ETRN viene sempre utilizzato quando il server SMTP non rimane connesso 24 ore al giorno, e la posta indirizzata a tale server debba rimanere archiviata temporaneamente su un altro server SMTP.

Se necessario, è possibile impostare il timeout del comando ETRN (nella scheda *Avanzate*).



Timeout comando ETRN

Questa opzione permette di specificare quanto tempo dopo la connessione il server SMTP di WinRoute dovrà interrogare il server SMTP per la posta.

Domini multipli

Domini multipli

Ad una stessa connessione Internet è possibile assegnate più domini. Se si possiedono più domini, immetterne i nomi, separati da punto e virgola, nella scheda *Generale* del menu *Impostazioni=>Server di posta elettronica.*

Assegnazione di domini multipli

Esistono due soluzioni per ordinare i domini multipli assegnati a una rete:

1 A ciascun dominio viene assegnato un indirizzo IP.

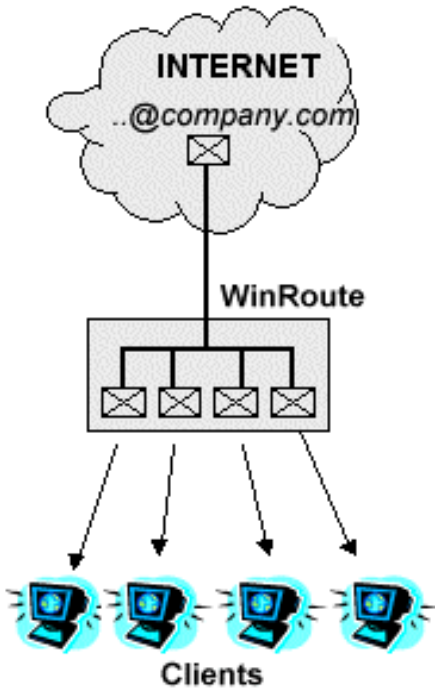
In questo scenario l'utente deve avere più indirizzi IP pubblici mappati all'interfaccia utilizzata da WinRoute per la connessione a Internet. Si dovranno pertanto eseguire più mappature di porte - una per ogni indirizzo IP - con lo stesso indirizzo IP di destinazione del computer WR.

2 Tutti i domini sono associati a un unico indirizzo IP.

Non sono richieste impostazioni particolari oltre alla mappatura della porta 25 per il protocollo TCP, associata all'indirizzo IP locale del computer WinRoute.

Il dominio dell'utente è assegnato a un account POP3

È possibile richiedere al provider Internet di inoltrare a un unico account tutti i messaggi di posta elettronica destinati al proprio dominio. WinRoute controllerà l'account, preleverà gli eventuali messaggi e li distribuirà nelle cassette postali degli utenti locali.

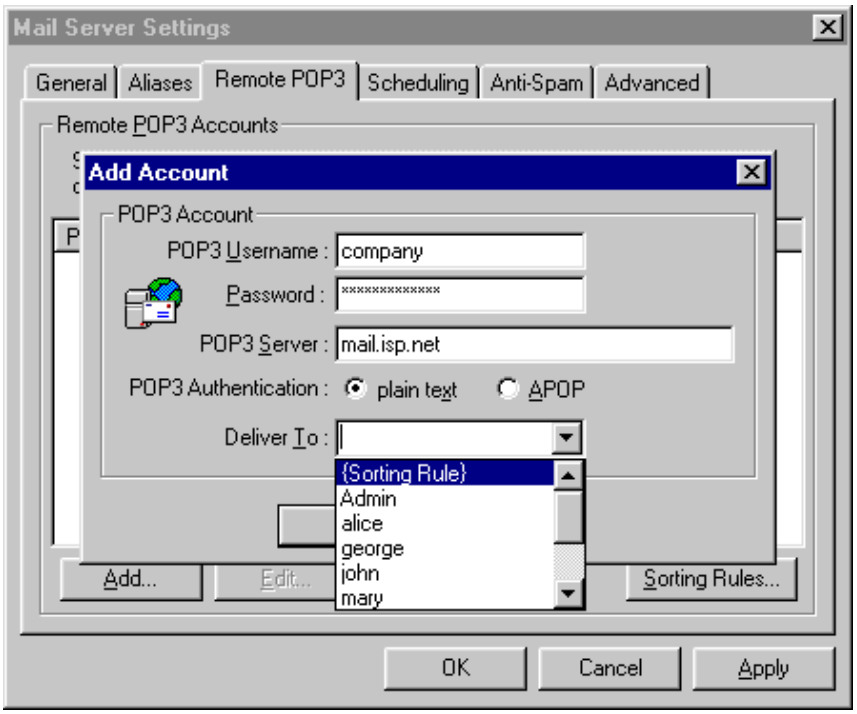


Esempio

Si supponga che la cassetta postale messa a disposizione dal provider Internet per la raccolta dei messaggi sia azienda@mail.isp.net. Anche se il dominio dell'utente fosse azienda.com, tutti i messaggi diretti al suo dominio (vendite@dominio.com, giovanni@dominio.com) arriverebbero alla cassetta postale azienda@mail.isp.net presso il provider Internet.

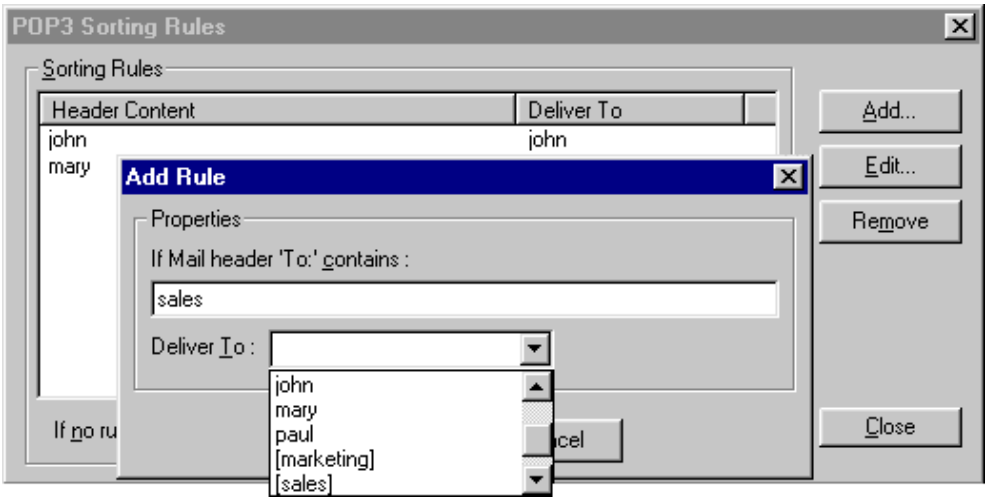
1 Scegliere il menu *Impostazioni=>Server di posta elettronica=>POP3 remoto*, aggiungere il nuovo account e i relativi dettagli.

2 Nel campo "Recapita a:" scegliere "Regole di ordinamento"



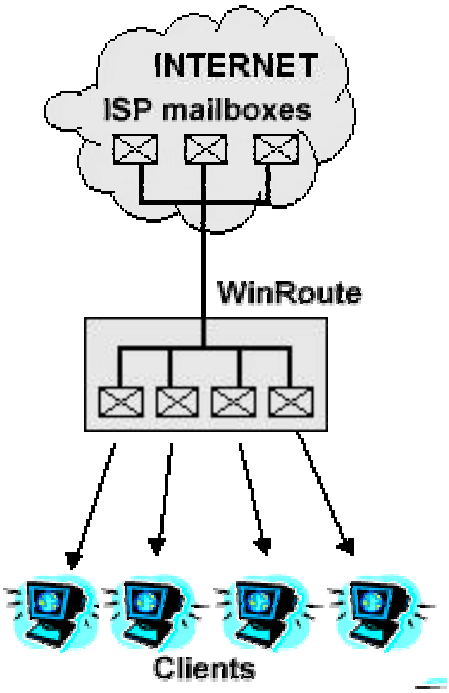
3 Scegliere Regole di ordinamento e aggiungere i nuovi criteri. WinRoute recapiterà i messaggi sulla base dell'indirizzo di posta elettronica del destinatario, di quello del mittente o dell'oggetto del messaggio.

4 Nella stessa finestra di dialogo, scegliere le cassette postali dell'utente o del gruppo di utenti a cui verrà recapitata la posta.



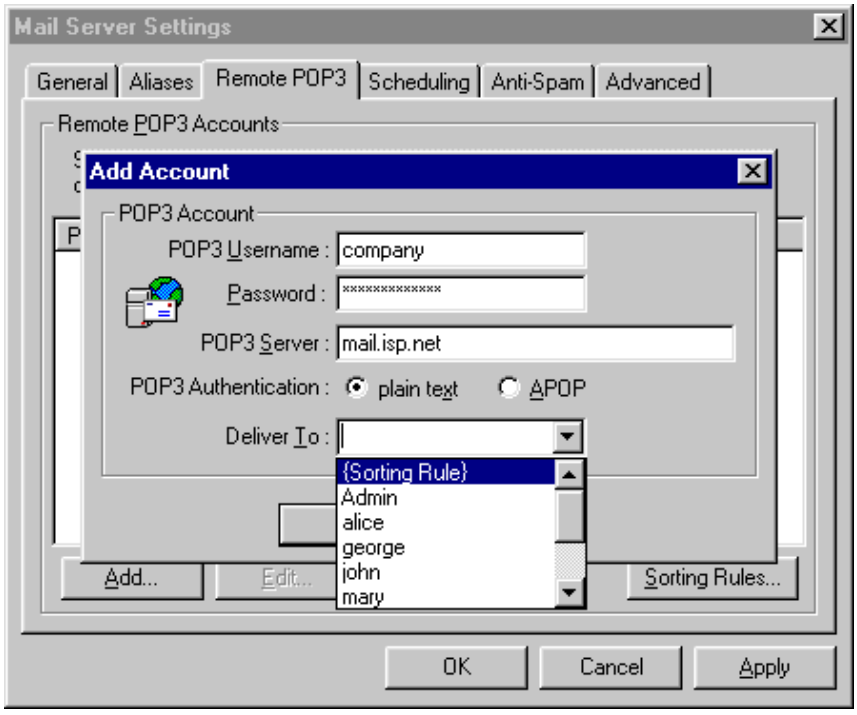
Ricezione della posta elettronica - l'utente possiede più cassette postali presso il provider Internet

WinRoute può controllare più account presso diversi provider Internet e recapitare automaticamente la posta elelttronica nelle cassette postali dei destinatari locali.



1 Scegliere il menu *Impostazioni=>Server di posta elettronica=>POP3 remoto*, aggiungere il nuovo account e i relativi dettagli.

2 Nel campo "Recapita a:" scegliere il destinatario o il gruppo di destinatari.



Impostazioni dell'applicazione client di posta elettronica

In questa sezione

Utilizzo del server di posta di WinRoute

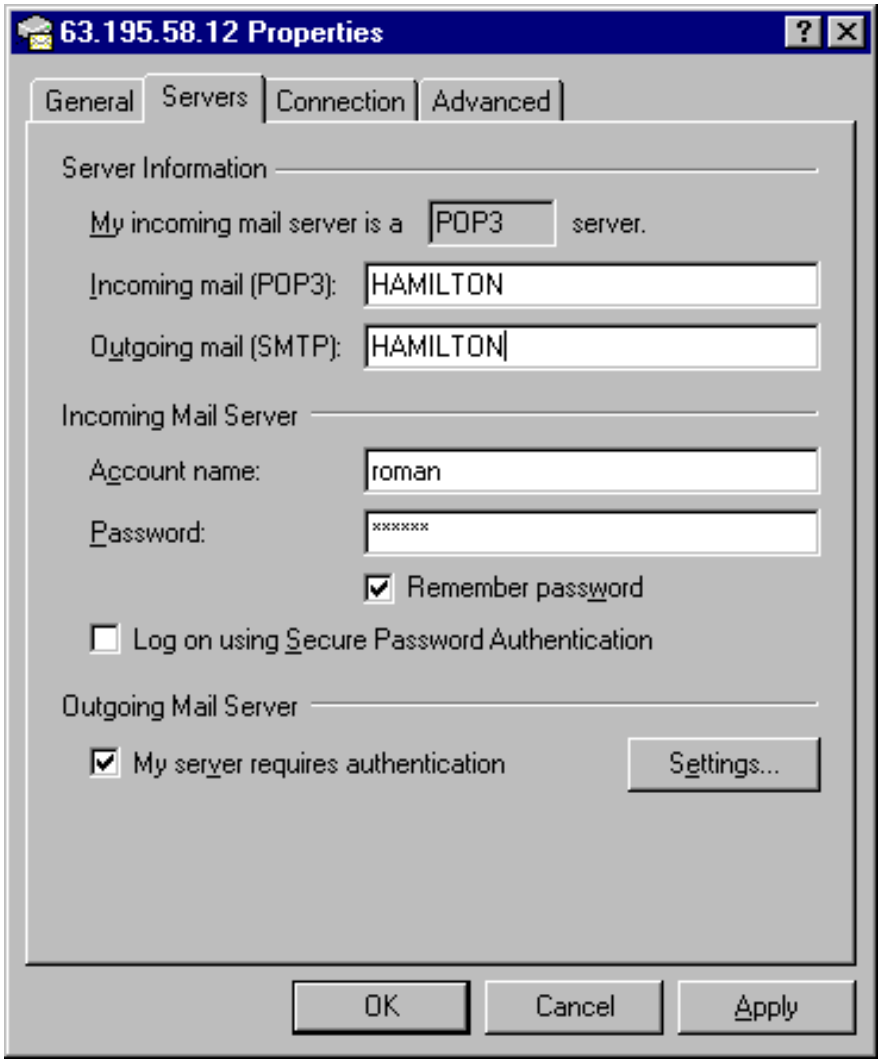
Utilizzo del server di posta elettronica di WinRoute

Per poter utilizzare il server di posta elettronica di WinRoute, è necessario dapprima configurare l'**applicazione di posta elettronica** che si desidera utilizzare. Il computer WinRoute fungerà da server di posta sia per i messaggi **in entrata** sia per quelli **in uscita** Per questo motivo è necessario immettere il nome del computer WinRoute nel campo appropriato dell'applicazione utilizzata per la posta elettronica. Se si verificano dei problemi durante l'invio o la ricezione dei messaggi, si raccomanda per prima cosa di immettere l'indirizzo IP invece del nome del computer. A volte i problemi di questo tipo sono dovuti alla risoluzione DNS nella rete locale, in base alla quale può sembrare che l'utente non stia utilizzando il server DNS di WinRoute.

Esempio:

si supponga che il server di posta elettronica di WinRoute venga eseguito su un computer provvisto di un indirizzo IP pubblico, assegnato dinamicamente, e dell'indirizzo IP privato 192.168.1.1, e si supponga inoltre che il nome del computer sia Rossi (vedere Rete nel Pannello di controllo).

