WinRoute Pro 3.0

Uživatelská příručka

Instalace

Obsah

Výběr počítače pro instalaci

WinRoute se instaluje na počítač, který bude zajišťovat připojení lokální sítě (nebo více sítí) do Internetu. Tento počítač by měl mít tedy jednu síťovou kartu pro připojení lokální sítě a nějaké zařízení pro připojení do Internetu: modem, ISDN adaptér, druhou síťovou kartu apod.

Systémové požadavky

Operační systém

WinRoute může být nainstalován na následujících operačních systémech:

- Windows NT 4.0 Workstation
- Windows NT 4.0 Server
- Windows NT 4.0 Terminal Server
- Windows 95
- Windows 98

Hardware

- PC s procesorem 486/66 nebo vyšším
- paměť:
  8 MB (16 doporučeno) pod Windows 95/98
  16 MB (24 doporučeno) pod Windows NT
- dostatečný prostor pro diskovou proxy-cache.

Celkové nároky na počítač stoupají při větším počtu uživatelů.

Systémový software

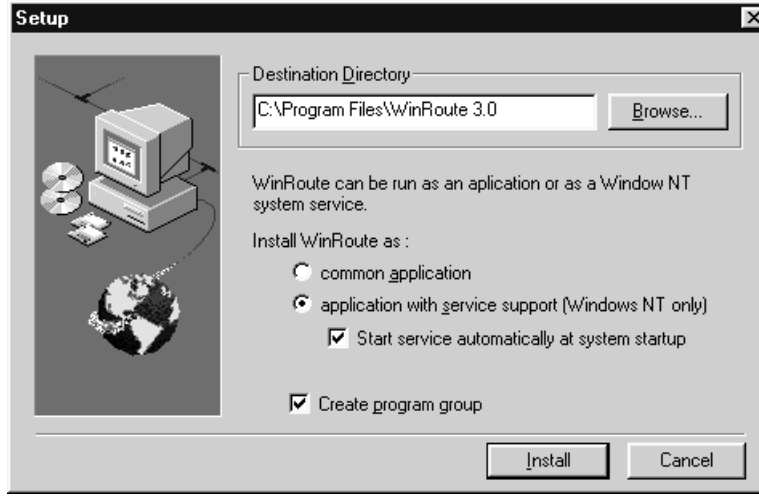
- TCP/IP protokol
- Telefonické připojení (RAS) v případě modemu nebo ISDN karty

Na Windows NT 4.0 je vhodné aplikovat Service Pack 3 nebo 4.

Na Windows 95 je vhodné nainstalovat Dial-up Networking 1.3.

Instalační program

Instalace se provede spuštěním instalačního programu. Instalační program je obsažen na distribučním médiu, nebo jej lze získat na Internetu.



Po spuštění instalačního programu si můžete zvolit:

- "Destination Directory"

  Adresář, do kterého bude WinRoute nainstalován.

- "Install WinRoute as"

  Tato volba určuje, zda má být program nainstalován jako normální aplikace (common application), nebo s podporou služby (aplication with service support). Pokud provedete instalaci s podporou služby, můžete WinRoute spouštět jako normální aplikaci nebo jako službu. Volba je dostupná pouze pod Windows NT.

- "Start service automatically at system startup"

  Pokud WinRoute instalujete jako službu, můžete zvolit, zda se má spouštět automaticky při startu operačního systému.

- "Create Program Group"

  Volba určuje, zda se má vytvořit skupinka v menu Start => Programy

  Po ukončení instalace budete vyzvání k restartu počítače.

Instalované soubory

Při instalaci se zkopírují následující výkonné soubory:

Do cílového adresáře:

- WinRoute.exe
- Server.exe

Do systémového adresáře:

- wrdrv.sys (v případě Windows NT)
- wrdrv.vxd (v případě Windows 95/98)

Do windows adresáře:

- snmpapi.dll (v případě Windows 95)

Odinstalace

Odinstalaci provádějte výhradně prostřednictvím odinstalačního programu. Odinstalační program lze spustit ze skupinky WinRoute v menu Start => Programy, nebo z Ovládací panely => Přidat nebo ubrat programy.

Po ukončení odinstalace je zapotřebí počítač restartovat, aby se deaktivoval síťový ovladač WinRoute.

Rychlé nastavení

Tato část manuálu popisuje, jak rychle provést nastavení produktu a počítačů v síti.

Po tomto nastavení je již produkt plně funkční.

Uvažovaná síť

V popisu se uvažuje následující (nejběžnější) konfigurace lokální sítě:

Na jednom segmentu je připojeno několik počítačů a jeden z nich je vybrán pro připojení do Internetu přes modem. Na tomto počítači je nainstalován WinRoute. Připojení do Internetu je realizováno přes jedinou IP adresu (dynamicky přidělenou při připojení).

Předpoklady:

- Na počítači s WinRoute je pro přístup do Internetu nainstalovaná služba RAS.
- Na všech počítačích se předpokládá nainstalované a fungující TCP/IP.

Nastavení WinRoute

V uvažovaném případě není zapotřebí WinRoute nastavovat. Pouze v případě, že máte v Telefonickém připojení vytvořeno více položek, je zapotřebí vybrat jednu, přes kterou si přejete, aby se WinRoute připojoval. Položku ve WinRoute zadáte následovně: z menu "Settings" vyberete "Interfaces" a ze seznamu zvolíte "RAS line0". V dialogu "Properties" zvolíte záložku "RAS Settings" a nastavíte požadované údaje.

Nastavení TCP/IP na počítačích v lokální síti

Na počítačích, které budou prostřednictvím WinRoute přistupovat do Internetu, je zapotřebí provést změny v nastavení TCP/IP protokolu. Změny se provádí z:

Windows 95/98: Ovládací panely => Síť => TCP/IP.

Windows NT: Ovládací panely => Síť => Protokoly => TCP/IP Protocol.

1. Nastavení IP adresy brány (gatewaye)

Na stanicích v sítě je zapotřebí zadat IP adresu WinRoute jako bránu. Adresa brány se zadává na záložce (v položce) „Brána“.

Upozornění: ***Adresu brány nezadávejte na počítači, kde je WinRoute nainstalován.***

2. Nastavení DNS serveru

Na záložce DNS zadejte IP adresu DNS serveru. Tuto adresu vám sdělí váš poskytovatel připojení.

<u>Upozornění:</u> Adresu DNS serveru je zapotřebí zadat i na počítači, kde je WinRoute nainstalován.

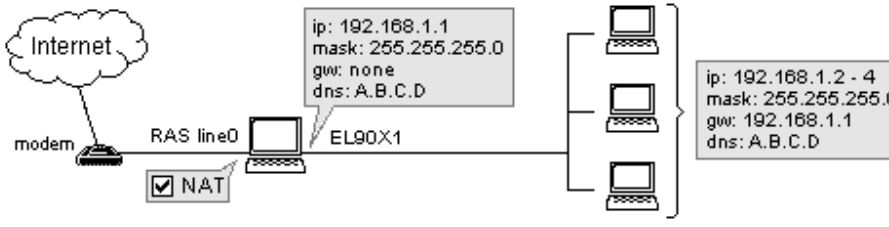
Změny nastavení TCP/IP protokolu vyžadují restart počítače. Po restartu jsou počítače připraveny pro přístup do Internetu.

Otestování

Spusťte WinRoute a z menu "Commands" vyberte příkaz "Dial". Po připojení mohou všechny počítače pracovat s Internetem.

Příklad nastavení

Hodnota A.B.C.D v obrázku označuje IP adresu DNS serveru poskytovatele připojení.



Základní popis

Obsah

Vlastnosti produktu

WinRoute je tvořen následujícími komponentami:

- NAT (Network Address Translation)

  Slouží pro přístup do Internetu přes jedinou IP adresu a pro automatické zabezpečení sítě.
- Mapované porty

  Mapované porty umožňují zpřístupnit služby, které pracují v síti chráněné pomocí NAT.
- Paketový filtr

  Umožňuje filtrování paketů na základě definovaných pravidel.
- DHCP Server

  Slouží pro automatické nastavení síťových parametrů klientských stanic.
- HTTP proxy cache

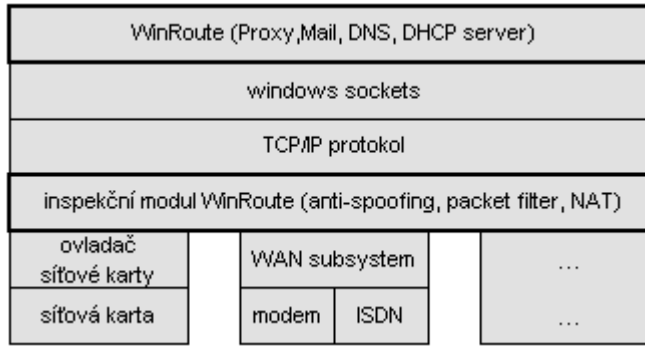
  Při použití zabudovaného proxy serveru jsou WWW stránky ukládány do cache a při opakovaných požadavcích se již nemusí stahávat z Internetu, ale jsou vzaty z cache.
- Mail Server

  Zpracovává elektronickou poštu.
- Jednoduchý DNS Server

  Slouží jako jednoduchý DNS server pro lokální síť. Umožňuje také forwardování dotazů a obsahuje cache.

Architektura

Následující obrázek zobrazuje architekturu WinRoute:



Síťová rozhraní

Síťová rozhraní (interfaces) slouží ve WinRoute k identifikaci sítí, které jsou připojené k počítači s WinRoute. Každé síťové rozhraní má jedinečné jméno.

WinRoute pracuje s následujícími třemi typy rozhraní (dle typu síťových zařízení):

- Ethernet (síťové karty)
- RAS (modemy, ISDN adaptéry)
- DirecPC (karta pro příjem dat přes satelit)

Seznam síťových rozhraní, která jsou k dispozici na vašem počítači, získáte v menu:

Settings => Interfaces

Při vybrání rozhraní a stisknutí tlačítka "Settings" se otevře dialog se záložkami obsahující nastavení rozhraní. Mohou se objevit následující záložky:

- "NAT"

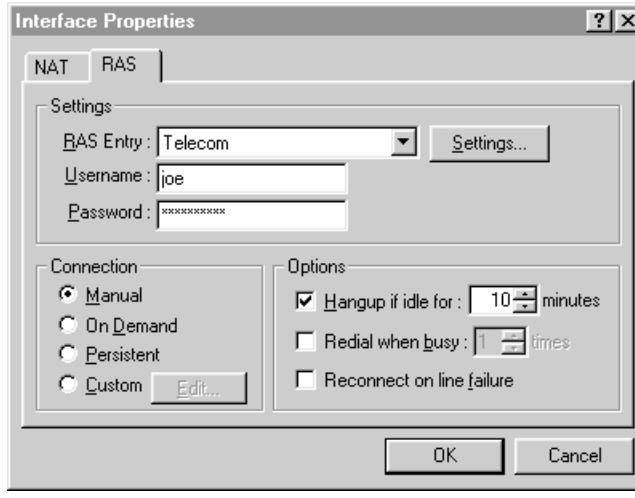
  Nastavení překladu IP adres. Více najdete v kapitole Zabezpečení.
- "RAS"

  Nastavení linek pro vzdálený přístup u rozhraní typu RAS. Nastavení jsou popsána v následující kapitole.
- "DirecPC"

  Nastavení rozhraní pro příjem dat přes satelit. Nastavení tohoto rozhraní jsou popsána v Dodatku.

Rozhraní typu RAS

Rozhraní typu RAS (Remote Access Service) slouží pro připojení prostřednictvím modemu nebo ISDN adaptéru. K rozhraním typu RAS je zapotřebí přidružit záznam z Telefonického připojení sítě. Tento záznam popisuje připojení k vašemu poskytovateli Internetu.



Nastavení rozhraní typu RAS se provádí v menu:

Settings => Interfaces => Settings => záložka RAS

- "RAS Entry"

  Označuje položku Telefonického připojení, se kterou bude toto rozhraní pracovat.

- "Username", "Password"

  Jméno a heslo k vybrané položce. Pokud jméno a heslo nezadáte, bude se brát jméno a heslo nastavené v Telefonickém připojení (za předpokladu, že jste jej povolili uložit).

- "Connection"

  Určuje způsob připojování. Jsou možné následující volby:

  - Manual
    Spojení navazuje ručně (z menu) uživatel.
  - On Demand
    Spojení je navázáno automaticky, když WinRoute rozpozná, že se nějaká aplikace snaží připojit (k Internetu). To se například stane, když si uživatel ve svém prohlížeči vyžádá nějakou WWW stránku.
  - Persistent
    Linka je neustále udržována připojená. Tato volba se používá např. u pevných linek.
  - Custom
    Slouží ke kombinaci předchozích způsobů s možností využití časových intervalů. Lze stanovit, zda je nebo není povoleno připojení On Demand nebo zda je povoleno jen v určitou denní dobu. Je také možné přikázat, že v nějakém časovém intervalu má být linka připojena trvale nebo naopak lze v nějakém časovém intervalu připojení zákázat.

- Hangup if idle for ...

  Zavěsí linku automaticky, jestliže přes ní neprocházela data po danou dobu.

- Redial when busy

  Jestliže připojení neproběhne úspěšně, např. protože je obsazeno, je pokus o spojení opakován.

- Reconnect on line failure

  Jestliže se spojení přeruší v důsledku chyby na lince, je spojení znovu vytvořeno.

Více rozhraní typu RAS

V případě, že se připojujete k různým poskytovatelům připojení, je možné vytvořit více RAS linek (rozhraní typu RAS). RAS linky je možné přidat/odebrat v menu Settings => Advanced => RAS Lines.

Více RAS linek není možné připojit najednou pro zvýšení rychlosti připojení. Jestliže je připojeno více RAS linek najednou, data prochází pouze přes jednu linku (podle routovací tabulky). Zvýšení rychlosti je ale možné využitím sdružení více zařízení pod jeden záznam Telefonického připojení (tzv. Multilink). Toto sdružení je možné provést v nastaveních daného záznamu Telefonického připojení.

Příklady nastavení

Následující příklady ukazují, jak nastavit WinRoute a počítače v lokální síti při nejběžnějších konfiguracích.

IP adresy a jména rozhraní (EL90X1, NE2000) použité v příkladech mají ilustrativní charakter a mohou se ve skutečnosti lišit.

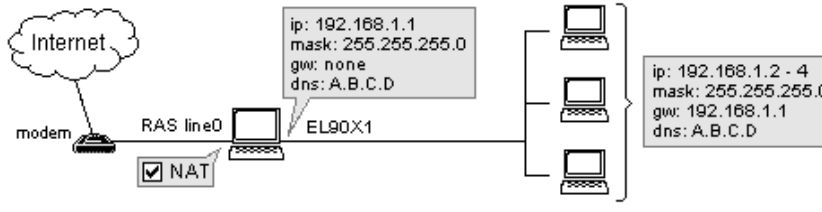
U nastavení IP adresy DNS serveru na počítačích je v příkladech uváděna adresa A.B.C.D. Za tuto adresu dosaďte IP adresu dle jednoho z následujících způsobů:

- IP adresu DNS serveru vašeho poskytovatele připojení. DNS dotazy pak budou chodit přímo na DNS server poskytovatele.
- IP adresu počítače s WinRoute, tedy 192.168.1.1. Ve WinRoute pak v menu "Settings" => "DNS Server" zapněte DNS server a nastavte forwardování DNS dotazů v políčku "Forward DNS queries to" na IP adresu DNS serveru vašeho ISP.

  DNS dotazy pak budou chodit nejprve na počítač s WinRoute a ten je bude přesměrovávat na DNS server poskytovatele.

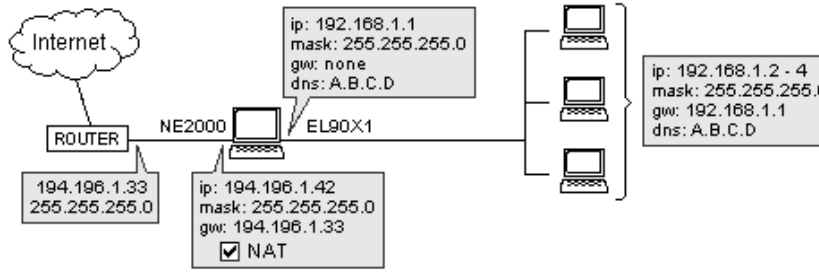
Příklad 1

Lokální síť připojená do Internetu pomocí telefonického připojení (modem, ISDN).



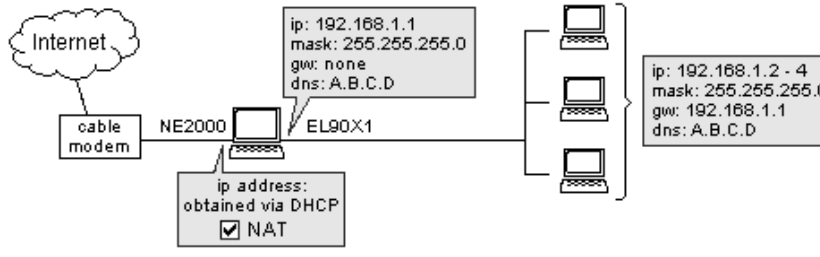
Příklad 2

Lokální síť připojená do Internetu pomocí druhé síťové karty.



