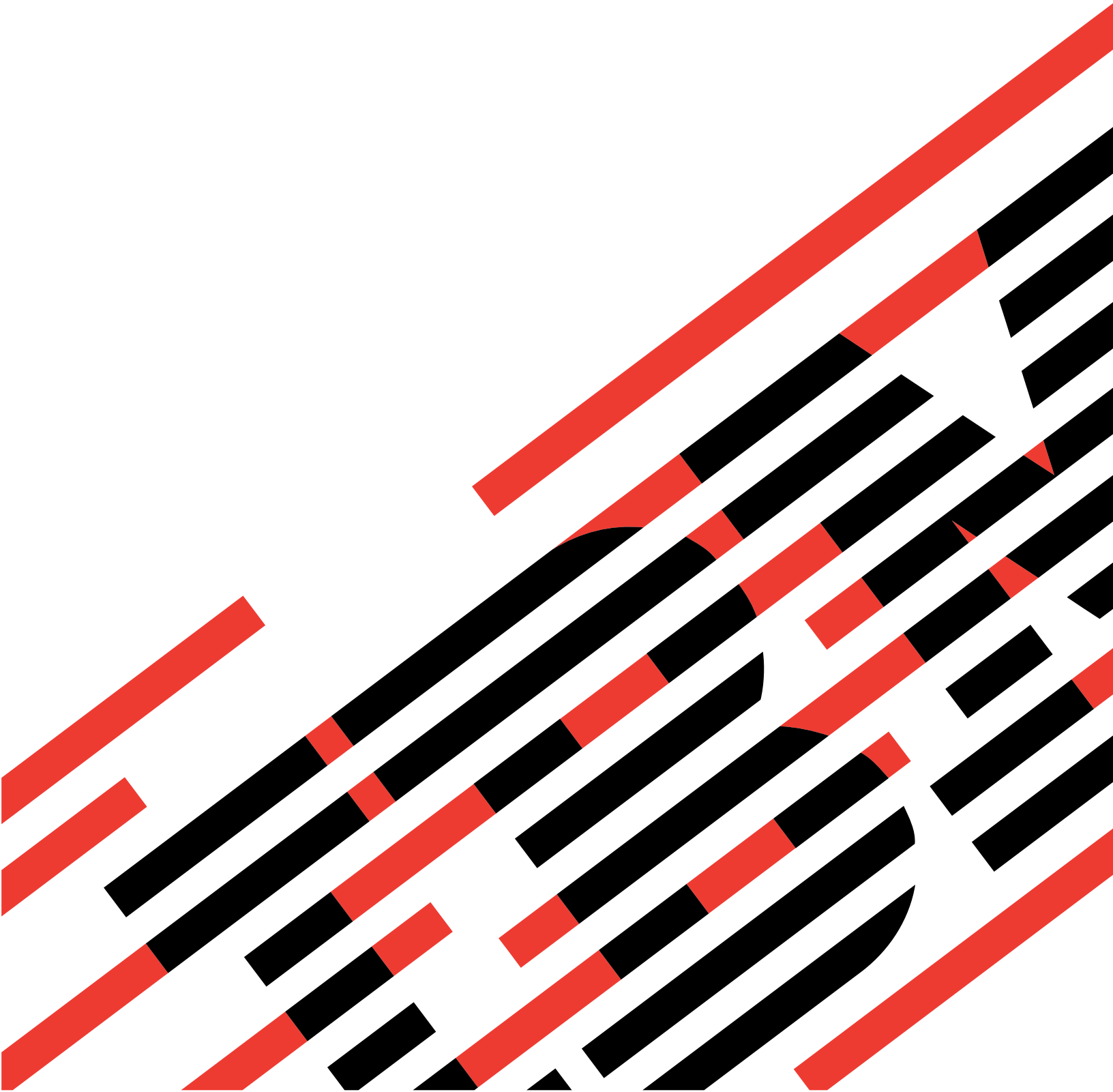
IBM

eserver

iSeries

Síťové technologie - Nastavení TCP/IP

verze 5, vydání 3



IBM

@server

iSeries

Síťové technologie - Nastavení TCP/IP

verze 5, vydání 3

Poznámka

Před použitím těchto informací a odpovídajícího produktu si přečtěte informace v části "Upozornění", na stránce 57.

Sedmé vydání (srpen)

Toto vydání se týká verze 5, vydání 3, modifikace 0 licencovaného programu Operating System/400 (5722–SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CICS.

Obsah

Část 1. Nastavení TCP/IP

Právě jste obdrželi váš server a jste připraveni začít jej používat. Toto téma popisuje nástroje a procedury konfigurace TCP/IP v operačním systému OS/400. Například můžete použít tyto informace k vytvoření popisu linky, TCP/IP rozhraní nebo přenosové cesty. Dozvíte se, jak přizpůsobit vaši konfiguraci TCP/IP s použitím produktu iSeries Navigator a poučíte se o různých technikách TCP/IP, které vám umožní směrovat data přenášená do vaší sítě a z vaší sítě.

Dříve než použijete tyto informace k nakonfigurování 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 vašeho serveru pomocí aplikací, protokolů a služeb TCP/IP tak, aby vyhovovaly vašim jedinečným potřebám.

Co je nového ve verzi V5R3
V této kapitole najdete informace o novinkách a změnách v TCP/IP.

Tisk tohoto tématu
Toto téma slouží k vytisknutí nebo stažení publikace Nastavení TCP/IP ve formátu PDF (Portable Document Format).

