UŽIVATELSKÝ MANUÁL

WinRoute PRO

Tiny Software Inc.

©1997–2001 TINY Software Inc. Všechna práva vyhrazena.

AuthorIT™ je ochranná známka společnosti Optical Systems Corporation Ltd.

Microsoft Word, Microsoft Office, Windows®, Window 95™, Window 98™, Windows NT® and Windows 2000™ jsou registrované ochranné známky a ochranné známky společnosti Microsoft Corporation.

TINY Software
Sedláčkova 16
301 11 PLZEŇ
Česká Republika
Tel.: +420-19-7338901
E-Mail: support@tinysoftware.cz
WWW: http://www.tinysoftware.cz

OBSAH

Kapitola 1

ÚVOD

WinRoute Pro

WinRoute Pro je 32-bitová aplikace pro sdílení Internetu určená pro platformy Windows 95/98/ME a Windows NT/2000.

WinRoute je jednoduchý a bezpečný způsob připojení celé vaší lokální sítě do Internetu přes jedinou fyzickou internetovou přípojku. To může být např. analogový modem, ISDN linka, pevná linka či DirecPC.

Základní vlastnosti a součásti WinRoute Pro:

Transparentní přístup do Internetu

Díky revoluční technologii NAT (Network Address Translation, překlad IP adres) je možno za jedinou veřejnou IP adresu (statickou i dynamickou) skrýt celou lokální síť. Všechny počítače v lokální síti ale přitom mají plný přístup do Internetu. Narozdíl od klasického proxy serveru lze v tomto případě na lokálních počítačích provozovat většinu běžných aplikací tak, jako kdyby byla celá síť připojena přímo do Internetu.

Bezpečnost

Integrovaný firewall ochrání celou vaši síť včetně počítače, na němž je WinRoute Pro nainstalován. WinRoute poskytuje ochranu srovnatelnou s mnohonásobně dražšími hardwarovými firewally.

Konfigurace sítě a řízení přístupu

WinRoute vám umožní jednoduše řídit přístup lokálních uživatelů do Internetu, případně k jednotlivým službám. Vytváření chráněných a demilitarizovaných zón, provozování WWW, FTP nebo mailových serverů pod jedinou veřejnou IP adresou, změna bezpečnostních pravidel v průběhu dne – to je jen několik málo z možností, které vám WinRoute Pro nabízí!

Mailserver

Velmi těžko lze nalézt mailserver nabízející takové možnosti jako mailserver ve WinRoute Pro. Plně podporuje standardní protokoly SMTP a POP3

a umožňuje jednak přijímat poštu protokolem SMTP nebo vybírat libovolný počet POP3 schránek v Internetu a doručovat (popř. třídit) maily do lokálních schránek, případně obojí zároveň.

DHCP server

Vestavěný DHCP server umožní automaticky konfigurovat parametry protokolu TCP/IP (IP adresu, bránu, adresu DNS serveru atd.) na všech počítačích ve vaší lokální síti. Nemusíte tak vůbec nic nastavovat, stačí ponechat výchozí volbu „Získávat IP adresu automaticky“!

Proxy server s URL filtrem

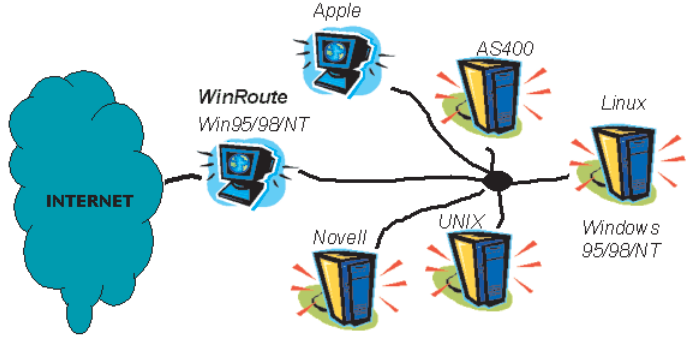
Přestože NAT umožňuje transparentní přístup do Internetu, obsahuje WinRoute Pro také proxy server s možností uchovávání často navštěvovaných stránek v cache a omezení přístupu uživatelů na konkrétní URL. Oba způsoby přístupu do Internetu lze samozřejmě kombinovat – např. ve WWW prohlížeči nastavit použití proxy serveru a v ostatních aplikacích využít přímý přístup přes NAT.

Vzdálená administrace

Oddělený administrační program umožňuje konfigurovat téměř všechna nastavení WinRoute nejen lokálně, ale i z libovolného počítače ve vaší lokální síti či v Internetu. Komunikace mezi WinRoute a administračním programem je plně šifrována, není tedy možné ji odposlouchávat a zneužít.

Různé operační systémy v lokální síti

WinRoute je vhodný pro připojení lokální sítě s různými operačními systémy. WinRoute funguje jako softwarový směrovač a podporuje standardní protokolovou sadu TCP/IP. WinRoute sice musí být nainstalován na počítači s operačním systémem Windows (95/98/ME/NT/2000), na ostatních počítačích ale může být provozován libovolný operační systém obsahující TCP/IP (Unix, MacOS atd.)



Možnost provozování na pracovní stanici

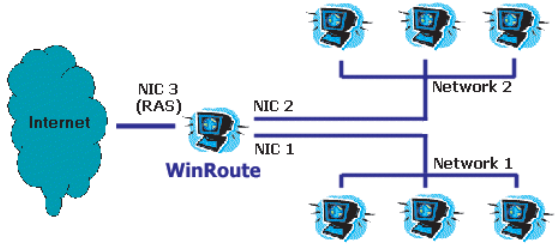
WinRoute Pro využívá za normálního provozu cca 1–20 % procesorového času. Počítač, na němž WinRoute běží, tedy může být rovněž využíván jako pracovní stanice – WinRoute nevyžaduje vyčleněný server.

Kapitola 2

INSTALACE

Systémové požadavky

WinRoute musí být nainstalován na počítač, který má přímé připojení do Internetu (analogovým modemem, ISDN, pevnou linkou apod.). Kromě toho musí mít alespoň jednu síťovou kartu (Ethernet nebo TokenRing) připojenou do lokální sítě.



WinRoute pak funguje jako směrovač mezi těmito rozhraními – tzn. každý příchozí IP paket je poslán na příslušné rozhraní (na základě cílové IP adresy).

Základní systémové požadavky na počítač, kde bude WinRoute Pro nainstalován:

- Procesor třídy Pentium nebo vyšší
- operační systém Windows 95 / 98 / ME / NT / 2000
- 32 MB operační paměti
- 2MB volného místa na disku (pouze pro instalaci WinRoute; v případě použití proxy cache je doporučeno alespoň 100 MB)
- minimálně 2 rozhraní (viz výše)

Operační systém Windows 95

V případě instalace WinRoute na počítač s Windows 95 je nutné pro zajištění bezproblémového chodu instalovat novější verze (upgrade) některých systémových součástí. Jsou to:

- Microsoft Dial-Up Networking (Telefonické připojení sítě) verze 1.3 (samozřejmě pouze v případě vytáčeného připojení do Internetu). Instalační archiv má název MSDUN13.EXE.
- V případě Windows 95A (nejstarší verze) také update knihovny COMCTL32.DLL. Archiv má název 401COMUPD.EXE.

Oba instalační balíky lze stáhnout buď přímo ze serverů fy. Microsoft, nebo také z adresy **http://www.tinysoftware.cz/ftp**.

Operační systém Windows NT 4.0 (Server / Workstation)

Je třeba instalovat Service Pack 3 nebo vyšší. Nedoporučuje se instalovat Service Pack 6, který obsahuje chybu v implementaci TCP/IP (později byla vydána oprava označovaná jako Service Pack 6a).

Konfliktní software

WinRoute může běžet na jednom systému s většinou běžných aplikací (včetně her apod.). Na tomtéž počítači však nemohou běžet aplikace používající stejné porty, tj. zejména SMTP / POP3 mailserver, DNS, DHCP a proxy server. Chcete-li zde některou z těchto aplikací provozovat, je třeba vypnout příslušný modul WinRoute.

Dále způsobují problémy zejména aplikace zasahující do síťového subsystému – proxy, firewally, ovladače zařízení apod. Uveďme alespoň několik nejrozšířenějších:

Bay Networks VPN klient (Nortel)

Přestože WinRoute podporuje protokol IPSec včetně implementace firmy Nortel, tento klient nemůže být provozován na jednom počítači společně s WinRoute. Klient musí být nainstalován na některý počítač ve vaší lokální síti.

Norton Antivirus

Používáte-li mailserver ve WinRoute, zakažte antivirovou kontrolu e-mailů. Jinak nebude mailserver fungovat správně. (Kontrola paměti a souborů na disku samozřejmě nevadí). Pro kontrolu příchozích e-mailů je v současné době možné použít pouze produkt Norton Antivirus for Internet E-mail Gateways (viz kapitola Speciální nastavení a příklady).

WinGate, MS Proxy server

Odinstalujte všechny komponenty těchto produktů (server i klienta) před instalací WinRoute.

WinProxy, MS Internet Connection Sharing (Sdílení Internetového připojení)

Oba tyto produkty používají nízkoúrovňové ovladače, které vykazují konflikt s ovladačem WinRoute.

Ovladače síťových karet

Používejte pokud možno standardní síťové karty renomovaných výrobců. Některé karty totiž mohou používat speciální instrukce a ovladač WinRoute pak nemůže s takovou kartou komunikovat. WinRoute se snaží podporovat co největší počet síťových karet, není ale možné testovat všechny modely všech výrobců. Zaznamenáte-li problémy s konkrétním typem síťové karty, můžete se obrátit na technickou podporu firmy TINY Software (viz **http://www.tinysoftware.cz**).

V každém případě se doporučuje nainstalovat nejnovější ovladače dané karty (zpravidla bývají k dispozici ke stažení na WWW stránkách příslušného výrobce).

Možná omezení

Jak bylo zmíněno v předchozí kapitole, WinRoute funguje především jako softwarový směrovač s překladem IP adres (NAT). To znamená, že ve všech paketech odcházejících z lokální sítě do Internetu je zdrojová IP adresa nahrazena IP adresou vnějšího síťového rozhraní. Celá lokální síť se pak navenek jeví jako jeden počítač s touto IP adresou (detailně viz kapitola NAT směrovač).

Z výše uvedeného vyplývá, že WinRoute se chová transparentně (tj. jako běžný směrovač) pro veškerou IP komunikaci zahájenou Z LOKÁLNÍ SÍTĚ. Toto je případ většiny běžných klientských aplikací (jako např. WWW prohlížeč, Telnet, FTP v pasivním módu atd.). Tyto aplikace lze provozovat zcela bez problémů a jejich použití nevyžaduje žádná další nastavení.

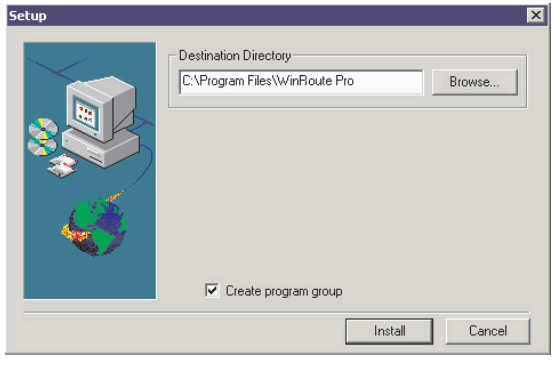
Problém nastává v případě aplikací typu SERVER. Serverová aplikace přijímá na určitém portu klientské požadavky a odpovídá na ně. Chce-li klient navázat spojení se serverem, vyšle požadavek na IP adresu a port, na němž server běží. Nachází-li se však server v síti za WinRoute, je z vnějšího pohledu skryt – klient z internetu „vidí“ pouze vnější IP adresu počítače s WinRoute. Přes NAT NENÍ MOŽNÉ navázat spojení zvenčí do lokální sítě.

Tento problém řeší WinRoute dvěma způsoby. Jednak obsahuje vestavěnou podporu pro celou řadu běžných aplikací (např. PPTP klient, ICQ atd.). V tomto případě nejsou třeba žádná speciální nastavení WinRoute ani aplikace – vestavěná podpora zpracuje správně celou komunikaci. Nemá-li aplikace ve WinRoute podporu, je možno použít tzv. mapování portů. Mapování portů umožní „přenést“ server (WWW, FTP atd.) z lokální sítě na vnější rozhraní počítače s WinRoute. Na každý port tohoto počítače může být samozřejmě namapován pouze jeden server.

Instalace

Instalační program (WinRoute Setup)

WinRoute Pro nainstalujete jednoduše spuštěním instalačního programu (typicky „wrp41en.exe“) z distribučního média. Nejnovější verzi WinRoute lze získat na Internetu na adrese **http://www.tinysoftware.cz**.



Po spuštění instalačního programu je možno zvolit adresář, kam bude WinRoute nainstalován. Dále lze zvolit, zda se má vytvářet skupina v nabídce Start –> Programy. Tlačítkem Install spustíte instalaci.

Celá instalace potrvá několik sekund (nejvýše několik desítek sekund). Po instalaci je nutno počítač restartovat, aby mohl být zaveden nízkoúrovňový ovladač WinRoute. Byla-li instalace úspěšná, WinRoute se po restartu automaticky spustí (podrobnosti viz následující kapitola).

➢ Poznámka: Provádíte-li upgrade, DOPORUČUJE SE instalovat WinRoute do téhož adresáře jako předchozí verzi. Zajistíte tím přepsání starých souborů a přenesení všech nastavení do nové instalace. Instalační program v tomto případě automaticky nabídne adresář předchozí instalace (namísto standardního „\Program Files\WinRoute Pro“). Zachovají se tak všechna nastavení včetně licence.

➢ Poznámka 2: V případě upgrade stávající verze je třeba ukončit všechny komponenty WinRoute – tedy WinRoute Engine, WinRoute Engine Monitor a WinRoute Administration!

Odinstalování WinRoute

Chcete-li WinRoute odstranit z vašeho počítače, postupujte následovně:

- Zastavte WinRoute Engine a ukončete aplikace WinRoute Engine Monitor a WinRoute Administration.
- Spusťte program Uninstall (z nabídky Start –> Programy –> WinRoute Pro) nebo zvolte odstranění WinRoute Pro v Ovládací Panely –> Přidat/Ubrat programy.
- Na výzvu počítač restartujte.

Po provedení těchto kroků bude WinRoute z vašeho počítače kompletně odstraněn (restart je nutný pro zavedení systému bez nízkoúrovňového ovladače WinRoute). V adresáři, kde byl WinRoute nainstalován, zůstanou podadresáře s logy a mailovými schránkami uživatelů.

Přenos WinRoute na jiný počítač

V některých případech může vzniknout požadavek přenesení WinRoute včetně kompletního nastavení a uživatelských mailových schránek na jiný počítač (např. má-li být počítač, kde WinRoute běží, nahrazen výkonnějším strojem nebo je nutno přeinstalovat systém Windows apod.). Aby nebylo nutné WinRoute znovu konfigurovat, je možno přenést stávající nastavení. Doporučený postup je následující:

- Na původním počítači (kde běží zkonfigurovaný WinRoute) nejprve zastavte WinRoute Engine, aby se do registru uložily i změny nastavení provedené od posledního spuštění WinRoute.
- Spusťte Editor registru (regedit.exe) a přepněte se do větve HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute. Volbou z menu Registr –> Uložit registrový soubor uložte tuto větev do souboru (např. „nastaveni.reg“).
- Na novém počítači spusťte instalaci WinRoute. Na výzvu o restart zvolte „I will restart the computer later“ (budu restartovat později) a importujte registrový soubor „nastaveni.reg“ (stačí jej pouze „spustit“ – např. v Průzkumníkovi).
- Na původním počítači otevřete adresář, v němž je WinRoute nainstalován (např. „C:\Program Files\WinRoute Pro“). Překopírujte podadresář „mail“ z tohoto adresáře do příslušného adresáře na novém počítači. Tím zajistíte, že uživatelé nepřijdou o své maily, které si z WinRoute dosud nestáhli.

- Je-li nový WinRoute nainstalován v jiném adresáři (či na jiném disku) než původní, je třeba nyní spustit Editor Registru a ve větvi HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute správně přenastavit všechny cesty (tj. položky „CacheDir“, „InstDir“, „LogsDir“, „MailDir“ a „MainDir“).
- Nyní nový počítač restartujte. Pokud jste již počítač restartovali dříve (tj. WinRoute již běží), jednoduše zastavte WinRoute Engine, proveďte import registrového souboru, překopírujte adresář „mail“ a WinRoute Engine opět spusťte. Výsledek bude tentýž.

Tento postup zajistí zachování všech nastavení WinRoute na původním počítači. Je však třeba dát pozor na dvě věci:

- Nový WinRoute bude obsahovat pouze ty uživatelské účty, které byly definovány v původním. Pokud tam byl odstraněn originální uživatel Admin, nebude existovat ani zde. V tomto případě je třeba si zapamatovat jméno a heslo uživatele, který má administrátorská práva!
- Nový počítač může obsahovat jiná síťová rozhraní (případně jiný počet rozhraní) než původní. Nová rozhraní budou po restartu správně detekována, ale v Interface Table mohou zůstat „mrtvá“ rozhraní z původního počítače. Ta lze ale jednoduše odstranit pomocí menu Settings –> Advanced –> Interface Maintenance.

Komponenty WinRoute

WinRoute Pro sestává ze tří součástí:

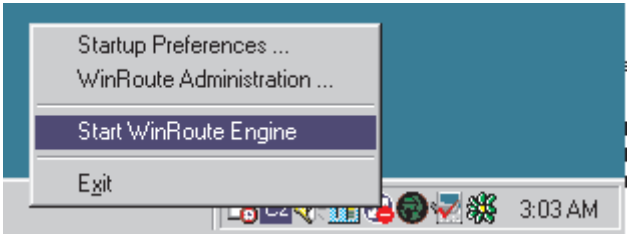
WinRoute Engine je vlastní výkonné jádro programu, které provádí všechny operace (směrování, filtrování paketů, zpracování mailů atd.). Běží jako aplikace na pozadí (ve Windows NT/2000 jako služba). Můžete jej spouštět a zastavovat pomocí WinRoute Engine Monitoru nebo nástrojem Služby v Ovládacích panelech (Windows NT/2000).

WinRoute Administration je uživatelské rozhraní pro konfiguraci WinRoute. Jedná se o samostatný program, který může být spouštěn i z jiného počítače než na kterém WinRoute běží. Detailní popis naleznete v kapitole Program WinRoute Administration.

WinRoute Engine Monitor je pomocný program, který zobrazuje stav WinRoute Engine (zda je spuštěn či zastaven). Zobrazuje se na liště (v system tray) jako modrobílá ikonka směrovače (logo WinRoute). Je-li WinRoute zastaven, signalizuje to ikona s červeným kolečkem.

Dvojitým kliknutím na ikonu levým tlačítkem myši se spustí program WinRoute Administration.

Po kliknutí pravým tlačítkem se zobrazí menu:



Startup Preferences – zde lze zvolit, zda se má po startu počítače automaticky spouštět WinRoute Engine a/nebo WinRoute Engine Monitor.

WinRoute Administration – spustí program WinRoute Administration (lze rovněž provést dvojitým kliknutím levým tlačítkem na ikoně).

Start / Stop WinRoute Engine – spouští a zastavuje WinRoute Engine (volba se mění v závislosti na jeho stavu).

Exit – ukončí WinRoute Engine Monitor.

➢ Pozor: Volba Exit ukončí pouze WinRoute Engine Monitor, nikoliv WinRoute Engine!

Kapitola 3

ADMINISTRACE WINROUTE

Lokální administrace

Chcete-li spravovat WinRoute přímo z počítače, na němž běží (dále jen „počítač s WinRoute“), proveďte následující:

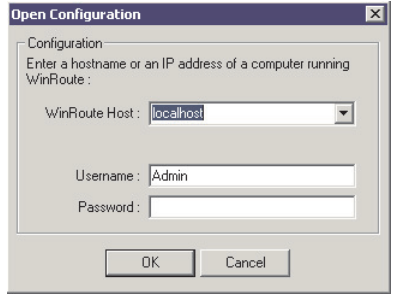
1. Zkontrolujte, zda je WinRoute Engine spuštěn

Spusťte program WinRoute Engine Monitor z menu Start –> Programy –> WinRoute Pro (pokud již neběží). Je-li přes ikonku na liště zobrazeno červené kolečko, znamená to, že WinRoute Engine neběží. Pravým tlačítkem na ikonce vyvolejte menu a volbou Start WinRoute Engine jej spusťte.

2. Spusťte program WinRoute Administration

Program spustíte buď dvojitým kliknutím na ikonku WinRoute Engine Monitoru na liště nebo z menu Start –> Programy –> WinRoute Pro.

Po spuštění se objeví přihlašovací dialog.



WinRoute Host je jméno či IP adresa počítače, na němž WinRoute běží. Pokud se přihlašujete lokálně (tj. přímo z tohoto počítače), vždy zde ponechte nastaveno „localhost“. Tak se můžete přihlásit i v případě, že dojde k výpadku síťového subsystému nebo že je TCP/IP komunikace zablokována z důvodu vypršení testovací periody. Zadejte jméno a heslo uživatele s administrátorskými právy (detaily viz kapitola Uživatelské účty).

- Poznámka: Pro prvotní přihlášení (než vytvoříte vlastní uživatelské účty) použijte vestavěný účet „Admin“ s prázdným heslem (tj. pole Password nevyplňujte).
- Poznámka 2: Od verze 4.1 se v uživatelských jménech nerozlišují malá a velká písmena (např. „admin“ je totéž co „Admin“). V heslech se ale malá a velká písmena vždy rozlišují!

Po úspěšném přihlášení se jméno počítače s WinRoute (např. „localhost“) objeví v titulku okna a položky menu se aktivují. Nyní můžete provádět veškeré administrační úkony.

Proč se nelze přihlásit?

Přihlášení může selhat z těchto důvodů:

- WinRoute Engine je zastaven. Použijte WinRoute Engine Monitor ke kontrole jeho stavu.
- Špatné uživatelské jméno, heslo či obojí. Nezapomeňte, že v hesle se rozlišují malá a velká písmena!
- Nemáte administrátorská práva. Detaily naleznete v kapitolách Uživatelské účty, případně Ztráta administrátorského hesla.

Administrace z lokální sítě

Stejně jako z počítače, na němž je nainstalován, můžete WinRoute spravovat i z libovolného počítače ve vaší lokální síti. Komunikace administračního programu s WinRoute Engine je silně šifrována, což znemožňuje její odposlech a zneužití.

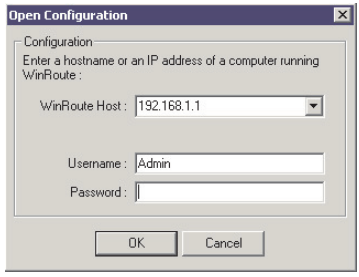
Postup je následující:

1. Zkopírujte program WinRoute Administration

V adresáři, kde je WinRoute nainstalován (typicky „C:\Program Files\WinRoute Pro“) nalezněte soubor „WRAdmin.exe“, zkopírujte jej na vybraný počítač a tam jej spusťte.

2. Přihlaste se ke vzdálenému WinRoute Engine

Do pole „WinRoute Host“ zadejte IP adresu (např. „192.168.1.1“) nebo jméno (např. „server.firma.cz“) počítače, na němž WinRoute běží. Zadejte jméno a heslo uživatele s administrátorskými právy.



Po úspěšném přihlášení máte přístup ke všem nastavením, až na následující výjimky:

- nelze importovat uživatele z NT domény (Settings –> Accounts –> Advanced)
- nelze editovat Windows RAS položky (resp. položky Telefonického připojení) v Interface Table
- nelze editovat soubor HOSTS (Settings –> DNS Forwarder –> Edit File)

Proč se nelze přihlásit?

Přihlášení může selhat z těchto důvodů:

- špatná kombinace jméno / heslo nebo WinRoute neběží (viz předchozí kapitola)
- špatné jméno nebo IP adresa v poli „WinRoute Host“
- vzdálená administrace není povolena. Ujistěte se, že je zaškrtnutá volba „Enable remote administration over network“ v menu Settings –> Advanced –> Remote Administration
- vzdálená administrace není povolena z konkrétní IP adresy. To může být nastaveno buď volbou „Allow access only from:“ v menu Settings –> Advanced –> Remote Administration nebo paketovým filtrem. Detaily naleznete v kapitolách Skupiny IP adres a Filtrování paketů.

Administrace z Internetu

Podobně jako případě lokální sítě je možno se připojit na vzdálený WinRoute z libovolného počítače v Internetu.

Pokud je však aktivován NAT, je celá lokální síť včetně počítače s WinRoute chráněna firewallem a není možné navázat spojení na žádný port tohoto počítače. Chcete-li se tedy připojit k WinRoute Engine „zvenčí“, je třeba provést **mapování portů**. Detaily naleznete v kapitole Mapování portů.

Pro přístup k administraci WinRoute je třeba namapovat port 44333 pro protokoly TCP a UDP. V menu Settings –> Advanced –> Port Mapping přidejte tlačítkem Add... následující mapování:

Protocol: TCP/UDP

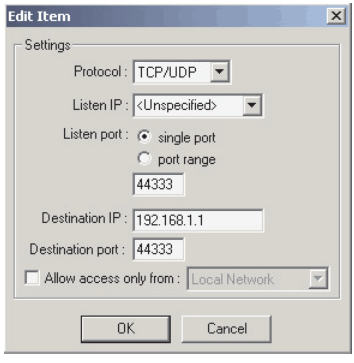
Listen IP: <Unspecified> (znamená primární adresu vnějšího rozhraní – pokud zde máte přiřazeno více adres, uveďte tu, na kterou se chcete připojovat)

Listen Port: 44333

Destination IP: IP adresa rozhraní do lokální sítě (např. „192.168.1.1“)

Destination Port: 44333

Allow acces only from: Tato volba umožňuje povolit přístup k mapovanému portu jen z určitých IP adres. Detaily naleznete v kapitole WinRoute – Popis a nastavení / Nástroje / Skupiny IP adres.



Dále postupujte stejně jako v případě administrace z lokální sítě (viz předchozí kapitola).

Proč se nelze přihlásit?

Přihlášení může selhat z těchto důvodů:

- špatná kombinace jméno / heslo nebo WinRoute neběží (viz předchozí kapitola)
- špatné jméno nebo IP adresa v poli „WinRoute Host“
- počítač s WinRoute není dostupný. Jeho dostupnost můžete ověřit např. příkazem „ping“.
- vzdálená administrace není povolena. Ujistěte se, že je zaškrtnutá volba „Enable remote administration over network“ v menu Settings –> Advanced –> Remote Administration

- vzdálená administrace není povolena z konkrétní IP adresy. To může být nastaveno buď volbou „Allow access only from:“ v menu Settings –> Advanced –> Remote Administration nebo paketovým filtrem. Detaily naleznete v kapitolách Skupiny IP adres a Filtrování paketů.
- port 44333 není namapován nebo je zde použita volba „Allow access only from“ omezující přístup na mapovaný port.

Licenční klíč

Po úspěšné instalaci WinRoute je třeba zadat licenční klíč. Pokud tak neučiníte, WinRoute se bude chovat jako demoverze, tzn. že po 30 dnech přestane fungovat a zablokuje veškerou TCP/IP komunikaci. Pak musíte buď zadat platný licenční klíč nebo zastavit WinRoute Engine (případně WinRoute odinstalovat).

Z toho zároveň vyplývá, že rozdíl mezi demoverzí a plnou verzí WinRoute je pouze v tom, zda se do něj zadá platný licenční klíč či nikoliv. Každý zákazník má možnost si WinRoute v třicetidenní lhůtě vyzkoušet, a pokud si jej zakoupí, stačí pouze zadat získaný licenční klíč do nainstalované demoverze. Není tedy třeba WinRoute přeinstalovávat a znovu nastavovat.

Zadání licenčního klíče do WinRoute

Spusťte program WinRoute Administration a přihlaste se. V menu Help –> About Application stiskněte tlačítko Set Licence... a zadejte obě části licenčního klíče. Je-li zadaný klíč správný, objeví se v okně About číslo licence (první část licenčního klíče) a informace o licenci (např. „Licensed for 25 users“). Druhá část licenčního klíče se nezobrazuje – klíč tak nemůže být přečten a zneužit.

Zadat licenční klíč můžete i v případě, že již vypršela třicetidenní testovací perioda a WinRoute je v „zablokovaném“ stavu. Stále je totiž možné se lokálně přihlásit administračním programem (v poli WinRoute Host je nutno uvést „localhost“). Zadáním platného licenčního klíče se WinRoute (a s ním i celá TCP/IP komunikace) odblokuje a může být dále používán.

Licenční klíč nebyl přijat?

Chybně zadaný licenční klíč WinRoute samozřejmě odmítne. Může však nastat případ, že zadáte správný licenční klíč a WinRoute zahlásí chybu „Too many users for this licence“. To znamená, že je ve WinRoute vytvořeno víc uživatelských účtů než povoluje zakoupená licence (demoverze se chová jako verze pro neomezený počet uživatelů). Pak je nutné buď nějakého uživatele odstranit anebo dokoupit licenci pro větší počet uživatelů.

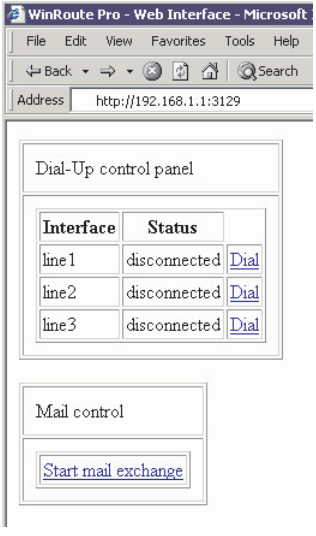
➢ Poznámka: Do celkového počtu uživatelů se započítává i originální uživatel Admin. Ten samozřejmě může být odstraněn, ale pak je nutné před jeho smazáním alespoň jednomu z dalších uživatelů přidělit administrátorská práva! Detaily naleznete v kapitole Uživatelské účty.

WWW administrační rozhraní

Kromě odděleného administračního programu obsahuje WinRoute navíc jednoduché WWW rozhraní umožňující dálkově vytáčet a zavěšovat modemové linky a spustit odeslání a příjem mailu (Mail Transfer).

K tomuto rozhraní se lze připojit libovolným WWW prohlížečem, jestliže v něm zadáte adresu či jméno počítače s WinRoute a port 3129. URL tedy bude mít tvar „http://192.168.1.1:3129“ nebo „http://server.firma.cz:3129“.

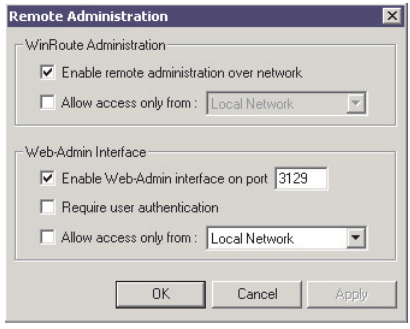
➢ Poznámka: Je NUTNÉ specifikovat protokol, tedy „http://“!



WWW rozhraní není chráněno – může jej použít libovolný uživatel ve vaší lokální síti. Chcete-li povolit přístup jen některým uživatelům, je to třeba specifikovat v nastavení vzdálené administrace – viz následující kapitola.

Nastavení vzdálené administrace

V menu Settings –> Advanced –> Remote Administration můžete povolit či zakázat vzdálenou administraci a/nebo WWW administrační rozhraní, případně omezit přístup uživatelů k administraci.



WinRoute Administration

První volba povoluje / zakazuje vzdálenou administraci WinRoute (je-li zakázána, lze se připojit pouze na „localhost“). Volba „Allow access only from:“ umožňuje zvolit skupinu IP adres, ze kterých bude administrace povolena (detaily naleznete v kapitole WinRoute – Popis a nastavení / Nástroje / Skupiny IP adres).

➢ Poznámka: V případě přístupu k administraci z Internetu přes mapovaný port se kombinuje volba „Allow access only from:“ s toutéž volbou u mapovaného portu. Doporučuje se volbu zapnout pouze na jednom místě, případně na obou místech uvést tutéž skupinu.

Web-Admin Interface

První volba povoluje / zakazuje vestavěný HTTP server, který poskytuje jednoduché WWW administrační rozhraní. Je zde možno zvolit port, na kterém bude toto rozhraní přístupné. Nedoporučuje se volit port menší než 1024, protože tyto porty jsou rezervovány pro systémové služby (výjimkou může být port 80 – pokud na tomto počítači neběží žádný WWW server, pak volba portu 80 umožní přístup k administračnímu rozhraní bez nutnosti specifikovat port – tedy např. „http://192.168.1.1“).

Volba „Require user authentication“ způsobí, že při volbě akce (Dial / Hangup / Mail Transfer) bude nutno zadat uživatelské jméno a heslo (samozřejmě uživatele, který má administrační práva do WinRoute). Volba „Allow access only from:“ opět povoluje přístup jen z vybrané skupiny IP adres.

Ztráta administrátorského hesla

V případě, že zapomenete administrátorské heslo, nebo se vám podaří smazat posledního uživatele s administrátorskými právy, nepropadejte panice, ale kontaktujte technickou podporu firmy TINY Software, kde vám rádi ochotně pomohou. Kontakty naleznete na konci tohoto manuálu, případně na WWW stránkách **http://www.tinysoftware.cz**.

Postup, jak opět získat přístup k administraci, je poměrně jednoduchý, ale z bezpečnostních důvodů jej v manuálu neuvádíme.

Kapitola 4

NASTAVENÍ WINROUTE A LOKÁLNÍ SÍTĚ

Rychlé nastavení (Quick Checklist)

Tato kapitola popisuje základní nastavení, jejichž provedení zajistí okamžitý přístup do Internetu ze všech počítačů ve vaší lokální síti.

Nastavení a pravidla pro počítač s WinRoute

1 Dvě síťová rozhraní
Počítač s WinRoute musí mít (alespoň) dvě síťová rozhraní: jedno do Internetu a druhé do lokální sítě. Rozhraní do Internetu může být např. modem, ISDN, síťová karta nebo DirecPC adaptér, rozhraní do lokální sítě pak síťová karta typu Ethernet nebo TokenRing.