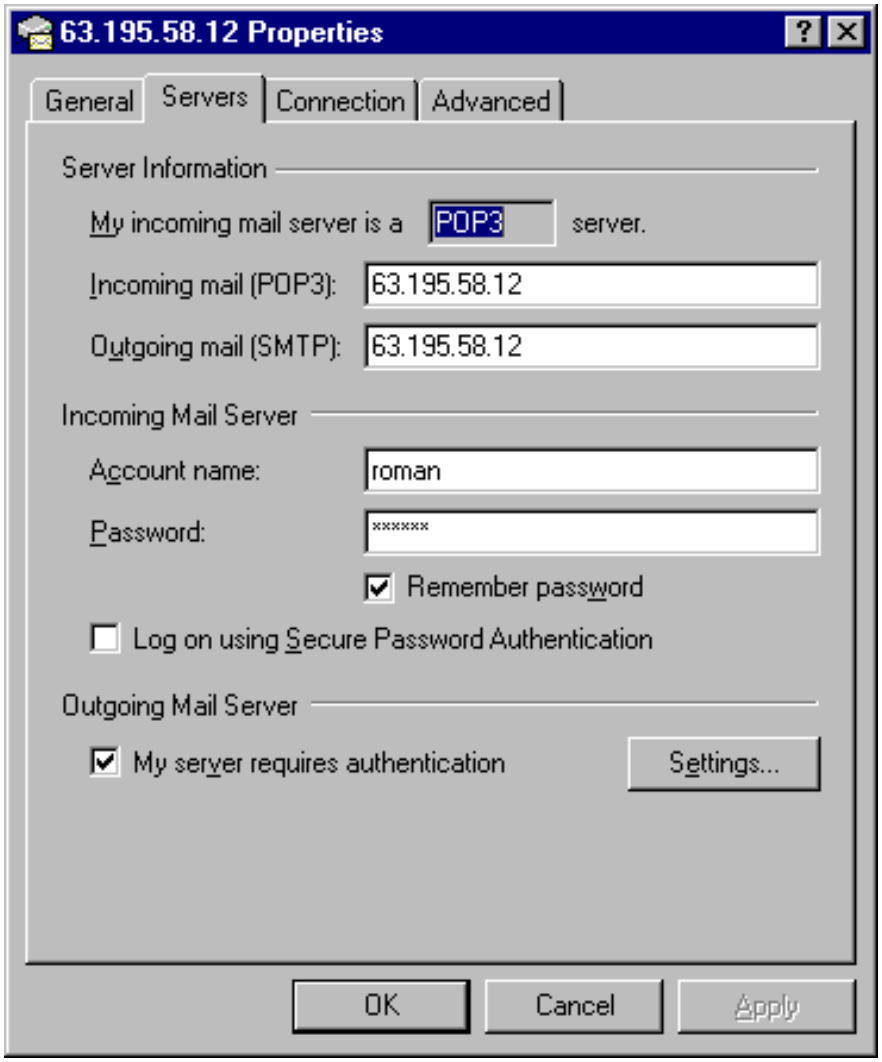
Sarà possibile immettere ROSSI o 192.168.1.1 nei campi In entrata (POP3) e In uscita (SMTP) del server dell'applicativo di posta elettronica.


63.195.58.12 Properties
General
Servers
Connection
Advanced
Server Information
My incoming mail server is a
POP3
server.
Incoming mail (POP3):
HAMILTON
Outgoing mail (SMTP):
HAMILTON
Incoming Mail Server
Account name:
roman
Password:
******
Remember password
Log on using Secure Password Authentication
Outgoing Mail Server
My server requires authentication
Settings...
OK
Cancel
Apply

Ignorare il server di posta elettronica di WinRoute

È possibile ignorare il server di posta elettronica di WinRoute e ricevere o inviare i messaggi direttamente con un client di posta, utilizzando il server del proprio provider Internet.

In questi casi sarà necessario specificare i nomi appropriati dei server di posta elettronica del proprio provider Internet nelle impostazioni dei messaggi in entrata e in uscita.



✍✍ ***Nota! Non impostare l'applicativo client di posta elettronica per l'utilizzo del server proxy! Per accedere a Internet è obbligatorio utilizzare la NAT di WinRoute e impostare l'applicativo client per l'accesso diretto a Internet. L'impossibilità di stabilire lo scambio di posta elettronica significa che NAT non è stata configurata correttamente. Per configurarla correttamente, fare riferimento a*** Elenco di controllo *!*

CAPITOLO 3

ESEMPI DI UTILIZZO

In questo capitolo

Soluzioni IPSEC, NOVELL e PPTP VPN

In questa sezione

IPSEC VPN

WinRoute Pro 4.1 supporta IPSEC in "**modalità tunnel**". La "**modalità tunnel**" supporta tutti i client IPSEC che consentono la modifica dell'indirizzo IP di trasporto.

Nota: WinRoute non supporta l'applicativo client VPN Checkpoint Secure Remote.

Impostazioni di WinRoute:

Crea porta mappata per ESP:

Protocollo: altro 50

IP in ascolto: <non specificato>

IP di destinazione: l'indirizzo IP privato del PC client

È inoltre consigliabile creare una porta mappata per IKE. L'operazione non è obbligatoria se la comunicazione è iniziata ALL'INTERNO di WinRoute ed è diretta a Internet. Alcune implementazioni di IPSEC richiedono tuttavia questa impostazione:

Mappatura porta IKE:

Protocollo: UDP

IP in ascolto: <non specificato>

Porta in ascolto: 500

IP di destinazione: l'indirizzo IP privato del PC client

Porta di destinazione: 500

Esecuzione simultanea di più sessioni IPSEC

Qualora esistano più client IPSEC, sarà necessario utilizzare un indirizzo IP separato per ciascuno di essi. Nota - NAT di WinRoute consente il transito simultaneo del numero di client specificato dall'utente, a condizione che la connessione sia iniziata DALLA rete locale e che ciascun client "utilizzi" un indirizzo IP assegnato all'interfaccia esterna di WinRoute.

Informazioni generali su IPSEC

IPSec è il protocollo crittografico di protezione utilizzato per la comunicazione tra computer.

IPSec utilizza l'algoritmo AH (Authentification Header) o ESP (Encapsulating Security Payload). Il primo esegue solo la verifica dell'identità del mittente e del contenuto del pacchetto. I dati non sono crittografati.

ESP crittografa i dati e consente l'utilizzo della cosiddetta "modalità tunnel", che è simile al protocollo PPTP. Il pacchetto include quindi l'intestazione IP (necessaria per il trasporto) che non è crittografata, e la porzione di dati in cui è contenuto l'intero pacchetto originale crittografato.

Il protocollo IKE (chiamato anche ISAKMP) è utilizzato per l'autenticazione (scambio di chiavi di protezione). Esso viene eseguito sul protocollo UDP della porta 500, utilizzata sia come origine sia come destinazione.

AH si serve del protocollo 51, mentre ESP utilizza il protocollo 50. IPSec può comunicare con l'autorità di certificazione anche con altri protocolli, che non si interfacciano con NAT.

Il protocollo 50 verrà incorporato automaticamente in WinRoute, e ciò renderà superflua la mappatura della porta. La sola condizione richiesta per stabilire automaticamente la connessione sarà che la connessione sia stata iniziata DALLA rete locale.

La maggior parte dei provider IPSec utilizza gli algoritmi MD5 e SHA1 per l'autentificazione e DES, 3DES e Blowfish per la crittografia. IPSec non ha legami stretti con nessun particolare algoritmo, pertanto non soffre di problemi di incompatibilità con le soluzioni proposte dai diversi fornitori.

Novell Border Manager VPN

Utilizzo di WinRoute Pro con Novell BorderManager VPN (IPSEC)

Il presente documento descrive l'impostazione che rende possibile la connessione di una rete locale che utilizzi il protocollo NAT per la condivisione di un unico indirizzo IP fornito dal provider Internet a una rete remota che utilizzi Novell BorderManager Enterprise Server per la connettività VPN.

In conformità a quanto enunciato nel file README.TXT, fornito sul dischetto di installazione di Novell BorderManager VPN Client,

"Non è possibile utilizzare NAT nel percorso tra un client e un server VPN, perché quando i pacchetti IP e IPX vengono incapsulati e crittografati sul client VPN, l'indirizzo IP di origine utilizzato per l'incapsulazione è lo stesso l'indirizzo del client VPN. Il calcolo dell'intestazione di autenticazione IPSEC del pacchetto si basa infatti su questo indirizzo e sull'indirizzo del server VPN di destinazione. Pertanto, se uno dei due indirizzi (quello del client o quello del server VPN) viene modificato da NAT, il calcolo eseguito dal server VPN di destinazione darà esito negativo e il pacchetto verrà rifiutato. Nella maggior parte dei casi , NAT ignorerà i pacchetti IPSEC perché gestisce solamente i pacchetti TCP, UDP e ICMP (Internet Control Message Protocol).

Se le workstation di un'Intranet devono comunicare in modo sicuro con le reti protette da un server VPN su Internet, è consigliabile utilizzare la funzionalità VPN "da sito a sito" di Novell BorderManager Enterprise Edition (al posto della funzionalità VPN "da client a sito")".

Novell BorderManager Enterprise Server costituisce tuttavia una soluzione troppo onerosa per l'utente privato, e richiede inoltre la complessa impostazione di route statiche sulla rete remota a cui si desidera accedere. La soluzione suggerita da Novell non è quindi praticabile per coloro che desiderano collegare la propria rete locale, che utilizza il protocollo NAT, a una rete remota tramite Novell BorderManager VPN.

È però possibile connettere una rete locale con protocollo NAT a una rete remota utilizzando WinRoute Pro e Novell BorderManager VPN Client. Questa configurazione consente a tutti i computer di una rete locale di accedere alle risorse della rete remota una volta che sul router sia stata stabilita la modalità tunnel VPN. Non è richiesta alcuna configurazione della rete remota.

Di seguto sono elencati i passaggi necessari per la configurazione della rete locale.

Passaggio 1: installare e configurare Novell BorderManager VPN Client sul computer che verrà utilizzato come router. Accertarsi che la connessione VPN alla rete remota avvenga correttamente e che le risorse sulla rete remota siano accessibili.

Passaggio 2: installare WinRoute Pro sul router. Seguire le istruzioni di configurazione di WinRoute rilasciate nella Guida per l'amministratore, e configurare i computer della rete locale per il funzionamento con WinRoute Pro. Utilizzare la configurazione standard per la condivisione di un unico indirizzo IP. Accertarsi che le risorse su Internet siano accessibili da tutti i computer della rete locale.

Passaggio 3: per accedere alle risorse sulla rete remota, eseguire lNovell BorderManager VPN Client sul router e connettersi alla rete remota.

Questa soluzione è possibile grazie all'architettura di WinRoute Pro. La traduzione dell'indirizzo viene effettuata prima dell'instradamento del pacchetto alla scheda di rete virtuale, perché avviene al livello dell'IPSEC, e i pacchetti inviati al server VPN mantengono il vero indirizzo IP di origine. Durante il percorso di ritorno, i pacchetti ricevuti dalla scheda di rete virtuale attraversano il livello in cui viene eseguita la traduzione dell'indirizzo e sono instradati correttamente al computer della rete locale.

Le limitazioni di questa impostazione consistono nel fatto che la connessione VPN deve essere eseguita manualmente sul router, e che il timeout della connessione VPN scatta dopo un certo periodo di inattività, secondo il valore impostato sul server VPN. Inoltre, i pacchetti IPX non vengono instradati anche se il protocollo IPX del tunnel VPN è stato abilitato. Il tunnel IPX sarà quindi disponibile solo sul router.

Nel complesso, questa impostazione rappresenta una soluzione efficace, anche in termini di rapporto tra costi e benefici, per collegare una rete locale che utilizzi il protocollo NAT a una rete remota che utilizzi Novell BorderManager VPN.

Esecuzione di un server PPTP a valle di NAT

Per poter eseguire un server PPTP sulla rete gestita da WinRoute (incluso il computer su cui è in esecuzione WinRoute) occorre eseguire la mappatura della porta.

*Importante: se il server VPN è installato sul computer host di WinRoute, è necessario mappare l'IP di destinazione all'**indirizzo pubblico** non a quello privato. L'IP in ascolto non deve essere specificato.*

Per la connessione di controllo:

- Protocollo: TCP
- IP in ascolto:

- Porta in ascolto: 1723
- IP di destinazione: indirizzo IP del proprio server PPTP (ad es. 192.168.1.12)
- Porta di destinazione: 1723

Per i pacchetti GRE (PPTP):

- Protocollo: PPTP
- IP in ascolto:
- IP di destinazione: indirizzo IP del proprio server PPTP (ad es. 192.168.1.12)

Dopo avere mappato la porta secondo le indicazioni sopra riportate, sarà possibile eseguire il server PPTP da qualunque punto a valle di WinRoute, INCLUSO il computer SU CUI WinRoute è in esecuzione. Gli utenti potranno accedere al server PPTP con una normale connessione all'indirizzo IP esterno (pubblico) della rete. Quando i pacchetti raggiungeranno il computer WinRoute, verranno automaticamente inoltrati al computer di competenza al di là del firewall.

Esempio di soluzione PPTP

WinRoute è la soluzione ottimale, anche sotto il profilo del rapporto tra costi e benefici, per la creazione di una rete WAN di collegamento tra filiali e casa madre tramite Internet. Nel presente documento si parte del presupposto che i lettori possiedano una conoscenza di base delle reti e di Windows NT.

La creazione di una WAN richiede pochi, semplici passaggi:

1 Controllare l'ambiente:

server NT a entrambe le estremità

WinRoute Pro installato su entrambe le estremità

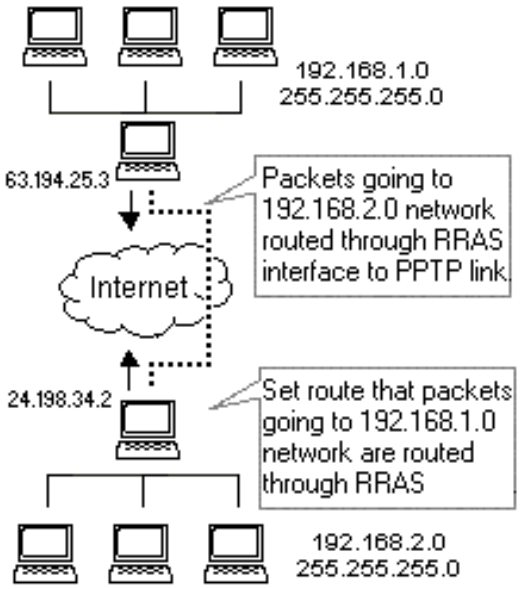
RRAS (Stealhead) installato su entrambi i server NT

2 Creare una route statica su entrambi i server NT, specificando che i pacchetti diretti alla rete opposta devono transitare dall'interfaccia RRAS. Visualizzando le proprietà TCP, nel registro di debug di Amministrazione di WinRoute, sarà possibile leggere il nome dell'interfaccia di accesso remoto tra le possibili opzioni.

3 In Amministrazione di WinRoute, scegliere Tabella interfacce e visualizzare le proprietà dell'interfaccia RAS utilizzata per il collegamento PPTP. Accertarsi che NAT non venga eseguita sull'interfaccia.

4 Nella scheda RAS delle proprietà dell'interfaccia RAS, scegliere la connessione PPTP. Se la connessione RAS non compare tra le scelte possibili, accertarsi di avere selezionato la rubrica giusta. Scegliere il menu *Impostazioni->Avanzate->Varie* e selezionare la rubrica RAS corretta.

5 Provare la connessione - deve essere possibile eseguire il ping sulla rete opposta e, nel contempo, accedere a Internet.



Esecuzione dei client PPTP a monte di NAT

Non sono richieste impostazioni particolari per eseguire i client PPTP a monte di WinRoute (NAT) quando si accede al server PPTP da Internet. È possibile stabilire qualsiasi numero di connessioni simultanee si ritenga necessario.

Soluzione DNS

In questa sezione

Server DNS sul PC WinRoute

L'esecuzione di un vero server DNS su un PC WinRoute non comporta particolari difficoltà. Tutte le richieste DNS presentate al server DNS otterranno risposta dal regolare indirizzo IP Internet associato a quel dominio. L'indirizzo IP deve essere associato all'interfaccia di rete che collega il PC WinRoute a Internet; i server WWW saranno in ascolto sulle interfacce pubblica e privata.

Supponendo che il PC locale invii una richiesta DNS per risolvere l'indirizzo www.miodominio.com, otterrà in risposta l'indirizzo IP pubblico associato a questo dominio e connetterà il server Web a un indirizzo IP (assegnato all'interfaccia Internet).