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

Plánování nastavení TCP/IP
Toto téma využijete při přípravě na instalaci a konfiguraci TCP/IP na serveru iSeries. Jsou zde uvedeny základní požadavky týkající se instalace a konfigurace. To znamená, že budete mít k dispozici veškeré informace, které potřebujete k tomu, abyste mohli začít s konfigurováním TCP/IP. Dále jsou zde uvedeny odkazy na související termíny a principy.

Instalace TCP/IP
Toto téma vás provede instalací produktů, jež připraví váš server iSeries na provoz.

Konfigurace TCP/IP
Toto téma uvádí postup, jak uvést server iSeries do provozu a jak nakonfigurovat TCP/IP. Kromě toho obsahuje pokyny ke konfiguraci protokolu IPv6.

Přizpůsobení TCP/IP pomocí produktu iSeries Navigator
Toto téma uvádí možnosti přizpůsobení TCP/IP pomocí produktu iSeries Navigator.

TCP/IP metody propojení přes virtuální sítě Ethernet
Dozvíte se, jak využít virtuální síť typu Ethernet v operačním systému OS/400.

Odstraňování problémů s TCP/IP
Setkáte-li se s jakýmikoliv problémy se spojením nebo provozem TCP/IP, možná řešení najdete v tématu Odstraňování problémů s TCP/IP. V této příručce najdete pomoc s řešením problémů souvisejících s protokoly IPv4 a IPv6.

Související informace k nastavení TCP/IP
Toto téma vám zodpoví otázku ″Co dalšího bych ještě mohl udělat?″ Můžete zde vyhledat odkazy na služby a aplikace, které zvýší výkon vašeho serveru.

Kapitola 1. Co je nového ve verzi V5R3

Vylepšení nastavení TCP/IP

Pokud používáte virtuální síť typu Ethernet k tomu, aby jednotlivé logické části mezi sebou komunikovaly, budete možná potřebovat rozšířit tuto komunikaci do externí fyzické sítě LAN. Více informací o připojení virtuální sítě Ethernet k externí síti LAN najdete v tématu TCP/IP metody připojení virtuální sítě Ethernet k externím sítím LAN. S pomocí těchto informací si můžete prostudovat příklady popisující tři rozdílné metody přemostění vašeho síťového provozu z virtuální sítě Ethernet do externí sítě LAN.

Další informace o novinkách a změnách v této verzi najdete v dokumentu Sdělení pro uživatele.

Jak zjistit, co je nového a co se změnilo

Za účelem snadnější identifikace míst, kde byly provedeny technické změny, jsou tyto informace označeny symbolem.

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

Kapitola 2. Tisk tohoto tématu

Chcete-li si prohlédnout nebo stáhnout verzi ve formátu PDF, vyberte odkaz Nastavení TCP/IP (zhruba 362 KB).

Jiné informace

Můžete si také prohlédnout nebo vytisknout jakýkoliv z těchto souborů PDF:

- Uživatelské příručky:
  - **TCP/IP Configuration and Reference** (zhruba 592 KB)
    Tato publikace nabízí informace o konfigurování TCP/IP (Transmission Control Protocol/Internet Protocol) a o provozu a správě sítě.
  - **Rady a nástroje pro zabezpečení serveru iSeries** (asi 1 MB)
    Tato publikace obsahuje základní doporučení k používání funkcí zabezpečení dat serveru iSeries k ochraně serveru a k provádění souvisejících činností.
- Červené knihy:
  - **TCP/IP Tutorial and Technical Overview** (zhruba 7 MB)
    Tato červená kniha obsahuje informace o základech TCP/IP.
  - **TCP/IP for AS/400: More Cool Things Than Ever** (zhruba 9 MB)
    Tato červená kniha obsahuje rozsáhlý seznam běžných aplikací a služeb TCP/IP.

Ukládání souborů PDF

K uložení PDF souboru na svou pracovní stanici za účelem prohlížení a tisku použijte tento postup:

1. Klepněte pravým tlačítkem myši v prohlížeči na odkaz na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Pokud používáte Internet Explorer, klepněte na **Save Target As... (Uložit cíl jako...)**. pokud používáte Netscape Communicator, klepněte na **Save Link As... (Uložit cíl jako...)**.
3. Vyhledejte adresář, do kterého chcete PDF soubor uložit.
4. Klepněte na **Save** (Uložit).

Stažení aplikace Adobe Acrobat Reader

K tomu, abyste si mohli prohlédnout či vytisknout tyto soubory typu PDF potřebujete Adobe Acrobat Reader. Kopii této aplikace si můžete stáhnout na webové stránce společnosti Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Kapitola 3. Protokol IP (Internet Protocol) verze 6 (IPv6)

Protokol IPv6 je aktualizovanou verzí protokolu IP (Internet Protocol) verze 4 (IPv4) a bude postupně nahrazovat protokol IPv4 jako standard sítě Internet.

Možná přemýšlíte, jak pomocí protokolu IPv6 zdokonalit elektronické podnikání své firmy. Možná jste programátor a chcete vytvářet aplikace založené na protokolu IPv6, aby vaše firma mohla využívat výhod tohoto zdokonaleného protokolu Internetu. Chcete-li získat základní informace o protokolu IPv6 a o způsobech jeho používání na serveru iSeries, přečtěte si tato témata:

Co je protokol IPv6?
V této části se dozvíte, proč protokol IPv6 nahradí protokol IPv4 jako standard sítě Internet a jak jej můžete využít ve svůj prospěch.