2 Zapněte NAT na INTERNETOVÉM rozhraní!
Volba NAT musí být zapnuta na rozhraní vedoucím do Internetu. V menu zvolte Settings –> Interface Table, zde vyberte příslušné rozhraní, stiskněte tlačítko Properties a v záložce NAT zapněte volbu „Perform NAT with the IP address of this interface on all communication passing through". **POZOR:** Nezapínejte volbu „Exclude this computer from NAT"! Tato volba zruší firewallovou ochranu počítače s WinRoute a ten se tak stane nechráněným vůči útokům z Internetu.

3 NEZAPÍNEJTE NAT na vnitřním rozhraní!
Přesvědčete se, že volba „Perform NAT..." NENÍ zapnutá na žádném rozhraní vedoucím do lokální sítě.

4 Nenastavujte ŽÁDNOU výchozí bránu na vnitřních rozhraních!
Na vnitřních rozhraních NESMÍ být nastavena výchozí brána. Na internetovém rozhraní bude samozřejmě výchozí brána nastavena podle údajů vašeho poskytovatele Internetu (zpravidla konfigurováno dynamicky).

5 Nastavte správně parametry DHCP serveru!
Nejjednodušším způsobem nastavení ostatních počítačů v lokální síti je použití DHCP serveru. Pokud jej zapnete, nezapomeňte správně nastavit

rozsah přidělovaných IP adres a ve volitelných parametrech (Options) alespoň adresu brány (Default Gateway) a DNS serveru – obojí na IP adresu vnitřního rozhraní počítače s WinRoute.

Nastavení ostatních počítačů v lokální síti

Použijete-li DHCP server (viz výše), není třeba na ostatních počítačích nic nastavovat. Ve vlastnostech protokolu TCP/IP jednoduše ponechte výchozí volbu „Získávat IP adresu automaticky“. Nechcete-li nebo nemůžete-li DHCP server z nějakého důvodu použít,

1. **Výchozí bránou je IP adresa vnitřního rozhraní počítače s WinRoute!** Počítač s WinRoute je VÝCHOZÍ BRÁNOU (default gateway) pro všechny počítače ve vaší lokální síti. Nastavte správně bránu ve vlastnostech protokolu TCP/IP! **POZNÁMKA:** Toto platí v případě, že je vaše lokální síť tvořena pouze jedním IP segmentem (tedy bez interních směrovačů). Popis nastavení pro více lokálních segmentů naleznete v kapitole Nastavení a příklady.

2. **Zapněte používání DNS a nastavte správně adresu DNS serveru!** Na lokálních počítačích musí být nastavena adresa (alespoň jednoho) DNS serveru. Můžete nastavit buď přímo DNS server vašeho poskytovatele Internetu, nejvhodnější však je použít DNS Forwarder ve WinRoute (zejména v případě vytáčené linky). V tomto případě nastavíte jako adresu DNS serveru rovněž adresu vnitřního rozhraní počítače s WinRoute (tedy stejně jako výchozí bránu).

➢ Poznámka: Ve Windows 95/98/ME je v záložce DNS třeba vyplnit položku Hostitel (Host), případně Doména (Domain). Hostitel je název vlastního počítače (shodný se jménem počítače v záložce Identifikace), NIKOLIV název počítače s WinRoute! Doména je pak název vaší domény (např. „firma.cz“). V případě, že vlastní doménu nemáte, ponechte tuto položku prázdnou.

Nastavení lokální sítě

IP adresa, maska subsítě

IP adresa je 32-bitové číslo, které jednoznačně identifikuje počítač v Internetu (dva počítače v Internetu nemohou mít shodnou IP adresu). Pro větší přehlednost se zapisuje jako čtyři byty oddělené tečkami (např. „1.2.3.4“).

Maska subsítě určuje, jaká část IP adresy adresuje síť a jaká počítač v rámci této sítě. Maska se zapisuje ve stejné notaci jako IP adresa, je však třeba ji vidět jako 32-bitové dvojkové číslo.

V jednom IP segmentu (tzv. subsíti) musejí mít všechny počítače stejnou masku subsítě a stejnou síťovou část IP adresy, jinak není komunikace protokolem IP možná. Jednotlivé IP segmenty musejí být odděleny IP směrovači.

Příklad:

IP adresa počítače v lokální síti je 192.168.1.1, maska subsítě je 255.255.255.0. Tuto masku lze zapsat ve dvojkové soustavě takto:

11111111.11111111.11111111.00000000

V tomto případě je tedy IP adresa rozdělena tak, že první 3 byty (tedy 192.168.1) znamenají adresu subsítě a poslední byte (1) adresu počítače v rámci této subsítě. Počítače v této subsíti mohou mít IP adresy 192.168.1.1 – 192.168.1.254.

Speciální IP adresy

IP adresy v určitém tvaru jsou vyhrazeny pro zvláštní účely a nelze je použít jako adresy počítačů. Jsou to následující:

- síť = xxx, počítač = 0..0 – např. 192.168.1.0

  Tato adresa označuje celou subsíť, též se nazývá adresa sítě. Znamená rozsah všech IP adres v dané subsíti.
- síť = 0..0, počítač = xxx – např. 0.0.0.1

  Znamená IP adresu v rámci lokální subsítě.
- síť = xxx, počítač = 1..1 – např. 192.168.1.255

  Všeobecná adresa (broadcast) – adresuje všechny počítače v dané subsíti.
- síť = 1..1, počítač = 1..1 – např. 255.255.255.255

  Omezená všeobecná adresa (limited broadcast) – adresuje všechny počítače v lokální subsíti.
- síť = 1..1, počítač = xxx – např. 255.255.255.1
- síť = 1..1. počítač = 0..0 – např. 255.255.255.0

  Tyto IP adresy jsou nepřípustné.

Privátní IP adresy

Existují určité vyhrazené rozsahy IP adres, které jsou určeny pro privátní sítě (tj. sítě, které nejsou zapojeny do Internetu – typicky lokální síť, která je připojena přes 1 IP adresu). Tyto IP adresy jsou nesměrovatelné (tzn. směrovače v Internetu pakety s těmito IP adresami zahazují).

Ve vaší lokální síti chráněné NAT je doporučeno používat IP adresy z těchto rozsahů. Použijete-li totiž libovolně (náhodně) zvolené IP adresy, riskujete, že tyto adresy již v Internetu existují a s takovou subsítí pak nebude možno z lokální sítě komunikovat.

Vyhrazené rozsahy privátních IP adres jsou tyto:

- 10.0.0.0, nejkratší maska: 255.0.0.0
- 172.16.0.0, nejkratší maska: 255.240.0.0
- 192.168.0.0, nejkratší maska: 255.255.0.0

„Nejkratší maska“ vymezuje daný rozsah. V rámci tohoto rozsahu můžete změnou masky definovat více subsítí – např. 192.168.1.0 / 255.255.255.0 a 192.168.2.0 /255.255.255.0 jsou regulérní privátní subsítě.

Co je to výchozí brána?

Výchozí brána (Default Gateway) je zařízení v síti (směrovač), na něž se posílají IP pakety s takovou cílovou adresou, která nepatří do lokální sítě, do níž je počítač přímo připojen.

Příklad:

Lokální počítač má jednu síťovou kartu s IP adresu 192.168.1.23. Maska subsítě je 255.255.255.0. Bude-li odchozí paket mít cílovou IP adresu 192.168.1.x (kde x je v rozsahu 1 až 255), znamená to, že je určen pro počítač v téže síti, který je přímo dosažitelný. Tento paket bude přímo odeslán na cílový počítač.

Bude-li ale cílová adresa jiná (např. 145.12.220.1), není takový počítač dosažitelný v lokální síti. Je-li na odesílajícím počítači nastavena výchozí brána, znamená to, že každý takový paket bude odeslán na tuto bránu. Tak bude moci být poslán do jiné subsítě (a tímto způsobem postupně až na cílový počítač).

Zjednodušeně tedy lze říci, že na bránu se posílá každý IP paket, který není určen do lokální sítě. Z toho vyplývají tyto dvě skutečnosti:

1 Výchozí brána MUSÍ být nastavena, chcete-li protokolem IP komunikovat s počítači mimo vaši lokální síť.

2 Výchozí brána MUSÍ být dosažitelná v rámci lokální sítě – její adresa musí patřit do této sítě.

➢ Poznámka: Tyto skutečnosti je třeba si dobře uvědomit, zejména v případě, že přecházíte na WinRoute z klasického proxy serveru. Proxy server z principu nastavení výchozí brány nepotřebuje, protože je zde oddělena komunikace klient – proxy a proxy – cílový server. WinRoute se však chová

jako směrovač, a proto je nastavení výchozí brány vyžadováno! Absence výchozí brány na lokálních stanicích je jedním z nejčastějších důvodů, proč sdílení internetového připojení přes WinRoute nefunguje.

Použití DHCP serveru ve WinRoute

Použití DHCP serveru je nejjednodušší způsob konfigurace protokolu TCP/IP na lokálních počítačích. V tomto případě totiž nemusíte nastavovat vůbec nic, pouze ponecháte výchozí volbu „Získávat IP adresu automaticky“.

POZOR: Použijete-li tuto volbu, NENASTAVUJTE ve vlastnostech TCP/IP žádnou bránu ani DNS server! DHCP server přidělí všechny tyto parametry společně s IP adresou. Pokud byly stanice dříve nastaveny ručně a nyní je přepínáte na automatickou konfiguraci, SMAŽTE všechna nastavení výchozí brány a DNS!

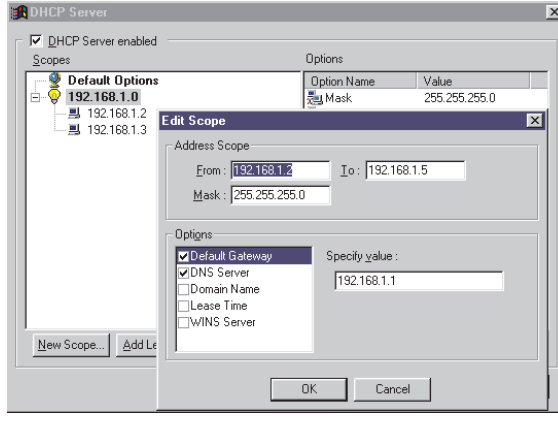
Nastavení DHCP serveru ve WinRoute:

1 V hlavním menu zvolte Settings / DHCP Server.

2 Zapněte DHCP server (tj. zaškrtněte volbu „DHCP Server enabled“).

3 Tlačítkem „New Scope...“ přidejte nový rozsah přidělovaných IP adres. Celý rozsah musí samozřejmě náležet do jedné subsítě a odpovídat zadané masce. **POZOR:** IP adresa vnitřního rozhraní musí být přiřazena PEVNĚ (tedy ručně) a nesmí být obsažena v rozsahu, z něhož DHCP server adresy přiděluje!

4 V poli „Options“ nastavte volitelné parametry, které bude DHCP server přidělovat společně s IP adresou (alespoň adresu výchozí brány a DNS serveru). Zaškrtnutím vždy zvolte parametr, který chcete přidělovat, a v poli „Specify value“ zadejte jeho hodnotu (např. IP adresu).



Použití jiného DHCP serveru

Pro automatickou konfiguraci lokálních počítačů je samozřejmě možné použít i jiný DHCP server než ten ve WinRoute. Pokud již ve vaší síti nějaký DHCP server běží, můžete jej využívat i nadále.

V tomto případě však zkontrolujte nastavení volitelných parametrů, které váš DHCP server přiděluje. Je bezpodmínečně nutné, aby přiděloval IP adresu výchozí brány a DNS serveru. Oba tyto parametry by měly obsahovat IP adresu vnitřního rozhraní počítače s WinRoute.

POZOR: Adresa vnitřního rozhraní WinRoute musí být nastavena pevně (ručně) a nesmí být obsažena v rozsahu adres, které váš DHCP server přiděluje!

V principu je možné, aby ve vaší síti běželo i více DHCP serverů současně, ale nedoporučuje se to. Chcete-li provozovat více DHCP serverů (např. z důvodu spolehlivosti), dejte pozor, aby se rozsahy přidělovaných adres nepřekrývaly – pak by mohlo docházet k vícenásobnému přidělení téže IP adresy různým stanicím.

Manuální konfigurace

Rozhodnete-li se konfigurovat počítače ve vaší lokální síti manuálně, je třeba nastavit alespoň následující parametry protokolu TCP/IP:

IP adresa

V lokální síti skryté za firewallem by měly být používány IP adresy z některého privátního rozsahu, tj. 10.x.x.x, 192.168.x.x nebo 172.16.x.x. Tyto adresy jsou vyhrazeny pro privátní sítě a nemohou se vyskytnout nikde v Internetu. Zvolte si schéma, podle kterého budete IP adresy přidělovat.

- Příklad 1: zvolíte adresy 192.168.1.x a masku subsítě 255.255.255.0. Takto můžete přidělit IP adresy 192.168.1.1 až 192.168.1.254 (adresy 192.168.1.0 a 192.168.1.255 mají zvláštní význam a nelze je použít jako adresy počítačů!).
- Příklad 2: 254 adres z předchozího příkladu nestačí – zvolíte adresy 192.168.x.x s maskou 255.255.0.0. Pak můžete ve vaší lokální síti přiřazovat adresy 192.168.0.1 až 192.168.255.254.

Díky možnosti definovat síťovou masku po jednotlivých bitech existuje mnoho dalších možností, jak zvolit IP adresy pro vaši lokální síť. V praxi je však rozdělení po jednotlivých bytech (tj. maska obsahuje jen hodnoty 255 a 0) zpravidla postačující.

Výchozí brána

Výchozí bránu na všech počítačích ve vaší síti nastavte na IP adresu VNITŘNÍHO rozhraní počítače s WinRoute. Doporučuje se přiřadit tomuto rozhraní nějakou snadno zapamatovatelnou IP adresu (např. 192.168.1.1, 192.168.1.100 apod.). Snížíte tak pravděpodobnost chyby při zadávání adresy výchozí brány na ostatních počítačích.

Nastavení DNS

Na všech počítačích je rovněž nutné nastavit adresu alespoň jednoho DNS serveru, aby bylo možno navázat spojení s počítačem zadaným DNS jménem (jinak by bylo nutno odkazovat všechny cílové počítače IP adresou). Adresu DNS serveru je nejvhodnější nastavit na VNITŘNÍ rozhraní počítače s WinRoute – vestavěný DNS Forwarder zajistí předání dotazu DNS serveru v Internetu, rychlé zodpovídání opakovaných dotazů, vytáčení na DNS dotazy (v případě dial-up připojení) a případně může fungovat také jako jednoduchý DNS server pro Vaši lokální doménu.

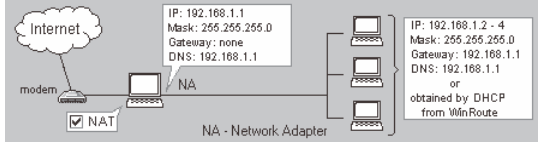
Místo DNS Forwarderu můžete nastavit přímo IP adresu DNS serveru vašeho poskytovatele Internetu (pro dial-up připojení se ale nedoporučuje) nebo IP adresu DNS serveru běžícího přímo ve vaší lokální síti (vypnete-li DNS Forwarder, může běžet i na tomtéž počítači jako WinRoute).

Připojení vaší sítě k Internetu

Vytáčené (dial-up) připojení – analogový modem nebo ISDN

V tomto případě musí být WinRoute nainstalován na počítač, který má:

- modem připojený k ISDN nebo telefonní lince
- síťovou kartu vedoucí do lokální sítě



Před zahájením instalace WinRoute...

Před spuštěním instalačního programu zkontrolujte zejména následující:

- na počítači je nainstalován protokol TCP/IP a je správně nakonfigurován (viz kap. Rychlé nastavení nebo Nastavení lokální sítě).

➢ TIP: Na vnitřní síťové kartě nastavte adresu DNS serveru „samu na sebe" (tj. stejnou adresu, jako má samotná karta). Tím zajistíte, že i DNS dotazy z tohoto počítače budou předávány DNS Forwarderu ve WinRoute. Je to jediný způsob, jak zajistit vytáčení na žádost z tohoto počítače (bude fungovat samozřejmě pouze tehdy, bude-li cílový počítač zadán DNS jménem a ne IP adresou).

- je nainstalována služba Telefonické připojení (Windows 95/98/ME) nebo RAS (Vzdálený přístup – Windows NT/2000)
- modem je připojen k lince i k počítači a je zapnut

WinRoute používá k připojování do Internetu standardní službu Telefonické připojení (příp. RAS). Je doporučeno vytvořit příslušnou položku připojení ještě PŘED instalací WinRoute a vyzkoušet funkčnost tohoto připojení. Ušetříte si tak mnoho problémů při odhalování chyb po instalaci WinRoute.

Konfigurace WinRoute

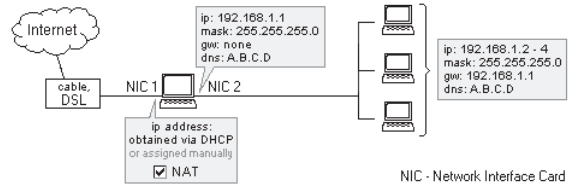
- Po instalaci WinRoute zvolte menu Settings –> Interface Table. Vyberte rozhraní „line1" (připravená interní linka WinRoute) a stiskněte tlačítko Properties.
- V záložce NAT zkontrolujte, zda je zaškrtnuta volba „Perform NAT with IP address of this interface on all communication passing through" (tato volba by měla být standardně zapnutá, protože WinRoute předpokládá, že RAS linka se používá pro připojení do Internetu). NEZAPÍNEJTE volbu „Exclude this computer from NAT"!
- V záložce RAS vyberte v poli „RAS Entry" položku telefonického připojení, kterou chcete používat pro připojení do Internetu. Tlačítkem Settings je možno upravit její vlastnosti (stejně jako v Ovládacích pane-

lech), případně vytvořit novou položku, pokud dosud žádná neexistuje. K vybrané položce je zde třeba zadat jméno a heslo.

- Dále můžete nastavit způsob vytáčení – ručně („Manual“), na žádost („On Demand“ – výchozí volba), trvalé připojení („Persistent“), případně nastavit, jak se bude způsob vytáčení v čase měnit („Custom“).
- Volba „Hang up if idle for:“ umožňuje nastavit dobu, po které se linka automaticky zavěsí, jestliže neprocházejí žádná data. Volba „Redial when busy:“ znamená počet opakování vytáčení, jestliže je linka obsazená, a „Reconnect on line failure“ umožní automatické obnovení spojení při výpadku linky.
- Na VNITŘNÍ síťové kartě NEZAPÍNEJTE volbu „Perform NAT with IP address of this interface on all communication passing through“!!!

Připojení kabelovým modemem nebo xDSL

Připojení kabelovým modemem, případně xDSL (ADSL, SDSL, ...) vyžaduje v počítači WinRoute dvě síťové karty: jednu pro připojení kabelového (či xDSL) modemu a druhou pro připojení lokální sítě.



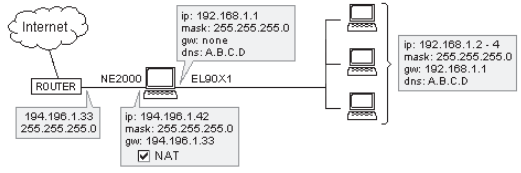
Konfigurace síťových karet a WinRoute

- Parametry protokolu TCP/IP na kartě připojené ke kabelovému (xDSL) modemu nastavte podle údajů získaných od vašeho poskytovatele Internetu (buď zadáte parametry ručně nebo nastavíte „Získávat IP adresu automaticky“).
- Na kartě vedoucí do vnitřní sítě nastavte ručně IP adresu a masku subsítě. NENASTAVUJTE zde žádnou výchozí bránu! Adresu DNS serveru můžete nastavit buď na DNS server providera, nebo na tutéž adresu, jakou má samotná karta (aby se DNS dotazy předávaly DNS Forwarderu). Pokud však nepoužíváte-li DNS pro lokální komunikaci, není nutné zde adresu DNS serveru vůbec nastavovat (adresa DNS serveru je systému známa z nastavení druhé karty).
- Ve WinRoute zvolte menu Settings –> Interface Table, vyberte kartu vedoucí do Internetu a stiskněte tlačítko „Properties“. V záložce NAT zapněte volbu „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!

- Na VNITŘNÍ síťové kartě NEZAPÍNEJTE volbu „Perform NAT with IP address of this interface on all communication passing through“!!!

Připojení lokální sítí (LAN)

Připojení lokální sítí vyžaduje v počítači WinRoute dvě síťové karty: jednu pro připojení do Internetu (zpravidla ke směrovači či mikrovlnné anténě) a druhou pro připojení vaší lokální sítě.



Konfigurace síťových karet a WinRoute

- Parametry protokolu TCP/IP na kartě připojené do Internetu nastavte podle údajů získaných od vašeho poskytovatele Internetu (buď zadáte parametry ručně nebo nastavíte „Získávat IP adresu automaticky“).
- Na kartě vedoucí do vnitřní sítě nastavte ručně IP adresu a masku subsítě. NENASTAVUJTE zde žádnou výchozí bránu! Adresu DNS serveru můžete nastavit buď na DNS server providera, nebo na tutéž adresu, jakou má samotná karta (aby se DNS dotazy předávaly DNS Forwarderu). Pokud však nepoužíváte-li DNS pro lokální komunikaci, není nutné zde adresu DNS serveru vůbec nastavovat (adresa DNS serveru je systému známa z nastavení druhé karty).
- Ve WinRoute zvolte menu Settings –> Interface Table, vyberte kartu vedoucí do Internetu a stiskněte tlačítko „Properties“. V záložce NAT zapněte volbu „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!
- Na VNITŘNÍ síťové kartě NEZAPÍNEJTE volbu „Perform NAT with IP address of this interface on all communication passing through“!!!

DirecPC připojení

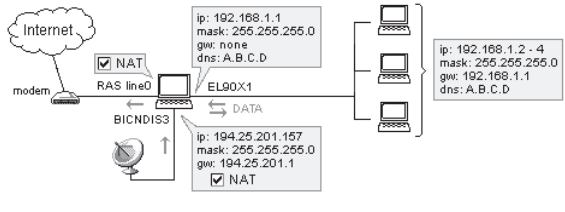
DirecPC je systém, který používá pro data stahovaná z Internetu (download) rychlou satelitní linku a pro data jdoucí do Internetu (upload) běžné připojení (zpravidla vytáčenou linkou). Je jedním z prvních rozšířenějších systémů tohoto druhu a WinRoute pro něj obsahuje speciální podporu, umožňující sdílení připojení technologií NAT stejně, jako např. v případě pevné linky.

Konfigurace WinRoute s DirecPC

Před zahájením instalace (resp. konfigurace) WinRoute je třeba nainstalovat a nastavit všechny komponenty DirecPC systému, tj. adaptér pro satelitní anténu, telefonické připojení (RAS) pro odchozí linku a obsluhující software. DirecPC adaptér WinRoute rozpozná jako speciální rozhraní a umožní pro něj nastavit specifické parametry.

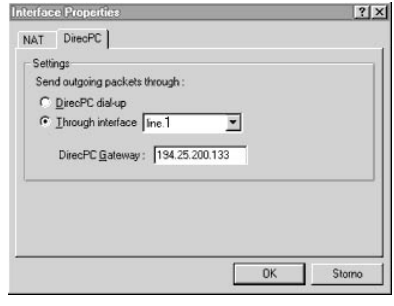
1. Použití RAS linky ve WinRoute

V případě vytáčené linky je možno využít buď DirecPC Dialer (tj. softwarová komponenta DirecPC zajišťující vytáčení odchozí linky) anebo přímo RAS linku ve WinRoute. Použití WinRoute je výhodnější a doporučuje se, protože pak může fungovat vytáčení linky na žádost a zavěšování při nečinnosti, což ušetří náklady na připojení.



V menu zvolte Settings –> Interface Table. Zde se objeví rozhraní typu DirecPC. Vyberte toto rozhraní a stiskněte tlačítko "Properties".

- V záložce „NAT“ zapněte volbu „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!
- V záložce „DirecPC“ zvolte „Through interface:“ a vyberte linku „line1“. Do pole „DirecPC Gateway“ je třeba zadat DirecPC bránu (to je „protější konec“ systému – tedy místo, kde se obě linky opět spojují). Tuto adresu vám sdělí poskytovatel DirecPC.



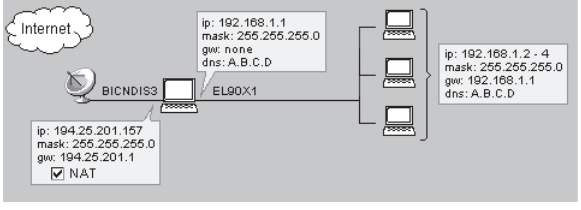
RAS linku ve WinRoute je rovněž nutno správně nastavit.

- V záložce „NAT“ zkontrolujte, zda je zapnuta volba „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!
- V záložce „RAS“ vyberte příslušnou položku telefonického připojení (RAS) a nastavte potřebné parametry (viz kap. Vytáčené připojení).

➢ POZOR: Ve vlastnostech protokolu TCP/IP příslušného telefonického připojení (resp. RAS položky) VYPNĚTE standardní volbu „Použít výchozí bránu na vzdálené síti“ („Use default gateway on remote network“)!!! Jinak budou všechny pakety směrovány přes tuto linku a DirecPC se vůbec nevyužije.

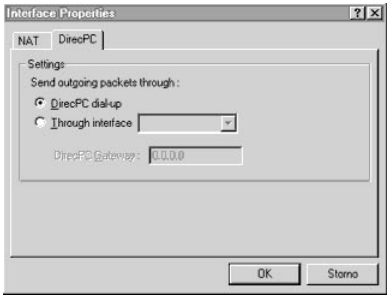
2. Použití DirecPC Dialeru

Pro vytáčení odchozí linky je možno využít DirecPC Dialer, i když se to příliš nedoporučuje (viz výše).



V menu zvolte Settings –> Interface Table. Zde se objeví rozhraní typu DirecPC. Vyberte toto rozhraní a stiskněte tlačítko "Properties".

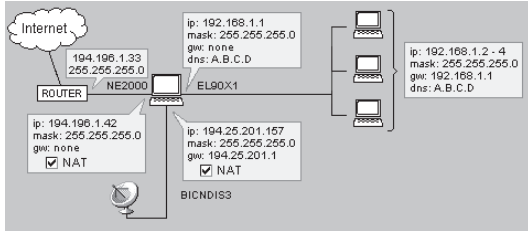
- V záložce „NAT“ zapněte volbu „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!
- V záložce „DirecPC“ zvolte „DirecPC dial-up“.



➢ Poznámka: I v tomto případě je třeba ve WinRoute správně nastavit RAS linku! Jinak nebude WinRoute linku znát a nebude ji moci použít pro odchozí pakety.

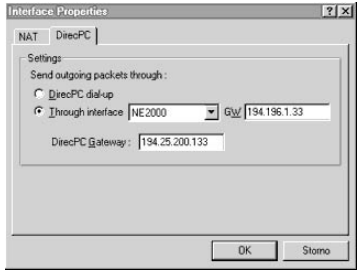
3. Použití síťové karty

Třetí možností je použít pro odchozí spojení pevnou linku. Rozhraním pro odchozí pakety je v tomto případě síťová karta.



V menu zvolte Settings –> Interface Table. Zde se objeví rozhraní typu DirecPC. Vyberte toto rozhraní a stiskněte tlačítko „Properties“.

- V záložce „NAT“ zapněte volbu „Perform NAT with IP address of this interface on all communication passing through“. NEZAPÍNEJTE volbu „Exclude this computer from NAT“!
- V záložce „DirecPC“ zvolte „Through interface:“ a vyberte síťovou kartu pro připojení do Internetu. Do pole „GW:“ zadejte výchozí bránu pro tuto kartu (adresu vám sdělí poskytovatel připojení pevnou linkou) a do pole „DirecPC Gateway“ DirecPC bránu (adresu vám sdělí poskytovatel DirecPC). Zkontrolujte pečlivě zadané hodnoty – pokud např. adresy zaměníte, nebude připojení vůbec fungovat.



➢ POZOR: Na vnější síťové kartě NESMÍ být nastavena žádná výchozí brána (narozdíl od připojení pouze pevnou linkou)! Jinak budou všechny pakety směrovány přes toto rozhraní a DirecPC se vůbec nevyužije.

Jiné satelitní systémy

WinRoute Pro 4.1 obsahuje speciální podporu pouze pro systém DirecPC. S jinými typy satelitních připojení jej lze použít, ale přístup z počítačů v lokální síti do Internetu je možný pouze přes vestavěný proxy server (nikoliv pomocí NAT).

Poskytovatelé těchto satelitních připojení zpravidla mají vlastní proxy server, přes který se musejí klienti připojovat. Proxy server ve WinRoute je možno nastavit tak, aby používal tento proxy server jako svůj nadřazený (tzv. parent proxy server). Následující odstavec stručně popisuje, jak nastavit používání nadřazeného proxy serveru. Detaily naleznete v kap. WinRoute – popis a nastavení / Proxy server.

Nadřazený proxy server (např. satelitní systém DVB)

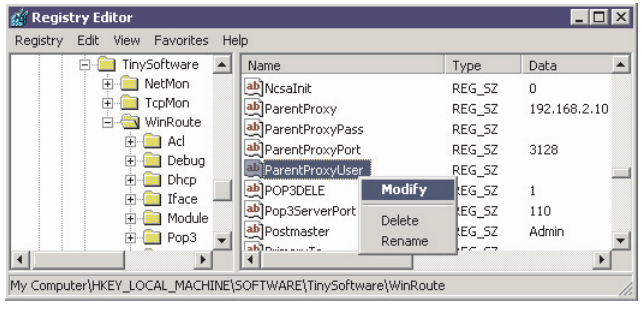
Před instalací WinRoute (resp. s vypnutým WinRoute Engine) ověřte funkčnost vlastního připojení. Ve WinRoute nezapínejte volbu „Perform NAT with the IP address of this interface on all communication passing through“ na ŽÁDNÉM rozhraní! NAT (bez speciální podpory, která funguje u DirecPC) nepropustí příchozí pakety ze satelitního adaptéru, protože jejich cílová IP adresa je jiná než zdrojová adresa v odchozích paketech.

Z menu zvolte Settings –> Proxy Server a vyberte záložku „Advanced“. Zde zadejte IP adresu a port nadřazeného proxy serveru (tyto informace získáte od poskytovatele satelitního připojení). Proxy server ve WinRoute tak nebude komunikovat přímo s cílovými servery, ale bude pouze předávat požadavky nadřazenému proxy serveru.

Ověřování uživatele nadřazeným proxy serverem

Vyžaduje-li nadřazený proxy server ověření uživatele jménem a heslem, postupujte následovně:

- Ověřte si, zda máte WinRoute Pro 4.1 Build 21 nebo novější (lze zjistit v menu Help –> About application...). Pokud ne, upgradujte na novější verzi (podrobnosti viz kap. Instalace). Starší verze ověření na nadřazeném proxy serveru nepodporují.
- Zastavte WinRoute Engine a spusťte Editor registru (regedit.exe). Přepněte se do větve „HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute“. V pravé polovině okna Editoru registru vyhledejte položky „ParentProxyUser“ a „ParentProxyPass“ a do nich zadejte správné jméno a heslo.



- Ukončete Editor registru a spusťte WinRoute Engine.

➢ Poznámka: Vyžaduje-li nadřazený proxy server ověření uživatele, lze to provést POUZE tímto způsobem. NENÍ MOŽNÉ provést autorizaci z koncového klienta (WWW prohlížeče). Tam se sice objeví okno pro zadání uživatelského jména a hesla, ale proxy server ve WinRoute nemůže tyto údaje na nadřazený server přenést.

Připojení PPPoE

Připojení PPPoE (Point-to-Point Protocol over Ethernet) používá lokální síť Ethernet a protokol PPP pro přístup k vysokorychlostním sítím širokopásmovým modemem (kabelovým nebo xDSL). Na počítači, který má být takto připojen, je třeba nainstalovat speciální software, který vytvoří v systému virtuální rozhraní (síťový adaptér nebo RAS připojení). Tento adaptér se pak použije pro připojení do Internetu pomocí PPPoE.

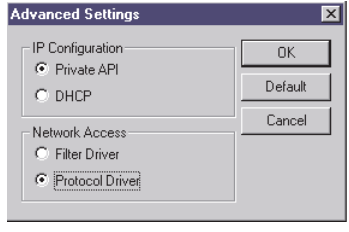
Příklady nastavení

V následujícím textu jsou popsána nastavení pro dva rozšířenější PPPoE klienty – EnterNet 300 a WinPoET.

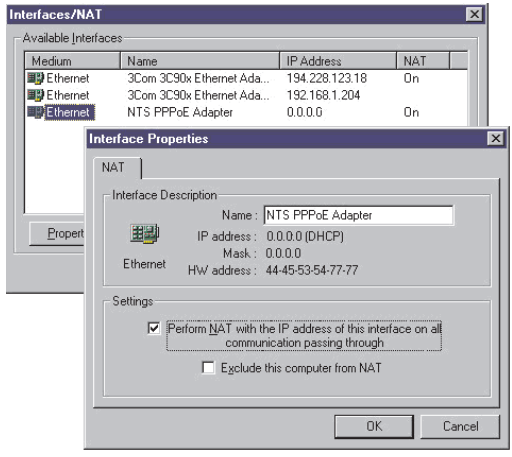
EnterNet 300

Po instalaci a restartu počítače EnterNet 300 spusťte, zvolte menu Connections –> Settings a stiskněte tlačítko „Advanced“. V dialogu „Advanced Settings“ vyberte volbu „Protocol Driver“. (Výběr mezi „Private API“ a „DHCP“ závisí na tom, jakým způsobem je PPPoE rozhraní přidělována IP adresa. Tuto informaci vám sdělí poskytovatel PPPoE připojení).

➢ POZOR: NENASTAVUJTE volbu „Filter Driver“. Tento ovladač s WinRoute nefunguje.



Ve WinRoute nejsou třeba žádná speciální nastavení. Zvolte menu Settings –> Interface Table, vyberte "NTS PPPoE Adapter" a zapněte na tomto rozhraní volbu "Perform NAT with the IP address of this interface on all communication passing through".

