kapitola

6

# Řešení problémů s protokolem TCP/IP

Obsah kapitoly:

V 90. letech společnost Microsoft výrazně zlepšila škálovatelnost svých síťových služeb uvedením zcela přepsaného zásobníku protokolu TCP/IP. Návrh nového zásobníku protokolu TCP/IP přináší mnohá zlepšení výkonu a usnadnění správy. Jedná se o vysoce efektivní implementaci oborového standardu protokolu TCP/IP.

S každou generací systému Microsoft® Windows® se implementace zásobníku protokolu TCP/IP společnosti Microsoft vyvíjí a zahrnuje nové funkce a služby, které zlepšují výkon, zabezpečení a spolehlivost. Zásobník protokolu TCP/IP pro operační systém Microsoft® Windows Server™ 2003 poskytuje vlastní optimalizaci, lepší škálovatelnost, snadnější správu, vyšší rychlost a silnější zabezpečení. Zásobník protokolu TCP/IP a jeho přidružené služby jsou součástí výchozí instalace a již je nelze odinstalovat pomocí funkce Network Connections.

Stejně jako v předchozích verzích serverových operačních systémů Windows jsou k dispozici různé nástroje pro diagnostiku a opravy, které pomáhají rychle izolovat a vyřešit komunikační problémy protokolu TCP/IP. Kromě nástrojů zahrnutých v předchozích verzích systému Windows Server byly doplněny nové nástroje a funkce, které usnadňují řešení komunikačních potíží protokolu TCP/IP.

V této kapitole se budeme zabývat různými nástroji pro řešení potíží, které jsou součástí systému Windows Server 2003, a představíme základní strukturu, která umožňuje řešit komunikační potíže týkající se protokolu TCP/IP.

# 6.1 Přehled komunikačních procesů protokolu TCP/IP

Protokol TCP/IP používá při navázání komunikačního spojení v rámci sítě nebo mezi samostatnými sítěmi pevně určený postup. Před odesláním prvního paketu, který naváže komunikační relaci, provede protokol TCP/IP odesílajícího hostitele čtyři oddělené kroky:

1. Protokol TCP/IP přeloží název hostitele nebo název NetBIOS na adresu IP.
2. Pomocí cílové adresy IP a tabulky směrování IP určí protokol TCP/IP použité rozhraní a adresu IP dalšího směrování.
3. V případě jednosměrového provozu IP nebo technologií sdíleného přístupu, jako je např. Ethernet, Token Ring a optické rozhraní FDDI (Fiber Distributed Data Interface) přeloží protokol ARP (Address Resolution Protocol) adresu IP dalšího směrování na adresu MAC (media access control), která se také označuje jako *adresa datové linkové vrstvy*.

   Pokud se používá vícesměrový provoz IP v sítích Ethernet a FDDI, je cílová adresa IP vícesměrového vysílání mapována na příslušnou adresu MAC vícesměrového vysílání. U vícesměrového provozu IP v sítích Token Ring se používá funkční adresa `0xC0-00-00-04-00-00`. Jestliže se jedná o všesměrový provoz v technologiích sdíleného přístupu, je adresa MAC mapována na adresu `0xFF-FF-FF-FF-FF-FF`.
4. Potom je odeslán datagram IP na adresu MAC, která je přeložena protokolem ARP, na mapování vícesměrového vysílání nebo na adresu všesměrového vysílání na úrovni MAC.

**Poznámka** Podrobné technické informace o protokolech a službách TCP/IP a jejich implementaci v systému Windows Server 2003 naleznete v knize *Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference* (Technická referenční příručka protokolů a služeb TCP/IP v systému Microsoft Windows Server 2003) autorů Joseph Davies a Thomas Lee (Microsoft Press, 2003).

# Komunikační proces protokolu TCP/IP

Zásobník protokolu TCP/IP vždy určuje, jak doručit paket z bodu do bodu, podle výše uvedeného postupu. Chcete-li se seznámit se standardním postupem řešení potíží, přečtěte si část „Nelze se připojit k hostiteli nebo názvu NetBIOS“ dále v této kapitole.

# Překlad názvu na adresu IP

Pokud je cílové umístění požadované programem ve formátu názvu NetBIOS nebo názvu hostitele, je nutné provést překlad názvu dříve, než může protokol IP odeslat první paket. Protokol IP rozumí pouze adresám IP. Názvy hostitele a názvy NetBIOS se překládají na adresy IP různými způsoby.

## Překlad názvu NetBIOS na adresu IP

Názvy NetBIOS lze přímo přeložit na adresu IP pomocí čtyř metod: hledáním v mezipaměti názvů NetBIOS, dotazem na server WINS, všesměrovým vysíláním nebo kontrolou souboru Lmhosts.

Počítače se systémem Windows Server 2003 vždy začínají kontrolou interní mezipaměti názvů NetBIOS hostitelského počítače. Pokud se přitom nepodaří adresu IP získat, lze název NetBIOS přeložit na adresu IP pomocí serveru WINS, série všesměrových vysílání nebo souboru `Lmhosts`. Výběr první z těchto tří metod v konkrétním počítači závisí na jeho typu uzlu. Výchozí typ uzlu je hybridní neboli uzel H, který se nejdříve dotáže serveru WINS a potom se pokusí přeložit název pomocí místního všesměrového vysílání. Pokud tyto metody nejsou úspěšné, převede klient název NetBIOS na název hostitele a provede překlad názvu hostitele.

Počítače se systémem Windows Server 2003 jsou ve výchozím nastavení uzly B. Jako uzel H jsou nastaveny při konfiguraci na server WINS. K dispozici jsou tyto typy uzlů:

- **Uzel B (všesměrové vysílání – broadcast)** Uzel B používá při registraci a překladu názvů NetBIOS dotazy typu všesměrového vysílání. Uzel B se vyznačuje dvěma hlavními problémy: Všesměrová vysílání zatěžují všechny uzly v síti a směrovače obvykle všesměrová vysílání nepředávají dál, takže lze přeložit pouze názvy NetBIOS v místní síti.
- **Uzel P (rovnocenný – peer-peer)** Uzel P překládá názvy NetBIOS pomocí názvového serveru NetBIOS (NBNS), jako je např. server WINS. Uzel P nepracuje s všesměrovým vysíláním. Místo toho posílá dotaz přímo na server NBNS.
- **Uzel M (smíšený – mixed)** Uzel M je kombinací uzlu B a uzlu P. Uzel M standardně funguje jako uzel B. Pokud uzel M nemůže přeložit název pomocí všesměrového vysílání, dotáže se serveru NBNS pomocí uzlu P.

- **Uzel H (hybridní – hybrid):** Uzel H představuje kombinaci uzlu P a uzlu B. Ve výchozím nastavení funguje uzel H jako uzel P. Jestliže uzel H nemůže přeložit název pomocí serveru NBNS, přeloží název s použitím všesměrového vysílání.

Pokud jediný problém spočívá v překladu názvů NetBIOS, může počítač nadále přistupovat ke vzdálenému prostředku pomocí jeho adresy IP.

Chcete-li použít jen překlad názvů NetBIOS, zadejte příkaz `nbtstat -a` *`NázevPočítače`*. Síťové příkazy, jako např. `net use`, se současně dotazují na NetBIOS a DNS. Příkaz `Nslookup` nelze při řešení potíží s překladem názvů NetBIOS použít, protože vrátí název hostitele, nikoli název NetBIOS.

### Překlad názvu hostitele nebo domény na adresu IP

Názvy hostitele lze přímo přeložit pomocí mezipaměti překládání klienta DNS, která obsahuje položky v souboru Hosts, nebo pomocí serveru DNS. Problémy v tomto případě zpravidla souvisí s nesprávně konfigurovaným serverem DNS, chybně zadanou položkou souboru `Hosts` nebo nesprávnou adresou IP, případě s více položkami pro jednoho hostitele v souboru `Hosts`. Problémy s překladem hostitele nebo domény lze diagnostikovat nástrojem `Nslookup` nebo `Netdiag`.

## Určení adresy IP a rozhraní dalšího směrování

Všechny počítače s libovolnou verzí systému Windows a standardním protokolem TCP/IP používají tabulku směrování IP. Tabulka směrování určuje adresu IP a rozhraní dalšího směrování. Tabulka směrování IP obsahuje informace o cílových umístěních a postupech, jak je lze kontaktovat. K dispozici je řada výchozích položek, které jsou založeny na konfiguraci uzlu. Položky lze přidávat pomocí nástrojů TCP/IP, jako je např. nástroj příkazového řádku `Route`, nebo dynamicky na základě interakce se směrovači.

Při předávání paketu IP určuje tabulka směrování IP následující faktory:

- **Adresa IP dalšího směrování** V případě přímého doručování (pokud je cílem sousední uzel) je adresa IP dalšího směrování cílovou adresou v paketu. Pokud se jedná o nepřímé doručování (není-li cílem sousední uzel), je adresa dalšího směrování adresou směrovače.
- **Rozhraní dalšího směrování** Rozhraní dalšího směrování určuje buď fyzické rozhraní (např. síťový adaptér), nebo logické rozhraní (např. rozhraní tunelového propojení), které slouží k předání paketu.

Po zjištění adresy a rozhraní dalšího směrování je paket předán protokolu ARP. V případě technologií místních sítí typu Ethernet a Token Ring se protokol ARP pokusí přeložit adresu MAC pro adresu dalšího směrování a předat paket pomocí rozhraní dalšího směrování.

### Obsah tabulky směrování IP

Typická položka tabulky směrování IP obsahuje následující pole:

- **Destination** Cílem může být adresa IP nebo ID sítě vytvořené jako podsíť nebo nadsíť na základě třídy. V tabulce směrování IP systému Windows Server 2003 je tento sloupec označen jako **Network Destination**.

- **Network mask** Bitová maska, která slouží k párování cílové adresy IP s hodnotou v poli Destination. V tabulce směrování IP systému Windows Server 2003 je tento sloupec označen jako **Netmask**.
- **Next-Hop** Adresa IP, na kterou je paket předáván. V tabulce směrování IP systému Windows Server 2003 je tento sloupec označen jako **Gateway**.
- **Interface** Síťové rozhraní, které se používá k předání paketu IP.
- **Metric** Číslo, které určuje náklady na trasu, aby bylo možné vybrat nejlepší trasu mezi mnoha trasami ke stejnému cíli. Metrika běžně udává počet směrování (tj. počet připojení nebo směrovačů, kterými je nutné projít) na trase k cíli.

### Typy položek tabulky směrování

Položky tabulky směrování mohou uchovávat následující typy tras.

- **Trasy přímo připojené sítě** Trasy pro podsítě, ke kterým je uzel připojen přímo. V případě tras přímo připojených sítí může být pole dalšího směrování prázdné nebo může obsahovat adresu IP rozhraní v příslušné podsíti. Pokud je adresa místní, nevyžaduje doručení další úsilí. Protokol ARP překládá adresu IP na hardwarovou adresu, obvykle adresu MAC cílové karty Ethernet. Problémy zde obvykle souvisí s mezipamětí ARP (např. duplicitními adresami) nebo maskou podsítě a lze je vyřešit pomocí nástrojů Arp nebo Ipconfig.
- **Trasy vzdálené sítě** Trasy pro podsítě, které jsou dostupné přes směrovače a nejsou přímo připojeny k uzlu. V případě tras vzdálené sítě je v poli Next-Hop uvedena adresa IP místního směrovače. Pokud je adresa vzdálená, spočívá další krok ve zjištění brány, která se použije k dosažení vzdálené adresy. V síti, kde externí připojení zajišťuje pouze jediný směrovač, je řešení tohoto problému relativně snadné. Jestliže se však jedná o libovolnou síť s více připojenými směrovači, je určení správné brány složitější.

  Protokol IP tento problém řeší hledáním ve své tabulce směrování. Tato tabulka směrování slouží jako rozhodovací strom, který protokolu IP umožňuje stanovit, které rozhraní a bránu má použít k odeslání odchozího provozu. Tabulka směrování obsahuje mnoho jednotlivých tras. Každá trasa zahrnuje cíl, masku sítě, rozhraní brány a metriku.

  Analýza tabulky směrování probíhá od nejkonkrétnějších k nejvíce obecným položkám, takže je paket odeslán na první brány, jejichž položka tabulky směrování se shoduje s cílem paketu. Pokud jsou dvě trasy identické, má přednost trasa s nižší metrikou před trasou s vyšší metrikou. V případě nerozhodného výsledku použije uzel libovolnou z těchto položek tabulky směrování. Související problémy se řeší pomocí nástroje `Route` nebo změn konfigurace sítě.
- **Hostitelské trasy** Trasa k určité adrese IP. Hostitelské trasy umožňují, aby směrování probíhalo v závislosti na jednotlivé adrese IP. V případě hostitelských tras je ID sítě konkrétní síťová adresa a maska sítě má hodnotu `255.255.255.255`.
- **Výchozí trasa** Tato trasa se použije, pokud není nalezena konkrétní síťová nebo hostitelská trasa. Cílem výchozí trasy je `0.0.0.0` s maskou sítě `0.0.0.0`. Adresou dalšího směrování výchozí trasy je zpravidla výchozí brána uzlu.

## Proces určení trasy

Při výběru položky tabulky směrování, která se použije při předávání, používá protokol IP následující proces:

- Pro každou položku v tabulce směrování je provedena bitová operace AND mezi cílovou adresou IP a polem Network Mask. Výsledek se porovná s polem Cíl položky, zda došlo ke shodě.

  Při bitové logické operaci AND mezi cílovou adresou IP a síťovou maskou trasy porovná protokol IP každý bit v cílové adrese IP s odpovídajícím bitem masky podsítě. Mají-li oba bity hodnotu 1, je výsledkem bit 1, jinak má výsledek hodnotu 0. Vzhledem k principu definice masky podsítě platí pro operaci bitové logické AND:

  - Pro každý bit v masce podsítě nastavený na hodnotu 1 je odpovídající bit ve výsledku zkopírován z cílové adresy IP.
  - Pro každý bit v masce podsítě nastavený na hodnotu 0 je odpovídající bit ve výsledku nastaven na hodnotu 0.

  Dobrým příkladem realizace bitové logické operace AND je určení adresy IP ID sítě pro konfiguraci adresy IP. Při určování adresy IP ID sítě se provádí bitová logická operace AND přiřazené adresy IP s její maskou podsítě. Výsledkem je adresa IP ID sítě.