Jaké funkce protokolu IPv6 jsou k dispozici?
Zde se dozvíte, jak je protokol IPv6 v současné době implementován na serveru iSeries.

Scénáře protokolu IPv6
Tyto příklady vám pomohou porozumět, ve kterých situacích byste mohli ve své firmě využít protokol IPv6.

Koncepce protokolu IPv6
V této části se seznámíte se základními koncepcemi protokolu IPv6. Nevíte-li jistě, jaké jsou mezi protokoly IPv4 a IPv6 rozdíly, můžete si přečíst podrobná porovnání, například porovnání adres IPv4 a IPv6 nebo rozdíly mezi záhlavími paketů IPv4 a paketů IPv6.

Konfigurace protokolu IPv6
Tato část obsahuje hardwarové a softwarové požadavky a pokyny ke konfigurování protokolu IPv6 na serveru.

Odstraňování problémů s protokolem IPv6
Zde najdete řešení problémů s protokolem IPv6.

Související informace k protokolu IPv6
Tato část obsahuje odkazy na zdroje informací, které vám pomohou seznámit se blíže s protokolem IPv6.

Co je protokol IPv6?

Protokol IPv6 je pokračováním vývoje protokolu IP (Internet Protocol). Ve větší části sítě Internet se v současné době používá protokol IPv4. Tento protokol je spolehlivý a odolný po více než 20 let. Protokol IPv4 však má závažná omezení, která budou s rozvojem Internetu způsobovat 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 řeší tento problém tím, že bude k dispozici 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. Konfigurování a údržba sítí je náročná činnost. Protokol IPv6 snižuje pracovní zátěž automatizací některých úkolů správce sítě.

Budete-li používat protokol IPv6, nebudete muset při přechodu k jinému poskytovateli služeb sítě Internet (ISP) přečíslovat adresy zařízení. Stávající adresy můžete zachovat, protože jsou globálně jedinečné.

Funkce automatické konfigurace zajišťuje automatické nakonfigurování adres rozhraní a směrovačů. Při bezestavové automatické konfiguraci vytvoří protokol IPv6 z adresy MAC počítače a z prefixu sítě poskytnutého lokálním uzlem novou jedinečnou adresu IPv6. Tato funkce odstraňuje potřebu serveru DHCP, což šetří čas administrátora a peníze firmy.

Odkazy na další zdroje informací o protokolu IPv6 najdete v části Související informace k protokolu IPv6.

Informace související konkrétně se serverem iSeries najdete v části Jaké funkce protokolu IPv6 jsou k dispozici?.

Jaké funkce protokolu IPv6 jsou k dispozici?

IBM implementuje protokol IPv6 pro server iSeries již v několika vydáních softwaru. Protokol IPv6 je v současné době implementován v platformě pro vývoj aplikací, která slouží k vývoji a testování aplikací IPv6. Funkce protokolu IPv6 jsou pro stávající aplikace TCP/IP transparentní a existují společně s funkcemi IPv4.

Hlavní funkce serveru iSeries ovlivněné IPv6 jsou tyto:

- **Konfigurace**
  Uvědomte si, že proces konfigurace se u protokolu IPv6 liší od procesu konfigurace u IPv4. Chcete-li používat funkce protokolu IPv6, musíte změnit konfiguraci TCP/IP serveru tím, že nakonfigurujete linku pro protokol IPv6. Protokol IPv6 můžete nakonfigurovat na lince Ethernet nebo na tunelové lince.

  Pokud pro provoz protokolu IPv6 nakonfigurujete linku Ethernet, budou pakety IPv6 posílány sítí IPv6. Scénář popisující situaci, kdy byste mohli nakonfigurovat linku Ethernet pro protokol IPv6, najdete v části Vytvoření lokální sítě IPv6 (LAN).

  Pokud nakonfigurujete tunelové linky, budou pakety IPv6 posílány stávající sítí IPv4. Scénáře popisující dvě situace, kdy byste mohli vytvořit konfigurovanou tunelovou linku pro protokol IPv6, najdete v částech Posílání paketů IPv6 lokální sítí IPv4 (LAN) a Posílání paketů IPv6 dálkovou sítí IPv4 (WAN).

  Chcete-li nakonfigurovat síť pro protokol IPv6, přejděte na část Konfigurace protokolu IPv6.
- **Sokety**
  K vývoji a testování aplikací typu soket slouží rozhraní API a nástroje protokolu IPv6. Protokol IPv6 vylepšuje sokety tak, že aplikace mohou používat protokol 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. Další informace o protokolu IPv6 pro sokety najdete v tématu věnovaném používání skupiny adres AF_INET6.
- **DNS**
  DNS (Domain Name System) 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**
  Pro sítě a tunely IPv6 můžete používat standardní nástroje pro odstraňování problémů, například příkazy PING a NETSTAT, trasování přenosové cesty a trasování komunikace. Tyto nástroje nyní podporují formát adres IPv6. Chcete-li řešit problémy se sítěmi IPv4 i IPv6, přejděte na téma Odstraňování problémů s TCP/IP.

Odkazy na zdroje informací o protokolu IPv6 najdete v části Související informace k protokolu IPv6.

Scénáře protokolu IPv6

Chcete-li porozumět, proč implementovat protokol IPv6 a jak nastavit síť v konkrétních situacích, seznamte se s těmito scénáři:

- Vytvoření lokální sítě IPv6 (LAN).
- Posílání paketů IPv6 lokální sítí IPv4 (LAN).
- Posílání paketů IPv6 dálkovou sítí IPv4 (WAN).