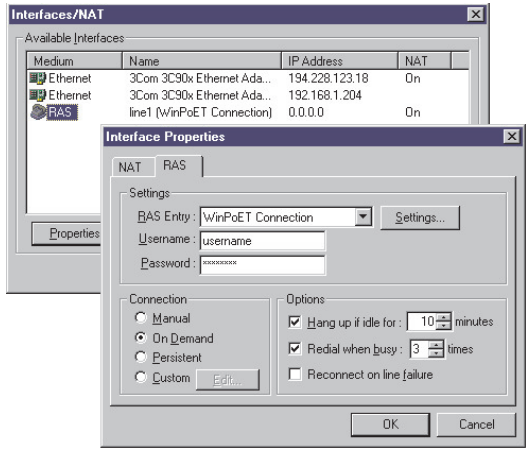


Ve vlastnostech protokolu TCP/IP pro tento adaptér zpravidla stačí ponechat výchozí volbu „Získávat IP adresu automaticky“. Detaily vám sdělí poskytovatel PPPoE připojení.

WinPoET

Po úspěšné instalaci se v systému objeví virtuální položka telefonického připojení (nazvaná „WinPoET Connection“). Ve WinRoute zvolte Settings –> Interface Table, vyberte RAS linku (např. „line1“) a přiřaďte této lince položku „WinPoET Connection“. Zadejte uživatelské jméno a heslo pro PPPoE připojení.

Po stisku tlačítka „Settings“ lze nastavit další volby, např. IP adresu PPPoE serveru, k němuž se připojujete.



Kapitola 5

WINROUTE – POPIS A NASTAVENÍ

Tabulka rozhraní (Interface Table)

Tabulku rozhraní otevřete volbou Settings –> Interface Table nebo stiskem ikony síťového adaptéru na nástrojové liště.

Tabulka rozhraní zobrazuje všechna rozhraní (např. Ethernet, TokenRing, DirecPC atd.), která má WinRoute k dispozici. Rozhraní zde nelze přidávat ani odebírat, WinRoute pouze načte rozhraní instalovaná ve Windows. Máte-li instalovaný nějaký adaptér, který WinRoute nezobrazí, znamená to, že adaptér je buď v systému zakázaný, nepracuje správně anebo nemá instalován správný ovladač.

V základním okně „Interface Table“ jsou pro každé rozhraní zobrazeny následující informace:

Medium

Typ rozhraní. Může být např. Ethernet, TokenRing, DirecPC, RAS atd.

Name

Pojmenování rozhraní. Zde se zobrazí identifikační řetězec adaptéru (např. „3Com 3C509 Ethernet Adapter“), případně ovladače (např. „NDIS 50 driver“). Ve WinRoute je možné tuto identifikaci nahradit libovolným jiným (srozumitelnějším) jménem.

IP Address

IP adresa přiřazená danému rozhraní. V případě, že je rozhraní neaktivní (např. zavěšená RAS linka či fyzicky nepřítomná síťová karta), zobrazuje se zde adresa „0.0.0.0“.

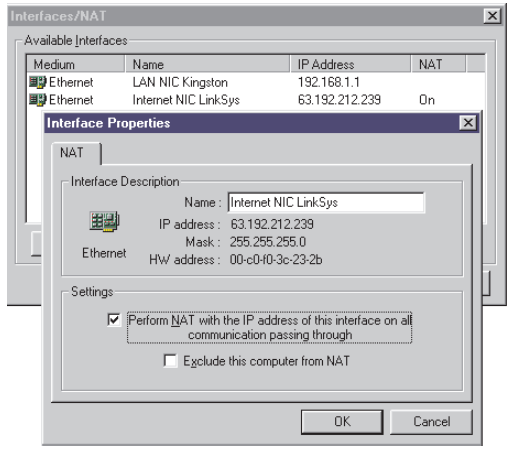
NAT

Zobrazuje, zda je na daném rozhraní zapnuta volba „Perform NAT with the IP address of this interface on all communication passing through“. „On“ znamená, že je volba zapnutá. „On!“ znamená, že je zároveň zapnuta volba „Exclude this computer from NAT“. Je-li NAT vypnut, nezobrazuje se zde nic.

Nastavení rozhraní (Properties)

Stiskem tlačítka „Properties“ je možné nastavovat vlastnosti vybraného rozhraní.

Záložka „NAT“



V záložce „NAT“ je nejdůležitější volba „Perform NAT with the IP address of this interface on all communication passing through“. Ta zapíná tzv. překlad IP adres (Network Address Translation), tzn., že ve všech IP paketech odcházejících z tohoto rozhraní je zdrojová IP adresa nahrazena IP adresou tohoto rozhraní. Z toho vyplývá, že tuto volbu lze zapnout jen na rozhraní vedoucím do Internetu (síťové kartě či RAS lince), aby byly „překládány“ privátní adresy lokální sítě na veřejnou adresu internetového rozhraní.

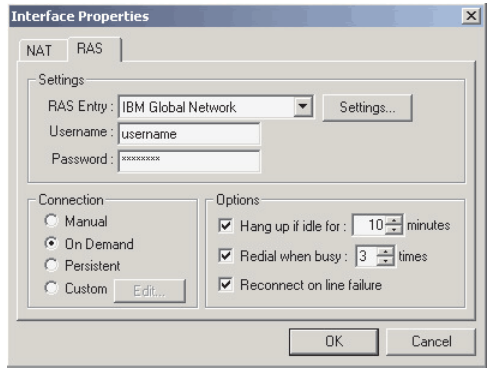
➢ Poznámka: Překlad adres opačným směrem nemá žádný smysl a způsobí nefunkčnost WinRoute (nebude možno směrovat mezi lokální sítí a Internetem). Proto dobře zkontrolujte, zda zapínáte NAT na správném rozhraní!

Druhou funkcí volby „Perform NAT with the IP address of this interface on all communication passing through“ je aktivace firewallu. Ten způsobí „uzavření“ všech TCP a UDP portů pro požadavky přicházející na toto rozhraní. Počítač s WinRoute je tak dokonale chráněn proti přístupu zvenčí.

Volba „Exclude this computer from NAT“ vypíná firewallovou ochranu popsanou v předchozím odstavci (překlad adres zůstává funkční). Neuvážené použití této volby může být velmi nebezpečné – počítač s WinRoute pak není nijak chráněn proti napadení. NEZAPÍNEJTE tuto volbu, pokud k tomu nemáte opravdu dobrý důvod (takovým důvodem může být např. krátkodobé umožnění připojení programem WinRoute Administration pracovníkovi technické podpory během vaší konzultace).

Záložka „RAS“

V této záložce lze vybrané lince (např. „line1“) přiřadit položku RAS (Telefonického připojení) a nastavit parametry vytáčení.



Pole „RAS Entry“ umožňuje vybrat některou z nadefinovaných položek. Tlačítkem „Settings“ lze upravovat parametry této položky (stejně jako v Ovládacích panelech). Není-li dosud žádná položka ve Windows vytvořena, pak toto tlačítko spustí průvodce vytvořením nového připojení.

V sekci „Connection“ lze zvolit způsob vytáčení: ručně (Manual), na žádost (On Demand – má význam pouze pro „line1“), trvalé připojení (Persistent) nebo vlastní nastavení (Custom). V případě poslední volby lze pak tlačítkem „Edit“ nastavit, kdy má fungovat vytáčení na žádost (Dial on demand), kdy má být trvale vytočeno (Keep the line connected) a kdy má linka zůstat trvale zavěšena (Keep the line disconnected). Každá z těchto voleb může být buď vypnuta (never) nebo nastaven časový interval její platnosti. Podrobnosti o nastavení časových intervalů naleznete v kap. Pomocné nástroje / Časové intervaly.

Sekce „Options“ pak umožňuje nastavení dalších parametrů: „Hang up if idle for“ znamená dobu (v minutách), po které dojde k automatickému zavěšení linky, jestliže po ní neprocházejí žádná data. „Redial when busy“ znamená opakování vytáčení, jestliže je linka momentálně obsazena. Lze nastavit maximální počet pokusů o vytočení. Volba „Reconnect on line failure“ znamená automatické obnovení spojení (znovuvytočení) po jeho výpadku.

Přidání a odebrání rozhraní (Interface Maintenance)

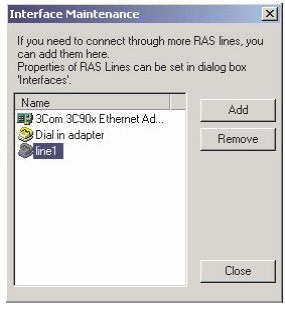
Po instalaci WinRoute se v Interface Table objeví všechny detekované síťové adaptéry a linka „line1“ (které je pak možno přiřadit RAS položku). Mohou ale nastat následující situace:

- Potřebujete více RAS linek (např. jednu pro připojení do Internetu a druhou do jiné privátní sítě, např. pomocí VPN).
- Došlo k výměně síťové karty, která sice byla správně detekována, ale v Interface Table kromě ní zůstala i původní, nyní již neaktivní karta.

Tyto situace lze ošetřit volbou Settings –> Advanced –> Interface Maintenance.

Zde můžete:

- Tlačítkem „Add“ přidat další RAS linku
- Tlačítkem „Remove“ odstranit RAS linku, případně neaktivní síťový adaptér. WinRoute nepovolí smazat aktivní adaptér nebo vytočenou linku.



Vytáčení na žádost

Vytáčení na žádost (Dial on demand) znamená vytočení připojení, jestliže je přijat paket s cílovou IP adresou, která nepatří do subsítě žádného z lokálních rozhraní. Vytočením připojení vznikne v systémové směrovací tabulce výchozí cesta (default route), na kterou jsou pak všechny takové pakety směrovány. Přestanou-li být data přenášena a je-li nastavena volba „Hang up if idle for“, dojde po definované době k zavěšení linky a s dalším odchozím paketem se může proces opakovat.

Aby mohlo vytáčení na žádost výše popsaným způsobem fungovat, musí být splněno několik základních podmínek:

- Na žádost může být vytáčena pouze jedna linka. Ve WinRoute je pro tento účel vyhrazena linka „line1“. Ostatní linky mohou být vytáčeny pouze ručně.
- Vytáčení na žádost funguje na základě neexistence výchozí cesty (výchozí cesta vznikne definicí výchozí brány na některém rozhraní). Není tedy např. možné vytáčet na žádost linku do jiné privátní sítě, jestliže existuje pevné připojení do Internetu síťovou kartou.

➢ Poznámka: Jednou z nejčastějších příčin nefunkčnosti vytáčení na žádost je (nechtěné) nastavení výchozí brány na některém z vnitřních síťových rozhraní.

- Vytáčení na žádost zajišťuje nízkoúrovňový ovladač WinRoute, jestliže na některém z vnitřních rozhraní zachytí paket výše popsaných vlastností. Pokud však vysílající aplikace běží na tomtéž počítači jako WinRoute, systém vyhodnotí nedostupnost cílové sítě a paket se k ovladači WinRoute vůbec nedostane. Z toho vyplývá, že vytáčení na žádost nefunguje z počítače s WinRoute.

Vytáčení na žádost z počítače s WinRoute

Výše popsaný nedostatek lze částečně odstranit následujícím způsobem:

- Zkontrolujte, zda je zapnut a správně nastaven DNS Forwarder.
- Na vnitřní síťové kartě (respektive na některé z vnitřních karet) nastavte adresu DNS serveru na tutéž adresu, jakou má přiřazenu přímo tato karta.

Tímto nastavením zajistíte, že i DNS dotazy z tohoto počítače budou předávány DNS Forwarderu. Ten dokáže zajistit vytočení linky, aby mohl kontaktovat příslušný DNS server (na nějž dotazy přeposílá). Bude-li tedy cílový server zadán DNS jménem, bude vytáčení na žádost fungovat i z tohoto počítače.

Dial in adapter

Dial in adapter je speciální interní RAS linka vyhrazená pro připojení vnějším klientem na RAS server. Tento adaptér se nezobrazuje v Interface table a nelze na něm zapnout funkci NAT (nemělo by to žádný smysl).

Dial in adapter se objevuje jako standardní rozhraní ve směrovací tabulce, to znamená, že klient připojený zvenčí se stává dalším segmentem privátní lokální sítě a je rovněž chráněn firewallem vůči zbytku Internetu.

➢ POZOR: Používáte-li RAS server společně s WinRoute, je třeba jej nastavit tak, aby klientům přiděloval IP adresy z jiné subsítě než je lokální síť! Jinak by totiž nefungovalo IP směrování mezi jednotlivými rozhraními správně.

Dial in adapter se rovněž zobrazuje jako rozhraní v paketovém filtru. Z toho vyplývá, že na připojeného vzdáleného klienta lze aplikovat samostatná filtrační pravidla.

Uživatelé a skupiny

Uživatelský účet

Uživatelský účet ve WinRoute má tyto základní funkce:

- představuje uživatelskou POP3 e-mailovou schránku
- umožňuje přihlášení k administraci WinRoute (pokud to nastavená přístupová práva povolují)
- jméno a heslo lze použít pro ověření přístupu k SMTP serveru, proxy serveru a WWW administračnímu rozhraní (je-li ověření vyžadováno).

Po instalaci WinRoute je zde vytvořen základní uživatel Admin. Doporučuje se neodstraňovat tento účet a přiřadit mu nějaké „nezapomenutelné“ heslo. Zapomenete-li toto heslo nebo uživatele Admin nechtěně smažete (a neexistuje jiný uživatel s administrátorskými právy), postupujte podle pokynů v kap. Program WinRoute Administration / Ztráta administrátorského hesla.

Uživatelé mohou být vytvořeni lokálně nebo importováni z NT domény. Nezávisle na tom lze nastavit u každého uživatele buď pevné heslo nebo ověřování v NT doméně. Uživateli Admin (resp. hlavnímu administrátorovi WinRoute) se doporučuje nastavit heslo ve WinRoute (lokální ověřování), aby se mohl přihlásit i v případě výpadku doménového serveru.

Vytvoření, editace a smazání uživatelského účtu

V hlavním menu zvolte Settings –> Accounts a vyberte záložku „Users“.

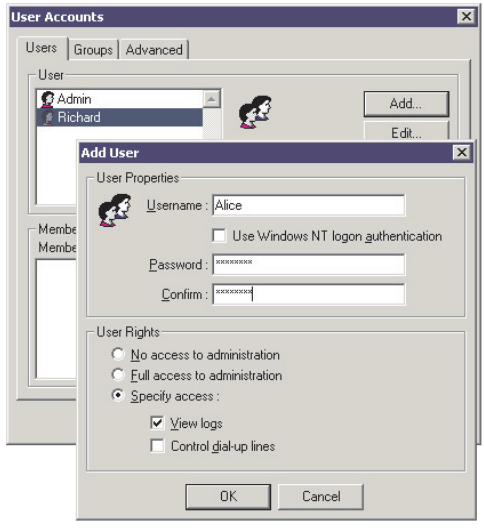
Vytvoření nového účtu

Stiskněte tlačítko „Add“. Nyní zadejte nové uživatelské jméno a zvolte ověřování v NT doméně („Use Windows NT logon authentication“) nebo ručně zadejte heslo. Heslo je nutno zadat dvakrát.

V sekci „User Rights“ nastavte uživateli požadovaná přístupová práva. Možnosti jsou následující:

- „No access to administration“ – uživatel nemá žádná přístupová práva, nemůže se vůbec přihlásit do programu WinRoute Administration.
- „Full access to administration“ – uživatel získá plná administrátorská práva, může i odstranit původního uživatele „Admin“.
- „Specify access“ – omezený přístup k administraci: „View logs“ umožňuje pouze prohlížet logy a „Control dial-up lines“ vytáčet a zavěšovat RAS linky.

➢ Poznámka: Zvolíte-li „Specify access“, a nezaškrtnete ani „View logs“ ani „Control dial-up lines“, je tato volba ekvivalentní volbě „No access to administration“.



Změna nastavení účtu

Změnu vlastností uživatelského účtu (hesla, ověřování, přístupových práv) provedete jednoduše výběrem účtu a stiskem tlačítka „Edit“. Dialog je shodný s dialogem pro vytvoření nového účtu.

Smazání účtu

Smazání účtu provedete výběrem účtu a stiskem tlačítka „Delete“.

➢ POZOR: Mažete-li uživatele „Admin“, ujistěte se, že ještě alespoň jeden další uživatel má nastavena práva „Full access to administration“. Jinak se již nebudete moci do administračního programu přihlásit!

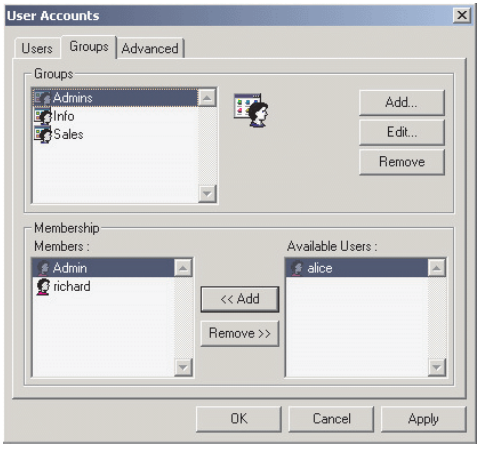
Skupiny uživatelů

Uživatele ve WinRoute lze sdružovat do skupin. Každý uživatel přitom může být členem několika skupin současně. Skupinu lze použít podobně jako uživatele, např.:

- skupině (tj. všem jejím členům) může být doručován e-mail, jestliže ji použijete v Aliases nebo Sorting Rules (viz kap. Mail server)
- skupině může být povolen či zakázán přístup na určité WWW stránky v proxy serveru (viz kap. Proxy server)

Skupiny lze vytvářet, upravovat a rušit podobně jako uživatele v menu Settings –> Accounts, záložka Users. Skupině lze nastavit globální přístupová práva (možnosti jsou stejné jako u jednotlivých uživatelů).

➢ POZOR: Skupinová práva se přidávají k právům uživatelů. Práva lze pouze rozšířit (tj. uživatel může zařazením do skupiny získat vyšší práva, ale nemohou mu být členstvím ve skupině omezena jeho vlastní práva).



Zařazení uživatelů do skupin

Zařadit uživatele do skupin můžete dvěma způsoby:

- V záložce „Groups“ v poli „Groups“ vyberte skupinu, do níž chcete uživatele zařadit. V poli „Available Users“ vyberte uživatele, kterého chcete do skupiny přidat (přidržením klávesy Ctrl lze vybrat více uživatelů najednou). Tlačítkem „<< Add“ zařadíte uživatele do vybrané skupiny. Uživatel se přesune do pole „Members“.
- V záložce „Users“ v poli „User“ vyberte uživatele, kterého chcete zařadit do skupiny. V poli „Available Groups“ vyberte skupinu (případně více skupin pomocí klávesy Ctrl). Tlačítkem „<< Add“ přesuňte vybranou skupinu do pole „Member of“. Uživatel se tak stane jejím členem.

Vyjmutí uživatele ze skupiny

Vyjmout uživatele ze skupiny lze opět dvěma způsoby (analogicky k přidání). Použijte tlačítko „Remove >>“.

Ověřování v NT doméně a import uživatelů

Chcete-li ověřovat uživatele v NT doméně (volba „Use Windows NT logon authentication"), je třeba specifikovat jméno této domény. Zvolte menu Settings –> Accounts, záložku „Advanced" a do pole „Authentication domain" zadejte jméno vaší domény. Tlačítkem „Import Users" (případně tlačítkem „Import" v záložce „Users") lze do WinRoute importovat uživatele z této domény.

Nespecifikujete-li doménu, WinRoute nabídne import lokálních uživatelů z Windows NT. Ve Windows 95/98/ME nejsou tlačítka „Import Users" a „Import" aktivní.

Import uživatelů pouze vytvoří účty stejných jmen jako v příslušné doméně. Doménová práva uživatelů se do WinRoute nijak nepromítnou. Z toho vyplývá:

- Importovaným uživatelům je třeba ručně nastavit přístupová práva (implicitní práva jsou „No access to administration").
- Všichni tito uživatelé mají nastavenu volbu „Use Windows NT logon authentication", tu lze však u jednotlivých uživatelů vypnout a nastavit jim heslo ručně (existuje-li pro to nějaký důvod).

Nástroje

Skupiny IP adres

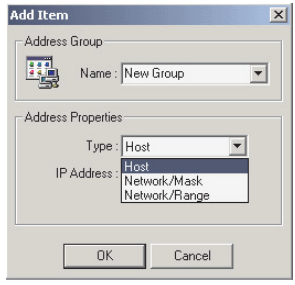
Skupiny IP adres lze ve WinRoute použít při omezování přístupu k určitým službám (např. u mapovaných portů, vzdálené administrace, antispamové ochrany apod.). Každá skupina přitom může obsahovat libovolný počet jednotlivých IP adres, rozsahů adres nebo celých subsítí definovaných adresou a maskou.

Vytvoření, editace a odstranění skupiny IP adres

Zvolte menu Settings –> Advanced –> Address Groups. Tlačítkem „Add" je možno:

- vytvořit novou skupinu IP adres. Do pole „Name" zadejte jméno nové skupiny. V sekci „Address Properties" definujte první položku nové skupiny – adresu jednoho počítače („Host"), subsíť („Network/Mask") nebo rozsah IP adres („Network/Range").
- přidat novou položku do existující adresní skupiny. V poli „Name" vyberte existující skupinu a definujte novou položku (viz výše). Tato

položka bude přidána do vybrané skupiny. Takto můžete do jedné skupiny přidat libovolný počet položek kteréhokoliv typu.



Tlačítkem "Edit" je možné buď změnit jednu položku skupiny nebo změnit název skupiny (podle toho, co v dialogu Network Address Groups vyberete). Tlačítkem "Remove" lze smazat vybranou položku ze skupiny, případně celou skupinu.

Časové intervaly

Časové intervaly lze ve WinRoute použít pro omezení platnosti určitých pravidel či akcí na část dne a/nebo vybrané dny v týdnu. Každý pojmenovaný časový interval se může sestávat z libovolného počtu podintervalů. Podinterval je určitý kontinuální úsek denního času (např. od 11 do 12 hodin) platný buď po celý týden, nebo jen ve vybrané dny.

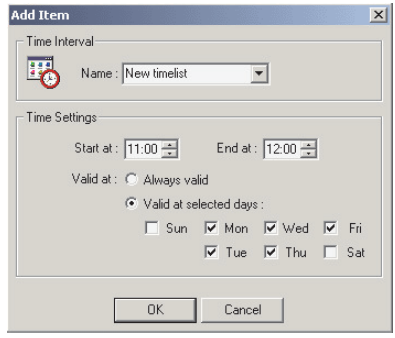
Časové intervaly můžete použít např.:

- při definici paketových filtrů
- při plánování příjmu a odesílání pošty
- v nastavení vytáčení na žádost

Vytvoření, editace a odstranění časového intervalu

Zvolte menu Settings –> Advanced –> Time Intervals. Tlačítkem „Add“ je možno:

- vytvořit nový časový interval. Do pole „Name“ zadejte jméno nového intervalu. V sekci „Time Settings“ definujte první podinterval: v polích „Start at:“ a „End at:“ nastavte počáteční a koncový čas podintervalu a zvolte, zda má platit po celý týden („Always valid“) nebo pouze ve vybrané dny („Valid at selected days“).
- přidat do existujícího časového intervalu nový podinterval. V poli „Name“ vyberte jméno intervalu a v sekci „Time Settings“ nastavte nový podinterval (viz výše).



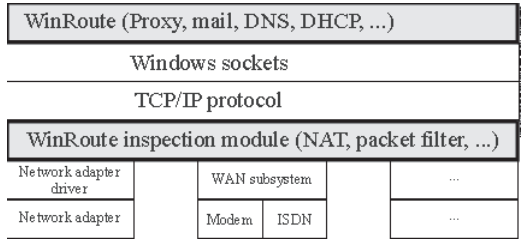
Tlačítkem „Edit“ lze změnit nastavení vybraného podintervalu, případně přejmenovat vybraný interval (podle toho, co v dialogu Time Intervals vyberete). Tlačítkem "Remove" můžete odstranit vybraný podinterval nebo smazat celý interval.

➢ Poznámka: Nelze vytvořit časový interval zasahující do dvou dnů současně. Chcete-li vytvořit např. interval od 18:00 do 6:00, je třeba jej složit ze dvou podintervalů: 18:00–23:59 a 0:00–6:00.

NAT směrovač

Architektura WinRoute

Tato kapitola vám poskytne základní informace o tom, jak WinRoute funguje a jak je začleněn do systému Windows.



1. Bezpečnost

WinRoute (resp. jeho nízkoúrovňový ovladač) je umístěn přímo nad ovladači síťových rozhraní. To umožňuje zachytit, analyzovat a případně odfiltrovat jakýkoliv paket dříve, než je zpracován dalšími subsystémy. Díky tomu je zabezpečení vaší lokální sítě i počítače s WinRoute prakticky 100%.

➢ Poznámka: WinRoute pracuje pouze s protokoly sady TCP/IP. Pakety ostatních protokolů (např. IPX/SPX, NetBEUI atd.) transparentně propouští.

2. Podpora aplikačních protokolů

WinRoute je softwarový směrovač. Narozdíl od klasických proxy serverů může být na klientském počítači (tj. počítači v privátní síti, která je přes WinRoute připojena k Internetu) provozována téměř libovolná aplikace. Klientský počítač přitom stačí nastavit tak, jako by byl připojen přes směrovač přímo do Internetu (tj. nastavit adresu výchozí brány a DNS serveru) – žádná další nastavení systému ani aplikace nejsou třeba!

3. Flexibilita

WinRoute podporuje libovolný počet síťových rozhraní. Funkci NAT (překlad IP adres) je přitom možno zapnout na kterémkoliv z nich – nezáleží tedy na typu internetového připojení (viz kap. Připojení vaší sítě k Internetu). Funkce NAT může být také vypnuta na všech rozhraních, pak se WinRoute chová jako softwarový směrovač a je možno jej použít např. pro oddělení dvou segmentů lokální sítě. Na každém rozhraní můžete navíc definovat svá vlastní bezpečnostní pravidla. WinRoute vám tak dává velmi široké možnosti při konfiguraci a zabezpečení vaší sítě.

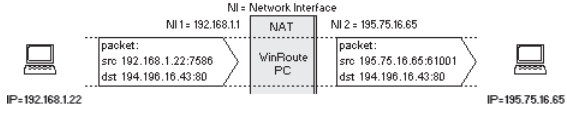
Jak funguje NAT

Překlad IP adres (Network Address Translation, zkr. NAT) znamená modifikaci IP adres v paketech jdoucích z a do chráněné privátní sítě.

Odchozí pakety

V paketech jdoucích z chráněné sítě do Internetu je původní (privátní) zdrojová IP adresa nahrazována (veřejnou) IP adresou vnějšího rozhraní počítače s WinRoute. V Internetu tedy všechny pakety vypadají tak, jako by byly vysílány přímo z tohoto počítače. Skutečná topologie vaší lokální sítě zůstane navenek zcela skryta.

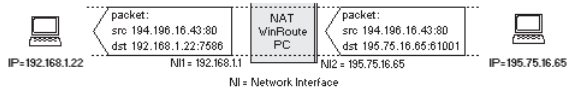
O každém takovém paketu je zároveň vytvořen záznam v tzv. NAT tabulce.



Příchozí pakety

Každý paket přijatý z Internetu je porovnán se záznamy v NAT tabulce. Je-li nalezen odpovídající záznam, provede se změna cílové IP adresy v tomto paketu na (privátní) adresu příslušného počítače v lokální síti a paket je

na tento počítač poslán. Tím je zajištěno, že odpověď na vyslaný paket je správně doručena vysílajícímu počítači.



Je zřejmé, že přesměrování paketu na počítač v lokální síti je možné pouze tehdy, jestliže existuje příslušný záznam v NAT tabulce. Komunikaci tedy musí vždy zahájit počítač (klient) v lokální síti, aby se na základě odchozího paketu tento záznam vytvořil. Z toho vyplývá, že NELZE navázat spojení z Internetu na počítač uvnitř lokální sítě.

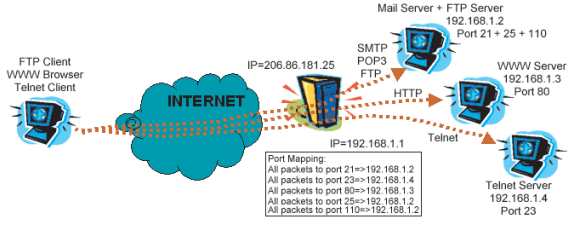
NAT tedy z principu chrání počítače ve vaší síti proti přístupu zvenčí.

Mapování portů

WinRoute provádí NAT, což znemožňuje přístup z Internetu do chráněné lokální sítě. Mapování portů (Port Mapping) umožňuje zpřístupnění vybraných aplikací (běžících na definovaných portech) do Internetu pod vnější IP adresou počítače s WinRoute. Nezáleží na tom, zda daná aplikace běží přímo na tomto počítači nebo na libovolném počítači uvnitř lokální sítě.

Jak funguje mapování portů

Je-li ve WinRoute definováno mapování alespoň jednoho portu, je každý paket přijatý z Internetu (resp. jeho protokol, cílová IP adresa a cílový port) porovnán se záznamy v tabulce mapovaných. Pokud je odpovídající záznam nalezen, je paket přeposlán na odpovídající cílovou adresu. V opačném případě je paket buď zpracován na počítači s WinRoute, nebo zahozen (v závislosti na nastavení WinRoute).



Příklad: V lokální síti běží na počítači s IP adresou 192.168.1.3 WWW server, který chcete zpřístupnit do Internetu. Ve WinRoute nastavíte mapování portu 80 (standardní port pro službu WWW) na cílovou adresu 192.168.1.3. Váš poskytovatel Internetu nastaví v DNS záznam pro jméno „www.vasedomena.cz“ na vnější IP adresu počítače s WinRoute (např. 206.86.181.25). Klienti z Internetu budou zdánlivě komunikovat s WWW

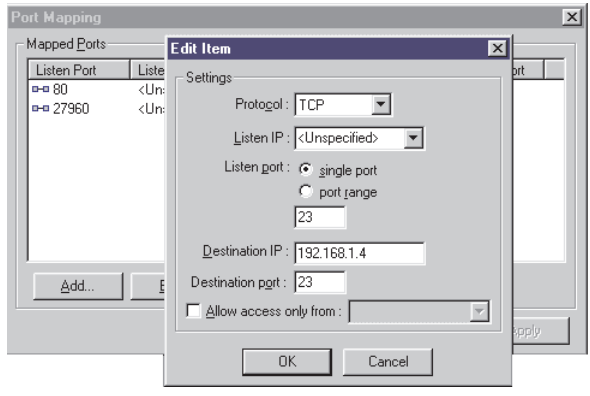
serverem běžícím na této adrese, ve skutečnosti bude ale všechna komunikace na portu 80 přesměrována na počítač s WWW serverem uvnitř vaší lokální sítě.

➢ Poznámka: Mapování portů funguje pouze při přístupu zvenčí (přesněji řečeno přes rozhraní, na němž se provádí NAT). V rámci vnitřní sítě jsou ale všechny služby přístupné na svých skutečných (privátních) IP adresách. V lokální DNS je tedy třeba jménu „www.vasedomena.cz“ přiřadit privátní adresu 192.168.1.3.

Nastavení mapování portů

Příklad: Vytvoření mapovaného portu pro Telnet server běžící na adrese 192.168.1.4. Telnet používá protokol TCP, port 23.

V hlavním menu zvolte Settings –> Advanced –> Port Mapping. Tlačítkem „Add“ přidejte nové mapování:



Protocol

Zvolte komunikační protokol, která daná aplikace používá (TCP nebo UDP). V případě, že aplikace používá na daném portu oba protokoly, je možno zvolit „TCP/UDP“ a namapovat tak port pro oba protokoly současně.

Listen IP

Má význam IP adresy, na kterou bude aplikace „přemapována“ (tedy vnější adresy počítače s WinRoute). Je-li vnějšímu rozhraní přiřazena pouze jedna IP adresa (nejčastější případ), stačí zde ponechat implicitní volbu „<Unspecified>“ – adresa bude rozpoznána automaticky. Máte-li však na vnějším rozhraní přiřazeno více IP adres (možno pouze ve Windows NT/2000), JE NUTNÉ zde uvést adresu, na kterou bude aplikace mapována. Tak je např. možné přes jedno internetové připojení zpřístupnit několik WWW serverů na různých adresách, všechny na portu 80 (viz příklad na konci této kapitoly).

Listen Port

Port, na němž bude aplikace zvenčí přístupná. Typicky je shodný s portem, na kterém aplikace skutečně běží (protože je to standardní port – např. 80 pro WWW), ale obecně lze „přemapovat" libovolný port na libovolný jiný. Na jeden port počítače s WinRoute (resp. na jednu dvojici Listen IP – Listen Port) lze ale vždy namapovat POUZE JEDNU aplikaci!

Listen Port může být buď jeden port („single port") nebo spojitý rozsah („port range"). Používá-li aplikace více portů, které netvoří jeden spojitý rozsah, je potřeba provést více samostatných mapování.

Destination IP

IP adresa počítače v lokální síti, kde aplikace skutečně běží.

➢ Poznámka: Uvede-li se v poli „Destination IP" adresu jednoho z rozhraní počítače s WinRoute (nezáleží na tom, kterého), znamená to zpřístupnění aplikace běžící přímo na tomto počítači (tzv. otevření portu).

Destination Port

Port (případně rozsah portů), který aplikace používá.

Allow acces only from

Tato volba umožňuje povolit přístup k mapovanému portu jen z určitých IP adres. Je zde možno vybrat jednu z předdefinovaných skupin IP adres. Detaily naleznete v kapitole WinRoute – Popis a nastavení / Nástroje / Skupiny IP adres.

Příklad: Zpřístupnění 5 WWW serverů

V tomto příkladu chceme zpřístupnit do Internetu 5 WWW serverů na různých veřejných IP adresách. Všechny tyto adresy jsou přiřazeny vnějšímu rozhraní počítače s WinRoute a jsou na ně nastavena příslušná DNS jména.

