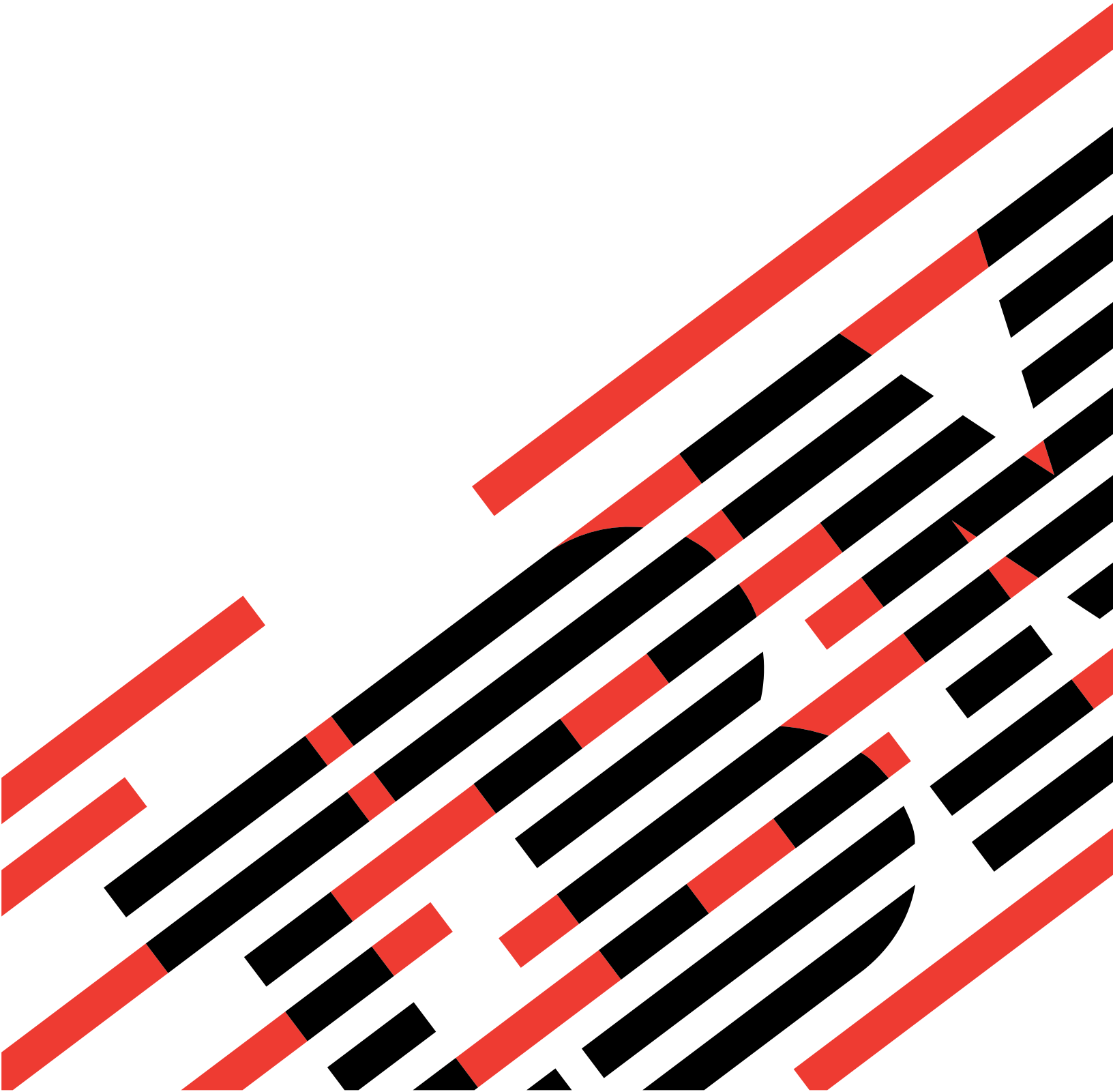
Systémy IBM - iSeries

# Síťové technologie - Nastavení TCP/IP

*Verze 5, vydání 4*



Systémy IBM - iSeries

# Síťové technologie - Nastavení TCP/IP

*Verze 5, vydání 4*

**Poznámka**

Před použitím těchto informací a odpovídajícího produktu si přečtěte informace v části “Poznámky”, na stránce 41.

**Osmé vydání (únor 2006)**

Toto vydání se vztahuje na verzi 5, vydání 4, modifikaci 9 operačního systému i5/OS (číslo produktu 5722–SS1) a na všechna následná vydání a modifikace, dokud nebude v nových vydáních uvedeno jinak. Tato verze nemůže být provozována na žádném počítači RISC (reduced instruction set computer) ani na modelech CISC.

# Obsah

# Nastavení TCP/IP

Právě jste obdrželi svůj server a jste připraveni začít jej používat. Toto téma popisuje nástroje a procedury konfigurace TCP/IP v operačním systému i5/OS.

Například můžete použít tyto informace k vytvoření popisu linky, rozhraní TCP/IP nebo přenosové cesty. Dozvíte se, jak lze přizpůsobit konfiguraci TCP/IP v prostředí produktu iSeries Navigator, a seznámíte se s různými technikami TCP/IP, které vám pomohou při směrování toků dat do sítě a ze sítě.

Dříve než použijete tyto informace při konfiguraci TCP/IP, prostudujte si téma Instalace a použití hardwaru a ujistěte se, že máte nainstalovány všechny nezbytné hardwarové komponenty. Poté, co dokončíte počáteční úkoly konfigurace TCP/IP, můžete rozšířit možnosti svého serveru pomocí aplikací, protokolů a služeb TCP/IP tak, aby vyhovovaly vašim jedinečným potřebám.

## Co je nového ve verzi V5R4

V tomto tématu jsou zdůrazněny změny provedené v této kolekci témat pro verzi V5R4.

### Vylepšení podpory IPv6

**Nové funkce protokolu IPv6 (Internet Protocol verze 6) jsou na úrovni produktů konzistentní se svými protějšky v protokolu IPv4.**

**IPv6 je nyní podporován pro tyto funkce:**

- Loopback
- Všechny adaptéry typu Ethernet (10/100 Mb/s, 1 Gb/s a 10 Gb/s)
- Virtuální síť typu Ethernet mezi logickými částmi

**S protokolem IPv6 lze používat současně několik adaptérů typu Ethernet.**

**IPv6 nyní podporuje tyto funkce:**

- Multicast
- Fragmentace a sestavení
- Základní rozšíření soketů (RFC 3494)

### Konfigurace IPv6

- Akce Spuštění a Zastavení TCP/IP ve složce **Konfigurace TCP/IP** byly odstraněny.
- IPv6 lze spustit a zastavit stejným způsobem jako IPv4, příkazy STRTCP (Spuštění TCP/IP) a ENDTCP (Ukončení TCP/IP). IPv6 nelze spustit ani zastavit nezávisle na IPv4.
- Podle předvoleného nastavení je rozhraní IPv6 typu loopback, ::1, automaticky vytvořeno při spuštění TCP/IP.
- Byl odstraněn průvodce konfigurací IPv6.
- Pomocí tohoto nového rozhraní můžete konfigurovat bezestavovou automatickou konfiguraci adres (Stateless Address Autoconfiguration).
- Pomocí nového průvodce můžete také vytvořit rozhraní IPv6.
- Do kontextové nabídky na obrazovce Protokol IPv6 Stateless Address Autoconfig byly pro linku přidány funkce Konfigurovat, Spustit, Zastavit a Odstranit.

## Aliasy jmen

V IPv4 a IPv6 můžete nyní používat aliasy jmen. Namísto zápisu pomocí tečkové konvence můžete zadat jméno, které určuje rozhraní buď v IPv4, nebo v IPv6. Jména aliasů rozhraní lze konfigurovat jak pomocí CL příkazů, tak v prostředí produktu iSeries Navigator.

## Seznam preferovaných rozhraní

Vytvoření seznamu preferovaných rozhraní vám umožní vybrat, které adaptéry a IP adresy budou preferovaným rozhraním pro výběr agenta ARP proxy virtuální IP adresy. Tento seznam je dostupný pro virtuální IP adresy i pro virtuální síť typu Ethernet.

## Změny ve verzi V5R4

**IPv6 již nepodporuje tunely:**

- Protokoly IPv6, IPv4 a PPPoE (Point-to-Point Protocol over Ethernet) mohou být použity na stejném adaptéru.
- Síťové směrovače mohou být použity při odesílání paketů IPv6 přes síť IPv4.

**Konfigurace IPv6 z předchozích vydání nebudou migrovány do verze V5R4.**

## Jak zjistit, co je nového a co je změněno

Místa, ve kterých byly provedeny technické změny, jsou označena níže uvedenými symboly, abyste je mohli snadno identifikovat.

- Symbol » označuje místo, kde začínají nové nebo změněné informace.
- Symbol « označuje místo, kde nové nebo změněné informace končí.

Další informace o novinkách a změnách v tomto vydání najdete v dokumentu Sdělení pro uživatele.

---

# Tisknutelný soubor PDF

Použijte toto téma, až budete chtít zobrazit nebo vytisknout soubor PDF s těmito informacemi.

Chcete-li zobrazit nebo stáhnout verzi PDF tohoto dokumentu, vyberte odkaz Nastavení TCP/IP (zhruba 667 kB).

Můžete zobrazit nebo stáhnout tato související témata:

- Plánování a nastavení zabezpečení serveru iSeries (2,8 MB)
  - Plánování základního zabezpečení systému a ochrana serveru iSeries a přidružených operací
  - Nastavení zabezpečení systému
- Odstraňování problémů s TCP/IP (920 kB)
  - Řešení problémů s připojením a provozem TCP/IP pro IPv4 i IPv6

## Další informace

Můžete také zobrazit nebo vytisknout libovolný z těchto souborů PDF:

- Červené knihy IBM:
  - **TCP/IP Tutorial and Technical Overview** (7 MB) Tato červená kniha IBM poskytuje základní informace o TCP/IP.
  - **TCP/IP for AS/400: More Cool Things Than Ever** (9 MB) Tato červená kniha IBM obsahuje rozsáhlý seznam běžných aplikací a služeb TCP/IP.

### Uložení souborů PDF

Chcete-li soubor PDF uložit na svou pracovní stanici, abyste ho později mohli prohlížet a vytisknout, postupujte takto:

1. Klepněte pravým tlačítkem myši v prohlížeči na odkaz na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na volbu, která ukládá soubor PDF lokálně.
3. Přejděte do adresáře, do kterého chcete soubor PDF uložit.
4. Klepněte na **Save** (Uložit).

### Stažení aplikace Adobe Reader

Zobrazení a tisk těchto souborů PDF vyžadují, aby byla v počítači nainstalována aplikace Adobe Reader. Kopii této aplikace můžete zdarma stáhnout z webové stránky společnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

---

## Protokol IP (Internet Protocol) verze 6

Protokol IP (Internet Protocol) verze 6 (IPv6) má klíčovou roli v budoucnosti Internetu. Protokol IPv6 můžete používat na serveru iSeries. Toto téma obsahuje obecné informace o protokolu IPv6 a o jeho implementaci na serveru iSeries.

Protokol IPv6 je aktualizovanou verzí protokolu IPv4 a postupně nahrazuje protokol IPv4 jako standard Internetu.

Následující témata poskytují základní informace o protokolu IPv6 a o tom, jak ho používat na serveru iSeries.

## Co je protokol IPv6?

Dozvíte se, proč protokol IPv6 nahrazuje protokol IPv4 jako standard Internetu a jak ho můžete využívat.

Protokol IPv6 je pokračováním vývoje protokolu IP (Internet Protocol). Ve větší části Internetu se používá protokol IPv4 a tento protokol byl spolehlivý a odolný po dobu 20 let. Protokol IPv4 však má omezení, která mohou s rozvojem Internetu vyvolávat další problémy.

Zejména se prohlubuje nedostatek adres IPv4 potřebných pro všechna nová zařízení připojovaná k Internetu. Podstatou zdokonalení protokolu IPv6 je rozšíření prostoru IP adres z 32 bitů na 128 bitů, které umožňuje fakticky neomezený počet jedinečných IP adres. Nový formát textu adres IPv6 je:

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
```

Každé x představuje hexadecimální číslici reprezentující 4 bity.

Rozšířená schopnost adresování IPv6 je řešením problému vyčerpání adres. Je to velmi důležité, protože stále více lidí používá přenosné počítače a mobilní telefony. Narůstající požadavky uživatelů s bezdrátovým připojením přispívají k vyčerpání adres IPv4. Rozšíření prostoru IP adres v IPv6 poskytuje dostatečný počet IP adres pro narůstající počet bezdrátových zařízení.

Kromě těchto možností adresování poskytuje protokolu IPv6 nové funkce, které zjednodušují konfigurování a správu adres v síti. Konfigurace a údržba sítí je náročná činnost. Protokol IPv6 snižuje pracovní zátěž automatizací některých úkolů správce sítě.

Používáte-li protokol IPv6, nemusíte provádět přečíslování adres zařízení při přechodu k jinému poskytovateli služeb sítě Internet (ISP). Přečíslování uzlů je důležitým prvkem architektury IPv6 a je z velké části automatické. Dolní polovina adresy IPv6 zůstane nezměněna, protože ji tradičně tvoří adresa MAC adaptéru typu Ethernet. Poskytovatel ISP vám přiřadí novou předponu IPv6 a tato nová předpona může být distribuována všem koncovým hostitelským systémům tím, že se provede aktualizace směrovačů IPv6 v síti a umožní se bezestavové automatické konfiguraci ″naučit se″ novou předponu.

Funkce automatické konfigurace protokolu IPv6 automaticky konfiguruje adresy rozhraní a předvolených cest. Při bezestavové automatické konfiguraci vytvoří protokol IPv6 novou jedinečnou adresu IPv6 z adresy MAC počítače a z předpony sítě poskytnutého lokálním směrovačem. Tato funkce eliminuje potřebu serveru DHCP.

**Související pojmy**

"Jaké funkce protokolu IPv6 jsou k dispozici?"
Dozvíte se, jak je protokol IPv6 na serveru iSeries implementován.

**Související odkazy**

"Související informace pro protokol IPv6" na stránce 17
Uvedené odkazy na zdroje informací vám pomohou porozumět protokolu IPv6.

## Jaké funkce protokolu IPv6 jsou k dispozici?

Dozvíte se, jak je protokol IPv6 na serveru iSeries implementován.

IBM implementuje protokol IPv6 pro server iSeries již v několika vydáních softwaru. Funkce protokolu IPv6 jsou pro stávající aplikace TCP/IP transparentní a existují společně s funkcemi IPv4.

Mezi základní funkce serveru iSeries, které jsou ovlivněny protokolem IPv6, patří:

- **Konfigurace**

  Zadáním parametru STRIP6 (Spuštění IPv6) v příkazu STRTCP (Spuštění TCP/IP) můžete volitelně spustit IPv6 při spuštění TCP/IP. Předvoleným nastavením parametru STRIP6 (Spuštění IPv6) příkazu STRTCP (Spuštění TCP/IP) je hodnota *YES.

  Při konfiguraci IPv6 odesíláte pakety IPv6 sítí IPv6. Scénář, který popisuje konfiguraci IPv6 v síti, najdete v části "Vytvoření lokální sítě IPv6" na stránce 5.

  Položky nabídky Spustit a Zastavit ve složce **Konfigurace TCP/IP** jsou odstraněny. IPv6 lze spustit i zastavit stejným způsobem jako IPv4, pomocí příkazů STRTCP a ENDTCP. IPv6 nelze spustit ani zastavit nezávisle na IPv4.

  Průvodce konfigurací IPv6 je z prostředí produktu iSeries Navigator odstraněn. Možnosti konfigurace jsou v průvodci nahrazeny akcemi na jednotlivých linkách ve složce **Linky**. Podobně můžete použít nového průvodce, chcete-li vytvořit rozhraní IPv6. Chcete-li konfigurovat síť pro IPv6, prostudujte další informace o nových funkcích v části "Konfigurace protokolu IPv6" na stránce 22.

- **Sokety**

  Při vývoji a testování aplikací, které pracují se sokety, používejte rozhraní API protokolu IPv6 a nástroje IPv6. IPv6 vylepšuje sokety tak, že aplikace mohou používat IPv6 s využitím nové skupiny adres AF_INET6. Tato vylepšení neovlivňují stávající aplikace IPv4. Můžete vytvářet aplikace, které podporují souběžný provoz protokolů IPv4 a IPv6 nebo pouze provoz protokolu IPv6.

- **DNS**

  Systém DNS (Systém pojmenování domén) podporuje adresy typu AAAA a novou doménu pro zpětná vyhledávání IP6.ARPA. Přestože DNS dokáže číst informace protokolu IPv6, server musí ke komunikaci s DNS používat protokol IPv4.

- **Odstraňování problémů s TCP/IP**

  V sítích IPv6 používejte standardní nástroje pro odstraňování problémů, například příkazy PING a netstat, trasování přenosové cesty a trasování komunikace. Tyto nástroje nyní podporují formát adres IPv6. Řešení problémů se sítěmi IPv4 a IPv6 najdete v části Odstraňování problémů s TCP/IP.

**Související pojmy**

"Co je protokol IPv6?" na stránce 3
Dozvíte se, proč protokol IPv6 nahrazuje protokol IPv4 jako standard Internetu a jak ho můžete využívat.

**Související odkazy**

"Související informace pro protokol IPv6" na stránce 17
Uvedené odkazy na zdroje informací vám pomohou porozumět protokolu IPv6.

# Scénář: Protokol IPv6

Uvedené příklady vám pomohou rozpoznat situace, ve kterých byste mohli ve svém podnikání využít protokol IPv6, a nastavit síť.

**Poznámka:** V tomto scénáři představuje IP adresa x:x:x:x:x:x:x:x IP adresy typu link-local. Všechny adresy použité v tomto scénáři jsou uvedeny jen jako příklad.

**Související pojmy**

"Konfigurace protokolu IPv6" na stránce 22
Proveďte konfiguraci serveru pro funkci protokolu IPv6 podle pokynů uvedených v tomto tématu. Oceníte rozšířené možnosti adresování a robustní vlastnosti tohoto protokolu Internetu.

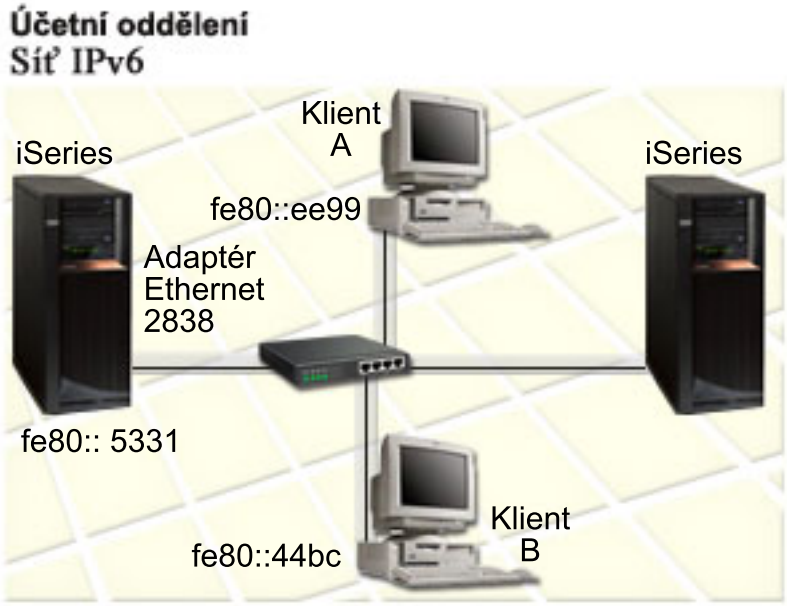
"Pojmy: IPv6" na stránce 6
V této části se seznámíte se základními pojmy protokolu IPv6. Pokud si nejste jisti, jaké jsou rozdíly mezi protokoly IPv4 a IPv6, prostudujte podrobné porovnání, například jak se adresy IPv4 a IPv6 navzájem porovnávají nebo jak se liší záhlaví paketů IPv4 od záhlaví paketů IPv6.

## Vytvoření lokální sítě IPv6

Tento scénář popisuje, jak lze vytvořit lokální síť IPv6.

## Situace

Protokol IPv6 nakonec nahradí protokol IPv4 jako standard sítě Internet. Vaše firma se proto rozhodne implementovat protokol IPv6 pro své finanční operace a zakoupí novou aplikaci pro účtování, která k připojování používá protokol IPv6. Tato aplikace se potřebuje připojovat k jiné instanci této aplikace, která je umístěna na jiném serveru připojeném do lokální sítě (LAN) typu Ethernet daného uzlu. Vaším úkolem je nakonfigurovat server pro protokol IPv6 tak, aby vaše firma mohla aplikaci pro účtování začítpoužívat. Uspořádání sítě pro tento scénář je znázorněno na následujícím obrázku.




## Řešení

Chcete-li vytvořit síť LAN IPv6, musíte pro IPv6 konfigurovat popis linky typu Ethernet. Pakety IPv6 jsou přenášeny mezi servery iSeries a klienty v síti, když zaměstnanci používají aplikaci pro účtování.

Požadavky na konfiguraci zahrnují:

- i5/OS verze 5, vydání 4

- iSeries Access for Windows a iSeries Navigator (síťová komponenta aplikace iSeries Navigator).
- Na serveru musí být nejprve konfigurován TCP/IP a server musí mít adresu IPv4, protože IPv6 musí být konfigurován v prostředí produktu iSeries Navigator. V současné době se produkt iSeries Navigator připojuje pouze pomocí IPv4. Pokud jste ještě neprovedli konfiguraci serveru pro IPv4, měli byste před konfigurací IPv6 na serveru prostudovat část První konfigurace TCP/IP .

### Konfigurace

Při konfiguraci IPv6 musíte použít produkt iSeries Navigator. IPv6 může být konfigurován pouze v prostředí iSeries Navigator a nelze ho konfigurovat ve znakově orientovaném rozhraní.

Spusťte IPv6 příkazem STRTCP s parametrem STRIP6 (*YES). Při zadávání možností konfigurace linek použijte akce na jednotlivých linkách ve složce **Linky**. Informace o automatické konfiguraci adres IPv6 v prostředí produktu iSeries Navigator najdete v kapitole“Bezestavová automatická konfigurace adres v protokolu IPv6” na stránce 22.

## Pojmy: IPv6

V této části se seznámíte se základními pojmy protokolu IPv6. Pokud si nejste jisti, jaké jsou rozdíly mezi protokoly IPv4 a IPv6, prostudujte podrobné porovnání, například jak se adresy IPv4 a IPv6 navzájem porovnávají nebo jak se liší záhlaví paketů IPv4 od záhlaví paketů IPv6.

**Související pojmy**

“Scénář: Protokol IPv6” na stránce 5
Uvedené příklady vám pomohou rozpoznat situace, ve kterých byste mohli ve svém podnikání využít protokol IPv6, a nastavit síť.

### Formáty adres IPv6

Velikost a formát adresy IPv6 přesahuje možnosti adresování.

Velikost adresy IPv6 je 128 bitů. Preferovaným znázorněním adresy IPv6 je formát: x:x:x:x:x:x:x:x, kde každé x je hexadecimální hodnota osmi 16bitových částí adresy. Rozsah adres IPv6 je od 0000:0000:0000:0000:0000:0000:0000:0000 do ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Kromě tohoto preferovaného formátu mohou být adresy IPv6 zadány ve dvou dalších zkrácených formátech:

**Vynechání vedoucích nul**

V adresách IPv6 lze vynechat úvodní nuly. Například adresu IPv6 1050:0000:0000:0000:0005:0600:300c:326b lze zapsat jako 1050:0:0:0:5:600:300c:326b.

**Dvě dvojtečky**

V adresách IPv6 lze místo série nul uvést dvě dvojtečky (::). Například adresu IPv6 ff06:0:0:0:0:0:0:c3 lze zapsat ve tvaru ff06::c3. Dvě dvojtečky lze v IP adrese použít jen jednou.

Alternativní formát adres IPv6 kombinuje zápisy s dvojtečkami a tečkami, takže lze adresu IPv4 vložit do adresy IPv6. Prvních 96 bitů ležících nejvíce vlevo se zapisuje hexadecimálně, zatímco 32 bitů ležících nejvíce vpravo se zapisuje dekadicky, což indikuje vloženou adresu IPv4. Tento formát zajišťuje kompatibilitu mezi uzly IPv6 a uzly IPv4 při práci ve smíšeném síťovém prostředí.

Adresa IPv6 namapovaná na adresu IPv4 používá tento alternativní formát. Tento typ adresy se používá k reprezentaci uzlů IPv4 jako adres IPv6. Umožňuje aplikacím založeným na protokolu IPv6 přímo komunikovat s aplikacemi používajícími IPv4. Například 0:0:0:0:0:ffff:192.1.56.10 a ::ffff:192.1.56.10/96 (zkrácený formát).

Všechny tyto formáty jsou platnými formáty adresy IPv6. Tyto formáty adres IPv6 můžete zadat prostředí produktu iSeries Navigator kromě adres IPv6 namapovaných na adresy IPv4.

## Typy adres IPv6

Používejte s protokolem IPv6 nové typy adres.

Adresy IPv6 se dělí do tří základních typů:

**Adresa unicast**

Adresa unicast označuje jediné rozhraní. Paket poslaný do cílového místa určeného adresou unicast putuje z jednoho hostitelského systému do cílového hostitelského systému.

Mezi tyto dva běžné typy adres patří:

**Adresa typu link-local**

Adresy typu link-local jsou určeny pro použití v jednom lokálním spoji (lokální síti). Adresy typu link-local jsou pro všechna rozhraní konfigurovány automaticky. U adresy typu link-local se používá předpona fe80::/10. Pakety s cílovou nebo zdrojovou adresou obsahující adresu typu link-local nepředávají směrovače dál.

**Globální adresa**

Globální adresy jsou určeny pro použití v libovolné síti. Předpona používaná v globální adrese začíná binární hodnotou 001.

Jsou definovány dvě speciální adresy unicast:

**Neuvedená adresa**

Neuvedenou adresou je adresa 0:0:0:0:0:0:0:0. Tuto adresu můžete zkrátit použitím dvou dvojteček (::). Neuvedená adresa indikuje, že adresa neexistuje a nelze ji přiřadit hostiteli. Může ji používat hostitel IPv6, kterému ještě adresa nebyla přiřazena. Odešle-li například hostitel paket, aby zjistil, zda nějakou adresu používá jiný uzel, použije hostitel neuvedenou adresu jako svoji zdrojovou adresu.

**Adresa typu loopback**

Adresou typu loopback je adresa 0:0:0:0:0:0:0:1. Tuto adresu lze zkrátit na ::1. Adresu typu loopback používá uzel k tomu, aby poslal paket sám sobě.

**Adresa anycast**

Adresa anycast určuje sadu rozhraní, případně v odlišných umístěních, které všechny sdílejí jednu adresu. Paket poslaný na adresu anycast dojde pouze nejbližšímu členovi skupiny. Server iSeries v současné době nepodporuje adresování anycast.

**Adresa multicast**

Adresa multicast určuje skupinu rozhraní, která mohou být v různých místech. U adresy multicast se používá předpona ff. Jestliže je na adresu multicast poslán paket, bude kopie paketu doručena každému členovi skupiny. Server iSeries poskytuje v současné době základní podporu pro adresy multicast.

## Zjišťování sousedních uzlů

Zjišťování sousedních uzlů umožňuje vzájemnou komunikaci hostitelů a směrovačů.

Funkce zjišťování sousedních uzlů jsou používány uzly IPv6 (hostitelskými systémy a směrovači) ke zjištění výskytu jiných uzlů IPv6, k určení adres (spojové vrstvy) uzlů, k vyhledání směrovačů schopných předávat pakety IPv6 a k udržování rychlé vyrovnávací paměti aktivních sousedních uzlů IPv6. Uzly IPv6 používají ke komunikaci s jinými uzly těchto pět zpráv ICMPv6 (Internet Control Message Protocol verze 6):

**Vyžádání směrovačů**

Hostitelské systémy odesílají tyto zprávy, aby požádaly směrovače o vygenerování oznámení směrovačů. Hostitelský systém odešle počáteční vyžádání směrovačů, když začne být poprvé k dispozici v síti.

**Oznámení směrovačů**

Směrovače odesílají tyto zprávy pravidelně nebo jako reakci na vyžádání směrovačů. Informace poskytnuté v oznámeních směrovačů jsou hostitelskými systémy použity k automatickému vytvoření globálních rozhraní a přidružených přenosových cest. Oznámení směrovačů také obsahují další informace o konfiguraci používané hostitelským systémem, například maximální přenosovou jednotku a mezní hodnotu směrovacích uzlů.

**Vyžádání sousedních uzlů**
Uzly odesílají tyto zprávy, aby určily adresu (spojové vrstvy) uzlu nebo aby ověřily, zda je sousední uzel stále dostupný.

**Oznámení sousedních uzlů**
Uzly odesílají tyto zprávy jako reakci na vyžádání sousedních uzlů nebo jako nevyžádanou zprávu oznamující změnu adresy.

**Přesměrování**
Směrovače pomocí těchto zpráv informují hostitelské systémy o lepším směrovacím uzlu na přenosové cestě k místu určení.

Další informace o zjišťování sousedních uzlů a směrovačů najdete v dokumentu RFC 2461. Chcete-li dokument RFC 2461 zobrazit, přejděte na webovou stránku RFC Editor (www.rfc-editor.org/rfcsearch.html) .

## Bezestavová automatická konfigurace adres
Bezestavová automatická konfigurace adres automatizuje některé úkoly správce sítě.

Bezestavová automatická konfigurace adres je postup, který používají uzly IPv6 (hostitelské systémy nebo směrovače) k automatické konfiguraci adres IPv6 pro rozhraní. Uzel sestavuje různé adresy IPv6 spojováním předpony adresy buď s identifikátorem odvozeným z adresy MAC daného uzlu, nebo s identifikátorem rozhraní zadaným uživatelem. Předpony zahrnují předponu typu link-local (fe80::/10) a předpony v délce 64 oznámené lokálními směrovači IPv6 (pokud nějaké existují).

Dříve než uzel přiřadí adresu k rozhraní, zjišťuje, zda neexistují duplicitní adresy - ověřuje tedy, zda je adresa jedinečná. Uzel odešle dotaz vyžadující reakci sousedních uzlů na novou adresu a čeká na odpověď. Nedostane-li uzel odpověď, předpokládá, že je adresa jedinečná. Pokud uzel obdrží odpověď ve formě oznámení sousedního uzlu, je adresa již používána. Jestliže uzel zjistí, že jeho pokusná adresa IPv6 není jedinečná, je automatická konfigurace ukončena a rozhraní je nutné nakonfigurovat ručně.

## Porovnání protokolu IPv4 s protokolem IPv6
Můžete porovnat atributy protokolu IPv4 s atributy protokolu IPv6.