Poznámka: V těchto scénářích představují IP adresy 10.x.x.x veřejné IP adresy. Všechny adresy použité v těchto scénářích jsou uvedeny jen jako příklad.

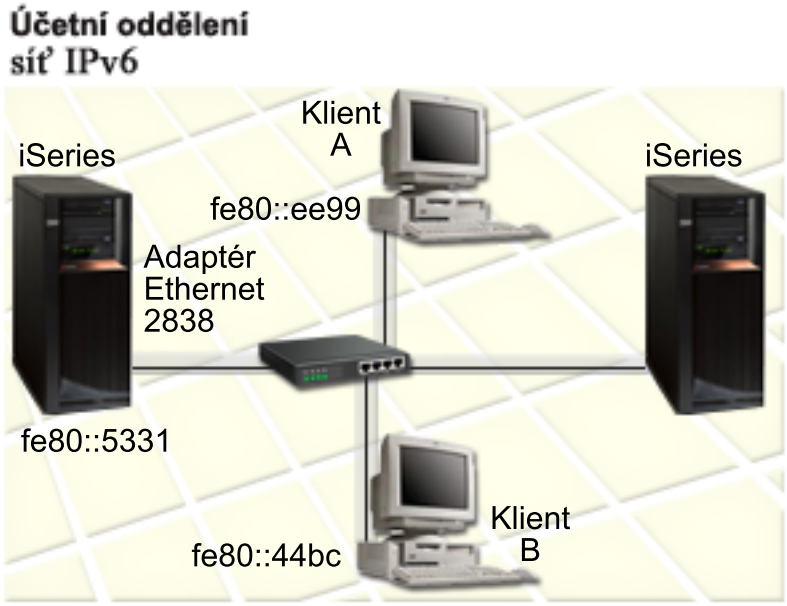
Chcete-li nakonfigurovat server pro protokol IPv6, přejděte na část Konfigurace protokolu IPv6.

Definice základních koncepcí protokolu IPv6 najdete v části Koncepce protokolu IPv6.

Vytvoření lokální sítě IPv6 (LAN)

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 účtovací aplikaci, 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 začít používat účtovací aplikaci. Uspořádání sítě pro tento scénář je znázorněno na následujícím obrázku.



Řešení

Chcete-li vytvořit LAN typu IPv6, musíte pro IPv6 nakonfigurovat popis linky Ethernet. Když zaměstnanci používají účtovací aplikaci, putují pakety IPv6 sítí mezi servery iSeries a počítači typu klient.

Požadavky na konfiguraci zahrnují:

- Operační systém OS/400 (verze 5 vydání 2 nebo novější).

- Adaptéry 2838 nebo 2849 typu Ethernet, které jsou v současné době jedinými typy hardwarových prostředků podporovaných pro IPv6.
- iSeries Access for Windows a iSeries Navigator (síťová komponenta aplikace iSeries Navigator).
- Na serveru musí být spuštěn TCP/IP. Proto musíte před konfigurováním linky Ethernet pro protokol IPv6 na serveru nakonfigurovat samostatné fyzické rozhraní protokolu IPv4. Pokud jste nenakonfigurovali server pro protokol IPv4, přejděte před konfigurováním linky pro protokol IPv6 na část První konfigurace TCP/IP.

Konfigurace

Chcete-li nakonfigurovat popis linky Ethernet pro protokol IPv6, musíte použít průvodce **konfigurací protokolu IPv6** v prostředí produktu iSeries Navigator. Protokol IPv6 je možné nakonfigurovat pouze v prostředí produktu iSeries Navigator - nelze použít znakově orientované rozhraní.

Průvodce požaduje jméno hardwarového komunikačního prostředku na serveru, na kterém chcete IPV6 nakonfigurovat; například CMN01. Musí to být adaptér 2838 nebo 2849 typu Ethernet, který není v současné době nakonfigurován pro IPv4.