Ve WinRoute definujeme následujících 5 mapování portů:

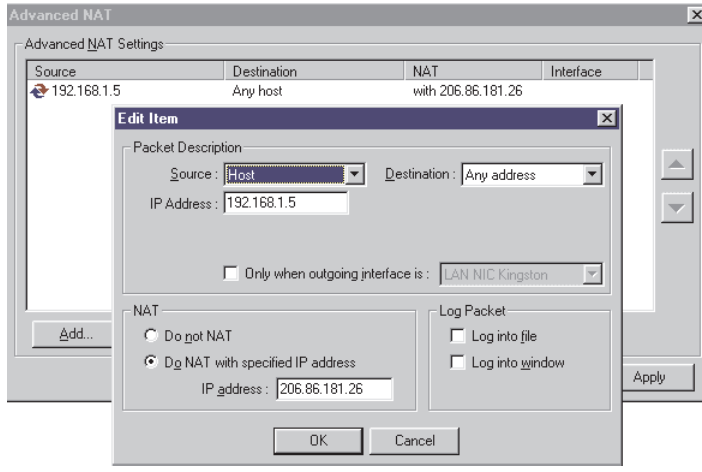
- Protocol: TCP
- Listen IP: jedna z IP adres vnějšího rozhraní, příslušná pro daný WWW server
- Listen Port: 80 (standardní port pro službu WWW)
- Destination IP: IP adresa WWW serveru v lokální síti
- Destination Port: 80

➢ Poznámka: Příklady mapování portů pro mnoho dalších aplikací naleznete v kap. Speciální nastavení a příklady.

Detailní nastavení NAT (Advanced NAT)

WinRoute umožňuje detailně nastavit, jak má být prováděn překlad privátních IP adres na veřejné. Lze např. nastavit, na kterou z vnějších adres mají být určité vnitřní adresy překládány, nebo přes WinRoute připojit privátní a veřejný segment současně (tzv. demilitarizovaná zóna).

Parametry NAT lze nastavit v menu Settings –> Advanced –> NAT:



Source, Destination

Definuje zdrojovou a cílovou adresu paketu, na který se má pravidlo vztahovat. Obojí může být definováno jako libovolná IP adresa (Any address), jedna IP adresa (Host), rozsah adres (Network/Range), subsíť zadaná adresou a maskou (Network/Mask) nebo předdefinovaná skupina IP adres (Address Group).

Pravidlo vždy popisuje paket jdoucí z lokální sítě do Internetu (na jehož základě se vytváří záznam v NAT tabulce). „Source“ je tedy adresa v lokální síti, zatímco „Destination“ adresa v Internetu. V případě volby „Do not NAT“ se automaticky povoluje průchod paketů opačným směrem (pro směr z Internetu tedy již NENÍ třeba přidávat další pravidlo).

Only when outgoing interface is

Tato volba určuje, že má pravidlo platit jen v případě, že je paket odesílán přes specifikované rozhraní. To má samozřejmě význam pouze v případě, jestliže je v systému více rozhraní se zapnutým NAT – např. DirecPC připojení.

Do not NAT

Neprovádět překlad adres. Tato volba se použije, jestliže je za WinRoute segment s veřejnými IP adresami (demilitarizovaná zóna). Pakety jsou pak směrovány beze změny.

Do NAT with specified IP address

Jestliže paket vyhovuje kritériím v sekci „Packet Description“, provede se překlad adres (NAT). Zdrojová adresa v paketu se ale (namísto primární IP adresy vnějšího rozhraní) nahradí adresou specifikovanou v poli „IP address“.

Log into file, Log into window

Zaznamenat paket do souboru „security.log“, případně do okna Security Log.

Příklad:

Chceme nastavit, aby se v komunikaci z počítače s IP adresou 192.168.1.5 používala speciální vnější adresa. Nastavíme:

- Source: „Host“, IP address: „192.168.1.5“
- Destination: „Any Address“ (tzn. libovolná adresa v Internetu; komunikaci v lokální síti WinRoute samozřejmě neovlivní)
- Only when outgoing interface is: není třeba zapínat (nebo je zde možno vybrat vnější rozhraní)
- Do NAT with specified IP address, do pole „IP address“ zadáme příslušnou vnější IP adresu.

➢ Poznámka: Další příklady nastavení (např. vytvoření demilitarizované zóny) naleznete v kap. Speciální nastavení a příklady.

Firewall

Základní informace

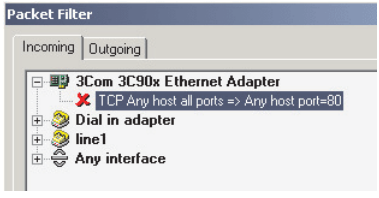
Je-li zapnuta funkce NAT, je celá lokální síť skryta a z Internetu nepřístupná (viz kap. NAT směrovač). Zároveň s funkcí NAT se také zapíná ochrana samotného počítače s WinRoute. Ta spočívá v tom, že při přístupu přes rozhraní, kde je zapnut NAT (typicky z Internetu) není možno komunikovat na žádném portu tohoto počítače s výjimkou mapovaných. Aplikace běžící na tomto počítači musejí být zpřístupněny mapováním portů, stejně jako aplikace běžící na počítačích v lokální síti.

Často je však potřeba omezovat přístup také z lokální sítě do Internetu – např. je-li potřeba snížit zatížení linky nebo zamezit uživatelům přístup na WWW stránky snižující produktivitu jejich práce apod. K tomuto účelu slouží ve WinRoute paketový filtr.

Další funkcí firewallu je zabránění zneužití IP adres (tzv. spoofingu). Toto nebezpečí hrozí, jestliže je WinRoute používán jen jako směrovač (bez funkce NAT). Jestliže bude mít útočník v jedné subsíti zdrojovou IP adresu patřící do subsítě jiného rozhraní, může tak snadno získat přístup ke službám, k nimž je povolen přístup pouze z lokální sítě. Firewall ve WinRoute tomu dokáže zabránit kontrolou platnosti zdrojové IP adresy na každém rozhraní.

Paketový filtr

Pravidla pro filtrování paketů lze nastavit v menu Settings –> Advanced –> Packet Filter.



Samostatná pravidla pro každé rozhraní

Filtrovací pravidla lze nastavit pro každé rozhraní zvlášť. To značně zjednodušuje definici těchto pravidel, zejména v případě, kdy má WinRoute několik rozhraní do lokálních segmentů. Rozhraní, pro které má být nový paketový filtr definován, lze jednoduše vybrat v okně Packet Filter.

Samostatná pravidla pro příchozí a odchozí pakety

Na každém rozhraní lze odděleně definovat pravidla pro příchozí a odchozí pakety. Pravidla pro příchozí pakety se definují v záložce „Incoming“, pro odchozí v záložce „Outgoing“. Seznam rozhraní je samozřejmě v obou záložkách stejný. Klasifikace paketů na odchozí a příchozí se provádí z pohledu daného rozhraní – např. pakety jdoucí z lokální sítě do Internetu jsou „Incoming“ na vnitřním rozhraní a „Outgoing“ na vnějším.

➢ Poznámka: Filtrování paketů se provádí DŘÍVE než NAT. Proto je možno i na vnějším rozhraní filtrovat pakety na základě privátních adres vaší lokální sítě.

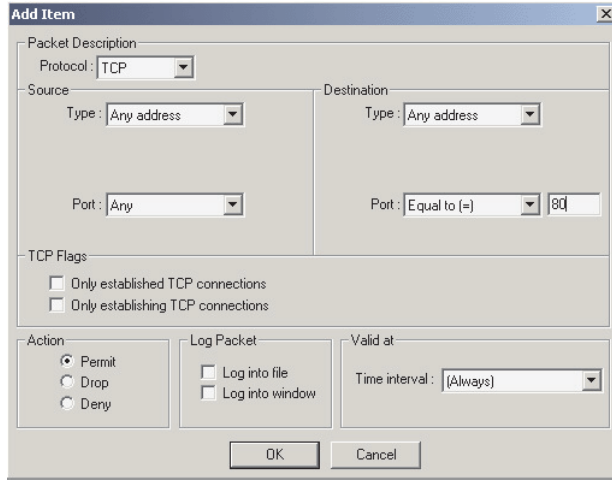
Aplikace pravidel: SHORA DOLŮ

Filtrovací pravidla jsou zpracovávána vždy shora dolů. Chcete-li tedy např. zakázat přístup na všechny WWW servery kromě jednoho, je třeba nejprve

definovat pravidlo povolující přístup na jeden konkrétní server a teprve pak pravidlo zakazující přístup na všechny servery. Pokud paket vyhoví kritériím určitého pravidla, pravidla pod ním se již nezpracovávají. Pořadí pravidel lze podle potřeby upravit tlačítky se šipkami (na pravém okraji okna Packet Filter).

Definice pravidel pro filtrování paketů

Nejprve je třeba určit, na kterém rozhraní a pro který směr má být pravidlo nastaveno. Podle toho vyberte záložku „Incoming“ nebo „Outgoing“ a příslušné rozhraní. Tlačítkem „Add“ přidejte nové filtrovací pravidlo:



Protocol

Specifikuje protokol, jehož pakety mají být filtrovány. Lze zvolit prakticky libovolný protokol transportní úrovně nesený v IP (předdefinovány jsou IP, TCP, UDP, ICMP, ARP a PPTP, volba „Other“ však umožňuje definovat protokol přímo číslem protokolu v IP záhlaví). Ve většině běžných případů však lze vystačit s protokolem TCP, případně UDP.

Source, Destination

Popis paketu, na nějž se má filtrovací pravidlo vztahovat. Paket je specifikován zdrojovou a cílovou IP adresou a v případě protokolů TCP a UDP také zdrojovým a cílovým portem.

V poli „Type“ lze vybrat typ zdrojové, resp. cílové adresy: libovolná adresa (Any Address), jeden počítač (Host), rozsah IP adres (Network/Range) nebo subsíť definovaná adresou a maskou (Network/Mask).

Je-li zvolen protokol TCP nebo UDP, je možno specifikovat také zdrojový, resp. cílový port: libovolný port („Any“), jeden konkrétní port (Equal to),

větší než (Greather than), menší než (Less than), neroven (Not equal to), v rozsahu (Between) nebo mimo rozsah (Not between).

TCP Flags, ICMP Types

Je-li zvolen protokol TCP nebo ICMP, je umožněna další specifikace:

- TCP Flags – filter se bude vztahovat jen na pakety navazující spojení (Only establishing TCP connections), nebo pouze na pakety v rámci již vytvořeného spojení (Only established TCP connections). Jsou-li obě volby vypnuty nebo naopak obě zapnuty, znamená to všechny TCP pakety.
- ICMP Types – filtrování jen vybraných typů ICMP zpráv (All = všechny).

Action

Akce, která se má provést s paketem vyhovujícím výše definovaným kritériím:

- „Permit“ – povolit. Tato volba se využije, má-li být definována výjimka z pravidla (např. zákaz přístupu na všechny WWW servery kromě jednoho) nebo pokud má být paket pouze zaznamenáván (viz volba „Log Packet“).
- „Drop“ – zahodit. Paket je „tiše zlikvidován“.
- „Deny“ – zakázat. Paket je rovněž zahozen, ale navíc se k jeho zdroji vyšle řídicí zpráva, že cíl je nedostupný. Tato volba je účinnější než „Drop“, protože klient (zdroj) se o nedostupnosti cíle okamžitě dozví, zatímco v případě „Drop“ se může domnívat, že se jedná o síťovou chybu, a pokusí se vysílání zopakovat. Volbu „Deny“ lze však použít pouze u protokolů IP, TCP a UDP.

Log Packet

Volby „Log into file“ a „Log into window“ zapínají záznam zachycených paketů do souboru „security.log“, resp. do okna Security Log.

Valid at

Tato volba umožňuje omezit platnost definovaného pravidla jen na vybraný časový interval (viz kap. Nástroje / časové intervaly).

Příklad nastavení paketového filtru

Uživatelům v lokální síti chceme povolit pouze přístup na WWW (TCP/80) a na Telnet servery (TCP/23). Kromě toho je třeba povolit DNS dotazy, aby uživatelé mohli zadávat cílové servery jmény.

Požadavky z lokální sítě PŘICHÁZEJÍ na VNITŘNÍ síťovou kartu – zvolíme tedy záložku „Incoming“ a vybereme rozhraní vedoucí do lokální sítě.

Přidáme následující pravidla:

1 Povol všechny TCP pakety s cílovým portem 23 (pro Telnet)

2 Povol všechny TCP pakety s cílovým portem 80 (pro WWW)

3 Povol všechny UDP pakety s cílovým portem 53 (pro DNS dotazy)

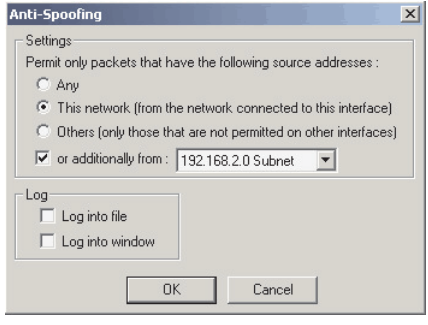
4 Zakaž veškerou ostatní IP komunikaci.

➢ Poznámka: Pravidla by bylo rovněž možno definovat na vnějším rozhraní v záložce „Outgoing“. Rozdíl je pouze v tom, že na vnitřním rozhraní budou filtrovány i pakety jdoucí přímo na počítač s WinRoute (v tomto případě nevadí).

Kontrola zdrojových IP adres (Anti-spoofing)

Je-li WinRoute použit jako směrovač (bez funkce NAT), není vaše lokální síť nijak chráněna (pokud se nepoužije např. paketový filtr). WinRoute umožňuje kontrolu, zda na každé rozhraní přicházejí pakety s platnými zdrojovými IP adresami. (Např. je-li jedno rozhraní připojeno do určité subsítě, neměly by se IP adresy z této subsítě vyskytovat jako zdrojové v paketech přicházejících na ostatní rozhraní.)

Kontrolu platnosti zdrojových adres (tzv. anti-spoofing) nastavíte v menu Settings –> Advanced –> Anti Spoofing. Vyberte rozhraní, na němž chcete nastavit platné zdrojové IP adresy, a stiskněte tlačítko „Settings“.



Settings

Možnosti volby „Permit only packets that have the following source address“ (povolit pouze pakety s následující zdrojovou adresou) jsou následující:

- „Any“ – povolena libovolná zdrojová adresa (anti-spoofing je vypnut)
- „This network (from the network connected to this interface)“ – jsou povoleny pouze zdrojové adresy ze subsítě, do níž je rozhraní přímo připojeno. Tuto volbu (samostatně) je možné použít pouze na rozhraní, které vede do lokální sítě tvořené jedním segmentem.
- „Others (only those that are not permitted on other interfaces)“ – povoluje pouze zdrojové adresy, které nejsou povoleny na ostatních rozhraních. Toto je typická volba pro rozhraní vedoucí do Internetu: tam se může vyskytovat téměř libovolná IP adresa kromě adres z lokálních sítí (připojených k ostatním rozhraním)
- „or additionally from“ – tato volba umožňuje rozšířit volby „This interface“ nebo „Others“ o další IP adresy.

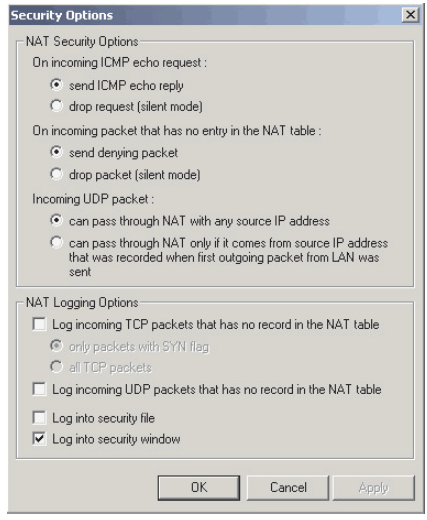
  Typické použití: k vnitřnímu rozhraní je připojena lokální síť tvořená dvěma IP segmenty. Na tomto rozhraní musejí být povoleny adresy z obou segmentů. Volba „This interface“ povolí adresy ze segmentu, do něhož je rozhraní připojeno (např. 192.168.1.x) a skupina adres uvedená ve volbě „or additionally from“ adresy ze druhého segmentu (např. 192.168.2.x). Volba „Others“ na internetovém rozhraní pak povoluje všechny zdrojové adresy s výjimkou těchto dvou subsítí.

Log

Volby „Log into file“ a „Log into window“ zapínají zaznamenávání paketů s neplatnými zdrojovými IP adresami (ve smyslu definovaných pravidel) do souboru „security.log“, resp. okna Security Log.

Volby zabezpečení

V menu Settings / Advanced / Security Options je možno nastavit další detailní parametry chování firewallu ve WinRoute.



NAT Security Options

Vlastní volby pro zabezpečení.

- On incoming ICMP echo request – zda má počítač s WinRoute odpovědět na přijatou zprávu Echo Request (PING). Volba „send ICMP echo reply“ znamená, že odpověď vyslána bude, „drop request (silent mode)“ naopak žádnou odpověď nevyšle a paket zahodí. Druhá možnost je též označována jako tzv. tichý mód (silent mode) a způsobuje, že je počítač z Internetu „neviditelný“.
- On incoming packet that has no entry in NAT table – jak se má reagovat na příchozí paket, pro nějž neexistuje záznam v NAT tabulce. Možnosti jsou: paket odmítnout (send denying packet) anebo jej zahodit a nereagovat na něj (drop packet (silent mode)). Odmítnutí paketu dá okamžitě vysílající straně na vědomí, že paket nebyl přijat, zatímco jeho zahození umožňuje utajit, že byl vůbec někým zachycen. Nastavení této volby by mělo korespondovat s nastavením volby předchozí.
- Incoming UDP packet – zda má být propuštěn UDP paket s libovolnou zdrojovou IP adresou (can pass through NAT with any source IP address) nebo pouze s takovou zdrojovou adresou, která byla zaznamenána v UDP paketu odcházejícím z lokální sítě (can pass through NAT only if it comes from source IP address that was recorded when first outgoing packet from LAN was sent).

  Je zřejmé, že druhá volba zaručuje vyšší bezpečnost; může ale způsobovat problémy např. v případě, že v chráněné privátní síti provozujete plnohodnotný DNS server, nebo když mají klientské stanice nastaveny přímo adresu nějakého DNS serveru v Internetu.

NAT Logging Options

Umožňuje nastavit, které pakety porušující bezpečnostní pravidla mají být zaznamenávány do Security Logu.

- Log incoming TCP packet that has no record in the NAT table – zaznamenat příchozí TCP paket, k němuž nebyl nalezen odpovídající záznam v NAT tabulce. Volba „only packet with SYN flag“ znamená, že se budou zaznamenávat pouze pakety navazující spojení (s příznakem SYN). Takový paket je zachycen typicky v případě, že se došlo k pokusu o navázání spojení na port chráněný firewallem. Volba „all TCP packets“ zapne záznam všech „podezřelých“ TCP paketů – tedy oproti první volbě navíc např. pakety se sekvenčním číslem, které nepatří do žádného otevřeného spojení.
- Log incoming UDP packet that has no record in the NAT table – zaznamenat příchozí UDP paket, k němuž nebyl nalezen odpovídající záznam v NAT tabulce, tedy takový paket, který není odpovědí na UDP paket vyslaný z lokální sítě.
- Log into security file – pakety se budou zaznamenávat do souboru „security.log“
- Log into security window – pakety se budou zaznamenávat do okna Security Log

DNS Forwarder

Základní informace

Každý počítač v Internetu je identifikován svou IP adresou. Ke komunikaci mezi počítači v Internetu je třeba znát IP adresu cílového počítače. Protože číselné adresy jsou těžko zapamatovatelné, byl vyvinut hierarchický systém jmen, nazvaný Domain Name System (zkr. DNS).

DNS je celosvětová distribuovaná databáze obsahující jména a k nim příslušné IP adresy (a další informace. Položky databáze jsou nazývány DNS záznamy). Uživatel tak nemusí znát přímo IP adresu cílového počítače, stačí znát jeho jméno. Navázání spojení klienta se serverem pak probíhá ve dvou fázích:

- zjištění cílové IP adresy ze jména
- navázání spojení na tuto adresu

Převod jmen na IP adresy zajišťují DNS servery. Klient pošle DNS serveru zprávu se jménem (tzv. dotaz) a DNS server vrátí odpověď s příslušnou

IP adresou (případně zprávu, že jméno neexistuje). Z toho vyplývá, že KAŽDÝ počítač v Internetu, který má být schopen komunikovat s počítači zadanými jménem, MUSÍ znát IP adresu alespoň jednoho DNS serveru.

DNS Forwarder ve WinRoute

WinRoute obsahuje modul nazvaný DNS Forwarder. Ten se navenek chová jako DNS server, tzn. odpovídá na dotazy klientů, ve skutečnosti ale pouze předává tyto dotazy jinému DNS serveru v Internetu. Zodpovězené dotazy ukládá do své cache, takže v případě opakovaného dotazu na totéž jméno je schopen odpovědět sám. Taková odpověď je samozřejmě několikanásobně rychlejší než odpověď DNS serveru v Internetu.

Kromě toho může DNS Forwarder sám fungovat jako jednoduchý DNS server pro jednu (lokální) doménu. Data pro tuto doménu čte se systémového souboru HOSTS. Přijme-li DNS Forwarder dotaz na jméno, zkontroluje nejprve, zda není toto jméno s příslušnou IP adresou uvedeno v souboru HOSTS. Pokud ano, dotaz zodpoví, jinak jej předá DNS serveru v Internetu.

Soubor HOSTS

Soubor HOSTS (jmenuje se přímo takto – tedy „HOSTS“ bez přípony) je systémový soubor, který může být vytvořen v každém systému podporujícím TCP/IP. Systémový DNS klient nejprve hledá dotazované jméno v tomto souboru, a teprve v případě neúspěchu pošle dotaz na DNS server. Struktura souboru HOSTS je velmi jednoduchá: na každé řádce je uvedeno jedno jméno a mezerou nebo tabulátorem oddělená příslušná IP adresa.

Ve Windows NT/2000 je tento soubor umístěn v adresáři „\WINNT\System32\drivers\etc“, ve Windows 95/98/ME je to adresář „\WINDOWS“. Správce WinRoute se však umístěním souboru nemusí zabývat – soubor lze modifikovat přímo z dialogu nastavení DNS Forwarderu.

Nastavení DNS Forwarderu

Zvolte menu Settings –> DNS Forwarder. Konfigurační dialog nabízí následující volby:

Enable DNS Forwarding

Zapnutí / vypnutí DNS Forwarderu. Po instalaci WinRoute je DNS Forwarder zapnut. Vypněte jej v případě, že budete chtít na tomtéž počítači provozovat jiný DNS server.

Forward DNS queries to the server automatically selected from DNS servers known to the operating system

Je-li nastavena tato (výchozí) volba, WinRoute přečte nastavení DNS serverů v systému Windows a předává dotazy primárnímu DNS serveru.

Forward DNS queries to the specified DNS server(s)

Použijte tuto volbu, jestliže chcete specifikovat DNS server, kterému budou dotazy předávány. Je možno zadat i více DNS serverů (např. primární a sekundární). Jednotlivé IP adresy se oddělují středníkem nebo mezerou.

➢ Poznámka: Z hlediska funkčnosti i rychlosti jsou obě volby výběru DNS serveru rovnocenné. Záleží víceméně na správci WinRoute, pro kterou z nich se rozhodne.

Enable cache for faster response of repeated queries

Zapnutí / vypnutí interní cache DNS Forwarderu pro ukládání odpovědí na DNS dotazy. Doporučuje se NEVYPÍNAT tuto volbu, protože by se tím činnost DNS Forwarderu značně zpomalila.

Cache má pevnou velikost a existuje pouze v operační paměti po dobu běhu WinRoute Engine. Doba uchovávání jednotlivých DNS záznamů je dána jejich dobou života (TTL, zpravidla 1 den).

HOSTS file

Zapíná použití systémového souboru HOSTS pro zodpovídání DNS dotazů. Dotaz se předá DNS serveru v Internetu teprve tehdy, není-li v souboru HOSTS dotazované jméno nalezeno.

Tlačítko „Edit file“

Stiskem tohoto tlačítka se spustí externí textový editor (obvykle Notepad – Poznámkový blok), v němž můžete upravovat soubor HOSTS.

DHCP lease table

Tato volba je dostupná pouze pokud je zapnut DHCP server ve WinRoute. Je-li zapnutá, DNS Forwarder zkusí před předáním dotazu jinému DNS serveru nalézt dotazované jméno v tabulce přidělených adres DHCP serveru. Tak lze velice snadno udržet lokální DNS aktuální, i když se dynamicky přidělované adresy jednotlivých počítačů v čase mění. (Jestliže se ve Windows konfigurují parametry TCP/IP protokolem DHCP, systém VŽDY pošle DHCP serveru své jméno. Například v systému Linux tomu ale tak není – DHCP klienta je třeba nakonfigurovat, aby jméno posílal.)

When resolving name from HOSTS file or lease table combine it with domain below

Používáte-li pro lokální DNS dotazy soubor HOSTS nebo tabulku přidělených adres DHCP, uveďte do tohoto pole název lokální domény (např. „FIRMA.CZ“). V souboru HOSTS pak není nutno uvádět celá DNS jména (např. „SERVER.FIRMA.CZ“), ale stačí pouze jména počítačů („SERVER“). (V tabulce DHCP serveru je rovněž uvedeno pouze jméno počítače bez domény).

Nastavíte-li správně lokální doménu, DNS Forwarder bude schopen správně zodpovědět dotaz na „SERVER“ i na „SERVER.FIRMA.CZ“.

DHCP server

Základní informace

Každý počítač ve vaší lokální síti musí mít správně nastaveny parametry protokolu TCP/IP, aby mohl komunikovat s ostatními počítači v lokální síti i v Internetu. Na každém počítači je tedy třeba nastavit IP adresu, masku subsítě, adresu výchozí brány a DNS serveru, případně další parametry. Obsahuje-li vaše síť desítky či stovky počítačů, je to poměrně náročná záležitost – jednak časově a jednak může snadno dojít k chybě, např. vícenásobné přiřazení téže IP adresy apod.

Pro zjednodušení tohoto úkolu byl vyvinut protokol DHCP (Dynamic Host Configuration Protocol). DHCP umožňuje dynamické přiřazování IP adres a dalších parametrů TCP/IP počítačům v síti. Klientský počítač vyšle při startu systému DHCP požadavek. DHCP server vybere vhodné konfigurační parametry a pošle je klientovi. Protokol TCP/IP je tak na klientské stanici nakonfigurován zcela automaticky.

DHCP server vždy zajistí, aby klientovi nebyla přidělena IP adresa kolidující s jiným klientem. Konfigurace je zpravidla přidělována na omezenou dobu (tzv. dobu pronájmu, angl. lease time).

Aby byla stanice se systémem Windows automaticky konfigurována protokolem DHCP, stačí pouze nastavit volbu „Získávat IP adresu automaticky“ („Obtain an IP address automatically“). Tato volba je výchozí volbou po instalaci Windows. Ve skutečnosti neznamená pouze automatické nastavení IP adresy, ale všech parametrů TCP/IP.

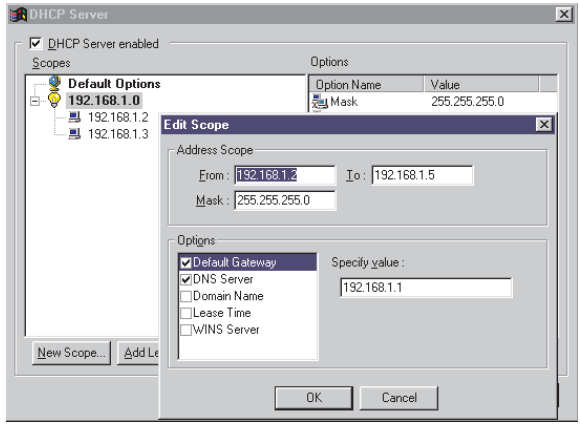
Ve vaší síti mohou být současně stanice konfigurované dynamicky protokolem DHCP a stanice, které mají z nějakého důvodu nastavenu IP adresu

ručně. Toto je samozřejmě bez problémů možné, pouze je potřeba nastavit v DHCP serveru rozsah přidělovaných adres tak, aby nekolidoval s adresami nastavenými ručně.

Konfigurace DHCP serveru ve WinRoute

Nejprve důkladně zkontrolujte, zda je na klientských počítačích nastavena volba „Získávat IP adresu automaticky“ („Obtain an IP address automatically“) a že NEJSOU ručně nastaveny žádné parametry protokolu TCP/IP.

V programu WinRoute Administration zvolte menu Settings –> DHCP Server. Tlačítkem „New Scope“ vytvořte nový rozsah přidělovaných IP adres:



From, To, Mask

Zadejte počátek a konec rozsahu přidělovaných adres a odpovídající masku subsítě. Dobře zkontrolujte, zda počáteční i koncová adresa náleží do stejné subsítě a obě adresy korespondují s uvedenou maskou!

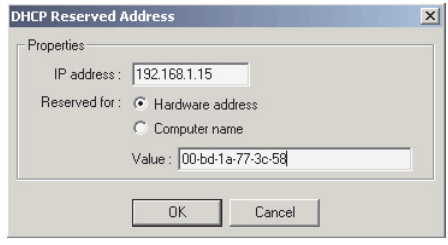
Options

Nastavte pečlivě volitelné parametry TCP/IP, které chcete DHCP serverem přidělovat. Je NUTNÉ nastavit alespoň výchozí bránu („Default Gateway“) a adresu DNS serveru. Máte-li vlastní lokální doménu, nezapomeňte ji zadat jako parametr „Domain Name“ (např. „FIRMA.CZ“). Nenastavíte-li některý parametr, použije se výchozí hodnota definovaná v „Default Options“ (pokud je tam nastavena), jinak parametr zůstane prázdný.

Další nastavení

Tlačítkem „Edit“ lze změnit nastavení vybraného rozsahu přidělovaných adres, případně výchozích parametrů (Default Options). Tlačítkem

„Remove“ vybraný rozsah odstraníte (Default Options odstranit nelze). Tlačítkem „Add Lease“ je možno vyhradit určitou IP adresu pro konkrétní ethernetovou adresu nebo jméno počítače. To má za následek, že příslušné stanici bude DHCP serverem přidělována stále stejná IP adresa (pokud nedojde k výměně síťové karty nebo ke změně jména počítače).



Hardwarová adresa se zapisuje v hexadecimální podobě a jednotlivé byty se zde oddělují pomlčkami, tedy např. "00-bd-1a-77-3c-58".

➢ TIP: Jak zjistit hardwarovou (ethernetovou) adresu určité stanice? Nechte stanici dynamicky nakonfigurovat protokolem DHCP a zjistěte si (např. příkazem „ipconfig“), jaká jí byla přidělena IP adresa. V DHCP serveru pak pod příslušným rozsahem vyberte tuto adresu a v pravé části okna můžete zjistit odpovídající hardwarovou adresu. Rezervovat IP adresu pro hardwarovou adresu je obvykle vhodnější než pro jméno stanice – to může její majitel či uživatel snadno změnit.

Mail server

Základní informace

WinRoute obsahuje propracovaný SMTP/POP3 mail server s následujícími vlastnostmi:

- možnost vytvoření lokálních uživatelských POP3 schránek (jejich maximální počet je dán licencí WinRoute)
- vytváření virtuálních adres (aliasů) pro jednotlivé uživatele a skupiny uživatelů
- vybírání vzdálených POP3 schránek a jejich doručování, případně třídění do lokálních schránek
- plánování časů a intervalů přijímání a odesílání pošty
- ochrana proti zneužití k rozesílání reklamních mailů (tzv. spamů)

Nechcete-li používat mail server ve WinRoute...

Pro komunikaci elektronickou poštou není nutno používat mail server ve WinRoute. WinRoute vám díky svým vlastnostem softwarového směrovače umožňuje připojit se poštovním klientem z lokální stanice přímo k SMTP a POP3 (příp. IMAP) serveru v Internetu (např. u vašeho poskytovatele internetového připojení), stejně jako provozovat ve vaší lokální síti libovolný jiný mail server.

- Poznámka: NEDOPORUČUJE se vytvářet e-mailové adresy (účty anebo aliasy) s českými písmeny (s háčky a čárkami)! Z hlediska WinRoute i Windows je to sice zcela korektní, ale uživatelé jiných systémů (Unix, Mac,...) vám pravděpodobně nebudou moci mail na takovou adresu vůbec poslat.

Uživatelské mailové schránky

Mailová schránka uživatele je ve WinRoute vytvořena automaticky při vytvoření uživatelského účtu. Platí následující pravidla:

Jeden uživatel = jedna schránka

Každý uživatel ve WinRoute má právě jednu schránku. Tato schránka je vytvořena jako podadresář v základním adresáři mailserveru (standardně „\Program Files\WinRoute Pro\mail“). Uživatelský podadresář má název shodný se jménem uživatelského účtu a vytváří se až v okamžiku přijetí prvního mailu pro daného uživatele.

- Poznámka: V adresáři „mail“ je kromě uživatelských schránek vytvořen ještě speciální adresář „spool“, který představuje odchozí frontu (tj. maily čekající na odeslání).

Jeden uživatel = více e-mailových adres

Máte-li vlastní internetovou doménu (např. „firma.cz“) a uvedete-li ji ve WinRoute jako lokální doménu (viz dále), získá každý uživatel automaticky adresu „jméno@firma.cz“ (kde „jméno“ je název příslušného uživatelského účtu). Dále je možno vytvářet tzv. aliasy, které umožňují uživateli používat více e-mailových adres nebo vytvoření skupinových adres (typu „info@firma.cz“, „obchod@firma.cz“). Možné kombinace jsou téměř nevyčerpatelné.

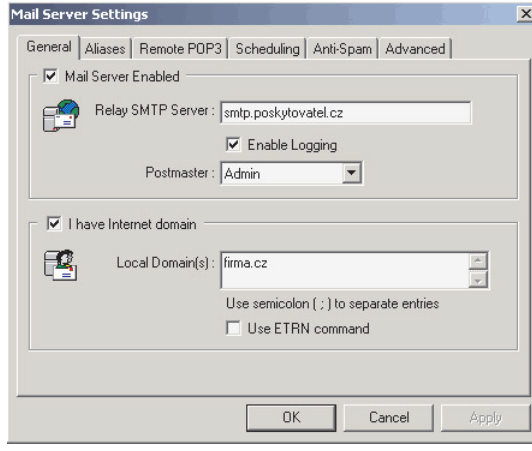
Vytvoření uživatelů (schránek)

Uživatelské účty vytvoříte volbou Settings –> Accounts. Podrobnosti viz kap. Uživatelé a skupiny.