✍✍ ***Accertarsi che la porta per le richieste DNS sia stata mappata, anche se il server DNS viene eseguito sul PC WinRoute! Mappare il protocollo UDP e la porta 53 all'indirizzo IP dell'interfaccia Internet.***

Server DNS a valle del PC WinRoute

È possibile eseguire un vero server DNS su qualunque PC di una rete locale. Di seguito sono indicate le impostazioni necessarie per la mappatura della porta:

Protocollo: UDP

IP in ascolto: non specificato, o l'indirizzo IP associato al server DNS (mappato come secondo indirizzo IP)

Porta in ascolto: 53

IP di destinazione: l'indirizzo IP privato del PC con il server DNS

Porta di destinazione: 53

Server DNS e WWW a valle di NAT

Se si eseguono i server DNS e WWW sulla stessa rete privata, sarà necessario rispondere ad alcuni quesiti:

Come gestire le richieste DNS per www.miodominio.com provenienti dalla LAN? Come otterranno risposta dall'indirizzo IP privato del server Web, mentre le richieste DNS provenienti da Internet avranno un regolare indirizzo IP Internet associato a www.miodominio.com?

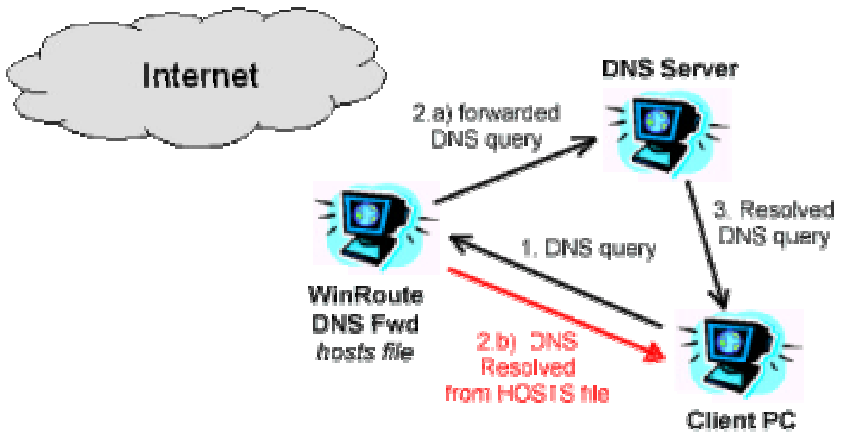
La risposta è semplice: sarà sufficiente utilizzare il **server d'inoltro DNS** integrato in WinRoute, che dovrà essere impostato come server DNS per tutti i PC client. Sul PC WinRoute sarà inoltre necessario eseguire le seguenti impostazioni:

- Attivare il server d'inoltro DNS di WinRoute.
- Modificare il file HOSTS:

  aggiungere un record che specifichi www.miodominio.com come indirizzo IP privato (quello utilizzato per l'esecuzione del server - ad es. 10.10.10.8). Il file HOSTS si trova nella directory principale di Windows (ovvero la directory in cui è stato installato Windows - c:\Windows o c:\win98 ecc.). È possibile accedere al file HOSTS anche dalla finestra di dialogo del server DNS di WinRoute, facendo clic su "Modifica file HOSTS".

Funzionamento

Tutte le richieste DNS inviate dai computer client della LAN verranno dapprima risolte dal server d'inoltro DNS di WinRoute, che le confronterà con i record del file HOSTS. Se esistono record corrispondenti, le informazioni in essi contenute saranno utilizzate per rispondere alle richieste (nello scenario dell'esempio, l'indirizzo IP privato).



Qualora il file HOSTS non contenga record corrispondenti, le richieste verranno confrontate con i record nella cache DNS di WinRoute (inclusa nel server d'inoltro DNS di WinRoute). Se anche la cache DNS non conterrà record corrispondenti, le richieste verranno inoltrate al server DNS preposto alla risposta, secondo le impostazioni eseguite nel server d'inoltro DNS di WinRoute.

Tutte le richieste DNS provenienti da Internet verranno inoltrate direttamente al server DNS, secondo le impostazioni eseguite in Mappatura porta, e risolte in base ai record in esso contenuti.

✍✍ ***Nota! Nello scenario sopra descritto non è possibile eseguire il server DNS sullo stesso computer su cui viene seguito WinRoute. Questo perché entrambi i servizi, vale a dire d'inoltro DNS di WinRoute e il server DNS dell'utente, utilizzano la stessa porta UDP 53. Se venissero eseguiti sullo stesso computer, provocherebbero un errore irreversibile del sistema.***

Problemi DNS

Esecuzione dei server Web (HTTP, ecc.) e DNS sulla stessa rete privata a valle di WinRoute NAT

È possibile eseguire un server Web con il dominio www.miodominio.com a valle di NAT, ed eseguire il server DNS sulla stessa rete per la risoluzione del nome.

Esecuzione di un server Web (HTTP, ecc.) sul PC WinRoute

Se si esegue un server Web sul PC WinRoute, le richieste locali non daranno mai problemi. Tutte le richieste DNS di www.qualunque.com in arrivo sul server DNS dell'utente saranno risolte con il normale indirizzo IP Internet associato al dominio. L'indirizzo IP dovrà essere associato all'interfaccia di rete che collega il PC WinRoute a Internet, e i server WWW potranno essere messi in ascolto sia sull'interfaccia pubblica sia su quella privata.

Se il PC locale invia una richiesta DNS per risolvere www.qualunque.com, otterrà un indirizzo IP pubblico associato al dominio, che consentirà di connettere il server Web all'indirizzo IP (assegnato all'interfaccia Internet secondo la procedura sopra descritta).

Esecuzione di un server Web (o FTP, ecc.) su un PC a monte di WinRoute

È possibile eseguire il server Web su un PC a monte di WinRoute (ad es. con indirizzo privato 10.10.10.8). Il server Web con www.miodominio.com è fisicamente all'indirizzo IP privato 10.10.10.8, ma la richiesta DNS dell'utente verrà risolta con un indirizzo IP regolare (ad es. 206.86.181.25) che verrà associato al dominio.

Il browser o il client ftp dell'utente approcceranno l'indirizzo pubblico, dove non ci sono server in esecuzione, perché il server Web è all'interno della rete.

Soluzione

Per risolvere il problema è necessario utilizzare il **server d'inoltro DNS** integrato in WinRoute come server DNS per tutti i computer dell'utente.

Nel file **HOSTS** dovrà essere aggiunta una nuova voce, per specificare che **www.miodominio.com** è operante all'indirizzo IP **interno** (classe privata) appropriato. In questo modo il server d'inoltro DNS dell'utente cercherà la risposta nel file HOSTS prima di inviare la richiesta DNS al server standard.

Ogniqualvolta gli utenti invieranno una richiesta di **www.miodominio.com**, in risposta verrà indicato l'indirizzo locale appropriato.

Server WWW, FTP, DNS e Telnet a valle di WinRoute

In questa sezione

Esecuzione di un server WWW a valle di NAT

Per eseguire un server Web a valle di NAT:

1. Scegliere il menu *Impostazioni ->Avanzate ->Mappatura porte*
2. Aggiungere una nuova mappatura:

   Protocollo: TCP

   IP in ascolto: non specificato o l'indirizzo IP associato al dominio. L'indirizzo IP deve essere associato all'interfaccia.

   Porta in ascolto: 80

   IP di destinazione: immettere l'indirizzo IP del server Web (ad es. 192.168.1.10).

   Porta di destinazione: 80

Gli utenti che accederanno a questi servizi utilizzeranno il nome di dominio o l'indirizzo IP pubblico della rete. Dopo che i pacchetti avranno raggiunto WinRoute, verranno deviati automaticamente verso il computer interno con l'indirizzo IP appropriato.

Esecuzione del server DNS a valle di NAT

Il server d'inoltro DNS integrato in WinRoute trasmette le richieste di risoluzione dei nomi di dominio a un server DNS regolare. Infatti, pur essendo in grado di risolvere le richieste DNS locali (quando viene utilizzato il nome del computer locale), non può risolvere richieste DNS quali *www.qualunque.com,* che verranno pertanto **trasferite** al **server DNS** dal **server d'inoltro DNS**

Esecuzione del server DNS a valle di NAT (WinRoute)

Per eseguire un server DNS a valle di NAT/WinRoute, è necessario impostare la mappatura della porta come di seguito descritto. I server DNS comunicheranno tra loro attraverso il protocollo **UDP** sulla **porta 53** Senza le necessarie impostazioni, il server DNS non funzionerà correttamente. Se il server DNS viene eseguito sullo stesso computer su cui è eseguito WinRoute, il modulo di ispezione di WinRoute eseguirà NAT **PRIMA** che i pacchetti raggiungano una qualunque applicazione, incluso il server DNS.

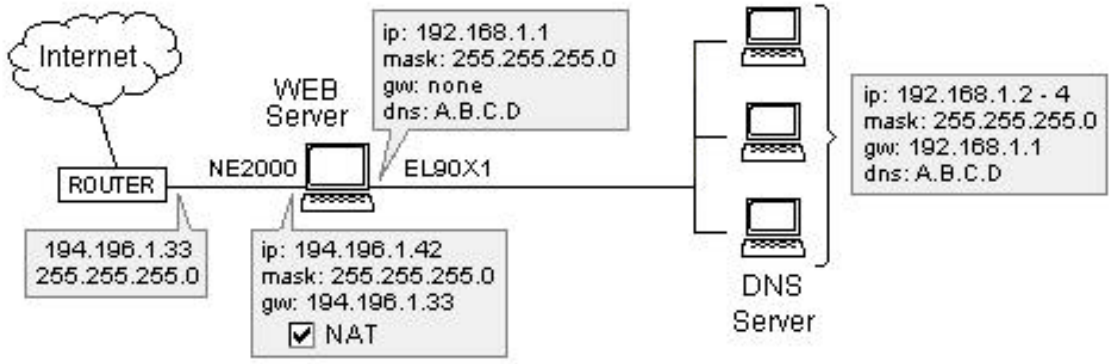
Protocollo: UDP

IP in ascolto: non specificato o l'indirizzo IP pubblico del server DNS che si desidera utilizzare.

Porta in ascolto: 53

IP di destinazione: indirizzo IP pubblico o privato del server del nome di dominio

Porta di destinazione: 53



✍✍ ***Nota!*** *Non è possibile* ***eseguire il server DNS sullo stesso computer su cui viene seguito WinRoute, perché entrambi i servizi utilizzano il protocollo UDP e la porta 53. Se venissero eseguiti sullo stesso computer, provocherebbero un errore irreversibile del routing IP. È tuttavia possibile disattivare il server d'inoltro di WinRoute se si desidera eseguire il server DNS sul PC WinRoute.***

Esecuzione di un server FTP a valle di NAT

Per eseguire un server FTP a valle di NAT:

1. Scegliere il menu *Impostazioni ->Avanzate ->Mappatura porte*
2. Aggiungere una nuova **mappatura porta**

   Protocollo: TCP

   IP in ascolto: non specificato o l'indirizzo IP associato al dominio, che deve essere associato all'interfaccia Internet.

   Porta in ascolto: 21

   IP di destinazione: immettere l'indirizzo IP del server FTP (ad es.192.168.1.10).

   Porta di destinazione: 21

Esecuzione di un server FTP con una porta non-standard:

mappare la porta in modo che corrisponda alla porta utilizzata dal server FTP.

Esecuzione del server di posta elettronica a valle di NAT

Per eseguire il server di posta elettronica a valle di WinRoute è necessario mappare due porte: una per il protocollo SMTP (che viene eseguito sulla porta 25) e una per il protocollo POP3 (che viene eseguito sulla porta 110). Ciò consentirà agli altri server SMTP di raggiungere il server SMTP dell'utente, che a sua volta sarà in grado di prelevare la posta elettronica da Internet tramite il protocollo POP3.

La mappatura delle porte è obbligatoria se il server di posta elettronica viene eseguito sul computer WinRoute, perché il modulo di ispezione di WinRoute, che opera al di sotto dello stack TCP, e i pacchetti vengono scambiati/rifiutati prima di raggiungere il sistema operativo.

Protocollo SMTP:

Protocollo: TCP

IP in ascolto:

Porta in ascolto: 25

IP di destinazione: immettere l'indirizzo IP del server di posta elettronica SMTP (ad es. 192.168.1.10)

Porta di destinazione: 25

Protocollo POP3:

Protocollo: TCP

IP in ascolto:

Porta in ascolto: 110

IP di destinazione: immettere l'indirizzo IP del server di posta elettronica POP3 (ad es. 192.168.1.10)

Porta di destinazione: 110

Esecuzione del server Telnet a valle di NAT

Telnet trova largo impiego presso molte aziende che operano a distanza, in particolare con i server AS 400.

Per eseguire un server Telnet a monte di WinRoute è necessario impostare la mappatura della porta per il protocollo TCP; sulla porta 23. Non sono richieste impostazioni particolari per eseguire il client Telnet che accede al server Telnet su Internet.

Protocollo: TCP

IP in ascolto: non specificato o l'IP del server Telnet

Porta in ascolto: 23

IP di destinazione: immettere l'insdirizzo IP del server Telnet (ad es. 192.168.1.10)

Porta di destinazione: 23

Problemi FTP legati all'utilizzo di porte non standard

In questa sezione

Accesso a un server FTP con porte non-standard

Se si opera a valle di WinRoute, e si cerca di accedere a un server FTP con un numero di porta diverso da 21, non si riceverà l'elenco delle directory. Perché l'operazione sia comunque possibile, è necessario procedere come di seguito indicato:

1. Andare al PC WinRoute.
2. Disabilitare WinRoute.
3. Scegliere il menu Avvio->Esegui sul desktop.
4. Digitare regedit per accedere all'editor di registro.
5. Trovare HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Module/0
6. Modificare SpecParams in modo che il valore corrisponda al numero di porta del server FTP a cui si desidera accedere.

7 Riabilitare WinRoute.

In questo modo gli utenti a monte di WinRoute potrà accedere a un server FTP di Internet con porta non standard.

✍✍ ***Nota! È possibile specificare più porte, separando i valori con uno spazio.***

Server FTP a valle di WinRoute con porta non standard

In alcune circostanze, come ad esempio nel caso di un client aziendale protetto da firewall, le restrizioni di accesso FTP imposte all'utente potrebbero essere solo di tipo **passivo**. Se il server FTP a valle di WinRoute utilizza una porta non standard, non sarà possibile stabilire accessi dalla modalità **passiva,** perché WinRoute (in base all'impostazione predefinita) considera la porta 21 destinata all'FTP; pertanto, qualora un utente desideri utilizzare una porta diversa, sarà necessario modificare le impostazioni di WinRoute. La procedura di seguito descritta serve a correggere il problema e a consentire l'accesso in modalità **passiva**

1 Andare al PC WinRoute.

2 Disabilitare WinRoute.

3 Scegliere il menu Avvio->Esegui sul desktop

4 Digitare regedit per accedere all'editor di registro.

5 Trovare HKEY_LOCAL_MACHINE/SOFTWARE/TinySoftware/WinRoute/Mport. Dovrebbero essere visualizzate delle sottocartelle contenenti le informazioni corrispondenti alle mappature delle porte. Se non ci sono sottocartelle, significa che le porte non sono state mappate.

6 Trovare la cartella contenente la mappatura porta relativa alla porta utilizzata dal server FTP.

7 Modificare la chiave *"flags"* in '1'

8 Modificare la chiave *"NatApp"* in 'FTP'

9 Riabilitare WinRoute.

Le impostazioni sopra descritte "indicheranno" a WinRoute che i pacchetti in entrata sulla porta definita utilizzano il FTP e WinRoute provvederà a far sì che questo complesso protocollo transiti senza problemi.

Reti speciali

In questa sezione

Reti Token Ring

Connessione alle reti Token Ring

Token Ring è un tipo di rete molto particolare. Supponendo che solo utenti professionisti la utilizzino, di seguito non verranno date spiegazioni dettagliate.