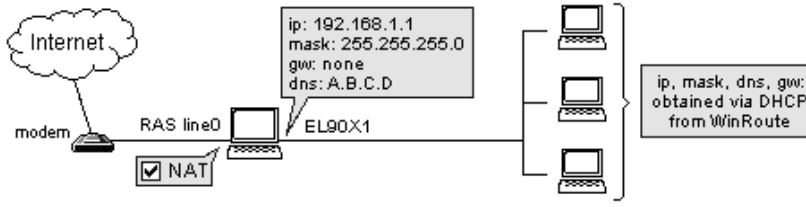
Příklad 3

Lokální síť připojená do Internetu pomocí kabelového modemu.

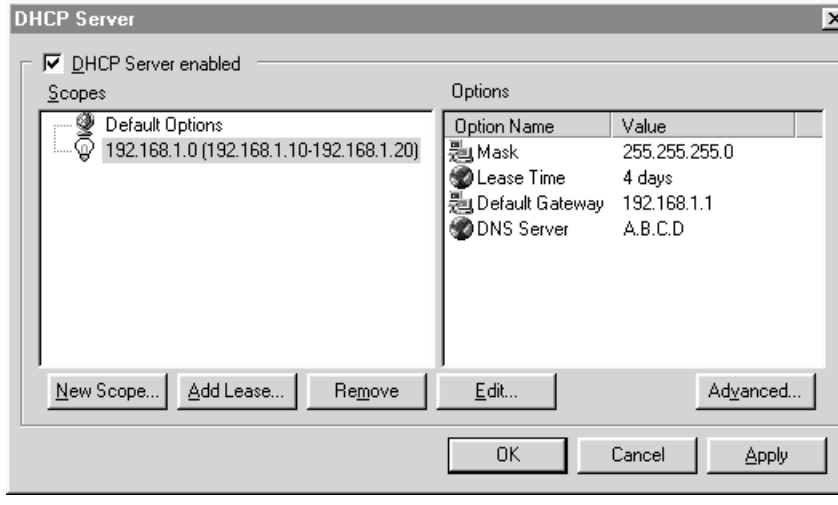


Příklad 4

Tento příklad je stejný jako příklad 1, ale využívá DHCP server pro nastavení klientských počítačů.



DHCP server je nastaven následovně:



Takto nastavený DHCP server přiděluje klientským stanicím nádledující parametry:

- IP adresy v rozsahu od 192.168.1.10 do 192.168.1.20
- Masku 255.255.255.0
- Router (gateway) 192.168.1.1
- DNS server A.B.C.D

IP adresa je přidělena na 4 dni.

Podobným způsobem jako v tomto případě je možné využít DHCP v příkladech 2 a 3.

Zabezpečení

Obsah

Úvod

WinRoute poskytuje následující techniky pracující s pakety (v síťové vrstvě OSI modelu):

- Překlad IP adres (NAT)
- Mapované porty
- Filtrování paketů
- Anti spoofing

Tyto techniky je možné použít k zabezpečení lokální sítě a překlad IP adres je navíc možné použít pro připojení sítě při nedostatku registrovaných IP adres, např. pro připojení celé sítě přes jednu IP adresu.

Překlad IP adres - NAT (Network Address Translation) je technika, která upravuje odcházející pakety z celé (nebo definované části) lokální sítě tak, že vypadají, jako by odcházely pouze z počítače, na kterém WinRoute běží (tedy v paketech mění původní adresu počítače za svoji), a v přicházející pakety, které jsou odpovědí, rozesílá zpět počítačům v lokální síti (upravuje cílovou adresu).

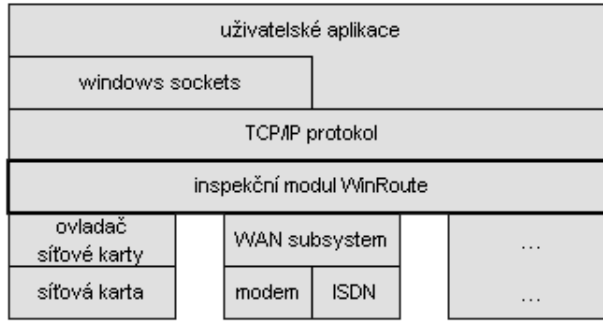
Mapované porty slouží ke zpřístupnění vybraných služeb v sítích, které jsou zabezpečeny NATem.

Filtrování paketů je základní bezpečnostní modul každého firewallu, který umožňuje na základě různých údajů v procházejících paketech (jako je zdrojová a cílová IP adresa, typ síťového protokolu, zdrojový a cílový port, ...) pakety buď propouštět, nebo zamítnout. Při uplatnění filtrovacího pravidla je možné (dle významu pravidla) zapnout zaznamenání informací o paketu.

Anti spoofing je doplněk k filtrování paketů, který slouží k ochraně lokální sítě proti napadení, při kterém útočník falšuje zdrojové IP adresy.

Pro dosažení vysoké úrovně bezpečnosti obsahuje WinRoute tzv. inspekční modul. Jedná se o speciální ovladač (driver) pracující mezi linkovou a síťovou vrstvou OSI modelu. Ovladač používá originální technologii, která zaručuje, že WinRoute dostává pakety přímo od ovladače síťové karty, tedy ještě předtím, než je dostane jakákoliv jiná komponenta operačního systému.

Umístění inspekčního modulu WinRoute pro kontrolu obsahu paketů v síťové architektuře operačních systémů Windows je zobrazeno na následujícím obrázku.



Použitá terminologie

V následujícím textu jsou použité některé termíny z problematiky síťových technologií, se kterými by se měl čtenář lépe seznámit. Zvláště pak, jestliže hodláte nastavovat filtrování paketů, je vhodné znát význam informací obsažených v hlavičkách paketu.

prostředí TCP/IP

WinRoute je produkt pracující v prostředí protokolů TCP/IP. Protokoly TCP/IP jsou navrženy tak, aby pracovaly ve vrstvách. Protokoly TCP/IP jsou hlavně rozuměny následující protokoly: IP, TCP, UDP, ICMP a další protokoly pracující nad IP.

síťové rozhraní (interface)

Síťovým rozhraním rozumíme takové zařízení, které spojuje počítač s ostatními počítači prostřednictvím určitého média. Síťovým rozhraním tedy může být síťová karta typu ethernet, modem, ISDN karta apod. Prostřednictvím síťového rozhraní počítač přijímá a odesílá pakety.

IP adresa

IP adresa je jedinečné 32-bitové číslo, identifikující v IP sítích počítač. Každý počítač v Internetu má tedy přiřazenu jednu IP adresu, která je jedinečná. Každý paket procházející Internetem obsahuje informaci, z které IP adresy byl odeslán (zdrojová IP adresa) a na jakou IP adresu má dojít (cílová IP adresa).

síťová maska

Síťová maska slouží k zařazení více IP adres do skupiny. Každá podsíť je tvořená skupinou IP adres, které je možné počítačům na dané podsíti přidělovat. Například maska 255.255.255.0 sdružuje 254 IP adres. Na podsíti např. 192.168.1.0 s maskou 255.255.255.0 je tedy možné přiřazovat IP adresy v rozsahu 192.168.1.1 až 192.168.1.254

port

Port je 16-bitové číslo (může nabývat hodnoty od 1 do 65535) využívané protokoly transportní vrstvy - TCP a UDP. Port slouží k adresování aplikace (služby) běžící na počítači. Důvod používaní portů je následující: Pokud by na počítači běžela pouze jedna aplikace pracující se sítí, nebylo by portu zapotřebí a k adresaci by stačila pouze IP adresa. Jelikož však na počítači může běžet více aplikací najednou, je zapotřebí mezi nimi rozlišovat. To se děje prostřednictvím čísla portu. Port je tedy možné chápat jako adresu aplikace na počítači.

paket

Paket je základní komunikační datová jednotka používaná při přenosu dat z jednoho počítače na jiný. Každý paket obsahuje data o určité velikosti. Maximální velikost paketu je závislá na přenosovém médiu a např. v sítích typu ethernet je tato velikost 1500 bytů.

Obsah paketu v každé vrstvě je možné rozdělit na 2 části: hlavičku a datovou část. Hlavička obsahuje řídící informace dané vrstvy a datová část obsahuje data vyšší vrstvy. Podrobnější informace o skladbě paketu je možné najít níže v sekci Filtrování paketů.

Překlad IP adres (NAT)

NAT (Network Address Translation) je možné s výhodou použít v následujících případech:

- automatické zabezpečení lokální sítě
- transparentní připojení sítě, nebo její části přes jednu IP adresu

Automatické zabezpečení je dosaženo díky následujícím skutečnostem: Lokální síť nepoužívá registrované IP adresy, čímž je schovaná vnitřní struktura sítě a není přímo přístupná z Internetu. Pro přístup do lokální sítě je zapotřebí prostředníka, kterým je modul provádějící NAT. Protože si modul NAT pamatuje veškerou komunikaci, která je zahájena z lokální sítě, propustí směrem z Internetu do lokální sítě pouze pakety, které jsou odpovědí na již zahájenou komunikaci. Jiné pakety jsou zamítnuty.

Připojení sítě přes jednu IP adresu je umožněno díky tomu, že modul NAT přepisuje zdrojové IP adresy v paketech odcházejících z počítačů v lokální síti za jedinou adresu, a to adresu počítače, na kterém WinRoute pracuje.

Transparentním připojením sítě je míněna skutečnost, že počítače v lokální síti používají WinRoute jako svoji výchozí bránu (default gateway). Z pohledu stanic to vypadá tak, jako by byly plnohodnotně připojeny do Internetu s registrovanými IP adresami. Přes NAT tedy funguje valná většina aplikací, aniž by bylo zapotřebí něco nastavovat na straně aplikace nebo serveru. Hlavně tím se NAT liší od různých proxy serverů a aplikačních bran, které z principu nemohou některé protokoly nikdy podporovat.

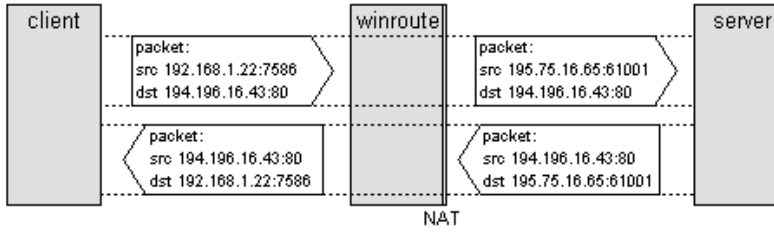
Jak pracuje NAT

Modul, který provádí NAT, pracuje s tabulkou, ve které má zaznamenané informace o každém spojení. Mezi hlavní informace patří tyto: zdrojová IP adresa a port, cílová IP adresa a port, IP adresa a port, kterými jsou pakety upravovány.

Způsob práce NATu si ukážeme na následujícím příkladu:

Uvažujeme, že máme lokální síť, na níž se rozhodne komunikovat počítač s IP adresou 192.168.1.22, z portu 7658 s WWW serverem v Internetu, který běží na IP adrese 194.196.16.43 a portu 80. Komunikace prochází přes WinRoute, který má na vnějším rozhraní IP adresu 195.75.16.65.

Nejdříve počítač 192.168.1.22 odešle paket z portu 7358 na počítač 194.196.16.43 a port 80. WinRoute se podívá do tabulky, zda již záznam existuje nebo ne, podle toho vytvoří nový, nebo použije již existující záznam. Poté modifikuje paket tak, že přepíše v paketu zdrojovou adresu na svoji a změní také zdrojový port. Zdrojová adresa v paketu pak bude 195.75.16.65 a např. port 61001. Poté paket odešle dál. Při příchodu odpovědi je samozřejmě jako cílová adresa 195.75.16.65 a port 61001. WinRoute se podívá do tabulky a podle čísla portu 61001 najde odpovídající záznam. Podle záznamu opraví cílovou adresu a port, tedy na 192.168.1.22 a 7658.



Čísla portů je zapotřebí modifikovat proto, aby když dvě nebo více stanic v lokální síti začne komunikovat ze stejného portu, bylo možné při příchodu paketu z Internetu rozlišit, které stanici paket patří. Porty NAT modul přiděluje v rozsahu od 61000 do 61600. Pro každé spojení je alokován jiný port.

Kritické body NAT

Obecně platí, že aplikace pracují přes NAT naprosto bez problémů, pokud je komunikace zahajována směrem z lokální sítě do Internetu, tak jako tomu je u většiny aplikací. Existují však i aplikace, které jsou špatně navrženy a narušují model klient-server. Tyto aplikace nemusí přes NAT pracovat, nebo jsou některé jejich funkce omezeny. Je to v důsledku toho, že používají více spojení, přičemž další spojení jsou navazována směrem z Internetu a jsou modulem NAT zamítána.

Konfigurace NAT

Základní nastavení

NAT se ve WinRoute zapíná jednoduše jednou volbou ve vlastnostech síťového rozhraní. Toto rozhraní by mělo být vnějším rozhraním, které připojuje lokální síť do Internetu.

NAT se nastavuje v menu:

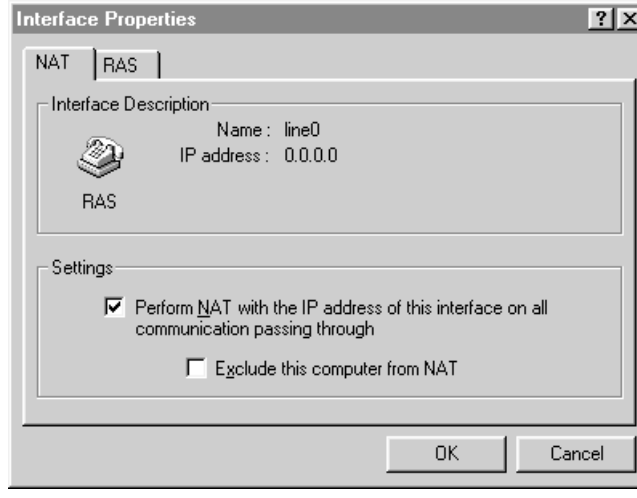
Settings => Interface Table => NAT

- "Perform NAT with the IP address of this interface on all communication passing through"

  Zapíná NAT na rozhraní. Při zapnutí je NAT aplikován na všechny pakety procházející přes toto rozhraní.

- "Exclude this computer from NAT"

  Tato volba říká, zda se má NAT aplikovat také na komunikaci z počítače, na kterém běží sám WinRoute. Jestliže tuto volbu zapnete, nebude NAT aplikován a počítač nebude NATem chráněn. To příliš nedoporučujeme, ale tuto volbu lze například použít, jestliže máte serverovou aplikaci, která má být přístupná z Internetu, ale nemůže pracovat za NATem (prostřednictvím mapovaného portu).



Rozšířené nastavení

Rozšířené nastavení NAT je možné použít v případě, jestliže potřebujete, aby nad částí sítě (segmenty sítě) byl NAT prováděn a nad částí ne. To je zapotřebí například, pokud máte část sítě tvořenou registrovanými IP adresami a je do ní možný přímý přístup z Internetu, a část sítě používá neregistrované adresy. Rozšířený NAT je také možné využít při vytváření demilitarizovaných zón (DMZ), ve kterých běží servery, které jsou přímo přístupné z Internetu. Další speciální možností je možnost specifikovat IP adresu, kterou jsou průchozí pakety NATem modifikovány (implicitně je použita IP adresa rozhraní).

Rozšířené nastavení NAT doplňují již existující nastavení NAT, a proto musí být již zapnut NAT na některém rozhraní. Typickým postupem tedy je, že zapneme NAT na některém rozhraní a potom v rozšířeném nastavení řekneme, kdy se NAT nemá dělat.

Rozšířené nastavení NAT je tvořeno tabulkou pravidel. Pravidla jsou procházena v uvedeném pořadí a při nalezení prvního vyhovujícího pravidla prohledávání končí. Pravidlo vyhovuje, pokud zdrojová a cílová adresa v paketu odpovídá nastavení v pravidlu.

Rozšířené (advanced) nastavení NAT se konfiguruje v menu:

Settings => Advanced => NAT => tlačítko Add/Edit

- "Packet Description"

  Určuje, jaké pakety pravidlu vyhoví. Paket je možné specifikovat na základě zdrojové a cílové adresy. Adresa může být uvedena pro jeden počítač nebo pro skupinu počítačů zadaných buď maskou, rozsahem, nebo pojmenovanou skupinou. Podmínka "Only when outgoing interface is" říká, že pravidlo vyhoví jen tehdy, pokud paket odchází na zadané rozhraní.

- "NAT"

  Stanovuje, co se má s paketem udělat, pokud vyhoví pravidlu. Jsou následující možnosti:

  "Do not NAT" - NAT se nebude provádět

  "Do NAT with specific IP address" - NAT se bude provádět s uvedenou IP adresou.