Odesílání pošty – SMTP server

WinRoute obsahuje SMTP server, přes který mohou klienti odesílat svou poštu. SMTP server odesílá všechnu poštu na jeden nadřazený SMTP server (Relay SMTP Server), což je obvykle SMTP server vašeho poskytovatele Internetu. Odeslání všech mailů na nadřazený SMTP server má výhodu, že všechny maily jsou odeslány rychle a jednorázově (rozesílání do cílových domén je pomalejší a v případě nedostupnosti cílového serveru se musí odesílání opakovat).

Nastavení SMTP serveru ve WinRoute se provádí v menu Settings –> Mail Server, záložka „General“.



Mail Server Enabled

Zapnutí / vypnutí SMTP a POP3 mailserveru ve WinRoute.

Relay SMTP Server

SMTP server, na který budou všechny odchozí maily poslány (typicky server vašeho poskytovatele). Je možné jej zadat IP adresou i DNS jménem.

Enable Logging

Zapnutí logování základních informací o činnosti mail serveru do okna Mail Log a souboru „mail.log“.

Postmaster

V tomto poli je možno uvést uživatele, kterému bude mail server posílat systémové a chybové zprávy.

I have Internet domain

Zapněte tuto volbu, jestliže máte internetovou doménu (např. „firma.cz“), která je z pohledu mailserveru ve WinRoute lokální, tj. všichni uživatelé v této doméně mají ve WinRoute své schránky.

- Poznámka: Nejsou-li všichni uživatelé ve vaší doméně lokální (tj. někteří mají svou schránku jinde), NELZE doménu definovat jako lokální! Podrobnosti viz kap. Aliasy.

Local Domain(s)

Zde uveďte název vaší domény. Můžete uvést i více domén, jsou-li z pohledu tohoto mail serveru lokální (Příklad: Vaše firma má domény „firma.cz“ a „firma.com“. Každý uživatel má jednu schránku, do níž se doručují maily poslané jak na „jméno@firma.cz“, tak na „jméno@firma.com“. Domény jsou v tomto případě rovnocenné a lze je tedy OBĚ prohlásit za lokální). Jednotlivá jména domén v poli „Local Domain(s)“ oddělujte středníky (tedy např. „firma.cz;firma.com“) nebo mezerami („firma.cz firma.com“). Z důvodu přehlednosti doporučujeme vybrat si pouze jednu z těchto možností.

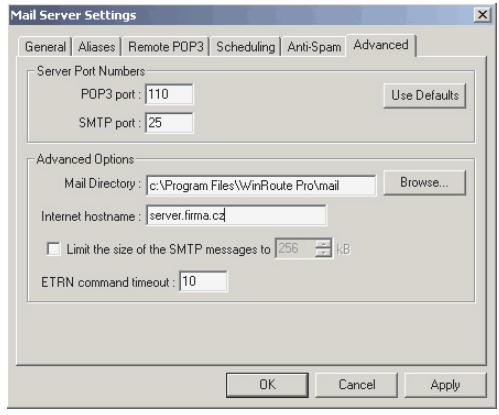
- POZOR: Pro KAŽDOU doménu v poli „Local Domain(s)“ platí, že mail poslaný na adresu „jméno@lokální_doména“ bude doručován do lokální schránky „jméno“. Mají-li být adresy „jméno@doména1“ a „jméno@doména2“ doručovány do různých schránek, NESMÍ být alespoň jedna z těchto domén uvedena jako lokální! Podrobnosti naleznete opět v kap. Aliasy.

Use ETRN command

Zaškrtněte tuto volbu, jestliže není váš server trvale připojen do Internetu (typicky máte-li vytáčené připojení) a zároveň chcete přijímat poštu protokolem SMTP. V ostatních případech nemá tato volba význam. Detaily viz kap. Příjem pošty.

Nastavení parametrů mail serveru

Zvolte menu Settings –> Mail Server a vyberte záložku „Advanced“. Zde je třeba provést některá upřesňující nastavení:



POP3 port, SMTP port

Porty, na nichž POP3 a SMTP server běží. NEMĚŇTE čísla portů, pokud si nejste OPRAVDU jisti, co děláte! Porty 110 a 25 jsou standardní a všechny mailové servery i klienti je používají. Standardní porty lze nastavit stiskem tlačítka „Use Defaults“.

Mail Directory

Určuje adresář, v němž budou vytvářeny uživatelské schránky a fronta mailů čekajících na odeslání. Doporučuje se měnit tento adresář pouze je-li k tomu opravdu závažný důvod (např. na disku, kde je WinRoute nainstalován, není dostatek volného místa).

- Poznámka: „Dostatek volného místa“ je velmi relativní pojem. Maily je možno ze schránek vybírat pouze protokolem POP3, a nemá-li uživatel nastavenu volbu „Ponechat kopie zpráv na serveru“ („Leave a copy of messages on server“), jsou při vybírání schránky maily přesunuty na lokální disk uživatele a místo na disku serveru tedy nezabírají. Jestliže ale uživatel schránku po několik dnů či týdnů nevybírá, maily se v ní hromadí a disk se zaplňuje. Je-li to možné, doporučujeme počítat s alespoň 10 MB diskového prostoru na jednu schránku.

Internet hostname

Tato položka by měla obsahovat plné DNS jméno vašeho mail serveru (pokud se např. počítač jmenuje „SERVER“ a lokální doména „FIRMA.CZ“, uvedete zde „SERVER.FIRMA.CZ“ (máte-li více lokálních domén, vyberte jednu z nich). Tímto jménem se váš SMTP server prokazuje při odesílání pošty na nadřazený (relay) SMTP server. Záleží na nadřazeném serveru, zda toto jméno kontroluje či nikoliv, přesto vám doporučujeme VŽDY tuto položku správně vyplnit (může se totiž stát, že správce nadřazeného SMTP serveru toto ověřování dostatečně zapne).

Je-li položka „Internet hostname“ vyplněna chybě (např. je zde ponecháno výchozí „unspecified.host“) a nadřazený SMTP server jméno odesílajícího serveru kontroluje, pošta se neodešle a v okně Error Log se objeví typicky toto hlášení:

mail: can’t send email: Server replied: 550 Relaying denied

Odesílatel (případně také uživatel Postmaster, je-li nastaven) rovněž obdrží zprávu s tímto chybovým hlášením. Tuto situaci lze zpravidla vyřešit správným nastavením položky „Internet hostname“.

➢ Poznámka: Máte-li položku „Internet hostname“ nastavenu správně a přesto obdržíte chybové hlášení podobné výše uvedenému, znamená to, že nadřazený server neakceptuje poštu přijatou z vašeho serveru nebo používá jiný typ ověřování. V tomto případě se dohodněte se správcem nadřazeného serveru (zpravidla je to váš poskytovatel Internetu). Informace o ověřování jménem a heslem naleznete na konci této kapitoly.

Limit the size of the SMTP messages to

Umožňuje stanovit maximální velikost zprávy (mailu), která bude SMTP serverem akceptována. Použijte tuto volbu, chcete-li zabránit posílání velkých mailů (např. s několikamegabytovými soubory v přílohách). To může být užitečné např. v případě pomalé vytáčené linky.

ETRN command timeout

Příkaz ETRN se používá, jestliže přijímáte poštu protokolem SMTP a váš server není trvale připojen k Internetu (detailně viz kap. Příjem pošty). Jestliže WinRoute pošle nadřazenému serveru příkaz ETRN, tento mu buď pošle nashromážděné maily, anebo mlčí (pokud žádné maily nemá). Na příkaz ETRN neexistuje záporná odpověď. Příkaz ETRN tedy musí mít definovánu dobu vypršení (timeout), po které vyhodnotí situaci tak, že žádné nové maily nepřišly, a spojení s nadřazeným serverem ukončí.

Doba vypršení se zde nastavuje v sekundách. Nejlepší je ji určit experimentálně, výchozí hodnota 10 sec však zpravidla postačí.

Ověřování u nadřazeného serveru jménem a heslem

Vyžaduje-li nadřazený SMTP server ověření uživatele jménem a heslem, je možné nastavit mail server ve WinRoute tak, aby tyto údaje nadřazenému serveru posílal.

K tomuto účelu je třeba mít WinRoute Pro verzi 4.1.25 (Build 25) nebo vyšší. Ve starších verzích není tato funkce k dispozici.

Nastavení je nutno provést v registru Windows. Nejprve zastavte WinRoute Engine (jinak by změny v registru byly neúčinné). Pak spusťte Registry Editor (regedit.exe) a přepněte se do větve HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute. Zde je třeba nastavit následující položky:

- MailRelayAuth – hodnota „1“ znamená, že se ověřování bude provádět. Chcete-li ověřování vypnout, nastavte zde původní hodnotu „0“
- MailRelayUser, MailRelayPass – uživatelské jméno a heslo pro ověření
- MailRelayPort – zde je možno nastavit port, na němž běží nadřazený SMTP server (výchozí hodnota je „25“ – standardní port pro SMTP)

Po provedení změn ukončete Registry Editor a spusťte WinRoute Engine.

Příjem pošty protokolem SMTP

WinRoute umožňuje přijímat poštu protokolem SMTP a/nebo vybírat libovolný počet POP3 schránek a doručovat, případně třídit je do schránek lokálních.

Chcete-li přijímat poštu protokolem SMTP, musejí být splněny následující dvě podmínky:

- DNS záznam „MX“ (Mail Exchange) pro vaši doménu musí být správně nasměrován na váš SMTP server (tj. počítač s WinRoute). Spravujete-li sami DNS server pro vaši doménu, nastavte správně tento záznam, jinak se dohodněte s vaším poskytovatelem Internetu.
- Port 25 vašeho SMTP serveru musí být z Internetu přístupný. Máte-li na vnějším rozhraní zapnutou funkci NAT, je třeba port 25 zpřístupnit (tj. namapovat jej na adresu některého rozhraní počítače s WinRoute). Podrobnosti naleznete v kap. NAT směrovač / Mapování portů.

➢ POZOR: Na mapovaný port 25 se může připojit KTERÝKOLIV SMTP SERVER v Internetu, aby mohl do vaší domény doručit mail. NENASTAVUJTE proto u mapovaného portu volbu „Allow access only from“ ani nepoužívejte žádný paketový filtr na port 25! Jinak vám pravděpodobně většina mailů nebude moci být doručena.

V závislosti na vašem internetovém připojení existují dva způsoby, jak přijímat poštu protokolem SMTP:

1. Pevné připojení

Splníte-li výše uvedené podmínky, není třeba žádných dalších nastavení. Nezapomeňte specifikovat lokální doménu (domény), případně nastavit příslušné aliasy (viz kap. Aliasy).

2. Vytáčené připojení (příkaz ETRN)

V tomto případě není váš mail server trvale dostupný a maily se shromažďují na SMTP serveru vašeho poskytovatele Internetu. V záložce „General“ je třeba nastavit volbu „Use ETRN command“. V okamžiku připojení vyšle váš SMTP server nadřazenému SMTP serveru příkaz ETRN, který říká „jsem připraven, můžeš mi poslat maily“. Nadřazený SMTP

server buď pošle maily se své fronty, anebo na příkaz ETRN neodpoví. Proto je třeba správně nastavit vypršení (timeout) příkazu ETRN v záložce „Advanced“ – viz kap. Nastavení parametrů mail serveru.

Aby mohlo přijímání pošty pomocí ETRN správně fungovat, je třeba splnit ještě následující podmínky.

- Pro vaši doménu musejí být nastaveny (alespoň) dva MX záznamy. První, s nejvyšší prioritou, bude nasměrován přímo na váš SMTP server (tj. počítač s WinRoute). V době, kdy budete do Internetu připojeni, budou maily posílány přímo vašemu serveru (tedy stejně jako v případě pevného připojení).

  MX záznam s druhou nejvyšší prioritou musí být na směrován na SMTP server vašeho poskytovatele Internetu, který podporuje příkaz ETRN. Bude-li váš SMTP server nedosažitelný (v době, kdy nejste připojeni), budou maily doručovány na tento server, odkud si je váš server po připojení vyžádá příkazem ETRN.
- SMTP server, nastavený v položce „Relay SMTP server“ (záložka „General“), musí bý tentýž server, na kterém jsou maily dočasně uchovávány. WinRoute komu ikuje pouze s jedním SMTP serverem.

➢ Poznámka: Detailní vysvětlení nastavování MX záznamů je nad rámec manuálu WinRoute Pro. Tato nastavení však zpravidla provádí váš poskytovatel Internetu – vám stačí pouze nastavit správný nadřazený SMTP server a zapnout používání příkazu ETRN.

Příjem pošty pro více domén

Má-li SMTP server ve WinRoute přijímat poštu pro více domén současně, mohou nastat dva případy:

1 MX záznamy pro všechny tyto domény jsou nastaveny na jednu IP adresu. Pak stačí, aby byl správně mapován port 25 (viz výše).

2 Každý MX záznam je nasměrován na jinou IP adresu. V tomto případě musí být všechny tyto adresy přiřazeny vnějšímu rozhraní počítače s WinRoute (možno pouze ve Windows NT/2000). Pro každou z těchto adres pak musíte provést mapování portů následujícím způsobem:

   Protocol: TCP

   Listen IP: jedna z vnějších adres (pro níž má být port 25 zpřístupněn)

   Listen port: single port 25

Destination IP: Shodná s „Listen IP“! Není možné provést vícenásobné mapování na tutéž dvojici <Destination IP; Destination Port>.

Destination port: 25

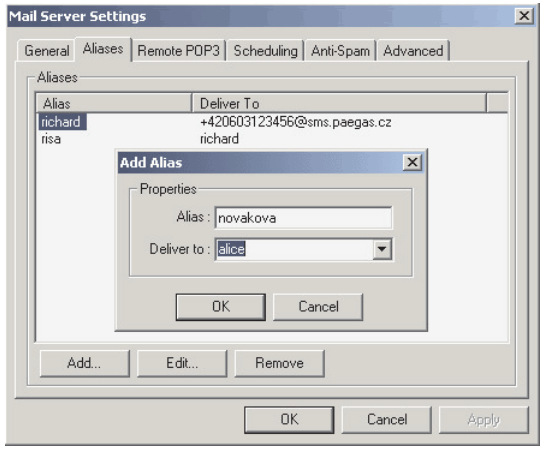
Aliasy

Aliasy ve WinRoute rozšiřují možnosti e-mailových adres. Použitím aliasů můžete např.:

- přiřadit konkrétnímu uživateli další e-mailovou adresu
- přiřadit jednu adresu skupině uživatelů, resp. více uživatelům
- posílat kopii mailu na jinou (externí) adresu

➢ POZOR: Aliasy se uplatňují pouze na maily přijaté protokolem SMTP (resp. zpracovávané SMTP serverem). Samy o sobě neovlivňují příjem mailů ze vzdálených POP3 schránek – ty lze pouze doručovat konkrétním uživatelům nebo třídit pomocí Sorting Rules.

Aliasy se definují v menu Settings –> Advanced, záložka „Aliases“.



Alias se skládá ze dvou částí:

- „Alias“ – tj. výsledná e-mailová adresa (nebo její část před znakem ‚@‘)
- „Deliver To“ – uživatel, skupina, JINÝ ALIAS nebo externí e-mailová adresa, kam má být mail doručen

Tlačítky „Add“, „Edit“ a „Remove“ lze vytvořit, změnit a smazat alias. Dialog pro vytvoření a změnu aliasu umožňuje pouze definovat výše uvedené položky „Alias“ a „Deliver To“. V položce „Deliver To“ se standardně nabízí seznam lokálních uživatelů a skupin, je však možno ručně zadat i jiný alias nebo externí e-mailovou adresu.

Tentýž alias (tj. řádka se stejnou hodnotou položky „Alias“) může být definován i vícekrát. Tak je možno zajistit např. doručování do lokální schránky a zároveň na externí adresu.

➢ Poznámka: Na pořadí aliasů nezáleží, protože jsou vždy procházeny všechny.

Příklady nastavení aliasů

Pro snazší pochopení ukažme alespoň několik častějších situací a způsoby, jak aliasy definovat.

- Je definována lokální doména „firma.cz“. Uživatel „richard“ chce kromě adresy „richard@firma.cz“ (která je mu vytvořena automaticky definicí lokální domény) používat také adresu „risa@firma.cz“ a zároveň požaduje posílat upozornění o každé zprávě na svůj mobilní telefon. Definujeme následující aliasy:

  Alias: „risa“ Deliver To: „richard“

  Alias: „richard“ Deliver To: „+420603123456@sms.paegas.cz“

  Alias: „richard“ Deliver To: „richard“ (nutné – jinak by mail byl doručen pouze na mobilní telefon a ne do lokální schránky)
- Mail poslaný na adresu „info@firma.cz“ má být doručen všem uživatelům ve skupině „Info“. Definujeme alias:

  Alias: „info“ Deliver To: „[Info]“
- Doména „jinafirma.cz“ není definována jako lokální, protože někteří uživatelé z této domény mají své schránky na jiném serveru. Pro jednoduchost předpokládejme pouze uživatele „pavel“ a „karel“. „pavel“ má svou schránku přímo ve WinRoute, zatímco „karel“ má svou schránku v doméně „nekdejinde.cz“. Definujeme aliasy:

  Alias: „pavel@jinafirma.cz“ Deliver To: „pavel“

  Alias: „karel@jinafirma.cz“ Deliver To: „karel@nekdejinde.cz“

  Všimněte si, že pokud není doména definována jako lokální, je třeba v hlavičce aliasu uvést CELOU adresu.

Speciální aliasy

Kromě výše popsaných způsobů je možno definovat ještě následující dva typy aliasů:

- Alias: „*“ Deliver To: ...

  Tento alias se uplatní v případě, že se e-mailová adresa přijatého mailu (resp. její část před znakem ‚@‘) neshoduje s žádným uživatelským jménem ani nevyhovuje žádnému definovanému aliasu. To může typicky nastat, udělá-li odesílatel v adrese chybu. Je-li definován tento alias, pak se takový mail rovněž doručí (jednomu uživateli, skupině, ...).
- Alias: „*@nejakadomena.cz“ Deliver To: ...

Alias v tomto tvaru umožní zpracování všech mailů pro danou doménu – typicky doručení do jedné schránky.

- Poznámka: Takto lze ve WinRoute vytvořit doménovou schránku…
- POZOR: Jiné použití znaku „*“ (hvězdička) (např. pro doplnění části uživatelského jména) je NEPŘÍPUSTNÉ!

Vybírání vzdálených POP3 schránek

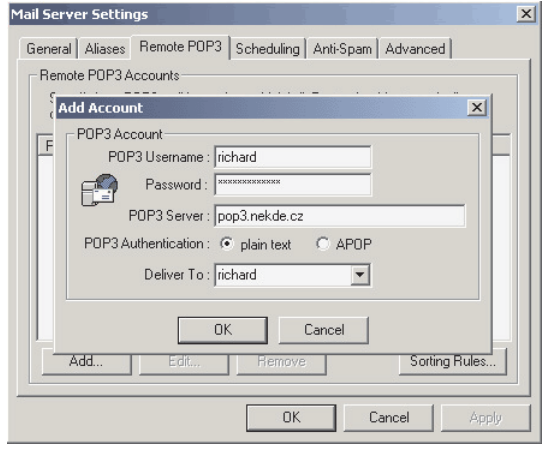
Kromě příjmu pošty protokolem SMTP umožňuje WinRoute také vybírání libovolného počtu POP3 schránek kdekoliv v Internetu a jejich doručování, případně třídění do schránek lokálních. Vybírání schránek je zcela nezávislé na nastavení SMTP serveru – např. může být vybírána schránka pro jinou doménu, než která je nastavena v „Local Domain(s)“ apod.

1. Soukromé schránky uživatelů

První možnost je, že každý uživatel má v Internetu svoji vlastní schránku. WinRoute tuto schránku vybere a doručí ji do schránky lokální.

- Poznámka: Mohlo by se zdát, že tato operace je zbytečná – klient na stanici v lokální síti se může připojit přímo na svou schránku v Internetu a vybrat ji sám. WinRoute ale umožňuje schránku vybírat v pravidelných intervalech (nejen na žádost uživatele). Uživatel pak komunikuje pouze s POP3 serverem ve WinRoute v rámci lokální sítě, což je nesrovnatelně rychlejší.

Zvolte menu Settings –> Mail Server a vyberte záložku „Remote POP3“. Pro každou schránku, kterou chcete vybírat, přidejte tlačítkem „Add“ jeden „účet“:



POP3 Server

Server, na kterém je schránka umístěna (např.server vašeho poskytovatele Internetu).

POP3 Username, Password

Přístupové jméno a heslo k této schránce.

POP3 Authentication

Způsob posílání hesla („plain text“ – v přímém tvaru, „APOP“ – šifrovaně). Poznámka: Většina POP3 serverů vyžaduje heslo v nešifrovaném tvaru („plain text“).

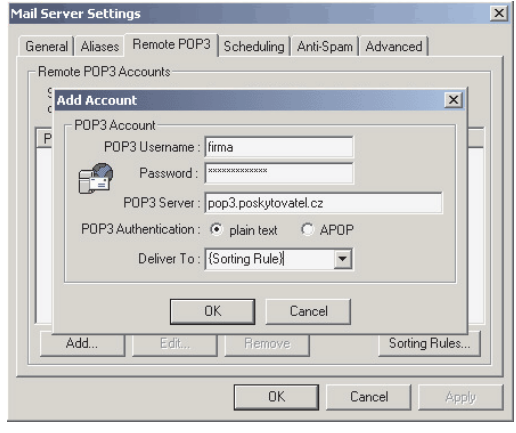
Deliver To

Uživatel, do jehož schránky mají být maily doručeny. V tomto poli se standardně zobrazí lokální uživatelé a skupiny, dále je zde však také možno ručně zapsat alias (definovaný v záložce „Aliases“) nebo libovolnou (externí) e-mailovou adresu. Z toho vyplývá, že maily vybrané z POP3 schránky mohou být doručeny nejen lokálnímu uživateli, ale také skupině uživatelů, přeposlány na vnější e-mailovou adresu apod.

2. Doménová schránka

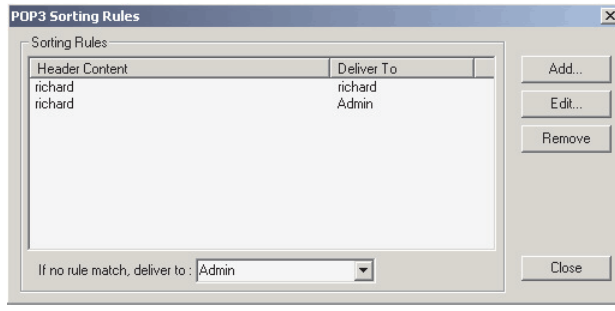
Doménová schránka je POP3 schránka, zpravidla na serveru poskytovatele Internetu, do níž jsou doručovány všechny maily pro danou doménu (část před znakem ‚@‘ se nerozlišuje). WinRoute umí maily z takovéto schránky stáhnout a roztřídit je (podle původních adresátů) do lokálních uživatelských schránek.

V záložce „Remote POP3“ definujte účet pro doménovou schránku.



Nastavení účtu je stejné jako v předchozím případě, pouze v poli „Deliver To:“ vyberte „{Sorting Rules}“. To znamená, že se přijaté maily budou zpracovávat podle speciálních třídicích pravidel.

V záložce „Remote POP3“ stiskněte tlačítko „Sorting Rules“ a definujte pravidla, podle kterých se mají maily třídit:



Header Content

Výraz, který se má vyskytovat v hlavičce mailu a který jednoznačně identifikuje adresáta. Tento výraz je jako PODŘETĚZEC vyhledáván v hlavičce zpracovávaného mailu, a to v položkách „To:“, „Cc:“ a „Apparently-To:“. Je-li v některé z těchto položek nalezen, doručí se mail příslušnému uživateli.

Deliver To

Uživatel, jemuž má být mail doručen. Při definici nového pravidla (po stisku tlačítka „Add“) je u této položky umožněn výběr ze seznamu lokálních uživatelů a skupin, kromě toho je však možné zde ručně zadat alias (definovaný v záložce Aliases) nebo libovolnou externí e-mailovou adresu. I při třídění mailů z doménové schránky je tedy možné je přeposílat na jiný server.

- Poznámka: V třídicích pravidlech se může pravidlo pro stejný obsah hlavičky (položka „Header Content“) vyskytovat i vícekrát. Můžete tak např. doručit mail lokálnímu uživateli a zároveň jej poslat na externí e-mailovou adresu, aniž byste museli použít alias.
- Poznámka 2: Na pořadí třídicích pravidel nezáleží, protože jsou vždy procházena všechna.

If no rule match, deliver to

Zde je možno specifikovat uživatele, kterému budou doručovány maily nevyhovující žádnému z definovaných pravidel. DOPORUČUJE SE zde nějakého uživatele nastavit – v opačném případě budou takové maily zahozeny.

Add, Edit a Remove

Těmito tlačítky lze přidat, změnit a odebrat třídicí pravidlo. Dialog pro přidání nebo změnu umožňuje pouze nastavit položky „Header Content“ a „Deliver To“.

Plánování přijímání a odesílání pošty

Plánování umožňuje následující volby:

- nastavení pravidelných intervalů, kdy má být pošta přijímána a odesílána
- nastavení pravidel pro odchozí e-maily
- omezení časové platnosti těchto pravidel na určitou část dne a/nebo dny v týdnu (lze použít předdefinované časové intervaly – viz kap. Nástroje / Časové intervaly).

Definice plánování se provádí v menu Settings –> Mail Server, záložka „Scheduling“. V hlavním okně je možno zvolit:

Start mail exchange when mail server has received a new outgoing mail

Každý přijatý mail je ihned odeslán do Internetu. Zároveň jsou vybrány všechny schránky definované v „Remote POP3“ (přijetí a odeslání pošty je ve WinRoute jednorázová operace).

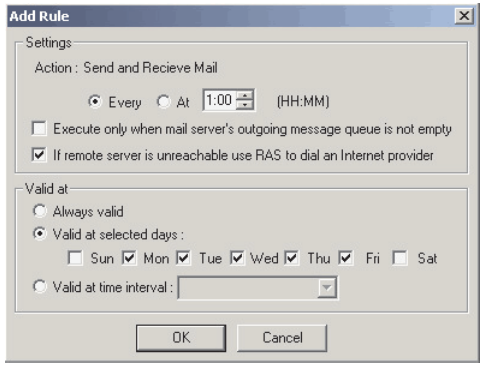
If remote server is unreachable use RAS to dial an Internet provider

Máte-li vytáčenou linku, pak tato volba povoluje mail serveru pro účely odeslání mailu vytočit, je-li právě zavěšeno. Bez této volby budou maily odcházet okamžitě pouze v době, kdy je linka vytočena (jinak se budou řadit do odchozí fronty, tj. do adresáře „mail\spool“). Jako upřesnění je možno zvolit, zda se má vytáčet pro každý mail („for any e-mail“) nebo jen pro mail s příznakem „Urgentní“ („for high priority (urgent) e-mail“).

V případě pevného připojení do Internetu nemá tato volba žádný účinek (nemáte-li v Interface Table ani jednu RAS linku, není volba přístupná).

Plánování časů odeslání a přijetí pošty

V poli „Scheduled mail exchange“ je možno definovat časy, kdy má být pošta odesílána a přijímána. Tlačítkem „Add“ přidáte nové plánování:



Every / At

Tato volba určuje, zda se jedná o interval („Every“ = každých, např. každou hodinu) nebo v určitém čase („At“ = v, např. ve 12:00 hodin).

Execute only when mail server‘s outgoing mail queue is not empty

Spustí akci (tj. odeslání a přijetí mailů) pouze v případě, že fronta odchozích mailů není prázdná.

➢ POZOR: NEDOPORUČUJE se používat tuto volbu, je-li v záložce „Scheduling“ nastavena volba „Start mail exchange when mail server has received new outgoing mail“. V tomto případě se maily odesílají ihned a fronta zůstává prázdná. Plánovaná akce by se tedy nikdy neprovedla.

If remote server is unreachable use RAS to dial an Internet provider

Určuje, zda má mail server právo pro tuto akci (v tomto naplánovaném čase) vytáčet linku, je-li právě zavěšeno. Není-li tato volba zapnuta, provede se akce pouze tehdy, pokud je linka právě vytočena.

➢ POZOR: Nezaměňujte tuto volbu se stejnojmennou volbou v záložce „Scheduling“. Tato volba se vztahuje k definovanému času, zatímco volba v záložce „Scheduling“ pouze k bezprostřednímu odeslání mailu!

Valid at

Omezuje časovou platnost definovaného pravidla. Možnosti jsou:

- „Always valid“ – platí vždy
- „Valid at selected days“ – platí jen v označených dnech.
- „Valid at time interval“ – platí ve zvoleném časovém intervalu (viz kap. Nástroje / Časové intervaly). Časový interval vám umožní omezit platnost pravidla zcela libovolným způsobem.

Optimální nastavení plánování

Ideální plánování příjmu a odesílání pošty závisí na mnoha okolnostech, zejména pak na typu linky a na požadavcích uživatelů. Máte-li pevnou linku, mohou být všechny maily odesílány okamžitě. V případě vytáčené linky je třeba řešit dilema mezi intervalem přijímání/odesílání pošty a cenou za připojení.

➢ POZOR: Máte-li pevnou linku a zároveň vybíráte nějaké POP3 schránky, je třeba TAKÉ nastavit časy, kdy se mají tyto schránky vybírat! Jinak by totiž byly schránky vybírány pouze v momentě, kdy nějaký uživatel odešle mail do Internetu. Nedoporučuje se však nastavovat vybírání schránek častěji než v intervalu 5–10 min (v závislosti na rychlosti linky). Jinak by totiž mohla nastat situace, že WinRoute nestihne stáhnout všechny maily a akce se již vyvolá znovu, čímž dojde k zahlcení.

Příklad nastavení plánování pro vytáčenou linku

Na ukázku uvádíme jeden příklad, jak lze optimalizovat cenu za připojení a aktuálnost přijatých a odeslaných mailů:

- Jestliže bude vytočeno, bude každý odchozí mail ihned odeslán, jinak se zařadí do fronty. V záložce „Scheduling“ zaškrtneme volbu „Start mail exchange when mail server has received new outgoing mail“ a nezaškrtneme volbu „If remote server is unreachable use RAS to dial an Internet provider“.
- Bude-li vytočeno, budou se pravidelně vybírat POP3 schránky po 15 minutách. Tlačítkem „Add“ přidáme plánování: „Every 00:15“, nezaškrtneme ani jednu z voleb, v sekci „Valid at“ ponecháme „Always valid“.
- Nebude-li vytočeno, pak se jednou za hodinu vytočí, odešlou maily z fronty a přijmou nové maily z POP3 schránek. Tlačítkem „Add“ přidáme druhé plánování: „Every 01:00“ a zaškrtneme volbu „If remote server is unreachable use RAS to dial an Internet provider“. Platnost tohoto plánování můžeme ještě omezit časovým intervalem např. pouze na pracovní dobu.

Antispamová ochrana mail serveru

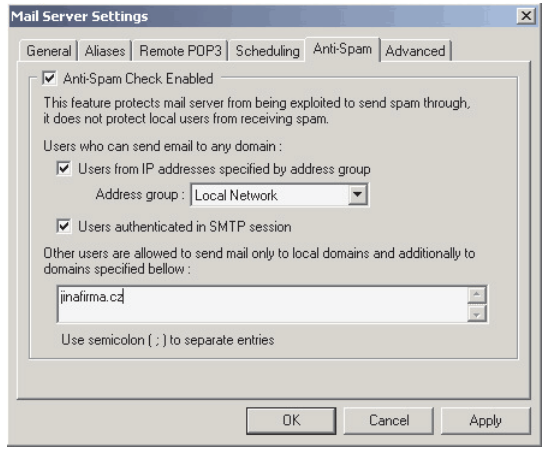
Je-li váš SMTP server zpřístupněn do Internetu (mapováním portu 25), může se na něj stejně jako z lokální sítě připojit také klient zvenčí a použít jej k odeslání pošty. Toho často zneužívají jednotlivci nebo firmy k rozesílání nevyžádaných, většinou reklamních mailů (tzv. spamů). V hlavičce takového mailu je pak vidět, že byl odeslán z vašeho mail serveru. Adresát se tedy bude domnívat, že nevyžádané maily jsou posílány z vaší domény, a v nejlepším případě se zhorší jeho mínění o vaší firmě.

Aby k těmto situacím nedocházelo, umožňuje mail server ve WinRoute kontrolovat odesílatele mailu, a to dvěma způsoby:

- kontrola IP adresy odesílatele
- ověření odesílatele jménem a heslem

Je-li splněna alespoň jedna z těchto podmínek (případně obě), může odesílatel přes tento SMTP server odeslat mail do libovolné domény. V opačném případě smí uživatel odesílat mail pouze do lokálních domén.

Nastavení antispamové ochrany se provádí volbou Settings –> Mail Server, záložka „Anti-Spam“.



Anti-Spam Check Enabled

Zapnutí / vypnutí antispamové ochrany.

➢ POZOR: Častou chybou správců WinRoute je, že zapnou pouze tuto volbu a další parametry již nenastaví. Pak lze ale odkudkoliv (tedy i z lokální) sítě poslat mail pouze do lokální domény! Je třeba řádně nastavit i ostatní volby.

Users from IP addresses specified by address group

Zde je možno specifikovat skupinu IP adres (typicky např. lokální síť), odkud je možno posílat mail do libovolné domény. Podrobnosti o skupinách adres naleznete v kap. Nástroje / Skupiny IP adres.

Users authenticated in SMTP session

Tato volba umožňuje odeslání mailu do libovolné domény uživatelům, kteří se na SMTP serveru ověří jménem a heslem. To je možno nastavit ve většině běžných e-mailových klientů – např. v programu Microsoft Outlook volbou „My server requires authentication“ – „Server odchozí pošty vyžaduje ověření“.

...domains specified below

Ostatní uživatelé mohou posílat mail pouze do lokálních domén. Pokud SMTP server ve WinRoute obsluhuje nějakou doménu, která nemůže být definována jako lokální (viz kap. Příjem pošty protokolem SMTP a Aliasy), je možno ji specifikovat v tomto poli. Jinak by do této domény nebylo možno zvenčí posílat maily.

Nastavení e-mailových klientů

V e-mailových klientech provozovaných ve vaší lokální síti stačí jednoduše nastavit (vnitřní) IP adresu nebo DNS jméno počítače s WinRoute jako server příchozí (POP3) a odchozí (SMTP) pošty. Pro přístup k POP3 schránce použijete jméno uživatelského účtu ve WinRoute a příslušné heslo.