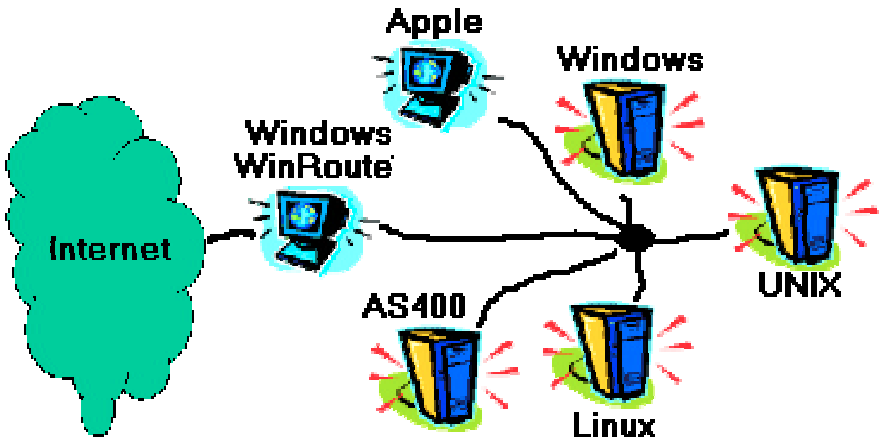
- Impostare a 1500 l'MTU (unità massima di trasmissione) di tutti i computer della rete Token Ring.
- Sul computer WinRoute, andare al menu Impostazioni->Avanzate->Varie e selezionare l'opzione "Supporto Token Ring abilitato"
- Seguire le altre istruzioni di impostazione specifiche per ciascun tipo di connessione Internet.

Ambiente operativo multisistema (Linux, AS400, Apple)

Connessione di ambienti operativi multipli (Linux, Unix, AS400, Apple)

WinRoute è idoneo per la connessione a Internet di ambienti operativi eterogenei. WinRoute agisce da router software, e come tale supporta qualsiasi ambiente operativo TCP/IP standard.

✍✍ ***NOTA: WinRoute deve essere eseguito su un PC su cui sia installato un sistema operativo Windows 95/98/NT. UNIX può essere utilizzato come sistema client.***



Connessione di reti multiple

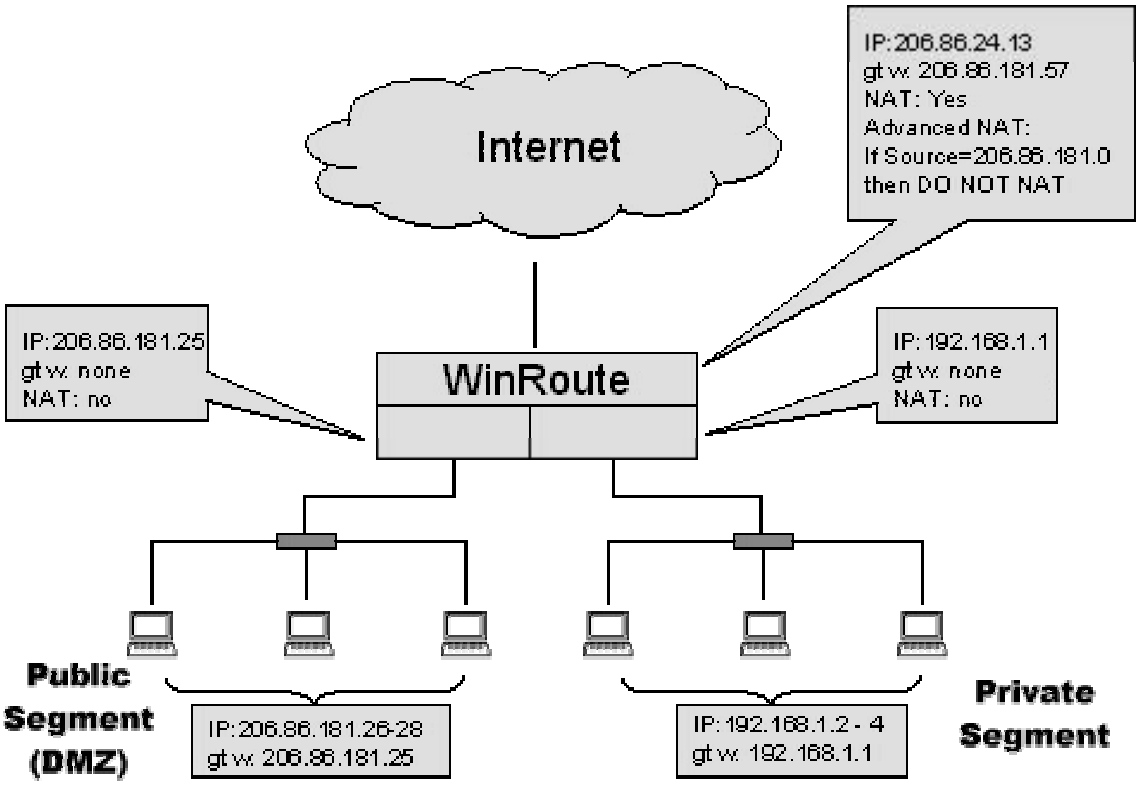
In questa sezione

Connessione di segmenti pubblici e privati (DMZ)

Un segmento privato si compone di più computer che utilizzano indirizzi Internet di tipo privato. Tali indirizzi sono dedicati alle reti private e non possono essere utilizzati per Internet. Per questo motivo è necessario che WinRoute traduca gli indirizzi privati in indirizzi pubblici, per consentire la connessione a Internet. I computer con indirizzi privati non sono accessibili direttamente dall'esterno (Internet).

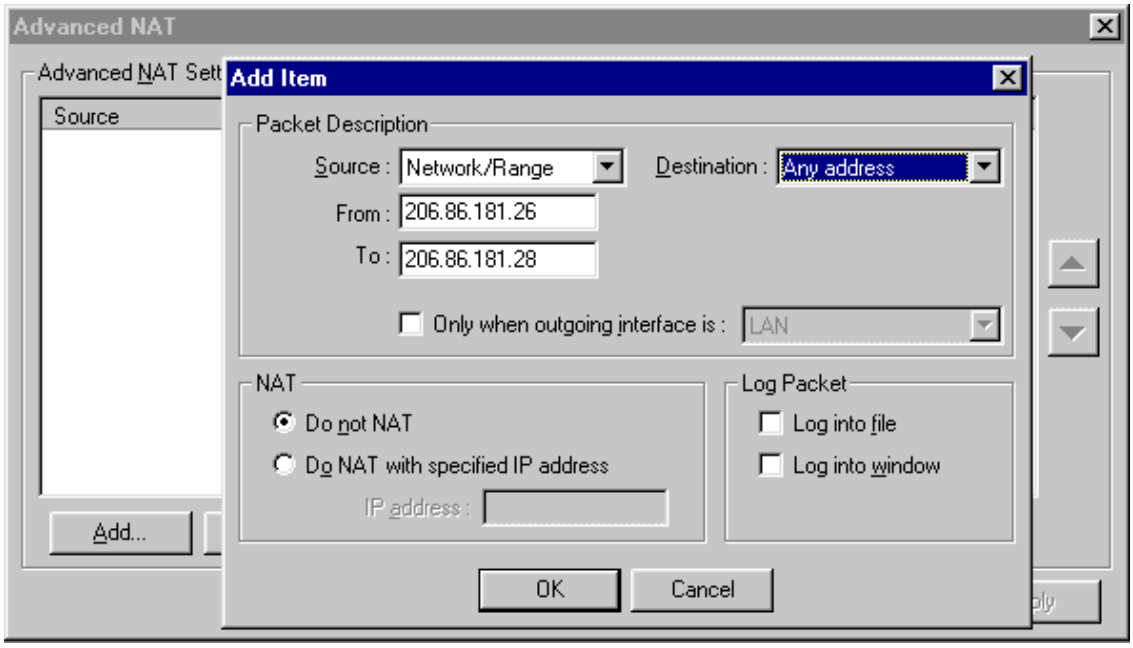
Un segmento pubblico si compone di più computer, ciascuno dei quali ha un proprio indirizzo IP pubblico. Se le regole di protezione lo consentono, è possibile accedere a questi sistemi direttamente da Internet

Ciascun segmento deve avere una propria interfaccia di rete nel computer WinRoute, per consentire a WinRoute di connettere a Internet i segmenti pubblici e privati.



Impostazioni di WinRoute

È necessario eseguire le impostazioni NAT avanzate, dal menu Impostazioni=>Avanzate=>NAT, per evitare che WinRoute esegua NAT sui pacchetti dei segmenti pubblici.



Impostazioni delle reti pubbliche e private

Le procedure di impostazione di questi tipi di reti sono simili a quelle descritte in altre parti del presente manuale. Nel caso dei segmenti pubblici, la sola differenza consiste nel fatto che su di essi verranno utilizzati degli indirizzi IP pubblici. In linea di massima le regole da applicare sono le seguenti:

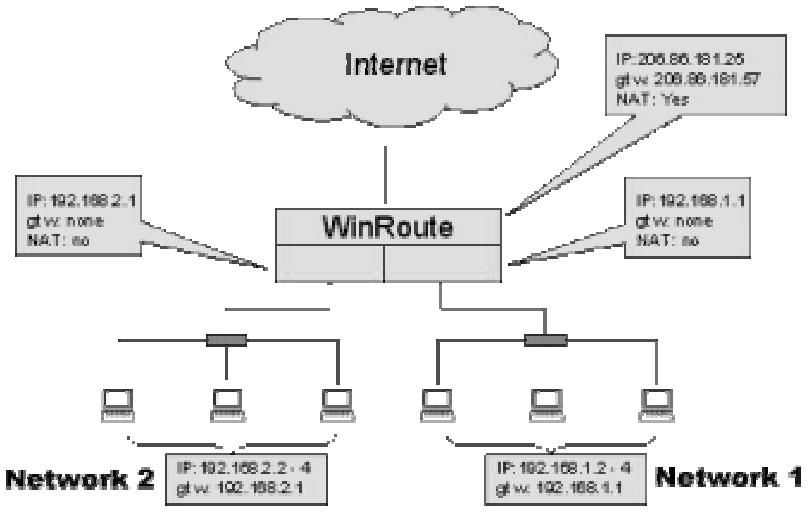
- Non impostare alcun gateway predefinito sulle interfacce di WinRoute.
- L'indirizzo IP di queste interfacce verrà utilizzato come gateway predefinito per il resto della rete.
- Non abilitare NAT sulle interfacce di WinRoute.

…per ulteriori informazioni, vedere ***Elenco di controllo*** .

Condivisione della connessione per due reti con un solo indirizzo

Nel caso in cui si preveda il collegamento di due reti a Internet tramite un solo computer WinRoute, non sono o richieste impostazioni particolari. Esistono molti segmenti che portano al computer WinRoute, ciascuno dei quali con un'interfaccia di rete separata. Nel caso dell'esempio, ci sono tre interfacce di rete nel computer WinRoute:

- Interfaccia Internet
- Interfaccia di rete 1
- Interfaccia di rete 2



Le sole impostazioni necessarie sono le seguenti:

Interfaccia Internet

NAT abilitata
Indirizzo IP impostato secondo le indicazioni del provider Internet
Gateway impostato secondo le indicazioni del provider Internet

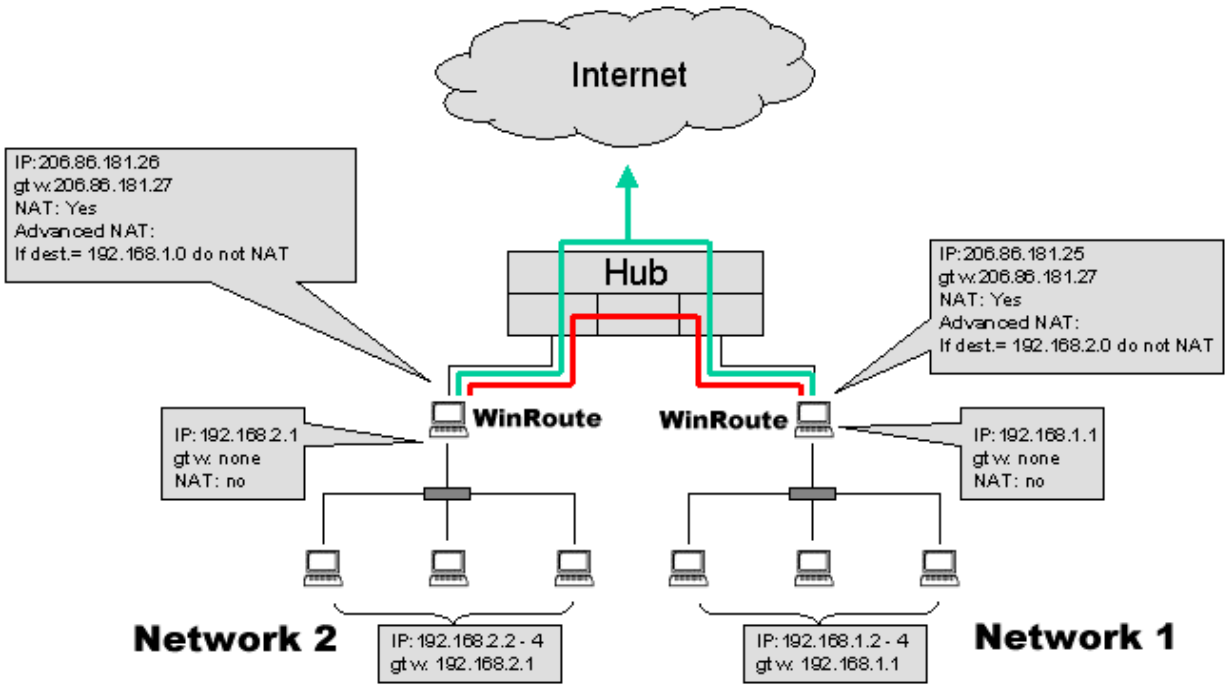
Interfacce interne

NAT DISABILITATA
Nessun gateway impostato sulle interfacce
Indirizzo IP impostato sul tipo interno (ad es. 192.168.1.1)

Le altre impostazioni sono uguali a quelle descritte in altre sezioni del presente manuale. Il traffico in arrivo da una sottorete viene instradato all'altra sottorete o a Internet, e viceversa.

Condivisione della connessione per due reti con due indirizzi

È possibile condividere un accesso Internet con due reti, ciascuna delle quali provvista di indirizzo IP pubblico separato.



Quando si esegue il seguente scenario di routing È ESTREMAMENTE importante rispettare le indicazioni di seguito riportate:

- NON ESEGUIRE NAT con i pacchetti diretti all'altra rete.
- ESEGUIRE NAT con i pacchetti diretti a Internet.

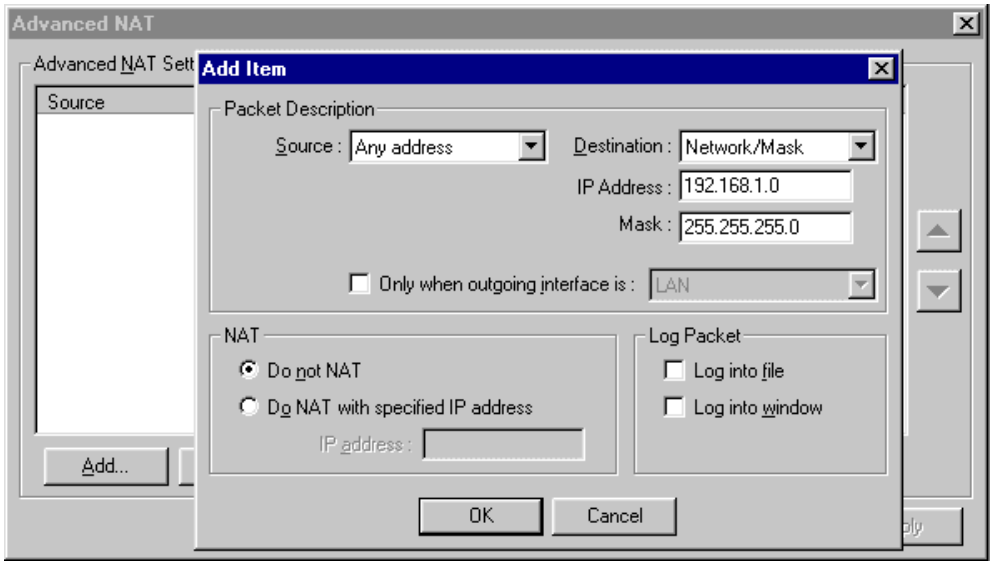
In altre parole, WinRoute eseguirà NAT in base alla destinazione dei pacchetti IP in transito. I pacchetti diretti alla rete remota non subiranno modifiche, mentre quelli diretti a Internet saranno soggetti a NAT.