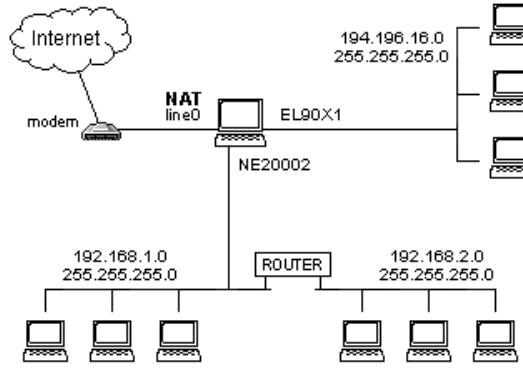
- "Log Packet"

  V případě uplatnění pravidla umožňuje zaznamenání informace. Logování má smysl hlavně v případě ověřování konfigurace či hledání problémů v nastaveni.

Příklad rozšířeného nastavení NAT

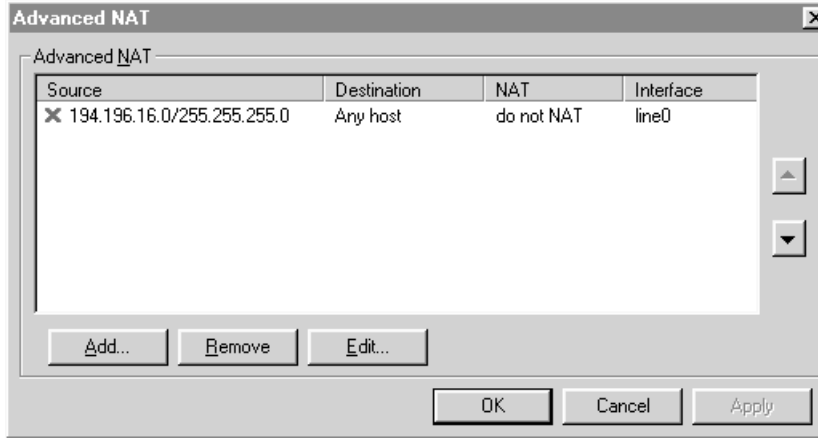
Následující obrázek ukazuje tři sítě:

1. 192.168.1.0 s maskou 255.255.255.0
2. 192.168.2.0 s maskou 255.255.255.0
3. 194.196.16.0 s maskou 255.255.255.0



První a druhá síť používá privátní IP adresy a pro přístup na Internet z těchto sítí se musí použít NAT. Třetí síť používá registrované IP adresy a je přímo přístupná z Internetu.

Nastavení NATu se v tomto případě provede tak, že se na rozhraní vedoucí do Internetu (line 0) zapne NAT a v rozšířeném nastavení NATu se uvede, že s pakety pro třetí síť se nemá NAT provádět. Nastavení rozšířeného NATu je ukázáno na následujícím obrázku:



Mapované porty

Metodou mapování portů je možno vytvořit komunikační kanály do lokální sítě, která je jinak nedostupná díky tomu, že WinRoute provádí překlad IP adres (NAT). Můžete tedy vytvořit veřejně přístupné služby (jako např. WWW server, FTP server apod.), jež jsou pak dostupné všem uzlům Internetu (tedy i stanicím mimo vaši LAN).

Jak fungují mapované porty

Každý paket, který je přijat z externí sítě (z Internetu), je zkontrolován, zda jeho atributy (tedy přenášený protokol, cílový port, příp. cílová IP adresa) neodpovídají hodnotám některé z položek tabulky mapovaných portů (Protocol, Listen Port, příp. Listen IP). Pokud je nalezena shoda u všech těchto atributů, je paket modifikován a odeslán do lokální sítě na stanici, jejíž IP adresa je nastavena jako "Destination IP", a na port, jehož hodnota je nastavena jako "Destination port".

Konfigurace mapovaných portů

Mapované porty se konfigurují v menu:

Settings => Advanced => Port Mapping => tlačítko Add/Edit

- "Protocol"

  Protokol, prostřednictvím kterého bude komunikace mapovaným portem probíhat.

- "Listen IP"

  Pokud je tato položka zadána (její zadaní není povinné), je cílová adresa přicházejících paketů porovnávána s touto hodnotou a paket je propuštěn přes mapovaný port jen v případě, že dojde ke shodě.

- "Listen Port"

  Udává port nebo rozsah, pro který je položka tabulky mapovaných portů vytvářena.

- "Destination IP"

  IP adresa stanice, na kterou jsou pakety, které vyhoví výše popsaným podmínkám mapovaného portu, směrovány.

- "Destination Port"

  Číslo portu cílové stanice, na který jsou pakety směrovány. Tato hodnota je ve většině případů stejná jako Listen Port.

Vybrané užitečné ukázky nastavení mapovaných portů jsou uvedeny v Dodatku.

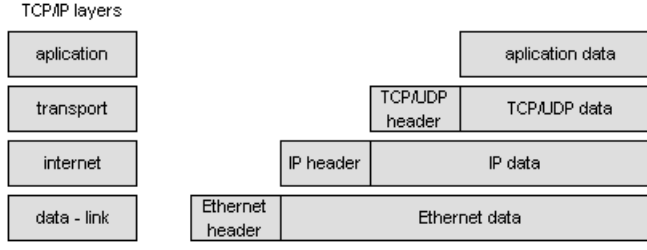
Filtrování paketů

Nastavení filtrovacích pravidel pro ochranu lokální sítě má význam hlavně tehdy, má-li lokální síť přidělené registrované IP adresy a je do ní možný přímý přístup z Internetu. Pokud používáte NAT pro celou vaši síť, není nutné filtrování paketů provádět.

Jak vypadá paket

Abychom mohli nastavovat filtrování paketů, je nutné pochopit, jak je s pakety zacházeno v jednotlivých vrstvách zásobníku protokolu TCP/IP.

Obsah paketu v každé vrstvě je možné rozdělit na 2 části: hlavičku a datovou část. Hlavička obsahuje řídící informace dané vrstvy a datová část obsahuje data vyšší vrstvy. Každá vrstva si tedy přidává svoji hlavičku a výsledné složení paketu tedy vypadá takto:



Na následujících stranách jsou zobrazeny hlavičky jednotlivých protokolů. Šedivá políčka označují data, které je možné využít při filtrování paketů.

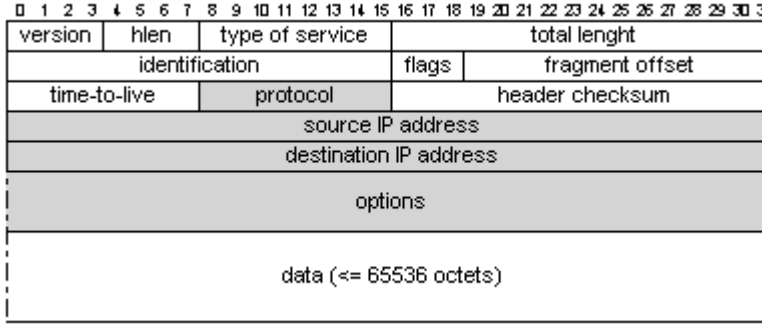
Protokol IP (internetová vrstva)

Protokol IP (Internet Protocol) je základní internetový protokol sloužící k (nespolehlivému) přenosu paketů vyšších vrstev.

Při filtrování je možné uplatnit následující informace:

- zdrojová IP adresa (source IP address)
- cílová IP adresa (destination IP address)
- typ protokolu (protocol) vyšší vrstvy, např.: TCP, UDP, ICMP apod.
- pole IP voleb (IP options)

Formát IP paketu je zobrazen na následujícím obrázku.



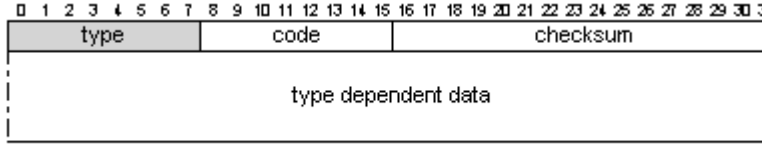
Protokol ICMP (internetová vrstva)

Protokol ICMP (Internet Control Message Protocol) slouží pro přenos chybových a řídících zpráv mezi počítači.

Při filtrování je možné uplatnit následující informace:

- typ ICMP zprávy (type)

Formát ICMP paketu je zobrazen na následujícím obrázku.



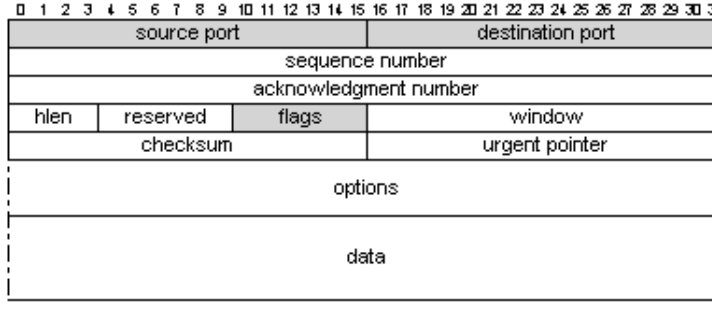
Protokol TCP (transportní vrstva)

Protokol TCP (Transmission Control Protocol) je určen pro spolehlivý přenos aplikačních dat mezi 2 počítači. Stanice spolu komunikují prostřednictvím "spojení". Vytváření spojení, přenos dat a ukončení spojení řídí speciální příznaky obsažené v hlavičce TCP paketu. Pro filtrování TCP paketů má velký význam příznak vytváření spojení, jelikož data nemohou být přenášena dříve, než je spojení úspěšně vytvořeno.

Při filtrování je možné uplatnit následující informace:

- zdrojový port (source port)
- cílový port (destination port)
- příznaky (flags)

Formát TCP paketu je zobrazen na následujícím obrázku.



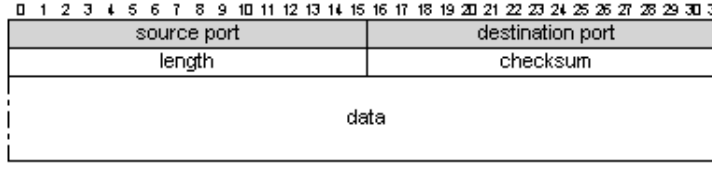
Protokol UDP (transportní vrstva)

Protokol UDP (User Datagram Protocol) nabízí aplikační vrstvě prostředek pro (nespolehlivý) přenos aplikačních dat. Protokol UDP na rozdíl od TCP nevytváří mezi 2 stanicemi spojení a pakety mohou být odeslány kdykoliv na jakoukoliv IP adresu a port.

Při filtrování je možné uplatnit následující informace:

- zdrojový port (source port)
- cílový port (destination port)

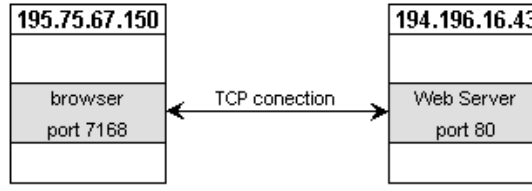
Formát UDP paketu je zobrazen na následujícím obrázku.



Jaká čísla portů používají aplikace

Zjednodušeně, v prostředí Internetu se vyskytují klientské a serverové aplikace. Klientskou aplikací je například WWW prohlížeč a odpovídající serverovou aplikací WWW server. Komunikace probíhá tak, že klientské aplikace se připojují k serverovým aplikacím. Serverové aplikace očekávají spojení na pevně daných portech. Tyto porty mají ve většině případů hodnotu menší než 1024. Naopak, klientské aplikaci většinou nezáleží na čísle portu, pomocí kterého bude komunikovat, a port je tedy volen dynamicky (aplikace požádá operační systém o přidělení nějakého volného portu). Čísla dynamicky zvolených portů jsou větší než 1024.

Komunikace např. prohlížeče a WWW serveru může vypadat takto:



Bezpečnostní politiky

Volba filtrovacích pravidel silně závisí na typu Internetových služeb, které chcete, aby mohli uživatelé v lokální síti používat, a na typu služeb, pro které chcete umožnit přístup z Internetu.

Platí, že příliš restriktivní pravidla mohou znemožnit uživatelům používat určité Internetové služby. Většinou se jedná o uživatelské aplikace, které očekávají navazovaní TCP spojení z Internetu, nebo aplikace, které využívají UDP. Naopak, při benevolentněji nastavených pravidlech může fungovat více aplikací, ale může se snížit míra zabezpečení.

Obecná zásada při nastavování filtrovacích pravidel je, že se snažíte zakázat přístup z Internetu do lokální sítě, zatímco přístup opačným směrem, tj. z lokální sítě do Internetu. ponecháváte volný. Poté, dle druhu využívaných služeb nebo služeb, které chcete nabízet do Internetu, dolaďujete nastavení pravidel. Nejdůležitější je ochrana služeb běžících na počítačích v lokální síti. Tyto služby (např. sdílení souborů, interní WWW server, SQL server a další) většinou poslouchají na portech menších než 1024. Služby poslouchající na portech menších než 1024 nemusí běžet jen na serverech, ale i na obyčejných stanicích, jako je tomu například u sdílení souborů. Uživatelské aplikace naopak využívají pro komunikaci porty větší než 1024. Od portu 1024 se tedy odvíjí nastavení bezpečnostních politik.

Každá rozumná politika zakazuje přístup z Internetu do lokální sítě na porty menší než 1024 pro TCP a UDP protokol. Individuálně je pak možné povolit služby, u kterých si přejete, aby

byly přístupné z Internetu, např. pro službu WWW povolíte protokol TCP a port 80.

Dále pak více restriktivní politika zakazuje veškeré přicházející UDP pakety a zakazuje TCP pakety, které se snaží navazovat spojení z Internetu i na porty větší než 1024. Taková politika tedy zakazuje zahájení jakékoliv komunikace z Internetu do lokální sítě, ale povoluje zahájení komunikace z lokální sítě. Při uplatnění této politiky mohou tedy přestat pracovat (nebo jen částečně, silně závisí na aplikaci) určité aplikace, které například očekávají, že se druhá strana připojí z Internetu na port větší než 1024. Také aplikace používající UDP nebudou pracovat.

Příklady politik:

Při nastavování pravidel je nutné pamatovat na to, že pravidla jsou procházena v zadaném pořadí a při vyhovění prvního pravidla se již další neprovádí.

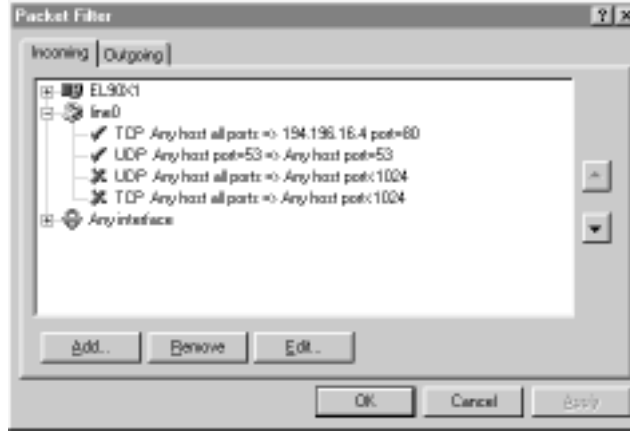
Následující příklady ukazují více a méně restriktivní politiku, kterou můžete uplatnit při nastavování pravidel:

méně restriktivní politika:

Na rozhraní (interface) připojenému k Internetu pro příchozí (incoming) pakety:

- individuálně povolit pakety s portem menším než 1024 pro služby, které chcete nabízet
- povolit UDP pakety přicházející od DNS serverů, tj. se zdrojovým portem 53 a cílovým portem 53
- zakázat TCP pakety s cílovým portem menším než 1024
- zakázat UDP pakety s cílovým portem menším než 1024

Příklad nastavení politiky ve filtru paketů:



více restriktivní politika:

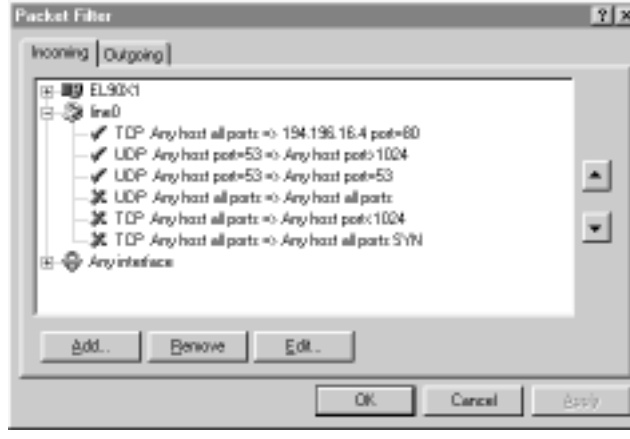
Na rozhraní (interface) připojenému k Internetu pro příchozí (incoming) pakety:

- individuálně povolit pakety s portem menším než 1024 pro služby, které chcete nabízet
- povolit UDP pakety přicházející od DNS serverů, tj. se zdrojovým portem 53 a cílovým portem větším než 1024
- povolit UDP pakety přicházející od DNS serverů, tj. se zdrojovým portem 53 a cílovým portem 53
- zakázat TCP pakety s cílovým portem menším než 1024
- zakázat TCP pakety navazující spojení (všechny porty)
- zakázat UDP pakety (všechny porty)

Pravidlo povolující určitou službu, např. WWW může vypadat takto:

povolit TCP pakety pro cílovou adresu WWW serveru a cílový port 80.