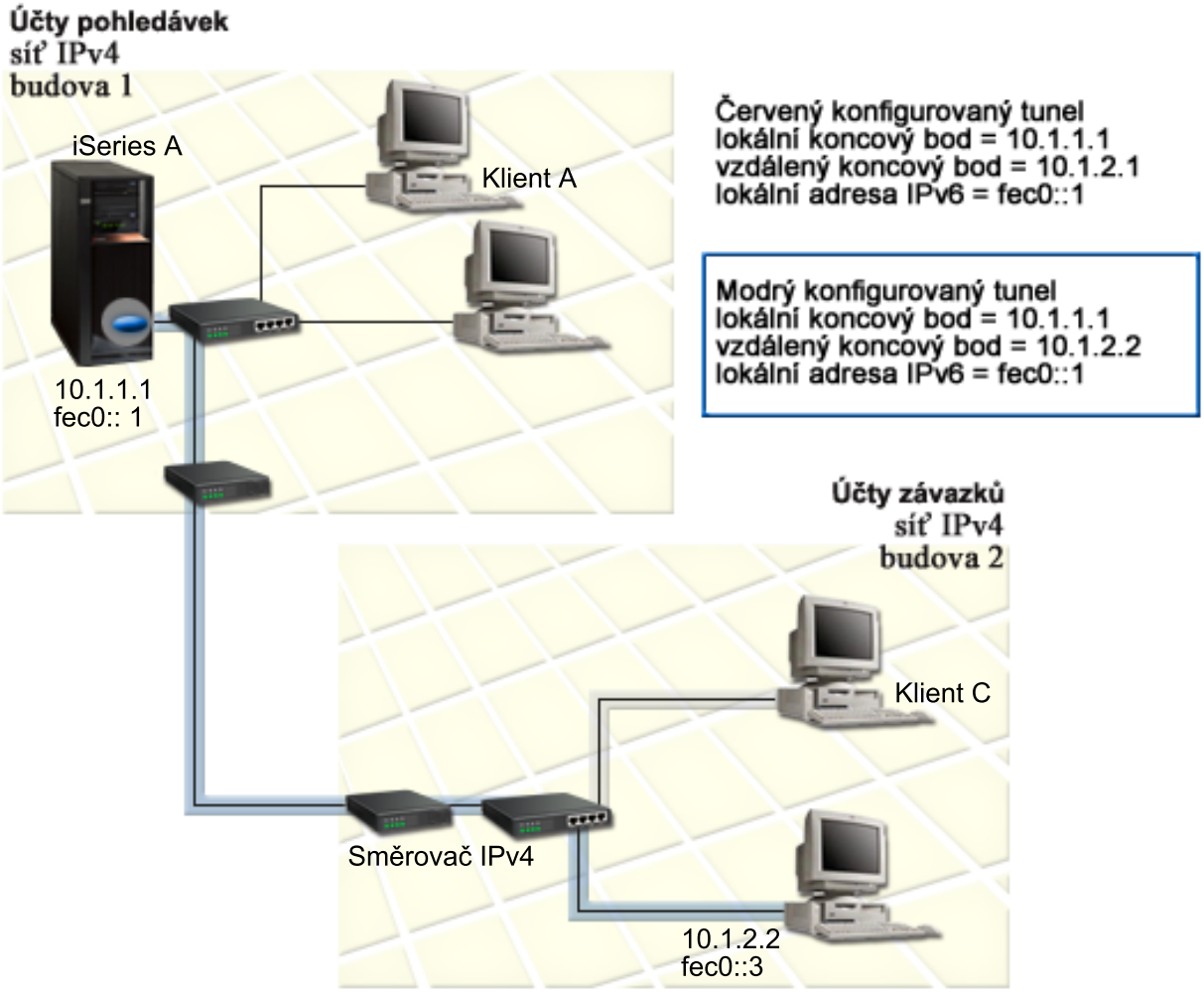
Chcete-li použít průvodce **konfigurací protokolu IPv6**, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť —> Konfigurace TCP/IP**.
2. Klepněte pravým tlačítkem myši na **IPv6**, vyberte **Konfigurace protokolu IPv6** a postupujte podle pokynů průvodce pro konfiguraci linky Ethernet pro IPv6.

Posílání paketů IPv6 lokální sítí IPv4 (LAN)

Situace

Vaše firma vytvořila novou účtovací aplikaci založenou na protokolu IPv6. Je to aplikace typu klient/server, kterou budete používat lokálně. Aplikace komunikuje se svými dalšími instancemi, které jsou umístěny ve stejném uzlu, avšak v jiných budovách a lokálních sítích. Vaše firma sice chce pro tuto aplikaci použít protokol IPv6, nehodlá však změnit celou infrastrukturu IPv4 na IPv6. Vaším úkolem je nakonfigurovat tunelové linky IPv6, které budou přenášet pakety IPv6 lokálními sítěmi IPv4. Uspořádání sítě pro tento scénář je znázorněno na následujícím obrázku.



Řešení

Chcete-li v těchto lokálních sítích IPv4 používat k přenosu protokol IPv6, musíte vytvořit dva konfigurované tunely a několik asociovaných přenosových cest. V tomto příkladu je jeden tunel znázorněn červeně a druhý tunel modře.

Nejdříve se zabývejme červeným tunelem:

- Červený tunel začíná na serveru iSeries A (lokální koncový bod 10.1.1.1) v budově 1 a končí v počítači typu klient C (vzdálený koncový bod 10.1.2.1) v budově 2.
- Server iSeries A zapouzdří paket IPv6 do paketu IPv4 a pošle paket IPv4 tunelem do počítače typu klient C. Ten odstraní obálku paketu IPv6, aby se mohl připojit k jiné instanci aplikace používající protokol IPv6.

Nyní se zabývejme modrým tunelem:

- Modrý tunel začíná podobně jako červený tunel na serveru iSeries A (lokální koncový bod 10.1.1.1) v budově 1. Končí však v počítači typu klient D (vzdálený koncový bod 10.1.2.2) v budově 2.
- Server iSeries A zapouzdří paket IPv6 do paketu IPv4 a pošle paket IPv4 tunelem do počítače typu klient D. Ten odstraní obálku paketu IPv6, aby se mohl připojit k jiné instanci aplikace používající protokol IPv6.

Všechna tunelová spojení jsou dvoubodová, u každého tunelu proto musíte definovat vzdálený koncový bod. Toho lze dosáhnout vytvořením dvou přenosových cest. Obě cesty jsou asociovány se stejnou tunelovou linkou, jako další směrovací uzel je však v každé z nich definován jiný vzdálený koncový bod. Jinak řečeno, při vytvoření přenosových cest definujete vzdálené koncové body pro oba tunely.

Kromě toho, že vytvoříte počáteční přenosové cesty, které definují koncové body tunelů a umožňují paketům dostat se do počítačů typu klient v budově 2, musíte vytvořit další dvě přenosové cesty, aby se pakety mohly vracet do serveru v budově 1.