Router o hub?

A seconda delle proprie esigenze è possibile scegliere se interporre un router tra le reti o se un hub sia sufficiente. Nello scenario dell'esempio, l'hub è sufficiente per consentire a due reti di condividere un'unica connessione Internet (ad alta velocità).

Per impostare WinRoute in modo che NAT venga eseguita solo in funzione della destinazione del pacchetto:

1. Scegliere il menu Impostazioni->Avanzate->NAT.
2. Immettere i criteri di destinazione - generalmente la sottorete o l'intervallo degli indirizzi IP.
3. Selezionare l'opzione "Non eseguire NAT".



Suggerimento: nelle impostazioni avanzate di NAT esiste un'altra opzione, che specifica di non eseguire NAT con determinati indirizzi IP di origine. Questa impostazione può essere utile se si conoscono le workstation che non richiedono accesso a Internet. In questo caso, piuttosto che impostare i criteri del firewall, è possibile trovare un'altra soluzione nelle impostazioni avanzate di NAT.

I pacchetti per i quali si sceglie di non eseguire NAT non riceveranno mai risposta, perché l'origine rimarrà come indirizzo interno. In altre parole, gli utenti potrebbero cercare di connettersi a Internet senza mai riuscirvi.

Server di accesso remoto (connessione e accesso a Internet)

Soluzione con server di accesso remoto

A volte può essere necessario accedere alla rete aziendale tramite linea telefonica esterna e utilizzare quell'accesso a Internet. WinRoute fornisce questa funzionalità su Windows NT, a condizione che i servizi RAS siano installati e configurati.

Esistono delle regole specifiche da rispettare:

- La rete aziendale deve avere una sottorete (ad es. 192.168.1.0).
- Il server DHCP di Windows NT deve fornire agli utenti provenienti da RAS indirizzi IP di sottoreti differenti (ad es. 192.168.2.0).
- NAT verrà eseguita solo sulle interfacce di collegamento a Internet.

In altre parole, la scheda di rete (NIC) di collegamento alla rete locale deve avere l'indirizzo IP di una sottorete (ad es. 192.168.1.1), mentre l'utente che si collega al server tramite RAS deve ottenere l'indirizzo IP da una rete differente (ad es. 192.168.2.1). WinRoute agisce da router, instradando i pacchetti tra due o più interfacce di reti diverse.

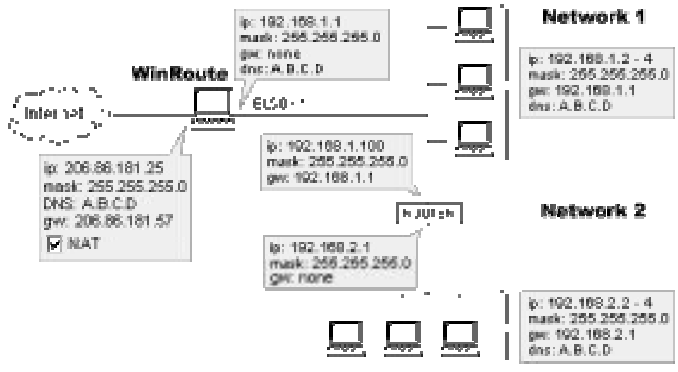
Questo tipo di impostazione riflette quella di un piccolo provider Internet. WinRoute non limita il numero di utenti che hanno accesso simultaneamente al server NT. Fino a che il server NT attribuirà agli utenti indirizzi IP remoti ottenuti da sottoreti differenti (non dalla rete principale), il numero degli utenti sarà limitato solo dal numero di interfacce RAS.

Connessione di segmenti sovrapposti tramite un indirizzo IP

L'impostazione in base alla quale le reti non sono connesse direttamente al computer WinRoute, ma sono collegate tra loro per mezzo di un router, si chiama "rete a segmenti sovrapposti".

Figure 1: Connecting cascaded segments to the Internet

Il router tra due reti può essere un qualunque tipo di router hardware o un computer Windows NT o Windows 95/98 con WinRoute. WinRoute svolgerà le funzioni di router e, a seconda dei casi, eseguirà o non eseguirà NAT.



In generale è necessario "indicare" al computer WinRoute dove verranno inviati i pacchetti proveniente da altre reti, mentre per i pacchetti in uscita devono esistere collegamenti simili sul router (divisione di due reti) che specifichino dove verranno inviati i pacchetti provenienti dalla seconda rete. Ciò può essere ottenuto aggiungendo nuove route - una al computer WinRoute (per i pacchetti in entrata) e una al router (per i pacchetti in uscita).

- La ROUTE sui computer WinRoute (membro della rete 1) instraderà i pacchetti IP per l'altra rete (rete 2) all'indirizzo IP specifico della rete 1 del router. Il router avrà il compito di inoltrare i pacchetti da quel momento in poi.
- La ROUTE PREDEFINITA sul router (che connette le due reti) instraderà tutti pacchetti provenienti dalla rete 2 all'indirizzo IP della rete 1 del computer WinRoute. WinRoute eseguirà quindi NAT sui pacchetti e li invierà a Internet.

Esempio

Nell'esempio si suppone che esistano due reti agli indirizzi 192.168.1.x e 192.168.2.x. e un router all'indirizzo 192.168.1.100.

Nota! Il router può essere indifferentemente di tipo hardware o software (Windows 95/98 o NT con WinRoute).

Impostazioni della rete 1 (rete primaria)

- Specificare al computer WinRoute che tutti i pacchetti diretti alla rete 192.168.2.0 devono passare dal router 192.168.1.100:
- 1. Andare al prompt di MS-DOS.
- 2. Immettere il seguente comando:

```
Route -p add 192.168.2.0 mask 255.255.255.0
192.168.1.100
```

- Sul router 192.168.1.100, la route predefinita deve portare al computer con WinRoute, ed es. 192.168.1.1. Occorre indicare al router quali sono i pacchetti diretti alla rete che transiteranno per il PC WinRoute.

Le ulteriori impostazioni saranno uguali a quelle già descritte in altri capitoli (impostazione della rete).

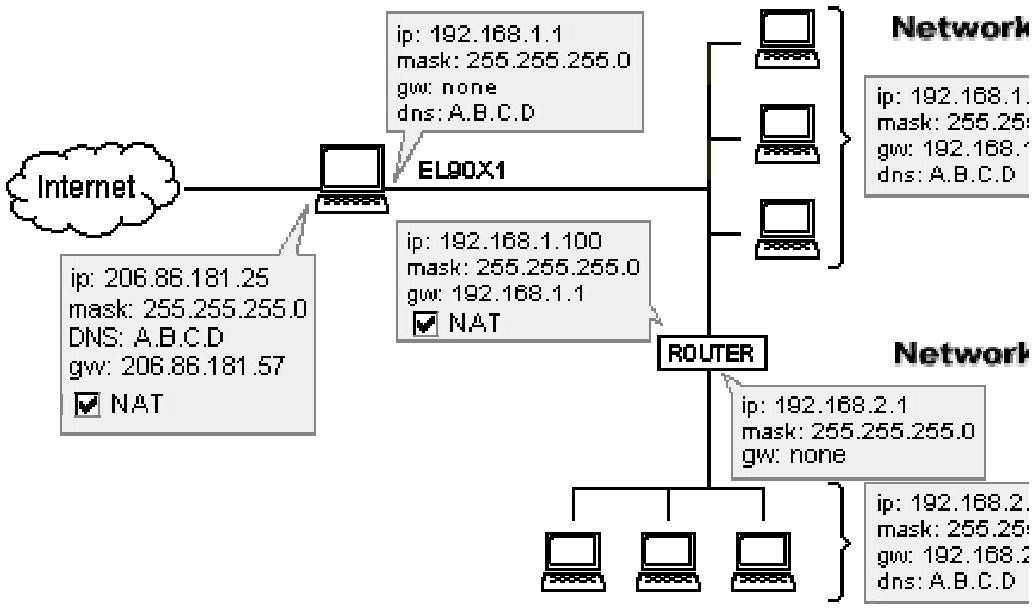
Impostazioni della rete 2 (rete secondaria)

Non sono richieste impostazioni particolari: la rete 2 sarà la rete indipendente. Il gateway predefinito su tutti i computer della rete 2 è impostato all'indirizzo IP della rete 2 del router (192.168.2.1 Nell'esempio).

NAT tra la rete 1 e la rete 2

È possibile utilizzare WinRoute con l'opzione NAT "abilitata" per connettere tra loro le reti primaria e secondaria. La rete secondaria sarà simile a un unico computer, con vantaggi per l'utente in termini di maggiore semplicità di amministrazione e maggiore protezione. È necessario eseguire correttamente le impostazioni avanzate di NAT, per evitare di modificare il traffico tra le due reti.

Figure 2: Connecting cascaded segments to the Internet



Impostazioni NAT avanzate sul PC WinRoute che divide la rete 1 dalla rete 2

Il protocollo NAT verrà eseguito, o non eseguito, in base all'indirizzo IP di destinazione. Nel caso dell'esempio, se la destinazione dei pacchetti è sulla rete 192.168.1.0, NAT non verrà eseguita, e la comunicazione tra le due reti avverrà come se NAT non esistesse.

Per le impostazioni della rete attenersi alle regole descritte nel presente manuale.

Schede Ethernet multiporta

Delle oltre 170.000 reti che attualmente utilizzano WinRoute Pro come router/firewall, la maggior parte utilizza la configurazione con due schede NIC (Network Interface Cards): una per il collegamento a Internet e una per il collegamento alla LAN (Local Area Network). Questa configurazione di base filtra i pacchetti diretti e provenienti da Internet, ma non può filtrare i pacchetti che viaggiano tra segmenti locali, perché non passano da WinRoute. Un esempio di configurazione a due schede è illustrato in figura 1.

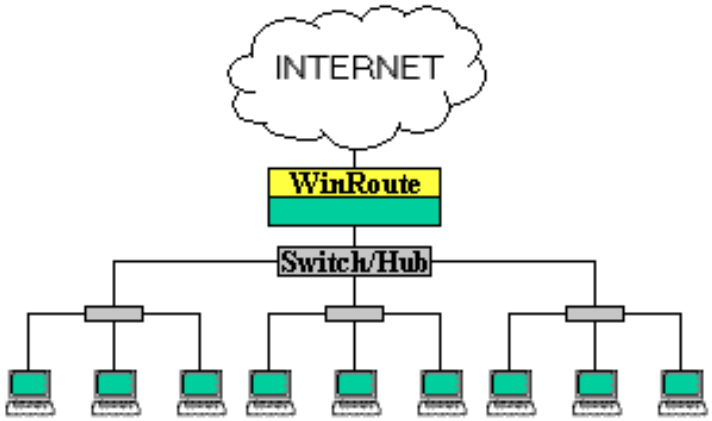


Figura 1. La configurazione più comune di WinRoute Pro.

In alcuni casi, sarà necessario aggiungere al computer WinRoute una terza NIC, per gestire il traffico con un segmento separato protetto. I pacchetti provenienti o indirizzati dal segmento protetto a Internet o ad altri segmenti locali verranno filtrati da WinRoute, e ciò costituirà un ulteriore livello di protezione.

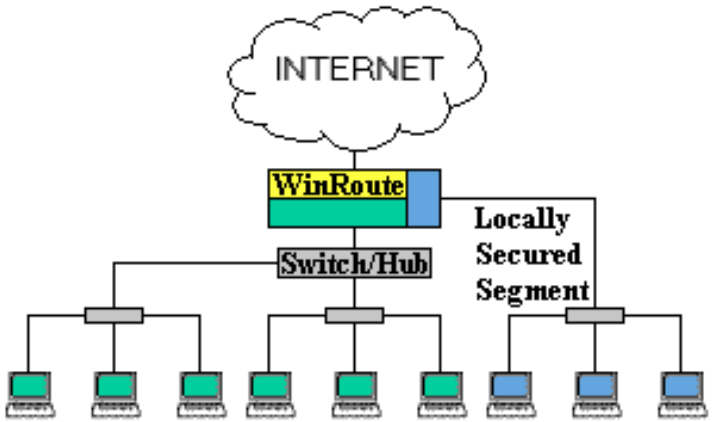


Figura 2. Una terza scheda NIC permette di aggiungere alla LAN un segmento separato.

Le reti di grandi dimensioni possono avere un numero maggiore di segmenti separati, ognuno dei quali protetto in modo differente. Il numero di possibili segmenti è limitato dal numero di porte disponibili sul PC WinRoute. Per questo motivo p necessario ricorrere all'aggiunta di dispositivi hardware che consentano di gestire ulteriori operazioni di routing/switching e politiche di protezione.
Grazie alla recente introduzione delle schede NIC Ethernet multiporta, WinRoute può essere utilizzato come unico controller del traffico in rete. Poiché tali schede consentono a WinRoute di gestire oltre 24 porte, in funzione del numero di slot per scheda disponibili sulla scheda madre, il PC WinRoute potrà operare come server, router, switch, controller di dominio ecc. In questo modo la gestione della rete potrà essere centralizzata e controllata da un solo punto. La figura 3 mostra WinRoute Pro utilizzato con una scheda NIC Ethernet multiporta, per il controllo di tre diverse reti.

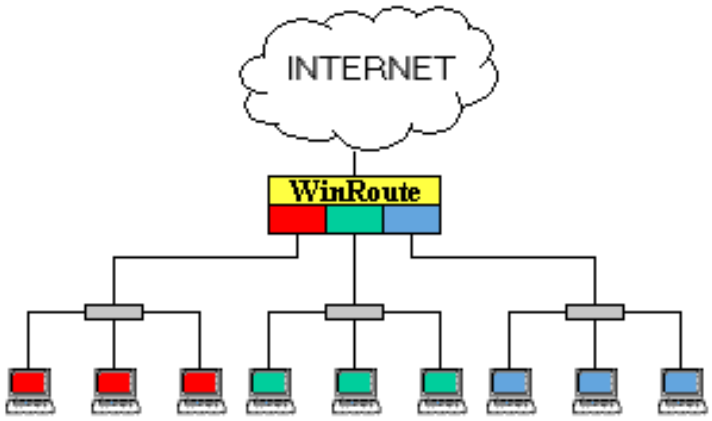


Figura 3. WinRoute Pro equipaggiato con una scheda NIC Ethernet multiporta.

Oltre a una migliore protezione e alla gestione centralizzata, l'adozione di una scheda NIC Ethernet multiporta, consente di usufruire di ulteriori vantaggi, quali il bilanciamento del carico e la protezione dal fail-over. Si noti l'assegnazione delle tre porte al segmento centrale proposto in figura 4.