Příklad nastavení politiky ve filtru paketů:



Zamezení přístupu uživatelů na určité služby v Internetu

Filtrování paketů je také možné použít pro omezení přístupu uživatelů z lokální sítě na určité Internetové služby. Omezit lze např. jen některé počítače, dle zdrojové IP adresy. Typ služby, který chcete omezit, se specifikuje číslem cílového portu služby.

Tedy například pro zamezení přístupu na službu FTP (přenos souborů):

Na rozhraní (interface) připojenému k Internetu pro odcházející (outgoing) pakety:

- zakázat TCP pakety s cílovým portem 21

Jestliže provozujete proxy server, na kterém máte nastavené filtrování podle URL a chcete přinutit uživatele, aby jej používali a nepřipojovali se přímo, můžete použít následující pravidla:

Na rozhraní (interface) připojenému k Internetu pro odcházející (outgoing) pakety:

- povolit TCP pakety z adresy proxy serveru a s cílovým portem 80
- zakázat TCP pakety s cílovým portem 80

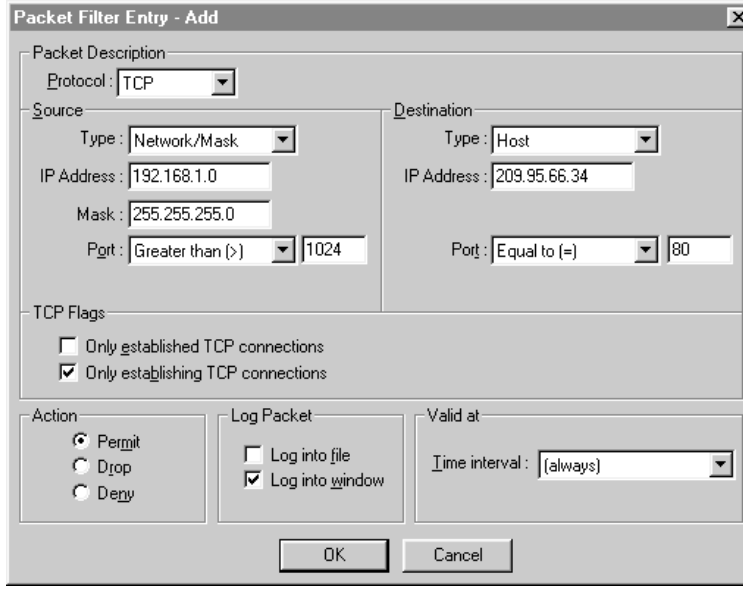
Konfigurace filtrování paketů

Na vstupu a výstupu každého rozhraní je možné nastavit filtrovací pravidla, určující které pakety budou propuštěny. Nastavení se provádí na úrovni IP adres, protokolů a portů.

Zpracování bezpečnostních pravidel probíhá tímto způsobem:

Pravidla jsou procházena v pořadí, v jakém jsou zobrazena. Při příchodu/odchodu paketu se zkontrolují pravidla nejprve pro rozhraní, ze kterého paket přišel, a poté pravidla platící pro každé rozhraní (any). Při nalezení prvního vyhovujícího pravidla se již další nekontrolují a je provedena příslušná akce: paket je buď propuštěn, zahozen nebo zamítnut. Volitelně je možné zvolit záznam informací o paketu do souboru nebo do okna WinRoute.

Pravidlo definuje zdrojovou adresu (rozsah adres, cílovou adresu) rozsah adres, v případě TCP a UDP zdrojový a cílový port. Dále u TCP je možné určit, zda se pravidlo vztahuje pouze k paketům (ne)navazující spojení.



Filtrování paketů se provádí v menu:

Settings => Advanced => Packet Filter => Add/Edit

- "Protocol"

  Síťový protokol. Možnosti jsou: IP, TCP, UDP, ICMP, PPTP.

- "Source", "Destination"

  Definice zdrojové a cílové IP adresy. Adresa může být uvedena pro jeden počítač nebo pro skupinu počítačů zadaných buď maskou, rozsahem, nebo pojmenovanou skupinou.

  V případě protokolu TCP nebo UDP je možné specifikovat zdrojový a cílový port.

- "ICMP type" (pouze v případě protokolu ICMP)

  Specifikování konkrétního typu ICMP zprávy.

- "TCP flags" (pouze v případě protokolu TCP)

  Je možné zadat, při jakém příznaku se pravidlo uplatní:

  "Only established TCP connections": pravidlo vyhoví, pokud se jedná o pakety, které nevytváří nové TCP spojení, tj. nemají nastaven příznak SYN.

  "Only establishing TCP connections": pravidlo vyhoví, pokud se jedná o pakety, které vytváří nové TCP spojení, tj. mají nastaven příznak SYN.

- "Action"

  V případě, že paket vyhoví nadefinovanému pravidlu, je provedena zvolená akce:

  Permit - paketu je povolen průchod do sítě

  Drop - paket je zahozen

  Deny - paket je zamítnut

  V případě zamítnutí paketu je jeho původci odeslán zamítající paket (tj. TCP reset, nebo ICMP port unreachable).

- "Log Packet"

  V případě uplatnění pravidla je možné zaznamenat tuto událost s informacemi o paketu. Záznam může probíhat buď do okna aplikace nebo do souboru.

- "Valid at"

  Stanovuje, v jakém časovém období pravidlo platí. Při zvolení (always) platí pravidlo vždy.

Anti spoofing

Některé síťové služby jsou zabezpečeny na základě IP adresy klienta. Jedná se například o rlogin, NFS (Network File Sharing). Tuto ochranu může případný útočník obelstít technikou nazývanou IP spoofing, která spočívá ve falšování zdrojové IP adresy. Tento způsob útoku je obvykle prováděn v kombinaci se TCP SYN floodingem nebo source routingem. Útočník může ohrozit správné fungovaní služby, nebo může dokonce získat neoprávněně přístup ke službě.

Kontrola spoofingu je prováděna při příchodu paketu. U každého rozhraní se nastavuje, jaké zdrojové IP adresy se mohou v paketech přicházejících na tomto rozhraní objevit. Pakety s jinou zdrojovou adresou jsou zahozeny a případně je proveden záznam do logu.

Filosofie nastavení anti-spoofingu ve WinRoute je tedy následující:

U každého rozhraní připojeného do lokální sítě se nastaví, že zdrojová adresa v příchozích paketech musí patřit do rozsahu adres přímo připojené sítě. Jestliže jsou v síti za nějakým routerem další segmenty sítě, je nutné je nadefinovat jako pojmenovanou skupinu adres a nastavit, že pakety mohou přijít přímo z připojené sítě a z této pojmenované skupiny adres.

U rozhraní připojeného do Internetu pochopitelně není možné vyjmenovat všechny adresy, které se mohou objevit v příchozích paketech. Paket je propuštěn, není-li jeho zdrojová adresa povolena u žádného rozhraní lokální sítě. V příchozích paketech se tedy může vyskytovat jakákoliv jiná zdrojová adresa než ta, která by byla akceptovaná na rozhraních lokální sítě. Tím se zajistí, že do sítě se nepropustí pakety, u nichž je zfalšovaná zdrojová adresa tak, že vypadají jako by přišly z lokální sítě.

Konfigurace anti spoofingu

Anti spoofing se nastavuje v menu:

Settings => Advanced => Anti-Spoofing => tlačítko Edit

- "Any"

  Není prováděna žádná kontrola. Z rozhraní může přijít jakýkoliv paket. Toto je výchozí nastavení po instalaci.

- "From the network connected to this interface"

  Z rozhraní může přijít paket, jehož zdrojová IP adresa patří do sítě přímo připojené k tomuto rozhraní. Obvykle se nastavuje na rozhraní lokální sítě.

- "Only those that are not permited on other interfaces"

  Z rozhraní může přijít paket s jakoukoliv zdrojovou adresou kromě těch, které jsou povoleny na jiných rozhraních. Obvykle nastavuje na rozhraní připojeném do Internetu.

- "or additionally from..."

  Povolené zdrojové adresy jsou specifikované ve vybrané pojmenované skupině adres. Volbu lze využít pouze v kombinaci s předchozími dvěma možnostmi. Tato možnost je potřebná v případě, že v lokální síti jsou ještě nějaké další segmenty.

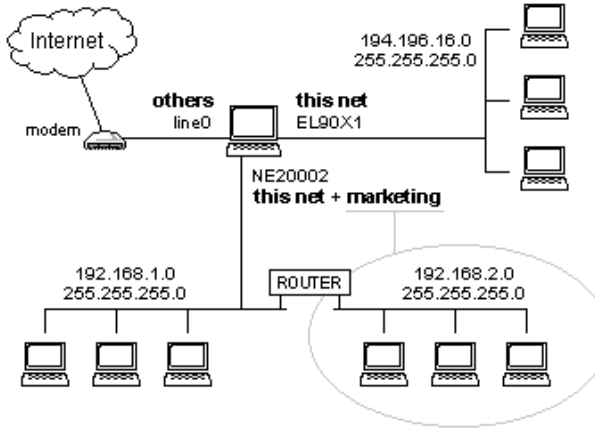
- "Log Packet"

  Záznam porušení pravidla do okna aplikace nebo do souboru.

Příklad nastavení anti spoofingu

Následující obrázek ukazuje tři sítě:

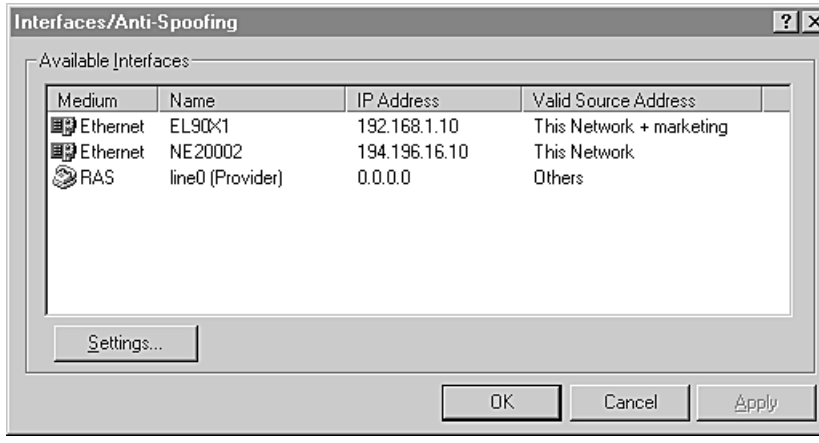
1. 192.168.1.0 s maskou 255.255.255.0
2. 192.168.2.0 s maskou 255.255.255.0
3. 194.196.16.0 s maskou 255.255.255.0

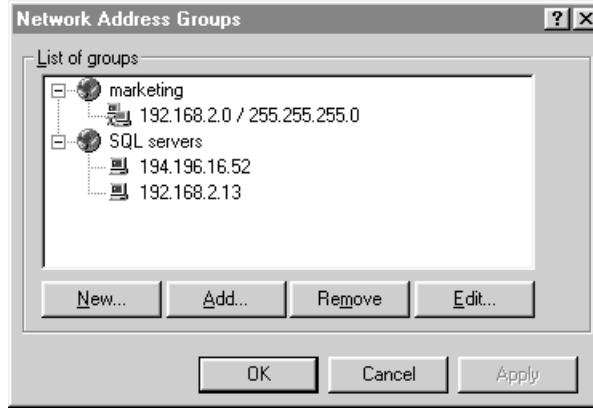


Filozofie nastavení je tato:

- na rozhraní NE20002 mohou přicházet pakety se zdrojovou adresou ze sítě jedna a dva
- na rozhraní EL90X1 mohou přicházet pakety se zdrojovou adresou ze sítě tři
- na rozhraní line0 mohou přicházet pakety s libovolnou zdrojovou adresou, kromě ze sítí jedna, dva a tři.

Nastavení v dialozích vypadá následovně:





Pojmenované skupiny adres a časové seznamy

Pojmenované skupiny adres a časové seznamy lze použít na jiných místech v konfiguraci.

Pojmenované skupiny adres (Address Groups)

Pojmenované skupiny adres je možné uplatnit všude v případech, kdy je zapotřebí specifikovat zdrojovou a cílovou IP adresu, tedy např. při filtrování paketů, v rozšířeném nastavení NAT apod.

Výhody jejich použití jsou následující:

- lze sloučit pod jeden název různé sítě a není tedy zapotřebí při definici zdroje/cíle vyjmenovávat každou síť zvlášť.
- při změně konfigurace sítě (např. přidání nového segmentu, změny IP adres, atd.) stačí upravit pojmenovanou skupinu
- u rozlehlejších sítí je odkazování přes jméno přehlednější

Pojmenované skupiny se nastavují v menu:

Settings => Advanced => Address Groups

Pod každou skupinkou lze vytvořit libovolný počet záznamů. Záznam může být buď jedna IP adresa, skupina IP adres určená síťovou maskou, nebo skupina adres zadaných rozsahem.

Časové intervaly (Time Intervals)

Pro zjednodušení práce s časovými údaji se ve WinRoute používají pojmenované časové intervaly.

Časové intervaly se nastavují v menu:

Settings => Advanced => Time Intervals

Pod každým intervalem lze vytvořit libovolný počet záznamů, což umožňuje velmi flexibilně určit požadovanou dobu.

Časové intervaly lze použít pro následující účely:

- Při plánování stahování a odesílání elektronické pošty (Scheduler).
- Časové nastavení RAS rozhranní - určení doby, kdy lze používat Dial on Demand, případně doby, po kterou se má spojení udržovat trvale nebo je připojení naopak zakázáno.
- Stanovení doby, kdy platí určité pravidlo filtrování paketů. Hodí se například v situaci, kdy potřebujete v některou denní dobu zabránit uživatelům ve vaší síti (nebo její části) v přístupu k některým službám Internetu.

DNS server

Obsah

Úvod

Každý počítač připojený k Internetu je identifikován číselnou IP adresou. Každá stanice, která se chce spojit v rámci Internetu, musí znát adresu partnerského uzlu. Protože IP adresy jsou obtížně zapamatovatelné, byla vyvinuta tzv. Služba doménových jmen (DNS - Domain Name Service). DNS je databáze snadno zapamatovatelných popisných jmen s přiřazenými IP adresami. V Internetu je provozována řada serverů, které tyto DNS služby nabízejí. Uživatel pak nemusí znát IP adresu serveru, se kterým chce komunikovat, ale stačí zadat pouze jeho odpovídající DNS jméno (např. www.seznam.cz) a z DNS databáze se zjistí skutečná IP adresa serveru.

DNS server ve WinRoute

WinRoute obsahuje modul DNS serveru, který je schopen DNS dotazy přeposílat (forwardovat) na zvolený DNS server v Internetu, přičemž výsledky dotazů ukládá do své interní cache, kde jsou po určitou dobu udržovány a následující dotazy jsou pak ihned zodpovězeny na základě obsahu cache bez toho, aby bylo nutno čekat na odezvu DNS serveru v Internetu. DNS server ve WinRoute je také schopen odpovídat na DNS dotazy dle uživatelsky definovaného souboru HOSTS.

Pozn.: Do cache jsou ukládány pouze odpovědi na dotazy Jmenná adresa => IP adresa. Výsledky dotazů jsou uchovávány po dobu zjištěnou z odpovědi DNS serveru.

Konfigurace DNS serveru

V konfiguraci TCP/IP na stanici, která má využívat WinRoute jako DNS server, je třeba nastavit jako adresu DNS serveru adresu stanice, kde WinRoute běží.

Konfigurace DNS serveru se provádí v menu: Settings => DNS Server.

Vzhled konfiguračního dialogu ukazuje následující obrázek:

- "DNS Server enabled"

  Zapnutí DNS serveru ve WinRoute. Vypnutím se znemožní WinRoute fungovat jako DNS server.

- "Enable lookup in HOST file"

  Zapnutím se umožní DNS serveru vytvářet odpovědi na DNS dotazy na základě uživatelsky definovaného souboru HOSTS.

- "Edit HOSTS file..."

  Tímto tlačítkem se spouští externí textový editor, kde je možno editovat soubor HOSTS přímo v prostředí WinRoute.

- "Enable lookup in DHCP lease table"

  Umožní odpovídat na DNS dotazy v závislosti na položce Host name u adres přidělených DHCP serverem. Tato položka je přístupná pouze v případě, že provozujete DHCP server WinRoute. Viz manuál k DHCP serveru.

- "DNS domain"

  Do této položky je možno zadat název domény (např. firma.cz). Tento název pak bude při sestavování odpovědi na DNS jméno připojován k Host name, zjištěném z HOSTS souboru, případně z DHCP lease table.