Požadavky na konfiguraci zahrnují:

- Operační systém OS/400 (verze 5 vydání 2 nebo novější).
- iSeries Access for Windows a iSeries Navigator (síťová komponenta aplikace iSeries Navigator).
- Dříve než vytvoříte konfigurovanou tunelovou linku, musíte na serveru nakonfigurovat TCP/IP (používající IPv4). Pokud jste nenakonfigurovali server pro IPv4, přejděte před konfigurováním tunelové linky pro protokol IPv6 na část První konfigurace TCP/IP.

Konfigurace

Chcete-li nakonfigurovat tunelovou linku, musíte použít průvodce **konfigurací protokolu IPv6** a průvodce **novou přenosovou cestou IPv6** v prostředí produktu iSeries Navigator. Protokol IPv6 je možné nakonfigurovat pouze v prostředí produktu iSeries Navigator - nelze použít znakově orientované rozhraní.

Chcete-li pomocí průvodce **konfigurací protokolu IPv6** vytvořit červenou tunelovou linku, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť —> Konfigurace TCP/IP**.
2. Klepněte pravým tlačítkem myši na **IPv6**, vyberte průvodce **konfigurací protokolu IPv6** a postupujte podle pokynů průvodce pro konfiguraci tunelové linky pro protokol IPv6. Průvodce **konfigurací protokolu IPv6** vás po dokončení vyzve k vytvoření nové přenosové cesty pro konfigurovanou tunelovou linku a objeví se dialog průvodce **novou přenosovou cestou IPv6**. Novou přenosovou cestu musíte vytvořit, aby mohly pakety IPv6 procházet červeným tunelem.
3. Pomocí průvodce **novou přenosovou cestou IPv6** vytvořte přenosovou cestu pro červený tunel. Jako následující směrovací uzel zadejte vzdálený koncový bod 10.1.2.1 a jako cílovou adresu zadejte fec0::2.

Pomocí průvodce **novou přenosovou cestou IPv6** vytvořte přenosovou cestu pro modrý tunel. Všimněte si, že není nezbytné vytvořit modrý tunel pomocí průvodce **konfigurací protokolu IPv6**. Modrý tunel se vytvoří, když pomocí průvodce **novou přenosovou cestou IPv6** definujete jeho vzdálený koncový bod. Při použití průvodce **novou přenosovou cestou IPv6** proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť —> Konfigurace TCP/IP —> IPv6**.
2. Klepněte pravým tlačítkem myši na **Přenosové cesty**, vyberte **Nová přenosová cesta** a podle pokynů průvodce nakonfigurujte přenosovou cestu IPv6 pro modrý tunel. Jako následující směrovací uzel zadejte vzdálený koncový bod 10.1.2.2 a jako cílovou adresu zadejte fec0::3.

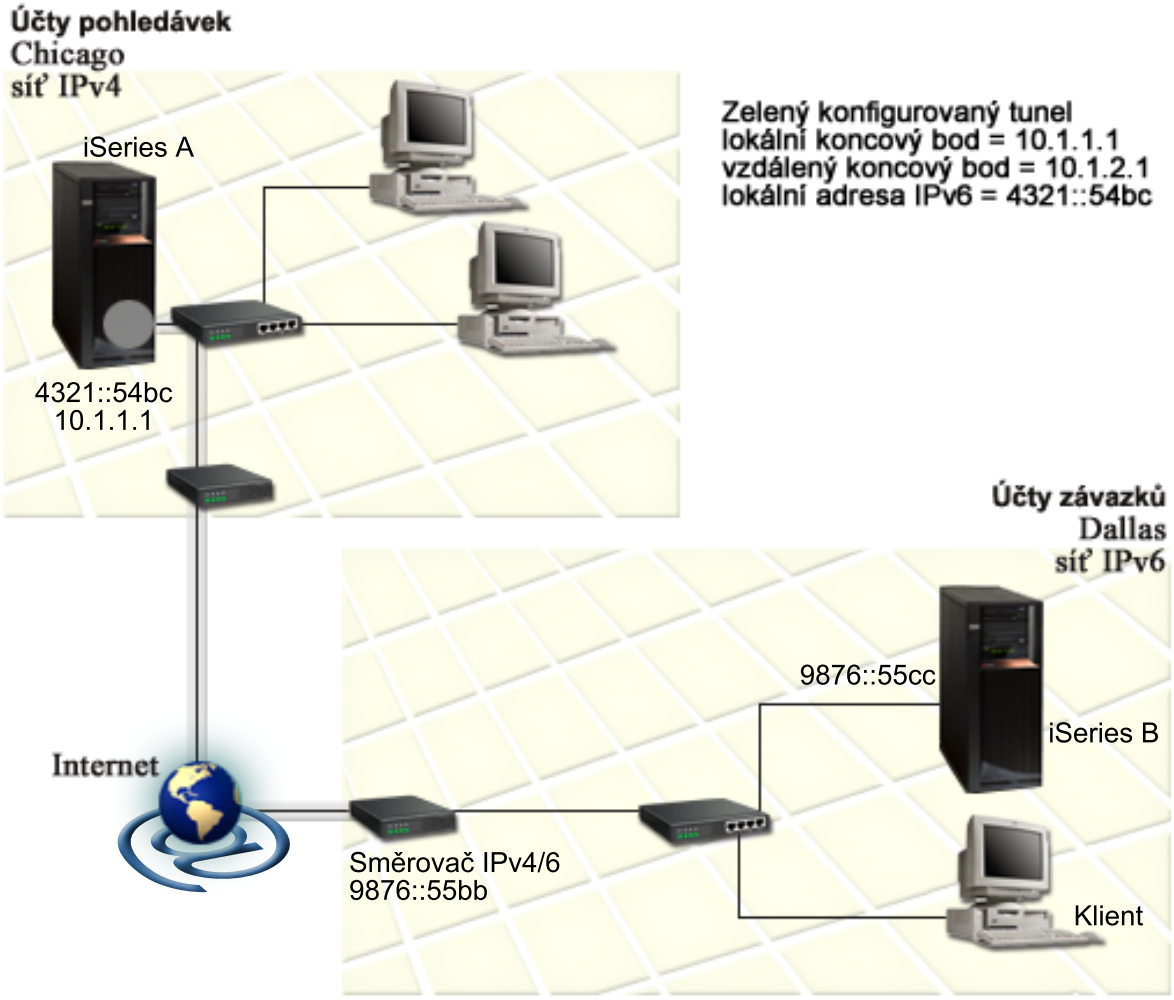
Po vytvoření konfigurovaných tunelových linek a přenosových cest, které definují koncové body tunelů, musíte vytvořit přenosovou cestu pro počítač typu klient C a přenosovou cestu pro počítač typu klient D - tyto cesty budou sloužit ke zpětnému přenosu paketů do serveru v budově 1. U obou těchto cest zadejte jako následující směrovací uzel koncový bod 10.1.1.1 a jako cílovou adresu uveďte fec0::1.