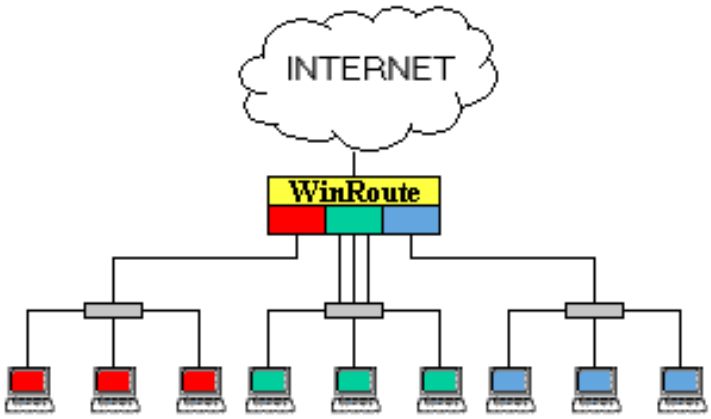


Figura 4. Al segmento centrale sono state assegnate tre porte di aggregazione.

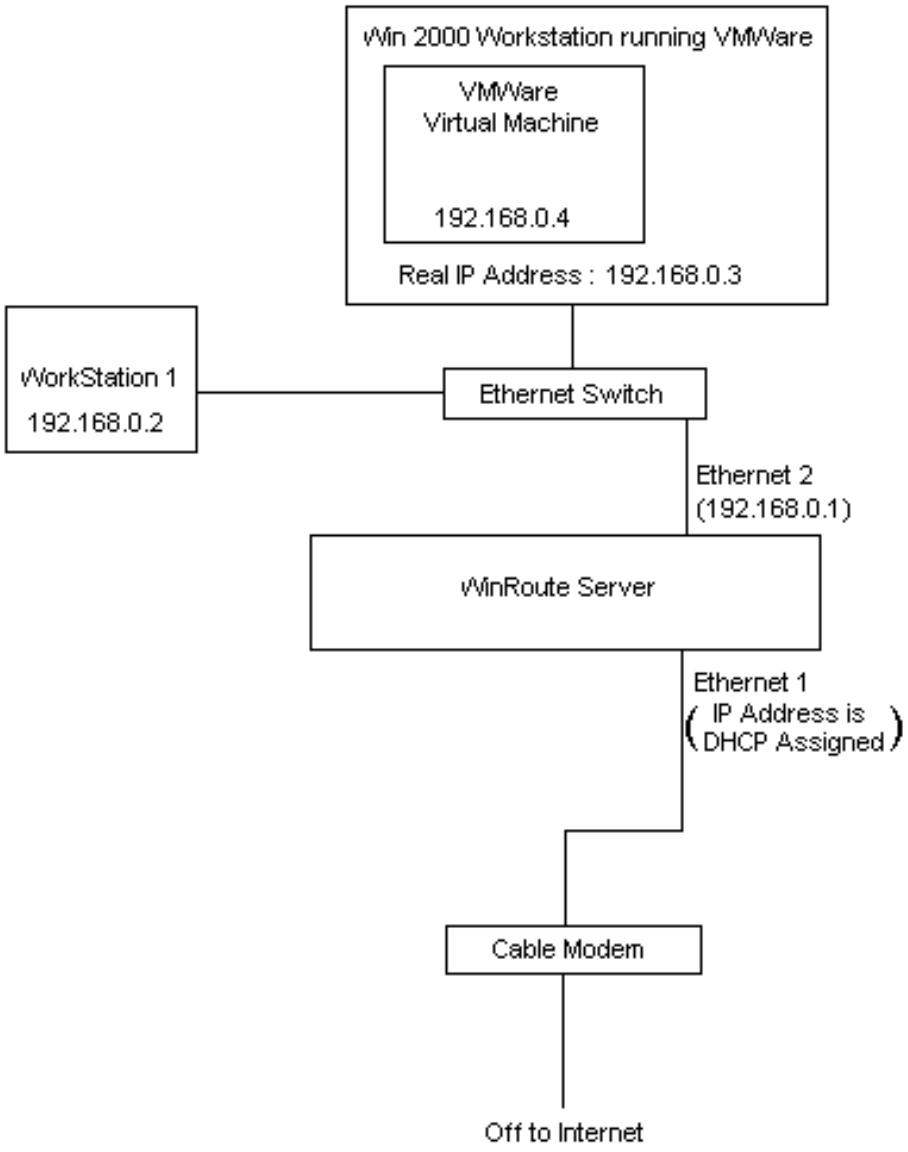
Il bilanciamento del carico può essere eseguito tramite le porte di aggregazione. Nella figura precedente, ad esempio, al segmento centrale di rete sono stati assegnate tre porte. Se il segmento utilizzasse uno switch per connettersi al PC WinRoute, ciascuno dei tre computer potrebbe recuperare dati alla velocità di 100 Mbps. Gli altri due segmenti potranno recuperare dati alla velocità combinata di 100 Mbps, perché solo una porta di quel segmento è collegata al PC WinRoute. Un'ulteriore funzionalità dell'aggregazione è la possibilità di proteggere le porte dagli errori. Infatti, qualora si verifichi un'interruzione di linea, il traffico verrà instradato alla prima porta successiva disponibile.

Utilizzando le schede NIC multiporta con WinRoute è possibile creare un sistema multi-routing estremamente efficiente e con un costo molto concorrenziale, gestito da un unico amministratore. Ad oggi, WinRoute è stato testato con D-Link 4 port DFE 570 TX e Adaptec 2 port Duralan ANA-62022. Non sono state testate altre schede.

Questo tipo di rete richiede la presenza di subnet differenti per ciascun segmento di rete collegato al PC WinRoute.

VMWare

VMWare è un'applicazione in grado di emulare il PC installato fino a livello hardware. La rete percepisce il computer virtuale come entità completamente separata. Poiché il computer virtuale dispone anche di proprietà di rete, WinRoute considererà il PC virtuale come un computer addizionale.



CAPITOLO 4

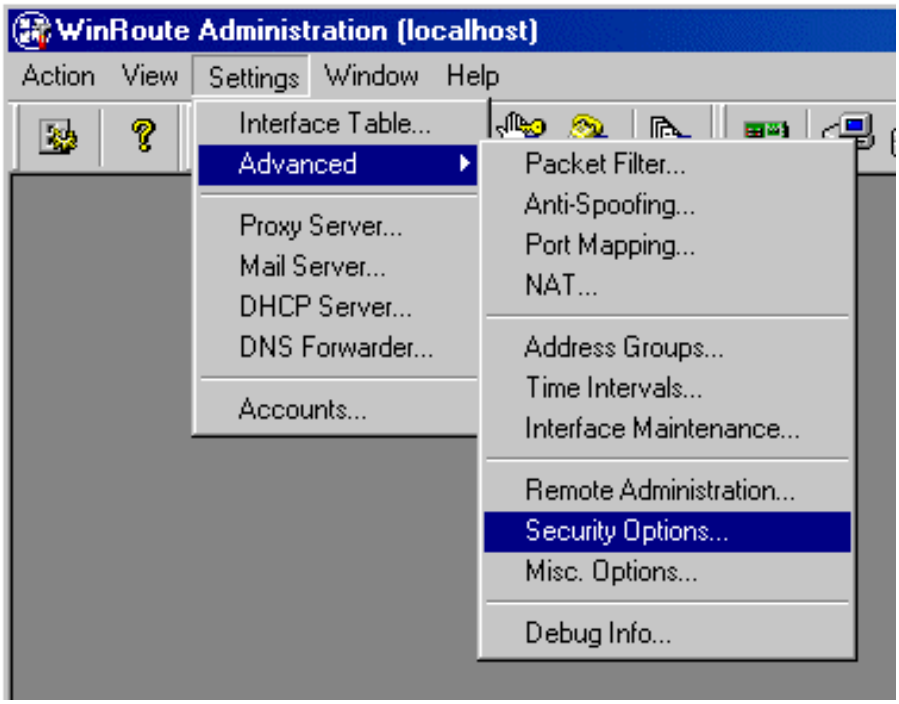
CONFIGURAZIONE DEL FIREWALL

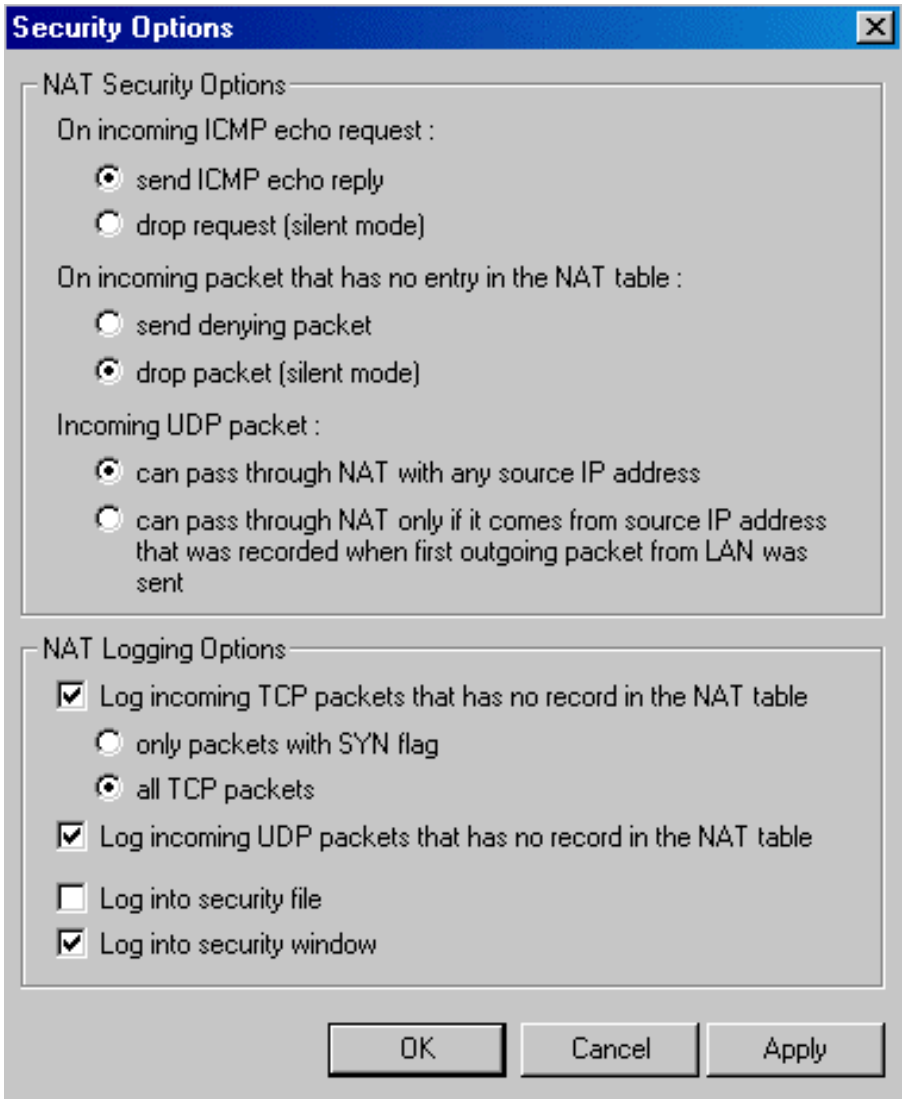
In questo capitolo

Trovare la porta di allocazione appropriata

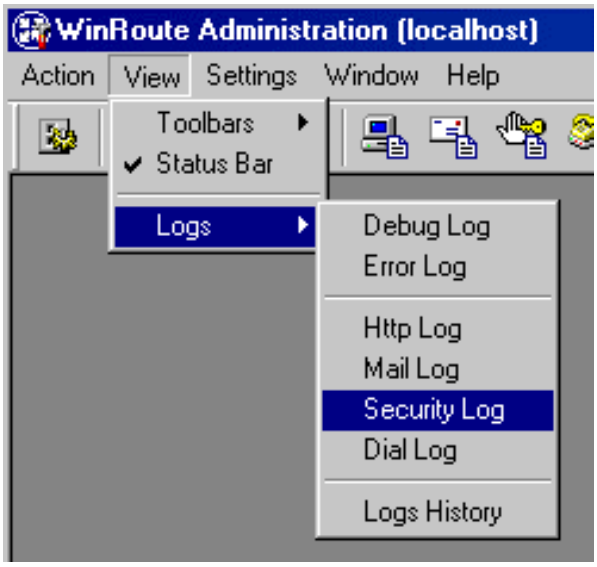
✍✍ ***Build 19 o superiore>***

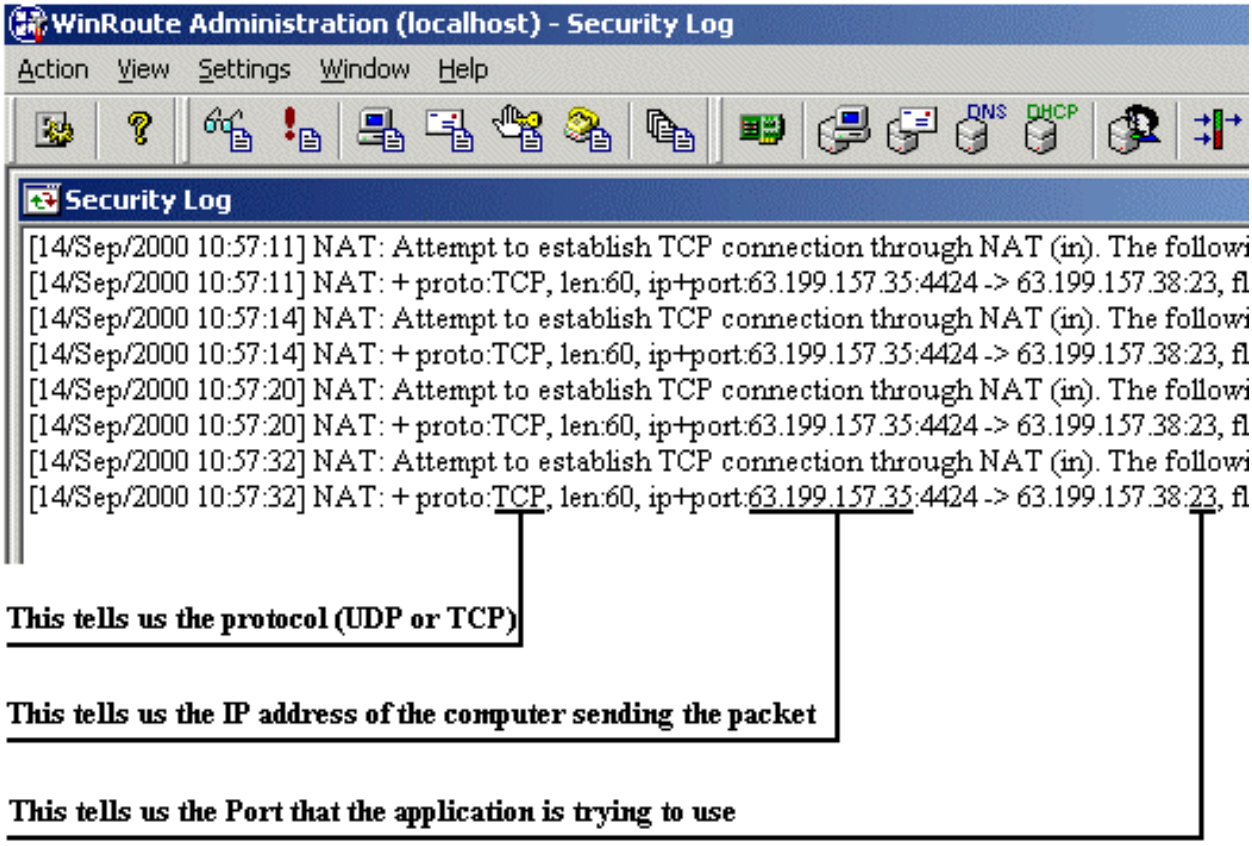
Nella finestra Amministrazione di WinRoute scegliere Impostazioni-> Avanzate> Opzioni di protezione




Security Options
NAT Security Options
On incoming ICMP echo request :
send ICMP echo reply
drop request (silent mode)
On incoming packet that has no entry in the NAT table :
send denying packet
drop packet (silent mode)
Incoming UDP packet :
can pass through NAT with any source IP address
can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent
NAT Logging Options
Log incoming TCP packets that has no record in the NAT table
only packets with SYN flag
all TCP packets
Log incoming UDP packets that has no record in the NAT table
Log into security file
Log into security window
OK
Cancel
Apply

Nella metà inferiore della finestra sono proposte alcune opzioni di registrazione log. Abilitare la registrazione dei pacchetti TCP e UDP non indicati nella tabella NAT. In questo modo verranno registrati solo i pacchetti iniziati all'esterno di WinRoute, che verranno ignorati a meno che ad essi non corrispondano mappature di porte. Poiché si tratta di una condizione limitata di registrazione, verrà preso in considerazione solo un numero scelto di pacchetti, per facilitare la descrizione dei pacchetti da ricercare. Il passaggio successivo consiste nell'apertura del registro log di protezione dal menu Visualizza -> Registri.