- "Forward DNS queries to"

  Do této položky je nutno zadat číselnou IP adresu DNS serveru, na který budou DNS dotazy forwardovány. Adresu DNS serveru volte tak, aby odpovídala serveru provozovaného vaším providerem, nebo některému snadno dostupnému serveru.

- "Enable DNS cache"

  Zapíná ukládání odpovědí na DNS dotazy do interní cache. Následující dotazy jsou pak vyřizovány na základě obsahu této cache, bez nutnosti čekat na odpověď od DNS serveru v Internetu.

DHCP server

Úvod

Každá stanice v síti musí mít odpovídajícím způsobem nakonfigurovaný TCP/IP protokol. Znamená to nastavit na všech stanicích IP adresy, masky sítě, adresy výchozí brány a adresu DNS serveru atd. Správce tedy musí ručně tyto hodnoty nakonfigurovat, a to u všech stanic, přičemž si musí udržet přehled o IP adresách, které jsou již přiděleny jiným stanicím, aby nedošlo ke kolizi a následně k nefunkčnosti celé sítě.

Za účelem usnadnění tohoto úkolu byl vyvinut protokol DHCP (Dynamic Host Configuration Protocol), který slouží k dynamické konfiguraci TCP/IP protokolu na klientských stanicích. Stanice pošle při bootování do sítě dotaz, na základě kterého DHCP server přidělí stanici konfigurační parametry TCP/IP protokolu. Jedná se především o IP adresu, masku sítě, výchozí brány (default gateway), adresu DNS serveru, doménového jména stanice apod. Server sestaví odpověď s konfiguračními daty a odešle jej stanici. Konfigurační parametry mohou být serverem přidělovány na omezenou dobu (tzv. lease time). Server vždy přiděluje konfiguraci IP adresy tak, aby nebyla v kolizi s adresou již přidělenou přes DHCP jiné stanici.

Pokud tedy má správce k dispozici DHCP server, stačí zvolit v nastavení TCP/IP na klientských stanicích volbu "Získat adresu IP ze serveru DHCP" a DHCP server převezme odpovědnost za správné nakonfigurovaní TCP/IP protokolu na stanicích, čímž se dají výrazně snížit náklady na údržbu a správu celé sítě.

DHCP server ve WinRoute

WinRoute obsahuje modul DHCP server, což je plnohodnotný DHCP server se schopností přidělovat dynamicky konfiguraci TCP/IP protokolu stanicím. Pokud chcete DHCP server WinRoute využívat, musíte odpovídajícím způsobem nakonfigurovat server

(viz níže) a v konfiguraci TCP/IP na stanicích zapnout volbu "Získávat adresu IP ze serveru DHCP". Pokud nebudete všechny stanice v síti konfigurovat dynamicky pomocí DHCP, ale některé z nich budou nakonfigurovány napevno, musíte zajistit, aby parametry přidělované pomocí DHCP nekolidovaly s pevným nastavením některé stanice.

Konfigurace DHCP serveru

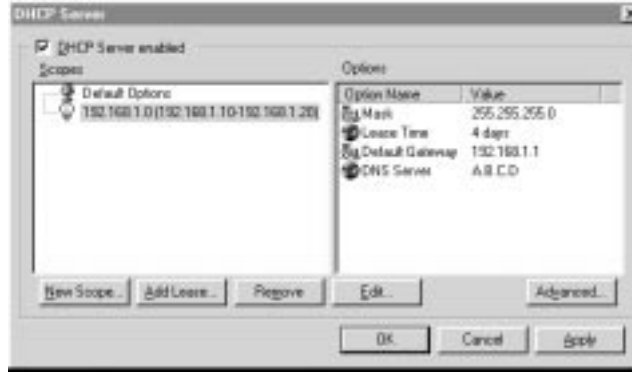
Konfigurace DHCP serveru se provádí v dialogu, který se vyvolá v menu.

Settings => DHCP server

- "DHCP server enabled"

  Zapíná DHCP server ve WinRoute. Po vypnutí se nastavené parametry neztrácí, ale WinRoute již nadále nepracuje jako DHCP server.

V dialogovém okně jsou dvě hlavní pole Scopes a Options:



V poli Scopes se zobrazují rozsahy IP adres přidělovaných klientům (tzv. SCOPE). Zobrazena je síťová adresa rozsahu a první a poslední IP adresa přidělitelná v rámci tohoto scope.

Ke každému scope můžeme navíc dodefinovat další parametry. Tyto parametry jsou pak zobrazeny v poli Options.

V poli Scopes je vždy zobrazena položka "Default Options", což je seznam hodnot parametrů, které jsou přidělovány stanicím v případě, že odpovídající parametr není ve scope nadefinován. To, zda je parametr globální, převzatý z "Default Options", poznáme dle ikony zobrazené u parametru pro daný scope:

- naznačuje, že daný parametr je specifický pro daný scope

- naznačuje, že daný parametr pochází z nastavení "Default Options"

V dolní části dialogu jsou tlačítka:

- "New Scope..."

  Po stisknutí se objeví editační dialog, kde je možno nadefinovat jednotlivé parametry nového scope.

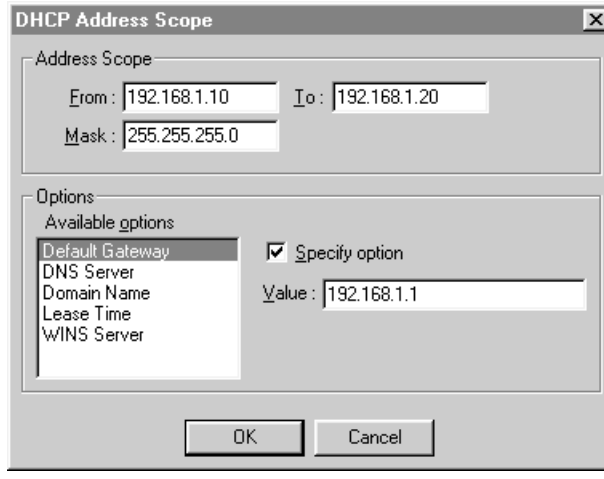
- "Edit..."

  Slouží k nastavení již nadefinovaného scope.

- "Remove"

  Slouží k úplnému odstranění definice scope.

Dialog nastavení scope ukazuje následující obrázek:



- "Address Scope"

  Zde se zadá rozsah IP adres přidělovaných klientům (do položek "From" a "To") a síťová maska do položky "Mask". IP adresy musí být z jednoho společného subnetu.

- „Options"

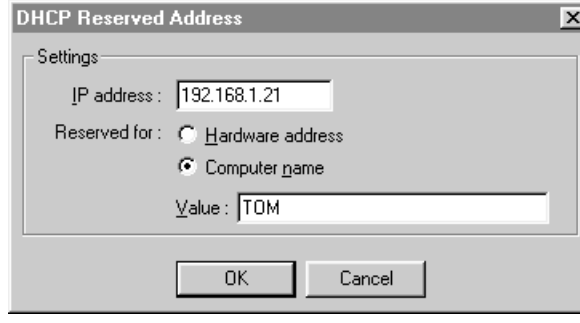
  Zde je k dispozici seznam dalších konfiguračních parametrů přiřazovaných stanicím v rámci daného scope. Pokud některý parametr není zadán (Check box "Specify option" není zvolen), použije se hodnota z Default Options. K dispozici jsou tyto parametry:

  - "Default Gateway"
    IP adresa výchozí brány (routeru), která je prostředníkem při komunikaci se stanicemi v jiných subnetech.
  - "DNS Server"
    IP adresa serveru, který budou stanice používat jako DNS server.
  - "Domain Name"
    Zde můžete vyplnit název své domény, pokud ji máte registrovánu.
  - "Lease Time"
    Udává dobu, po kterou budou stanici konfigurační data přidělena. Po vypršení této doby přestanou být konfigurační data platná a stanice si musí novým dotazem na DHCP server parametry TCP/IP znovu vyžádat.
  - "WINS Server"
    Adresa WINS serveru, který slouží k distribuci potřebných informací v prostředí sítí, kde se sdílí síťové prostředky pomocí Microsoft Network.

V každém scope můžeme rezervovat IP adresu pro určitou stanici pomocí tlačítka "Add Lease...".

Pokud takto rezervujeme IP adresu pro nějakou stanici, je zaručeno, že tato adresa bude vždy vyhrazena pro danou stanici (což je užitečné např. v případě, že na této stanici provozujeme nějakou veřejně přístupnou službu, např. tiskový server).

Dialog pro rezervování adresy ukazuje následující obrázek:



- "IP address"

  Udává adresu, kterou chceme rezervovat.

- "Reserved for"

  Umožňuje navolit, podle čeho má být rozpoznána stanice, pro kterou je IP adresa vyhrazena:

- "Hardware address"

  Stanice je identifikována hardwarovou adresou. Do položky "Value" se adresa zadá jako šestibajtová hodnota, kde jednotlivé bajty jsou odděleny pomlčkou. (Např. 00-60-08-5f-75-b9)

- "Computer name"

  Stanice je identifikována svým názvem, zadávaným v konfiguraci sítě v MS Windows.

Tlačítko "Advanced..."

Slouží k zapnutí funkce, kdy DHCP server odpovídá i na dotazy pomocí protokolu BOOTP, což je starší verze protokolu pro konfiguraci TCP/IP. Tuto funkci zapněte v případě, že ve vaší síti provozujete starší verze klientů, kteří používají protokol BOOTP.

Pozn.: Přehledný seznam adres přidělených pomocí DHCP jednotlivým klientům je možno získat v hlavním logovacím okně WinRoute kliknutím pravým tlačítkem myši a vybráním v menu Show => Leased IPs, příp. stisknutím kombinace kláves CTRL+SHIFT+L

Konfigurace v prostředí vícesegmentových sítí

Aby bylo možno používat DHCP server i v případě vícesegmentových sítí, je nutno nakonfigurovat brány mezi těmito segmenty tak, aby forwardovali DHCP dotazy od klientů na DHCP server, který je umístěný v některém jiném segmentu. Dále následují příklady takové konfigurace pro vybrané typy routerů:

- Windows NT

  Na počítači provozující operační systém Windows NT Server, a který slouží jako IP router, je potřeba nainstalovat službu "DHCP Relay Agent". V konfiguraci TCP/IP pak přepneme na záložku DHCP Relay, kde vyplníme adresu DHCP serveru, na který se mají DHCP dotazy směrovat (tzn. IP adresu stanice, kde běží WinRoute s DHCP serverem).

- Novell Netware

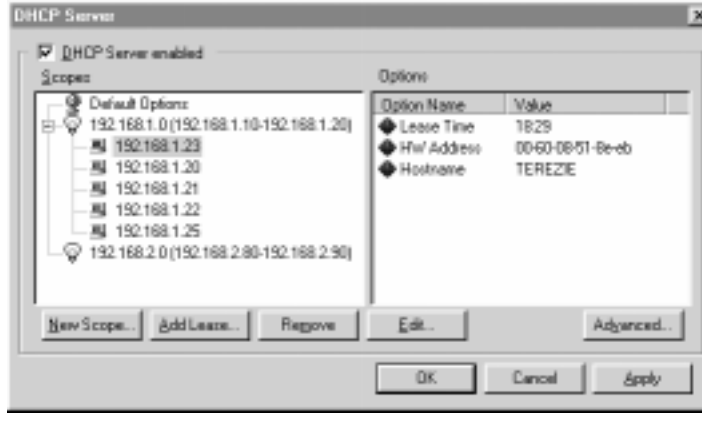
  Na serveru Netware, pokud tento slouží jako IP router, je nutno natáhnout modul BOOTPFWD.NLM, který zajistí přeposílání DHCP a BOOTP dotazů. Syntaxe je:

  load bootpfwd.nlm <IP adresa DHCP serveru>

  Jako IP adresu DHCP serveru zde uvedeme IP adresu stanice, kde běží WinRoute.

Příklad nastavení

Na následujícím obrázku je vidět příklad nastavení DHCP serveru:



Na obrázku jsou nakonfigurovány dva scope, první pro síť 192.168.1.0, druhý pro síť 192.168.2.0. První scope přiděluje adresy z rozsahu 192.168.1.10 až 192.168.1.20, druhý pak z adres o rozsahu 192.168.2.80 až 192.168.2.90.

Na obrázku je dále vidět, že ze scope pro síť 192.168.1.0 jsou již stanicím přiděleny adresy 192.168.1.23, 192.168.1.20, 192.168.1.21, 192.168.1.22 a 192.168.1.25. Ze scope 192.168.2.0 není dosud přidělena žádná adresa.

Kurzor v okně "Scopes" je umístěn na přidělené adrese 192.168.1.23, čímž se zobrazily podrobnější informace jako je doba, po kterou jsou konfigurační parametry dané stanici přiděleny, dále je zde možno vidět, že se jedná o stanici s hardwarovou adresou 00-60-08-51-8e-eb a že hostname stanice je "TEREZIE".

Proxy server

Úvod

Použití proxy serveru přináší následující výhody:

Ukládání procházejících dat do cache

Nejoblíbenější Internetová služba WWW pracuje tak, že data (stránky) vyžádané WWW prohlížečem uživatele jsou přenášena z WWW serverů. Při použití proxy serveru mohou být tato data ukládána do sdílené cache. Cache pracuje tak, že ukládá procházející data do souboru na disku na lokálním počítači. Jestliže si (jiný) uživatel vyžádá stejné WWW stránky, jsou tyto stránky převzaty z cache a není tedy nutno čekat na odezvu vzdáleného WWW serveru v Internetu. Použití cache rovněž zrychluje práci s Internetem a snižuje zatížení linky. Technologie uložení dat do cache je popsána v části „Technologie cache“.

Možnost omezení přístupu ke zdrojům v Internetu

Při použití proxy serveru je možné omezit přístup uživatelů k službě WWW. Je tedy možné např. omezit přístup uživatelů pouze na vybrané WWW servery. Omezení přístupu je možné nastavit individuálně podle jednotlivých uživatelů, nebo podle skupin.

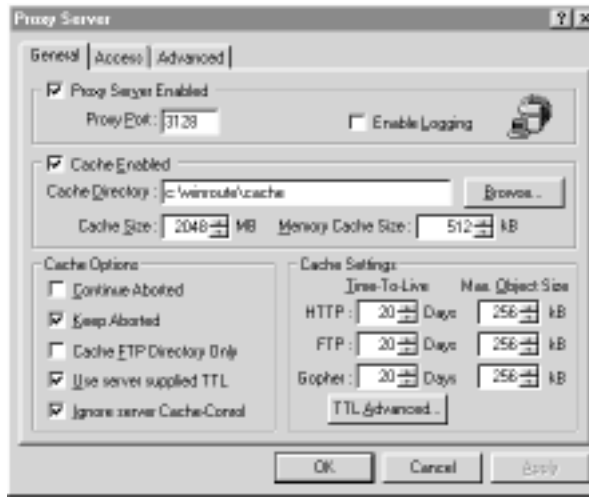
Konfigurace proxy serveru

Konfigurace proxy serveru se provádí v dialogu, který se vyvolá v menu:

Settings => Proxy server...

Konfigurační dialog se skládá z několika záložek.

Záložka General:



- "Port"

  Číslo portu, na kterém proxy server komunikuje s prohlížeči. Standardní hodnota je 3128 a není ji většinou zapotřebí měnit.
- "Enable Logging"

  Zapíná/vypíná generování záznamů o procházejících adresách stránek (URL) do souboru.
- "Cache Enabled"

  Zapíná/vypíná funkci WinRoute jako proxy cache. Jestliže je tato volba vypnuta, nejsou žádná data do cache ukládána.
- "Cache Directory"

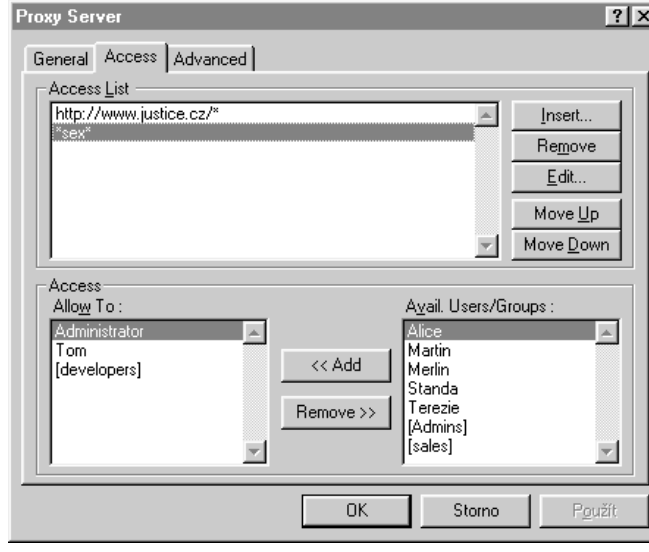
  Adresář pro cache. Do tohoto adresáře ukládá proxy server procházející data.
- "Cache Size"

  Maximální velikost cache v megabytech. Po překročení této velikosti jsou z cache postupně umazávány objekty z nejstarším datem.
- "Continue Aborted"

  Ovlivňuje chování proxy serveru v případě, když uživatel přeruší přenos stránky z WWW serveru (buď tlačítkem stop v prohlížeči, nebo při přechodu na jinou stránku před úplným načtení stránky). V případě, že je tato volba zapnuta, je i takto přerušený download stránky dokončen a stránka je uložena do cache.