Klient se připojuje k mail serveru ve WinRoute lokální sítí. Obecně platí několik základních pravidel:

- Vnitřní adresa počítače s WinRoute (resp. jeho DNS jméno) je adresou SMTP i POP3 serveru.
- V klientovi nenastavuje žádný proxy server
- Nenastavujte žádné vytáčení připojení, a to ani v klientovi na počítači s WinRoute. Vytáčení připojení je čistě záležitostí WinRoute!

Většina e-mailových klientů umožňuje definovat současně více e-mailových účtů. Nic nebrání tomu, abyste např. používali mail server ve WinRoute a současně vybírali privátní POP3 schránku v Internetu. Zpravidla je však výhodnější, aby takové schránky vybíral WinRoute a doručoval poštu do lokální schránky (viz kap. Vybírání vzdálených POP3 schránek).

➢ Poznámka: Volba „Odeslat / Přijmout“ v klientovi vybírá pouze lokální POP3 schránku ve WinRoute. Touto volbou NENÍ MOŽNÉ vyvolat přijetí mailů ze schránek definovaných v „Remote POP3“. To se provádí pouze v plánovaných intervalech nebo při odeslání mailu do Internetu (v závislosti na nastavení plánování).

Proxy server

Základní informace

Nejdůležitější informace: s WinRoute NEPOTŘEBUJETE proxy server pro přístup do Internetu. Technologie NAT vám umožňuje přístup do Internetu téměř stejně, jako byste do něj byli připojeni přímo – přes směrovač

(viz kap. NAT směrovač). NAT nabízí nesrovnatelně širší možnosti než technologie proxy.

Přesto je ve WinRoute obsažen také klasický proxy server. Jeho hlavním účelem je snížit zatížení vaší internetové linky. Přistupujete-li do Internetu přes proxy server, ukládají se stahované objekty (HTML stránky, obrázky a další typy souborů) do jeho cache.

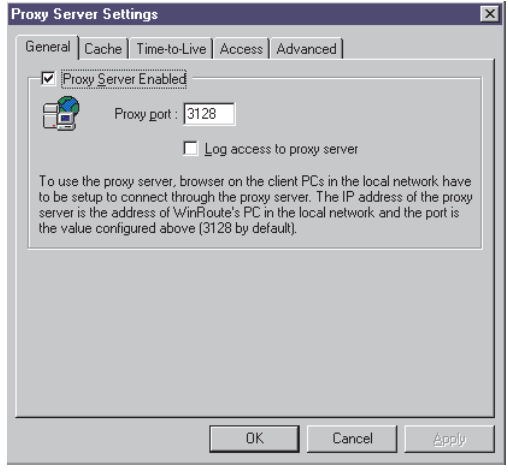
Jsou-li objekty stahovány opakovaně (ať už tímtéž uživatelem nebo kýmkoliv jiným), proxy server vezme tyto objekty ze své cache. Objekty tak nemusejí být znovu stahovány z Internetu, čímž se sníží zatížení internetového připojení.

Objekty v cache mají omezenou životnost. V proxy serveru můžete nastavit standardní dobu uchovávání objektů jednotlivých typů, tak i definovat výjimky pro určité specifické stránky (abyste si např. na Internetu nečetli včerejší noviny).

Nastavení proxy serveru

Abyste mohli používat pro přístup do Internetu proxy server ve WinRoute, proveďte následující:

- V programu WinRoute Administration zvolte menu Settings –> Proxy Server. V záložce „General“ zaškrtněte volbu „Proxy Server Enabled“. Je-li to možné, ponechte výchozí port 3128. Chcete-li provozovat proxy server na jiném portu, přesvědčete se, že na tomto portu neběží žádná jiná aplikace!



- V klientovi (typicky WWW prohlížeči) zvolte ruční konfiguraci proxy serveru. Je-li to možné, vyberte volbu „použít stejný proxy pro všechny

protokoly“ („Use the same proxy for all protocols“), jinak vyplňte tytéž údaje pro protokoly HTTP, FTP a Gopher. Zadejte IP adresu vnitřního rozhraní počítače s WinRoute (např. 192.168.1.1) a port nastavený v záložce „General“ (typicky 3128).

- Vyzkoušejte nastavení otevřením nějaké WWW stránky.

➢ Poznámka: Chcete-li provozovat FTP přes proxy server ve WinRoute, je možné soubory ze serveru pouze stahovat (download), nelze je na server nahrávat (upload). Doporučuje se NEPOUŽÍVAT FTP přes proxy!

➢ Poznámka 2: Proxy server ve WinRoute NEPODPORUJE protokol SOCKS. Protože ale WinRoute umožňuje přístup do Internetu pomocí NAT a mapování portů, protokol SOCKS nepotřebujete. Aplikaci nastavíte tak, aby NEPOUŽÍVALA proxy server, a port, na němž běží, zpřístupníte mapováním. Konkrétní příklady naleznete v kap. Speciální nastavení a příklady.

Proxy Server Enabled

Tato volba zapíná / vypíná proxy server na definovaném portu.

Proxy port

Zde je možno nastavit port, na němž proxy server poběží. Výchozí hodnota je 3128, dále se často používají porty 80 a 8080. Je-li to možné, ponechte výchozí port 3128. Chcete-li číslo portu změnit, ujistěte se, že na tomto počítači na vámi vybraném portu neběží žádná jiná aplikace.

Log access to proxy server

Zapnutím této volby se budou veškeré požadavky klientů na proxy server zaznamenávat do okna HTTP Log a souboru „http.log“.

Řízení přístupu uživatelů na proxy server

Proxy server ve WinRoute umožňuje administrátorovi omezovat přístup uživatelů na konkrétní WWW stránky (resp. na konkrétní URL). K vybraným stránkám je možno přiřadit uživatele (popř. skupiny), kteří budou mít na tyto stránky přístup. Ostatním uživatelům bude přístup zamezen.

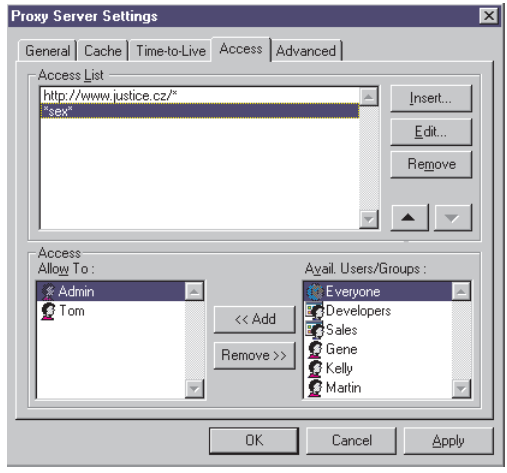
Povolení přístupu na WWW pouze přes proxy server

Chcete-li omezovat přístup na určité stránky v proxy serveru, je vhodné zakázat přímý přístup na WWW (tj. přes NAT). Jinak by se totiž mohlo stát, že si některý zdatnější uživatel vypne nastavení proxy serveru a získá tak neomezený přístup ke všem stránkám.

Omezení přístupu provedete nastavením paketového filtru zakazující všechny pakety jdoucí z lokální sítě na cílový port 80. Detaily naleznete v kap. Firewall / Paketový filtr.

Nastavení omezení přístupu v proxy serveru

Zvolte menu Settings –> Proxy server, záložku „Access“.



Access List

Seznam URL, na něž má být omezen přístup. URL je možno zadat v následujících tvarech:

- kompletní URL (např. „http://www.justice.cz/index.html“)
- URL začínající daným řetězcem (např. „http://www.justice.cz/*“)
- URL končící daným řetězcem (např. „*.cz“)
- podřetězec URL (např. „*sex*“)
- libovolná adresa („*“)

➢ Poznámka: WinRoute Pro 4.1 považuje údaj v poli „Access List“ za PODŘETĚZEC skutečného URL. Hvězdičkovou konvenci pak není třeba vůbec používat (výraz „sex“ je ekvivalentní výrazu „*sex*“). Je ale třeba si uvědomit, že např. výraz „.sk“ pokryje nejen všechny slovenské stránky, ale také např. adresu „http://www.skola.cz“.

Seznam URL je vždy procházen shora dolů a použije se první odpovídající záznam. Z toho vyplývá, že URL musí být v seznamu seřazeny od nejspecifičtějšího (např. konkrétní adresa) k nejobecnějšímu (např. „*“). Tlačítky se šipkami (v pravé části dialogového okna) je možno pořadí URL v seznamu upravit dle potřeby.

Allow To

Seznam uživatelů (příp. skupin), kteří mají na OZNAČENÝ URL povolen přístup (nastavuje se pro každý URL zvlášť). Tyto uživatele lze přidat / odebrat tlačítky „<< Add“ a „Remove >>“.

Avail. Users/Groups

Seznam uživatelů a skupin definovaných ve WinRoute. Tlačítkem „<< Add“ se uživatel (skupina) z tohoto seznamu „přesune“ do pole „Allow To“, tlačítkem „Remove >>“ nazpět.

Pokusí-li se uživatel otevřít některou stránku z výčtu „Access List“, bude prohlížečem vyzván, aby zadal své uživatelské jméno a heslo (rozumí se jméno a heslo k uživatelskému účtu ve WinRoute). WinRoute ověří, zda je jméno a heslo správné a zda má tento uživatel přístup na konkrétní stránku. Pokud ano, stránka se zobrazí; v opačném případě se objeví zpráva, že uživatel nemá právo přístupu na tuto schránku (záleží na typu prohlížeče, zda zobrazí chybovou stránku proxy serveru nebo vlastní chybové hlášení).

Zadané jméno a heslo si prohlížeč uloží do paměti, aby nebylo nutno při každém dalším přístupu na stránku zadávat heslo znovu. Z bezpečnostních důvodů je ale heslo zapamatováno pouze do uzavření prohlížeče – po jeho novém spuštění je třeba zadat heslo znovu.

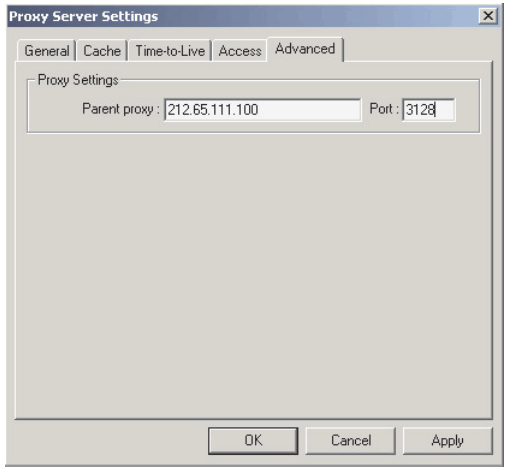
Přistupuje-li uživatel na stránky, které nejsou uvedeny v Access Listu, případně na stránky, na něž je povolen přístup speciální skupině „Everyone“ (= všichni uživatelé), není zadání jména a hesla vyžadováno.

V některých případech mají poskytovatelé Internetového připojení svůj proxy server, který musí jejich zákazníci pro přístup do Internetu používat – přímý přístup do Internetu není možný (např. satelitní systém DVB). Proxy server ve WinRoute je možno nastavit tak, aby používal tento proxy server jako svůj nadřazený (tzv. parent proxy server). I v tomto případě tedy WinRoute umožní sdílení internetového připojení pro celou lokální síť.

Nastavení nadřazeného proxy serveru

Z menu zvolte Settings –> Proxy Server a vyberte záložku „Advanced“. Zde zadejte IP adresu a port nadřazeného proxy serveru (tyto informace získáte od poskytovatele internetového připojení). Proxy server ve WinRoute tak nebude komunikovat přímo s cílovými servery, ale bude pouze předávat požadavky nadřazenému proxy serveru.

➢ Poznámka: Nadřazený proxy server je nutno zadat IP adresou, NIKOLIV DNS jménem! DNS totiž nemusí být v takovém případě vůbec k dispozici.

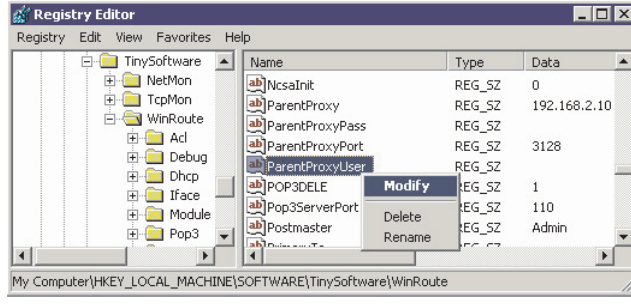


➢ Poznámka 2: Chcete-li nastavení nadřazeného proxy serveru zrušit (tj. aby se již nadřazený server nepoužíval), je třeba důsledně vymazat pole „Parent proxy“ (pozor, nesmí zde zůstat ani znak „mezera“ nebo „tabulátor“). Pole „Port“ naopak smazáno být nesmí (je kontrolováno na číslo v rozsahu 1–65535).

Ověřování uživatele nadřazeným proxy serverem

Vyžaduje-li nadřazený proxy server ověření uživatele jménem a heslem, postupujte následovně:

- Ověřte si, zda máte WinRoute Pro 4.1 Build 21 nebo novější (lze zjistit v menu Help –> About application...). Pokud ne, upgradujte na novější verzi (podrobnosti viz kap. Instalace). Starší verze ověření na nadřazeném proxy serveru nepodporují.
- Zastavte WinRoute Engine a spusťte Editor registru (regedit.exe). Přepněte se do větve „HKEY_LOCAL_MACHINE\Software\TinySoftware\WinRoute“. V pravé polovině okna Editoru registru vyhledejte položky „ParentProxyUser“ a „ParentProxyPass“ a do nich zadejte správné jméno a heslo.



- Ukončete Editor registru a spusťte WinRoute Engine.

➢ Poznámka: Vyžaduje-li nadřazený proxy server ověření uživatele, lze to provést POUZE tímto způsobem. NENÍ MOŽNÉ provést autorizaci z koncového klienta (WWW prohlížeče). Tam se sice objeví okno pro zadání uživatelského jména a hesla, ale proxy server ve WinRoute NEMŮŽE tyto údaje na nadřazený server přenést.

Proxy cache

Cache proxy serveru ve WinRoute používá velmi ekonomický způsob ukládání dat. Všechny objekty jsou ukládány do JEDNOHO SOUBORU PEVNÉ DÉLKY. Většina ostatních proxy serverů naopak ukládá každý objekt do samostatného souboru. Používá-li však souborový systém velké alokační jednotky (jako např. FAT16), představuje tato metoda ZNAČNÉ PLÝTVÁNÍ diskovým prostorem, protože většina komponent WWW stránek jsou velmi malé soubory (statisticky bylo zjištěno, že přes 50% těchto souborů je menších než 6kB), zatímco alokační jednotka na disku se systémem FAT16 má velikost až 32 kB (v závislosti na velikosti disku).

Díky tomu, že WinRoute používá ukládání dat do jednoho velkého souboru, se ušetří okolo 90% diskového prostoru. Proxy server ve WinRoute tedy potřebuje přibližně desetinásobně menší prostor než klasický proxy server. Získané místo je vám k dispozici pro vaše programy a data.

Ukládání do jednoho souboru je také rychlejší než ukládání jednotlivých souborů. WinRoute navíc používá speciální techniku indexování v tomto souboru, takže cache proxy serveru je také mimořádně rychlá.

Nastavení cache

Nastavení vlastností proxy cache se provádí v menu Settings –> Proxy Server, záložka „Cache“. Následující volby umožní výkon cache ještě dále optimalizovat.

Cache Enabled

Zapnutí / vypnutí používání cache. Je-li cache vypnuta, proxy server musí vždy všechny objekty stahovat přímo z cílového serveru.

Cache Directory

Adresář, kde bude cache uložena. Může jej být vhodné změnit např. v případě, že máte na jiné diskové jednotce více volného místa. Tlačítkem „Browse“ lze vyhledat, příp. vytvořit požadovaný adresář.

Cache size

Velikost souboru cache na disku (v MB). Při rozhodování o velikosti doporučujeme vzít v úvahu počet uživatelů a objem dat, který z Internetu stahují. Máte-li dostatek místa na disku, vytvořte cache co největší. Maximální velikost je 2 GB (2048 MB).

Memory cache size

Velikost cache v paměti. Tato část cache je velmi rychlá a ukládají se do ní nejčastěji přistupované objekty. Volba její velikosti závisí především na velikosti operační paměti, kterou má počítač s WinRoute k dispozici. Nezapomeňte, že zabrání velké části operační paměti může značně snížit výkonnost systému! Nenastavujte proto paměťovou cache na více než 10% operační paměti!

Continue Aborted

Je-li tato volba zaškrtnutá, pak bude proxy server automaticky „dotahovat" objekty, jejichž stahování bylo uživatelem přerušeno (stiskem tlačítka „Stop" v prohlížeči). Ve velkém počtu případů totiž uživatel přerušuje otevírání stránky právě z toho důvodu, že se natahuje příliš pomalu. Rozhodne-li se uživatel navštívit stránku znovu (případně ji navštíví jiný uživatel), bude stránka k dispozici nesrovnatelně rychleji.

Keep Aborted

Říká proxy serveru, aby ponechal v cache i nekompletní objekty (jejichž stahování bylo přerušeno). To způsobí částečné urychlení natahování při opakované návštěvě stránky. Je-li nastavena volba „Continue Aborted", je tato volba ignorována.

Cache FTP directory only

Tato volba znamená, že má proxy server ukládat do cache pouze adresář FTP serveru (stahování z FTP je zpravidla jednorázová záležitost a soubory mohou být veliké, zabíraly by v cache zbytečně místo). Chcete-li přesto ukládat do cache i soubory stahované protokolem FTP, vypněte tuto volbu. Maximální velikost uloženého souboru lze nastavit v sekci „Max. Object Size" (viz dále).

Use server supplied Time-to-Live

Time-to-Live (TTL, doba života) je doba, po které je stránka považována za neplatnou a musí být znovu stažena ze serveru. Tato volba říká proxy serveru ve WinRoute, aby akceptoval TTL nastavenou na jednotlivých stránkách (nemá-li stránka TTL nastavenu, použije se výchozí hodnota – viz následující kapitola).

Ignore server Cache-Control directive

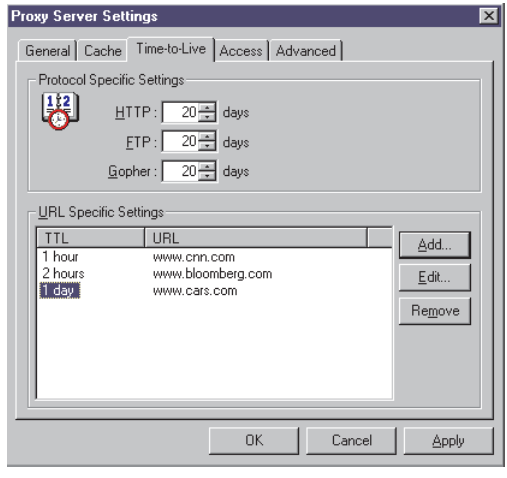
Jestliže se obsah nějaké stránky velmi často mění, její autor na ni zpravidla umístí tzv. direktivu „no-cache“ – tedy instrukci, aby se stránka neukládala do cache. To může být užitečné, ale v některých případech je tato direktiva používána nerozumně, např. na všech stránkách na WWW serveru, někdy i za účelem „vyřazení proxy serveru z cesty“. Volba „Ignore server Cache-Control Directive“ vás může ochránit před takovýmito stránkami.

Max. Object Size

Zde je možno nastavit maximální velikost objektů (souborů), které se mají ukládat do cache. Různé velikosti lze nastavit pouze pro protokoly, kterými jsou objekty stahovány, nikoliv pro jednotlivé typy souborů. Větší objekty jsou pouze staženy a poslány klientovi, ale nejsou uloženy do cache.
V cache zpravidla není třeba uchovávat velké soubory (např. archivy), protože je nestahujete opakovaně.

Životnost objektů v cache (Time-to-Live)

V menu Settings –> Proxy Server, záložka „Time-to-Live“, je možno nastavit výchozí doby, po které budou objekty stažené jednotlivými protokoly uchovávány v cache, a výjimky pro konkrétní stránky.



Protocol Specific Settings

Zde jsou nastaveny výchozí hodnoty uchování objektů v cache, v závislosti na tom, kterým protokolem byly staženy. Optimální hodnoty je nejvhodnější určit experimentálně.

➢ Poznámka: Informace o aktuálním stavu zaplnění cache lze získat v okně Debug Log stiskem pravého tlačítka myši a volbou Show –> Cache statistics.

Tyto hodnoty se uplatní vždy u WWW stránek, kde není TTL definována, a v případě vypnutí volby „Use server supplied Time-to-Live" i u všech ostatních stránek.

URL Specific Settings

Zde je možno definovat výjimky pro konkrétní stránky. Tlačítkem „Add" přidejte URL stránky, pro niž chcete nastavit specifickou dobu životnosti. WinRoute považuje výraz zadaný jako „URL" za podřetězec skutečného URL, čím je možno pokrýt i větší množinu stránek.

Nastavení doby „0 dní – 0 hodin" znamená, že stránka nemá být do cache vůbec ukládána (ve sloupci „TTL" se objeví „no cache"). Tlačítky „Edit" a „Remove" lze nastavení pro vybranou stránku změnit či smazat.

➢ Poznámka: Je-li zapnuta volba „Use server supplied Time-to-Live" (záložka „Cache"), má hodnota TTL definovaná na stránce VYŠŠÍ PRIORITU než „URL Specific Settings". Chcete-li tedy nastavovat vlastní doby uchovávání v cache, je vhodné tuto volbu vypnout.

Proxy versus NAT

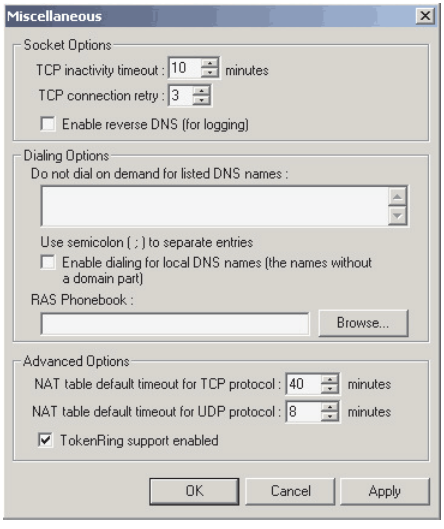
Přestože na mnoha místech tohoto manuálu již bylo řečeno, že technologie NAT vám dává nesrovnatelně větší možnosti než přístup přes proxy serveru, existuje v případě služby WWW několik argumentů hovořících ve prospěch proxy serveru (pro ostatní služby a aplikace je jednoznačně doporučeno použití „přímého" přístupu přes NAT).

- Access List umožňuje omezit přístup na konkrétní stránky, zadané přímo URL, a to na základě uživatelského jména a hesla. Paketový filtr naproti tomu umožňuje pouze filtrování paketů podle zdrojových a cílových adres. Je tedy nutno zjišťovat IP adresy příslušných WWW serverů a nelze ošetřit situaci, kdy se u téhož počítače střídá několik uživatelů.
- Cache umožňuje snížit zatížení vaší internetové linky a urychlit otevírání opakovaně navštěvovaných stránek.
- Proxy server může spolupracovat s nadřazeným proxy serverem a umožnit tak sdílení i takového připojení, kde je přístup do Internetu možný pouze přes proxy server poskytovatele.

Další nastavení

Miscellaneous Options

Dialogové okno Miscellaneous Options (menu Settings / Advanced / Misc. Options) umožňuje provést různá další upřesňující nastavení.



Socket Options

- TCP inactivity timeout – nastavení doby, po jejímž uplynutí bude TCP spojení automaticky ukončeno, jestliže jím nejsou přenášena žádná data.
- TCP connection retry – počet pokusů o opakované navázání TCP spojení v případě neúspěchu.

Tyto parametry jsou za normálních okolností záležitostí TCP klienta – v případě použití funkce NAT však WinRoute přebírá jeho roli. Ve většině případů ale není potřeba výchozí hodnoty upravovat.

- Enable reverse DNS (for logging) – je-li tato volba zapnuta, pak se v záznamových oknech (např. HTTP Log nebo Mail Log) převádějí IP adresy počítačů v lokální síti na jejich DNS jména (pokud jsou příslušné údaje v DNS zaneseny). To může být užitečné při vyhodnocování logů, avšak tato volba může znatelně zpomalit činnost WinRoute, na což je po jejím zapnutí uživatel upozorněn varovným hlášením.

Dialing Options

Volby pro vytáčení.

- Do not dial on demand for listed DNS names – nevytáčet pro uvedená DNS jména. Tato volba říká DNS forwarderu, aby při přijetí dotazu na některé z uvedených jmen nevytáčel internetové připojení.
- Enable dialing for local DNS names (the names without a domain part) – povolit vytáčení pro lokální DNS jména (bez doménové části). Tato volba může být využita v případě, že DNS server pro lokální síť je umístěn mimo ni. V ostatních případech se nedoporučuje zapínat tuto volbu.
- RAS phonebook – zde je možno zvolit telefonní seznam telefonického připojení (RAS Phonebook) ve Windows NT/2000. To může být třeba v případě, že bylo připojení vytvořeno jiným uživatelem, než který provedl instalaci WinRoute. Pak se připojení v nastavení RAS linky nezobrazí, není-li zde vybrán telefonní seznam příslušného uživatele.

Advanced Options

- NAT table default timeout for TCP (UDP) protocol – čas vypršení záznamu v NAT tabulce pro TCP a UDP pakety. Za normálních okolností je záznam z tabulky smazán při ukončení spojení. Je-li však spojení ukončeno nekorektně (např. z důvodu výpadku sítě), ke smazání záznamu nedojde. Takové záznamy jsou pak odstraňovány po uplynutí nastavené doby. Bez existence tohoto mechanismu by brzy došlo k úplnému zaplnění NAT tabulky.
- TokenRing support enabled – podpora TokenRing adaptérů. Je-li ve vašem počítači instalován TokenRing adaptér, ujistěte se, že je tato volba zapnutá. V ostatních případech nemá žádný účinek.

Logy ve WinRoute

Logy jsou nástrojem umožňujícím sledovat, co se děje „uvnitř WinRoute“. Je možno sledovat činnost jednotlivých serverů, aktivitu uživatelů (nikoliv ovšem objem přenesených dat nebo čas strávený na Internetu. K tomuto účelu doporučujeme produkt TINY Network Monitor – viz http://www.tinysoftware.cz „http://www.tinysoftware.cz“.

Jednotlivé logy je možno otevřít v menu View –> Logs –> <název logu>. Lze vybrat z následujících:

- Debug Log – základní log, v němž se zobrazují nejpodrobnější informace. Správce WinRoute má možnost detailně nastavit, které informace chce zobrazovat (např. za účelem odhalení chyby).
- Error Log – zobrazuje závažná chybová hlášení. Výpis do tohoto logu nelze nijak ovlivnit.
- HTTP Log – požadavky klientů na proxy server

- Mail Log – základní informace o přijatých a odeslaných mailech
- Security Log – informace týkající se firewallu a NAT (např. filtrované pakety, pokusy o útok apod.)
- Dial Log – informace o vytáčení a zavěšování RAS linek

Error, HTTP, Mail, Security a Dial log jsou po určité době ukládány do souborů. Tyto soubory jsou uloženy v podadresáři „logs“ adresáře, kde je WinRoute instalován (např. „\Program Files\WinRoute Pro\logs“) a jsou nazvány „error.log“, „http.log“ atd. Nové informace se vždy zapisují do příslušného okna a po určité době je obsah okna přepsán do souboru. V souborech lze vyhledávat volbou View –> Logs –> Logs History.

Výjimku tvoří Debug Log, který se do souboru neukládá a je tedy k dispozici pouze po dobu, kdy běží WinRoute Engine. Dále záleží na množství vypisovaných informací – v případě nedostatku paměti se nejstarší informace odmazávají.

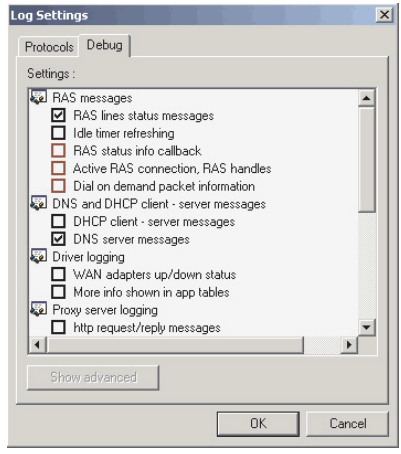
Uložení a smazání výpisu

V každém logu je možno stiskem pravého tlačítka myši vyvolat kontextové menu umožňující tyto volby:

- Save Screen – uložení obrazovky do souboru ve formátu HTML. POZOR: je uložena pouze aktuálně viditelná část logu. Svislou posuvnou lištou okna nastavte takovou pozici, abyste uložili požadované informace.
- Clear – vymazání CELÉHO obsahu logového okna.

Debug Log

Debug Log je nejdůležitějším logem ve WinRoute. Umožňuje detailní sledování velkého množství nejrůznějších informací. Ve většině případů ale potřebujete sledovat pouze určitý typ informace (např. DNS dotazy nebo stav vytáčení RAS linky). Proto je možné v Debug Logu poměrně detailně nastavit, jaký typ informace se má zobrazovat. To lze nastavit v menu Settings –> Advanced –> Debug Info nebo přímo v okně Debug Log – stiskem pravého tlačítka myši v okně vyvolejte kontextové menu a zvolte Log Settings.



- V záložce „Protocols“ lze zapnout sledování paketů jednotlivých protokolů (ARP, ICMP, TCP, UDP a DNS). Za běžného provozu však přes počítač s WinRoute prochází velmi mnoho paketů a zobrazované informace zpravidla ani nelze sledovat. Nedoporučuje se zapínat sledování více než jednoho protokolu současně.
- V záložce „Debug“ je možno detailněji specifikovat typ sledované informace. Informace jsou rozděleny do dvou úrovní: hlubší úroveň se zobrazí po stisku tlačítka „Show Advanced“ (detailní popis viz dále).

➢ Poznámka: Doporučuje se zapínat vypisování informací do Debug Logu pouze v případě, že chcete skutečně něco sledovat. Jinak výpisy zbytečně zpomalují činnost WinRoute.

Kromě vybraných informací se v Debug Logu zobrazují ještě některé systémové informace – např. verze WinRoute a spuštěné moduly po startu WinRoute Engine apod.

Nastavení detailních ladicích informací

V záložce Debug dialogu Log Settings je možno velmi detailně nastavit informace, které chcete v okně Debug Log sledovat. V následujícím odstavci jsou popsány všechny možnosti, tedy i ty, které se zobrazí až po stisku tlačítka „Show Advanced“.

RAS Messages – informace o vytáčených linkách

- RAS lines status messages – základní informace o stavu linek (vytočení, zavěšení, přidělená IP adresa atd.)
- Idle timer refreshing – informace o čítači doby nečinnosti (po níž dojde k automatickému zavěšení)

- RAS status info callback – detailní informace o stavu linky (vytáčení, připojení, ověřování...)
- Active RAS connections, RAS handles – detailní informace o jednotlivých spojeních a jejich systémové identifikátory
- Dial on demand packet information – výpis paketů, které způsobily vytočení linky na žádost
  (velmi užitečné např. pro zjištění, proč došlo k vytočení linky)

DNS and DHCP client – server messages

- DHCP client – server messages – detailní informace o komunikaci mezi DHCP klientem a serverem, typy zpráv, přidělené IP adresy atd.
- DNS server messages – detailní výpis DNS dotazů přijatých DNS forwarderem

Driver logging – záznamy nízkoúrovňového ovladače

- WAN adapters up/down status – stav internetového rozhraní detekovaný přímo ovladačem
- More info shown in app tables – tabulka rozhraní (vypisovaná v TCP/IP info) je rozšířena o hardwarovou adresu a identifikátor ovladače

Proxy server logging

- HTTP request/reply messages – detailní informace o HTTP požadavcích a odpovědích. Odděleně je sledována komunikace klient – proxy server a proxy server – WWW server.
- Cache processing – informace o ukládání, vybírání a mazání objektů do/z cache

Mail

- Mail processing information – velmi detailní informace o odesílání pošty na nadřazený SMTP server a vybírání vzdálených POP3 schránek
- SMTP and POP3 server session info – informace o komunikaci poštovních klientů s mail serverem ve WinRoute
- Alias processing – zpracování aliasů a třídicích pravidel
- Anti-virus check processing – nečinné, rezervováno pro budoucí použití

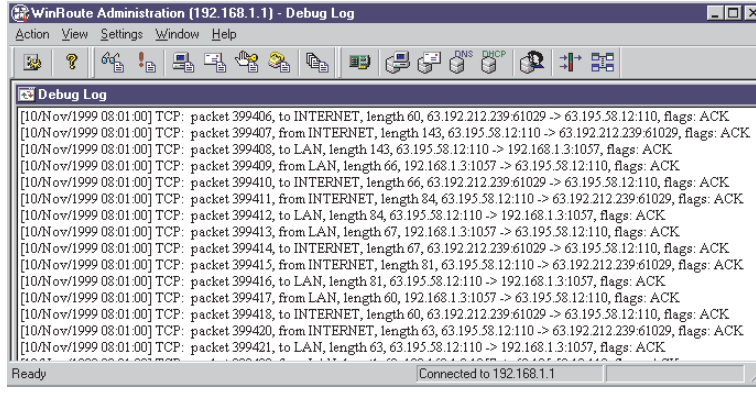
Misc

- Discarded packets – informace o zahozených paketech (mimo pořadí, neplatný kontrolní součet apod.)
- DirecPC info – interface for outgoing packets – informace o směrování paketů při použití rozhraní DirecPC
- Packet probes – informace o hardwarových adresách v paketech apod.
- Temporary messages – nečinné, rezervováno pro ladicí účely

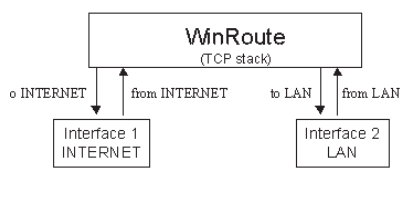
- Connection establishing, remote IP and DNS server check – navazování TCP spojení, kontrola vzdálené IP adresy a DNS serveru
- Time interval processing – zpracování časových intervalů, provádění naplánovaných akcí
- Other IP traffic – informace o jiných protokolech než TCP, UDP a ICMP

Jak číst Debug Log?