Posílání paketů IPv6 dálkovou sítí IPv4 (WAN)

Situace

Vaše firma používá účtovací aplikaci pro účty pohledávek na serveru ve své pobočce v Chicagu. Potřebujete, aby se aplikace připojovala k serveru v pobočce v Dallasu. Tato aplikace používá na serverech v obou městech adresování IPv6. Protože váš poskytovatel služeb sítě Internet (ISP) nemůže mezi těmito dvěma uzly poskytnout směrovače IPv6, musíte mezi oběma servery nakonfigurovat tunel. Pakety aplikace budou procházet při přenosu mezi vašimi dvěma servery tímto tunelem vedoucím přes dálkovou síť (WAN) typu IPv4. Uspořádání sítě pro tento scénář je znázorněno na následujícím obrázku.

Poznámka: V tomto scénáři představují IP adresy 10.x.x.x veřejné IP adresy, které mohou být globálně směrovány. Všechny použité adresy jsou uvedeny jen jako příklad.



Řešení

Chcete-li používat protokol IPv6 přes dálkovou síť (WAN) tvořenou infrastrukturou IPv4, musíte vytvořit konfigurovanou tunelovou linku a několik asociovaných přenosových cest. Funguje to takto:

- Tunel začíná na serveru iSeries A (lokální koncový bod 10.1.1.1) v Chicagu a končí ve směrovači IPv4/6 (vzdálený koncový bod 10.1.2.1) v Dallasu.
- Aplikace umístěná na serveru iSeries A se potřebuje připojit k aplikaci umístěné na serveru iSeries B. Server iSeries A zapouzdří paket IPv6 do paketu IPv4 a pošle ho tunelem do směrovače IPv4/6. Směrovač odstraní obálku paketu IPv6 a pošle paket IPv6 serveru iSeries B.
- Paket se vrátí do Chicaga opačnou cestou.

Tunelové spojení je dvoubodové, u tunelu proto musíte definovat vzdálený koncový bod. Dosáhnete toho vytvořením přenosové cesty, která je asociována s touto tunelovou linkou. Přenosová cesta definuje jako následující směrovací uzel vzdálený koncový bod (10.1.2.1). Jinak řečeno, vzdálený koncový bod definujete při vytvoření přenosové cesty. Přenosová cesta kromě toho definuje cílovou adresu jako 9876::55cc (adresu IPv6 asociovanou se serverem iSeries B).

Kromě toho, že vytvoříte výchozí přenosovou cestu, která definuje koncový bod tunelu a umožňuje průchod paketů do serveru iSeries B v Dallasu, musíte vytvořit dvě další přenosové cesty, aby se pakety mohly vracet do serveru iSeries A v Chicagu.

Požadavky na konfiguraci zahrnují:

- Operační systém OS/400 (verze 5 vydání 2 nebo novější).
- iSeries Access for Windows a iSeries Navigator (síťová komponenta aplikace iSeries Navigator).
- Dříve než vytvoříte konfigurovanou tunelovou linku, musíte na serveru nakonfigurovat TCP/IP (používající IPv4). Pokud jste nenakonfigurovali server pro IPv4, přejděte před konfigurováním tunelové linky pro IPv6 na část První konfigurace TCP/IP.

Konfigurace

Chcete-li nakonfigurovat tunelovou linku, musíte použít průvodce **konfigurací protokolu IPv6** a průvodce **novou přenosovou cestou IPv6** v prostředí produktu iSeries Navigator. Konfigurované tunely je možné nakonfigurovat pouze v prostředí produktu iSeries Navigator - nelze použít znakově orientované rozhraní.