- "Keep Aborted"
  Určuje, zda bude do cache uložen i neúplný objekt (html stránka, obrázek). Neúplný objekt může vzniknout přerušením datového spojení v době, kdy je objekt stahován ze vzdáleného WWW serveru.
- "Cache FTP directory only"
  Tato volba řídí, zda se při práci s FTP ukládají do cache pouze obsahy adresářů (volba zapnuta), nebo zda se při downloadu souborů z FTP serveru ukládají i celé stahované soubory (volba vypnuta).
- "Time-To-Live"
  Stanovení doby životnosti pro jednotlivé protokoly. Doba životnosti určuje, jak dlouho mohou zůstat objekty (html stránky, obrázky, ...) v cache uloženy. Doba života se uvádí ve dnech.
- "TTL Advanced"
  Nastavení doby života podle URL. URL se musí uvést ve formátu: scheme://host/path. V URL je možné uvést znak *, nahrazující libovolný řetězec. Např.: *www*, ftp://*.zip
- "Max. Object Size"
  Nastavuje maximální velikost objektu, který může být do cache uložen. Nastavení se provádí pro jednotlivé protokoly.

Záložka Access:



Podrobnosti o záložce "Access" jsou popsány v kapitole Řízení přístupu.

Záložka Advanced:

- "Parent Proxy"
  DNS jméno nebo IP adresa a port nadřazeného proxy serveru. Proxy cache WinRoute pak postupuje tak, že pokud požadovaný objekt nenalezne ve své cache, obrací se na nadřazený proxy server a ten teprve, pokud objekt nenalezne ve své cache, provede jeho načtení. Pokud tedy tuto hodnotu nastavíte, veškeré požadavky budou postoupeny na zpracování nadřazenému proxy serveru.
- "Autoconfig File"
  Jméno souboru usnadňující konfiguraci proxy v Netscape Navigatoru a novějších verzí prohlížeče Internet Explorer. Před vlastním použitím je však nutné tento soubor upravit. Jeho umístění - Configuration location (URL) je: http://<host>:3129/autoconfig , kde <host> je počítač, na kterém běží proxy server.
- "Idle Timeout"
  Určuje čas, po jehož uplynutí bude uzavřeno spojení s klientem, pokud od něj nebudou procházet žádná data.
- "Connect Retry"
  Nastavuje počet pokusů o navázání spojení se serverem v Internetu, pokud předchozí pokusy selhaly.
- "Enable Reverse DNS"
  Zpětný převod IP adres klientů na DNS jména použité pro záznam informací o požadavcích zapisovaných do souboru access.log.

Nastavení klientů

Aby mohl prohlížeč využívat služeb proxy serveru, je zapotřebí v prohlížeči uvést port a IP adresu počítače, na kterém běží WinRoute.

Příklady nastavení pro nejoblíbenější prohlížeče:

Netscape Navigator 2.0, 3.0

1. menu Options -> Network Configuration -> záložka Proxies
2. zvolíme Manual Proxy Configuration
3. stiskneme tlačítko View
4. do políček HTTP Proxy, FTP Proxy a GOPHER Proxy uvedeme IP adresu počítače, kde běží WinRoute, a port nastavíme na 3128.

Netscape Communicator

1. menu Edit -> Preferences -> Advanced -> Proxies
2. zvolíme Manual Proxy Configuration
3. stiskneme tlačítko View
4. do políček pro HTTP, FTP a GOPHER uvedeme IP adresu počítače, kde běží WinRoute, a port nastavíme na 3128.

MS Internet Explorer 3.02 CZ

1. menu Zobrazit -> záložka Možnosti -> tlačítko Připojení
2. zvolíme připojovat se přes proxy server
3. stiskneme tlačítko Nastavení
4. do políčka HTTP uvedeme IP adresu počítače s WinRoute a port nastavíte na 3128.
5. Zaškrtněte volbu pro všechny protokoly používat týž proxy server.

MS Internet Explorer 4.01 CZ

1. menu Zobrazit -> Možnosti sítě Internet -> záložka Připojení
2. zvolíme připojovat se k síti Internet pomocí proxy serveru
3. do políčka Adresa uvedeme IP adresu počítače s WinRoute a Port nastavíte na 3128.

Řízení přístupu

Řízení přístupu umožňuje nastavit, na které servery v Internetu mohou uživatelé přistupovat a na které mají přístup zakázán.

Záložka Access

Kontrola přístupu uživatelů k jednotlivým URL se provádí podle Access Listu. URL jsou uváděny ve formátu scheme://host/path. V URL je možné použít znak "*", který zastupuje libovolný řetězec. Při přístupu na tyto URL je vyžadována autentifikace uživatele. Aby mohl uživatel na tyto adresy přistoupit, musí být uveden v seznamu uživatelů, nebo členem skupiny, kteří mají povolen přístup k této URL. Po přidání nové URL do Access Listu nemá k této URL nikdo přístup.

Omezení uvedená v Access Listu se netýkají uživatelů, kteří jsou členy skupiny Admins.

Stanovení přístupu podle Access Listu je následující:

Při požadavku na stažení stránky (URL) je prohledán Access List na URL, které vyhovují URL požadované stránky. URL v access listu jsou procházena v pořadí, jak jsou zobrazena. Při nalezení prvního vyhovujícího ULR se již další nekontrolují. Pokud žádná URL z Access Listu nesouhlasí s URL požadavku, je požadavek přijat. V opačném případě se proxy server pokusí zjistit z požadavku autentifikační informace - jméno a heslo uživatele. Pokud nejsou v požadavku uvedeny, je uživatel vyzván k jejich poskytnutí. V případě, že tyto informace jsou k dispozici, následuje ověření jména a hesla uživatele. Pokud jsou v pořádku a uživatel se nachází v Access Listu pro danou URL nebo je členem skupiny uvedené v Acceess Listu, požadavek je přijat. V ostatních případech je zamítnut.

Omezení přístupu na web rozhraní WinRoute

Omezit přístup uživatelů na web rozhraní je také možné. Je zde však jedna výjimka, a to že jméno počítače (host) je vždy převedeno na "WinRoute". Potom například omezení přístupu na web rozhraní WinRoute je možné přidáním této řádky do Access Listu : http://WinRoute/admin/*

Pokud hodláte provést omezení přístupu na web rozhraní, nezapomeňte stanovit alespoň jednoho uživatele, který na toto rozhraní bude mít přístup, nebo který je ve skupině Admins.

Poznámky

- Prohlížeče, které nepodporují proxy autentifikaci, mohou proxy server nadále využívat. Je jim znemožněn přístup na URL uvedené v Access Listu. Nejrozšířenější prohlížeče Netscape Navigator a Microsoft Internet Explorer proxy autentifikaci podporují.

- Uživatel je vyzván k zadání jména a hesla pouze jednou při prvním požadavku na přístup na chráněnou stránku. Prohlížeč pak automaticky doplňuje tyto informace s každým dalším požadavkem.

Řízení přístupu - příklady

1. Potřebujeme následující: aby uživatelé, kteří jsou ve skupině [users], směli pouze do těchto domén : domain.cz, work.cz a uživatel boss směl všude. Access List a přístup uživatele / skupiny nastavíme následovně:

Access List	uživatel / skupina
.domain.cz/	[users]
.work.cz/	[users]
*	boss

2. Potřebujeme, aby nikdo nesměl do domény bad.cz :

Access List	uživatel / skupina
.bad.cz/	

Technologie cache

Tato kapitola popisuje pokročilou technologii cache proxy serveru ve WinRoute. Na rozdíl od jiných proxy serverů (včetně Microsoft Proxy serveru a Netscape Proxy serveru) ukládá WinRoute proxy data do jediného souboru předem stanovené velikosti, místo aby používala jeden soubor pro každý uložený objekt. Soubor cache je organizován podobně jako FAT s alokační jednotkou o velikosti 1024 bytů. To umožňuje výrazně snížit velikost obsazeného diskového prostoru. Pro lepší pochopení se podívejte na následující tabulku, která ukazuje typické rozdělení objektů v cache podle velikosti:

Velikost cache: 150 MB		
velikost objektu v kB	počet objektů	% všech objektů
1	5738	17.57
2	5626	17.23
3	4804	14.71
4	3254	9.96
5	2615	8.01
6	1975	6.05
7	1303	3.99
8	962	2.95
9	877	2.69
10	660	2.02
11	596	1.83
12	485	1.49
13	417	1.28
14	298	0.91

Z tabulky je vidět, že 50% všech objektů v cache je menší než 6 kB. Důvodem je to, že WWW stránky obvykle sestávají z více malých objektů (samotná html stráka, ikony, ...). Ukládat každý objekt do samostatného souboru znamená velké plýtvání diskovým prostorem.

Následující výpočet předpokládá nejhorší případ: velký disk naformátovaný 16-ti bitovým FAT. Velikost alokační jednotky je v tomto případě 32 kB.

Skutečná velikost alokovaná na disku běžnou cache s více soubory:

$32 \cdot (5738 + 5626 + 4804 + 3254 + 2615 + 1975 + 1303) = 32 \cdot 25315 = 810080$ kB = **791 MB**

Skutečná velikost obsazená v cache WinRoute:

$5738 + 2 \cdot 5626 + 3 \cdot 4804 + 4 \cdot 3254 + 5 \cdot 2615 + 6 \cdot 1975 + 7 \cdot 1303 = 78464$ kB = **76 MB**

WinRoute potřebuje pro uložení stejného objemu dat 10.4-krát menší prostor.

Mail server

Obsah

Úvod

WinRoute Mail server je možné s výhodou použít pro výměnu elektronické pošty mezi lokální sítí a Internetem, i pro poštu v rámci lokální sítě. WinRoute Mail server pracuje tak, že shromažďuje poštu zaslanou uživateli z lokální sítě a poštu přicházející z Internetu. Dále pak poštu, která je určená pro Internet, odesílá do Internetu a poštu určenou pro lokální uživatele ukládá do jejich poštovních schránek.

V případě připojení lokální sítě přes telefonické připojení (dial-up) je možné stanovit čas, kdy má probíhat příjem a odeslání pošty pro Internet.

Uživatelé v lokální síti mohou použít pro práci s Mail serverem libovolný SMTP/POP3 poštovní klient (MS Internet Mail, Netscape Mail client, MS Exchange, Eudora, Pegasus mail, ...).

Příjem pošty z Internetu

WinRoute Mail Server umožňuje přijímat poštu z Internetu několika způsoby:

Vyzvedávání jednotlivých schránek

WinRoute Mail server umožňuje nastavit vyzvedávání jednotlivých POP3 schránek, které jsou umístěné u poskytovatele, nebo kdekoliv v Internetu. Vyzvednutá pošta je doručena do poštovních schránek uživatelů.

Nastavení vzdálených POP3 schránek se provádí v menu:

Settings => Mail Server => záložka Remote POP3

Při přidání nebo editaci musíte zadat následující položky:

- "POP3 Username"

  Jméno ke vzdálenému POP3 poštovnímu učtu. Toto jméno je obvykle shodné jako část e-mail adresy před znakem "@".

- "Password"

  Heslo ke vzdálenému POP3 poštovnímu učtu.

- "POP3 Server"

  IP adresa nebo DNS jméno POP3 serveru, na kterém je poštovní účet.

- "POP3 Authentication"

  Způsob autentizace (ověření jména a hesla). Jsou podporovány následující dva způsoby: plain text (heslo je posláno nezašifrovaně) a APOP (heslo je zašifrované). Autentizace APOP je bezpečnější, ale nemusí být serverem podporována. Bližší informace vám sdělí váš poskytovatel připojení.

- "Deliver To"

  Určuje, komu se bude pošta doručovat. Jsou následující možnosti:

  - Uživatel nebo skupina

    Pošta se doručí uživateli nebo skupině, které je možné vybrat ze seznamu.

  - Alias

    Pošta se bude doručovat podle zadaného aliasu.

  - E-mail adresa

    Pošta se přepošle na zadanou e-mail adresu.

E-mail adresy přidaných schránek nastavte jako aliasy příslušným lokálním uživatelům (záložka "Aliases"). Bez uvedeného nastavení by pošta na tyto e-mail adresy posílaná z lokální sítě šla přes Internet, namísto aby byla ihned doručena v rámci lokální sítě. Viz příklady nastavení.

Vyzvedávání schránky pro celou doménu

Někteří poskytovatelé umožňují shromažďovat poštu pro celou doménu do jedné (vzdálené) POP3 schránky. Například vlastníte-li doménu firma.cz, potom veškerá pošta adresovaná do domény @firma.cz je ukládána do jedné schránky u poskytovatele.

WinRoute Mail server umožňuje po vyzvednutí schránky roztřídění pošty jednotlivým uživatelům podle hlavičky To:.

Nastavení doménové POP3 schránky se provádí v menu:

Settings => Mail Server => záložka Remote POP3

Nastavení hodnot "POP3 Username", "Password", "POP3 Server", "POP3 Authentication" se provádí stejně jako v předchozím případě. Rozdíl je v případě položky

- "Deliver To"

  kde se vybere <Sorting Rules>

Nastavení třídících pravidel se provádí v menu:

Settings => Mail Server => záložka Remote POP3 => tlačítko Sorting Rules

Při přidání nebo editaci pravidla musíte zadat následující položky:

- "If mail header 'To' contains"

  Určuje obsah hlavičky To: (adresa příjemce), aby pravidlo vyhovělo. Zadaná hodnota je hledána jako podřetězec v hlavičce To. Většinou se zde uvádí email adresa uživatele.
- "Deliver To"

  Určuje, komu se bude pošta doručovat, jestliže pravidlo vyhoví. Jsou následující možnosti:
  - Uživatel nebo skupina

    Pošta se doručí uživateli nebo skupině, které je možné vybrat ze seznamu.
  - Alias

    Pošta se bude doručovat podle zadaného aliasu.
  - E-mail adresa

    Pošta se přepošle na zadanou e-mail adresu.

Dále pak je zapořebí nastavit v Mail serveru jméno domény. To se provádí v menu:

Settings => Mail Server => záložka General

Zaškrtněte volbu "I have Internet domain" a do políčka "Local Domain(s)" uveďte vaši doménu (např. firma.cz). Volba "Use ETRN command" není použita.

Příjem pošty pro doménu

Příjem pošty pro doménu pomocí SMTP je výhodný, jestliže je lokální síť připojena do Internetu nepřetržitě, např. pevnou linkou. V případě, že lokální síť se připojuje do Internetu pomocí telefonického připojení (dial-up), je nutná statická IP adresa a připojovat se v pravidelných intervalech, aby pošta nebyla vrácena odesílateli. MX záznam domény musí ukazovat na IP adresu, na které je přístupný WinRoute Mail server. Pokud se používá NAT, je dále zapotřebí přidat mapovaný port.

Nastavení se v tomto případě provede v menu:

Settings => Mail Server => záložka General

Zaškrtněte volbu "I have Internet domain" a do políčka "Local Domain(s)" uveďte vaši doménu (např. firma.cz).

Volbu "Use ETRN command" je dobré použít, pokud se připojujete přes telefonické připojení a vzdálený SMTP server podporuje tento příkaz. Příkaz způsobí, že pošta nahromaděná pro vaši doménu (po dobu, kdy jste nebyli připojeni) bude ihned odeslána na WinRoute Mail server.

Odeslání pošty do Internetu

Poštu určenou pro odeslání do Internetu ukládá Mail server do výstupní fronty. Ve stanovených okamžicích se připojuje do Internetu a odesílá poštu na zadaný server.

Nastavení se provádí v menu:

Settings => Mail Server => záložka General

- "Relay SMTP server"

  IP adresa nebo DNS jméno SMTP serveru, na který bude odesílána pošta určená pro Internet.

- "Send mail immediately"

  Jestliže je tato volba povolena, bude odchozí pošta odesílána do Internetu ihned, bez uchovávání v poštovní frontě.

Bezchybnost nastavení údajů Mail serveru lze ověřit vyvoláním zpracování pošty přes web rozhraní na stránce Manual.

Stanovení času příjmu a odeslání pošty

Příjem a odeslání pošty je možné plánovat. Například je možné zvolit, v jaký den, v jakou hodinu a minutu se má pošta kontrolovat. Plánování se nastavuje v menu:

Settings => Mail Server => záložka General => tlačítko Scheduling

- "Action"
  Určuje, jaký typ akce se má s poštou provést. Jsou následující možnosti:
  - "Send/Receive Mail" - příjem a odeslání pošty
  - "Send Mail (if any)" - odeslání nové pošty, pokud nějaká je
- "Allow to dial"
  Umožní vytvořit telefonické připojení, pokud je to zapotřebí.
- "Every - At"
  Určuje, zda se má akce provádět v pravidelných intervalech nebo v určitý čas.
- "Valid At"
  Omezení platnosti akce na určitou dobu. Možnosti jsou následující:
  - "Always valid" - Akce je prováděna vždy.
  - "Valid at selected days" - Limituje platnost akce na zvolené dny v týdnu.
  - "Valid at time interval" - Limituje platnost akce na zvolený časový interval. Časové intervaly se nastavují v menu Settings => Advanced => Time Intervals.