Nel caso dell'esempio, il computer all'indirizzo 63.199.157.35 invia, tramite la porta 4424, un pacchetto al computer 63.199.157.38, che lo riceverà alla porta 23. La porta 23 è la porta standard utilizzata da Telnet. Se il server Telnet fosse in esecuzione su alcuni indirizzi privati, quali 192.168.1.3, sarebbe in ascolto sulla porta 23. Per questo motivo è consigliabile mappare i pacchetti TCP alla porta 192.168.1.3.

Servizi di messaggistica e telefonia

Esistono o attualmente diversi servizi di messaggistica istantanea che supportano il trasferimento di file e offrono possibilità di conversazione da PC a PC o da telefono a PC. WinRoute Pro è stato testato con le seguenti configurazioni di **AOL instant messenger**, **Yahoo instant messenger**, **MSN Messenger**, e **ICQ**.

AIM non richiede impostazioni specifiche. Utilizzare le impostazioni predefinite e accertarsi che non sia specificato l'utilizzo del server proxy.

Gli utenti di **Yahoo IM** devono selezionare nelle preferenze di Accesso -> Connessione l'opzione "Nessuna rete rilevata". Tutti i servizi Yahoo IM a valle di NAT funzionano correttamente con queste impostazioni.

MSN Messenger funziona meglio se si utilizza il proxy HTTP. Abilitare il proxy di WinRoute sulla porta predefinita 3128 (in aggiunta a NAT). La conversazione da PC a PC non funziona a valle di WinRoute; mentre funziona la conversazione da PC a telefono.

ICQ funziona quasi sempre con le impostazioni predefinite dell'**ultima** versione. Se si sperimentano difficoltà con il trasferimento di file, si raccomanda di utilizzare il proxy HTTPS, scegliendo Preferenze -> Connessioni -> Server e firewall. Abilitare il proxy di WinRoute sulla porta predefinita 3128 (in aggiunta a NAT).

Nota: nessuna delle applicazione richiede la mappatura delle porte.

H.323 - NetMeeting 3.0

WinRoute include il supporto al protocollo H.323. Ciò significa che tutte le applicazioni di telefonia Internet possono comunicare tramite WinRoute. Tali applicazioni sono Microsoft NetMeeting, CuSeeMee, telefonia Internet (utilizzando un telefono IP Siemens con WinRoute, ad esempio) e altre.

Se la comunicazione inizia valle di WinRoute

Non è richiesta alcuna impostazione. WinRoute supporterà un numero di fatto illimitato di connessioni simultanee.

Se la comunicazione viene stabilita da Internet ed è diretta a un PC a valle di WinRoute

È necessario mappare la porta, ovvero indicare a WinRoute dove instradare i pacchetti H.323 in entrata. Impostare le seguenti mappature porte:

Protocollo:	TCP
IP in ascolto:	non specificato, o l'indirizzo IP utilizzato per la comunicazione H.323, in presenza di sistemi multihomed
Porta in ascolto:	1720
IP di destinazione:	l'indirizzo IP LAN dell'applicazione H.323
Porta di destinazione:	1720

Il protocollo H.323 non viene eseguito sulla porta 1720 - WInRoute aggiungerà le altre connessioni automaticamente. A motivo delle limitazioni del protocollo H.323, esso può essere utilizzato per la comunicazione da una workstation per volta.

IRC - Internet Relay Chat

Non sono richieste impostazioni speciali per eseguire il client IRC. Anche DCC (Direct Chat/Send(Receive) Files) funzionerà automaticamente se si utilizza la porta standard 6667 di IRC.

Per eseguire il server IRC a monte di NAT è necessario mappare le porte seguenti:

Protocollo: TCP

IP in ascolto: non specificato, o l'indirizzo IP che si desidera utilizzare per il server IRC.

Porta in ascolto: 6667

IP di destinazione: indirizzo IP del PC con il server IRC dell'utente

Porta di destinazione: 6667

L'utilizzo di porte non standard impedirà il funzionamento di DCC.

CITRIX Metaframe

WinRoute supporta il protocollo **CITRIX Metaframe** Per accedere da Internet al server CITRIX Metaframe in esecuzione su una rete interna a WinRoute, è necessario eseguire le seguenti mappature:

Per CITRIX Metaframe:

Protocollo: TCP

IP in ascolto: non specificato, o l'indirizzo IP pubblico da utilizzare con il server

Porta in ascolto: 1494

IP di destinazione: indirizzo IP di classe privata del server interno alla rete

Porta di destinazione: 1494

È possibile creare un numero maggiore di porte mappate e accedere a più server simultaneamente. Per poterlo fare, è necessario preimpostare le porte che i computer client dovranno utilizzare per accedere al server. Impostare le porte nel file .ini del client, in occasione della creazione dell'icona di connessione.

MS Terminal Server

WinRoute supporta il protocollo **MS Terminal Server**. Per accedere da Internet dal server terminal MS in esecuzione su una rete interna a WinRoute, è necessario eseguire le seguenti mappature:

Per il server terminal MS:

Protocollo: TCP

IP in ascolto: non specificato, o l'indirizzo IP pubblico da utilizzare con il server

Porta in ascolto: 3389

IP di destinazione: indirizzo IP di classe privata del server interno alla rete

Porta di destinazione: 3389

È possibile creare un numero maggiore di porte mappate e accedere a più server simultaneamente. Per poterlo fare, è necessario preimpostare le porte che i computer client dovranno utilizzare per accedere al server. Impostare le porte nel file .ini del client, in occasione della creazione dell'icona di connessione.

Telefonia Internet - BuddyPhone

WinRoute è il primo router/firewall software che conferisce alla telefonia Internet lo stato di piena fruibilità. BuddyPhone permette di telefonare tramite Internet da una rete all'altra.

Il supporto per BuddyPhone funziona meglio con ICQ. Dopo essersi registrati come utenti di questa applicazione software di messaggeria istantanea, comunicare con i propri amici sarà un'operazione semplicissima.

Tutti gli utenti attivi nell'elenco degli amici di ICQ appaiono anche nella rubrica di BuddyPhone. Per comunicare telefonicamente con loro sarà sufficiente selezionarne il nome.

Se si utilizzano congiuntamente BuddyPhone e ICQ non sono richieste impostazioni particolari.

Utilizzo di BuddyPhone senza ICQ

WinRoute devia le chiamate in arrivo da Internet al destinatario nella rete in base alla porta specificata.

Utilizzare i numeri a partire da 710 per assegnare agli utenti locali la propria porta personale.

Esempio:

tre utenti della LAN utilizzano BuddyPhone.

Nome utente	Indirizzo IP interno dell'utente	Porta assegnata all'utente
Giovanni	192.168.1.2	710

Guido	192.168.1.3	711
Roberta	192.168.1.4	712

La mappatura delle porte sarà:

Porta in ascolto	IP di destinazione	Porta di destinazione
710	192.168.1.2	700
711	192.168.1.3	700
712	192.168.1.4	700

Per telefonare a un utente sarà sufficiente immetterne il nome e il numero di porta nella finestra di dialogo per le chiamate dirette di BuddyPhone. Ad esempio: vendite.gamerouter.com:711.

✍✍ ***Nota! Non si tratta di un errore: il numero della porta di destinazione utilizzato da BuddyPhone è effettivamente 700. WinRoute eseguirà il routing in base alla porta in ascolto.***

CU-YouSeeMe

La seguente mappatura porte è necessaria per ricevere le chiamate **CU-SeeMe** tramite NAT:

Protocollo: UDP

IP in ascolto: <non specificato>

Porta in ascolto: 7648

IP di destinazione: l'indirizzo IP della workstation su cui viene eseguito il client CU-SeeMe

Porta di destinazione: 7648

Protocollo: UDP

IP in ascolto: <non specificato>

Porta in ascolto: 7649

IP di destinazione: l'indirizzo IP della workstation su cui viene eseguito il client CU-SeeMe

Porta di destinazione: 7649

Limitazioni:

- Attualmente non è possibile eseguire più di un client CU-SeeMe sulla stessa LAN
- Non è possibile connettersi a un "reflector" protetto da password.

Accesso remoto - PC Anywhere

In questa sezione

PC Anywhere

Il supporto a Symantec PC AnyWhere incluso in WinRoute è sicuramente il migliore tra quelli offerti da qualunque altro router in circolazione. PC AnyWhere permette all'utente di accedere e gestire i computer della rete. Procedere come di seguito indicato:

1. Eseguire PC Anywhere Host sui computer gestito.
2. Eseguire PC Anywhere Remote sul computer remoto.
3. Configurare Mappatura porte sul computer WinRoute come di seguito indicato:

   Protocollo: TCP/UDP

   IP in ascolto: non specificato

   Porta in ascolto (intervallo): 5631-5632

   IP di destinazione: indirizzo IP del computer host PC Anywhere della rete (ad es.192.168.1.12)

   Porta di destinazione: 5631-5632

Problemi di protezione

Per aumentare la protezione ed evitare di aprire la rete al mondo esterno, WinRoute permette agli utenti di scegliere un indirizzo IP specifico da cui consentire l'accesso a porte specifiche. Questa configurazione consente l'accesso al sistema da Internet solamente ad alcuni computer della rete.

Per impostare i computer a cui è consentito l'accesso alla rete, è necessario definire prima un gruppo di indirizzi (anche se si immette un solo computer). Per configurare il gruppo, scegliere Impostazioni=>Avanzate=>Gruppi di indirizzi.

Modifica dell'accesso ai diversi computer

È possibile impostare i diritti dell'amministratore direttamente in WinRoute, per consentire di stabilire una connessione diretta all'host di WinRoute. Dall'host sarà possibile modificare l'IP di destinazione in Mappatura porte e accedere direttamente al PC scelto.

Gateway PC Anywhere

Se si esegue PC Anywhere in modalità gateway sul firewall WinRoute sarà possibile permettere al client remoto di recuperare un elenco di host PC Anywhere disponibili a valle del firewall. L'elenco consente di gestire qualunque host a valle del firewall di WinRoute.

Per l'esecuzione dei passaggi di seguito indicati si presuppone che l'utente utilizzi PC Anywhere 9.0 e che il firewall di WinRoute non applichi alcun tipo di filtro ai pacchetti in entrata/uscita.

- Eseguire PC Anywhere Host sui computer gestiti a valle del firewall di WinRoute per mezzo del protocollo TCP/IP.
- Eseguire PC Anywhere Remote sul computer remoto per mezzo del protocollo TCP/IP.
- Installare PC AnyWhere sul firewall di WinRoute tramite la modalità gateway. Durante la configurazione del gateway, impostare su TCP/IP sia i dispositivi in entrata sia quelli in uscita.

- Configurare PC AnyWhere sul firewall di WinRoute in modo che ascolti sulla NIC interna (ad es. 192.168.1.1). Per informazioni sulla configurazione della modalità di ascolto di PC AnyWhere su uno specifico indirizzo IP/NIC, visitare il sito Web Symantec.
- Aggiungere gli indirizzi IP specifici dei computer da gestire tramite Opzioni di rete di PC AnyWhere. Per controllare l'intera sottorete, utilizzare 255 come ultimo ottetto (192.168.1.255).
- Mappare la porta in WinRoute come di seguito indicato:

  Protocollo: TCP/UDP

  IP in ascolto: NIC esterna (206.86.181.25)

  Porta in ascolto: INTERVALLO (5631-5632)

  IP di destinazione: NIC interna (192.168.1.1)

  Porta di destinazione: 5631-5632

Sezione giochi

In questa sezione

Informazioni sull'esecuzione dei giochi a valle di NAT

Giochi

Molti dei giochi attualmente in circolazione supportano l'ambiente multi-utente. I partecipanti si affrontano da un capo all'altro di Internet o della LAN, o partecipano ai giochi proposti da uno dei tanti server di gioco di Internet. È anche possibile ospitare propri server di gioco per giocare con amici, familiari o sconosciuti.

Esistono molti giochi che non richiedono la messa in atto di particolari impostazioni di WinRoute. Prima di configurare WinRoute per un gioco specifico, è consigliabile caricare la versione demo. A differenza dei server proxy, l'architettura di base di WinRoute supporta molti dei giochi reperibili in commercio.

Alcuni giochi richiedono una configurazione specifica della porta di WinRoute. Le porte vengono utilizzate dal server di gioco per identificare i giocatori (in generale).

Se il gioco richiede l'associazione di una porta specifica, configurare Mappatura porte di WinRoute in modo da inoltrare i pacchetti in arrivo al computer dei giocatori a valle del firewall.

Le porte utilizzate variano da gioco a gioco. Per ulteriori informazioni, fare riferimento alla documentazione di accompagnamento del gioco o contattare il supporto tecnico del fornitore del gioco. Il presente manuale contiene alcuni esempi di impostazioni, adatte ai giochi più conosciuti.

Aasheron's call

Asheron's call è un gioco molto conosciuto di Microsoft Gaming Zone. Per potervi giocare da un computer a valle di GameRouter sono necessarie le mappature di porta di seguito indicate:

1 Scegliere il menu *Impostazioni->Avanzate->Mappatura porte*

2 Eseguire le seguenti impostazioni:

Nome:	S1	S2	S3	S4	S:
Numero porta:	2300-2400	9000-9013	6667	28800 - 29000	
IP di destinazione:	IP del PC con il gioco	IP del PC con il gioco	IP del PC con il gioco	IP del PC con il gioco	IF cc
Protocollo:	TCP/UDP	UDP	TCP	TCP	

Battle.net (Blizzard)

Per giocare con battle.net è necessario mappare la porta come di seguito indicato, ricordando che è ammesso un solo giocatore per volta.

Protocollo: TCP/UDP

IP in ascolto: non specificato

Porta in ascolto: 6112

IP di destinazione: indirizzo IP del computer del giocatore (ad es. 192.168.1.6)

Porta di destinazione: 6112

Half-Life

Half-Life

Protocollo: TCP/UDP

IP in ascolto: non specificato

Porta in ascolto: 27015

IP di destinazione: indirizzo IP del computer del giocatore (ad es.192.168.1.6)

Porta di destinazione: 27015

MSN Gaming zone

La configurazione di seguito riportata è stata testata con MechWarior3 su **MSN Gaming Zone** Un solo computer per volta può accedere a MSN.

1. Scegliere il menu *Impostazioni->Mappatura porte*
2. Aggiungere una nuova mappatura

   Protocollo: TCP

   IP in ascolto: "non specificato"

   Porta in ascolto: intervallo da 2300 a 2400

   IP di destinazione: l'indirizzo IP locale del computer che si desidera connettere a MSN

   Porta di destinazione: intervallo da 2300 a 2400
3. Aggiungere una nuova mappatura

   Protocollo: UDP

   IP in ascolto: "non specificato"

   Porta in ascolto: intervallo da 28800 a 28912

IP di destinazione: l'indirizzo IP locale del computer che si desidera connettere a MSN

Porta di destinazione: intervallo da 28800 a 28912

Quake

Quake 3

Client Quake 2/3

Non richiede impostazioni speciali.