IBM implementuje protokol IPv6 pro server iSeries již v několika vydáních softwaru. Protokol IPv6 je připraven k použití s produkty.

Možná by vás zajímalo, jak se protokoly IPv6 a IPv4 liší. Následující tabulka vám umožňuje rychle vyhledávat určité funkce a porovnávat jejich užívání v obou protokolech Internetu. Výběrem atributu v následujícím seznamu se dostanete k porovnání odpovídajících atributů v tabulce.
- Adresa
- Alokace adresy
- Doba trvání adresy
- Maska adresy
- Předpona adresy
- Protokol ARP
- Rozsah adres
- Typy adres
- Komunikační trasa
- Konfigurace
- DNS (Systém pojmenování domén)
- Protokol DHCP (Dynamic Host Configuration Protocol)
- Protokol FTP (File Transfer Protocol)
- Fragmenty
- Tabulka hostitelů
- Rozhraní
- Protokol ICMP (Internet Control Message Protocol)
- Protokol IGMP (Internet Group Management Protocol)

- Záhlaví IP
- Parametry záhlaví IP
- Bajt v protokolu záhlaví IP
- Bajt TOS (Type of Service) záhlaví IP
- Podpora produktu iSeries Navigator
- Připojení k síti LAN
- Protokol L2TP (Layer 2 Tunnel Protocol)
- Adresa typu loopback
- Maximální přenosová jednotka (MTU)
- Netstat
- Převod síťové adresy (NAT)
- Tabulka sítí
- Dotaz na informace o uzlu
- Filtrování paketů
- Přesměrování paketů
- Testování spojení
- Protokol PPP (Point-to-Point Protocol)
- Omezení portu
- Porty
- Soukromé a veřejné adresy
- Tabulka protokolů
- QoS (Quality of Service)
- Přečíslování
- Předepsaná cesta
- Protokol RIP (Routing Information Protocol)
- Tabulka služeb
- Protokol SNMP (Simple Network Management Protocol)
- Rozhraní API pro sokety
- Výběr zdrojové adresy
- Spuštění a zastavení
- Telnet
- Cesta trasování
- Přenosové vrstvy
- Nezadaná adresa
- Vytváření sítě VPN (Virtual Private Networking)

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Adresa** | Adresa je dlouhá 32 bitů (4 bajty). Adresa je tvořena síťovou a hostitelskou částí. Tyto části závisejí na třídě adresy. Podle několika počátečních bitů jsou definovány různé třídy adres: A, B, C, D nebo E. Celkový počet adres IPv4 je 4 294 967 296.<br><br>Textový tvar adresy IPv4 je nnn.nnn.nnn.nnn, kde 0<=*nnn*<=255, a *n* je dekadická číslice. Vedoucí nuly lze vynechat. Maximální počet tiskových znaků je 15, nepočítaje masku. | Adresa je dlouhá 128 bitů (16 bajtů). Základní architektura je 64 bitů pro síťové číslo a 64 bitů pro hostitelské číslo. Hostitelská část adresy IPv6 (nebo její část) bývá často odvozena z adresy MAC nebo jiného identifikátoru rozhraní.<br><br>Adresa IPv6 má v závislosti na předponě podsítě složitější architekturu než adresa IPv4.<br><br>Počet adres IPv6 je $10^{28}$ (79 228 162 514 264 337 593 543 950 336)krát větší než počet adres IPv4. Textový tvar adresy IPv6 je xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, kde x je hexadecimální číslice, která je znázorněna čtyřmi bity. Vedoucí nuly lze vynechat. V textovém tvaru adresy lze jednou označit libovolný počet bitů 0 pomocí dvou dvojteček (::). Například adresa ::ffff:10.120.78.40 je adresou IPv6 namapovanou na adresu IPv4. (Podrobnosti najdete v dokumentu RFC 3513.<br><br>Chcete-li tento dokument zobrazit, přejděte na webovou stránku RFC Editor (www.rfc-editor.org/rfcsearch.html). |
| **Alokace adresy** | Adresy byly původně přidělovány podle tříd sítí. S pokračujícím vyčerpáváním adresového prostoru jsou prováděna menší přidělení pomocí CIDR (Classless Inter-Domain Routing). Přidělování nebylo v rámci států a institucí vyvážené. | Přidělování je v nejranějších fázích. Společnosti IETF (Internet Engineering Task Force) a IAB (Internet Architecture Board) doporučily, aby v podstatě každé organizaci, domácnosti nebo entitě byla přidělena délka předpony podsítě /48 bitů. Tak by 16 bitů zůstalo pro práci organizace s podsítěmi. Adresový prostor je dost velký, aby každá osoba mohla pro sebe mít délku předpony podsítě /48. |
| **Doba trvání adresy** | Toto není obecně použitelný pojem, platí pouze u adres přidělených pomocí protokolu DHCP. | Adresy IPv6 mají dvě doby trvání: preferovanou a platnou, přičemž vždy preferovaná doba trvání <= platná doba trvání.<br><br>Až preferovaná doba trvání adresy vyprší, nebude již možné tuto adresu použít jako zdrojovou IP adresu pro nová připojení, pokud bude k dispozici stejně dobrá preferovaná adresa. Až preferovaná doba trvání adresy vyprší, nebude již tato adresa používána (rozpoznávána) jako platná IP adresa pro příchozí pakety ani jako zdrojová IP adresa.<br><br>Podle definice mají některé adresy IPv6 neomezenou preferovanou i platnou dobu trvání, například adresy typu link-local (viz Rozsah adres). |
| **Maska adresy** | Používá se k určení sítě z hostitelské části. | Nepoužívá se (viz Předpona adresy). |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Předpona adresy** | Někdy se používá k určení sítě z hostitelské části. V prezentačním tvaru adresy se někdy zapisuje jako přípona /nn. | Používá se v adrese k určení předpony podsítě. Zapisuje se jako přípona /nnn (až 3 dekadické číslice, 0 <= nnn <= 128) za tiskovým tvarem. Příkladem může být adresa fe80::982:2a5c/10, kde prvních 10 bitů tvoří předpona podsítě. |
| **Protokol ARP (Address Resolution Protocol)** | Protokol ARP je používán protokolem IPv4 k vyhledání fyzické adresy (například adresy MAC nebo adresy linky) přidružené k adrese IPv4. | IPv6 vkládá tyto funkce do samotného protokolu IP jako součást algoritmu automatické bezestavové konfigurace a zjišťování sousedních uzlů pomocí protokolu ICMPv6 (Internet Control Message Protocol, verze 6). Něco jako ARP6 proto neexistuje. |
| **Rozsah adres** | Tento pojem se netýká adres unicast. Existují určené rozsahy soukromých adres a adres typu loopback. Adresy mimo tento rozsah jsou považovány za globální. | U IPv6 je rozsah adresy součástí architektury. Adresy unicast mají dva definované rozsahy včetně adres typu link-local a globálních adres; adresy multicast mají 14 rozsahů. Rozsah je brán v úvahu při výběru předvolených zdrojových i cílových adres.<br><br>Zóna rozsahu je instancí rozsahu v konkrétní síti. V důsledku toho musejí být adresy IPv6 někdy zadávány s ID zóny nebo k němu přidruženy. Syntaxe je %zid, kde zid je číslo (obvykle malé) nebo jméno. ID zóny se píše za adresou a před předponou. Například 2ba::1:2:14e:9a9b:c%3/48. |
| **Typy adres** | Unicast, multicast nebo broadcast. | Unicast, multicast nebo anycast. Popis najdete v části Typy adres IPv6. |
| **Komunikační trasa** | Nástroj určený ke shromažďování podrobných informací o trasování paketů TCP/IP (i jiných), které na server iSeries přicházejí a odcházejí z něj. | Totéž platí pro protokol IPv6, protokol IPv6 je podporován. |
| **Konfigurace** | Než bude moci nově instalovaný systém komunikovat, musí být provedena konfigurace, tj. musejí být přiřazeny IP adresy a přenosové cesty. | Konfigurace je volitelná v závislosti na požadovaných funkcích. Protokol IPv6 může být používán s libovolným adaptérem typu Ethernet a spouštěn přes rozhraní typu loopback. Rozhraní IPv6 se konfigurují sama pomocí bezestavové automatické konfigurace IPv6. Lze je také konfigurovat ručně. Systém tedy dokáže komunikovat s jinými lokálními a vzdálenými systémy; v závislosti na typu sítě a na tom, zda existuje směrovač IPv6. |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **DNS (Systém pojmenování domén)** | Aplikace přijímají hostitelská jména a potom pomocí DNS získávají IP adresy - pomocí funkce rozhraní API soketů gethostbyname().<br><br>Aplikace také přijímají IP adresy a potom používají DNS k získání hostitelských jmen pomocí funkce gethostbyaddr() .<br><br>Doménou pro zpětná vyhledávání pro IPv4 je in-addr.arpa. | Totéž platí i pro IPv6. Protokol IPv6 je podporován pomocí typu záznamu AAAA (čtveřice A) a zpětného vyhledávání (převod IP na jméno). Aplikace si může vybrat, zda přijímat adresy IPv6 od DNS nebo ne a zda potom používat IPv6 ke komunikaci nebo ne.<br><br>Protokol IPv4 je podporován pouze funkcí rozhraní API soketů gethostbyname(). Pomocí nové funkce getaddrinfo() rozhraní API lze v protokolu IPv6 získat buď pouze adresy IPv6, nebo adresy IPv4 i IPv6 (podle výběru v aplikaci).<br><br>Doménou používanou u protokolu IPv6 pro zpětné vyhledávání je ip6.arpa. Nelze-li tuto doménu nalézt, používá se doména ip6.int (viz funkce rozhraní API getnameinfo()). |
| **Protokol DHCP (Dynamic Host Configuration Protocol)** | Tento protokol se používá k dynamickému získávání IP adres a jiných informací o konfiguraci. Server iSeries podporuje server DHCP pro IPv4. | V současné době není protokol IPv6 implementací protokolu DHCP v operačním systému i5/OS podporován. |
| **Protokol FTP (File Transfer Protocol)** | Tento protokol umožňuje přenášet (odesílat a přijímat) soubory v sítích. | V současné době není protokol IPv6 implementací protokolu FTP v operačním systému i5/OS podporován. |
| **Fragmenty** | Pokud je paket pro následující spoj, kterým má být přenesen, příliš velký, může být odesílatelem (hostitelským systémem nebo směrovačem) rozdělen na fragmenty. | U IPv6 může k fragmentaci docházet pouze ve zdrojovém uzlu a k opětovnému sestavení v cílovém uzlu. Je použito rozšířené záhlaví fragmentace. |
| **Tabulka hostitelů** | Tabulka konfigurovatelná pomocí produktu iSeries Navigator, která přiřazuje internetové adrese jméno hostitele; například 127.0.0.1, loopback. Tuto tabulku používá rozlišovač jmen u soketů, a to buď před vyhledáváním DNS, nebo po selhání vyhledávání DNS (je to určeno prioritou vyhledávání jmen hostitelů). | Tato tabulka v současné době nepodporuje IPv6. Zákazníci musejí kvůli rozlišování domén IPv6 nakonfigurovat záznam AAAA v DNS. DNS můžete spustit lokálně ve stejném systému jako rozlišovač, nebo v jiném systému. |
| **Rozhraní** | Koncepční nebo logická entita používaná TCP/IP k odesílání a přijímání paketů. Je vždy pojmenována adresou IPv4 nebo je s ní alespoň těsně asociována. Někdy se nazývá logické rozhraní.<br><br>Rozhraní mohou být spouštěna a ukončována nezávisle na sobě a nezávisle na TCP/IP pomocí příkazů STRTCPIFC a ENDTCPIFC nebo v prostředí produktu iSeries Navigator. | Stejný princip jako u IPv4.<br><br>Rozhraní mohou být spouštěna a ukončována nezávisle na sobě a nezávisle na TCP/IP pouze v prostředí produktu iSeries Navigator. |
| **Protokol ICMP (Internet Control Message Protocol)** | Protokol ICMP je používán IPv4 k přenosům síťových informací. | U IPv6 se používá podobným způsobem, protokol IMMPv6 (Internet Control Message Protocol verze 6) však nabízí některé nové vlastnosti.<br><br>Základní typy chyb zůstávají, například cíl nedostupný, žádost o odezvu (echo) a odpověď. Jsou přidány nové typy a kódy pro podporu zjišťování sousedních uzlů a souvisejících funkcí. |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Protokol IGMP (Internet Group Management Protocol)** | Protokol IGMP je používán směrovači IPv4 k vyhledání hostitelských systémů, které požadují provoz pro určitou skupinu multicast. Také ho používají hostitelské systémy IPv4 k informování směrovačů IPv4 o existujících posluchačích skupin multicast (v hostitelském systému). | U IPv6 byl nahrazen protokolem MLD (Multicast Listener Discovery). Provádí v podstatě totéž jako IGMP u IPv4, používá však ICMPv6 tak, že přidává několik hodnot typů ICMPv6 specifických pro MLD. |
| **Záhlaví IP** | 20 až 60 bajtů; délka záhlaví závisí na přítomných parametrech IP. | 40 bajtů; délka záhlaví je pevná. Žádné parametry záhlaví IP neexistují. Záhlaví IPv6 je obecně jednodušší než záhlaví IPv4. |
| **Parametry záhlaví IP** | Záhlaví IP mohou být doprovázena různými parametry (před jakýmkoliv transportním záhlavím). | Záhlaví IPv6 nemá žádné parametry. IPv6 místo toho používá dodatečná (volitelná) rozšířená záhlaví. K rozšířeným záhlavím patří AH a ESP (stejná jako u IPv4), hop-by-hop, směrovací záhlaví, záhlaví fragmentu a cílové záhlaví. Protokol IPv6 podporuje v současné době některá rozšířená záhlaví. |
| **Bajt v protokolu záhlaví IP** | Kód protokolu přenosové vrstvy nebo payload paketů, například ICMP. | Typ záhlaví bezprostředně následující po záhlaví IPv6. Využívá stejné hodnoty jako pole protokolu IPv4. Cílem z hlediska architektury je umožnit momentálně definovaný rozsah dalších záhlaví, který lze snadno rozšiřovat. Následujícím záhlavím bude transportní záhlaví, rozšířené záhlaví nebo ICMPv6. |
| **Bajt TOS (Type of Service) záhlaví IP** | QoS a specializované služby ho používají k určení třídy provozu. | Určuje třídu provozu IPv6; podobně jako u IPv4. Používá jiné kódy. IPv6 v současné době nepodporuje TOS. |
| **Podpora produktu iSeries Navigator** | Produkt iSeries Navigator poskytuje kompletní řešení pro konfiguraci TCP/IP. | Totéž platí i pro IPv6. Pro konfiguraci IPv6 nejsou k dispozici žádné CL příkazy. |
| **Připojení k síti LAN** | Je používáno rozhraním IP k přístupu do fyzické sítě. Existuje mnoho typů, například Token ring a Ethernet. Někdy se používají označení jako: fyzické rozhraní, propojení, spoj, spojení nebo linka. | Protokol IPv6 může být používán s libovolným adaptérem typu Ethernet a spouštěn přes rozhraní typu loopback. |
| **Protokol L2TP (Layer 2 Tunnel Protocol)** | L2TP můžeme považovat za virtuální PPP (dvoubodový spoj), který funguje u všech podporovaných typů linek. | V současné době není protokol IPv6 implementací protokolu L2TP v operačním systému i5/OS podporován. |
| **Adresa typu loopback** | Rozhraní s adresou 127.*.*.* (obvykle 127.0.0.1), které může uzel použít pouze tehdy, odesílá-li pakety sám sobě. Fyzické rozhraní (popis linky) má jméno *LOOPBACK. | Stejný princip jako u IPv4. Jedinou adresou typu loopback je 0000:0000:0000:0000:0000:0000:0000:0001 nebo její zkrácená verze ::1. Jméno virtuálního fyzického rozhraní je *LOOPBACK. |
| **Maximální přenosová jednotka (MTU)** | Maximální přenosová jednotka spoje (linky) je maximální počet bajtů, který konkrétní typ spoje (například Ethernet nebo modem) podporuje. U IPv4 je 576 typická minimální hodnota MTU. | U IPv6 je dolní hodnota MTU 1280 bajtů dána architekturou. Znamená to, že IPv6 nebude fragmentovat pakety pod tuto mezní hodnotu. Pokud mají spojem procházet fragmenty IPv6 s hodnotou MTU menší než 1280, musejí být pakety IPv6 transparentně fragmentovány a defragmentovány ve spojové vrstvě. |
| **Netstat** | Nástroj k zjišťování stavu spojení, rozhraní a přenosových cest TCP/IP. Je dostupný v produktech iSeries Navigator a 5250. | Totéž platí pro IPv6. IPv6 je podporován produkty 5250 i iSeries Navigator. |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Převod síťové adresy (NAT)** | Základní funkce ochranné bariéry (firewall) integrované v TCP/IP; ke konfiguraci slouží produkt iSeries Navigator. | NAT v současné době nepodporuje IPv6. Obecněji řečeno, IPv6 nevyžaduje NAT. Rozšířený adresový prostor IPv6 odstraňuje problém nedostatku adres a usnadňuje přečíslování. |
| **Tabulka sítí** | Tabulka, kterou lze v produktu iSeries Navigator konfigurovat a která přidruží jméno sítě k IP adrese bez masky. Přidruží například hostitelský systém Network14 k IP adrese 1.2.3.4. | V protokolu IPv6 se tato tabulka v současné době nemění. |