    Tuto volbu je výhodné využít pokud např. požadujeme, aby se pošta přenášela každých 15 minut, ale pouze v době od 9:00 do 15:00 hodin v pracovním týdnu.

Aliasy

Aliasy mohou být použity k vytvoření přezdívek uživatelů a pro přesměrování pošty. Aliasy jsou prováděny vždy, když Mail server přijme novou poštu, tj. v následujících případech:

- když je pošta přijata přes SMTP (tj. zaslána uživatelem nebo došlá z Internetu přes SMTP)
- předtím, než je pošta stažená ze vzdálené POP3 schránky doručena do lokální schránky.

Nastavení Aliasů se provádí v menu:

Settings => Mail Server => záložka Aliases

- "Alias"

  Jestliže je adresa příjemce ve zprávě shodná s touto hodnotou, provede se doručení.
- "Deliver To:"

  Stanovuje, komu se zpráva doručí. Jsou následující možnosti:
  - Uživatel nebo skupina

    Pošta se doručí uživateli nebo skupině, které je možné vybrat ze seznamu.
  - Alias

    Pošta se bude doručovat podle zadaného (dalšího) aliasu.
  - E-mail adresa

    Pošta se pošle na zadanou e-mail adresu.

Nastavení uživatelských poštovních klientů

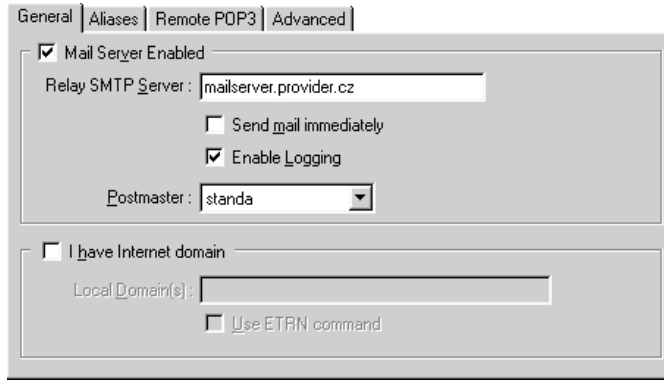
Každý uživatel, který bude pracovat s Mail serverem, musí mít na WinRoute zřízen uživatelský účet. Uživatelské účty se zřizují v dialogu "Accounts" (menu "Settings, Accounts").

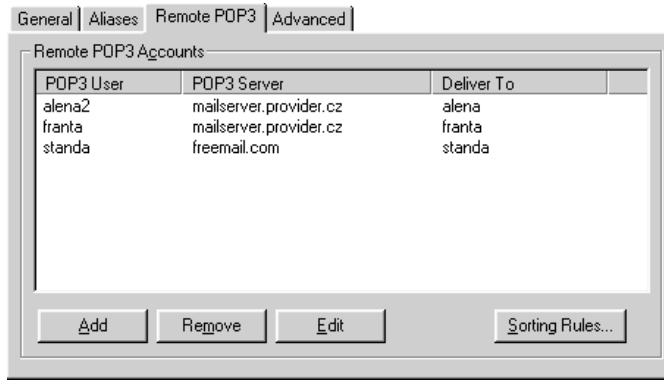
Nastavení poštovního klienta provede uživatel tak, že zadá IP adresu počítače, kde běží WinRoute Mail Server, jako adresu serveru pro odchozí poštu (SMTP) a příchozí poštu (POP3). Jako uživatelské jméno a heslo uvede jméno a heslo k účtu, který má uživatel zřízen na WinRoute.

Příklady nastavení Mail serveru

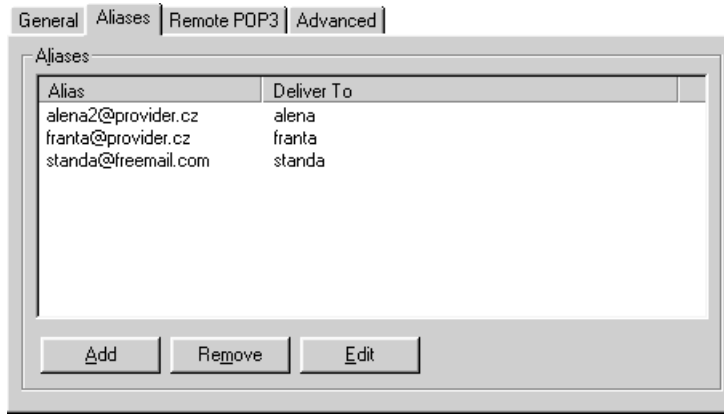
1. Vyzvedávání jednotlivých schránek

Uživatelé mají jednotlivé poštovní schránky u poskytovatele připojení. Pro odchozí poštu je používán poštovní server mailserver.provider.cz.





Dále je vhodné umístit e-mailové adresy uživatelů do aliasů. Je to pro případ, že by si jednotliví uživatelé lokální sítě posílali poštu. Bez tohoto nastavení by WinRoute nepoznal, že dopis je určen pro lokálního uživatele, odeslal by jej do Internetu, a potom by ho opět vyzvedl ze vzdálené poštovní schránky.



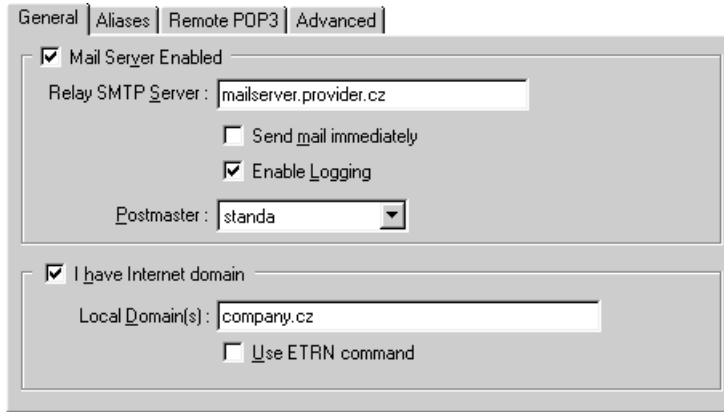
2. Vyzvedávání schránky pro celou doménu

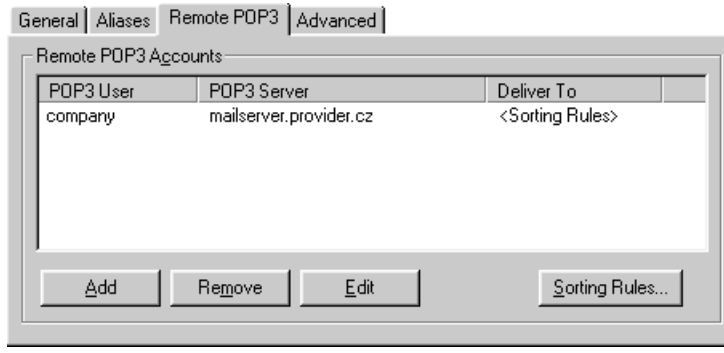
Budeme uvažovat firmu s 5 uživateli. Každý z nich má na WinRoute zřízeno konto; jména jsou následující: alena, martin, standa, tereza a tom.

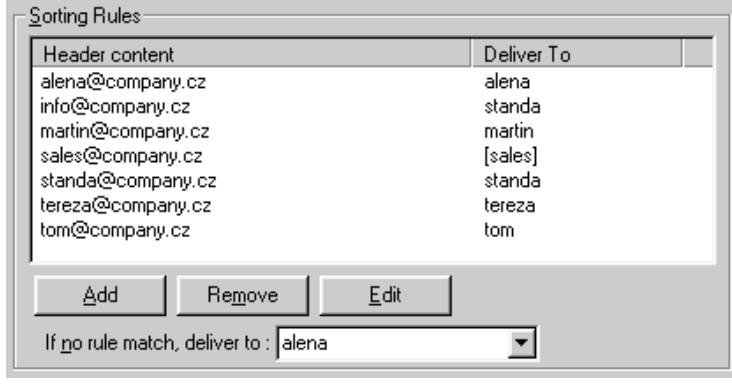
Firma má zaregistrovánu doménu company.cz, poskytovatel Internetu ukládá veškerou poštu pro doménu company.cz do jedné poštovní schránky nazvané company na svém serveru mailserver.provider.cz. Stejný poštovní server je používán i pro odesílání pošty.

Firma chce využívat obecné adresy info@company.cz a sales@company.cz. Pošta směrovaná na adresu info@company.cz má být doručena uživateli standa, pošta směrovaná na adresu sales@company.cz má být doručena členům skupiny sales.

Na záložce General se zaškrtne volba I have Internet domain a do políčka Local Domain(s) se uvede company.cz.







Pošta, pro kterou nevyhoví žádné pravidlo v sorting rules, bude předána uživateli alena. V případě, že by nebyl zvolen žádný uživatel, kterému je doručována tato pošta, je dopis předán uživateli postmaster nastavenému na záložce General.

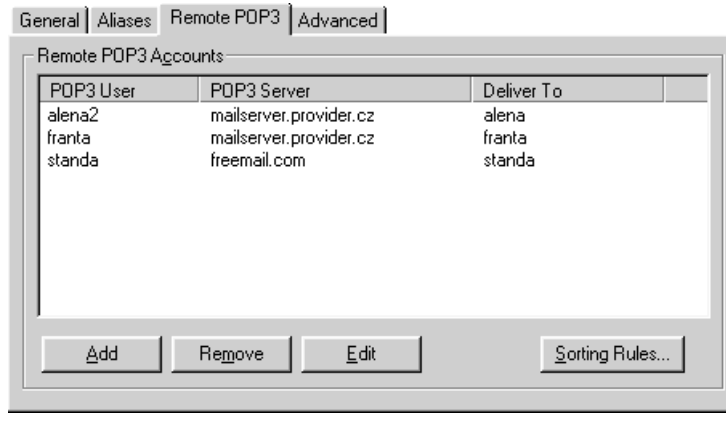
3. Příjem pošty pro doménu

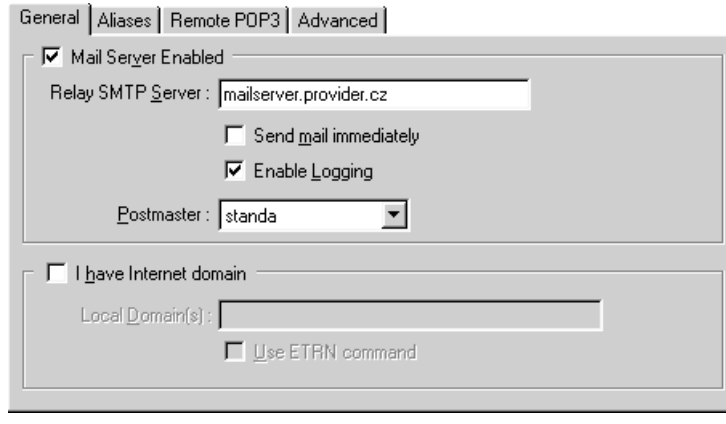
Budeme uvažovat podobnou firmu jako v předchozím příkladu, tedy firmu s 5 uživateli, z nichž každý má na WinRoute zřízeno konto; jména jsou následující: alena, martin, standa, tereza a tom.

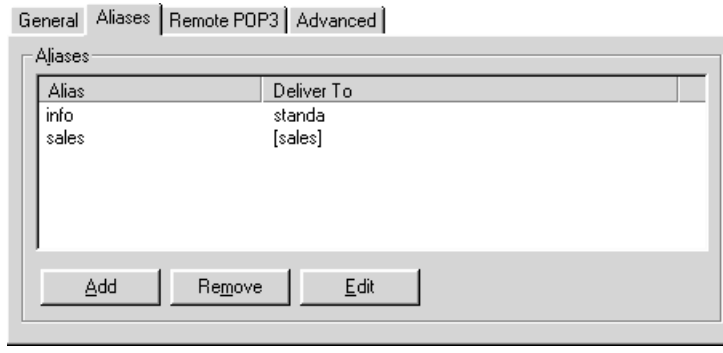
Firma má zaregistrovánu doménu company.cz, a pošta pro doménu bude přijímána pomocí protokolu SMTP. V tomto případě je nutné mít přidělenou pevnou IP adresu, tzn. při každém připojení stejnou. Poskytovatel internetu nasměruje MX záznam pro doménu

company.cz na tuto pevnou IP adresu. Adresa poštovní serveru poskytovatele je mailserver.provider.cz.

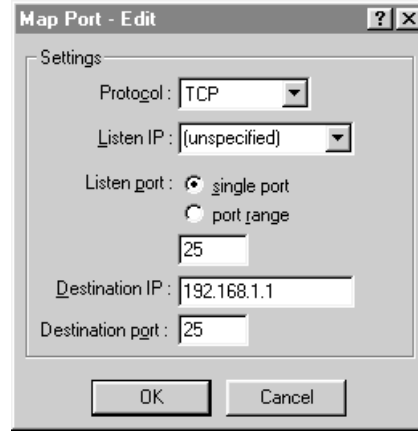
Firma chce využívat obecné adresy info@company.cz a sales@company.cz. Pošta směrovaná na adresu info@company.cz má být doručena uživateli standa, pošta směrovaná na adresu sales@company.cz má být doručena členům skupiny sales.







V případě, že svoji síť chráníte NATem (Network Address Translation), je nutné pro tento způsob příjmu pošty vytvořit mapovaný port (menu Settings - Advanced - Mapped ports).



192.168.1.1 je IP adresa počítače, na kterém běží WinRoute.

Dodatky

Obsah

Směrování (Routing)

Směrování je proces, který řídí, jakými cestami (přes jaké počítače) musí paket při cestě od odesílatele k příjemci projít.

Z pohledu směrování lze počítače rozdělit na dvě skupiny:

- Stanice

  Mají většinou jeden síťový adaptér a nepřeposílají pakety z jednoho rozhraní na jiné. Obsahují směrovací tabulku, ale využívají ji pouze pro odesílání vlastních paketů. Ve směrovací tabulce mají obvykle nastaven implicitní směr na směrovač, ke kterému jsou přímo připojeny.

- Směrovače (routery, gatewaye)

  Obsahují více síťových adaptérů (rozhraní). Síťová rozhraní slouží k propojení dvou nebo více sítí. Při příchodu paketu z jedné sítě se rozhodují, na jaké rozhraní bude paket dále odeslán. O tom, na jaké rozhraní se paket přepošle, se rozhoduje na základě cílové IP adresy v paketu a směrovací tabulky (routing table), kterou si udržuje počítač.

Počítač, na kterém běží WinRoute, pracuje jako směrovač.

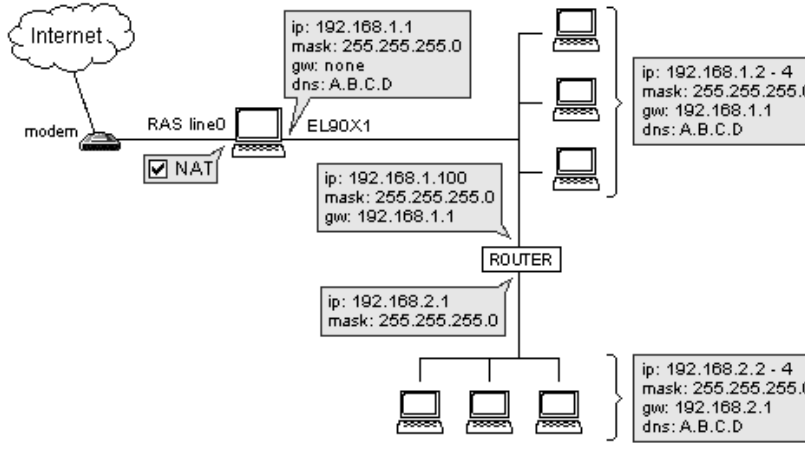
U jednodušších případů sítí, jako například jedné lokální sítě připojené do Internetu přes modem, není zapotřebí směrovací tabulku na počítači s WinRoute upravovat. Směrovací tabulku ale může být zapotřebí upravit v případě, pokud se jedná o rozsáhlejší síť s více segmenty.

Nastavení směrování u sítě s více segmenty

V případě rozsáhlejších sítí s více segmenty, které se nacházejí za dalšími směrovači, může být zapotřebí (jestliže síť nepoužívá některý směrovací protokol) ručně přidat směry na jednotlivé segmenty.

Následující příklad ukazuje síť se dvěma segmenty odělenými routerem.

Nastavení směrování v tomto případě je následující:



- Na počítači s WinRoute musí být uveden směr do segmentu 192.168.2.0. To je možné provést z příkazového řádku následovně:

  c:\route -p add 192.168.2.0 mask 255.255.255.0 192.168.1.100

- Na routeru 192.168.1.100 musí být nastaven implicitní směr (default route) na adresu počítače s WinRoute, tedy 192.168.1.1.