Server Quake 2/3

Per il server master:

Protocollo: UDP

IP in ascolto: non specificato

Porta in ascolto: singolo 8002

IP di destinazione: x.x.x.x

Porta di destinazione: 8002

Per i client conessi al server Quake3 Arena:

Protocollo: UDP

IP in ascolto: non specificato

Porta in ascolto: singolo 27960

IP di destinazione: x.x.x.x

Porta di destinazione: 27960

StarCraft

Giocare con StarCraft

WinRoute Pro include un supporto speciale per tutti i giocatori di StarCraft (Blizzard Entertainment). Più giocatori della rete connessa a Internet tramite WinRoute Pro possono divertirsi giocando contro nemici virtuali su Internet.

Attualmente il supporto completo è disponibile solo nel caso in cui tutti i giocatori appartengano alla stessa rete e utilizzino computer a valle di WinRoute Pro e non il computer host.

Per ulteriori informazioni, visitare il sito Web www.tinysoftware.com

Mappature supplementari per i giochi e le applicazioni più diffuse

Porte necessarie per le diverse applicazioni

Age of Empires II due mappature porte

Protocollo: TCP

IP di origine: non specificato

Porta di origine: 47624

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 47624

Protocollo: TCP/UDP

IP di origine: non specificato

Porta di origine: intervallo 2300 - 2400

IP di destinazione: l'indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: intervallo 2300 - 2400

Delta Force

Protocollo: TCP

IP di origine: non specificato

Porta di origine: intervallo 3568 - 3569

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: intervallo da 3568 a 3569

Dial Pad

Protocollo: UDP

IP di origine: non specificato

Porta di origine: intervallo 51200 - 51201

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: intervallo 51200 - 51201

Gamespy

Registrazione

Protocollo: UDP

IP di origine: non specificato

Porta di origine: 25635

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 25665

Per i giochi

Protocollo: UDP

IP di origine: non specificato

Porta di origine: intervallo 25000 - 30000

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: intervallo 25000 - 30000

Kali - tre mappature porte

Protocollo: UDP

IP di origine: non specificato

Porta di origine: 2213

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 2213

Protocollo: UDP

IP di origine: non specificato

Porta di origine: 6666

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 6666

Protocollo: UDP

IP di origine: non specificato

Porta di origine: 57

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 57

Mplayer

Protocollo: TCP/UDP

IP di origine: non specificato

Porta di origine: 8000 - 9000

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 8000 - 9000

PCanywhere versioni 2.07.51 - due mappature porte

Protocollo: TCP

IP di origine: non specificato

Porta di origine: 65301

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 65301

Protocollo: UDP

IP di origine: non specificato

Porta di origine: 22

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 22

Quicktime- due mappature porte

Protocollo: TCP

IP di origine: non specificato

Porta di origine: 554

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 554

Protocollo: UDP

IP di origine: non specificato

Porta di origine: intervallo 6970 - 6999

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: intervallo 6970 - 6999

RTSP

Protocollo: UDP

IP di origine: non specificato

Porta di origine: intervallo 6970 - 7170

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Intervallo porta di destinazione: 6970 - 7170

VNC

Protocollo: TCP

IP di origine: non specificato

Porta di origine: 59xx (in funzione del numero di display)

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 59xx

Protocollo: TCP

IP di origine: non specificato

Porta di origine: 58xx

IP di destinazione: indirizzo IP del computer su cui viene eseguita l'applicazione

Porta di destinazione: 58xx

GLOSSARIO DEI TERMINI

A

ARP

Il protocollo ARP (Address Resolution Protocol) associa un indirizzo IP a un indirizzo hardware, richiedendo al computer mittente informazioni supplementari, denominate indirizzo MAC. WinRoute utilizza ARP solo con finalità di registrazione log, per potenziale il fattore di protezione.

B

BOOTP

Il protocollo Bootstrap, che si riferisce ai computer di una LAN che sono stati impostati per accettare gli indirizzi IP dinamici assegnati dal server DHCP.

C

Cache

Il luogo in cui i dati vengono conservati per un dato periodo di tempo. WinRoute utilizza la memoria cache per archiviare le pagine Web e mantenere la larghezza di banda.

Cassette postali in WinRoute

Le cassette postali sono archiviate in una sottodirectory separata nella directory di installazione di WinRoute. Generalmente l'indirizzo è c:/Program files/WinRoute/Mail.

Subito dopo l'installazione del programma le cassette postali non sono visibili, anche se sono state create dagli utenti. Diventeranno REALI solo dopo la ricezione del primo messaggio da parte dell'utente.

D

DHCP

DHCP (Dynamic Host Configuration Protocol) è un protocollo per organizzare e semplificare l'amministrazione degli indirizzi IP dei computer locali. Spesso, come nel caso di WinRoute, il server DNS è integrato nel server DHCP, a beneficio di una maggiore semplicità operativa. Specificando l'indirizzo IP di un particolare dispositivo di rete, che generalmente è il dispositivo collegato a Internet, DHCP utilizzerà i valori DNS associati al dispositivo.

DNS

DNS (Domain Name System) è il nome dello schema utilizzato per gli indirizzi IP. Ad esempio, www.tinysoftware.com è un nome di dominio a cui è associato un indirizzo IP. Il server DNS trova l'equivalenza tra i nomi di dominio e i corrispondenti indirizzi IP. I nomi di dominio vengono utilizzati perché si ricordano più facilmente delle sequenza numeriche.

E

ETRN

Il comando ETRN è utilizzato dai server SMTP per prolungare il periodo di attesa successivo alla connessione, trascorso il quale il server SMTP inizierà la ricerca di nuovi messaggi.

Il comando ETRN viene sempre utilizzato quando il server SMTP non rimane connesso 24 ore al giorno, e la posta indirizzata a tale server debba rimanere archiviata temporaneamente su un altro server SMTP.

F

Firewall

Un modulo di filtraggio ubicato sul computer gateway che esamina tutto il traffico in entrata e in uscita per determinare se possa essere instradato a destinazione. WinRoute fornisce un firewall completo tramite la funzionalità NAT, l'assegnazione di regole per specifici indirizzi IP e la capacità di registrare determinate informazioni quando il pacchetto è in uscita, che ne consentano l'autorizzazione al suo ritorno.

Flag

I flag sono l'estensione con le informazioni sul pacchetto. Contengono informazioni supplementari per i router. Di seguito viene riportato l'elenco dei flag utilizzati da WinRoute:

SYNC - Sincronizza - pacchetto di sincronizzazione di una connessione TCP

ACK - Riconosci - riconoscimento dello scambio di dati

RST - Ripristina - richiesta di ripristino della connessione

URG - Urgente - pacchetto urgente

PSH - Push - richiesta di consegna immediata del pacchetto ai livelli più alti

FIN - Finalizza - finalizza la connessione

FTP

FTP (File Transfer Protocol) è un protocollo applicativo utilizzato in Internet per trasferire, aggiornare, eliminare, spostare, rinominare o copiare i dati.

G

Gateway

Il punto di passaggio da una rete all'altra. Un gateway è responsabile della corretta distribuzione dei dati in entrata e in uscita da una rete locale. WinRoute deve essere installato sul PC su cui è installato il gateway, conosciuto anche come computer host.

I

ICMP

Il protocollo ICMP (Internet Control Message Protocol) utilizza datagrammi per la creazione di report di errore durante le trasmissioni tra l'host e il gateway.

Indirizzo IP

L'indirizzo IP è una sequenza numerica univoca a 32 bit che identifica il computer di una rete IP. Un indirizzo IP univoco viene assegnato a ciascun computer connesso a Internet. Tutti i pacchetti che transitano per la Rete contengono le informazioni che indicano la provenienza de pacchetto (indirizzo IP di origine) e la sua destinazione (indirizzo IP di destinazione).

Indirizzo MAC

L'indirizzo MAC (Media Access Control) è più specifico di un indirizzo IP e non può essere modificato, perché identifica ogni singolo dispositivo hardware della rete.

Interfaccia di rete

L'interfaccia di rete è un dispositivo che connette un computer ad altri computer tramite un mezzo di comunicazione. L'interfaccaia di rete può essere una scheda Ethernet, un modem, una scheda ISDN e così via. Il computer utilizza l'interfaccia di rete per l'invio e la ricezione dei pacchetti.

IPSEC

Il protocollo di protezione IPSEC (Internet Protocol Security) consente alle reti private di utilizzare l'autenticazione e la codifica del mittente. WinRoute supporta anche le varianti IPSEC implementate da Novell e Cisco.

L

LAN

La LAN (Local Area Network) è un gruppo di computer connessi tra loro in grado di condividere le risorse.

M

Mappatura della porta

La mappatura della porta (o Traslazione dell'indirizzo della porta - PAT) è il processo grazie al quale i pacchetti che arrivano all'interfaccia vengono controllati sulla base del numero di porta e dell'indirizzo IP di destinazione. In base ai numeri di porta, un indirizzo IP trova i pacchetti che sono stati inoltrati all'indirizzo IP predefinito di classe privata sulla rete locale.

Maschera di rete

La maschera di rete consente di creare un gruppo di indirizzi IP. Ad ogni gruppo di indirizzi viene assegnato un segmento di rete. Ad esempio, la maschera 255.255.255.0 raggruppa 254 indirizzi IP. Se esiste una sottorete 194.196.16.0 la cui maschera è 255.255.255.0, gli indirizzi che potranno essere assegnati ai computer della sottorete saranno compresi tra 194.196.16.1 e 194.196.16.254.

N

NAT

Con NAT - Network Address Translator - è possibile connettere una rete a Internet tramite un unico indirizzo IP, e i computer della rete utilizzerannp Internet come se fossero connessi direttamente (con alcune limitazioni).

La connessione di un'intera rete con un solo indirizzo IP registrato è possibile perché NAT sostituisce l'indirizzo di origine dei pacchetti inviati dal computer della rete locale con l'indirizzo del computer su cui WinRoute è in esecuzione.

NAT differisce significativamente da altri server proxy e gateway a livello di applicazione, perché è in grado di supportare un numero di protocolli molto maggiore.

P

Pacchetto

Un pacchetto è l'unità base utilizzata per la trasmissione dei dati da un computer all'altro. Ogni pacchetto contiene un certo numero di dati. La lunghezza massima del pacchetto dipende dal mezzo di comunicazione utilizzato. Nelle reti Ethernet, ad esempio, la lunghezza massima è di 1500 byte. In ciascun livello è possibile suddividere il contenuto del pacchetto in due parti: l'intestazione e i dati. L'intestazione contiene le informazioni relative a un particolare livello, i dati contengono invece le informazioni che appartengono al livello superiore. Per ulteriori informazioni sulla struttura del pacchetto, fare riferimento alla sezione sul filtro pacchetto.

POP3

Il protocollo **POP3** viene utilizzato principalmente dal software client di posta elettronica per prelevare i messaggi dalle cassette postali di un server di posta conforme a POP3. Il server di posta di WinRoute possiede tale funzionalità, e può pertanto prelevare automaticamente i messaggi da qualunque server di posta conforme a POP3 e distribuirli nelle cassette di posta dei destinatari locali.

POP3 è un protocollo di tipo **TCP** e utilizza la **porta 110** Se si desidera accedere al server di posta in esecuzione a valle o sul computer WinRoute (per prelevare i messaggi provenienti DA Internet) è necessario eseguire la **mappatura alla porta** 110 per inviare i messaggi all'indirizzo IP di **classe privata** del PC su cui viene eseguito il server di posta elettronica.

Porta

Una porta è un numero a 16 bit (l'intervallo ammesso è 1 - 65535) utilizzato dai protocolli del livello di trasporto TCP e UDP. Le porte servono per indirizzare le diverse applicazioni (servizi) eseguite sul computer. Se sul computer venisse sempre eseguita una sola applicazione, non ci sarebbe bisogno di avere più numeri di porta, e l'indirizzo IP sarebbe sufficiente per l'indirizzamenrto dei servizi.

In realtà è possibile che più applicazioni siano eseguite contemporaneamente su un dato computer, ed è pertanto necessario adottare un metodo che le differenzi tra loro. Questo metodo è precisamente il sistema di numerazione delle porte. Un numero di porta può essere infatti interpretato anche come l'indirizzo di un'applicazione all'interno del computer.

PPTP

PPTP (Point To Point Tunnelling Protocol) è un protocollo VPN utilizzato dai sistemi operativi Microsoft per creare una connessione crittata tra due computer.

Protocollo

Definisce le regole per la trasmissione dei dati.

Proxy

Proxy è un altro metodo di condivisione dell'accesso Internet. Agisce sui dati a un livello di protocollo più alto, e per questo motivo non è mai stato considerato un metodo di condivisione Internet particolarmente affidabile. Inoltre, richiede uno speciale gateway di applicazione per ogni protocollo di rete.

R

RAS

RAS (Remote Access Service) fa riferimento alla capacità di collegarsi in modalità remota a un computer o a una rete. Nel contesto di WinRoute, RAS identifica più semplicemente le connessioni di accesso remoto.

Record MX

I record MX contengono informazioni sugli altri server di posta elettronica di Internet. Essi consentono di aggirare il server di posta elelttronica del proprio provider Internet e consegnare la posta direttamente al server di posta di destinazione.

La procedura è vantaggiosa nel caso in cui il server di posta elettronica *non sia affidabile*. D'altro canto il fatto di cercare di recapitare i messaggi *a destinazione* può influire negativamente sul tempo di consegna. Qualora il *server di posta elettronica di destinazione* non fosse raggiungibile, la posta rimarrebbe nella coda dei messaggi *non inviati* sul server di posta di WinRoute.

S

SMTP

Il protocollo **SMTP** (Simple Mail Transfer Protocol) viene utilizzato per la comunicazione diretta tra i server di posta elettronica (quali il server di posta di WinRoute e quello del provider Internet) e per l'invio dei messaggi dal software client di posta elettronica. SMTP è un protocollo "a senso unico", ovvero consente l'invio e la ricezione dei messaggi dal server di posta elettronica, ma non permette di prelevare la posta da altri server.

Il protocollo SMTP funziona sulla **porta 25**. Se si desidera accedere a questo protocollo quando il server di posta elettronica è in esecuzione a valle o sul PC WinRoute (per consentire ad altri server di posta di inviare messaggi o per utilizzare il server per la posta in uscita all'interno della LAN) è necessario eseguire la **mappatura della porta** per il protocollo TCP, con la porta 25 inviata a un indirizzo IP **di classe privata** del PC su cui viene seguito il server di posta elettronica.

T

Tabella di routing

Le tabelle di routing sono degli insiemi di regole generate dai sistemi operativi Microsoft sulla base delle impostazioni eseguite per il protocollo TCP/IP. La tabella di routing viene utilizzata da WinRoute come insieme di regole per instradare i pacchetti. Per vedere la tabella di routing, passare alla finestra di prompt di MS-DOS e digitare il comando `route print`.

TCP/IP

TCP/IP è la somma di più protocolli di rete utilizzati per la comunicazione tra computer. Tutti i protocolli si basano sull'utilizzo dei pacchetti, il che significa che i dati vengono suddivisi in porzioni più piccole prima di essere inviati in rete. I protocolli TCP/IP sono: IP, TCP, UDP, ICMP e altri, sempre basati su IP.

U

UDP

Il protocollo UDP (User Datagram Protocol) utilizza un tipo speciale di pacchetti, chiamato datagramma. I datagrammi non richiedono risposta, perché sono a senso unico. Generalmente vengono utilizzati per il flusso multimediale, perché anche un'eventuale perdita di pacchetti non influenzerà la qualità finale del prodotto trasmesso.

V

VPN

VPN (Virtual Private Network) raggruppa le LAN capaci di condividere risorse su Internet, creando un tunnel diretto che esegue la codifica e la decodifica su entrambe le estremità. WinRoute supporta il networking privato virtuale tramite PPTP.

INDEX

A

B

C

L

M

N

O

P

Q

R

S

T

U

V