| **Dotaz na informace o uzlu** | Neexistuje. | Jednoduchý a praktický síťový nástroj, který by měl fungovat podobně jako příkaz pro testování spojení (PING), až na obsah: Uzel IPv6 by mohl položit jinému uzlu IPv6 dotaz požadující informace o cílovém uzlu - jméno DNS, adresu unicast IPv6 nebo adresu IPv4. V současné době není podporován. |
| **Filtrování paketů** | Základní funkce ochranné bariéry (firewall) integrované v TCP/IP; ke konfiguraci slouží produkt iSeries Navigator. | S protokolem IPv6 nelze filtrování paketů použít. |
| **Přesměrování paketů** | Server iSeries lze konfigurovat tak, aby směroval přijaté IP pakety na jiné IP adresy než lokální. Příchozí a odchozí rozhraní jsou obvykle připojena k různým lokálním sítím (LAN). | Pakety IPv6 nejsou přesměrovány. |
| **Testování spojení** | Základní nástroj TCP/IP k testování dosažitelnosti. Je dostupný v produktech iSeries Navigator a 5250. | Totéž platí pro IPv6. IPv6 je podporován jak 5250, tak produktem iSeries Navigator. |
| **Protokol PPP (Point-to-Point Protocol)** | Protokol PPP podporuje komutovaná rozhraní přes různé typy modemů a linek. | V současné době není protokol IPv6 implementací protokolu PPP v operačním systému i5/OS podporován. |
| **Omezení portu** | Tyto panely iSeries umožňují zákazníkům konfigurovat vybrané číslo portu nebo rozsahy čísel portů pro protokoly TCP a UDP tak, aby byly dostupné pouze pro určitý profil. | Totéž platí i pro IPv6. Omezení portů pro protokol IPv6 jsou stejná jako omezení, která jsou k dispozici v protokolu IPv4. |
| **Porty** | TCP a UDP mají samostatné prostory portů, každý je identifikován čísly portů v rozsahu 1 - 65 535. | U IPv6 je funkce portů stejná jako u IPv4. Protože tyto porty jsou umístěny v nové skupině adres, existují nyní čtyři samostatné prostory portů. Například existují dva prostory TCP portů 80, ke kterým může aplikace vytvořit vazbu - jeden v AF_INET a druhý v AF_INET6. |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Soukromé a veřejné adresy** | Všechny adresy IPv4 jsou veřejné, kromě tří rozsahů adres, které byly v dokumentu RFC 1918 společnosti IETF určeny jako soukromé: 10.*.*.* (10/8), 172.16.0.0 až 172.31.255.255 (172.16/12) a 192.168.*.* (192.168/16). Soukromé adresové domény jsou často používány uvnitř organizací. Soukromé adresy nelze směrovat přes Internet. | U IPv6 je použit podobný princip, avšak s důležitými rozdíly.<br><br>Adresy jsou veřejné nebo dočasné (dříve nazývané anonymní). Informace najdete v dokumentu RFC 3041. Na rozdíl od soukromých adres IPv4 mohou být dočasné adresy globálně směrovány. Účel je také jiný: Dočasné adresy IPv6 mají skrýt identitu klienta, když iniciuje komunikaci (kvůli utajení). Dočasné adresy mají omezenou dobu trvání a neobsahují identifikátor rozhraní, který je adresou spoje (MAC). Obecně je nelze odlišit od veřejných adres.<br><br>Protokol IPv6 obsahuje pojem omezeného rozsahu adres, který je součástí definice označování rozsahu (viz Rozsah adres). |
| **Tabulka protokolů** | Tabulka, kterou lze v produktu iSeries Navigator konfigurovat a která jméno protokolu přidružuje k přiřazenému číslu protokolu, například UDP, 17. Systém je dodáván s malým počtem položek v této tabulce: IP, TCP, UDP, ICMP. | Tuto tabulku můžete beze změny použít pro protokol IPv6. |
| **QoS (Quality of Service)** | QoS umožňuje u aplikací TCP/IP požadovat prioritu paketů a šířku pásma. | V současné době není protokol IPv6 implementací QoS v operačním systému i5/OS podporován. |
| **Přečíslování** | Provádí se ruční rekonfigurací, s možnou výjimkou u DHCP. Je to obtížný a komplikovaný proces, kterému by se měly síťové uzly nebo organizace vyhnout, je-li to možné. | Jedná se o důležitý prvek architektury protokolu IPv6, který je z velké části automatický, zejména v rámci předpony /48. |
| **Předepsaná cesta** | Tento logický pojem představuje mapování skupiny IP adres (může obsahovat pouze jednu IP adresu) na fyzické rozhraní a na jedinou IP adresu následujícího směrovacího uzlu. IP pakety, jejichž cílová adresa je definována jako součást uvedené skupiny adres, jsou pomocí linky směrovány do dalšího směrovacího uzlu. Přenosové cesty IPv4 jsou asociovány s rozhraním IPv4, a tedy s adresou IPv4.<br><br>Předvolená přenosová cesta je *DFTROUTE. | Princip je stejný jako u IPv4, s jednou důležitou výjimkou: Přenosové cesty jsou v protokolu IPv6 přidruženy k fyzickému rozhraní (propojení, jako je například ETH03), ne k rozhraní obecně. Jedním z důvodů, proč je přenosová cesta přidružena k fyzickému rozhraní, je to, že výběr zdrojové adresy funguje v protokolu IPv6 jinak než v protokolu IPv4. Viz Výběr zdrojové adresy. |
| **Protokol RIP (Routing Information Protocol)** | RIP je směrovací protokol podporovaný směrovacím démonem. | RIP v současné době nepodporuje IPv6. Při směrování IPv6 se používají statické přenosové cesty. |
| **Tabulka služeb** | Tabulka na serveru iSeries, kterou lze konfigurovat a která přidružuje jméno služby k portu a protokolu, například jméno služby FTP-control, port 21, protokoly TCP a UDP.<br><br>V tabulce služeb je uveden velký počet dobře známých služeb. Mnoho aplikací pomocí této tabulky určuje, který port použít. | U IPv6 se tato tabulka nemění. |

| Popis | IPv4 | IPv6 |
|---|---|---|
| **Protokol SNMP (Simple Network Management Protocol)** | SNMP je standardní protokol pro správu systémů. | V současné době není protokol IPv6 implementací protokolu SNMP v operačním systému i5/OS podporován. |
| **Rozhraní API pro sokety** | Tato rozhraní API poskytují aplikacím způsob, jak používat TCP/IP. Aplikace, které nepotřebují IPv6, nejsou ovlivněny změnami soketů týkajícími se podpory IPv6. | IPv6 vylepšuje sokety tak, že aplikace nyní mohou používat IPv6 s využitím nové skupiny adres: AF_INET6.<br><br>Vylepšení byla navržena tak, aby stávající aplikace IPv4 nebyly vůbec ovlivněny protokolem IPv6 a změnami rozhraní API. Aplikace, které mají podporovat souběžný provoz IPv4 a IPv6 nebo pouze provoz IPv6, lze snadno přizpůsobit pomocí adres IPv6 mapovaných na adresy IPv4 ve formě ::ffff:a.b.c.d, kde a.b.c.d je adresa IPv4 počítače typu klient.<br><br>Nová rozhraní API také podporují konverzi adres IPv6 z textové formy do binární a naopak.<br><br>Další informace o vylepšení soketů pro protokol IPv6 najdete v části Použití řady adres AF_INET6. |
| **Výběr zdrojové adresy** | Aplikace může určit zdrojovou IP adresu (obvykle pomocí funkce soketů bind()). Pokud vytvoří vazbu na INADDR_ANY, je zdrojová IP adresa zvolena na základě přenosové cesty. | Aplikace může určit zdrojovou adresu IPv6 pomocí funkce bind() stejně jako v protokolu IPv4. Podobně jako u IPv4 může použitím in6addr_any dosáhnout toho, aby zdrojovou adresu IPv6 zvolil systém. Protože však linky IPv6 mají mnoho adres IPv6, je interní metoda volby zdrojové IP adresy jiná. |
| **Spuštění a zastavení** | Ke spuštění nebo ukončení TCP/IP použijte příkazy STRTCP nebo ENDTCP. | Totéž jako u IPv4. IPv4 a IPv6 nejsou spouštěny a ukončovány nezávisle na sobě nebo nezávisle na TCP/IP. To znamená, že spustíte nebo ukončíte veškeré funkce TCP/IP, nejen pouze IPv4 nebo IPv6.<br><br>Všechna rozhraní IPv6 jsou spuštěna automaticky, pokud parametr AUTOSTART = *YES (předvolba). IPv6 nelze používat ani konfigurovat bez IPv4. Rozhraní ::1 typu loopback protokolu IPv6 bude definováno automaticky a aktivováno po spuštění IPv6. |
| **Telnet** | Telnet umožňuje přihlásit se k vzdálenému počítači a pracovat s ním, jako byste k němu byli připojeni přímo. | V současné době není protokol IPv6 implementací Telnet v operačním systému i5/OS podporován. |
| **Cesta trasování** | Základní nástroj TCP/IP k určení cesty. Je dostupný v produktech iSeries Navigator a 5250. | Totéž platí pro IPv6. IPv6 je podporován produkty 5250 i iSeries Navigator. |
| **Přenosové vrstvy** | TCP, UDP, RAW. | V protokolu IPv6 existují stejné přenosy. |
| **Nezadaná adresa** | Očividně adresa, která jako taková není definována. Při programování soketů se jako adresa 0.0.0.0 používá INADDR_ANY. | Adresa definovaná jako ::/128 (128 bitů 0). Používá se jako zdrojová IP adresa v některých paketech pro zjišťování sousedních uzlů a v různém jiném kontextu, například u soketů. Při programování soketů se jako adresa 0.0.0.0 používá in6addr_any. |
| **Vytváření sítě VPN (Virtual Private Networking)** | Technologie VPN (používající IPsec) umožňuje rozšířit zabezpečenou soukromou síť přes stávající veřejnou síť. | V současné době není protokol IPv6 implementací sítě VPN i5/OS podporován. |

## Odstraňování problémů s protokolem IPv6

Při řešení problémů s protokoly IPv4 a IPv6 můžete použít mnohé z nástrojů pro odstraňování problémů.

Máte-li na serveru konfigurován IPv6, můžete použít několik stejných nástrojů pro odstraňování problémů jako u IPv4. Například nástroje, jako jsou trasování přenosové cesty a testování spojení, akceptují jak formát adres IPv4, tak IPv6, můžete je tedy použít při testování připojení a přenosových cest pro oba typy sítí. Kromě toho můžete trasovat data na komunikačních linkách IPv4 i IPv6 pomocí funkce trasování komunikace.

Obecné pokyny k řešení problémů souvisejících s IPv4 a IPv6 najdete v tématu Odstraňování problémů s TCP/IP.

## Související informace pro protokol IPv6

Uvedené odkazy na zdroje informací vám pomohou porozumět protokolu IPv6.

- IETF (Internet Engineering Task Force) (www.ietf.cnri.reston.va.us/) Seznámí vás se skupinou osob, která pracuje na vývoji protokolu Internetu včetně protokolu IPv6.
- IPv6 (IP Version 6) (http://playground.sun.com/pub/ipng/html/ipng-main.html) Umožňuje vyhledat aktuální specifikace protokolu IPv6 a odkazy na několik zdrojů o protokolu IPv6.
- IPv6 Forum (www.ipv6forum.com/) Poskytuje články a události s novinkami o nejnovějším vývoji protokolu IPv6.

# Plánování nastavení TCP/IP

Toto téma vám pomůže při přípravě instalace a konfigurace TCP/IP na serveru iSeries. Obsahuje základní požadavky na instalaci a konfiguraci, takže až začnete s konfigurací TCP/IP, budete mít všechny nezbytné informace po ruce.

Dříve než začnete s instalací a konfigurací serveru iSeries, věnujte nějaký čas naplánování operací. Níže uvedená témata vám poslouží jako vodítko při plánování. Toto vodítko při plánování se týká základního nastavení TCP/IP při použití IPv4. Pokud máte v úmyslu konfigurovat IPv6, najdete požadavky a pokyny pro konfiguraci v části Konfigurace protokolu IPv6.

## Shromažďování informací o konfiguraci TCP/IP

Základní informace o konfiguraci, které budete potřebovat pro nastavení TCP/IP, byste měli shromáždit a zaznamenat.

Vytiskněte si tuto stránku a poznamenejte si údaje o konfiguraci serveru a síti TCP/IP, k níž se připojujete. Tyto informace budete potřebovat později, až budete konfigurovat TCP/IP. Pod tabulkou jsou uvedeny pokyny, pokyny, podle kterých můžete zjistit hodnoty pro první dva řádky. Pokud kterýkoliv z těchto termínů ještě neznáte, prostudujte informace o základních postupech při instalaci a konfiguraci v červené knize IBM TCP/IP for AS/400: More Cool Things Than Ever .

| Požadovaný údaj | Pro váš systém | Příklad |
|---|---|---|
| Typ komunikačního adaptéru ve vašem systému (viz pokyny pod tabulkou) | | Ethernet |
| Jméno prostředku | | CMN01 |
| IP adresa pro váš server iSeries | | 199.5.83.158 |
| Maska podsítě pro váš server iSeries | | 255.255.255.0 |
| Adresa síťové brány | | 199.5.83.129 |
| Jméno hostitele a jméno domény pro váš systém | | sys400.xyz.company.com |

| Požadovaný údaj | Pro váš systém | Příklad |
|---|---|---|
| IP adresa pro server jmen domény | | 199.4.191.76 |

Chcete-li zjistit údaje o svém komunikačním adaptéru, použijte tento postup:

1. Na příkazový řádek serveru zadejte go hardware a stiskněte klávesu Enter.
2. Chcete-li vybrat volbu Práce s komunikačními prostředky (volba 1), zadejte hodnotu 1 a stiskněte klávesu Enter.

   Zobrazí se vaše komunikační prostředky, seřazené podle jména prostředku. Budete-li chtít s těmito prostředky nějak pracovat nebo prohlížet podrobnější údaje, postupujte podle pokynů na obrazovce.

**Další krok**: Instalace TCP/IP

## Pokyny pro zabezpečení ochrany TCP/IP

Před instalací TCP/IP zvažte své požadavky na zabezpečení.

Při plánování konfigurace TCP/IP byste měli zvážit, jaké zabezpečení budete potřebovat. Níže uvedené strategické postupy mohou omezit riziko pro TCP/IP:

- **Spouštějte pouze ty aplikace TCP/IP, které potřebujete.** Každá aplikace TCP/IP má svoje vlastní bezpečnostní rizika. Nespoléhejte se na to, že směrovač bude odmítat Požadavky na konkrétní aplikaci. Jako sekundární ochranu nastavte pro aplikace, které nepožadujete, hodnoty automatického spouštění na NO.
- **Omezte dobu, po kterou jsou aplikace TCP/IP spuštěny.** Omezte riziko snížením počtu hodin, kdy jsou vaše servery spuštěny. Je-li to možné, ponechávejte servery TCP/IP, jako např. FTP a Telnet, v mimopracovní době zastaveny.
- **Kontrolujte, kdo může spouštět a měnit aplikace TCP/IP.** Standardně je ke změně nastavení konfigurace TCP/IP potřebné oprávnění *IOSYSCFG. Uživatel, který nemá oprávnění *IOSYSCFG, potřebuje oprávnění *ALLOBJ nebo explicitní oprávnění pro příkazy, které spouštějí TCP/IP. Udělování zvláštních oprávnění uživatelům představuje bezpečnostní riziko. U každého uživatele dobře zvažte nutnost zvláštních oprávnění a udržujte jejich počet na minimu. Sledujte, kteří uživatelé mají zvláštní oprávnění, a pravidelně prověřujte jejich požadavky na toto oprávnění. Tím také omezíte možnost přístupu na server mimo pracovní dobu.
- **Kontrolujte směrování TCP/IP:**
  - Nepovolujte postoupení pomocí IP, aby počítačoví piráti nemohli zneužít vašeho webového serveru k napadení dalších důvěryhodných systémů.
  - Definujte pouze jedinou předepsanou cestu ke svému veřejnému webovému serveru: předvolenou předepsanou cestu svého poskytovatele služeb sítě Internet.
  - Nekonfigurujte hostitelská jména a IP adresy svých vnitřních bezpečných systémů v hostitelské tabulce TCP/IP na svém webovém serveru. V této tabulce uvádějte pouze jména jiných veřejných serverů, na které chcete přistupovat.
- **Kontrolujte servery TCP/IP, které jsou určeny pro vzdálené interaktivní přihlašování.** Aplikace, jako například FTP a Telnet, jsou riziku vnějšího napadení mnohem více vystaveny. Podrobnější informace o tom, jak lze vystavení riziku kontrolovat, najdete v tématu o kontrole interaktivního přihlašování v kapitole Systémové hodnoty přihlášení.

Další informace o zabezpečení a dostupných možnostech najdete v tématu Zabezpečení serveru iSeries a Internetu.

## Instalace TCP/IP

Toto téma vás provede instalací produktů, která server iSeries připraví na provoz.

Základní podpora TCP/IP je dodávána spolu s operačním systémem i5/OS a umožňuje připojit server iSeries k síti. Budete-li však chtít použít libovolnou aplikaci TCP/IP, jako je např. Telnet, FTP nebo SMTP, budete muset nainstalovat i produkt TCP/IP Connectivity Utilities. Jedná se o licencovaný program, který je možné nainstalovat samostatně a který je součástí dodávaného operačního systému.