  Pokud je například adresa IP 192.168.98.112 s maskou podsítě `255.255.255.0`, má výsledek bitové logické operace AND následující hodnotu:

  - Pro prvních 24 bitů, které odpovídají části „`255.255.255`“ masky podsítě, je zkopírován odpovídající bit z cílové adresy IP s výsledkem `192.168.98` v prvních třech oktetech.
  - Pro posledních 8 bitů, které odpovídají části „0“ masky podsítě je odpovídající bit nastaven na hodnotu 0 s výsledkem 0 v posledním oktetu.

  Operace `192.168.98.112 AND 255.255.255.0` tedy má hodnotu `192.168.98.0`.

- Je zkompilován seznam odpovídajících tras. Vybrána je trasa, která má nejdelší shodu (tj. trasa s největším počtem bitů nastavených v masce podsítě na hodnotu 1). Trasa s nejdelší shodou je nejkonkrétnější trasa k cílové adrese IP. Existuje-li více tras s nejdelší shodou (například více tras ke stejnému ID sítě), použije směrovač k výběru optimální trasy nejnižší metriku. Jestliže je k dispozici více tras s nejdelší shodou a nejnižší metrikou, použije uzel libovolnou z těchto položek tabulky směrování.

Výsledkem procesu určení trasy je výběr jediné trasy z tabulky směrování. Pokud se v tomto procesu nepodaří vybrat trasu, oznámí protokol IP chybu směrování. V případě odesílajícího hostitele je chyba směrování IP oznámena interně protokolu vyšší vrstvy, jako je např. protokol TCP nebo UDP (User Datagram Protocol). Jedná-li se o směrovač, je odesílajícímu hostiteli odeslána zpráva „ICMP Destination Unreachable-Host Unreachable“ a paket je následně zahozen.

## Proces určení adresy a rozhraní dalšího směrování

Jakmile je zjištěna konkrétní trasa v tabulce směrování, na kterou má být paket předán, určí se adresa a rozhraní dalšího směrování následujícím procesem:

- Pokud je adresa v poli Next-Hop prázdná nebo se jedná o adresu přiřazenou rozhraní na uzlu pro předávání, postupuje se takto:
  - Adresa dalšího směrování je nastavena na cílovou adresu IP paketu IP.
  - Rozhraní dalšího směrování je nastaveno na rozhraní, které je uvedeno v poli Interface.
- Pokud se adresa v poli Next-Hop liší od adresy přiřazené rozhraní na uzlu pro předávání, postupuje se takto:
  - Adresa dalšího směrování je nastavena na adresu v poli Next-Hop pro trasu.
  - Rozhraní dalšího směrování je nastaveno na rozhraní, které je uvedeno v poli Interface.

## Příklad tabulky směrování IP systému Windows Server 2003

Následující příklad představuje výchozí tabulku směrování hostitele se systémem Windows Server 2003 (tj. nikoli směrovače), který nemá instalován protokol IPv6. Hostitel je vybaven jediným síťovým adaptérem a má nastavenu adresu IP `157.60.136.41`, masku podsítě `255.255.252.0` (`/22`) a výchozí bránu `157.60.136.1`. Chcete-li zobrazit tabulku směrování IP v počítači se systémem Windows Server 2003, zadejte na příkazový řádek `route print` nebo `netstat -r`. Zobrazí se výstup podobný následujícímu:

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 b0 d0 e9 41 43 ...... 3Com 3C920 EtherLink PCI
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   157.60.136.1   15.60.136.41       1
        127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1       1
     157.60.136.0    255.255.252.0  157.60.136.41  157.60.136.41       1
    157.60.136.41  255.255.255.255      127.0.0.1      127.0.0.1       1
   157.60.255.255  255.255.255.255  157.60.136.41  157.60.136.41       1
        224.0.0.0        240.0.0.0  157.60.136.41  157.60.136.41       1
  255.255.255.255  255.255.255.255  157.60.136.41  157.60.136.41       1

Default Gateway: 157.60.136.1
===========================================================================
Persistent Routes:
None
```

Všimněte si, že jsou uvedena dvě rozhraní. Jedno rozhraní odpovídá instalovanému síťovému adaptéru (`3Com EtherLink PCI`) a druhé je rozhraní vnitřní zpětné smyčky (`MS TCP Loopback Interface`).

Tabulka směrování IP systému Windows Server 2003 určuje rozhraní v poli `Interface` trasy pomocí adresy IP. Adresa a rozhraní dalšího směrování se proto určují následujícím procesem:

- Pokud je adresa v poli `Gateway` přiřazena rozhraní na uzlu pro předávání, postupuje se takto:

  - Adresa dalšího směrování je nastavena na cílovou adresu IP paketu IP.
  - Rozhraní dalšího směrování je nastaveno na rozhraní, ke kterému je přiřazena adresa v poli `Interface`.
- Pokud se adresa v poli `Gateway` liší od adresy přiřazené rozhraní na uzlu pro předávání, postupuje se takto:
  - Adresa dalšího směrování je nastavena na adresu v poli `Gateway`.
  - Rozhraní dalšího směrování je nastaveno na rozhraní, ke kterému je přiřazena adresa v poli `Interface`.

**Položky tabulky směrování IP systému Windows Server 2003** Ukázka tabulky směrování IP systému Windows Server 2003 obsahuje následující položky:

- První položka – síťový cíl `0.0.0.0` a maska sítě (netmask) `0.0.0.0` (`/0`) – určuje výchozí trasu. Adresa IP s libovolným cílem dává po bitové logické operaci AND s adresou `0.0.0.0` výsledek `0.0.0.0`. Výchozí trasa tedy vyhovuje pro libovolnou adresu IP. Pokud je výchozí trasa trasou s nejdelší shodou, je adresa dalšího směrování `157.60.136.1` a rozhraní dalšího směrování představuje síťový adaptér, který má přiřazenu adresu `IP 157.60.136.41`.
- Druhá položka – síťový cíl `127.0.0.0` a maska sítě `255.0.0.0` (`/8`) – je trasou sítě zpětné smyčky. Pro všechny pakety odeslané na adresu ve tvaru `127.x.y.z` je adresa dalšího směrování nastavena na `127.0.0.1` (adresa zpětné smyčky) a rozhraním dalšího směrování je rozhraní, které má přiřazeno adresu `127.0.0.1` (rozhraní zpětné smyčky).
- Třetí položka – síťový cíl `157.60.136.0` a maska sítě `255.255.252.0` (`/22`) – představuje trasu přímo připojené sítě. Je-li tato trasa trasou s nejdelší shodou, je adresa dalšího směrování nastavena na cílovou adresu v paketu a rozhraní dalšího směrování je nastaveno na síťový adaptér, který má přiřazenu adresu IP `157.60.136.41`.
- Čtvrtá položka – síťový cíl `157.60.136.41` a maska sítě `255.255.255.255` (`/32`) – udává hostitelskou trasu pro adresu IP hostitele. Pro všechny pakety IP odeslané na adresu `157.60.136.41` je adresa dalšího směrování nastavena na `127.0.0.1` a rozhraním dalšího směrování je rozhraní zpětné smyčky.
- Pátá položka – síťový cíl `157.60.255.255` a maska sítě `255.255.255.255` (`/32`) – je hostitelská trasa, která odpovídá adrese všesměrového vysílání pro ID sítě třídy B `157.60.0.0` (`/16`), které je směrováno do všech podsítí. Pro všechny pakety IP odeslané na adresu `157.60.255.255` je adresou dalšího směrování `157.60.255.255` a rozhraním dalšího směrování je síťový adaptér, který má přiřazenu adresu IP `157.60.136.41`.
- Šestá položka – síťový cíl `224.0.0.0` a maska sítě `224.0.0.0` (`/3`) – znamená trasu pro vícesměrové vysílání odesílané tímto hostitelem. V případě všech paketů vícesměrového vysílání je adresa dalšího směrování nastavena na cílovou adresu a rozhraní dalšího směrování je nastaveno na síťový adaptér, který má přiřazenu adresu IP `157.60.136.41`.
- Sedmá položka – síťový cíl `255.255.255.255` a maska sítě `255.255.255.255` (`/32`) – určuje hostitelskou trasu, která odpovídá adrese omezeného všesměrového vysílání. Pro všechny pakety IP odeslané na adresu `255.255.255.255` je adresa

dalšího směrování nastavena na 255.255.255.255 a rozhraním dalšího směrování je síťový adaptér, který má přiřazenu adresu IP 157.60.136.41.

**Určení adresy dalšího směrování pomocí tabulky směrování** Následující příklady dokumentují, jak lze pomocí ukázkové tabulky směrování určit adresu IP a rozhraní dalšího směrování pro několik odlišných cílů:

- **Cíl jednosměrového vysílání 157.60.136.48** Trasou s nejdelší shodou je trasa pro přímo připojenou síť (157.60.136.0/22). Adresa IP dalšího směrování je nastavena na cílovou adresu IP (157.60.136.48) a rozhraní dalšího směrování je nastaveno na síťový adaptér, který má přiřazenu adresu IP 157.60.136.41.
- **Cíl jednosměrového vysílání 192.168.0.79** Trasou s nejdelší shodou je výchozí trasa (0.0.0.0/0). Adresa IP dalšího směrování je nastavena na adresu výchozí brány (157.60.136.1) a rozhraním dalšího směrování je síťový adaptér, který má přiřazenu adresu IP 157.60.136.41.
- **Cíl vícesměrového vysílání 224.0.0.1** Trasou s nejdelší shodou je trasa 224.0.0.0/3. Adresa IP dalšího směrování je nastavena na cílovou adresu IP (224.0.0.1) a rozhraním dalšího směrování je síťový adaptér, který má přiřazenu adresu IP 157.60.136.41.
- **Cíl všesměrového vysílání podsítě 157.60.139.255** Trasou s nejdelší shodou je trasa pro přímo připojenou síť (157.60.136.0/22). Adresa IP dalšího směrování je nastavena na cílovou adresu IP (157.60.139.255) a rozhraní dalšího směrování je nastaveno na síťový adaptér, který má přiřazenu adresu IP 157.60.136.41.
- **Cíl jednosměrového vysílání 157.60.136.41** Trasou s nejdelší shodou je hostitelská trasa pro místně přiřazenou adresu IP (157.60.136.41/32). Adresa IP dalšího směrování je nastavena na cílovou adresu (157.60.136.41) a rozhraní dalšího směrování je nastaveno na adaptér zpětné smyčky.



# 6.2 Přehled řešení problémů

Následující části poskytují informace, jak určit problémy s komunikací a konfigurací protokolu TCP/IP, a obsahují postupy, pomocí kterých lze tyto problémy vyřešit.

Při řešení potíží protokolu TCP/IP se obvykle postupuje podle daného schématu:

1. Ověřte, zda rozhraní příslušného počítače není odpojeno od média.
2. Zkontrolujte, zda je protokol TCP/IP v příslušném počítači správně konfigurován.
3. Ověřte, zda existuje cesta směrování mezi problematickým počítačem a jeho cílem.
4. Pokud máte podezření na spolehlivost propojení, použijte v různou denní dobu nástroj Pathping a zaznamenejte podíl úspěšných pokusů.

Nepodaří-li se pomocí těchto kroků příčinu problému zjistit, zachycujte síťový provoz pomocí analyzátoru protokolu, jako je např. nástroj Microsoft Network Monitor.

**Další informace** Informace o nástroji Network Monitor naleznete v publikaci *Microsoft® Windows Server™ 2003 Administrator's Companion* (Příručka správce systému Microsoft® Windows Server™ 2003) autorů Russel, Crawford a Gerend (Microsoft Press, 2003).

Při řešení potíží s komunikací pomocí protokolu TCP/IP si položte následující otázky:

- Je cílový prostředek dostupný jiným počítačům ve stejné podsíti?
- Které aplikace nejsou funkční, které úspěšně komunikují, a jaký lze mezi nimi najít vztah nebo souvislost?
- Spočívá problém v základní konektivitě IP nebo souvisí s překladem názvů? Pokud je problémem překlad názvů, používá neúspěšná aplikace názvy NetBIOS nebo názvy hostitele?
- Fungovaly některé problémové aplikace v příslušném počítači dříve?
- Můžete určit změny provedené v počítači nebo síti od období, kdy tyto aplikace úspěšně fungovaly, do období, kdy přestaly komunikovat?

Stanovte prostorový a časový výskyt problému, abyste zúžili rozsah možných řešení problému. Kromě toho můžete systematicky prozkoumat selhání protokolu TCP/IP tak, že se zaměříte na postup, kterým protokol TCP/IP navazuje komunikaci. Popis tohoto postupu naleznete v části „Přehled komunikačních procesů protokolu TCP/IP“ v této kapitole.

## Nelze se připojit k adrese IP

Zásobník protokolu TCP/IP, který je součástí systému Windows Server 2003, je spolehlivější než implementace protokolu TCP/IP v jiných verzích systému Windows. Přesto může několik faktorů zabránit, aby došlo ke správnému navázání komunikace TCP/IP. Může se jednat například o vadnou kabeláž a hardware nebo chybné nastavení sítě. Tato část popisuje několik dostupných nástrojů, které umožňují detekovat a opravit chybně fungující hardware a zjistit nesprávnou konfiguraci sítě.

### Kontrola síťového připojení – stav odpojeného média

Nástroj `MediaSense` systému Windows Server 2003 zajišťuje automatickou detekci a oznámení odpojeného nebo poškozeného média. Problém odpojených médií se sice netýká pouze protokolu TCP/IP, ale způsobí zastavení komunikace protokolu TCP/IP.

Pokud je síťový kabel odpojen nebo poškozen, nástroj `MediaSense` to detekuje a ikona síťového připojení ve složce Network Connections v oznamovací oblasti na pravé straně hlavního panelu se zobrazí s červeným symbolem X. Červený symbol X je ve složce Network Connections zobrazen i v případě, že dojde k poškození síťového rozbočovače, ke kterému je systém připojen, nebo je tento rozbočovač odpojen od zdroje napájení. Při řešení potíží s konektivitou nejdříve zkontrolujte, zda jsou ikony některých síťových připojení zobrazeny s červeným symbolem X. Znamená to, že připojení je ve „stavu odpojeného média“.

Pokud má například počítač s více adresami více síťových adaptérů připojených k jednomu síťovému rozbočovači a ikony všech síťových připojení těchto adaptérů jsou zobrazeny s červeným X, je možné, že rozbočovač daných připojení nefunguje správně. Jestliže je více počítačů připojeno ke společnému rozbočovači a všechna jejich síťová připojení jsou zobrazena s červeným X, může to také znamenat nesprávnou činnost rozbočovače, ke kterému jsou počítače připojeny. Je-li naopak s červeným X zobrazen pouze jeden ze dvou adaptérů připojených ke stejnému

rozbočovači, je pravděpodobnější, že není správně zapojen kabel spojující příslušný adaptér s rozbočovačem nebo že je kabel poškozen.

Dále zkontrolujte, zda nebylo připojení zakázáno.

## Použití funkce Repair

Jakmile jste zkontrolovali, že adaptér není ve stavu odpojeného média ani není zakázán, můžete se pomocí funkce `Repair` pokusit o obnovení z běžných síťových stavů. Klepnutím na možnost `Repair` obnovíte nastavení sítě. Klepněte pravým tlačítkem myši na ikonu síťového připojení, která je zobrazena ve složce Network Connections nebo v oznamovací oblasti. Potom v místní nabídce klepněte na příkaz `Repair`. Tabulka 6.1 obsahuje akce funkce `Repair` a odpovídající příkazy pro příkazový řádek.

Tabulka 6.1: Pořadí akcí příkazu Repair

| Postup | Pořadí | Ekvivalent pro příkazový řádek |
|---|---|---|
| 1 | Zkontroluje, zda je povolen protokol DHCP. Pokud ano, obnoví všesměrové vysílání, aby došlo k aktualizaci adresy IP. | Plní obdobnou funkci jako příkaz ipconfig `/renew` * |
| 2 | Vyprázdní mezipaměť ARP. | arp -d * |
| 3 | Vyprázdní mezipaměť NETBios. | nbtstat -R |
| 4 | Vyprázdní mezipaměť překládání klienta DNS. | ipconfig /flushdns |
| 5 | Opakuje registraci pro službu WINS. | nbtstat -RR |
| 6 | Opakuje registraci pro službu DNS. | ipconfig /registerdns |

* Obnovení všesměrového vysílání (Repair) způsobí, že počítač přijme zapůjčení z libovolného dostupného serveru DHCP. Oproti tomu obnovení jednosměrového vysílání (ipconfig /renew) obnoví pouze existující zapůjčení z posledního serveru DHCP, který klientovi zapůjčil adresu. Obnovení všesměrového vysílání je vhodnější v případech, kdy problém způsobuje server DHCP, od kterého klientský počítač naposledy získal zapůjčenou adresu.

## Kontrola konfigurace sítě

Pokud jste ověřili, že počítač není odpojen od média, spustili jste příkaz `Repair` a počítač nadále vykazuje problémy s konektivitou, zkontrolujte nastavení konfigurace sítě a hardwaru pomocí zobrazení příkazu nabídky Status pro síťové připojení, nebo pomocí programu `Netdiag.exe` či nástroje ipconfig pro příkazový řádek. Informace poskytované těmito nástroji se sice do určité míry překrývají, ale každý z nich má specifické vlastnosti.

**Použití příkazu Status** Pomocí příkazu **Status** pro síťové připojení můžete rychle získat přístup k mnoha nastavením konfigurace a statistikám daného připojení. Informace jsou zobrazeny v rozšířeném uživatelském rozhraní síťového připojení. Chcete-li zkontrolovat stav připojení, otevřete složku **Network Connections**, klepněte pravým tlačítkem myši na připojení a vyberte příkaz **Status**.

**Network Connection Status: karta General** Karta **General** dialogového okna **Status** pro síťové připojení obsahuje následující informace:

- Připojený nebo odpojený stav vytáčeného, bezdrátového či vysokorychlostního internetového připojení nebo připojení RAS.
- Uplynulý čas síťového, vytáčeného, bezdrátového či vysokorychlostního internetového připojení nebo připojení RAS.
- Rychlost v okamžiku připojení.
- V případě místních připojení počet odeslaných a přijatých bajtů v průběhu připojení. Pro jiné typy připojení karta General znázorňuje také počet odeslaných a přijatých bajtů během připojení a související statistiky komprese a chyb.

**Network Connection Status karta Support** Přejdete-li v dialogu **Status** síťového připojení z karty **General** na kartu **Support**, můžete zkontrolovat následující podrobnosti konfigurace:

- typ adresy,
- adresa IP,
- maska podsítě,
- výchozí brána.

**Network Connection Status: karta Support – Details** Pokud na kartě **Support** klepnete na možnost **Details**, získáte podrobnější přehled následujících konfiguračních informací:

- fyzická adresa,
- adresa IP,
- maska podsítě,
- výchozí brána,
- server DHCP,
- získání zapůjčení,
- konec platnosti zapůjčení,
- servery DNS,
- servery WINS.

Kontrola konfigurace a statistik pomocí příkazu **Status** poskytuje následující výhody:

- Sledujete aktivitu sítě v reálném čase. Můžete tedy určit, zda síťový adaptér skutečně zpracovává provoz nebo nikoli.
- Klepnutím na možnost **Properties** získáte snadný přístup k vlastnostem připojení, které poté můžete zkontrolovat nebo změnit síťové komponenty Client, Service či Protocol.

Kontrola konfigurace a statistik touto metodou má následující nevýhody:

- Není přístupný stav připojení k místní síti, které je ve stavu odpojení od média.
- Dostupné podrobnosti konfigurace jsou velmi omezené. Neoznamují se například žádné přípony DNS.
- Výsledky se zobrazují pouze na základě připojení.

- Jsou zobrazeny pouze výsledky protokolu IPv4, nikoli protokolu IPv6.
- Výsledky z dialogu **Status** nelze tisknout ani je přesměrovat do souboru typu TXT nebo DOC.

**Použití příkazu Ipconfig** Příkaz `ipconfig /all` poskytne podrobnou konfigurační zprávu pro všechna rozhraní, včetně všech konfigurovaných adaptérů vzdáleného přístupu. Výstup příkazu Ipconfig lze přesměrovat do textového souboru (typu TXT) nebo do souboru aplikace Word (typu DOC), je-li tento program nainstalován. Na příkazový řádek zadejte následující řetězec s příslušnou příponou souboru:

```
ipconfig > Adresář\NázevSouboru.Přípona
```

Následující ukázka například uloží výstup jako textový soubor s názvem `ipcfg.txt` do adresáře `F:\NetTest\`.

```
ipconfig /all > F:\NetTest\ipcfg.txt
```

Výstup příkazu `Ipconfig` si můžete prohlédnout a vyhledat v něm libovolné problémy týkající se konfigurace počítačové sítě. Pokud například počítač při konfiguraci dostal adresu IP, která je duplicitní vůči existující adrese IP, která již byla detekována, zobrazí se maska podsítě jako `0.0.0.0`.

Následující příklad dokumentuje výsledky příkazu `ipconfig /all` pro počítač s více adresami, který:

- používá k automatické konfiguraci protokolu TCP/IP server DHCP,
- překládá názvy pomocí serverů WINS a DNS,
- nemá nainstalován protokol IPv6.

```
Windows IP Configuration

  Host Name . . . . . . . . . . . . : testpc1
  Primary Dns Suffix . . . . . . . : contoso.example.com
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No
  DNS Suffix Search List. . . . . . : contoso.example.com
                                      contoso.com
                                      example.com

Ethernet adapter Local Area Connection 1:

  Connection-specific DNS Suffix . .: corp.example.com
  Description . . . . . . . . . . . : PCI 100 Ethernet Adapter
  Physical Address. . . . . . . . . : 00-02-B3-22-01-5D
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  IP Address. . . . . . . . . . . . : 172.16.48.10
  Subnet Mask . . . . . . . . . . . : 255.255.248.0
  Default Gateway . . . . . . . . . : 172.16.48.03
  DHCP Server . . . . . . . . . . . : 157.54.8.118
  DNS Servers . . . . . . . . . . . : 172.16.14.119
                                      172.56.236.138
```

```
  Primary WINS Server . . . . . . . : 172.16.48.04
  Secondary WINS Server . . . . . . : 172.16.48.05
  Lease Obtained. . . . . . . . . . : Thursday, July 10, 2003 1:49:40 PM
  Lease Expires . . . . . . . . . . : Friday, July 18, 2003 1:49:40 PM

Ethernet adapter Local Area Connection 2:

  Connection-specific DNS Suffix . .:
  Description . . . . . . . . . . . : PCI Fast Ethernet Adapter
(Generic)
  Physical Address. . . . . . . . . : 00-00-F8-03-6F-D3
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Autoconfiguration IP Address. . . : 169.254.225.167
  Subnet Mask . . . . . . . . . . . : 255.255.0.0
  Default Gateway . . . . . . . . . :
```

Použití příkazu `Ipconfig` přináší následující výhody:

- V jediné operaci lze získat informace o počítačích s více adresami.
- Výsledky příkazu `Ipconfig` lze přesměrovat a uložit jako soubor typu TXT nebo DOC, pokud je v počítači nainstalován program Word.
- Příkaz `Ipconfig` zobrazuje výsledky pro protokol IPv4 i IPv6.
- Příkaz `Ipconfig` skýtá více informací o připojení, než lze získat příkazem Status.

Kontrola konfigurace pomocí příkazu Ipconfig má následující nevýhodu:

- Příkazem `Ipconfig` nelze zobrazit konfiguraci vzdáleného počítače.

**Použití programu Netdiag.exe** Nástroj `Netdiag.exe` izoluje problémy se sítí a konektivitou. Provádí přitom rozsáhlejší sadu testů než příkaz `Ipconfig`. Tyto testy a jimi poskytované klíčové informace o stavu sítě pomáhají identifikovat a izolovat problémy se sítí. Tento nástroj nevyžaduje specifikaci parametrů ani možností. Můžete se proto zaměřit na analýzu výstupu a není nutné školit uživatele, jak nástroj používat.

Program `Netdiag.exe` a dodatečné nástroje podpory můžete instalovat spuštěním balíčku `Suptools.msi`, který naleznete ve složce `Support\Tools\` na instalačním disku CD systému Windows Server 2003. Poklepáním na balíček `Suptools.msi` spustíte průvodce Windows Support Tools Setup Wizard.

**Poznámka** Stránka průvodce **Destination Directory** ve výchozím nastavení nainstaluje nástroje podpory do složky *systemroot*`\Program Files\Support Tools\`. **Protože je nástroj** `Netdiag.exe` **nutné spouštět z příkazového řádku, může být vhodné určit jiné umístění instalace, abyste zkrátili cestu, kterou budete muset při každém spuštění nástroje zadávat. Během instalace můžete například pomocí tlačítka Browse v průvodci nastavit dříve vytvořenou složku** `D:\Tools`.

Chcete-li instalovat nástroj `Netdiag.exe` nezávisle na jiných nástrojích podpory, poklepejte na soubor `Support\Tools\Support.cab` na instalačním disku CD systému Windows Server 2003. Poklepáním na soubor `Netdiag.exe` spustíte extrakci. Potom postupujte podle zobrazených pokynů.

Chcete-li spustit program Netdiag.exe z příkazového řádku, zadejte cestu k umístění extrahovaného souboru Netdiag.exe. Pokud jste například program Netdiag.exe extrahovali do vytvořené složky, již jste nazvali E:\Tools, zadejte na příkazový řádek:

```
e:\tools\netdiag.exe
```

Případně můžete přejít do adresáře E:\Tools a potom zadat příkaz Netdiag.exe.

Výstup programu Netdiag.exe je možné přesměrovat do složky a uložit jako soubor typu TXT nebo DOC. Chcete-li to provést, zadejte na příkazový řádek následující řetězec s příslušným názvem a příponou souboru:

```
netdiag.exe > Adresář\NázevSouboru
```

Příklad zadání na příkazový řádek:

```
E:\Tools\Netdiag.exe > E:\NetTest\Ntdiag.doc
```

Program Netdiag bude spuštěn z adresáře E:\Tools a výsledky se uloží do souboru s názvem E:\NetTest\ jako dokument Ntdiag.doc programu Word.

Výstup programu Netdiag.exe poskytuje podrobný seznam konfiguračních informací a přehled provedených testů. Ve výstupu programu Netdiag.exe si můžete ověřit správnou konfiguraci adresy IP, masky podsítě, výchozí brány, serverů DNS a WINS. Můžete zde také zkontrolovat oznámené chyby. Výsledky zahrnují podrobnosti o chybách konfigurace, které program Netdiag.exe detekoval. Prohlédněte si položky se zprávami Skipped, Failed a WARNING, které souvisí s různými testy.

V následujícím příkladu je program Netdiag spuštěn v počítači, který je nastaven tak, aby automaticky získával konfiguraci protokolu TCP/IP ze serveru DHCP a k překladu názvů používal servery WINS a DNS. Zobrazí se výstup podobný následujícímu:

```
    Computer Name: testpc1
    DNS Host Name: testpc1.contoso.example.com
    System info : Windows Server 2003
    Processor : x86 Family
    List of installed hotfixes :
        Q147222

Netcard queries test . . . . . : Passed
    [WARNING] The net card 'PCI Fast Ethernet Adapter (Generic)' may not be
working because it as not received any packets.

    Adapter : Local Area Connection 1

        Netcard queries test . . . : Passed
        Host Name. . . . . : testpc1.example.com
        IP Address . . . . . : 172.16.48.10
        Subnet Mask. . . . . : 255.255.248.0
        Default Gateway. . . . . : 172.16.48.03
        Primary WINS Server. . . . : 172.16.48.04
        Secondary WINS Server. . . : 172.16.48.05
        Dns Servers. . . . . : 172.16.14.119
                               172.56.236.135
```

```
        AutoConfiguration results. . . . . : Passed

        Default gateway test . . . : Passed

        NetBT name test. . . . . : Passed
            [WARNING] At least one of the <00> 'WorkStation Service', <03>
'Messenger Service', <20> WINS' names is missing.

        WINS service test. . . . . : Passed

    Adapter : Local Area Connection 2

        Netcard queries test . . . : Passed
        Host Name. . . . . : testpc1
        Autoconfiguration IP Address : 169.254.225.167
        Subnet Mask. . . . . : 255.255.0.0
        Default Gateway. . . . . :
        Dns Servers. . . . . :

        AutoConfiguration results. . . . . : Failed
            [WARNING] AutoConfiguration is in use. DHCP not available.

        Default gateway test . . . : Skipped
            [WARNING] No gateways defined for this adapter.

        NetBT name test. . . . . : Passed
            [WARNING] At least one of the <00> 'WorkStation Service', <03>
'Messenger Service', <20> WINS' names is missing.
            No remote names have been found.