Příklad logování TCP paketů – zleva doprava:



- časová značka (v hranatých závorkách) – datum a čas, kdy přesně událost nastala
- protokol
- from / to <rozhraní> – Jméno rozhraní a zda je paket příchozí či odchozí z pohledu rozhraní



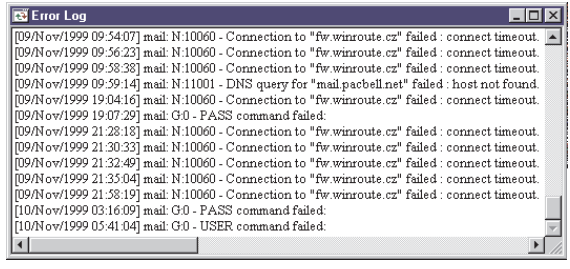
- Zdrojová IP adresa –> cílová IP adresa
- Příznaky (závislé na protokolu)

Error Log

Error Log zobrazuje závažná chybová hlášení všech modulů WinRoute (např. chyby RAS linek, neúspěšné připojení na nadřazený SMTP či DNS server apod.)

Objeví-li se v Error Logu nové hlášení, zobrazí se v pravé části stavového pruhu (View –> Status Bar) zpráva „! Errors detected“. Tato zpráva zmizí v okamžiku otevření okna Error Log (či jeho aktivace). WinRoute podle toho předpokládá, že si správce nová hlášení v Error Logu přečetl.

Příklad (zleva doprava):



- časová značka
- „mail“ – modul, v němž k chybě došlo (v tomto případě mail server)
- „N:10060“ – typ a číslo chyby
- „Connection to „fw.winroute.cz“ failed : connection timeout“ – textový popis chyby (vypršel časový limit při pokusu o navázání spojení se serverem)

HTTP Log

HTTP Log zobrazuje všechny požadavky uživatelů na proxy server. Může být tedy použit zejména ke sledování uživatelských aktivit (kdy a na které stránky přistupovali apod.). Každý požadavek je zobrazen na jednom řádku a tento log je i pro laika poměrně dobře čitelný.

➢ Poznámka: HTTP Log má standardní formát logu proxy serveru a lze na něj aplikovat programy pro vyhodnocování statistik proxy serveru. Některé z těchto produktů jsou dokonce volně šiřitelné (např. Webalizer, ClearRoute). Takto můžete získat ještě přehlednější informace.

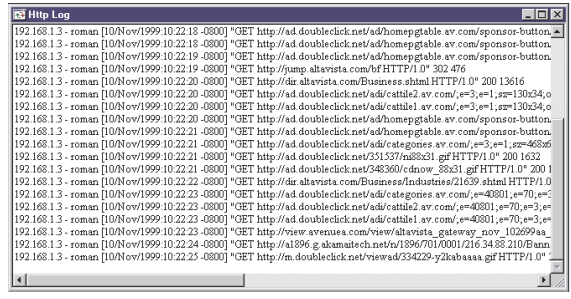
Kdy jsou požadavky klientů zaznamenávány v HTTP Logu?

- HTTP Log zobrazuje pouze požadavky uživatelů na proxy server. Přistupují-li tedy uživatelé do Internetu přímo, požadavky se nezobrazí.

- V nastavení proxy serveru (Settings –> Proxy Server, záložka „General“) je nutno zapnout volbu „Log access to proxy server“. Nezajímá-li vás HTTP Log, doporučujeme tuto volbu vypnout.

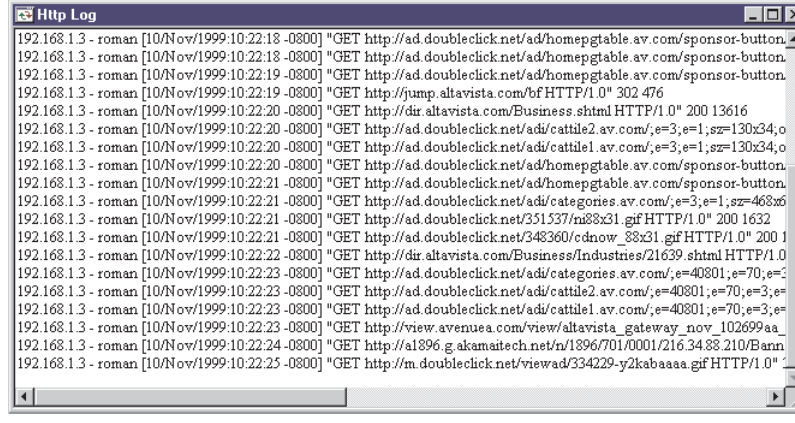
Jak číst HTTP Log?

Příklad (zleva doprava):



- „192.168.1.3 – roman“ – IP adresa a jméno klientského počítače

➢ POZOR: Jméno počítače se zde zobrazí pouze tehdy, zapnete-li v menu Settings –> Advanced –> Misc. Options volbu „Enable reverse DNS (for logging)“. V opačném případě se zobrazí místo jména počítače pomlčka – tedy např.: „192.168.1.3 - -“.

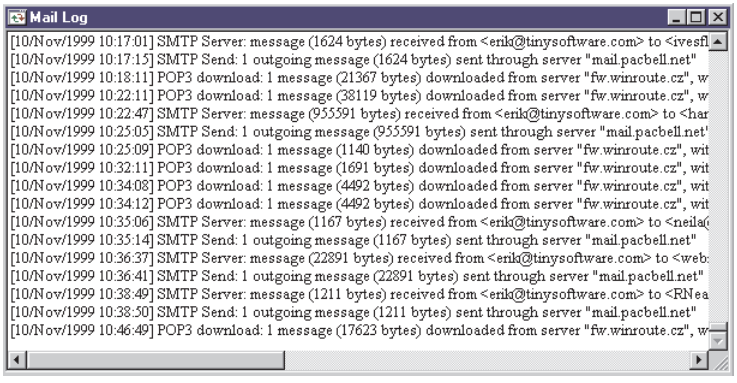


- časová značka (v tomto případě obsahuje i posun vůči GMT/UTC)
- vlastní požadavek (uzavřený v uvozovkách) – obsahuje typ metody (GET nebo POST) a vlastní URL
- návratový kód protokolu HTTP (např.: 200 = v pořádku, 404 = objekt nenalezen atd.)
- velikost objektu v bytech

Mail Log

Mail Log zobrazuje základní informace o operacích prováděných mail serverem ve WinRoute:

- SMTP zprávy přijaté od klientů k odeslání
- odesílání mailů na nadřazený (relay) SMTP server
- vybírání mailů ze vzdálených POP3 schránek
- vybírání lokálních POP3 schránek klienty



Detailnější informace o přijímání a odesílání mailů lze sledovat v okně Debug Log – viz nastavení "Log Settings" v kap. Debug Log.

➢ Poznámka: Informace se v okně Mail Log zobrazují pouze tehdy, je-li v nastavení mail serveru (Settings –> Mail Server, záložka „General“) zapnuta volba „Enable Logging“.

Dial Log

Dial Log zobrazuje informace o vytáčení a zavěšování RAS linek. Ve zprávě o zavěšení je uvedena doba, po kterou byla linka připojena. Tyto záznamy se provádějí automaticky vždy, je-li použita některá RAS linka.

Příklad:

```
[31/Jan/2001 10:12:40] line1 (IBM Global
Network): successfuly connected

[31/Jan/2001 10:14:34] line1 (IBM Global
Network): disconnected, connection time 00:01:54
```

Security Log

Security Log zobrazuje informace týkající se zabezpečení, filtrování paketů atd. V zásadě se vždy jedná o výpis zachyceného paketu, který splňuje či nesplňuje určité podmínky.

Jaké informace mají být do Security Logu zaznamenávány, určují dvě nastavení:

- Settings / Advanced / Security Options, sekce „NAT Logging Options“ – zde lze určit, zda se mají zaznamenávat pokusy o komunikaci na portech chráněných firewallem.
- Settings / Advanced / Packet Filter – v definici každého filtrovacího pravidla lze nastavit, zda má být paket zaznamenán. Pakety se zaznamenávají právě do Security Logu, a to bez ohledu na to, zda jsou povoleny, odmítnuty či zahozeny.

V obou těchto případech je navíc možno zvolit, zda má být paket zaznamenán pouze do okna Security Log (Log into window), pouze do souboru „security.log“ (Log into file), příp. obojí.

Kapitola 6

SPECIÁLNÍ NASTAVENÍ A PŘÍKLADY

Vícesegmentové lokální sítě

Obecné informace

WinRoute je softwarový směrovač umožňující připojení jedné či více lokálních IP subsítí přes jediné internetové připojení (jednu veřejnou IP adresu). Tyto segmenty mohou být i fyzické sítě různých typů – Ethernet, Token Ring atd. WinRoute může obsluhovat libovolný počet rozhraní (pokud je lze do počítače fyzicky nainstalovat), není tedy omezen pouze na situaci jedno rozhraní do Internetu – jedno do lokální sítě.

Funkci NAT (překlad IP adres) přitom není nutné zapínat na žádném rozhraní – WinRoute tedy může být také použit např. jako směrovač mezi dvěma lokálními segmenty. Mějte však na paměti, že pro KAŽDOU instalaci WinRoute je třeba zakoupit samostatnou licenci!

V následujících kapitolách uvádíme několik typických konfigurací a několik složitějších příkladů. Získané informace by vám měly umožnit nastavení téměř libovolné síťové konfigurace.

Připojení kaskádních segmentů přes 1 IP adresu

Kaskádními segmenty je nazývána taková síťová konfigurace, kdy je několik lokálních segmentů propojeno směrovači a do jednoho z nich je připojen počítač s WinRoute. Uvažujme pro názornost 2 kaskádní segmenty, následující úvahy jsou však platné pro libovolný počet segmentů.

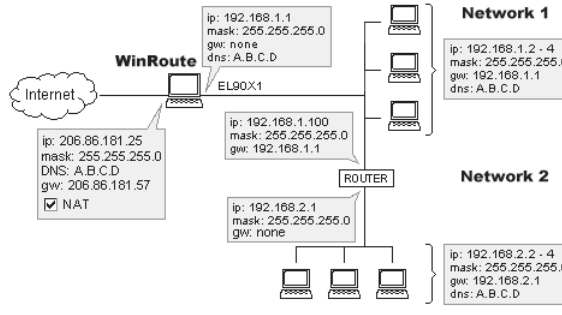
Směrování mezi těmito segmenty může provádět buď hardwarový směrovač (router), počítač s Windows NT nebo počítač s libovolnou verzí Windows a WinRoute. WinRoute zde může provádět buď klasické směrování nebo směrování s překladem IP adres (ano, překlad adres může být prováděn vícekrát za sebou! Můžete tak např. chránit určitý segment vůči zbytku lokální sítě).

Aby fungovalo směrování správně, je třeba jednak nastavit směrovač spojující oba segmenty, aby pakety do Internetu posílal přes WinRoute, a jednak sdělit WinRoute, že pakety pro druhý segment nemá posílat do Internetu, ale přes vnitřní směrovač do tohoto segmentu. V praxi to znamená následující:

- na počítači s WinRoute je nastavit CESTU (tj. přidat záznam do směrovací tabulky) do druhého segmentu přes vnitřní směrovač
- na vnitřním směrovači nastavit jako VÝCHOZÍ BRÁNU (Default Gateway) adresu vnitřního rozhraní počítače s WinRoute – přes něj budou odesílány pakety, jejichž cílová IP adresa nepatří do žádného z lokálních segmentů

Příklad:

Mějme dva lokální segmenty s IP adresami 192.168.1.x a 192.168.2.x (maska subsítě je 255.255.255.0). Vnitřní rozhraní počítače s WinRoute má IP adresu 192.168.1.1, rozhraní interního směrovače mají IP adresy 192.168.1.100 a 192.168.2.1.



Nastavení segmentu 192.168.1.x (primárního)

- Na počítači s WinRoute je třeba nastavit: „Směruj pakety s cílovou adresou 192.168.2.x na bránu 192.168.1.100“ (směrování ostatních paketů je již zajištěno správně).

  Běží-li na tomto počítači systém Windows NT/2000, otevřete Příkazový řádek (Command Prompt) a zadejte příkaz:

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

  V případě systému Windows 95/98/ME vytvořte dávkový soubor (např. „ADDROUTE.BAT“) obsahující následující řádek:

  ```
  route add 192.168.2.0 mask 255.255.255.0 192.168.1.100
  ```

  Do menu Start / Programy / Po spuštění (Start / Programs / Startup) přidejte zástupce (Shortcut) tohoto souboru a restartujte počítač.

- Na interním směrovači musí být nastavena výchozí brána na vnitřní rozhraní počítače s WinRoute – tedy na IP adresu 192.168.1.1. Jedná-li se o softwarový směrovač, jednoduše nastavte tuto výchozí bránu na síťové kartě s adresou 192.168.1.100. V případě hardwarového směrovače postupujte podle pokynů v návodu.
- Všechny ostatní počítače v segmentu 192.168.1.x budou nastaveny tak, jako by existoval pouze tento segment a byl připojen přes WinRoute do Internetu (viz kap. Nastavení WinRoute a lokální sítě). Výchozí brána MUSÍ být nastavena na WinRoute, nikoliv na interní směrovač.

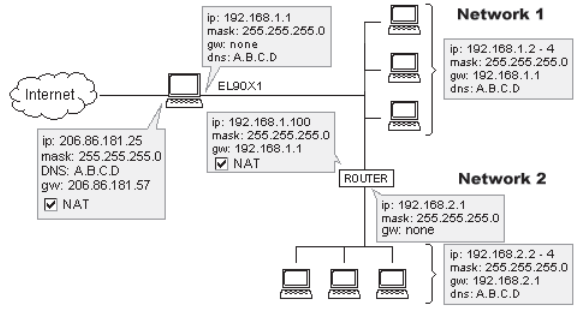
➢ Poznámka: Možná se vám bude zdát podivné, že pakety do segmentu 192.168.2.x jsou posílány nejprve na WinRoute a odtud na interní směrovač a na cílový počítač. Ve skutečnosti je takto směrován pouze první paket vyslaný z daného počítače. Tomu je totiž zároveň poslána řídicí zpráva „ICMP Redirect“, která způsobí změnu v je o směrovací tabulce. To již ale není vaše starost – přesměrování se provádí automaticky.

Nastavení segmentu 192.168.2.x (sekundárního)

Všechna nastavení zůstanou stejná jako před instalací WinRoute. Výchozí brána MUSÍ být nastavena na příslušné rozhraní interního směrovače – tedy 192.168.2.1 v našem příkladě.

NAT mezi interními segmenty

Pro směrování mezi interními segmenty můžete použít WinRoute se zapnutou funkcí NAT (samozřejmě na rozhraní směrem k Internetu, nikoliv do „koncového“ segmentu!). Celý sekundární segment bude z pohledu počítačů v primárním vypadat jako jeden počítač. To umožňuje ochránění tohoto segmentu před uživateli v primárním segmentu. Z „dvojnásobného NAT“ přitom nevyplývají žádná další omezení (oproti „jednoduchému NAT“). Chcete-li však zpřístupnit do Internetu službu běžící na počítači v sekundárním segmentu, je potřeba provést „dvojnásobné“ mapování portů.

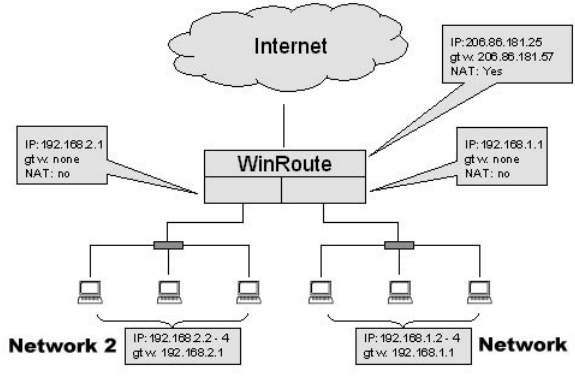


Připojení dvou segmentů přes 1 IP adresu

Máte-li více lokálních segmentů (pro jednoduchost předpokládejme pouze dva, ale následující úvahy platí zcela obecně), přičemž každý segment je připojen na jednu síťovou kartu počítače s WinRoute, NENÍ TŘEBA žádných speciálních nastavení. Počítače v každém lokálním segmentu budou nastaveny tak, jako by byl k WinRoute připojen pouze tento segment (není tedy třeba nastavovat žádné cesty do ostatních segmentů apod.). WinRoute bude provádět směrování paketů mezi každým lokálním segmentem a Internetem, stejně jako mezi lokálními segmenty navzájem.

Příklad:

WinRoute má (kromě rozhraní do Internetu) dvě síťové karty, k nimž jsou připojeny segmenty 192.168.1.x a 192.168.2.x.



Jediná nastavení, která musíte provést jsou následující:

Internetové rozhraní

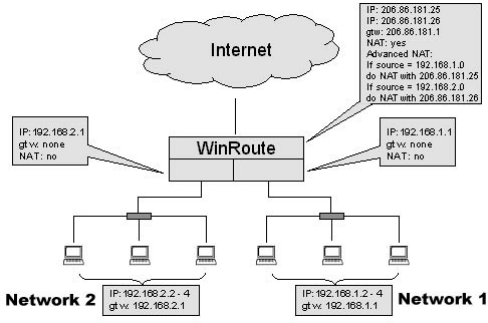
- NAT je ZAPNUT
- IP adresa, výchozí brána a DNS server(y) – podle pokynů poskytovatele připojení (příp. konfigurováno dynamicky)

Vnitřní rozhraní

- NAT NENÍ zapnut
- IP adresa z privátního rozsahu (např. 192.168.1.1 nebo 10.1.1.1)
- NENÍ nastavena výchozí brána na ŽÁDNÉM vnitřním rozhraní

Připojení dvou segmentů přes 2 IP adresy

Dva lokální segmenty mohou sdílet Internetové připojení, přičemž každý segment bude „maskován“ jinou IP adresou. Jinými slovy – je možné simulovat situaci, jako by byl každý segment připojen samostatně přes vlastní veřejnou adresu vlastním WinRoute. Ve skutečnosti lze tuto situaci realizovat přes jediné fyzické připojení a jediný WinRoute. Obě veřejné IP adresy budou přiřazeny vnějšímu rozhraní počítače s WinRoute (je třeba použít operační systém Windows NT/2000).



Co je třeba nastavit

V tomto případě stačí v menu Settings –> Advanced –> NAT definovat, jakou IP adresou se má nahrazovat zdrojová adresa v paketech odcházejících z jednotlivých vnitřních segmentů:

Source: Network/Mask

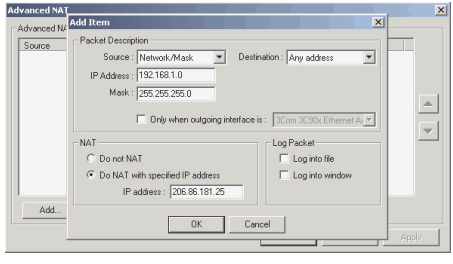
IP Address: IP adresa sítě lokálního segmentu (192.168.1.0 či 192.168.2.0)

Mask: odpovídající subsíťová maska (255.255.255.0)

Destination: Any address

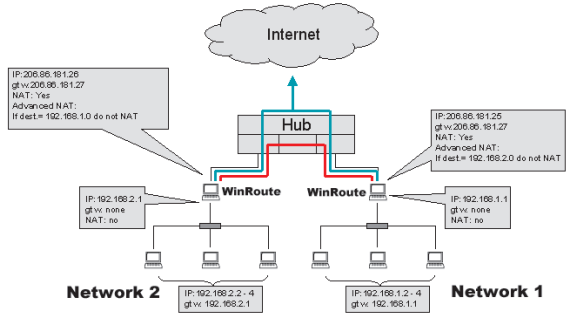
Do NAT with specified IP address

IP Address: příslušná vnější IP adresa



2 segmenty, 2x WinRoute, 1 fyzické připojení

Předpokládejme následující situaci: 2 lokální segmenty jsou odděleně připojeny do Internetu – každý z nich má svou bránu (tj. počítač s WinRoute) a svou vnější IP adresu, oba jsou ale připojeny přes jednu fyzickou internetovou přípojku do téže sítě. Oba WinRoute je pak možno nastavit tak, aby lokální segmenty mohly komunikovat mezi sebou navzájem.



Co je třeba nastavit

- V OBOU WinRoute musí být nastaveno, aby se v paketech jdoucích do druhé lokální sítě neprováděl překlad IP adres. V menu Settings –> Advanced –> NAT je třeba provést nastavení: pro libovolnou zdrojovou adresu a cílovou adresu patřící do druhé lokální sítě neprovádět NAT.

  Source: Any address

  Destination: Network/Mask **IP Address:** IP adresa druhé lokální sítě

  Mask: subsíťová maska v této síti

  Do not NAT

- Na každém počítači s WinRoute musí být do směrovací tabulky přidána cesta do druhé lokální sítě – přes vnější rozhraní druhého WinRoute, tedy např.:

  ```
  route -p add 192.168.2.0 mask 255.255.255.0
  206.86.181.26
  ```

  (na příkazovém řádku ve Windows NT/2000) nebo (v případě systému Windows 95/98/ME) vytvořte dávkový soubor (např. „ADDROUTE.BAT“) obsahující následující řádek:

  ```
  route add 192.168.2.0 mask 255.255.255.0 192.168.1.100
  ```

  Do menu Start / Programy / Po spuštění (Start / Programs / Startup) přidejte zástupce (Shortcut) tohoto souboru a restartujte počítač.

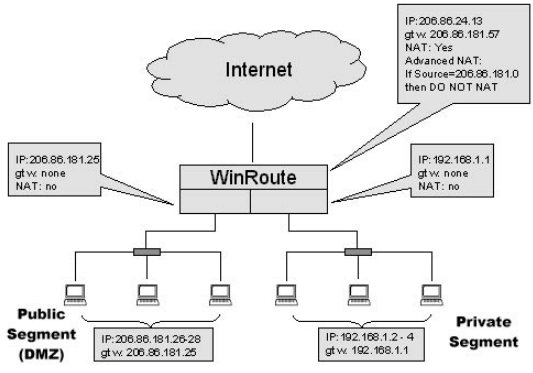
Připojení privátního a veřejného segmentu (DMZ)

Privátní segment obsahuje počítače, které používají privátní IP adresy. Při přístupu z tohoto segmentu do Internetu se provádí překlad adres (NAT) na přidělenou veřejnou adresu. Celá síť je tedy chráněna a z Internetu vypadá jako jediný počítač.

Veřejný segment (tzv. demilitarizovaná zóna, zkr. DMZ) obsahuje počítače s veřejnými IP adresami, které jsou plně přístupné z Internetu (nejsou-li nastaveny žádné paketové filtry).

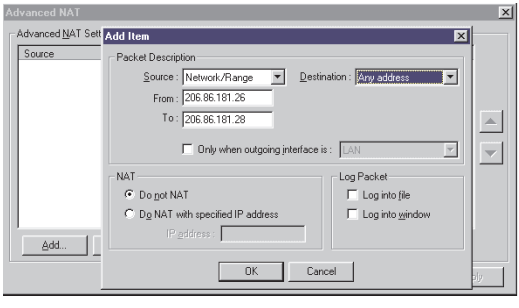
WinRoute umožňuje současné připojení veřejného a privátního segmentu s jednou IP adresou.

- POZOR: Ve DMZ segmentu NELZE používat adresy ze subsítě, do níž je připojeno vnější (internetové) rozhraní! Jinak by totiž nebylo možné směrovat pakety mezi vnější sítí a DMZ. DMZ musí mít poskytovatelem internetového připojení přidělenu vlastní IP subsíť !



Nastavení WinRoute

Ve WinRoute je nutné nastavit, aby pro pakety jdoucí z / do DMZ segmentu nebyl prováděn překlad IP adres (NAT) – zde jsou již přímo veřejné adresy. Toto nastavení provedete v menu Settings –> Advanced –> NAT.



Definované pravidlo říká, že budou-li zdrojové IP adresy v odchozích paketech v rozsahu 206.86.181.26 – 206.86.181.28 (adresy použité v DMZ v našem příkladu), pak se nemá provádět NAT. Pro ostatní adresy (tedy z privátního segmentu) se NAT provádět bude.

Nastavení počítačů v privátném a ve veřejném (DMZ) segmentu

Není třeba žádných speciálních nastavení. V každém segmentu použijte jako výchozí bránu IP adresu toho rozhraní počítače s WinRoute, k němuž je daný segment připojen. Jediná odlišnost veřejného segmentu je v tom, že se zde používají veřejné IP adresy namísto privátních.

Služby Windows

Síť Microsoft Network

V některých případech může být požadováno, aby byl počítač chráněný NAT zvenčí viditelný v Okolních počítačích a byly dostupné jeho sdílené prostředky (diskové jednotky, tiskárny). Mohou to být např. následující situace:

- vaše lokální síť se skládá z několika IP segmentů a některé jsou chráněny vůči ostatním pomocí NAT
- chcete WinRoute použít jako firewall pro ochranu koncové stanice

Pro zpřístupnění služeb sítě Microsoft Networks proveďte následující mapování portů:

Protocol: TCP/UDP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: port range 137-139

Destination IP: shodná s Listen IP (viz kap. Mapování portů)

Destination Port: 137–139

RAS server (server telefonického připojení)

RAS server (server telefonického připojení) umožňuje vzdálené připojení do lokální sítě pomocí modemu. WinRoute obsahuje pro tento účel speciální RAS linku označenou jako „Dial-in adapter“. Toto rozhraní se nezobrazuje

v Interface Table, protože na něm nelze zapnout funkci NAT ani nastavovat žádné další parametry (to je záležitost RAS serveru). WinRoute RAS server nijak neomezuje, je-li splněna následující podmínka:

- RAS server musí mít nastavenu a klientům přidělovat IP adresu z JINÉ SUBSÍTĚ než je lokální síť (př.: používáte-li ve vaší lokální síti IP adresy 192.168.1.x s maskou 255.255.255.0, použijte v RAS serveru IP adresy 192.168.2.x s toutéž maskou. Jinak nebude směrování mezi lokální sítí a vzdálenými klienty fungovat správně.

➢ Poznámka: Používáte-li RAS server ve Windows NT bez WinRoute, pak je možné používat IP adresy přímo z lokální subsítě. Windows NT dokáží takovou situaci ošetřit. WinRoute ale provádí regulérní IP směrování, a proto vyžaduje, aby na každém rozhraní byly IP adresy z JINÉ subsítě.

Tato konfigurace představuje situaci malého poskytovatele Internetu (pro internetové připojení musí být použit jiný modem nebo pevná linka). Pak totiž získá vzdálený klient přístup nejen do lokální sítě, ale i do Internetu. WinRoute nijak neomezuje počet vzdáleně připojených uživatelů.

WWW, FTP, DNS a Telnet server za WinRoute

Zpřístupnění WWW serveru běžícího za WinRoute

Pro zpřístupnění WWW serveru běžícího ve vaší lokální síti (příp. přímo na počítači s WinRoute) proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo adresa, na niž má být WWW server namapován (má-li vnější rozhraní více IP adres)

Listen port: single port 80

Destination IP: IP adresa WWW serveru v lokální síti (např. 192.168.1.10)

Destination Port: 80

Uživatelé v Internetu budou s WWW serverem komunikovat, jako kdyby běžel přímo na příslušné adrese vnějšího rozhraní. V DNS pro vaši doménu je samozřejmě třeba nastavit jméno „www.vasedomena.cz“ na tuto adresu.

DNS server za WinRoute

DNS Forwader ve WinRoute umožňuje předávání dotazů jinému DNS serveru a zároveň zodpovídání lokálních dotazů podle údajů v souboru HOSTS a tabulkách DHCP serveru. To je ve většině případů postačující, přesto však někdy může vzniknout požadavek provozování vlastního plnohodnotného DNS serveru (např. chcete-li DNS server pro vaši doménu spravovat sami a mít jej umístěný v lokální síti).

DNS server používá pro komunikaci s klienty (zodpovídání dotazů) protokol UDP, port 53. Kromě toho umožňuje navázání TCP spojení (na tomtéž portu) pro přenos údajů o celé doméně, typicky mezi primárním a sekundárním DNS serverem nebo pro výpis domény v programu NSLOOKUP. Pro zpřístupnění DNS serveru do Internetu je tedy třeba provést následující mapování portů:

Protocol: TCP/UDP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 53

Destination IP: IP adresa DNS serveru v lokální síti (např. 192.168.1.10)

Destination Port: 53

Samozřejmě je třeba, aby v DNS nadřazené domény (zpravidla „.cz“) byla správně uvedena IP adresa primárního DNS serveru pro vaši doménu (tedy adresa vnějšího rozhraní počítače s WinRoute).

- POZOR: Chcete-li provozovat vlastní DNS server na tomtéž počítači jako WinRoute, musíte VYPNOUT DNS Forwarder! Jinak nastane na portu 53 kolize.

Problematika DNS

Předpokládejme situaci, že ve vaší lokální síti běží WWW server, který je mapováním portu zpřístupněn do Internetu. Přirozený požadavek je, aby na tento server mohlo být přistupováno jménem „www.firma.cz“ jak z Internetu, tak z lokální sítě. Problém je ale v tom, že v lokální síti má tento server privátní adresu, zatímco v Internetu je reprezentován IP adresou vnějšího rozhraní počítače s WinRoute. Tento problém lze řešit dvěma způsoby:

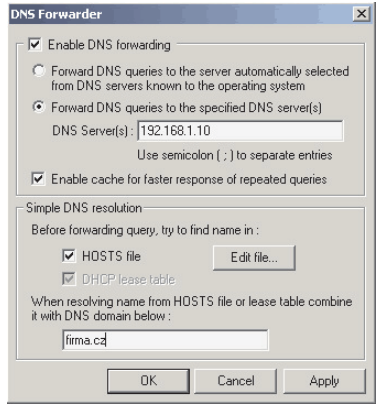
1. Dva DNS servery pro tutéž doménu

- DNS server pro vaši doménu bude umístěn u vašeho poskytovatele Internetu (častý případ). Zde bude jménu „www.firma.cz“ přiřazena veřejná IP adresa počítače s WinRoute. Klient z Internetu dotazem na toto jméno obdrží platnou veřejnou adresu, na níž je server namapován, a spojení se serverem tedy bude moci navázat.
- Ve vaší lokální síti rozběhnete vlastní DNS server, který bude rovněž primárním serverem pro vaši doménu. Zde ale jménům jednotlivých počítačů přiřadíte jejich skutečné (privátní) IP adresy.
- Všem počítačům v lokální síti nastavíte jako adresu DNS serveru adresu VAŠEHO DNS serveru. Klient z lokální sítě tedy dotazem na „www.firma.cz“ obdrží privátní adresu vašeho WWW serveru a v rámci lokální sítě s ním naváže spojení.

Tento postup je regulérní, jestliže budou klienti v lokální síti používat lokální DNS server a tento server nebude zpřístupněn do Internetu.

2. Využití DNS Forwarderu ve WinRoute

- Primární DNS server pro doménu bude pouze jeden. Nezáleží na tom, zda bude umístěn přímo v Internetu (např. u poskytovatele připojení) nebo ve vaší lokální síti a do Internetu zpřístupněn mapováním portů.
- Ve WinRoute zapnete DNS Forwarder. Chcete-li, aby byly dotazy předávány vašemu DNS serveru, zvolte „Forward DNS queries to the specified DNS server(s)“ a uveďte IP adresu vašeho DNS serveru (např. 192.168.1.10). Dále zde nastavte jméno lokání domény (v poli „When resolving name from HOSTS file or lease table combine it with DNS domain below“ – např. „firma.cz“) a tlačítkem „Edit file“ do tohoto souboru zadejte požadovaná jména (např. „www“) a odpovídající privátní IP adresy. Podrobnosti viz kap. WinRoute – popis a nastavení / DNS Forwarder.



- Klientské počítače je třeba nastavit tak, aby používaly DNS Forwarder. Jako adresu DNS serveru tedy zadejte IP adresu vnitřního rozhraní počítače s WinRoute. Bude-li se pak klient dotazovat na jméno „www.firma.cz“, DNS Forwarder nalezne toto jméno v souboru HOSTS a v odpovědi vrátí příslušnou privátní IP adresu serveru. Ostatní DNS dotazy bude správně předávat na váš DNS server, případně na jiný DNS server (dle nastavení).

➢ Poznámka: Váš vlastní DNS server nemůže v tomto případě běžet na tomtéž počítači jako WinRoute, protože stejně jako DNS Forwarder využívá port 53. Dvě aplikace nemohou běžet na tomtéž portu.

➢ Poznámka 2: DNS Forwarder lze využít i v situaci podle bodu 1. – díky schopnosti vyhledávání v souboru HOSTS může být použit jako interní DNS server vaší domény. Toto řešení je nejjednodušší a zpravidla plně postačující.

FTP klient

Protokol FTP používá pro komunikaci dvě TCP spojení – řídicí (standardně na portu 21) a datové (standardní port 20). Komunikaci zahajuje VŽDY FTP klient navázáním řídicího spojení. Datové spojení pak může navazovat buď také klient, nebo server na klienta (na předem dohodnutém portu). Podle toho, kdo naváže datové spojení, se rozlišují dva režimy (módy) FTP:

- PASIVNÍ MÓD – obě spojení (řídicí i datové) navazuje sám klient. Protože se v obou případech jedná o spojení navazovaná z chráněné lokální sítě směrem do Internetu, neklade WinRoute žádná omezení. FTP server může běžet i na nestandardním portu (tedy jiném než 21).
- AKTIVNÍ MÓD – klient naváže pouze řídicí spojení a server navazuje (v opačném směru) spojení datové. Navázat spojení přes NAT z Internetu do vnitřní sítě nelze. WinRoute však obsahuje speciální podporu pro FTP, která dokáže zpracovat požadavek FTP serveru na navázání datového spojení a správně jej přesměrovat na klientský počítač. Omezením této podpory ale je, že funguje pouze, běží-li FTP server na standardním portu 21 (právě podle čísla portu se totiž rozpozná, že se jedná o FTP spojení).

Závěr:

Běží-li FTP server na standardním portu 21, lze v lokální síti za WinRoute provozovat FTP klienty bez omezení. V případě nestandardního portu je třeba nastavit klienta do PASIVNÍHO MÓDU.