Chcete-li nainstalovat produkt TCP/IP Connectivity Utilities na server iSeries, postupujte takto:

1. Vložte instalační médium pro TCP/IP do serveru. Je-li tímto médiem CD-ROM, vložte jej do optického zařízení. Pokud je tímto médiem páska, vložte ji do páskové mechaniky.
2. Na příkazový řádek zadejte GO LICPGM a stiskněte klávesu Enter. Objeví se obrazovka Práce s licencovanými programy.
3. Na obrazovce Práce s licencovanými programy vyberte volbu 11 (Instalovat licencované programy). Zobrazí se seznam licencovaných programů a jejich volitelných součástí.
4. Vedle položky 57*xx*TC1 (TCP/IP Connectivity Utilities for iSeries) ve sloupci Option napište hodnotu 1 (Install). Stiskněte klávesu Enter. Objeví se obrazovka Confirm Licensed Programs to Install, která obsahuje licencované programy vybrané k instalaci. Potvrďte stisknutím klávesy Enter.
5. Na obrazovce Install Options vyplňte tyto volby:

| | |
|---|---|
| Installation device | Instalujete-li z CD-ROM, napište QOPT.<br><br>Instalujete-li z páskové mechaniky, napište TAP01. |
| Objects to install | Tato volba umožňuje vybrat pro instalaci programy i jazykové objekty, nebo pouze programy či pouze jazykové objekty. |
| Automatic restart | Tato volba určuje, zda se systém po úspěšném dokončení instalace automaticky znovu spustí. |

   Po úspěšné instalaci produktu TCP/IP Connectivity Utilities se zobrazí buď nabídka Práce s licencovanými programy, nebo obrazovka Sign On.
6. Vyberte volbu 50 (Zobrazit protokol pro zprávy) a ověřte, zda je licencovaný program úspěšně nainstalován.

   Pokud se vyskytnou nějaké chyby, uvidíte v dolní části obrazovky Práce s licencovanými programy zprávu Funkce Práce s licencovanými programy nebyla dokončena. Vyskytne-li se problém, pokuste se produkt TCP/IP Connectivity Utilities přeinstalovat. Pokud se tím problém nevyřeší, měli byste se obrátit na zákaznickou podporu.

**Poznámka:** Další licencované programy, které můžete chtít nainstalovat:

- IBM eServer iSeries Access for Windows (5722–XE1) poskytuje podporu produktu iSeries Navigator, který je používán při konfiguraci některých komponent TCP/IP.
- IBM HTTP Server for iSeries (57*xx*–DG1) poskytuje podporu webovému serveru.
- Některé aplikace TCP/IP vyžadují instalaci dalších licencovaných programů. Chcete-li zjistit, které další programy budete potřebovat, přečtěte si pokyny pro nastavení konkrétní aplikace, kterou si chcete pořídit.

## Konfigurace TCP/IP

Obsahem tohoto tématu je postup při uvádění serveru do provozu a při konfiguraci TCP/IP. Jsou zde také uvedeny pokyny pro konfiguraci protokolu IPv6.

| Možná provádíte konfiguraci TCP/IP poprvé nebo se snažíte změnit stávající konfiguraci kvůli použití funkcí protokolu
| IPv6. V následujících částech najdete pokyny ke konfiguraci TCP/IP na serveru.

## První konfigurace TCP/IP

Postupujte takto, jestliže chcete nakonfigurovat nový server. Poprvé vytvoříte připojení a nakonfigurujete TCP/IP.

Chcete-li na novém serveru nastavit TCP/IP, vyberte jednu z následujících metod.

### Konfigurace TCP/IP pomocí průvodce EZ-Setup

Použijte tuto preferovanou metodu, je-li váš počítač vybaven pro použití průvodce EZ-Setup. Průvodce EZ-Setup je dodáván spolu se serverem iSeries.

Produkt iSeries Navigator má grafické uživatelské rozhraní se stručnými dialogovými okny a průvodci ke konfiguraci TCP/IP. Provádíte-li počáteční nastavení poprvé, navažte spojení a nakonfigurujte TCP/IP pomocí průvodce EZ-Setup v prostředí produktu iSeries Navigator. Tuto metodu práce se serverem byste měli preferovat, protože používání tohoto rozhraní je snadné. Disk CD-ROM, který obsahuje průvodce EZ-Setup, je dodáván spolu se serverem iSeries.

Chcete-li konfigurovat server, postupujte takto:

1. Použijte průvodce EZ-Setup. Průvodce spustíte z disku CD-ROM dodaného spolu se serverem. Při konfiguraci TCP/IP postupujte podle pokynů průvodce.
2. Spusťte TCP/IP.
   a. V prostředí produktu iSeries Navigator rozbalte *svůj server* → **Síť**.
   b. Pravým tlačítkem myši klepněte na **Konfigurace TCP/IP** a vyberte **Spustit**. Současně se spuštěním TCP/IP se spustí všechna rozhraní a servery, které byly nastaveny na automatické spuštění při startu TCP/IP.

Postup konfigurace TCP/IP na serveru je ukončen. Bude-li třeba konfiguraci sítě změnit, použijte produkt iSeries Navigator.

Chcete-li přidat přenosové cesty a rozhraní nebo konfigurovat IPv6 tak, aby byl v síti používán protokol IP verze 6, přizpůsobte TCP/IP v prostředí produktu iSeries Navigator.

## Konfigurace TCP/IP pomocí průvodce znakově orientovaným rozhraním

Používejte tuto metodu, nemůžete-li použít průvodce EZ-Setup.

Nemůžete-li použít v prostředí produktu iSeries Navigator průvodce EZ-Setup, použijte místo něj průvodce znakově orientovaným rozhraním. Chcete-li například použít produkt iSeries Navigator v počítači, který před spuštěním produktu iSeries Navigator vyžaduje základní konfiguraci TCP/IP, měli byste při provádění základní konfigurace použít znakově orientované rozhraní.

Při provádění konfiguračních kroků popsaných v této části musí váš uživatelský profil obsahovat speciální oprávnění *IOSYSCFG. Další informace o tomto typu oprávnění najdete v kapitole o uživatelských profilech v publikaci iSeries Zabezpečení - Referenční informace .

Chcete-li konfigurovat TCP/IP pomocí znakově orientovaného rozhraní, proveďte následující kroky:

1. Na příkazový řádek napište GO TCPADM. Zobrazí se nabídka Administrace TCP/IP. Potom stiskněte klávesu Enter.
2. Vyberte volbu 1 (Konfigurovat TCP/IP). Zobrazí se nabídka CFGTCP (Konfigurace TCP/IP). Potom stiskněte klávesu Enter. Pomocí této nabídky vyberte úkoly konfigurace. Dříve než začnete server konfigurovat, věnujte určitý čas prohlídce nabídky.

Při konfigurování TCP/IP na serveru proveďte tyto kroky:

**Konfigurace popisu linky (Ethernet):**

Tyto pokyny se týkají konfigurace TCP/IP přes komunikační adaptér typu Ethernet.

Chcete-li konfigurovat popis linky, postupujte takto:

1. Na příkazový řádek napište CRTLINETH. Zobrazí se panel s náznakem CRTLINETH (Vytvoření popisu linky (Ethernet)). Potom stiskněte klávesu Enter.
2. Zadejte jméno linky. (Použijte libovolné jméno.)
3. Zadejte zdroj linky.
4. Spusťte příkaz několikerým stisknutím klávesy Enter.

**Zapnutí postoupení datagramu pomocí IP:**

Zapněte postoupení datagramu pomocí IP. Pakety pak budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, postupujte takto:
1. Na příkazový řádek napište CHGTCPA a potom stiskněte klávesu F4.
2. Na náznak *Postoupit datagram pomocí IP* zadejte *YES.

**Konfigurace rozhraní:**

Chcete-li konfigurovat rozhraní, postupujte takto:
1. Na příkazový řádek napište CFGTCP. Zobrazí se nabídka Konfigurovat TCP/IP. Potom stiskněte klávesu Enter.
2. V nabídce Konfigurovat TCP/IP vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
3. Vyberte volbu 1 (Přidat). Zobrazí se obrazovka Přidání rozhraní TCP/IP. Potom stiskněte klávesu Enter.
4. Zadejte adresu, která má reprezentovat váš server iSeries, adresu masky podsítě a jméno dříve definovaného popisu linky a potom stiskněte klávesu Enter.

Chcete-li nakonfigurované rozhraní spustit, zadejte pro toto rozhraní volbu 9 (Spustit) a potom stiskněte klávesu Enter.

**Konfigurace přenosové cesty:**

Mají-li být vzdálené sítě dosažitelné, je nutná alespoň jedna směrovací položka. Nejsou-li ručně přidány žádné směrovací položky, nejsou pro server dosažitelné systémy, které nejsou ve stejné síti, k níž je server připojen. Směrovací položky je nutné přidat také proto, aby správně fungovali klienti TCP/IP pokoušející se o přístup k vašemu serveru ze vzdálené sítě.

Měli byste naplánovat takovou definici směrovací tabulky, aby vždy obsahovala položku alespoň pro jednu předvolenou přenosovou cestu (*DFTROUTE). Nebude-li nalezena shoda s žádnou jinou položkou ve směrovací tabulce, budou data poslána směrovači IP uvedenému v první dostupné položce předvolené přenosové cesty.

Chcete-li konfigurovat předvolenou přenosovou cestu, proveďte následující kroky:
1. V nabídce Konfigurace TCP/IP vyberte volbu 2 (Pracovat s přenosovými cestami TCP/IP) a potom stiskněte klávesu Enter.
2. Vyberte volbu 1 (Přidat). Zobrazí se obrazovka ADDTCPRTE (Přidání přenosové cesty TCP/IP). Potom stiskněte klávesu Enter.
3. Jako cíl přenosové cesty zadejte *DFTROUTE, jako masku sítě zadejte *NONE, zadejte IP adresu dalšího směrovacího uzlu a potom stiskněte klávesu Enter.

**Definice jmen lokální domény a hostitelského systému:**

Chcete-li definovat jména lokální domény a hostitelského systému, postupujte takto:
1. V nabídce Konfigurovat TCP/IP vyberte volbu 12 (Změnit doménu TCP/IP) a potom stiskněte klávesu Enter.
2. Zadejte jména, která jste vybrali jako jméno lokálního hostitelského systému a jméno lokální domény. U ostatních parametrů ponechte předvolené hodnoty a stiskněte klávesu Enter.

**Definice tabulky hostitelů:**

Chcete-li definovat tabulku hostitelů, postupujte takto:
1. V nabídce Konfigurace TCP/IP vyberte volbu 10 (Pracovat se záznamy tabulky hostitelů TCP/IP) a potom stiskněte klávesu Enter.
2. Vyberte volbu 1 (Přidat). Objeví se obrazovka Přidání záznamu do tabulky hostitelů TCP/IP. Potom stiskněte klávesu Enter.
3. Zadejte IP adresu, přidružené jméno lokálního hostitelského systému a plně kvalifikované hostitelské jméno a potom stiskněte klávesu Enter.
4. V případě potřeby zpřístupněte prostor pro více než jedno jméno hostitele zadáním znaménka plus (+).

5. Opakujte kroky 1 až 4 pro každého z dalších hostitelů v síti, se kterým chcete komunikovat podle jména, a přidejte pro každého jednu položku.

**Spuštění TCP/IP:**

Služby TCP/IP nejsou dostupné, dokud TCP/IP nespustíte.

Chcete-li spustit TCP/IP, napište v příkazovém řádku příkaz STRTCP.

Příkaz STRTCP (Spustit TCP/IP) inicializuje a aktivuje zpracování TCP/IP, spustí rozhraní TCP/IP a úlohy na serveru. Příkazem STRTCP se spouštějí pouze rozhraní TCP/IP a servery, pro které je parametr AUTOSTART nastaven na hodnotu *YES. Všechna rozhraní TCP/IP a všechny servery, které mají parametr AUTOSTART nastaven na hodnotu *YES, profily PPP a IPv6 mohou být spouštěny volitelně.

Postup konfigurace TCP/IP na serveru je ukončen. Bude-li třeba konfiguraci sítě změnit, použijte produkt iSeries Navigator. Chcete-li přidat přenosové cesty a rozhraní nebo konfigurovat IPv6 tak, aby v síti používal protokol IP verze 6, přizpůsobte TCP/IP pomocí produktu iSeries Navigator.

# Konfigurace protokolu IPv6

Proveďte konfiguraci serveru pro funkci protokolu IPv6 podle pokynů uvedených v tomto tématu. Oceníte rozšířené možnosti adresování a robustní vlastnosti tohoto protokolu Internetu.

Pokud protokol IPv6 ještě neznáte, prostudujte přehled v části Protokol IPv6 (Internet Protocol version 6). Než začnete konfigurovat protokol IPv6, musíte mít na serveru nakonfigurovaný protokol TCP/IP.

Budete-li v síti používat protokol IPv6, budete připraveni na využívání Internetu nové generace. Chcete-li protokol IPv6 používat, můžete ho konfigurovat na stávající lince jednou nebo oběma z následujících metod: ruční konfigurací rozhraní a použitím funkce bezestavové automatické konfigurace adres v protokolu IPv6.

**Související pojmy**

"Scénář: Protokol IPv6" na stránce 5
Uvedené příklady vám pomohou rozpoznat situace, ve kterých byste mohli ve svém podnikání využít protokol IPv6, a nastavit síť.

## Požadavky na hardware a software

Toto téma uvádí přehled hardwarových a softwarových požadavků pro konfiguraci serveru pro IPv6.

## Konfigurace linky typu Ethernet pro IPv6

Konfigurace linky typu Ethernet, která umožní práci s protokolem IPv6, vyžaduje, aby systém splňoval tyto požadavky na server:

- Operační systém i5/OS verze 5, vydání 4.
- Produkty iSeries Access for Windows a iSeries Navigator:
  - Síťová komponenta produktu iSeries Navigator.
- Směrovač podporující IPv6, pokud chcete odesílat provoz IPv6 za hranice nejbližší sítě (LAN).
- TCP/IP (používající IPv4). Musí být nakonfigurován proto, že na serveru musí být spuštěn TCP/IP. Pokud jste konfiguraci serveru pro IPv4 ještě neprovedli, prostudujte před konfigurací linky pro IPv4 část První konfigurace TCP/IP.

## Bezestavová automatická konfigurace adres v protokolu IPv6

Chcete-li používat protokol IPv6, můžete použít funkci bezestavové automatické konfigurace adres v protokolu IPv6. Můžete to provést jedním ze dvou způsobů.

Při bezestavové automatické konfiguraci adres v protokolu IPv6 postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte **Síť → Konfigurace TCP/IP → Linky**.

2. Klepněte pravým tlačítkem myši na jednu z linek v pravém panelu a vyberte **Konfigurovat → IPv6 Stateless Address Autoconfig**.
3. Klepněte pravým tlačítkem myši na linku, kterou jste konfigurovali, vyberte **Spustit → IPv6 Stateless Address Autoconfig**.

Bezestavovou automatickou konfiguraci adres IPv6 můžete také provést takto:

1. V prostředí produktu iSeries Navigator rozbalte **Síť → Konfigurace TCP/IP → Linky**.
2. Klepněte pravým tlačítkem myši na **Linky** a potom vyberte volbu **Protokol IPv6 Stateless Address Autoconfig**.

**Poznámka:** Chcete-li zajistit, aby byla automaticky spuštěna při spuštění TCP/IP, vyberte na obrazovce **Konfigurovat linku pro IPv6** volbu **Spustit při spuštění TCP/IP**.

### Vytvoření nového rozhraní IPv6

Protokol IPv6 můžete také použít k ručnímu vytvoření nového rozhraní IPv6 pomocí nového průvodce.

Chcete-li vytvořit nové rozhraní IPv6, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte **Síť → Konfigurace TCP/IP → IPv6**.
2. Klepněte pravým tlačítkem myši na **Rozhraní** a potom vyberte volbu **Nové rozhraní**.
3. Vytvořte nové rozhraní IPv6 podle pokynů v průvodci novým rozhraním IPv6. Až konfiguraci dokončíte, objeví se nové rozhraní v pravém panelu.
4. Klepněte pravým tlačítkem myši na nové rozhraní IPv6 a potom vyberte **Spustit**.

   Můžete také zaškrtnout okénko **Spustit při spuštění TCP/IP** v průvodci novým rozhraním IPv6, chcete-li zajistit, aby bylo nové rozhraní automaticky spuštěno při příštím spuštění TCP/IP.
5. Vyzkoušejte nové rozhraní IPv6 v produktu iSeries Navigator pomocí příkazu **Síť → Konfigurace TCP/IP → Obslužné programy → Testování spojení** a ověřte, že je připojeno k síti.

   **Poznámka:** Položka nabídky Nové rozhraní je povolena pouze tehdy, máte-li oprávnění *IOSYSCFG.

## Konfigurace TCP/IP, když je operační systém ve stavu omezení

Metoda uvedená v tomto tématu je určena k použití v případě, že potřebujete spustit TCP/IP, když je operační systém ve stavu omezení.

### Situace

Jako síťový administrátor budete potřebovat obdržet zprávu o stavu zálohování na svém serveru. Když spouštíte procedury zálohování, musí být operační systém ve stavu omezení, aby uživatelé nemohli provádět změny v konfiguracích. Protože jste připojeni vzdáleně, přistupujete ke stavovým zprávám prostřednictvím zařízení PDA (nebo jakéhokoliv síťového zařízení TCP/IP). PDA využívá aplikaci podporující sokety, která ke komunikaci vyžaduje aktivní rozhraní TCP/IP. Tuto komunikaci umožníte tak, že spustíte TCP/IP se speciálními parametry. Po spuštění TCP/IP budete muset spustit specifické rozhraní TCP/IP, abyste povolili přístup k systému. Níže uvedené informace vám poskytnou podrobnější popis.