        WINS service test. . . . . : Skipped
            There are no WINS servers configured for this interface.

Global results:

Domain membership test . . . . . : Passed

NetBT transports test. . . . . : Passed
    List of NetBt transports currently configured:
        NetBT_Tcpip_{0B19AD54-2CA7-4795-8729-FE7494F2316A}
        NetBT_Tcpip_{C3C96E7E-4C54-4C87-9462-67D21D3E3D74}
    2 NetBt transports currently configured.

Autonet address test . . . . . : Passed

IP loopback ping test. . . . . : Passed

Default gateway test . . . . . : Passed

NetBT name test. . . . . : Passed
    [WARNING] You don't have a single interface with the <00> 'WorkStation
```

```
Service', <03> 'Messenger Service', <20> 'WINS' names defined.

Winsock test . . . . . . . . . . . : Passed

DNS test . . . . . . . . . . . . . : Passed
    [WARNING] Cannot find a primary authoritative DNS server for the name
testpc1.contoso.example.com.'. [ERROR_TIMEOUT]
    The name 'testpc1.contoso.example.com.' may not be registered in DNS.

Redir and Browser test . . . . . . : Passed
    List of NetBt transports currently bound to the Redir
        NetBT_Tcpip_{0B19AD54-2CA7-4795-8729-FE7494F2316A}
        NetBT_Tcpip_{C3C96E7E-4C54-4C87-9462-67D21D3E3D74}
    The redir is bound to 2 NetBt transports.

    List of NetBt transports currently bound to the browser
        NetBT_Tcpip_{0B19AD54-2CA7-4795-8729-FE7494F2316A}
        NetBT_Tcpip_{C3C96E7E-4C54-4C87-9462-67D21D3E3D74}
    The browser is bound to 2 NetBt transports.

DC discovery test. . . . . . . . . : Passed

DC list test . . . . . . . . . . . : Passed

Trust relationship test. . . . . . : Passed
    Secure channel for domain 'contoso' is to '\\contoso-dc-
02.contoso.example.com'.

Kerberos test. . . . . . . . . . . : Passed

LDAP test. . . . . . . . . . . . . : Passed

Bindings test. . . . . . . . . . . : Passed

WAN configuration test . . . . . . : Skipped
    No active remote access connections.

Modem diagnostics test . . . . . . : Passed

IP Security test . . . . . . . . . : Skipped
    Note: run "netsh ipsec dynamic show /?" for more detailed information

The command completed successfully
```

Použití programu `Netdiag.exe` přináší následující výhody:

- Informace o počítačích s více adresami lze získat v jediné operaci na rozdíl od dialogu **Status** síťového připojení, který zobrazuje údaje na základě připojení.
- Výsledky programu `Netdiag.exe` lze přesměrovat a uložit do souboru typu TXT nebo DOC. Dialog Status síťového připojení neumožňuje přesměrovat výstup do souboru typu TXT nebo DOC.
- Program `Netdiag.exe` zobrazuje výsledky pro protokol IPv4 i IPv6.

- Z programu `Netdiag.exe` lze spustit více variant testů, které poskytují podrobnější diagnostickou zprávu než příkaz Ipconfig nebo dialog Status síťového připojení.

## Test síťového připojení pomocí nástrojů Ping a Pathping

Pokud v konfiguraci protokolu TCP/IP nejsou patrné žádné chyby, lze v dalším kroku pomocí nástrojů `Ping` a `Pathping` vyzkoušet, zda se počítač může připojit k jiným hostitelským počítačům v síti TCP/IP.

Nástroj `Ping` pomáhá ověřit konektivitu na úrovni protokolu IP. Nástroj `Pathping` detekuje ztráty paketů při přenosech s více směrováními. Příkaz `ping` odesílá řadu zpráv „Echo" protokolu ICMP (Internet Control Message Protocol) směrem k cíli. Přitom využívá hostitelský název nebo adresu IP cíle. Příkaz Ping použijte vždy, potřebujete-li ověřit, zda může hostitelský počítač odesílat pakety IP cílovému hostiteli. Nástrojem `Ping` lze také odhalit problémy síťového hardwaru a nekompatibilní konfigurace.

**Poznámka** Pokud spustíte příkaz `ipconfig /all` a konfigurace adresy IP se zobrazí správně, není nutné pomocí příkazu ping zjišťovat dostupnost adresy zpětné smyčky nebo adresy IP místního počítače – příkaz `ipconfig` to již provedl, aby mohl zobrazit konfiguraci hostitele.

Při ověřování, zda existuje trasa mezi místním počítačem a síťovým hostitelem, je nejvhodnější nejdříve použít příkaz ping s adresou IP síťového hostitele, ke kterému se chcete připojit. Příkaz má následující syntaxi:

```
ping AdresaIP
```

Při práci s příkazem `Ping` postupujte takto:

Zadejte příkaz `ping` s adresou zpětné smyčky, abyste ověřili, zda je v místním počítači správně nainstalován a nakonfigurován protokol TCP/IP.

```
ping 127.0.0.1
```

Zadejte příkaz `ping` s adresou IP místního počítače, abyste zkontrolovali, zda byl správně přidán do sítě. Uvědomte si, že pokud je tabulka směrování správná, tento příkaz pouze předá paket na adresu zpětné smyčky `127.0.0.1`.

```
ping AdresaIPMístníhoHostitele
```

Zadáním příkazu `ping` s adresou IP výchozí brány ověříte, zda funguje výchozí brána a zda lze komunikovat s místním hostitelem v místní síti.

```
ping AdresaIPVýchozíBrány
```

Pokud zadáte příkaz `ping` s adresou IP vzdáleného hostitele, zjistíte, zda je možné komunikovat přes směrovač.

```
ping AdresaIPVzdálenéhoHostitele
```

Zadejte příkaz `ping` s hostitelským názvem vzdáleného hostitele, abyste ověřili, zda funguje překládání názvu vzdáleného hostitele.

```
ping HostitelskýNázevVzdálenéhoHostitele
```

Spusťte pro vzdáleného hostitele analýzu `Pathping`, abyste zkontrolovali, zda správně fungují směrovače na cestě k cílovému umístění.

```
pathping AdresaIPVzdálenéhoHostitele
```

**Poznámka** Pokud je místní adresa vrácena jako `169.254.y.z`, přiřadila počítači adresu IP funkce APIPA (Automatic Private IP Addressing – automatické přiřazení privátní adresy IP) systému Windows Server 2003. To znamená, že místní server DHCP není správně nakonfigurován nebo není z počítače dosažitelný a adresa IP byla přiřazena automaticky s maskou podsítě `255.255.0.0`. Povolte server DHCP nebo změňte jeho konfiguraci, restartujte místní počítač a zkontrolujte, zda problém se sítí přetrvává.

**Poznámka** Je-li místní adresa vrácena ve tvaru `0.0.0.0`, zjistil nástroj `MediaSense`, že síťový adaptér není připojen k síti. Chcete-li tento problém vyřešit, zkontrolujte, zda jsou síťový adaptér a síťový kabel připojeny k funkčnímu rozbočovači. Jestliže je připojení stabilní, opakujte instalaci ovladačů síťového adaptéru nebo nainstalujte nový síťový adaptér.

Příkaz `ping` překládá název počítače na adresu IP pomocí překladu názvu hostitele. Pokud je tedy příkaz ping s použitím adresy úspěšný, ale při zadání názvu neúspěšný, spočívá problém v překladu názvu hostitele, nikoli v síťové konektivitě. Další informace o řešení potíží s překladem názvu hostitele naleznete v části „Nelze se připojit k hostiteli nebo názvu NetBIOS“ v této kapitole.

Pokud v libovolné fázi nelze příkaz ping úspěšně použít, zkontrolujte, zda:

- Adresa IP místního počítače je platná a je správně zobrazena na kartě General dialogu Internet Protocol (TCP/IP) Properties a na kartě Support dialogu Status síťového připojení, nebo se zobrazuje při použití nástroje `Ipconfig` či `Netdiag.exe`.
- Je nakonfigurována výchozí brána a propojení mezi hostitelem a výchozí branou je funkční. Pokud zadáte příkaz `ping` s adresou výchozí brány, měli byste dostat odpověď. Systém Windows Server 2003 používá rozpoznání mrtvé brány. Rozpoznání mrtvé brány se uplatní v případech, kdy konfigurace počítače zahrnuje více bran a připojení směrované přes výchozí bránu se několikrát pokusí odeslat paket TCP, aniž by byla doručena odpověď. Funkce rozpoznání mrtvé brány pak zajistí, že adresa dalšího směrování pro připojení TCP se změní tak, aby používala další výchozí bránu ze seznamu.



**Poznámka** Pokud připojení vzdáleného systému, který je testován příkazem `ping`, vykazuje velké zpoždění (například v případě satelitního propojení), může vrácení odpovědí trvat dále. Delší časový limit lze zadat pomocí možnosti `-w` (wait – čekání). V následujícím příkladu je pomocí možnosti `-w` nastaven časový limit čekání na odpověď 2 sekundy (2 000 milisekund), možnost `-n` (number of pings – počet příkazů `ping`) je nastavena na dvě zprávy „Echo“ a možnost `-l` určuje, že každý paket příkazu ping bude mít velikost 1 450 bajtů. Příkaz `ping` v tomto příkladu ověří adresu `172.16.48.10`.

```
C:\>ping -w 2000 -n 2 -l 1450 172.16.48.10
```

Zobrazí se následující výstup:

```
Pinging 172.16.48.10 with 1450 bytes of data:

Reply from 172.16.48.10: bytes=1450 time=1542ms TTL=32
Reply from 172.16.48.10: bytes=1450 time=1787ms TTL=32