FTP server za WinRoute

FTP používá dvě TCP spojení: řídicí (standardně na portu 21) a datové (standardní port 20). Použije-li FTP klient aktivní mód, pak klient navazuje pouze řídicí spojení (datové naváže server na klienta). Teoreticky by tedy stačilo zpřístupnit (namapovat) pro FTP server port 21. Aby se však k FTP serveru mohl připojit klient v libovolném módu (některé klienty nastavení módu neumožňují), je třeba provést mapování OBOU portů.

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: port range 20-21

Destination IP: IP adresa FTP serveru v lokální síti (např. 192.168.1.10)

Destination Port: 20-21

Mail server

Mail server je obvykle složen ze dvou částí: SMTP a POP3 server. Do Internetu můžete chtít zpřístupnit buď jen SMTP server, nebo jen POP3 server, nebo oba. Rozhodněte se správně, který server zpřístupníte:

- SMTP server je třeba zpřístupnit, jestliže je přímo na váš server (počítač s WinRoute) nasměrován MX záznam pro vaši doménu. Pokud tedy např. pošta pro vaši doménu chodí do doménové schránky u poskytovatele Internetu, není třeba SMTP server zpřístupňovat.
- POP3 server musí být přístupný pouze tehdy, chtějí-li si (někteří) vaši uživatelé vybírat své schránky odjinud než z vaší lokální sítě.

Zpřístupnění SMTP serveru

Pro zpřístupnění vašeho SMTP serveru proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 25

Destination IP: IP adresa SMTP serveru v lokální síti (např. 192.168.1.10)

Destination Port: 25

POP3 server

Stejným způsobem proveďte mapování portu 110.

IMAP server

Jestliže mail server používá pro přístup do mailových schránek namísto POP3 protokol IMAP (Internet Message Access Protocol), proveďte mapování portu 143.

Telnet server

Telnet

Telnet je velmi rozšířený protokol pro vzdálený přístup k systému – tzv. virtuální terminál (např. na všechny systémy typu Unix se lze Telnetem přihlásit). Pro svou činnost používá jednoduché TCP spojení. Chcete-li umožnit přístup z Internetu na systém ve vaší lokální síti protokolem Telnet, proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 23

Destination IP: IP adresa Telnet serveru (unixového systému) v lokální síti (např. 192.168.1.10)

Destination Port: 23

SSH (Secure SHell)

SSH je obdoba Telnetu, ale komunikace mezi klientem a serverem je šifrována, aby ji nebylo možno odposlouchávat. SSH používá protokol TCP, port 22 (zpřístupnění SSH serveru tedy provedete mapováním portu 22).

Vzdálený přístup do Windows

Microsoft Terminal Server

Chcete-li umožnit terminálovým klientům vně lokální sítě připojit se na váš terminálový server, proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 3389

Destination IP: IP adresa MS Terminal Serveru v lokální síti (např. 192.168.1.10)

Destination Port: 3389

CITRIX Metaframe

WinRoute plně podporuje protokol aplikace CITRIX Metaframe. Pro přístup k CITRIX Metaframe serveru ve vaší lokální síti z Internetu proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 1494

Destination IP: IP adresa CITRIX Metaframe serveru v lokální síti (např. 192.168.1.10)

Destination Port: 1494

V případě CITRIX Metaframe je možno vytvořit více mapovaných portů pro přístup k více serverům současně. Klienty je samozřejmě nutné nastavit tak, aby se připojovali vždy na správný port.

PC Anywhere

WinRoute obsahuje speciální podporu pro PC Anywhere fy. Symantec. PC Anywhere umožňuje kompletní vzdálený přístup k vybranému počítači. Pro umožnění vzdáleného přístupu uvnitř vaší lokální sítě proveďte následující:

- Na spravovaném počítači nainstalujte aplikaci PC Anywhere Host.
- Na vzdáleném (spravujícím) počítači nainstalujte PC Anywhere Remote.
- Ve WinRoute proveďte následující mapování portů

  Protocol: TCP/UDP

  Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

  Listen port: port range 5631-5632

  Destination IP: IP adresa PC Anywhere Host v lokální síti (např. 192.168.1.10)

  Destination Port: 5631-5632

Bezpečnost

Pro zvýšení bezpečnosti je doporučeno mapování portů doplnit omezením přístupu z vybraných IP adres. Podrobnosti naleznete v kap. WinRoute – popis a nastavení / Mapování portů.

Změna spravovaného počítače

Mapování portů lze vždy provést pouze pro jeden cílový počítač ve vaší lokální síti. PC Anywhere Host však můžete nainstalovat na libovolný počet počítačů a před vlastním vzdáleným připojením se připojit k WinRoute programem WinRoute Administration a nastavit „Destination IP“ na vybraný počítač. Tak můžete vzdáleně přistupovat k libovolnému počítači ve vaší lokální síti (vždy však pouze k jednomu).

Pozn.: Pro vzdálené připojení programem WinRoute Administration je třeba provést mapování portu 44333 (viz kap. Program WinRoute Administration / Administrace z Internetu.

Virtuální privátní sítě (VPN)

PPTP server za WinRoute

PPTP server

Pro zpřístupnění PPTP serveru ve vaší lokální síti, příp. na počítači s WinRoute, je třeba provést následující mapování portů:

Pro řídicí TCP spojení

Protocol: TCP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

Listen port: single port 1723

Destination IP: IP adresa PPTP serveru v lokální síti (např. 192.168.1.20)

Destination Port: 1723

Pro pakety PPTP (GRE)

Protocol: PPTP

Listen IP: <Unspecified> nebo adresa vnějšího rozhraní (tj. toho, na němž je zapnut NAT)

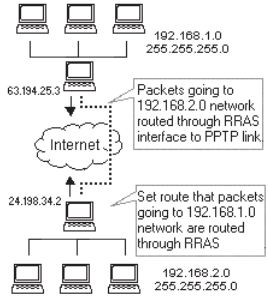
Destination IP: IP adresa PPTP serveru v lokální síti (např. 192.168.1.20)

PPTP klient

Díky vestavěné podpoře pro PPTP ve WinRoute je možno provozovat v lokální síti libovolný počet PPTP klientů bez nutnosti dalších nastavení.

Příklad realizace VPN

Použitím WinRoute a protokolu PPTP lze velmi efektivně propojit dvě lokální sítě (např. pobočky firmy) připojené do Internetu. Vytvořené propojení (tzv. tunel) umožňuje bezpečnou komunikaci mezi oběma lokálními sítěmi.



Realizace takovéto VPN předpokládá následující:

- Windows 2000 Server na obou stranách
- WinRoute na obou stranách
- RRAS (Routing and Remote Access Service – Směrování a vzdálený přístup) na obou Windows 2000 serverech

1 Na obou serverech přidejte do směrovací tabulky cestu do lokální sítě na druhé straně PPTP tunelu přes RRAS rozhraní.

2 V programu WinRoute Administration zvolte Settings –> Interface Table a vyberte RAS linku pro PPTP spojení (je-li třeba, přidejte novou linku v menu Settings –> Advanced –> Interface Maintenance). Ujistěte se, že na tomto rozhraní není zapnut NAT (platí pro obě strany tunelu).

3 V záložce RAS přiřaďte vybrané lince příslušné PPTP připojení.

4 Otestujte propojení (např. příkazem ping) – z libovolného počítače ve vaší lokální síti by měly být dosažitelné jak počítače v lokální síti na druhé straně PPTP tunelu, tak i počítače v Internetu.

➢ POZOR: Nelze použít operační systém Windows NT Server! Implementace služby RRAS v tomto systému využívá vlastní směrování nezávislé na systémové směrovací tabulce, a proto WinRoute nemůže pakety směrovat správně.

PSec klient

WinRoute podporuje protokol IPSec v tzv. tunelovém módu. Tunelový mód by měl umožňovat libovolný IPSec klient povolující změnu IP adresy. Ve WinRoute je třeba provést následující mapování portů:

Mapování portů pro ESP (Encapsulation Security Payload)

Protocol: Other 50

Listen IP: <Unspecified>

Destination IP: IP adresa počítače, na němž běží IPSec client

Dále doporučujeme definovat mapování portů pro IKE (Internet Key Exchange). Toto sice není nutné, pokud IPSec spojení navazuje klient z lokální sítě do Internetu. Některé implementace IPSec však mohou toto mapování vyžadovat.

Mapování portů pro IKE

Protocol: UDP

Listen IP: <Unspecified>

Listen Port: single port 500

Destination IP: IP adresa počítače, na němž běží IPSec klient

Destination Port: 500

Provozování více IPSec klientů současně

Spuštění více IPSec klientů ve vaší lokální síti je možné, ale každý klient vyžaduje vlastní vnější IP adresu (tj. na vnějším rozhraní počítače s WinRoute musíte mít přiřazeno tolik IP adres, kolik IPSec klientů chcete současně provozovat. Pro každého klienta provedete výše uvedená mapování portů („Listen IP" bude vždy jedna z vnějších IP adres a „Destination IP" adresa počítače v lokální síti, na němž běží příslušný IPSec klient.

➢ Poznámka: Implementace protokolu IPSec jednotlivých výrobců mohou být značně odlišné. Z tohoto důvodu nelze zaručit stoprocentní funkčnost všech typů klientů.

Novell Border Manager

Novell Border Manager je implementací protokolu IPSec. Jedná se o softwarový balík určený k vytváření virtuálních privátních sítí. Na straně klienta se používá aplikace Border Manager VPN Client, na straně serveru (tj. ve vzdálené síti, do níž klient vytváří „tunel") Border Manager Enterprise Server.

V souboru README.TXT na instalačním disku se uvádí následující:

„Není možné použít NAT na cestě mezi VPN klientem a VPN serverem. IP a IP pakety jsou zapouzdřeny a šifrovány VPN klientem a pro zapouzdření je použita zdrojová adresa VPN klienta. Zabezpečující hlavička IPSec (Authentication Header) je vytvořena na základě IP adres VPN klienta a VPN serveru. Změní-li NAT některou z těchto adres (klienta nebo serveru), ověření zabezpečení po přijetí paketu selže a paket bude zahozen. NAT také zpravidla zpracovává pouze protokoly TCP, UDP a ICMP a ostatní pakety zahazuje.

Chcete-li sdílet VPN připojení pro celou lokální síť, doporučuje se namísto Border Manager VPN klienta použít Border Manager Enterprise Server a vytvořit VPN typu server – server."

Border Manager Enterprise Server je ale velmi drahý pro domácí uživatele a malé firmy. Navíc vyžaduje nastavení statického směrování ve vzdálené síti, do níž se připojujete. Řešení doporučované firmou Novell je pro lokální síť připojenou jednou internetovou přípojkou (pomocí NAT) nepoužitelné.

Experimentálně však bylo ověřeno, že je možné propojení realizovat za použití WinRoute a Novell Border Manager VPN Client, jestliže bude VPN Client nainstalován přímo na počítači s WinRoute. Tato konfigurace umožní všem počítačům ve vaší lokální síti přístup do vzdálené sítě. Není nutná žádná konfigurace vzdálené sítě.

Postup při instalaci

1 Nainstalujte Border Manager VPN Client na počítač, který bude branou do Internetu (na nějž bude nainstalován WinRoute). Přesvědčete se, že je možno navázat spojení do vzdálené sítě a počítače v ní jsou dostupné.

2 Nainstalujte na tento počítač WinRoute Pro a proveďte konfiguraci WinRoute a ostatních počítačů v síti (viz kap. Instalace a Nastavení WinRoute a lokální sítě) – bez ohledu na VPN. Ujistěte se, že přístup do Internetu přes WinRoute z lokální sítě funguje.

3 Pro vytvoření VPN spusťte Border Manager VPN Client a přihlaste se do vzdálené sítě.

Toto je možné díky podpoře IPSec ve WinRoute Pro. Ta zajistí, že se překlad adres (NAT) provede DŘÍVE, než je paket směrován na virtuální IPSec rozhraní. Tím je zajištěno, že při zapouzdření bude mít paket již správnou zdrojovou IP adresu (tj. veřejnou adresu vnějšího rozhraní WinRoute). Pro příchozí pakety je proces obrácený: nejprve proběhne odpouzdření paketu a teprve potom zpětný překlad adres. Paket pak může být směrován na správný počítač uvnitř lokální sítě.

Omezení této konfigurace spočívá v tom, že připojování VPN klienta do vzdálené sítě se musí provádět ručně. Klient nemůže být připojen trvale – po určité době nečinnosti (nastavené na VPN serveru) dojde k automatickému odpojení. Přestože Border Manager podporuje i směrování IPX paketů, nelze v tomto případě mezi lokální a vzdálenou sítí protokolem IPX komunikovat, protože WinRoute směruje pouze IP pakety. Komunikace IPX by tedy fungovala pouze z počítače s WinRoute / Border Manager VPN klientem.

Chat, multimédia a videokonference

ICQ

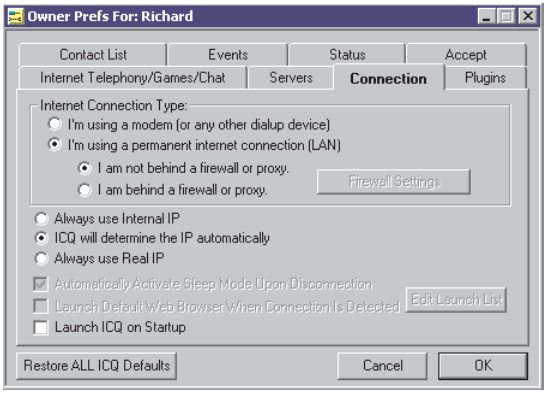
ICQ je chat (tj. program pro online komunikaci mezi uživateli), který umožňuje buď vytvoření přímého spojení mezi dvěma uživateli anebo komunikaci uživatelů přes ICQ server.

Nastavení WinRoute

WinRoute Pro 4.1 obsahuje speciální podporu pro ICQ, takže není nutné nic nastavovat (ani mapování portů, které bylo vyžadováno v předchozích verzích).

Nastavení ICQ

ICQ nastavte tak, jako by byl příslušný počítač připojen přímo do Internetu (žádný firewall, žádný proxy server).



Omezení

Nevýhodou ICQ je, že jeho autoři v každé verzi mění komunikační protokol. Podpora ICQ ve WinRoute byla vyvinuta pro verzi 99b. Starší verze nelze s WinRoute používat. Verze 2000a a 2000b lze používat, ale není možné navázat chat a přenos souboru směrem z Internetu do lokální sítě.

IRC (Internet Relay Chat)

Provozování IRC klienta za WinRoute nevyžaduje žádná speciální nastavení. Funkce DCC (Direct Chat/Send/Receive Files) ale vyžaduje použití standardního portu 6667.

Chcete-li provozovat IRC server ve vaší lokální síti, je třeba provést následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> (nebo jedna z adres vnějšího rozhraní, kterou chcete pro IRC server použít)

Listen Port: single port 6667

Destination IP: IP adresa IRC serveru (např. 192.168.1.30)

Destination Port: 6667

V případě použití jiného portu nebude DCC fungovat.

Telefonování po Internetu – BuddyPhone

WinRoute je první router/firewall, který podporuje telefonování po Internetu. S použitím aplikace BuddyPhone (**http://www.buddyphone.com**) umožňuje volat po Internetu z vaší sítě do libovolné jiné.

Podpora pro BuddyPhone pracuje nejlépe s ICQ. Všichni aktivní uživatelé z vašeho ICQ Buddy List se zároveň objeví v seznamu BuddyPhone Phone Book. Pro zavolání pak stačí jednoduše vybrat uživatele z tohoto seznamu.

Používáte-li BuddyPhone společně s ICQ, není třeba žádné speciální nastavení. Cílový port je 700 (standardní port používaný aplikací BuddyPhone).

➢ Poznámka: Protože je plně podporována pouze verze ICQ 99b, je třeba použít tuto verzi (viz kap. ICQ).

Použití BuddyPhone bez ICQ

WinRoute umožňuje rozlišit příchozí hovory (z Internetu do lokální sítě) na základě portu. Pro každého uživatele je tedy potřeba vytvořit mapovaný port (viz kap. WinRoute – Popis a nastavení / Mapování portů).

Protocol: TCP/UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: single port 710

Destination IP: 192.168.1.2

Destination Port: 710

Vytvořte toto mapování pro každého uživatele. Použijte porty 710, 711 atd.

Tři uživatelé, kteří budou používat BuddyPhone.

Jméno	Interní IP adresa	Přiřazený port
Petr	192.168.1.2	710
Honza	192.168.1.3	711
Mirek	192.168.1.4	712

Zavolání uživateli pak spočívá pouze v uvedení adresy (jména) počítače s příslušným portem v BuddyPhone Direct Dial dialogu. Např. uživateli „Honza“ zavoláte zadáním „server.vase-domena.cz:711“.

ICUii videokonference

WinRoute je první softwarový firewall / směrovač, který umožňuje provozování videokonferencí z chráněné lokální sítě za použití aplikace ICUii (**http://www.icuii.com**).

Pro používání ICUii v lokání síti je třeba provést následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> (nebo jedna z adres vnějšího rozhraní)

Listen Port: port range 2000-2038

Destination IP: IP adresa počítače s ICUii, kde budete chtít přijímat hovory (např. 192.168.1.22)

Destination Port: 2000-2038

CU-SeeMe

Pro příjem hovorů v aplikaci CU-SeeMe je třeba provést následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> (nebo jedna z adres vnějšího rozhraní, kterou chcete pro CU-SeeMe použít)

Listen Port: port range 7648-7649

Destination IP: IP adresa počítače, na němž běží CU-SeeMe (např. 192.168.1.30)

Destination Port: 7648-7649

Omezení:

- Ve vaší lokální síti je možno provozovat pouze jednoho CU-SeeMe klienta.
- Není možno připojit se k „reflektoru“ chráněnému heslem.

Microsoft Windows NetMeeting

WinRoute obsahuje omezenou podporu pro Microsoft NetMeeting pro přenos hlasu a videa. Není možno používat adresářové služby.

Pro příjem hovorů v NetMeetingu je třeba provést následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> (nebo jedna z adres vnějšího rozhraní)

Listen Port: single port 1720

Destination IP: IP adresa stanice, na níž budete NetMeeting provozovat (např. 192.168.1.30)

Destination Port: 1720

- POZOR: Mapování portu je nutné provést pouze pro protokol TCP, nikoliv pro UDP (resp. TCP/UDP). Mapováním portu pro UDP vyřadíte vestavěnou podporu ve WinRoute z činnosti!

Omezení:

Přijímat hovory lze pouze na jednom počítači ve vaší lokální síti (na nějž je port 1720 namapován).

H.323 (VoIP) Gateway

Chcete-li zpřístupnit do Internetu H.323 Gateway běžící v lokální síti, proveďte následující mapování portů:

Protocol: TCP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní

Listen Port: single port 1720

Destination IP: IP adresa počítače, na němž H.323 Gateway běží (např. 192.168.1.100)

Destination Port: 1720

Na jednu vnější (veřejnou) IP adresu lze namapovat vždy pouze jednu H.323 Gateway.

- POZOR: Mapování portů pro H.323 Gateway je stejné jako pro Microsoft NetMeeting (ten rovněž používá protokol H.323). Z toho vyplývá, že nelze provozovat H.323 Gateway a NetMeeting současně, nemáte-li na více veřejných IP adres (přiřazených vnějšímu rozhraní).

Hry

Provozování her za NAT

Mnoho současných her má multiuživatelské prostředí: uživatelé mohou hrát proti sobě po síti anebo se mohou připojit na existující herní servery v Internetu. Mohou také vytvořit svůj vlastní herní server a umožnit ostatním připojit se do hry.

Velké množství her nepotřebuje žádné speciální nastavování firewallu (tedy WinRoute). Doporučujeme každou hru nejprve vyzkoušet (bez nastavování WinRoute). Narozdíl od proxy serverů, základní architektura WinRoute (směrovač + NAT) podporuje mnoho her bez dalšího nastavení.

Některé hry však potřebují nastavit mapování portů ve WinRoute (aby bylo možno navázat spojení z Internetu na hráčův počítač – viz kap. WinRoute – popis a nastavení / NAT směrovač / Jak funguje NAT).

To však není žádný problém, stačí vytvořit příslušné mapované porty s cílovou IP adresou hráčova počítače. Používané porty se u jednotlivých her samozřejmě liší. V následujících kapitolách budou popsána nastavení pro několik nejrozšířenějších her. Další informace pak můžete nalézt v manuálu k příslušné hře, případně zavolat na linku technické podpory výrobce této hry.

MSN Gaming Zone

Následující nastavení bylo důkladně testováno na hře MechWarrior3 v MSN Gaming Zone. Přístup do MSN Gaming Zone je možný pouze z jednoho počítače v lokální síti, pro který provedete následující mapování portů:

1 **Protocol:** TCP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: port range 2300-2400

Destination IP: IP adresa počítače, který se má připojovat do MSN Gaming Zone

Destination Port: 2300-2400

2 **Protocol:** UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: 28800-28912

Destination IP: IP adresa počítače, který se má připojovat do MSN Gaming Zone

Destination Port: 28800-28912

Quake

Quake 2/3 klient

Quake klient nevyžaduje žádná speciální nastavení. V lokální síti může běžet i více klientů současně.

Quake 2/3 Server:

Mapování portů pro Quake Master Server:

Protocol: UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: single port 8002

Destination IP: IP adresa počítače, kde běží Quake Master Server (např. 192.168.1.22)

Destination Port: 8002

Mapování portů pro Quake3 Arena Server

Protocol: UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: single port 27960

Destination IP: IP adresa počítače, kde běží Quake3 Arena Server (např. 192.168.1.22)

Destination Port: 27960

Half-Life

Hru Half-Life lze do Internetu zpřístupnit pouze z jednoho počítače ve vaší lokální síti. Proveďte následující mapování portů:

Protocol: TCP/UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: single port 27015

Destination IP: IP adresa hráčova počítače (např. 192.168.1.11)

Destination Port: 27015

Battle.net (Blizzard)

Pro hraní her na Battle.net je nutno provést následující mapování portů. Připojit se může vždy jen jeden počítač v lokální síti.

Protocol: UDP

Listen IP: <Unspecified> nebo jedna z adres vnějšího rozhraní počítače s WinRoute

Listen Port: single port 6112

Destination IP: IP adresa hráčova počítače (např. 192.168.1.11)

Destination Port: 6112

Speciální sítě

Sítě Token Ring

TokenRing je velmi specifický typ sítě. Předpokládáme, že síť TokenRing spravují pouze zkušení síťoví administrátoři, a zde se omezíme pouze na nastavení nutná pro správnou činnost WinRoute s rozhraními typu TokenRing.

- na všech počítačích v síti TokenRing nastavte MTU (Maximum Transmission Unit) na **1500**
- ve WinRoute v menu Settings –> Advanced –> Misc. Options zapněte volbu „TokenRing support enabled“
- ostatní nastavení proveďte dle typu vašeho internetového připojení (viz kap. Nastavení WinRoute a lokální sítě)

Kapitola 7

TECHNICKÁ PODPORA

Základní informace

Společnost Tiny Software poskytuje na produkt WinRoute Pro bezplatnou e-mailovou a telefonickou technickou podporu. Kontakty naleznete na našich WWW stránkách **http://www.tinysoftware.cz**. Naši technici vám rádi ochotně pomohou s jakýmkoliv problémem.

Značné množství problémů lze ale vyřešit (zpravidla i rychleji) svépomocí. Než se rozhodnete kontaktovat technickou podporu fy. Tiny Software, proveďte prosím následující.

- Pokuste se najít odpověď v tomto manuálu. Jednotlivé kapitoly obsahují velmi detailní popis funkcí a nastavení jednotlivých částí WinRoute. Popis je doplněn příklady, které jsou z převážné části kopiemi reálných situací u našich zákazníků.
- Nenaleznete-li odpověď na vaši otázku zde, pokuste se ji nalézt na našich WWW stránkách v sekci Technická podpora. Zde je odkaz na stránku často kladených otázek (Frequently Asked Questions – FAQ) a odpovědí na ně. Otázky jsou rozděleny do několika skupin podle typu problému.

Pokud ani jeden z výše uvedených postupů nepomohl vyřešit Váš problém a rozhodli jste se kontaktovat naši technickou podporu, přečtěte si prosím nejprve pozorně následující kapitolu.

Údaje pro technickou podporu

Abychom vám mohli co nejlépe a nejrychleji pomoci, potřebujeme získat maximum informací o vaší konfiguraci a řešeném problému. V e-mailu pro technickou podporu uveďte prosím následující:

Popis problému

Uvedte slovní popis vašeho problému. Snažte se uvést co nejvíce informací, které by mohly s problémem souviset (např. zda se chyba projevila po instalaci nové aplikace apod.).

Soubor s informacemi o konfiguraci (cfgdump.txt)

- spusťte WinRoute Engine a přihlašte se do programu WinRoute Administration
- jestliže máte vytáčenou linku do Internetu, nejprve se připojte.
- v programu WinRoute Administration stiskněte kombinaci kláves Ctrl-S. Soubor „cfgdump.txt“ bude uložen do adresáře, kde je WinRoute nainstalován (např. „C:\Program Files\WinRoute Pro“).

Soubor s chybovými zprávami nízkoúrovňového ovladače WinRoute

Soubor wrdrv.log se vytváří pouze v okamžiku, kdy ovladač WinRoute zaznamená nějakou závažnou chybu. Naleznete jej:

- v případě Windows 95/98/ME v kořenovém adresáři systémového disku (většinou „C:\“)
- v případě Windows NT/2000 v adresáři, kde jsou Windows instalovány (většinou „C:\WINNT“)

Soubory se záznamy o chybách

V adresáři, kde je WinRoute nainstalován (např. „C:\Program Files\ WinRoute Pro“) je vytvořen podadresář „logs“. V něm naleznete soubor „error.log“.

Následující body proveďte v případě, máte-li nějaký problém se sítí (typicky nemůžete-li komunikovat s počítačem v Internetu).

Poznámka: jestliže se připojujete do Internetu vytáčenou linkou, ujistěte se, že jste připojeni.

Test programem PING

V programu WinRoute Administration otevřete okno Debug Log a zapněte zaznamenávání ICMP paketu (v ploše okna stiskněte pravé tlačítko myši, zvolte „Log Settings...“ a zašktněte volbu „ICMP“).

Na klientské stanici (tj. stanici uvnitř lokální sítě) zadejte v příkazovém řádku:

```
ping ns.winroute.cz
```

Odpoví-li příkaz PING „Neznámý hostitel“ („Unknown host“), uveďte tuto skutečnost do e-mailu pro technickou podporu a vyzkoušejte příkaz:

```
ping 194.228.3.66
```

Po skončení zkopírujte výstup programu přes schránku. V okně Debug Log stiskněte pravé tlačítko myši a vyberte „Save screen...“ K vašemu e-mailu se žádostí o technickou podporu připojte obsah schránky (výpis programu PING) a uložený Debug Log.

Výpis programu TRACERT

Nejprve na počítači s WinRoute a pak na některé klientské stanici zadejte v příkazovém řádku:

```
tracert -d 194.228.3.68
```

Po skončení příkazu přeneste výstup programu přes schránku do e-mailu pro technickou podporu.

REJSTŘÍK

SLOVNÍČEK POJMŮ

E

ETRN

Přijímáte-li poštu protokolem SMTP a váš server není trvale připojen do Internetu, může se pošta shromažďovat na jiném SMTP serveru. Tento SMTP server musí být nastaven jako nadřazený (relay) SMTP server. V okamžiku připojení do Internetu vyšle váš SMTP server příkaz ETRN (jeden z příkazů protokolu SMTP), čímž si žádá o poslání uložených mailů.

Nejsou-li na nadřazeném SMTP serveru žádné maily uloženy, nadřazený SMTP server na příkaz ETRN neodpoví. Proto je třeba definovat dobu (timeout), po které váš SMTP server ukončí spojení, jestliže žádné maily nepřijal.

I

IP adresa

IP adresa je jedinečné 32-bitové číslo identifikující počítač v Internetu. Každý paket posílaný Internetem obsahuje informaci, odkud byl vyslán (zdrojová IP adresa) a kam má být doručen (cílová IP adresa).

IPSec

Protokol pro vytvoření bezpečného (šifrovaného) spojení mezi dvěma počítači. Používá se pro vytváření virtuálních privátních sítí (VPN). Standard IPSec definuje tvar paketů, nespecifikuje však např. šifrovací algoritmy. Proto se implementace IPSec jednotlivých výrobců mohou navzájem lišit.

M

Mailové schránky

Mailová schránka je místo, kde jsou přijaté maily uloženy, než si je klient vybere (typicky protokolem POP3). Fyzicky je schránka reprezentována adresářem na disku, který je vytvořen v adresáři mail serveru (typicky „\Program Files\WinRoute Pro\mail“).

Schránky nejsou vytvořeny při definici uživatelů, konkrétní schránka je vždy vytvořena až po přijetí prvního mailu, který do ní má být uložen.

Mapování portů

Mapování portů znamená přesměrování paketů s určitými cílovými porty přicházejících na vnější rozhraní počítače provádějícího NAT (tedy jedinou zvenčí viditelnou IP adresu) na vybraný počítač v lokální síti. Tak je možno zpřístupnit do Internetu aplikaci běžící uvnitř chráněné (nepřístupné) lokální sítě.

Maska subsítě

Maska subsítě rozděluje IP adresu na dvě části: vyšší, označující síť, a nižší, označující počítač v rámci této sítě. Maska se zapisuje stejně jako IP adresa (např. 255.255.255.0), ale je třeba ji vidět jako 32 bitové číslo, mající zleva určitý počet jedniček a zbytek nul (maska tedy nemůže obsahovat libovolné hodnoty). Jednička v masce označuje bit adresy sítě a nula bit adresy počítače. Všechny počítače v jednom IP segmentu musejí mít stejnou masku subsítě a stejnou síťovou část IP adresy.

MX záznamy

Záznam MX je jedním z typů záznamů, které mohou být uloženy v DNS. Obsahuje informaci o mail serveru pro danou doménu (tzn. na který SMTP server má být poslán mail pro tuto doménu). MX záznamů pro jednu doménu může být více, pak mají různou prioritu a mohou definovat např. primární a záložní mail server.

N

NAT

Použitím technologie NAT (Network Address Translation – překlad IP adres) je možno připojit lokální síť do Internetu přes jedinou veřejnou IP adresu. Celá síť tak navenek vypadá jako jeden počítač, ale počítače v ní mají přístup na Internet, jako by k němu byla síť připojena klasickým směrovačem (platí zde určitá omezení).

Ve všech paketech jdoucích z lokální sítě do Internetu je zdrojová IP adresa nahrazena vnější IP adresou a proveden záznam do tzv. NAT tabulky. Odpovídá-li příchozí paket některému záznamu v tabulce, provede se nahrazení cílové adresy původní IP adresou a paket je směrován na správný počítač v lokální síti. Jinak je paket zahozen. NAT tak chrání celou lokální síť proti přístupu zvenčí.

Oproti klasickým proxy serverům a aplikačním branám se NAT vyznačuje tím, že dokáže propustit téměř libovolný protokol založený na IP. Umožňuje tedy přístup do Internetu stejným způsobem, jako běžný směrovač.

P

Paket
Paket je základní datová jednotka přenášena počítačovou sítí. Každý paket se skládá z tzv. hlavičky (tj. např. zdrojovou a cílovou adresu, typ protokolu a další informace) a datové části obsahující vlastní přenášená data. Maximální velikost datové části (MTU) je dána typem sítě – např. v síti Ethernet je to 1500B. Data přenášená sítí jsou vždy rozdělena do (relativně malých) paketů. Při ztrátě či chybě v jednom paketu nemusí být opakován celý přenos, stačí zopakovat vyslání chybného paketu.

POP3
POP3 je protokol používaný zejména e-mailovým klientem k vybírání poštovní schránky. Pro komunikaci používá protokol TCP, port 110. Aby se zabránilo neoprávněnému přístupu do schránky, používá POP3 ověření uživatele jménem a heslem.

Port
Port je 16-bitové číslo (1–65535) používaná protokoly TCP a UDP pro identifikaci aplikací (služeb) na daném počítači. Na jednom počítači (jedné IP adrese) může totiž běžet více aplikací současně (WWW server, WWW klient – prohlížeč, FTP klient atd.). Každá aplikace je však jednoznačně určena číslem portu. Porty 1–1023 jsou vyhrazené a používají je standardní, příp. systémové služby (např. 80 = WWW). Porty 1024 mohou být volně použity libovolnou aplikací (typicky klientem jako zdrojový port nebo nestandardní aplikací serverového typu).

PPTP
PPTP (Point-to-Point Tunelling Protocol) je protokol používaný operačním systémem Windows pro vytváření bezpečného (šifrovaného) spojení. Typicky se používá pro vytváření virtuálních privátních sítí (VPN).

Proxy
Proxy je velmi rozšířená metoda sdílení internetového připojení. Proxy server představuje prostředníka mezi klientem a cílovým serverem. Pracuje však na aplikační úrovni a je přizpůsoben několika typům aplikačních protokolů. Ve srovnání s technologií NAT jsou jeho možnosti velmi omezené.

S

Síťové rozhraní

Síťové rozhraní je obecné označení pro zařízení, které propojuje počítač s ostatními počítači určitým typem komunikačního média. Síťové rozhraní může být např. karta Ethernet, karta TokenRing, modem atd. Prostřednictvím síťového rozhraní počítač vysílá a přijímá pakety.

Směrovací tabulka

Směrovací tabulka je množina pravidel, jak posílat pakety mezi jednotlivými síťovými rozhraními daného počítače. Směrování se provádí výhradně dle cílové adresy paketu. Systémovou směrovací tabulku lze zobrazit příkazem „route print“ z příkazového řádku.

SMTP

SMTP (Simple Mail Transfer Protocol) je protokol používaný pro komunikaci mezi mail servery a pro odesílání pošty klientem na mail server. Pro komunikaci používá protokol TCP, port 25. Samotný protokol obsahuje pouze příkazy pro vytvoření a odeslání zprávy, neumožňuje žádné zabezpečení ani ověření uživatele.

T

TCP/IP

TCP/IP je společné označení pro komunikační protokoly používané v Internetu (např. IP, ICMP, TCP, UDP atd.). Všechny tyto protokoly jsou založené na paketech (tzv. paketově orientované). TCP/IP NENÍ konkrétní protokol!