Směrování v prostředí Windows

Tato kapitola detailněji popisuje směrování s ohledem na prostředí operačních systémů Windows.

Směrovací tabulka

WinRoute pracuje se směrovací tabulkou, kterou udržuje operační systém. Výpis směrovací tabulky je možné získat ve WinRoute stisknutím pravého tlačítka myši a vybráním "Show" => "Routing Table".

Pro práci se směrovací tabulkou se používá systémový příkaz "route", který se zadává z příkazové řádky.

Příkaz route je možné použít následujícím způsobem:

- route print (vypíše obsah směrovací tabulky)
- route add (přidání směru)
- route delete (odebrání směru)

Jak již bylo řečeno, směrovací tabulka slouží ke stanovení rozhraní, na které bude paket poslán. Hlavní položky směrovací tabulky jsou:

- síť/maska
- metrika
- rozhraní
- brána

Při rozhodování, na které rozhraní se paket pošle, je uplatněn následující algoritmus:

Projdou se všechny záznamy ve směrovací tabulce a vybere se záznam, u kterého odpovídá síť a cílová IP adresa v paketu (při kombinaci s maskou). Pokud vyhoví záznamů více, má přednost záznam s vyšší hodnotou masky. Jestliže je stále více záznamů, uplatní se záznam s nižší metrikou.

Paket se pošle na rozhraní uvedené v příslušném záznamu. Jestliže se cílový počítač ještě nenachází přímo na síti připojené k vybranému rozhraní, pošle se paket na počítač uvedený jako brána.

Zvláštní význam má záznam s nulovou hodnotou sítě a masky, označovaný za implicitní směr (default route). Tento záznam říká, přes jaké rozhraní bude paket poslán, pokud nevyhoví žádný jiný záznam.

Položky směrovací tabulky lze rozčlenit podle jejich původu:

- přímé (direct)

  Tyto směry jsou do tabulky vloženy na základě IP adresy a masky přidělené jednotlivým rozhraním a identifikují přímo připojené sítě.

- trvalé (persistent)

  Identifikují sítě, které nejsou přímo připojené k rozhraní. Jsou většinou zadány uživatelem a obnovující se při startu operačního systému.

- dočasné (temporary)

  Směry zadané uživateli nebo přijaté pomocí směrovacích protokolů. Při vypnutí počítače jsou zapomenuty.

Obsah směrovací tabulky Windows je po startu sestaven takto:

Jsou vytvořeny přímé směry a z registry načteny trvalé směry (trvalé směry lze nastavit pouze pod windows NT). Jsou také přidány implicitní směry, které se v nastavení TCP/IP protokolu jednotlivých síťových adaptérů označují jako brány. Jestliže však máte více síťových adaptérů, má smysl nastavit tuto bránu pouze u jednoho adaptéru, a to u toho, který připojuje počítač k vnější síti (Internetu).

V průběhu činnosti se upravuje směrovací tabulka následovně:

Tabulka se upravuje podle zásahů uživatele nebo podle směrovacího protokolu (např. RIP), pokud se používá. Jestliže se připojíte telefonickým připojením, přidají Windows v závislosti na nastavení příslušné položky telefonického připojení implicitní směr. Jestliže je již nějaký implicitní směr v tabulce, je mu zvednuta metrika, takže přednost bude mít směr telefonického připojení. Při odpojení je směr opět zrušen.

Příklady mapování portů

Zatímco uvedené příklady neohrožují nijak výrazně bezpečnost lokální sítě, je třeba pamatovat na to, že mapované porty umožňují (omezený) přístup do lokální sítě, neboť mapované porty jsou přístupné z celého Internetu. K omezení přístupu na mapovaný port je možné použít filtrování paketů a omezit tak přístup jen na některé adresy.

WWW

Předpokládejme, že máte ve vaší privátní síti WEB server (dejme tomu na adrese 192.168.1.10) a chcete jej zpřístupnit uživatelům v Internetu. Je tedy nutno vytvořit mapovaný port, a to takto:

Protocol :TCP

Listen IP: <unspecified>

Listen Port: 80

Destination IP: zde zadáte IP adresu stanice, kde WEB server běží (v našem případě je to 192.168.1.10)

Destination Port: 80

SMTP

Máte-li ve vaší LAN Mail server a chcete-li přijímat poštu z Internetu pomocí SMTP protokolu, přidejte následující položku do tabulky mapovaných portů:

Protocol: TCP

Listen IP: <unspecified>

Listen Port: 25

Destination IP: zde zadejte IP adresu počítače, na kterém Mail server běží

Destination Port: 25

PPTP

Pokud provozujete Point to Point Tunneling Protocol server ve vaší LAN a chcete umožnit uživatelům z Internetu připojovat se k vašemu serveru přes PPTP, musíte vytvořit následující dva mapované porty:

1. **pro řídící spojení:**
   Protocol: TCP
   Listen IP: <unspecified>
   Listen Port: 1723
   Destination IP: IP adresa vašeho PPTP serveru
   Destination Port: 1723

2. **pro GRE (PPTP) pakety:**
   Protocol: PPTP
   Listen IP: <unspecified>
   Destination IP: opět IP adresa vašeho PPTP server

CU-SeeMe

V základní konfiguraci byste neměli mít problém při vytváření spojení s jinými uživateli CU-SeeMe. Pokud ale chcete mít možnost přijímat volání od jiných uživatelů, musíte vytvořit následující mapované porty:

Protocol: UDP

Listen IP: <unspecified>

Listen Port: 7648

Destination IP: IP adresa vaší stanice, kde provozujete CU-SeeMe klienta

Destination Port: 7648

Protocol: UDP

Listen IP: <unspecified>

Listen Port: 7649

Destination IP: IP adresa vaší stanice, kde provozujete CU-SeeMe klienta

Destination Port: 7649

Omezení:

- v současné době není možno provozovat v jednom okamžiku více CU-SeeMe klientů na jedné LAN (pochopitelně neplatí pro routovanou síť)
- není možno se připojovat na "reflector" chráněný heslem.

ICQ

Připojovat se na ICQ server a komunikovat s ostatními uživateli (tzn. posílat zprávy, navazovat chat či posílat soubory) by neměl být problém, aniž byste museli vytvářet mapované porty. Pokud chcete mít možnost přijímat volání od jiných uživatelů, musíte vytvořit následující položku v tabulce mapovaných portů:

Protocol: TCP

Listen IP: <unspecified>

Listen Port: 5000 - 5011

Destination IP: IP adresa stanice, kde provozujete ICQ klienta

Destination Port: 5000 - 5011

V ICQ "Preferences" pak vyberte "Connection", "I'm using a permanent internet connection (LAN)", "I'm behind a firewall or proxy". V nastavení "Firewall Settings" vyberte "I don't use a SOCKS Proxy server ...", stiskněte tlačítko "Next", vyberte "Use the following

TCP listen ports for incoming event" a zadejte rozsah od 5000 do 5011.

Z výše uvedeného vyplývá, že pokud chcete provozovat ve vaší LAN více ICQ klientů (a tito mají mít možnost přijímat volání od jiných uživatelů), musíte vytvořit položku v tabulce mapovaných portů pro porty např. 5012 - 5023 a odpovídajícím způsobem nastavit i klienta. To opakujete pro všechny klienty vaší LAN, ale vždy s jiným rozsahem portů...

Využití WinRoute s technologií DirecPC

Následující popis předpokládá, že jste s technologií DirecPC již dostatečně obeznámeni a máte odpovídající softwarové moduly nainstalované a funkční.

WinRoute umožňuje spolupráci s DirecPC dvěma způsoby v závislosti na tom, jakým způsobem jsou odesílány pakety do Internetu:

- Pakety odesílá DirecPC software (DirecPC Navigator).
- Pakety jsou odesílané WinRoutem přes zvolené rozhraní.

V obou případech při používaní DirecPC je zapotřebí, aby byl spuštěný DirecPC software (DirecPC Navigator).

V druhém případě je zapotřebí vybrat rozhraní pro odesílání paketů (u rozhraní typu

Settings => Interfaces => interface Settings => DirecPC

- "Send outgoing packets through"

  Vybírá způsob odesílání paketů. Pro odesílání paketů přes zvolené rozhraní zvolte "Through interface" a vyberte požadované rozhraní.

- "GW"

  V případě zvolení rozhraní typu Ethernet je zapotřebí do uvedeného políčka zadat IP adresu routeru/gatewaye na síti připojené k vybranému rozhraní.

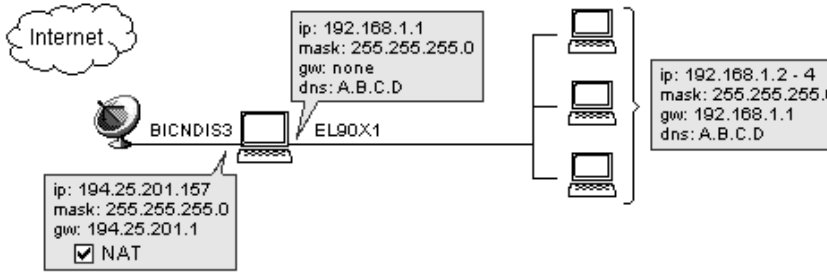
- "DirecPC Gateway"

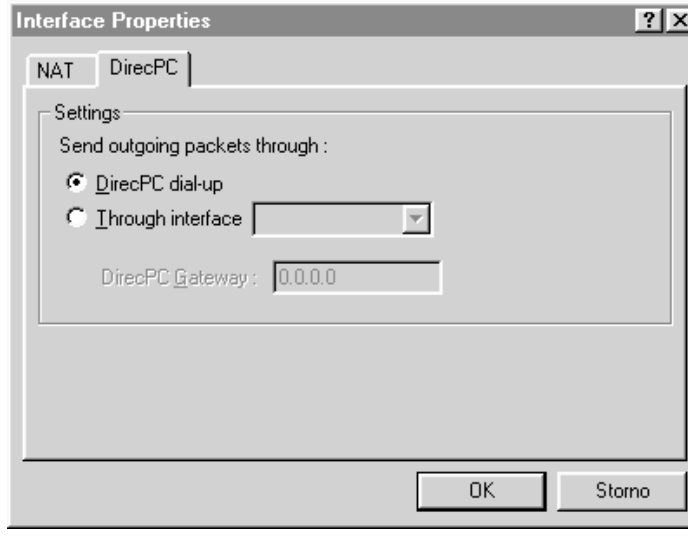
  IP adresa DirecPC Gatewaye. Tato hodnota je stejná jako ta, kterou uvádíte v nastavení DirecPC software. Pokud vám tato adresa není známa, obraťte se na svého dodavatele DirecPC.

DirecPC). To lze provést v menu:

Jestliže vyberete rozhraní typu RAS, pak v nastavení TCP/IP dané RAS položky nesmí být zaškrtnuta volba "Použít výchozí bránu vzdálené sítě".

Příklad nastavení 1

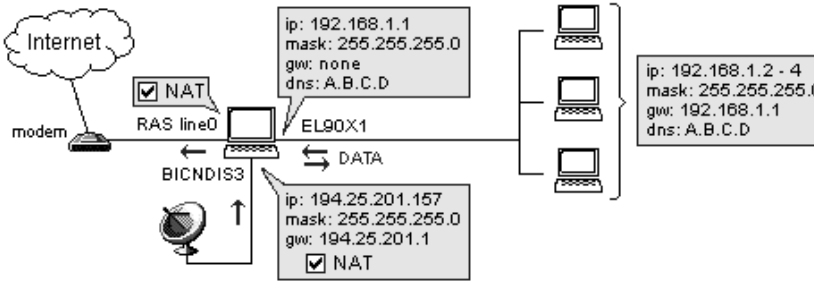


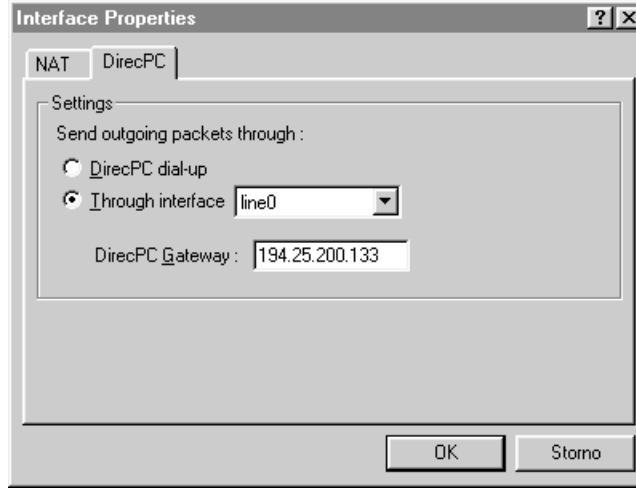


Následující obrázek ukazuje nastavení sítě při použití prvního způsobu (pakety jsou odesílány do Internetu přes DirecPC software (DirecPC Navigator).

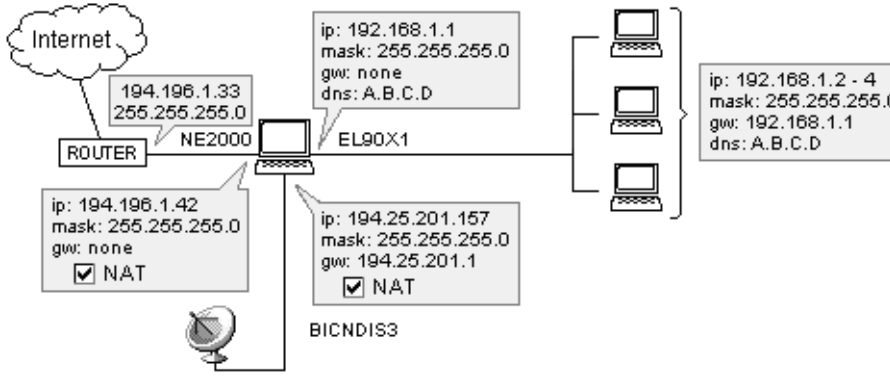
Příklad nastavení 2

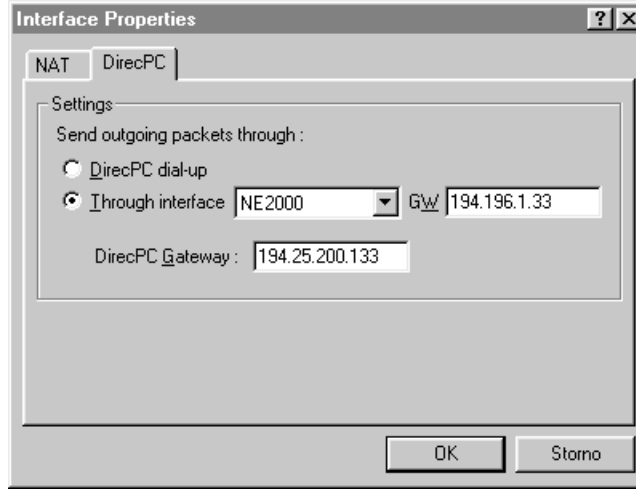
Následující obrázek ukazuje nastavení sítě při použití druhého způsobu: pakety jsou odesílány do Internetu přes rozhraní RAS. K tomuto rozhraní může být připojen například





modem nebo ISDN adaptér. V nastavení TCP/IP dané RAS položky nesmí být zaškrtnuta volba "Použít výchozí bránu vzdálené sítě", jinak bude veškerý provoz směrován na RAS adaptér a DirecPC bude mimo provoz !!





Příklad nastavení 3

Následující obrázek ukazuje nastavení sítě při použití druhého způsobu: pakety jsou odesílány do Internetu přes rozhraní typu Ethernet.

Klávesové zkratky ve WinRoute

Ctrl + Shift + I - Interface table
Ctrl + Shift + R - Routing table
Ctrl + Shift + Q - Queue table
Ctrl + Shift + N - NAT table
Ctrl + Shift + L - Leased table
Ctrl + Shift + C - DNS Cache
Ctrl + Shift + S - Statistic

Ctrl + I - Interfaces/NAT
Ctrl + D - Simple DNS Server

Ctrl + H - DHCP Server
Ctrl + F - Packet Filter
Ctrl + A - Interfaces/Anti-Spoofing
Ctrl + M - Port Mapping
Ctrl + N - Advanced NAT
Ctrl + G - Network Address Group
Ctrl + T - Time intervals
Ctrl + L - RAS Lines
Ctrl + S - Configuration dump

Doporučená literatura

Windows NT Server Resource Kit, Microsoft Press, český překlad Computer Press

Interworking pomocí TCP/IP, Pavel Šmrha, Vladimír Rudolf, nakladatelství KOPP, 1994 ISBN 80-85828-09-X

Konfigurace a správa sítí TCP/IP (TCP/IP Network Administration), Graig Hunt, O'Reilly, 1992, český překlad Computer Press, 1997, IBSN 80-7226-024-3

Firewally - Principy budování a udržování (Building Internet Firewalls), D. Brent Chapman, Elizabeth D. Zwicky, O'Reilly, 1995, český překlad Computer Press, 1998, IBSN 80-7226-051-0