### Omezení

Pokud je systém provozován ve stavu omezení, platí následující omezení:

- Nelze spustit servery TCP/IP (CL příkaz STRTCPSRV), protože vyžadují aktivní podsystémy.
- Lze spustit pouze jedno rozhraní pro každý specifický typ linky (Ethernet, token-ring, nebo DDI), který není připojený k NWSD (popisu síťového serveru) nebo k NWID (popisu síťového rozhraní).

### Postup konfigurace

1. Spusťte TCP/IP se speciálními parametry.

Až bude systém serveru iSeries ve stavu omezení, zadejte na příkazový řádek následující příkaz: STRTCP STRSVR(*NO) STRIFC(*NO) STRPTPPRF(*NO) STRIP6(*NO). Když je operační systém ve stavu omezení, mohou být akceptovány pouze tyto parametry. Výše uvedený příkaz spustí TCP/IP; avšak nespustí a ani nemůže spustit aplikační servery nebo IP rozhraní.

2. Spusťte požadované rozhraní TCP/IP. Až spustíte TCP/IP ve stavu omezení, můžete spustit rozhraní, které potřebujete pro aplikaci pracující se sokety.
   a. Ověřte, zda rozhraní, které chcete spustit, používá popis linky typu *ELAN, *TRLAN nebo *DDI.

      Chcete-li zobrazit typ linky svého rozhraní, zadejte v příkazovém řádku CFGTCP a vyberte volbu 1 (Pracovat s rozhraními TCP/IP).
   b. Ověřte, zda rozhraní není připojeno k NWID ani k NWSD. Všechny ostatní pokusy vyvolají chybovou zprávu.

      Chcete-li ověřit, zda rozhraní není připojeno k NWID ani k NWSD, zadejte v příkazovém řádku DSPLIND *abc* (kde *abc* je jméno popisu linky). Ověřte, zda jméno prostředku není *NWID nebo *NWSD.

      **Poznámka:** Je-li rozhraní připojeno k NWID nebo k NWSD, doporučuje se vybrat jiné rozhraní.
   c. Spusťte rozhraní. Na příkazový řádek zadejte: STRTCPIFC INTNETADR('*a.b.c.d*'). Nahraďte řetězec *a.b.c.d* IP adresou rozhraní.

      **Poznámka:** Ověřte, zda není zadáno STRTCPIFC INTNETADR(*AUTOSTART).
3. Ověřte, že je rozhraní aktivní.

   Otestujte spojení specifického rozhraní aplikace. Existuje pouze velmi málo obslužných programů TCP/IP, které mohou být provozovány ve stavu omezení. Můžete použít příkazy ping a netstat. Další informace o použití příkazů ping a netstat najdete v části Nástroje k ověření síťové struktury v tématu Odstraňování problémů s TCP/IP.

---

## Přizpůsobení TCP/IP pomocí produktu iSeries Navigator

Toto téma obsahuje možnosti přizpůsobení pomocí produktu iSeries Navigator.

Po provedení konfigurace TCP/IP můžete konfiguraci přizpůsobovat. V důsledku neustálého rozšiřování sítě může být nezbytné měnit vlastnosti sítě, rozhraní nebo přidávat do serveru předepsané cesty. Budete-li chtít používat aplikace IPv6, budete muset server nakonfigurovat pro protokol IPv6. Mnohé z těchto úkolů můžete rychle provést pomocí průvodců v prostředí produktu iSeries Navigator.

Chcete-li konfiguraci přizpůsobit v prostředí produktu iSeries Navigator, vyberte libovolné z níže uvedených témat. Tato témata jsou výchozím bodem při správě konfigurace TCP/IP v prostředí produktu iSeries Navigator.

## Změna nastavení TCP/IP

Pokyny v tomto tématu vám pomohou při konfiguraci odpovídajících nastavení TCP/IP.

Nastavení TCP/IP můžete zobrazit a měnit v prostředí produktu iSeries Navigator. Můžete například měnit vlastnosti pro jména hostitelů a domén, server jmen, záznamy v tabulce hostitelů, atributy systému, omezení portů, servery a připojení klientů. Můžete měnit obecné vlastnosti i vlastnosti, které jsou specifické buď pro IPv4, nebo pro IPv6, například přenosy.

Chcete-li získat přístup ke stránkám s obecnými vlastnostmi TCP/IP, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**. Otevře se dialogové okno **Vlastnosti TCP/IP**.
3. Na jednotlivých kartách tohoto dialogového okna můžete zobrazovat a upravovat údaje o TCP/IP.

Chcete-li přidat nebo upravit položky hostitelské tabulky, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť**.

2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Tabulka hostitelů**. Otevře se dialogové okno **Tabulka hostitelů**.
3. V dialogovém okně **Tabulka hostitelů** můžete přidávat, upravovat a odstraňovat záznamy tabulky hostitelů.

Chcete-li získat přístup ke stránkám s vlastnostmi specifickými pro IPv4, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **svůj server → Síť**.
2. Klepněte pravým tlačítkem myši na **IPv4** a vyberte **Vlastnosti**. Otevře se dialogové okno **Vlastnosti IPv4**.
3. Na jednotlivých kartách tohoto dialogového okna můžete zobrazovat a upravovat nastavení vlastností IPv4.

Chcete-li získat přístup ke stránkám s vlastnostmi specifickými pro IPv6, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť**.
2. Klepněte pravým tlačítkem myši na **IPv6** a vyberte **Vlastnosti**. Otevře se dialogové okno **Vlastnosti IPv6**.
3. Na jednotlivých kartách tohoto dialogového okna můžete zobrazovat a upravovat nastavení vlastností IPv6.

## Konfigurace protokolu IPv6

Pokyny v tomto tématu vám pomohou při konfiguraci IPv6.

Pokud protokol IPv6 ještě neznáte, prostudujte přehled v části “Protokol IP (Internet Protocol) verze 6” na stránce 3.

Chcete-li konfigurovat IPv6, musíte změnit konfiguraci serveru v prostředí produktu iSeries Navigator. Před konfigurací prostudujte pokyny a speciální požadavky v části “Konfigurace protokolu IPv6” na stránce 22.

## Přidání rozhraní IPv4

Pokyny v tomto tématu vám pomohou při vytváření nových rozhraní IPv4.

Chcete-li vytvořit nové rozhraní IPv4, postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť** → **Konfigurace TCP/IP** → **IPv4**.
2. Klepněte pravým tlačítkem myši na **Rozhraní**, vyberte **Nové rozhraní** a vyberte odpovídající typ rozhraní IPv4: **Lokální síť (LAN)** , **Dálková síť (WAN)** nebo **Virtuální IP**.
3. Při vytváření nového rozhraní IPv4 postupujte podle pokynů průvodce.

## Přidání rozhraní IPv6

Pokyny v tomto tématu vám pomohou při vytváření nových rozhraní IPv6.

Chcete-li vytvořit nové rozhraní IPv6, postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť** → **Konfigurace TCP/IP** → **IPv6**.
2. Klepněte pravým tlačítkem myši na **Rozhraní** a vyberte **Nové rozhraní**.
3. Při vytváření nového rozhraní IPv6 postupujte podle pokynů průvodce.

## Přidání přenosových cest IPv4

Pokyny v tomto tématu vám pomohou při konfiguraci nových přenosových cest IPv4.

Jakékoliv změny, které provedete v informacích o přenosové cestě, začnou platit okamžitě.

Chcete-li konfigurovat novou přenosovou cestu IPv4, postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť** → **Konfigurace TCP/IP** → **IPv4**.
2. Klepněte pravým tlačítkem myši na **Přenosové cesty** a vyberte **Nová přenosová cesta**.
3. Při konfiguraci nové přenosové cesty IPv4 postupujte podle pokynů průvodce.

## Přidání přenosových cest IPv6

Pokyny v tomto tématu vám pomohou při konfiguraci nových přenosových cest IPv6.

Jakékoliv změny, které provedete v informacích o přenosové cestě, začnou platit okamžitě.

Chcete-li konfigurovat novou přenosovou cestu IPv6, postupujte takto:

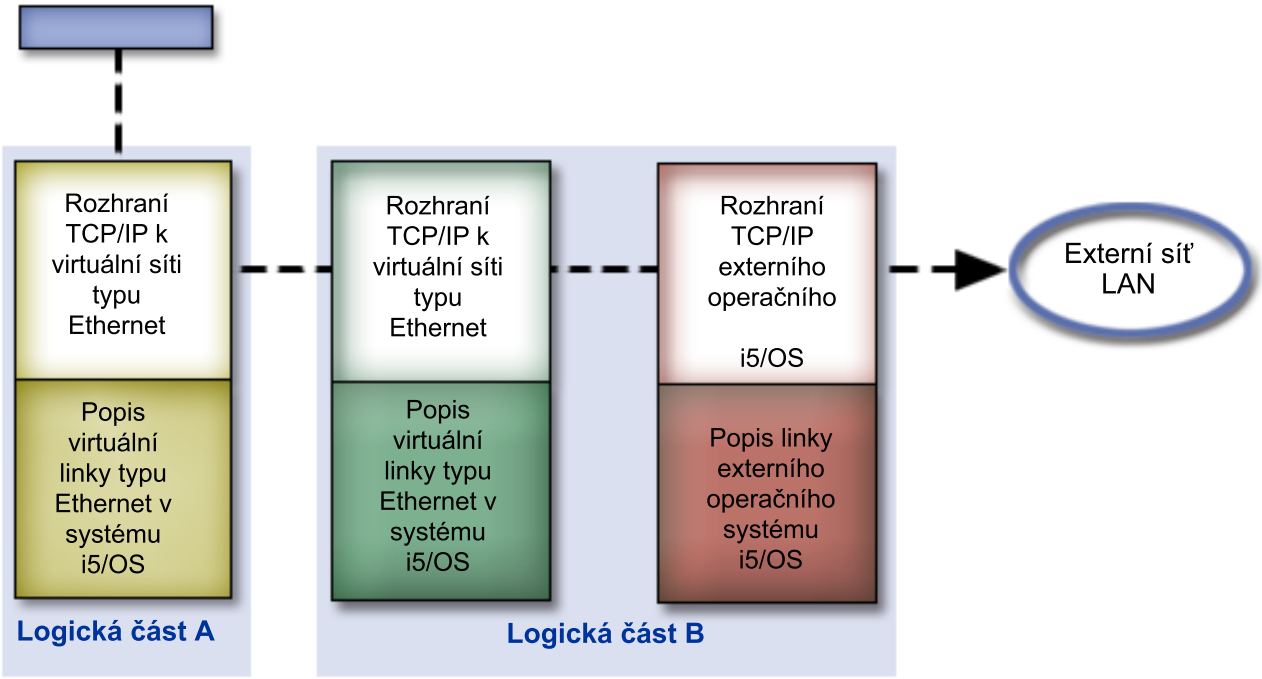
1. V prostředí produktu iSeries Navigator vyberte *svůj server* → **Síť** → **Konfigurace TCP/IP** → **IPv6**.
2. Klepněte pravým tlačítkem myši na **Přenosové cesty** a vyberte **Nová přenosová cesta**.
3. Při konfiguraci nové přenosové cesty IPv6 postupujte podle pokynů průvodce.

---

# Techniky TCP/IP pro propojení virtuální sítě Ethernet s externími sítěmi LAN

Můžete využívat výhody virtuální sítě typu Ethernet v operačním systému i5/OS.

Používáte-li při komunikaci mezi logickými částmi virtuální síť typu Ethernet, budete možná chtít logickým částem umožnit rozšíření této komunikace do externí fyzické sítě LAN. Existuje několik způsobů, jak navázat spojení mezi virtuální sítí typu Ethernet a externí sítí LAN s využitím různých metod TCP/IP. Budete muset povolit postup provozu TCP/IP mezi virtuální sítí typu Ethernet a externí sítí typu LAN. Tento obrázek ukazuje logický postup IP paketů.




IP provoz iniciovaný logickou částí A postupuje z rozhraní virtuální sítě typu Ethernet do rozhraní virtuální sítě typu Ethernet logické části B. Pomocí implementace jedné ze tří technik TCP/IP popsaných níže můžete umožnit paketům IP pokračovat do externího rozhraní a dále na místo určení.

Existují tři metody propojení virtuální sítě typu Ethernet a externí sítě typu LAN. Každá metoda má své nuance, které ji činí více či méně vhodnou vzhledem k prostředí a vašim znalostem TCP/IP. Zvolte si jednu z těchto metod:

- Metoda ARP proxy
- Metoda převodu síťové adresy
- Metoda směrování TCP/IP

## Metoda ARP proxy

Tato metoda ARP proxy využívá transparentního vytváření podsítí k přidružení virtuálního rozhraní logické části k externímu rozhraní. Funkce ARP proxy je součástí balíku TCP/IP. Pokud znáte potřebné IP adresy, doporučujeme vám použít tuto metodu.

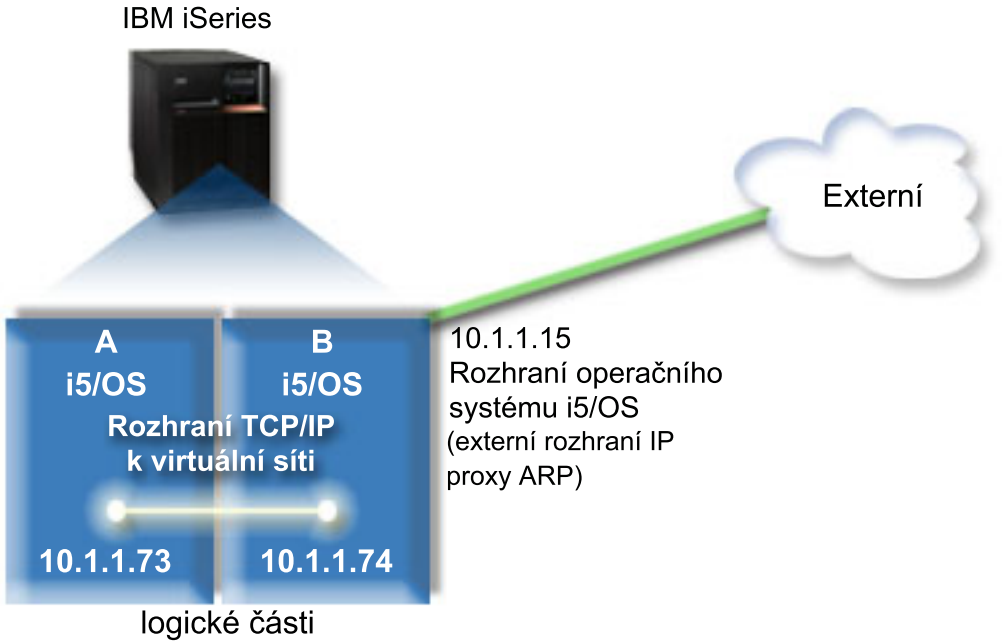
Více informací o technice transparentního vytváření podsítí se dozvíte zde:

- V4 TCP/IP for AS/400: More Cool Things Than Ever

  Tato červená knihaIBM obsahuje vzorové scénáře, které ukazují běžná řešení spolu s příklady konfigurací. Pomůže vám také s plánováním, instalací, přizpůsobením, konfigurací a odstraňováním problémů s TCP/IP na serveru iSeries.
- Vyvažování směrování a vytížení TCP/IP

  Toto téma pojednává o technikách a pokynech směrování a vyvažování zatížení.

Pokud se rozhodnete použít metodu ARP proxy, musíte mít dobré znalosti o vytváření podsítí a TCP/IP. Musíte získat souvislý blok IP adres, které je možné směrovat vaší sítí. Z těchto IP adres vytvoříte podsíť. V tomto příkladu je použitý souvislý blok čtyř IP adres (10.1.1.72 až 10.1.1.75). Protože se jedná o blok čtyř adres, je maskou podsítě pro tyto adresy 255.255.255.252. Každému virtuálnímu rozhraní TCP/IP přiřadíte jednu tak, jak to zobrazuje tento obrázek.




V tomto příkladu je provoz TCP/IP veden z logické části A přes virtuální síť typu Ethernet do rozhraní 10.1.1.74 v logické části B. Protože rozhraní 10.1.1.74 je přidruženo k externímu rozhraní ARP proxy 10.1.1.15, pokračují pakety z virtuální sítě typu Ethernet dále pomocí rozhraní ARP proxy.

Chcete-li konfigurovat virtuální síť typu Ethernet tak, aby používala metodu propojení ARP proxy, postupujte takto:

### Krok 1: Povolte logickým částem být součástí virtuální sítě typu Ethernet

**Poznámka:** Nastavujete-li virtuální síť typu Ethernet na modelu serveru 5*xx*, najdete další informace v části Virtual Ethernet pro logické části operačního systému i5/OS v rámci aplikace IBM Systems Hardware Information Center.

Chcete-li povolit virtuální síť typu Ethernet, postupujte takto:

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a potom stiskněte klávesu Enter.

2. Zadejte svůj ID uživatele servisních nástrojů a heslo.
3. Na panelu SST (System Service Tools) vyberte volbu 5 (Work with System Partitions).
4. Na panelu Work with System Partitions vyberte volbu 3 (Work with Partition Configuration).
5. Stiskněte klávesu F10 (Práce s produktem Virtual Ethernet).
6. Ve sloupci, který odpovídá logické části A a logické části B, zadejte hodnotu 1. Umožníte tak logickým částem vzájemnou komunikaci přes virtuální síť typu Ethernet.
7. Ukončete SST (System Service Tools) a vraťte se na příkazový řádek.

**Související informace**

Konsolidace logických částí operačních systémů i5/OS, AIX® a Linux® v systému IBM eServer™ i5

## Krok 2: Vytvořte popis linky sítě typu Ethernet.

Podle modelu serveru, který používáte, provedete tento krok jedním ze dvou způsobů.

**Vytvoření popisu linky typu Ethernet na modelech serveru 270 a 8*xx*:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci modelů serverů 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Ethernet port označený jako 268C je prostředkem virtuální sítě typu Ethernet. Pro každou virtuální síť typu Ethernet spojenou s danou logickou částí je zde jeden port.
3. Na panelu Zobrazení podrobností prostředku posuňte kurzor svisle tak, aby se zobrazila adresa portu. Adresa portu odpovídá virtuální síti typu Ethernet, kterou jste vybrali během konfigurace logických částí.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy konfigurací) vedle příslušného portu virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.
5. Na panelu Práce s popisy konfigurací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky - Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Název VETH0, přestože může být libovolný, odpovídá číslovanému sloupci na stránce Virtual Ethernet, kde jste povolili komunikaci jednotlivým logickým částem. Pokud pro popisy linek a přidružené sítě typu Ethernet použijete stejný název, můžete snadno sledovat konfigurace svých virtuálních sítí typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).
7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

**Vytvoření popisu linky typu Ethernet na jiných modelech serveru, než je 270 a 8xx:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci jiných modelů serverů než 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Ethernet porty označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet je zde jeden port. Každý port označený jako 268C má přidružený kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).
3. Na panelu Zobrazení podrobností prostředku posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro tuto virtuální síť typu Ethernet.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy konfigurací) vedle příslušného prostředku virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.
5. Na panelu Práce s popisy konfigurací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Pokud použijete pro popisy linek a přidružené sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace svých virtuálních sítí typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).
7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky sítě typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

## Krok 3: Zapněte postoupení datagramu pomocí IP

Zapněte postoupení datagramu pomocí IP, aby mohly být pakety doručovány mezi různými podsítěmi.

Chcete-li zapnout postoupení datagramu pomocí IP, postupujte takto:

1. Na příkazový řádek logické části B zadejte CHGTCPA a stiskněte klávesu F4.
2. Na náznak *Postoupit datagram pomocí IP* zadejte *YES.

## Krok 4: Vytvořte rozhraní, které povolí ARP proxy

Při vytváření rozhraní TCP/IP, které povolí ARP proxy, postupujte takto:

1. Musíte získat souvislý blok IP adres, které je možné směrovat vaší sítí.

   Protože v této virtuální síti typu Ethernet používáte dvě logické části, budete potřebovat blok čtyř adres. Hodnota čtvrtého segmentu první IP adresy v bloku musí být dělitelná čtyřmi. První a poslední IP adresy tohoto bloku znamenají IP adresu podsítě a IP adresu vysílání; tyto adresy nelze použít. Druhá a třetí IP adresa může být použita pro rozhraní TCP/IP virtuální sítě typu Ethernet v logické části A a logické části B. Pro tuto proceduru je blok IP adres definován od 10.1.1.72 do 10.1.1.75 s maskou podsítě 255.255.255.252.