Ping statistics for 172.16.48.10:
```

```
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1787ms, Average = 1664ms
```

### Vyprázdnění mezipaměti ARP

Nesprávné položky v mezipaměti ARP někdy znemožňují konektivitu k místním nebo vzdáleným hostitelům (pokud není položka mezipaměti ARP pro výchozí bránu správná). Obsah mezipaměti ARP lze zobrazit příkazem `arp -a` nebo `arp -g`. Chcete-li mezipaměť ARP vyprázdnit, zadejte `arp -d *`. Výsledky příkazů `arp -a` nebo `arp -g` lze přesměrovat a uložit do souboru typu TXT nebo DOC, je-li nainstalován program Word, s použitím syntaxe `arp -a > Adresář\NázevSouboru` (s příslušnou příponou názvu souboru TXT nebo DOC). Než změníte konfiguraci mezipaměti ARP, je vhodné zaznamenat nastavení konfigurace přesměrováním obsahu mezipaměti ARP do souboru typu TXT nebo DOC.

### Ověření výchozí brány

Zkontrolujte výchozí bránu. Adresa brány musí být ve stejné podsíti jako místní hostitel. V opačném případě nelze pakety z hostitelského počítače předat do žádného umístění mimo místní podsíť. Potom pomocí automatické nebo ruční konfigurace ověřte, zda je v hostiteli správně nakonfigurována adresa výchozí brány.

### Kontrola vzdáleného hostitele příkazem ping

Pokud výchozí brána odpovídá správně, zadejte příkaz `ping` s adresou vzdáleného hostitele, abyste ověřili, zda komunikace se vzdálenou sítí funguje podle očekávání. Jestliže příkaz `ping` není úspěšný, prozkoumejte cestu k cílovému umístění nástrojem `Tracert`. Plní-li funkci směrovačů IP počítače se systémem Microsoft Windows NT®, Windows 2000 nebo Windows Server 2003, prozkoumejte tabulku směrování IP pomocí příkazu `route print` nebo služby Routing and Remote Access. V případě směrovačů IP, které nejsou založeny na operačních systémech Windows NT, Windows 2000 ani Windows Server 2003, použijte k analýze tabulky směrování IP příslušný nástroj nebo funkci.

Příkaz `ping` při řešení potíží obvykle vrací čtyři chybové zprávy.

**TTL Expired in Transit** Počet směrování nutných k dosažení cíle překračuje hodnotu TTL (Time to Live), kterou pro předání paketů nastavuje odesílající hostitel. Příkaz `ping` odesílá zprávy ICMP „Echo“ s výchozí hodnotou TTL 128. Pokud tato hodnota nedostačuje k přenesení paketu přes požadovaný počet propojení směrem k cíli, můžete hodnotu TTL zvýšit příkazem `ping -i` až na 255 propojení. Jestliže se zvýšením hodnoty TTL nepodaří problém vyřešit, jsou pakety předávány ve smyčce směrování – tzn. v kruhové cestě mezi směrovači. Příkazem `Tracert` můžete zjistit skupinu směrovačů ve smyčce směrování. Tato skupina se projevuje jako opakovaná sekvence stejných adres IP ve zprávě příkazu `Tracert`. Proveďte vhodné změny v tabulkách směrování směrovačů ve smyčce směrování nebo o problému informujte správce vzdáleného směrovače.

**Destination Host Unreachable** Tato zpráva znamená jeden ze dvou problémů: místní systém nemá trasu k požadovanému cíli nebo o nedostupnosti trasy k cíli informuje vzdálený směrovač. Mezi oběma problémy lze rozlišit podle tvaru zprávy:

- Pokud zpráva sděluje pouze „Destination Host Unreachable“, neexistuje trasa z místního systému a vůbec nedošlo k pokusu o odeslání paketů do sítě. Pomocí nástroje `Route` zkontrolujte v místní tabulce směrování, zda není trasa k cíli chybná nebo nedostupná.
- Pokud má zpráva podobu „Reply From AdresaIP: Destination Host Unreachable“, došlo k problému se směrováním na vzdáleném směrovači s uvedenou adresou IP. Příslušným nástrojem zkontrolujte tabulku směrování IP směrovače, kterému je přiřazena příslušná adresa IP uvedená ve zprávě.

Pokud jste zadali příkaz `ping` s adresou IP, opakujte jej s názvem hostitele, abyste si ověřili, že je uvedená adresa IP správná.

**Request Timed Out** Tato zpráva oznamuje, že ve výchozím časovém intervalu čtyř sekund nebyly přijaty žádné zprávy odpovědi echa. Může to mít několik odlišných příčin. Zpravidla se jedná o zahlcení sítě, neúspěšný překlad adresy MAC dalšího směrování protokolem ARP, filtrování paketů, chybu směrování nebo tiché vyřazení. Nejčastěji to znamená, že selhala trasa zpět k odesílajícímu hostiteli. Může k tomu dojít proto, že trasu zpět k odesílajícímu hostiteli nezná cílový hostitel, jeden z mezilehlých směrovačů nebo dokonce výchozí brána cílového hostitele. Než zkontrolujete tabulky směrování na směrovačích, ověřte, zda tabulka směrování cílového hostitele obsahuje trasu k odesílajícímu hostiteli.

Pokud jsou vzdálené tabulky směrování správné a obsahují platnou trasu zpět k odesílajícímu hostiteli, vytiskněte příkazem `arp -a` obsah mezipaměti ARP a přesvědčte se, zda v mezipaměti ARP nechybí správná adresa. Ověřte si také pomocí masky podsítě, zda nebyla vzdálená adresa interpretována jako místní.

Dále určete pomocí nástroje `Tracert` cestu k cíli. Nástroj `Tracert` nezaznamená cestu, kterou na zpáteční cestě sledují zprávy odpovědi echa. Může však zjistit, zda byly pakety doručeny do cíle. V tomto případě se pravděpodobně jedná o problém směrování na zpáteční cestě. Pokud trasování nedospěje až k cíli, může to být způsobeno tím, že cílový hostitel je chráněn bránou firewall. Je-li cíl chráněn branou firewall, nemohou pakety příkazu `ping` – ani libovolné jiné zprávy ICMP – kvůli filtrování paketů ICMP projít přes bránu firewall a dosáhnout cíle.

Pokud chcete ověřit, zda není síť zahlcena, stačí pomocí příkazu `ping -w` zvýšit povolenou latenci nastavením delší doby čekání, např. na 5 000 milisekund. Pokuste se znovu zadat příkaz `ping` s adresou cíle. Jestliže stále dochází k vypršení časového limitu požadavku, není to způsobeno zahlcením sítě.

**Unknown Host** Tato chybová zpráva informuje o tom, že požadovaný název hostitele nelze přeložit na příslušnou adresu IP. Zkontrolujte, zda jste název zadali správně a zda jej servery DNS mohou přeložit.

## Testování překladu adres IP na adresy MAC pomocí ARP

Protokol TCP/IP v systému Windows Server 2003 umožňuje aplikacím komunikovat po síti s jiným počítačem pomocí adresy IP, názvu hostitele nebo názvu NetBIOS. Bez ohledu na použitou konvenci názvů je nakonec vždy nutné pro média se sdíleným přístupem, jako jsou sítě Ethernet a Token Ring, přeložit adresu dalšího sme-

rování cíle na hardwarovou adresu – která se také označuje jako adresa MAC (media access control).

Protokol ARP umožňuje, aby hostitel zjistil adresu MAC adresy IP dalšího směrování ve stejné fyzické síti. Aby mohl protokol ARP účinně fungovat, ukládá každý počítač mapování adres

IP na adresy MAC do mezipaměti. Díky tomu není nutné opakovat požadavky všesměrového vysílání ARP.

Nástroj `Arp` uživateli umožňuje zobrazit a upravit položky tabulky ARP v místním počítači. Příkaz `arp` je vhodný k prohlížení mezipaměti ARP a řešení problémů s překladem adres.

Příkazem `arp -s` AdresaIP AdresaMAC lze do souboru ARP přidat statickou položku. Při přidávání těchto statických položek mezipaměti ARP však dbejte opatrnosti, protože lze snadno zadat chybnou adresu MAC pro adresu IP. Všimněte si, že statické položky ARP jsou vymazány při restartu počítače.

## Detekce duplicitních adres IP pomocí protokolu ARP

Systém Windows při spuštění provede automatickou kontrolu ARP kvůli zjištění případných duplicit s vlastní adresou IP. Automatická kontrola ARP je požadavek ARP na vlastní adresu IP uzlu. Pokud uzel odešle rámec požadavku ARP na svou vlastní adresu IP a nepřijme žádný rámec odpovědi ARP, zjistí, že jemu přiřazenou adresu IP nepoužívají žádné jiné uzly. Tento postup sice detekuje většinu případů duplicitních adres IP, ale v několika málo situacích mohou být ve stejné síti nakonfigurováni dva hostitelé TCP/IP (se systémem Microsoft nebo jiným systémem), kteří mají shodnou adresu IP.

Mapování adres MAC a IP zajišťuje modul ARP, který používá první přijatou odpověď ARP. Odpověď z chybně konfigurovaného počítače je tedy v některých případech doručena zpět dříve než odpověď z cílového počítače.

Příkazem `arp -a` lze zobrazit mapování v mezipaměti ARP. Znáte-li adresu MAC vzdáleného počítače, který chcete použít, můžete snadno určit, zda se údaje shodují. Pokud se neshodují, odstraňte položku pomocí příkazu `arp -d` a poté spusťte příkaz `ping` se stejnou adresou (tím vynutíte ARP). Následně znovu zkontrolujte adresu MAC v mezipaměti příkazem `arp -a`.

Jsou-li oba počítače ve stejné síti, dostanete nakonec odpověď z chybně konfigurovaného počítače. V opačném případě může být nutné zachytávat provoz z chybně konfigurovaného hostitele nástrojem Network Monitor, abyste určili vlastníka nebo umístění systému.

**Další informace** Další informace o nástroji Network Monitor naleznete v publikaci *Microsoft® Windows Server™ 2003 Administrator's Companion* (Příručka správce systému Microsoft® Windows Server™ 2003) autorů Russel, Crawford a Gerend (Microsoft Press, 2003).

## Detekce neplatných položek v mezipaměti ARP

Řešení potíží s mezipamětí ARP někdy patří k nejobtížnějším úlohám správy sítě, protože související problémy se často vyskytují nahodile. Výjimkou z tohoto pravi-

dla je, pokud zjistíte, že na požadavek ARP odpovídá nesprávný hostitel a kvůli tomu v mezipaměti ARP vznikne chybná položka. Příznaky chybných položek v mezipaměti ARP je obtížnější reprodukovat a způsobují občasné problémy, které se týkají pouze několika hostitelů. Výchozí problém spočívá v tom, že dva počítače v síti používají stejnou adresu IP. Problémy se objevují pouze občas, protože nejaktuálnější položka tabulky ARP vždy pochází z hostitele, který na libovolný konkrétní požadavek ARP odpověděl rychleji.

Chcete-li tento problém vyřešit, zobrazte tabulku ARP. Na příkazový řádek zadejte:

```
C:\>arp -a 172.16.0.142
```

Zobrazí se výstup podobný následujícímu:

```
Interface: 172.16.0.142
  Internet Address      Physical Address      Type
  172.16.0.1            00-e0-34-c0-a1-40     dynamic
  172.16.1.231          00-00-f8-03-6d-65     dynamic
  172.16.3.34           08-00-09-dc-82-4a     dynamic
  172.16.4.53           00-c0-4f-79-49-2b     dynamic
  157.59.5.102          00-00-f8-03-6c-30     dynamic
```

Adresy přiřazené serverem DHCP zpravidla nezpůsobují konflikty adres, které jsou uvedeny výše. Hlavním zdrojem těchto konfliktů proto bývají statické adresy IP. Jestliže udržujete seznam statických adres (a odpovídajících adres MAC) tak, jak jsou přiřazovány, můžete si tím usnadnit nalezení případných konfliktů adres. Stačí prozkoumat dvojice adres IP a MAC z tabulky ARP a porovnat je se zaznamenanými hodnotami.

Pokud nemáte záznamy o všech dvojicích adres IP a MAC ve své síti, můžete se pokusit vyhledat v adresách MAC nekonzistence v bajtech výrobce. První tři bajty každé adresy MAC určují výrobce karty. Tato tříbajtová čísla se označují jako *identifikátory OUI* (Organizationally Unique Identifiers) a přiřazuje je organizace IEEE (Institute of Electrical and Electronics Engineers). Znáte-li instalované komponenty a porovnáte-li je s hodnotami, které vrátil příkaz **arp -a**, můžete určit, která statická adresa byla zadána chybně.



## Ověření trvalých položek tabulky směrování

Další oblast, kterou je nutné prozkoumat, jsou trvalé položky v použitých tabulkách směrování. Můžete je zobrazit nástrojem `Route`. Trvalé položky lze přidat příkazem `route add -p` nebo pomocí služby Routing and Remote Access. Nesprávné položky můžete změnit příkazem `route change`. Statickou trasu lze přidat pomocí služby Routing and Remote Access.

### Přidání statické trasy pomocí služby Routing and Remote Access

1. Otevřete modul Routing and Remote Access (Směrování a vzdálený přístup).
2. Ve stromu konzoly rozbalte položku **IP Routing** (**Směrování IP**) a klepněte pravým tlačítkem myši na položku **Static Routes (Statické směrování)**.
3. Klepněte na příkaz **New Static Route**.

4. V dialogu **Static Route (Nové statické směrování)** zadejte rozhraní, cíl, masku sítě, bránu a metriku. Pokud se jedná o rozhraní vyžádaného volání, není pole **Gateway (Brána)** k dispozici.

## Použití nástrojů Tracert a Pathping

Pokud je konfigurace tabulky směrování správná, může být problém způsoben směrovačem nebo propojením v libovolném bodě trasy. Chcete-li problém přesně lokalizovat, můžete trasovat cestu k cílovému počítači pomocí nástrojů `Tracert` a `Pathping`.

Pokud k cílovému hostiteli nevede pouze jediná cesta, nezapomeňte mapování trasy pomocí těchto nástrojů několikrát zopakovat, zejména v případech, kdy se pakety ztrácejí pouze občas. Datagram může být odeslán různými cestami a příčinou problému může být vadný směrovač.

Nástroj `Tracert` použijte v případě, kdy nemáte k určitému serveru žádnou konektivitu. Tento nástroj totiž oznámí, kde je konektivita přerušena. Nástroj `Pathping` je užitečnější v případech, kdy k serveru existuje konektivita, ale dochází ke ztrátě některých paketů nebo velkému zpoždění. V těchto případech nástroj `Pathping` přesně informuje, kde ztráta paketů nastává.

## Ověření serverových služeb ve vzdáleném počítači

Systém konfigurovaný jako vzdálená brána nebo směrovač někdy nefunguje jako směrovač. Chcete-li si ověřit, zda je vzdálený počítač, ke kterému se chcete připojit, nastaven k předávání paketů, můžete jej prozkoumat pomocí nástroje pro vzdálenou správu (za předpokladu, že tento počítač sami spravujete) nebo se můžete obrátit na osobu, která počítač spravuje.

Správce odpovědného za vzdálenou síť můžete kontaktovat pomocí údajů v databázích, které udržuje organizace InterNIC. Nejjednodušší je pomocí nástroje `Whois` najít jméno a kontaktní informace příslušné osoby v databázi InterNIC. Nástroj `Whois` naleznete na webu organizace InterNIC na adrese `http://go.microsoft.com/fwlink/?linkid=8177`.

## Kontrola protokolu IPSec v hostiteli, který zahajuje komunikaci

Protokol IP security (IPSec) může zlepšit odolnost sítě před napadením, ale někdy také komplikuje změnu konfigurace sítě nebo řešení potíží. Protokol IPSec spuštěný v iniciujícím hostiteli zkoumaného počítače může způsobit problémy s připojením k jinému hostiteli. Chcete-li určit, zda se jedná o příčinu problémů, dočasně protokol IPSec vypněte pomocí příkazu `net stop policyagent` a potom se pokuste spustit požadovanou síťovou službu nebo funkci.

Pokud se při vypnutí nastavení zásad protokolu IPSec problém neobjeví, je zřejmé, že je způsoben dodatečnou výpočetní zátěží protokolu IPSec nebo jeho filtrování paketů. Abyste tento problém vyřešili, restartujte službu IPSec příkazem `net start policyagent` a potom použijte následující postup.

Chcete-li zobrazit aktivní filtry, zadejte na příkazový řádek následující příkaz:

```
netdiag /test:ipsec /debug
```

Chcete-li výstup tohoto příkazu zobrazit v textovém editoru (např. v Poznámkovém bloku), můžete jej přesměrovat následujícím příkazem:

```
netdiag /test:ipsec /debug > NázevSouboru.txt
```

### Přiřazení nebo zrušení přiřazení zásady IPSec pro zásady skupiny založené na službě Active Directory

1. Spusťte nástroj Active Directory Users and Computers. (Chcete-li spustit nástroj Active Directory Users and Computers, klepněte na tlačítko **Start** a příkaz **Control Panel**, poklepejte na položku **Administrative Tools** a potom poklepejte na položku **Active Directory Users and Computers**.)
2. Ve stromu konzoly rozbalte řadič domény, název domény a organizační jednotku nebo podřízenou organizační jednotku, pro kterou chcete nastavit zásady skupiny.
3. Klepněte na příkaz **Properties** a potom klepněte na kartu **Group Policy**.
4. Klepnutím na tlačítko **Edit** otevřete objekt Group Policy, který chcete upravit, nebo klepnutím na tlačítko **New** vytvořte nový objekt Group Policy a potom klepněte na tlačítko **Edit**.
5. Ve stromu konzoly Group Policy rozbalte název zásady počítače, přejděte na položku **Computer Configuration**, **Windows Settings** a **Security Settings** a potom klepněte na položku **IP Security Policies on Active Directory**.
6. V podokně podrobností klepněte na zásadu protokolu IPSec, kterou chcete přiřadit nebo zrušit její přiřazení, a potom zvolte jednu z následujících akcí:
   - Chcete-li přiřadit zásadu, klepněte v nabídce **Action** na příkaz **Assign**.
   - Pokud chcete zrušit přiřazení zásady, klepněte v nabídce **Action** na příkaz **Unassign**.

### Přiřazení nebo zrušení přiřazení zásady IPSec pro zásady místního počítače

1. Klepněte na tlačítko **Start** a příkaz **Run**, zadejte `MMC` a klepněte na tlačítko **OK**.
2. V nabídce **File** klepněte na příkaz **Add/Remove Snap-in** a klepněte na tlačítko **Add**.
3. Klepněte na položku **Group Policy Object Editor** a potom na tlačítko **Add**.
4. Klepněte postupně na tlačítka **Finish**, **Close** a **OK**.
5. Ve stromu konzoly **Group Policy** rozbalte položku **Local Computer Policy**, přejděte na položku **Computer Configuration**, **Windows Settings** a **Security Settings** a potom klepněte na položku **IP Security Policies on Local Computer**.
6. V podokně podrobností klepněte na zásadu protokolu IPSec, kterou chcete přiřadit nebo zrušit její přiřazení, a potom zvolte jednu z následujících akcí:
   - Chcete-li přiřadit zásadu, klepněte v nabídce **Action** na příkaz **Assign**.
   - Pokud chcete zrušit přiřazení zásady, klepněte v nabídce **Action** na příkaz **Unassign**.

**Poznámka** Další informace o protokolu IPSec v systému Windows Server 2003 získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh IPSECconcepts.chm` a klepnete na tlačítko **OK**.

**Důležité** Zásada protokolu IPSec může zůstat aktivní i poté, co byl odstraněn objekt zásad protokolu IPSec nebo objekt zásad skupiny, ke kterému je přiřazena. Dříve než odstraníte objekt zásad nebo objekt zásad skupiny, měli byste proto zrušit přiřazení zásady protokolu IPSec. Chcete-li předejít potížím, zrušte přiřazení zásady protokolu IPSec v objektu zásad skupiny. Vyčkejte 24 hodin, abyste zajistili, že se změna rozšířila, a potom odstraňte nastavení zásad protokolu IPSec nebo objekt zásad skupiny.

# Kontrola filtrování paketů

Libovolné chyby filtrování paketů na úrovni protokolu TCP/IP, směrovač, serveru proxy, služby Routing and Remote Access nebo protokolu IPSec mohou způsobit selhání překladu adres nebo konektivity. Chcete-li určit, zda je zdrojem problému sítě filtrování protokolu TCP/IP, musíte zakázat filtrování paketů TCP/IP.

## Zakázání filtrování paketů TCP/IP

1. V okně **Control Panel** poklepejte na položku **Network Connections**.
2. Klepněte pravým tlačítkem na připojení a vyberte příkaz **Properties**.
3. Vyberte možnost **Internet Protocol (TCP/IP)** a klepněte na kartu **Properties (Vlastnosti)**.
4. Klepněte na příkaz **Advanced (Upřesnit)** a potom klepněte na kartu **Options (Možnosti)**.
5. Pod nadpisem **Optional Settings** klepněte na položku **TCP/IP Filtering (Filtrování protokolu TCP/IP)** a potom na položku **Properties**.
6. Zrušte zaškrtnutí políčka **Enable TCP/IP Filtering (All adapters) (Povolit filtrování protokolu TCP/IP)** a klepněte na tlačítko **OK**.

Pokuste se znovu zadat příkaz `ping` se zadáním adresy pomocí názvu DNS, názvu NetBIOS nebo číselné adresy IP. Je-li pokus úspěšný, jsou možnosti filtrování paketů pravděpodobně chybně nakonfigurovány nebo jsou příliš omezující. Filtrování může například umožňovat, aby počítač fungoval jako webový server, ale přitom může zakazovat nástroje, jako je `ping` nebo nástroj pro vzdálenou správu. Širší rozsah přípustných možností filtrování obnovíte změnou povolených hodnot portů TCP, UDP a IP.

**Poznámka** Pokud ani tento postup není úspěšný, může být činnost sítě narušena jinou formou filtrování paketů. Další informace o funkcích filtrování paketů IP služby Routing and Remote Access získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh RRASconcepts.chm` a klepnete na tlačítko **OK**. Další informace o filtrování paketů IPSec získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh IPSECconcepts.chm` a klepnete na tlačítko **OK**.

# 6.3 Nelze se připojit k hostiteli nebo názvu NetBIOS

Protokol TCP/IP v systému Windows Server 2003 umožňuje aplikacím komunikovat po síti s jiným počítačem pomocí tří typů označení cíle:

- adresa IP,
- název hostitele,
- název NetBIOS.

Tato část popisuje způsob řešení potíží s překladem názvů hostitele nebo názvů NetBIOS. Problémy s adresováním IP se zabývá část „Nelze se připojit k adrese IP“ v této kapitole.

Nejdříve je nutné určit, které aplikace nejsou funkční. K těmto aplikacím obvykle patří Internet Explorer, `net use`, Telnet a FTP. Tyto informace vám pomohou při dalším kroku, který určuje, zda je selhání způsobeno problémem názvu hostitele nebo problémem překladu názvu NetBIOS.

Chcete-li rozlišit problémy názvů hostitele od problémů s překladem názvů NetBIOS, je nejjednodušší zjistit, zda chybně fungující aplikace pracuje s názvy NetBIOS nebo se sokety. Pokud používá sokety, spočívá problém v překladu názvu hostitele. Aplikace založené na názvech NetBIOS patří k nejrozšířenějším. Jedná se mj. o různé příkazy `net`, Průzkumník Windows a složku My Network Places. Sokety používá např. aplikace Internet Explorer a jiné webové prohlížeče, služby Telnet a FTP.

V následujících částech jsou popsány procesy, ke kterým dochází, když se pro připojení k hostiteli v síti TCP/IP používá název hostitele nebo název NetBIOS.



## Error 53

Problémy s překladem názvů NetBIOS se nejčastěji projevují tím, že příkaz `ping` vrací zprávu Error 53. Zpráva Error 53 je obvykle vrácena v případě, že překlad názvů není pro určitý název počítače úspěšný. Zpráva Error 53 se také může objevit, pokud dojde k problémům při navázání relace NetBIOS. Chcete-li mezi těmito případy rozlišit, postupujte následovně:

### Určení příčiny zprávy Error 53

- Na příkazový řádek zadejte

  `net view \\`*`NázevHostitele`*

  kde *`NázevHostitele`* je síťový prostředek, o kterém víte, že je aktivní.

Pokud je příkaz úspěšný, znamená to, že překlad názvů pravděpodobně potíže nezpůsobuje. Abyste si to ověřili, zadejte příkaz `ping` s názvem hostitele, protože překlad názvů může někdy fungovat správně i v případech, kdy příkaz `net use` vrací zprávu Error 53 (např. tehdy, kdy server DNS nebo WINS obsahuje chybnou položku). Pokud příkaz `ping` potvrdí, že překlad názvů není úspěšný (vrácením zprávy „Unknown host“), zkontrolujte stav své relace NetBIOS.

### Kontrola stavu relace NetBIOS

- Na příkazový řádek zadejte

  `net view \\AdresaIP`

  kde *AdresaIP* označuje stejný síťový prostředek, který jste použili v postupu pro určení příčiny zprávy Error 53.

Není-li ani tento postup úspěšný, leží problém v navazování relace.

Jestliže je počítač v místní podsíti, zkontrolujte, zda jste jeho název zadali správně a zda je protokol TCP/IP spuštěn i v cílovém počítači. Pokud počítač není v místní podsíti, ověřte si, zda je mapování jeho názvu a adresy IP k dispozici v databázi DNS, souboru `Hosts` či `Lmhosts` nebo v databázi WINS.

Jestliže se domníváte, že jsou všechny prvky protokolu TCP/IP nainstalovány správně, použijte příkaz `ping` s adresou vzdáleného počítače. Tím zkontrolujete, zda je protokol TCP/IP funkční.

## Nelze se připojit ke vzdáleným systémům pomocí názvu hostitele

Pokud potíže nezpůsobuje název NetBIOS, ale sokety, souvisí problém buď s položkou v souboru Hosts, nebo chybou konfigurace DNS. Chcete-li určit, proč lze připojení ke vzdáleným počítačům navázat pouze pomocí adres IP a nikoli názvů hostitele, zkontrolujte, zda byl v počítači nakonfigurován příslušný soubor `Hosts` a nastaven systém DNS.

### Kontrola souboru Hosts

Položky v souboru `Hosts` slouží k vytvoření položek v mezipaměti překládání klienta DNS, které lze zobrazit příkazem `ipconfig /displaydns`. Zkontrolujte, zda mezipaměť překládání klienta DNS a soubor Hosts obsahují správné položky.

### Kontrola konfigurace DNS

Používáte-li systém DNS, ověřte si, zda jsou ve vlastnostech TCP/IP správně zadány adresy IP serverů DNS a mají správné pořadí. Postupujte přitom následovně:

### Kontrola konfigurace DNS

1. V dialogu Control Panel poklepejte na položku Network Connections.
2. Klepněte pravým tlačítkem na připojení, které chcete prozkoumat, a vyberte příkaz **Properties**.
3. Vyberte možnost **Internet Protocol (TCP/IP)** a klepněte na kartu **Properties**.
4. V dialogu **Microsoft TCP/IP Properties** klepněte na tlačítko **Advanced**.
5. Klepněte na kartu **DNS**.
6. Zkontrolujte, zda je systém DNS nakonfigurován správně. Pokud chybí adresa IP serveru DNS, přidejte ji do seznamu adres serverů DNS.

Tento postup je určen pro systémy, kde je na kartě **General** okna **TCP/IP Properties** zaškrtnuto políčko **Use the following DNS server address (Použít následu-**

**jící adresy serverů DNS)** (staticky konfigurované počítače). Klienti DHCP nemají v seznamu servery DNS.

Zadejte příkaz `ping` s názvem hostitele vzdáleného počítače a potom s jeho adresou IP, abyste určili, zda dochází ke správnému překladu adresy hostitele. Pokud příkaz `ping` není úspěšný s názvem hostitele, ale pouze s použitím adresy IP, spočívá problém v překladu názvů. Chcete-li vyzkoušet, zda jsou servery DNS spuštěny, zadejte příkaz `ping` s jejich adresou IP nebo na serveru DNS otevřete relaci Telnet na portu 53. Je-li připojení úspěšně navázáno, služba DNS na serveru DNS funguje. Jakmile jste ověřili, že je služba DNS spuštěna, můžete pomocí nástroje `Nslookup` odesílat dotazy na server DNS, abyste dále zkontrolovali stav hledaných záznamů.

**Tip** Další informace o programu Telnet získáte zadáním příkazu `Telnet /?` na příkazový řádek.

Pokud nejsou úspěšné příkazy `ping` s adresou IP ani s názvem, jedná se o potíže se síťovou konektivitou, např. základní konektivitou nebo směrováním. Další informace o řešení potíží se síťovou konektivitou naleznete v části „Řešení potíží směrování IP“ v této kapitole.

**Překlad názvu hostitele pomocí serveru DNS** DNS je distribuovaná databáze, která mapuje názvy domén na data. Uživatel, který chce vyhledat počítače a jiné prostředky v síti IP, se může dotázat služby DNS pomocí hierarchických popisných názvů. Služba díky tomu z velké části nahrazuje funkci, kterou dříve plnil soubor `Hosts`. Služba DNS překládá popisné názvy na adresy IP, jak je popsáno v následujícím příkladu.

**Poznámka** Odpověď na dotaz může poskytnout libovolný server na trase. Další iterativní dotazy proto nejsou nutné.

- Klient kontaktuje názvový server DNS s rekurzivním dotazem na adresu *name*.contoso.com. Server musí nyní vrátit odpověď nebo chybovou zprávu.
- Názvový server DNS zkontroluje své soubory mezipaměti a zóny, ale nepodaří se mu odpověď najít. Kontaktuje kořenový server Internetu (kořenový server DNS) s iterativním dotazem na název *name*.contoso.com.
- Kořenový server odpověď nezná, takže odpoví odkazem na oprávněný server v doméně .com.
- Názvový server DNS kontaktuje server v doméně .com a předá mu iterativní dotaz na název .contoso.com.
- Server v doméně .com nedokáže poskytnout přesnou odpověď, takže odpoví odkazem na oprávněný server v doméně contoso.com.
- Názvový server DNS kontaktuje server v doméně contoso.com a předá mu iterativní dotaz na název *name*.contoso.com.
- Server v doméně contoso.com odpověď zná. Odešle odpověď se správnou adresou IP.
- Názvový server DNS poskytne klientovi jako odpověď na dotaz adresu IP serveru *name*.contoso.com.

**Další informace** Tento příklad se týká pouze Internetu. Další informace o překladu názvu hostitele DNS, rekurzivních a iterativních dotazech získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh DNSconcepts.chm` a klepnete na tlačítko **OK**.

**Chybové zprávy DNS** K chybám v překladu názvů může dojít, pokud nejsou položky serveru DNS nebo klienta nakonfigurovány správně, server DNS není spuštěn nebo nastaly potíže se síťovou konektivitou. Chcete-li určit příčinu případného problému s překladem názvů, můžete použít nástroj `Nslookup`.

Neúspěšné dotazy vrátí různé zprávy, které závisí na povaze selhání. Pokud např. při zadání následujícího příkazu:

```
C:\nslookup CílovýHostitel
```

server nedokáže název přeložit, je zobrazen tento výstup:

```
Server: ÚplnýNázevDomény
Address: AdresaIPServeru
*** ÚplnýNázevDomény can't find CílovýHostitel: Non-existent domain
```

V jiných případech vyprší časový limit požadavku na službu DNS bez odpovědi a vrácena je zpráva v následujícím formátu:

```
C:\nslookup PlatnýHostitel
Server: [AdresaIP]
Address: w.x.y.z
DNS request timed out.
timeout was 2 seconds.
```

Pokud server na požadavek neodpoví, vrátí nástroj `Nslookup` chybovou zprávu v následujícím formátu:

```
C:\nslookup
*** Can't find server name for address AdresaIP: No response from server
*** Default servers are not available.
```

Tato zpráva znamená, že server DNS je nedosažitelný. Neuvádí, proč není server dostupný. Server může být offline, v hostitelském počítači nemusí být povolena služba DNS nebo mohlo dojít k potížím hardwaru nebo směrování.

**Další informace** Další informace o řešení potíží služby DNS získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh DNSconcepts.chm` a klepnete na tlačítko **OK**.

**Překlad názvu hostitele pomocí souboru Hosts** Počítač, který překládá názvy pomocí souboru `Hosts`, provádí následující kroky.

- Počítač A zadá příkaz pomocí názvu hostitele počítače B.
- Počítač A zkontroluje obsah mezipaměti překládání klienta DNS, která obsahuje položky v souboru `Hosts`. Pokud je hostitelský název počítače B nalezne, přeloží se na adresu IP. Potom je odeslán paket s použitím běžných postupů pro určení směrování a překlad adres.

Následující problémy souboru Hosts mohou být příčinou síťových chyb:

- Soubor Hosts neobsahuje název příslušného hostitele.
- Název hostitele v souboru Hosts nebo v příkazu je zadán chybně.
- Adresa IP pro název hostitele v souboru Hosts není platná nebo je chybná.
- Soubor Hosts obsahuje na samostatných řádcích více položek pro stejného hostitele. Analýza souboru Hosts probíhá od začátku souboru. Do mezipaměti překládání klienta DNS je proto umístěna první položka.

Tento soubor není aktualizován dynamicky. Všechny položky se přidávají ručně a adresa IP a popisný název hostitele se vždy oddělují jednou nebo více mezerami nebo tabulátory. Soubor má následující formát:

```
Adresa IP           Popisný název
172.16.48.10        testpc1          # Poznámky jsou označeny znakem #.
```

Pokud dochází k potížím při připojení ke vzdálenému systému pomocí názvu hostitele a používáte k překladu názvů soubor Hosts, může být problém způsoben obsahem tohoto souboru. Zkontrolujte, zda je správně zadán název vzdáleného počítače v souboru Hosts a v aplikaci, která jej používá. Soubor Hosts je umístěn ve složce *systemroot*\System32\Drivers\Etc.

## Kontrola souboru Lmhosts

Problém s překladem názvů může spočívat v souboru Lmhosts, který umožňuje sekvenční vyhledání adres pro názvy NetBIOS odshora dolů. Pokud je pro stejný název hostitele uvedeno více adres, vrátí protokol TCP/IP první nalezenou hodnotu bez ohledu na to, zda je správná.

Soubor Lmhosts naleznete ve složce *systemroot*\System32\Drivers\Etc. Tento soubor není ve výchozím nastavení vytvořen. Existuje ukázkový soubor s názvem Lmhosts.sam. Chcete-li tento soubor použít, musíte jej nejdříve přejmenovat nebo zkopírovat na soubor Lmhosts.

Výchozím adresářem tohoto souboru je sice *systemroot*\System32\Drivers\Etc, ale konkrétní dotazovaný soubor Lmhosts závisí na hodnotě položky DataBasePath v následujícím podklíči registru:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Položka DataBasePath sděluje místnímu počítači, kde je soubor Lmhosts umístěn.

**Upozornění** Nesprávné úpravy registru mohou vážně poškodit systém. Před prováděním změn registru je vhodné zálohovat všechna důležitá data v počítači.

**Dlouhé navazování připojení pomocí souboru Lmhosts** Chcete-li určit příčinu pomalého navazování připojení poté, co jste přidali položku do souboru Lmhosts, zkontrolujte pořadí položek v tomto souboru.

Připojení se může navazovat dlouho, pokud je konkrétní položka umístěna na konci velkého souboru Lmhosts. Pokud chcete překlad položky urychlit, označte položku v souboru Lmhosts jako přednačtenou položku tím, že za mapováním uvedete značku

#PRE. Potom příkazem nbtstat -R proveďte okamžitou aktualizaci místní mezipaměti názvů NetBIOS.

Případně můžete umístit mapování blíže k začátku souboru Lmhosts. Při hledání položek bez klíčového slova #PRE je soubor Lmhosts analyzován sekvenčně od začátku. Často používané položky je proto vhodné vždy umístit poblíž začátku souboru a položky označené značkou #PRE na konec souboru.

**Další informace** Další informace o mapování položky v souboru Lmhosts pomocí klíčového slova #PRE naleznete v příručce *Microsoft Windows 2000 Server TCP/IP Core Networking Guide* (Průvodce základy sítí TCP/IP systému Microsoft Windows 2000 Server) (Microsoft Press, 2002).

### Kontrola konfigurace WINS

Zkontrolujte, zda je v počítači správně nakonfigurována služba WINS. Ověřte zejména adresu serveru WINS.

### Prozkoumání konfigurace WINS

1. V okně Control Panel poklepejte na položku Network Connections.
2. Klepněte pravým tlačítkem na připojení, které chcete prozkoumat, a vyberte příkaz **Properties**.
3. Na kartě **General** vyberte možnost **Internet Protocol (TCP/IP)** a klepněte na položku **Properties**.
4. V dialogu **Internet Protocol (TCP/IP) Properties** klepněte na tlačítko **Advanced**.
5. V dialogu **Advanced TCP/IP Settings** klepněte na kartu **WINS**.
6. Do dialogu **WINS Configuration** přidejte adresu IP serveru (pokud není žádná adresa uvedena) a ověřte, zda je povolena možnost **Lmhosts lookup (Povolit hledání v souboru LMHOSTS)**. Zkontrolujte také, zda je rozhraní NetBIOS nad protokolem TCP/IP převzato ze serveru DHCP, je povoleno nebo zakázáno. Používáte-li v tomto hostitelském počítači službu DHCP, převezměte hodnotu ze serveru DHCP. Jinak povolte rozhraní NetBIOS nad protokolem TCP/IP.

## 6.4 Řešení problémů se směrováním IP

Systém Windows Server 2003 podporuje směrování IP v počítačích s jednou či více adresami bez ohledu na to, zda používají službu Routing and Remote Access. Služba Routing and Remote Access zahrnuje směrovací protokoly RIP (Routing Information Protocol) a OSPF (Open Shortest Path First). Směrovače si mohou pomocí protokolů RIP nebo OSPF dynamicky vyměňovat informace o směrování.

Tato část obsahuje informace o tabulce směrování v systému Windows Server 2003, jak se používá v počítačích s jednou či více adresami a se službou Routing and Remote Access nebo bez ní. Tyto teoretické informace usnadňují řešení potíží protokolu TCP/IP.

**Další informace** Další informace o jednosměrovém a vícesměrovém směrování TCP/IP naleznete v příručce *Microsoft Windows 2000 Server Resource Kit Internetworking Guide* (Průvodce propojením sítí) sady Resource Kit systému Microsoft Windows 2000 Server (Microsoft Press, 2002).

## Nelze se připojit k zadanému serveru

Máte-li problémy s připojením k určitému serveru pomocí protokolu NetBIOS, zjistěte pomocí příkazu `nbtstat -n`, které názvy NetBIOS server použil při registraci do sítě.

Výstup příkazu `nbtstat -n` obsahuje několik názvů, které počítač registroval. Součástí výpisu by měla být položka, která připomíná název počítače tak, jak je uveden na ploše. V opačném případě vyzkoušejte jeden z dalších jedinečných názvů zobrazených příkazem `nbtstat`.

Nástroj `nbtstat` může také zobrazit položky uložené do mezipaměti na základě položek typu PRE v souboru `Lmhosts` nebo z aktuálně přeložených názvů NetBIOS. Pokud se shoduje název NetBIOS, který počítače pro tento server používají, a jiné počítače jsou ve vzdálené podsíti, zkontrolujte, zda mohou počítač mapovat pomocí svých souborů Lmhost nebo serverů WINS.

### Servery s více funkcemi

Služby směrování mohou poskytovat servery s jinými úlohami, zejména v místních sítích. Máte-li přístup k serveru, který se chová problematicky, zejména pouze občas, můžete ověřit, zda prostředky serveru nejsou zatěžovány jinými službami či aplikacemi nebo zda některý uživatel nekopíruje velké soubory na server nebo z něj. Toto doporučení se týká i klientských počítačů. Lze to zjistit např. následujícím postupem: spusťte aplikaci Computer Management (klepněte pravým tlačítkem myši na ikonu **My Computer** a vyberte příkaz **Manage**), rozbalte položku **Shared Folders** a vyberte složku **Sessions**, abyste zobrazili uživatele aktuálních relací počítače. Z konzoly Computer Management lze spustit nástroj Event Viewer, který umožňuje zobrazit, kdo přistupoval k serveru, případně zda v určitých časech nebo s pravidelnou frekvencí nedocházelo k jiným potížím. Jinou metodou je spustit Task Manager a zkontrolovat, které aplikace nebo procesy jsou spuštěny a jak ovlivňují využití procesoru.

### Zablokované připojení ke vzdálenému hostiteli

Chcete-li určit, proč připojení TCP/IP ke vzdálenému počítači nefunguje správně, zobrazte příkazem `netstat -a` stav veškeré aktivity na portech TCP a UDP v místním počítači.

Kvalitní připojení TCP zpravidla ukazuje 0 bajtů ve frontách **Sent** a **Received**. Pokud jsou data v některé z front blokována, připojení pravděpodobně nefunguje správně. V opačném případě se nejspíše jedná o zpoždění sítě nebo aplikace.

### Prozkoumání tabulky směrování příkazem Route

Aby si dva hostitelé mohli vyměňovat datagramy IP, musejí mít oba trasu k sobě navzájem nebo používat výchozí brány, které trasu znají. Směrovače si obvykle mezi sebou vyměňují informace pomocí směrovacího protokolu, jako je např. RIP.

### Povolení směrování IP

Směrování IP je ve výchozím nastavení zakázáno. Chcete-li směrování IP povolit, musíte počítači umožnit předávat pakety IP, které přijme. Pokud nepovolíte směrování pomocí služby Routing and Remote Access, musíte ručně upravit registr.

**Upozornění** Nesprávné úpravy registru mohou vážně poškodit systém. Před prováděním změn registru je vhodné zálohovat všechna důležitá data v počítači.

### Povolení směrování IP

1. Klepněte na tlačítko **Start** a příkaz **Run**, zadejte `regedit.exe` a klepněte na tlačítko **OK**.
2. V programu Registry Editor přejděte na klíč `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`
3. Vyberte položku `IPEnableRouter`.
4. Klepněte na nabídku **Edit** a vyberte příkaz **Modify**.
5. V poli **Value data** nastavte hodnotu 1, abyste povolili směrování IP pro všechna síťová připojení, která jsou v příslušném počítači nainstalována a používána.
6. Ukončete program Registry Editor.

Jestliže směrovač se systémem Windows Server 2003 nemá rozhraní s danou podsítí, vyžaduje zadání trasy, která vede do dané podsítě. Lze k tomu použít výchozí trasu nebo je možné přidat statické trasy. Chcete-li přidat statickou trasu, použijte službu Routing and Remote Access nebo příkaz `route add`. Například:

```
route add 172.16.41.0 mask 255.255.255.0 172.16.40.1 metric 2
```

V tomto příkladu příkaz `route add` určuje, že podsíť `172.16.41.0` s maskou `255.255.255.0` je přístupná pomocí brány `172.16.40.1`. Ukazuje také, že podsíť je vzdálena dvě směrování. U podřízených směrovačů může být nutné přidat statické trasy, které určují, jak lze přejít zpět do podsítě `172.16.40.0/24`.

Pokud požadujete, aby trasa přetrvala i po restartu, přidejte na konec příkazového řádku parametr `-p`. Trvalé trasy jsou zaznamenány do registru.

### Prozkoumání cest příkazem Tracert

`Tracert` je nástroj na trasování tras, který postupně zvyšuje hodnoty pole TTL v záhlaví paketu IP, aby určil síťovou trasu od jednoho hostitele k druhému. Odesílá přitom zprávy ICMP „Echo“ a analyzuje vrácené chybové zprávy protokolu ICMP. Nástroj `Tracert` umožňuje určit cestu paketu předaného ze směrovače na směrovač do vzdálenosti 30 směrování. Pokud došlo k chybě směrovače nebo je paket směrován ve smyčce, nástroj `Tracert` tento problém odhalí. Jedná-li se o cizí směrovač, lze po nalezení problémového směrovače kontaktovat jeho správce. Jestliže je směrovač pod vaší kontrolou, můžete plně obnovit jeho funkční stav.

## Řešení problémů s branami

Pokud se při instalaci a konfiguraci operačního systému zobrazí zpráva „Your default gateway does not belong to one of the configured interfaces…“, zkontrolujte,

zda je výchozí brána umístěna ve stejné logické síti jako síťový adaptér počítače. Nejjednodušší je přitom porovnat části adres IP výchozí brány a síťových adaptérů počítače, které odpovídají ID sítě. Jinými slovy zkontrolujte, zda se logická bitová funkce AND adresy IP a masky podsítě rovná logické bitové funkci AND výchozí brány a masky podsítě.

Počítač s jediným síťovým adaptérem, který má nastavenu adresu IP `172.16.27.139` a masku podsítě `255.255.0.0` například vyžaduje výchozí bránu ve tvaru `172.16.y.z`. ID sítě rozhraní IP je `172.16.0.0/16`. Pomocí masky podsítě může protokol TCP/IP určit, že veškerý provoz v této síti je místní. Všechna ostatní data je nutné odeslat bráně.

## Řešení problémů s ARP přes server proxy

ARP přes server proxy odpovídá na požadavky ARP ve prospěch jiného uzlu. Jak je popsáno ve standardu RFC 925, uplatňuje se ARP přes server proxy v situacích, kdy je podsíť rozdělena bez použití směrovače. Zařízení ARP přes server proxy je umístěno mezi uzly, které nejsou ve stejné logické podsíti. ARP přes server proxy odpovídá na požadavky ARP a umožňuje předávat pakety IP jednosměrového vysílání při komunikaci mezi uzly v oddělených segmentech.

K příkladům zařízení ARP přes server proxy patří:

- Služba Routing and Remote Access v počítačích se systémem Windows Server 2003, která pomocí ARP přes server proxy umožňuje komunikaci mezi klienty vzdáleného přístupu a uzly v síťovém segmentu, ke kterému je připojen server vzdáleného přístupu.
- Funkce Network Bridge v systémech Windows XP a Windows Server 2003 Standard Edition a ve 32bitové verzi systému Windows Server 2003 Enterprise Edition, která funguje jako zařízení ARP přes server proxy v případech, kdy zajišťuje přemostění mezi síťovými segmenty na vrstvě 3.

Síťový provoz v některých případech nefunguje, protože požadavek ARP přes server proxy směrovače vrátí chybnou adresu. Směrovač odešle tento požadavek ARP ve prospěch adresy IP ve svých interních podsítích (stejně jako server vzdáleného přístupu provádí požadavek na místní síť za své klienty vzdáleného přístupu). Problém spočívá v tom, že požadavek ARP přes server proxy odeslaný směrovačem vrátí odesílajícímu hostiteli chybnou adresu MAC. Odesílající hostitel proto odešle data na nesprávnou adresu MAC. Jinými slovy jsou potíže způsobeny odpověďmi ARP přes server proxy.

Chcete-li tento problém vyřešit, zachyťte trasu pomocí nástroje Network Monitor. Pokud trasování ukáže, že když odesílající hostitel odešle požadavek ARP na adresu MAC cílové adresy IP, odpoví zařízení (obvykle směrovač) chybnou adresou MAC, pravděpodobně není správný překlad adresy IP na adresu MAC v cílovém počítači.

**Další informace** Další informace o nástroji Network Monitor získáte, když v počítači se systémem Windows Server 2003 klepnete na tlačítko **Start** a příkaz **Run**, zadáte příkaz `hh NETMNconcepts.chm` a klepnete na tlačítko **OK**.

Abyste určili, zda se jedná o tento problém, zkontrolujte, zda má mezipaměť ARP zdrojového hostitele k dispozici správný překlad adres IP na adresy MAC. Případně

lze zachytávat veškerý provoz nástrojem Network Monitor a poté zachycený provoz odfiltrovat, aby se zobrazily pouze protokoly ARP a RARP (Reverse Address Resolution Protocol). Protokol RARP převádí adresy MAC na adresy IP a je definován ve standardu RFC 903.

Potíže protokolu ARP lze vyřešit zakázáním ARP přes server proxy v zařízení, které problémy způsobuje. Přesný postup závisí na výrobci a modelu zařízení. Informace naleznete v dokumentaci dodané výrobcem.

## Řešení problémů přemostění s překladem

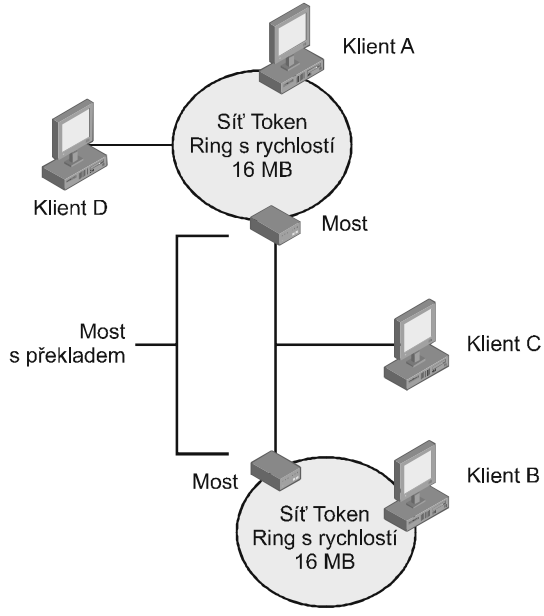
Chcete-li umožnit segmentům sítě Ethernet, aby komunikovaly s uzly v síti Token Ring, je nutné vyřešit několik problémů. Dále jsou uvedeny nejčastější potíže, které se týkají přemostění s překladem.

Za potíže v této konfiguraci odpovídá zejména odlišná hodnota MTU (Maximum Transmission Units) mezi segmenty. Hodnoty MTU v síti Token Ring kolísají mezi 4 464 a 17 914 bajty. Hodnota MTU v síti Ethernet je 1 500. Segment FDDI má hodnotu MTU 4 532 bajtů. Pokud jsou tyto odlišné síťové technologie propojeny mostem nebo přepínačem vrstvy 2, mohou být některé pakety zahozeny, protože přepínač vrstvy 2 nedokáže fragmentovat data ani upozornit odesílající uzel na sníženou hodnotu MTU.

V příkladu na obrázku 6.1 spojuje páteřní síť Ethernet dvě sítě Token Ring s rychlostí 16 MB. Místo směrovače propojuje segmenty most s překladem v podobě přepínače vrstvy 2. V tomto případě místní provoz v sítích Token Ring používá hodnotu MTU 17 914 a most na něj nemá vliv. Pokud však klient A potřebuje komunikovat s klientem B, zahodí most velké pakety, aniž by klienta A upozornil na nutnost fragmentace. V této situaci klient A nedokáže nijak zjistit hodnotu MTU na druhé straně mostu.

Problémy přemostění s překladem se také mohou projevit tím, že lze úspěšně odeslat příkaz `ping` na počítač na vzdálené straně mostu a navázat připojení, ale není možné odesílat objemná data. Dochází k tomu proto, že zprávy „Echo“ a segmenty pro navázání připojení TCP jsou malé. Při odesílání objemných dat se však odesílají velké segmenty s velikostí MTU místně připojené sítě, které přepínač vrstvy 2 zahodí. Jiným příkladem je, když počítač může navázat relaci pomocí FTP, ale nelze použít příkaz `get` *`NázevSouboru`*, který předpokládá odeslání většího paketu přes přepínač.

V systému Windows Server 2003 je možné upravit položku registru pro hodnotu MTU tak, aby splňovala požadavky MTU segmentu sítě Ethernet, který spojuje oba segmenty sítě Token Ring. Hodnota MTU je přitom snížena na nejnižší velikost, kterou podporují všechna propojení v podsíti. Hodnota MTU všech uzlů je omezena na 1 500 bajtů, aby vyhovovala požadavkům páteřní sítě Ethernet. Toto řešení však vyžaduje, aby byl veškerý provoz (včetně místního provozu v síti Token Ring) odesílán s omezenou hodnotou MTU.




**OBRÁZEK 6.1:** Propojení dvou sítí Token Ring pomocí mostu sítě Ethernet

## Určení hodnoty MTU příkazem Ping

Pomocí příkazu `ping -l -f` můžete odesílat pakety zpráv ICMP „Echo“ s určenou velikostí dat. Parametr `-f` zajišťuje, že pakety nebudou fragmentovány. Odesláním paketů s různou velikostí lze určit hodnotu MTU pro libovolný konkrétní most na základě velikosti paketů, které jsou úspěšně přeneseny přes most. Na obrázku 6.1 lze například z klienta A klientovi C odeslat paket příkazu `ping` s velikostí 1 472 bajtů, který generuje paket odpovědi echa od klienta C. Pokud se však použije velikost 1 473 bajtů nebo větší, mezilehlý přepínač paket zahodí. Klient C zprávu „Echo“ neobdrží a negeneruje žádnou odpověď echa.

Výchozí zpráva ICMP „Echo“ obsahuje 32 bajtů dat. Pomocí příkazu `ping` *`AdresaIP`* nebo *`NázevHostitele`* `-l` *`VelikostDat`* můžete určit jinou velikost dat. Zadáním následujícího příkazu můžete například odeslat příkaz `ping` s maximální velikostí dat sítě Ethernet:

```
ping 134.56.78.1. -l 1472
```

Parametrem `-l` je nastavena velikost 1 472 místo hodnoty 1 500 pro IP MTU sítě Ethernet, protože 20 bajtů je vyhrazeno pro záhlaví paketu IP a 8 bajtů je nutné přidělit záhlaví zprávy ICMP „Echo“.

Když jste zjistili hodnotu MTU, můžete nastavit velikost paketu na obou stranách mostu změnou hodnoty položky registru. Položku registru pro hodnotu MTU naleznete v následujícím podklíči:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
Interfaces\GUID_Adaptéru
```

**Upozornění** Nesprávné úpravy registru mohou vážně poškodit systém. Před prováděním změn registru je vhodné zálohovat všechna důležitá data v počítači.

**Další informace** Další informace o hodnotě MTU naleznete v knize *Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference* (Technická referenční příručka protokolů a služeb TCP/IP v systému Microsoft Windows Server 2003) autorů Joseph Davies a Thomas Lee (Microsoft Press, 2003).

## Řešení problémů se směrovači PMTU „černá díra"

Některé směrovače neodesílají zprávu „ICMP Destination Unreachable-Fragmentation Needed and DF Set", když nemohou předat datagram IP. Místo toho datagram tiše zahodí. Datagram IP nelze předat obvykle proto, že je jeho maximální velikost segmentu pro přijímající server příliš velká a v záhlaví datagramu je nastaven bit „Don't Fragment". Směrovače, které tyto datagramy ignorují a neodesílají žádnou zprávu, se označují jako směrovače PMTU „černá díra".

Abyste mohli účinně reagovat na směrovače „černá díra", musíte v protokolu TCP/IP povolit funkci PMTU rozpoznávání černých děr. PMTU rozpoznávání černých děr detekuje opakované nepotvrzené přenosy a reaguje na ně vypnutím bitu „Don't Fragment". Po úspěšném přenosu datagramu omezí maximální velikost segmentu a znovu bit „Don't Fragment" zapne.

Funkce PMTU rozpoznávání černých děr je ve výchozím nastavení zakázána, ale můžete ji povolit, když do registru přidáte položku `EnablePMTUBHDetect` a nastavíte její hodnotu na `1`. `EnablePMTUBHDetect` je volitelná položka, která není v registru obsažena, dokud ji nepřidáte do následujícího podklíče:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

**Upozornění** Nesprávné úpravy registru mohou vážně poškodit systém. Před prováděním změn registru je vhodné zálohovat všechna důležitá data v počítači.

PMTU rozpoznávání černých děr lze zakázat odstraněním položky `EnablePMTUBHDetect` z registru nebo nastavením její hodnoty na `0`.

Problém směrovačů PMTU „černá díra" řeší i druhá položka registru, `EnablePMTUDiscovery`. Tento klíč je ve výchozím nastavení povolen. Položka `EnablePMTUDiscovery` kompletně povoluje nebo zakazuje mechanismus rozpoznávání PMTU. Pokud je rozpoznávání PMTU zakázáno, používá se pro všechny adresy, které nejsou místní, hodnota MSS (Maximum Segment Size) protokolu TCP 536 bajtů.

## Rozpoznání PMTU příkazem Ping

Hodnotu PMTU mezi dvěma hostiteli lze zjistit ručně pomocí příkazu `ping -f`:

```
ping -f -n PočetPříkazůPing [-l Velikost] CílováAdresaIP
```

Následující příklad znázorňuje, jak je možné měnit parametr velikosti příkazu `ping`, dokud není zjištěna hodnota MTU. Všimněte si, že parametr velikosti příkazu `ping` určuje pouze velikost odeslaných dat zprávy ICMP „Echo" a nezahrnuje záhlaví paketu IP a zprávy ICMP „Echo". Záhlaví zprávy ICMP „Echo" má 8 bajtů a záhlaví paketu IP je

obvykle velké 20 bajtů. V tomto případě sítě Ethernet zahrnuje hodnota MTU linkové vrstvy maximální velikost vyrovnávací paměti příkazu `Ping` zvýšenou o 28, což poskytuje 1 500 bajtů v prvním příkazu `ping` a 1 501 v druhém příkazu:

```
C:\>ping -f -n 1 -l 1472 10.99.99.10
Pinging 10.99.99.10 with 1472 bytes of data:
Reply from 10.99.99.10: bytes=1472 time<10ms TTL=128
Ping statistics for 10.99.99.10:
  Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping -f -n 1 -l 1473 10.99.99.10
Pinging 10.99.99.10 with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Ping statistics for 10.99.99.10:
  Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

V druhém příkazu `ping` vrátí vrstva IP chybovou zprávu ICMP, kterou příkaz `Ping` interpretuje. Pokud se jedná o směrovač „černá díra“, neodešle odpověď na příkaz `Ping` poté, co jeho velikost překročí maximální hodnotu MTU, kterou směrovač dokáže zpracovat. Tímto způsobem lze pomocí příkazu `Ping` příslušný směrovač zjistit.

# 6.5 Řešení problémů služeb



Protokol TCP/IP zajišťuje základní síťovou komunikaci a kromě toho jsou na něm založeny mnohé síťové služby, jako například Routing and Remote Access, tisk, IPSec a Computer Browser. Tyto služby jsou podrobněji popsány v jiných kapitolách, ale v této části si uvedeme několik příkladů, jak řešit jejich běžné potíže.

## Nelze odeslat příkaz ping přes směrovač jako klient vzdáleného přístupu

Tento problém se objevuje, pokud jste na kartě **General** dialogu **Advanced Internet Protocol (TCP/IP) Properties** na stránce **Dial-Up Connections** zaškrtli políčko **Use default gateway on remote network**. Tato funkce přidá do tabulky směrování výchozí trasu, která má nižší metriku než existující výchozí trasa, a případně upraví metriku existující výchozí trasy. Veškerý provoz, který není místní, je nyní směrován na bránu propojení vzdáleného přístupu. Kvůli přístupu k síti Internet je však nutné tuto funkci povolit.

Chcete-li odeslat příkaz `ping` nebo se jinak připojit k počítačům ve vzdálené podsíti za směrovačem, jste-li připojeni jako klient vzdáleného přístupu k serveru vzdáleného přístupu vzdáleného systému Windows, přidejte příkazem `route add` trasu podsítě, kterou chcete použít.

## Řešení problémů s databázomi soubory TCP/IP

Tabulka 6.2 uvádí databázové soubory ve formátu UNIX, které jsou po instalaci protokolu Microsoft TCP/IP uloženy v adresáři *systemroot*\System32\Drivers\Etc.

**TABULKA 6.2:** Databázový soubor TCP/IP

| Název souboru | Funkce |
|---|---|
| Hosts | Poskytuje překlad názvů hostitele na adresy IP pro aplikace, které používají sokety systému Windows. |
| Lmhosts.sam | Ukázkový soubor souboru Lmhosts, který zajišťuje překlad názvů NetBIOS na vzdálené adresy IP pro aplikace protokolu NetBIOS. |
| Networks | Poskytuje překlad názvů sítí na ID sítí pro aplikace, které používají sokety systému Windows. |
| Protocols | Poskytuje překlad názvů protokolů na ID protokolů pro aplikace, které používají sokety systému Windows. |
| Services | Poskytuje překlad názvů služeb na ID portů pro aplikace, které používají sokety systému Windows. |

Chcete-li vyřešit potíže některého z těchto souborů v místním počítači, zkontrolujte, zda formát položek v každém souboru odpovídá formátu ukázkového souboru, který byl původně instalován s protokolem Microsoft TCP/IP. Ověřte, zda jsou údaje zapsány správně a nejsou uvedeny neplatné adresy IP a identifikátory.

# 6.6 Další zdroje

- Další informace o protokolech a procesech TCP/IP a detailech implementace v systému Windows naleznete v knize *Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference* (Technická referenční příručka protokolů a služeb TCP/IP v systému Microsoft Windows Server 2003) autorů Joseph Davies a Thomas Lee, 2003, Redmond, Washington: Microsoft Press.
- Další informace o protokolech TCP/IP naleznete v příručce *Microsoft Windows 2000 Server TCP/IP Core Networking Guide* (Průvodce základy sítí TCP/IP systému Microsoft Windows 2000 Server) společnosti Microsoft Corporation, 2002, Redmond, Washington: Microsoft Press.
- Další informace o řešení potíží protokolů TCP/IP naleznete v knize *Windows NT TCP/IP Network Administration* (Správa sítě TCP/IP systému Windows NT) autorů Craig Hunt a Robert Bruce Thompson, 1998, Sebastopol, California: O'Reilly.
- Další informace o nástroji Network Monitor naleznete v publikaci *Microsoft Windows Server 2003 Administrator's Companion* (Příručka správce systému Microsoft Windows Server 2003) autorů Charlie Russel, Sharon Crawford a Jason Gerend, 2003, Redmond, Washington: Microsoft Press.