   Také potřebujete jednu IP adresu jako externí adresu TCP/IP. Tato IP adresa nemusí náležet k použitému bloku souvislých adres, ale musí být součástí původní masky podsítě 255.255.255.0. V této proceduře je použita externí adresa 10.1.1.15.

2. Vytvořte rozhraní TCP/IP operačního systému i5/OS pro logickou část B. Toto rozhraní je známo jako externí IP rozhraní ARP proxy. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '10.1.1.15'.
   e. Na náznak *Popis linky* zadejte název popisu linky, například ETHLINE.
   f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
3. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.

## Krok 5: Vytvořte virtuální rozhraní TCP/IP v logické části A

Při vytváření virtuálního rozhraní postupujte takto:

1. Na příkazový řádek logické části A zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
2. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
3. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
4. Na náznak *Internetová adresa* zadejte '10.1.1.73'.
5. Na náznak *Popis linky* zadejte název popisu linky, na příklad VETH0.
6. Na náznak *Maska podsítě* zadejte '255.255.255.252'.
7. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.

## Krok 6: Vytvořte virtuální rozhraní TCP/IP v logické části B

Při vytváření virtuálního rozhraní postupujte takto:

1. Na příkazový řádek logické části B zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
2. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
3. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
4. Na náznak *Internetová adresa* zadejte '10.1.1.74'.
5. Na náznak *Popis linky* zadejte název popisu linky, na příklad VETH0.
6. Na náznak *Maska podsítě* zadejte '255.255.255.252'.
7. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.

## Krok 7: Vytvořte seznam preferovaných rozhraní

Vytvoření seznamu preferovaných rozhraní vám umožní kontrolovat, které adaptéry a IP adresy budou preferovaným rozhraním pro výběr agenta ARP proxy virtuální sítě typu Ethernet.

Chcete-li vytvořit seznam preferovaných rozhraní, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte **Síť → Konfigurace TCP/IP → IPv4**.
2. Vyberte volbu **Rozhraní**.
3. V zobrazeném seznamu rozhraní vyberte rozhraní virtuální sítě typu Ethernet, pro které chcete seznam preferovaných rozhraní vytvořit.
4. Klepněte pravým tlačítkem myši na vybrané rozhraní a potom klepněte na **Vlastnosti**.
5. Klepněte na kartu **Rozšířené**.
6. Na zobrazeném panelu vyberte adresy rozhraní v seznamu Dostupná rozhraní a klepněte na tlačítko **Přidat**.

Rozhraní můžete z pravého podokna seznamu preferovaných rozhraní odstranit klepnutím na tlačítko **Odstranit**. Můžete také změnit pořadí rozhraní v tomto podokně tím, že vybrané rozhraní přemístíte nahoru nebo dolů v seznamu pomocí tlačítek **Přemístit nahoru** a **Přemístit dolů**.

7. Chcete-li tento seznam povolit, zaškrtněte okénko **Umožnit ARP proxy**.
8. Klepnutím na tlačítko **OK** uložte právě vytvořený seznam preferovaných rozhraní.

**Poznámky:**

a. Pro seznam preferovaných rozhraní je podporováno pouze 10 rozhraní. Konfigurujete-li více než 10 rozhraní, bude seznam zkrácen na prvních 10 položek.

b. Rozhraní, pro které chcete seznam preferovaných rozhraní vytvořit, musí být neaktivní, jinak nelze seznam konfigurovat. Rozhraní uvedená v seznamu preferovaných rozhraní nemusejí být při konfiguraci tohoto seznamu neaktivní.

### Krok 8: Vytvořte přenosovou cestu

Při vytváření předvolené přenosové cesty umožňující paketům opustit virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište CFGTCP a potom stiskněte klávesu Enter.
2. Vyberte volbu 2 (Pracovat s přenosovými cestami TCP/IP) a potom stiskněte klávesu Enter.
3. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter.
4. Na náznak *Místo určení předepsané cesty* zadejte *DFTROUTE.
5. Na náznak *Maska podsítě* zadejte *NONE.
6. Na náznak *Další směrovací uzel* zadejte '10.1.1.74'.

   Pakety jsou z logické části A přenášeny přes virtuální síť typu Ethernet do rozhraní 10.1.1.74 pomocí této předvolené přenosové cesty. Rozhraní 10.1.1.74 je přidruženo k externímu rozhraní ARP proxy 10.1.1.15, a proto pakety pokračují z virtuální sítě typu Ethernet pomocí rozhraní ARP proxy.

### Krok 9: Ověřte síťové komunikace

Ověřte funkčnost své síťové komunikace příkazem ping:

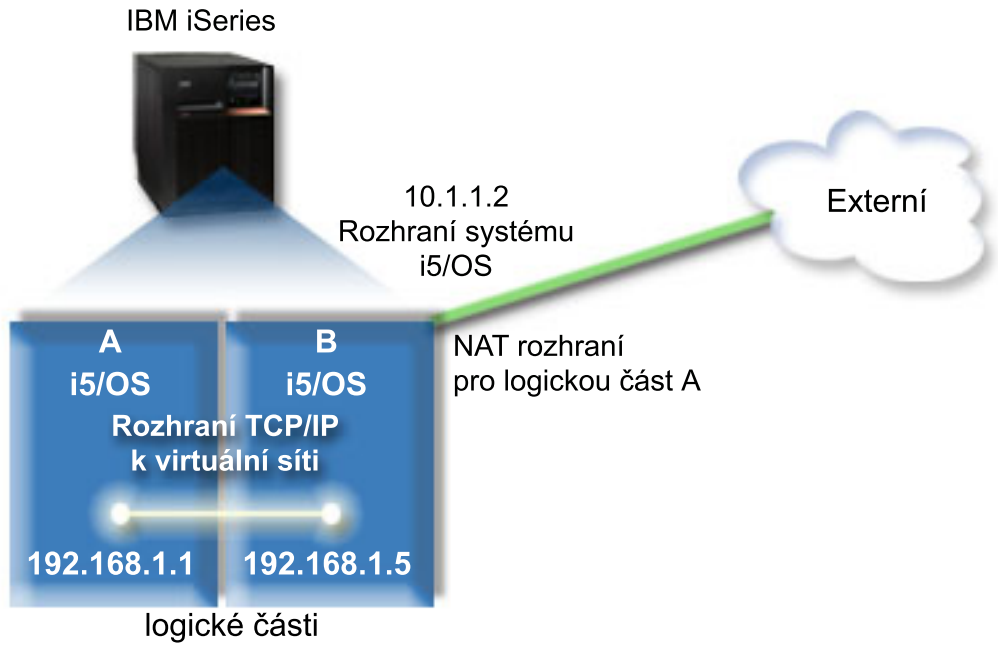
- Pomocí příkazu ping v logické části A otestujte spojení rozhraní 10.1.1.74 virtuální sítě Ethernet a externího hostitele.
- Pomocí příkazu ping v externím hostitelském systému i5/OS otestujte spojení rozhraní 10.1.1.73 a 10.1.1.74 virtuální sítě Ethernet.

## Metoda převodu síťové adresy

Při směrování provozu mezi logickou částí a vnější sítí můžete použít filtrování paketů v operačním systému i5/OS.

Pomocí metody NAT (převod síťové adresy) lze směrovat provoz mezi virtuální sítí typu Ethernet a externí sítí. Tato zvláštní forma NAT se nazývá statický NAT a umožňuje příchozímu a odchozímu provozu IP postupovat do a z virtuální sítě typu Ethernet. Můžete také použít jiné formy NAT, například maskovací NAT, pokud virtuální síť typu Ethernet nevyžaduje, aby byl přijímaný provoz iniciován externími klienty. Stejně jako metody směrování TCP/IP a ARP proxy můžete využít stávající připojení do sítě operačního systému i5/OS. Protože budete používat pravidla paketů IP, musíte při vytváření a používání svých pravidel použít produkt iSeries Navigator.

Následující obrázek představuje příklad použití NAT (převod síťové adresy) k navázání spojení mezi virtuální sítí typu Ethernet a externí sítí. Síť 10.1.1.*x* představuje externí síť, síť 192.168.1.*x* představuje virtuální síť typu Ethernet.




V tomto příkladu veškerý provoz TCP/IP existující pro server postupuje přes rozhraní 10.1.1.2. Je vytvořeno nové rozhraní 10.1.1.3 pro komunikaci mezi sítěmi 10.1.1.x a 192.168.1.x. Protože se jedná o scénář se statickým mapováním, je příchozí provoz převáděn z rozhraní 10.1.1.3 do rozhraní 192.168.1.5. Odchozí provoz je převáděn z rozhraní 192.168.1.5 do rozhraní 10.1.1.3. Logické části A a B používají při vzájemné komunikaci svá virtuální rozhraní 192.168.1.1 a 192.168.1.5.

Chcete-li uvést statický NAT do provozu, musíte nejprve nastavit komunikaci operačního systému i5/OS a TCP/IP. Poté vytvoříte a použijete některá pravidla paketů IP. Při konfiguraci virtuální sítě typu Ethernet tak, aby používala metodu propojení NAT, postupujte takto:

## Krok 1: Povolte logickým částem být součástí virtuální sítě typu Ethernet

**Poznámka:** Nastavujete-li virtuální síť typu Ethernet na modelu serveru 5*xx*, najdete další informace v tématu Virtual Ethernet pro logické části operačního systému i5/OS v rámci aplikace IBM Systems Hardware Information Center.

Chcete-li povolit virtuální síť typu Ethernet, postupujte takto:

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a potom stiskněte klávesu Enter.
2. Zadejte svůj ID uživatele servisních nástrojů a heslo.
3. Na panelu SST (System Service Tools) vyberte volbu 5 (Work with System Partitions).).
4. Na panelu Work with System Partitions vyberte volbu 3 (Work with partition configuration).
5. Stiskněte klávesu F10 (Work with Virtual Ethernet).
6. Zadejte hodnotu 1 do příslušného sloupce pro logickou část A a logickou část B, čímž umožníte logickým částem navzájem komunikovat přes virtuální síť typu Ethernet.
7. Ukončete SST (System Service Tools) a vraťte se na příkazový řádek.

**Související informace**

Konsolidace logických částí operačních systémů i5/OS, AIX® a Linux® v systému IBM eServer™ i5

## Krok 2: Vytvořte popis linky sítě typu Ethernet

Podle modelu serveru, který používáte, provedete tento krok jedním ze dvou způsobů. K vytvoření popisu linky vyberte jednu z těchto metod dle konkrétního modelu svého serveru.

**Vytvoření popisu linky typu Ethernet na modelech serveru 270 a 8*xx*:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci modelů serverů 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Ethernet port označený jako 268C je prostředkem virtuální sítě typu Ethernet. Pro každou virtuální síť typu Ethernet spojenou s danou logickou částí je zde jeden port.
3. Posouváním kurzoru v panelu Zobrazení podrobností prostředku vyhledejte adresu portu. Adresa portu odpovídá virtuální síti typu Ethernet, kterou jste vybrali během konfigurace dané logické části.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy konfigurací) vedle příslušného portu virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.
5. Na panelu Práce s popisy konfigurací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky - Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Název VETH0, přestože může být libovolný, odpovídá číslovanému sloupci na stránce Virtual Ethernet, kde jste povolili komunikaci jednotlivým logickým částem. Pokud použijete pro popisy linek a přidružené sítě typu Ethernet stejný název, můžete snadno sledovat konfiguraci virtuální sítě typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).
7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky sítě typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

**Vytvoření popisu linky typu Ethernet na jiných modelech serveru, než je 270 a 8xx:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci jiných modelů serverů než 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Porty typu Ethernet označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet je zde jeden port. Každý port označený jako 268C má přidružený kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).
3. Na panelu Zobrazení podrobností prostředku posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro tuto virtuální síť typu Ethernet.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy konfigurací) vedle příslušného prostředku virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.

5. Na panelu Práce s popisy konfigurací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky - Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Pokud použijete pro popisy linek a přidružené sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace svých virtuálních sítí typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).
7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky sítě typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

## Krok 3: Zapněte postoupení datagramu pomocí IP

Zapněte postoupení datagramu pomocí IP. Pakety pak budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, postupujte takto:

1. Na příkazový řádek logické části A napište CHGTCPA a potom stiskněte klávesu F4.
2. Na náznak *Postoupit datagram pomocí IP* zadejte *YES.

## Krok 4: Vytvořte rozhraní

Při vytváření rozhraní TCP/IP postupujte takto:

1. V logické části B vytvořte a spusťte rozhraní TCP/IP operačního systému i5/OS pro příchozí a odchozí obecnou komunikaci se serverem. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '10.1.1.2'.
   e. Na náznak *Popis linky* zadejte ETHLINE.
   f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
   g. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.
2. Vytvořte a spusťte další rozhraní TCP/IP, které naváže spojení s externí sítí. Mělo by použít stejný popis linky jako existující externí rozhraní TCP/IP. Toto rozhraní posléze provede převod adres logických částí. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '10.1.1.3'.
   e. Na náznak *Popis linky* zadejte ETHLINE.

f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
g. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.

3. V logické části A vytvořte a spusťte rozhraní TCP/IP operačního systému i5/OS pro virtuální síť typu Ethernet. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části A zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '192.168.1.1'.
   e. Na náznak *Popis linky* zadejte VETH0.
   f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
   g. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.
4. V logické části B vytvořte a spusťte rozhraní TCP/IP operačního systému i5/OS pro virtuální síť typu Ethernet. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '192.168.1.5'.
   e. Na náznak *Popis linky* zadejte VETH0.
   f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
   g. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.

## Krok 5: Ověřte síťové komunikace

Ověřte funkčnost síťové komunikace pomocí příkazu ping:

- V logické části A zadejte příkaz ping a otestujte spojení rozhraní 192.168.1.5 virtuální sítě typu Ethernet a externího hostitele.
- V externím hostiteli operačního systému i5/OS otestujte spojení každého z rozhraní 192.168.1.1 a 192.168.1.5 virtuální sítě typu Ethernet.

## Krok 6: Vytvořte pravidla paketu

Chcete-li vytvořit pravidla paketu, která mapují soukromou adresu v logické části A na veřejnou adresu v logické části B, použijte průvodce překladem adres v prostředí produktu iSeries Navigator.

Při vytváření pravidel paketu postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte *svůj server* → **Síť** → **Metody IP**.
2. Klepněte pravým tlačítkem na položku **Pravidla paketu** a vyberte **Editor pravidel**.
3. Vyberte **Převod adresy** v nabídce **průvodce**.
4. Při vytváření pravidel paketu postupujte podle pokynů průvodce. Tato procedura zahrnuje výběr těchto položek:
   - Vyberte možnost **Mapovat převod adresy**.
   - Zadejte soukromou adresu 192.168.1.1.
   - Zadejte veřejnou IP adresu 10.1.1.3.
   - Vyberte linku, na které jsou rozhraní konfigurována, například ETHLINE.
5. Vyberte položku **Aktivovat pravidla** v nabídce **Soubor**.

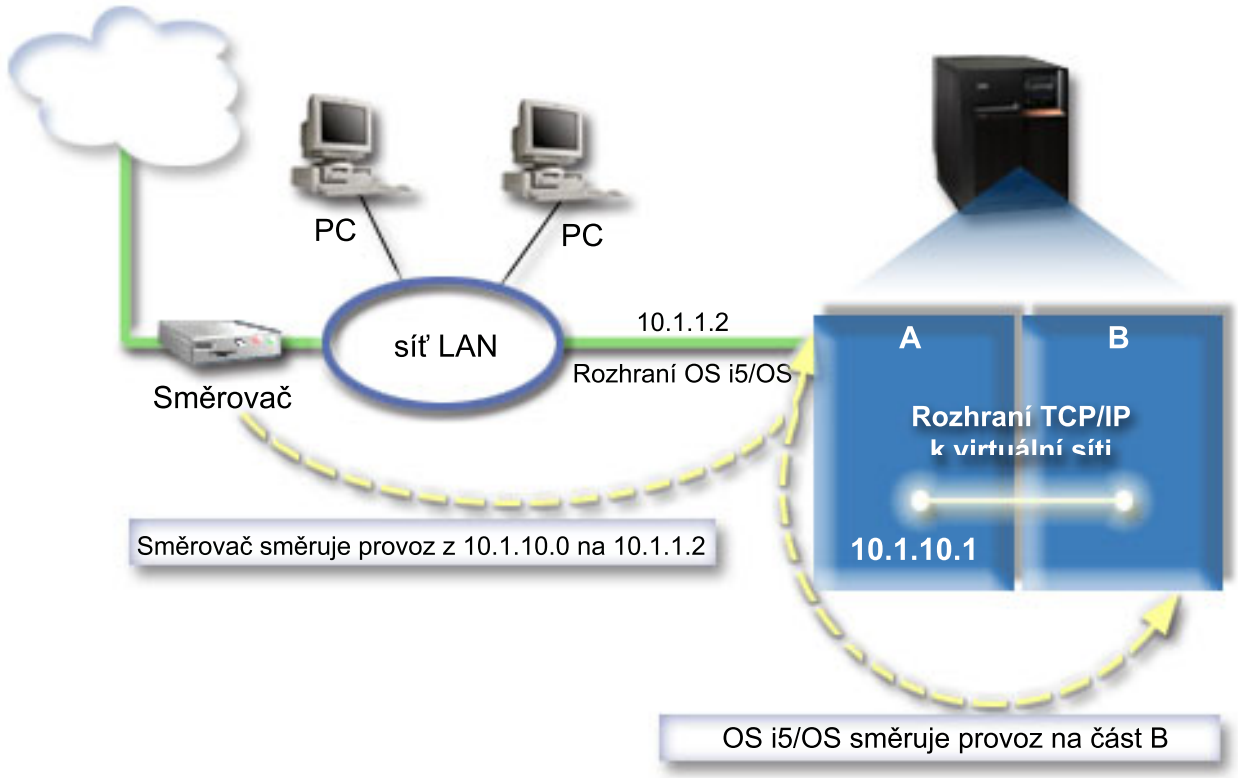
### Krok 7: Ověřte síťové komunikace

Poté, co vytvoříte pravidla paketu, byste měli ověřit síťové komunikace. Chcete-li otestovat odchozí komunikaci, otestujte pomocí příkazu ping spojení s hostitelským systémem z logické části A. Chcete-li otestovat příchozí komunikaci, použijte příkaz ping z hostitelského systému na logickou část A.

## Metoda směrování TCP/IP

Standardní směrování TCP/IP se používá při směrování provozu do virtuální sítě typu Ethernet stejným způsobem, jakým definujete směrování do libovolné jiné sítě LAN. Vyžaduje to aktualizaci informací o směrování ve vaší síti.

Provoz můžete také směrovat do svých logických částí pomocí serveru iSeries s využitím různých technik směrování. Toto řešení není obtížné z hlediska konfigurace,ale jeho implementace nemusí být vhodná vzhledem k topologii vaší sítě. Prohlédněte si tento obrázek.




Existující rozhraní TCP/IP (10.1.1.2) naváže spojení se sítí LAN. Síť LAN je spojena se vzdálenou sítí pomocí směrovače. Virtuální rozhraní TCP/IP v logické části B je adresováno jako 10.1.10.2 a virtuální rozhraní TCP/IP v logické části A jako 10.1.10.1. Zapnete-li v operačním systému i5/OS postoupení datagramu IP, přesměruje operační systém i5/OS IP pakety do logické části B a z logické části B. Definujete-li připojení TCP/IP pro logickou část B, musí být adresa směrovače 10.1.10.1.

Obtížnost tohoto typu směrování spočívá v doručení IP paketů na server iSeries. V tomto scénáři můžete definovat přenosovou cestu na směrovači tak, aby předávala pakety určené pro síť 10.1.10.0 do rozhraní 10.1.1.2. Toto je možné u vzdálených síťových klientů. Funguje to také u klientů lokální sítě LAN (klientů připojených ke stejné síti LAN jako server iSeries), pokud rozeznají stejný směrovač jako svůj další směrovací uzel. V opačném případě musí mít každý klient přenosovou cestu, která směruje provoz 10.1.10.0 do rozhraní 10.1.1.2 operačního systému i5/OS. V tom spočívá nepraktičnost této metody. Máte-li mnoho klientů LAN, musíte definovat mnoho přenosových cest.

Ke konfiguraci virtuální sítě typu Ethernet tak, aby používala metodu směrování TCP/IP, postupujte takto:

## Krok 1: Povolte logickým částem být součástí virtuální sítě typu Ethernet

**Poznámka:** Nastavujete-li virtuální síť typu Ethernet na modelu serveru 5*xx*, najdete další informace v části Virtual Ethernet pro logické části operačního systému i5/OS v rámci aplikace IBM Systems Hardware Information Center.

Chcete-li povolit virtuální síť typu Ethernet, postupujte takto:

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a potom stiskněte klávesu Enter.
2. Zadejte svůj ID uživatele servisních nástrojů a heslo.
3. Na panelu SST (System Service Tools) vyberte volbu 5 (Work with System Partitions).
4. Na panelu Work with System Partitions vyberte volbu 3 (Work with partition configuration).
5. Stiskněte klávesu F10 (Work with Virtual Ethernet).
6. Zadejte hodnotu 1 do příslušného sloupce pro logickou část A a logickou část B, čímž umožníte logickým částem navzájem komunikovat přes virtuální síť typu Ethernet.
7. Ukončete SST (System Service Tools) a vraťte se na příkazový řádek.

**Související informace**

Konsolidace logických částí operačních systémů i5/OS, AIX® a Linux® v systému IBM eServer™ i5

## Krok 2: Vytvořte popis linky sítě typu Ethernet

Podle modelu serveru, který používáte, provedete tento krok jedním ze dvou způsobů. K vytvoření popisu linky vyberte jednu z těchto metod dle konkrétního modelu svého serveru.

**Vytvoření popisu linky typu Ethernet na modelech serveru 270 a 8*xx*:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci modelů serverů 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Ethernet port označený jako 268C je prostředkem virtuální sítě typu Ethernet. Pro každou virtuální síť typu Ethernet spojenou s danou logickou částí je zde jeden port.
3. Posouváním kurzoru v panelu Zobrazení podrobností prostředku vyhledejte adresu portu. Adresa portu odpovídá virtuální síti typu Ethernet, kterou jste vybrali během konfigurace logických částí.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy komunikací) vedle příslušného portu virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.
5. Na panelu Práce s prostředky komunikací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky - Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Název VETH0, přestože může být libovolný, odpovídá číslovanému sloupci na stránce Virtual Ethernet, kde jste povolili komunikaci jednotlivým logickým částem. Pokud použijete pro popisy linek a přidružené sítě typu Ethernet stejný název, můžete snadno sledovat konfiguraci virtuální sítě typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).

7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky sítě typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

**Vytvoření popisu linky typu Ethernet na jiných modelech serveru, než je 270 a 8xx:**

Vytvoření popisu linky typu Ethernet je prvním krokem konfigurace pro server, který má používat virtuální síť typu Ethernet. Při konfiguraci jiných modelů serverů než 270 a 8*xx* můžete použít následující postup.

Při konfiguraci nového popisu linky typu Ethernet podporující virtuální síť typu Ethernet postupujte takto:

1. Na příkazový řádek logické části A napište WRKHDWRSC *CMN a potom stiskněte klávesu Enter.
2. Na panelu Práce s prostředky komunikací vyberte volbu 7 (Zobrazit podrobnosti prostředku) vedle příslušného portu virtuální sítě typu Ethernet.

   Porty typu Ethernet označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet je zde jeden port. Každý port označený jako 268C má přidružený kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).
3. Na panelu Zobrazení podrobností prostředku posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro tuto virtuální síť typu Ethernet.
4. Na panelu Práce s prostředky komunikací vyberte volbu 5 (Pracovat s popisy konfigurací) vedle příslušného prostředku virtuální sítě typu Ethernet a potom stiskněte klávesu Enter.
5. Na panelu Práce s popisy konfigurací vyberte volbu 1 (Vytvořit) a stiskněte klávesu Enter. Zobrazí se panel CRTLNIETH (Vytvoření popisu linky - Ethernet).
   a. Na náznak *Popis linky* zadejte VETH0. Pokud použijete pro popisy linek a přidružené sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace svých virtuálních sítí typu Ethernet.
   b. Na náznak *Rychlost linky* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximální velikost rámce* zadejte 8996 a potom stiskněte klávesu Enter. Změnou velikosti rámce na 8996 bude zlepšen přenos dat přes virtuální síť typu Ethernet.

      Uvidíte zprávu potvrzující vytvoření popisu linky.
6. Logicky zapněte popis linky. Zadejte WRKCFGSTS *LIN a potom pro VETH0 vyberte volbu 1 (Logicky zapnout).
7. Opakujte kroky 1 až 6, ale nyní je proveďte z příkazového řádku v logické části B, čímž vytvoříte popis linky sítě typu Ethernet pro logickou část B.

   I když názvy popisů linek mohou být libovolné, je užitečné používat stejné názvy pro všechny popisy linek přidružených k virtuální síti typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

**Další krok**: Zapnutí postoupení datagramu pomocí IP

## Krok 3: Zapněte postoupení datagramu pomocí IP

Zapněte postoupení datagramu pomocí IP. Pakety pak budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, postupujte takto:

1. Na příkazový řádek logické části A napište CHGTCPA a potom stiskněte klávesu F4.
2. Na náznak *Postoupit datagram pomocí IP* zadejte *YES.

## Krok 4: Vytvořte rozhraní

Při vytváření rozhraní TCP/IP postupujte takto:

1. Vytvořte rozhraní TCP/IP operačního systému i5/OS v logické části A. Při vytváření tohoto rozhraní postupujte takto:
   a. Na příkazový řádek logické části A zadejte CFGTCP a potom stiskněte klávesu Enter. Zobrazí se panel Konfigurace TCP/IP.
   b. Vyberte volbu 1 (Pracovat s rozhraními TCP/IP) a potom stiskněte klávesu Enter.
   c. Vyberte volbu 1 (Přidat) a potom stiskněte klávesu Enter. Zobrazí se panel ADDTCPIFC (Přidání rozhraní TCP/IP).
   d. Na náznak *Internetová adresa* zadejte '10.1.1.2'.
   e. Na náznak *Popis linky* zadejte název popisu linky, například ETHLINE.
   f. Na náznak *Maska podsítě* zadejte '255.255.255.0'.
2. Spusťte rozhraní. Na panelu Práce s rozhraními TCP/IP vyberte volbu 9 (Spustit) vedle příslušného rozhraní.
3. Opakujte kroky 2 a 3, kterými vytvoříte a spustíte rozhraní TCP/IP v logické části A a logické části B.

   Tato rozhraní jsou použita pro virtuální síť typu Ethernet. Pro tato rozhraní použijte IP adresy 10.1.10.1 a 10.1.10.2 a masku podsítě 255.255.255.0.

## Pokyny k virtuální síti typu Ethernet

Jako alternativu k použití síťové karty ke komunikaci mezi logickými částmi můžete použít virtuální síť typu Ethernet.

Produkt Virtual Ethernet vám umožňuje zavést vysokorychlostní komunikaci mezi logickými částmi, aniž byste museli dokupovat další hardware. Pro každý z 16 aktivních portů vytvoří systém virtuální komunikační Ethernet port, jako například CMN*xx* s typem prostředku 268C. Logické části přiřazené ke stejné lokální síti LAN tak budou moci komunikovat přes toto spojení. Fyzický systém umožňuje konfigurovat až 16 různých virtuálních lokálních sítí. Virtuální síť typu Ethernet poskytuje stejné funkce jako použití 1 GB adaptéru typu Ethernet. Sítě Token Ring, Ethernet 10 Mb/s a 100 Mb/s lokální sítě nejsou podporovány virtuální sítí typu Ethernet.

Virtuální síť typu Ethernet je úsporné řešení vytváření sítí poskytující další důležité výhody:

- Hospodárnost: Není nutné dokupovat další síťový hardware. Můžete k serveru přidávat logické části a komunikovat s externí sítí typu LAN bez nutnosti instalace dalších fyzických karet LAN. Pokud má současný server omezený počet dostupných slotů vhodných k instalaci dalších karet LAN, nabízí virtuální síť typu Ethernet možnost obsluhovat logické části bez nutnosti přechodu na vyšší verzi serveru.
- Flexibilita: Je možné konfigurovat maximálně 16 charakteristických propojení umožňujících konfiguraci výběrových komunikačních cest mezi logickými částmi. Další flexibility lze dosáhnout tím, že model konfigurace umožňuje implementovat jak virtuální síť typu Ethernet, tak fyzické připojení k síti LAN. Tato funkce je užitečná, používáte-li logickou část s operačním systémem Linux jako hostitelský systém pro aplikaci ochranné bariéry (firewall).
- Rychlost: Virtuální síť typu Ethernet emuluje 1 GB spojení typu Ethernet a poskytuje rychlý a pohodlný způsob komunikace mezi logickými částmi. To rozšiřuje možnost integrace oddělených aplikací provozovaných na různých logických částech.
- Všestrannost: Bez ohledu na to, zda jsou logické části spouštěny pod operačním systémem i5/OS nebo Linux, mohou být všechny připojeny ke stejné virtuální síti typu Ethernet.
- Snížení zahlcení: Použitím virtuální sítě typu Ethernet ke komunikaci mezi logickými částmi se snižuje komunikační provoz v externí síti typu LAN. To v případě sítě Ethernet, která využívá standard collision-based, samozřejmě pomáhá zabránit zhoršení vlastností služeb poskytovaných ostatním uživatelům sítě LAN.

## Související informace pro nastavení TCP/IP

Zde jsou uvedeny příručky produktů a červené knihy IBM (ve formátu PDF), webové stránky a témata aplikace Information Center, která se vztahují k tématu nastavení TCP/IP. Libovolný z těchto souborů PDF můžete zobrazit nebo vytisknout.

## Červené knihy IBM

- TCP/IP Tutorial and Technical Overview  (7 MB) Tato červená kniha IBM poskytuje základní informace o TCP/IP.
- TCP/IP for AS/400: More Cool Things Than Ever  (9 MB) Tato červená kniha IBM obsahuje rozsáhlý seznam běžných aplikací a služeb TCP/IP.

## Webové stránky

- IETF (Internet Engineering Task Force)  (www.ietf.cnri.reston.va.us)
  Zde se seznámíte se skupinou osob, které vyvíjejí protokol IP (včetně IPv6).
- IPv6 (IP Version 6)  (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  Zde najdete aktuální specifikace IPv6 a odkazy na různé zdroje informací o IPv6.
- IPv6 Forum  (www.ipv6forum.com)
  Zde najdete nové články a akce poskytující informace o nejnovějším vývoji IPv6.

## Další informace

- TCP/IP: Toto téma obsahuje informace o aplikacích a službách TCP/IP, které přesahují rozsah konfigurace.
- Odstraňování problémů s TCP/IP: Informace v tomto tématu vám pomohou při řešení problémů týkajících se připojení TCP/IP a provozu TCP/IP pro IPv4 i IPv6.
- Plánování a nastavení zabezpečení systému: Toto téma obsahuje informace o plánování a nastavení zabezpečení pro server iSeries.

## Uložení souborů PDF

Chcete-li soubor PDF uložit na svou pracovní stanici, abyste ho později mohli prohlížet a vytisknout, postupujte takto:

1. V prohlížeči klepněte pravým tlačítkem myši na odkaz na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na volbu, která ukládá soubor PDF lokálně.
3. Přejděte do adresáře, do kterého chcete soubor PDF uložit.
4. Klepněte na **Uložit**.

## Stažení aplikace Adobe Reader

Zobrazení a tisk těchto souborů PDF vyžadují, aby byla v počítači nainstalována aplikace Adobe Reader. Kopii této aplikace můžete zdarma stáhnout z webové stránky společnosti Adobe (www.adobe.com/products/acrobat/readstep.html)  .

# Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí nabízet produkty, služby nebo funkce popsané v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba IBM. Použít lze jakýkoliv funkčně ekvivalentní produkt, program či službu neporušující práva IBM na duševní vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Vlastnictví tohoto dokumentu vám nedává k těmto patentům žádná práva. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve vaší zemi, nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

**Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům:** SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, " JAKÁ JE" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

Licencovaný program popsaný v těchto informacích a veškeré licencované materiály, které jsou pro něj k dispozici, poskytuje IBM na základě podmínek smlouvy IBM Customer Agreement, Mezinárodní licenční smlouvy IBM na programy, smlouvy IBM License Agreement for Machine Code nebo jiné ekvivalentní smlouvy s IBM.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a v těchto případech nelze zaručit, že tato měření budou stejná ve všeobecně dostupných systémech. Kromě toho mohla být některá měření odhadnuta na základě extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Informace týkající se produktů jiných firem než IBM byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM netestovala tyto produkty a nemůže potvrdit přesnost údajů týkajících se výkonu, kompatibility nebo přesnost jiných prohlášení vztahujících se k produktům od jiných dodavatelů. Dotazy, které se týkají vlastností produktů jiných firem než IBM, musí být adresovány jejich dodavatelům.

Veškerá prohlášení týkající budoucích trendů nebo strategií IBM podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Tyto informace obsahují příklady dat a sestav používaných v každodenních operacích. Za účelem co nejpřesnější ilustrace obsahují tyto příklady jména osob, společností, značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami používanými ve skutečných obchodních firmách je čistě náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Každá kopie nebo část těchto vzorových programů nebo jakákoliv odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno vaší společnosti) (rok). Části tohoto kódu jsou odvozeny ze vzorových programů IBM. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

## Informace o programovacím rozhraní

Tato publikace Nastavení TCP/IP je určena pro programovací rozhraní, které umožňuje zákazníkům psát programy za účelem získání služeb operačního systému IBM i5/OS.

## Ochranné známky

Následující výrazy jsou ochrannými známkami IBM ve Spojených státech a případně v dalších jiných zemích.

| AIX
| AS/400
| eServer
| i5/OS
| IBM
| IBM (logo)
| iSeries
| Redbooks

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

| Linux je ochranná známka, jejímž majitelem je Linus Torvalds, ve Spojených státech a případně v dalších jiných
| zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

## Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

**Osobní použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

**Komerční použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.

Vytištěno v  Dánsku společností IBM Danmark A/S.