Chcete-li pomocí průvodce **konfigurací protokolu IPv6** vytvořit tunelovou linku, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť —> Konfigurace TCP/IP**.
2. Klepněte pravým tlačítkem myši na **IPv6**, vyberte **Konfigurace protokolu IPv6** a postupujte podle pokynů průvodce pro konfiguraci tunelové linky pro protokol IPv6. Průvodce **konfigurací protokolu IPv6** vás po dokončení vyzve k vytvoření nové přenosové cesty pro konfigurovanou tunelovou linku a objeví se dialog průvodce **novou přenosovou cestou IPv6**. Novou přenosovou cestu musíte vytvořit, aby mohly pakety IPv6 procházet tunelem.
3. Pomocí průvodce **novou přenosovou cestou IPv6** vytvořte hostitelskou přenosovou cestu pro tunel. Jako následující směrovací uzel zadejte vzdálený koncový bod 10.1.2.1 a jako cílovou adresu zadejte 9876::55cc.

Po vytvoření konfigurované tunelové linky a přenosové cesty definující koncový bod tunelu musíte na serveru iSeries B a směrovači IPv4/6 vytvořit přenosové cesty, které umožní přenos paketů zpět do Chicaga. U přenosové cesty na serveru iSeries B zadejte jako následující směrovací uzel 9876::55bb a jako cílovou adresu uveďte 4321::54bc. U přenosové cesty ve směrovači IPv4/6 zadejte jako následující směrovací uzel 10.1.1.1 a jako cílovou adresu uveďte 4321::54bc.

Poznámka: Směrovač IPv4/6 v Dallasu vyžaduje přímou přenosovou cestu do 9876::55cc, protože však je tato přenosová cesta vytvořena automaticky, není ruční konfigurování nutné.

Koncepce protokolu IPv6

Chcete-li lépe rozumět, jak protokol IPv6 funguje, přečtěte si popisy koncepcí protokolu IPv6:

Porovnání protokolu IPv4 s protokolem IPv6
V této části najdete porovnání atributů IPv4 s atributy IPv6. Tato tabulka umožňuje rychlé vyhledávání určitých funkcí a porovnávání jejich použití v obou protokolech Internetu.

Formáty adres IPv6
V této části zjistíte velikost a formát adresy IPv6.

Typy adres IPv6
V této části se seznámíte s novými typy adres v oblasti IPv6.

Tunelování IPv6
Zde zjistíte, jak tunelování IPv6 umožňuje průchod sítí IPv4.

Zjišťování sousedních uzlů
Zde se dozvíte, jak zjišťování sousedních uzlů umožňuje vzájemnou komunikaci hostitelských systémů a směrovačů.

Bezestavová automatická konfigurace adres
Zde zjistíte, jak bezestavová automatická konfigurace adres umožňuje automatizaci některých úkolů správce sítě.

Formáty adres IPv6

Velikost adresy IPv6 je 128 bitů. Preferovaná reprezentace adresy IPv6 je: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, kde každé x označuje hexadecimální číslici představující 4 bity. 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:

- **Vynechané úvodní nuly**
  V adresách IPv6 lze vynechat úvodní nuly. Například adresu IPv6 1050:0000:0000:0000:0005:0600:300c:326b je možné zapsat takto: 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 je možné zapsat takto: ff06::c3. Dvě dvojtečky je možné v IP adrese použít jen jednou.

Alternativní formát adres IPv6 kombinuje zápisy s dvojtečkami a tečkami, takže adresa IPv4 může být vložena v adrese 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.

Tento alternativní formát se používá v následujících dvou typech adres IPv6:

- **Adresa IPv6 mapovaná na adresu IPv4**
  Tento typ adresy se používá k reprezentaci uzlů IPv4 jako adres IPv6. Umožňuje aplikacím založeným na protokolu IPv6 přímo komunikovat s aplikacemi používajícími IPv4. Příkladem může být adresa 0:0:0:0:0:ffff:192.1.56.10 a její zkrácený formát ::ffff:192.1.56.10/96.
- **Adresa IPv6 kompatibilní s adresou IPv4**
  Tento typ adresy se používá při tunelování. Umožňuje uzlům IPv6 komunikovat přes infrastrukturu IPv4. Příkladem může být adresa 0:0:0:0:0:0:192.1.56.10 a její zkrácený formát ::192.1.56.10/96.

Všechny tyto formáty jsou platnými formáty adresy IPv6. V prostředí produktu iSeries Navigator můžete uvést kterýkoliv z těchto formátů adres IPv6.

Typy adres IPv6

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.

Existují tři typy adres unicast:

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 prefix fe80::/10. Pakety s cílovou nebo zdrojovou adresou obsahující adresu typu link-local nepředávají směrovače dál.

Adresa typu site-local
Adresy typu site-local jsou určeny pro použití v konkrétním uzlu. U adresy typu site-local se používá prefix fec0::/10. Pakety s cílovou adresou obsahující adresu typu site-local nepředávají směrovače ven z konkrétního uzlu.

Globální adresa
Globální adresy jsou určeny pro použití v libovolné síti. Prefix používaný v globální adrese začíná binární hodnotou 001.

Existují tři speciální typy adres unicast:

Neuvedená adresa
Neuvedená adresa je 0:0:0:0:0:0:0:0 nebo může být zkrácena na dvě dvojtečky (::). Neuvedená adresa indikuje neexistenci adresy. Nesmí být přidělena hostitelskému systému. Používat ji může hostitelský systém IPv6, který dosud nemá přidělenu adresu. Jestliže například hostitelský systém odešle paket, aby zjistil adresu z jiného uzlu, použije jako svou zdrojovou adresu neuvedenou adresu.

Adresa typu loopback
Adresa typu loopback je 0:0:0:0:0:0:0:1 nebo může být zkrácena na tvar ::1. Uzel používá adresu typu loopback k tomu, aby poslal paket sám sobě.

Adresa anycast
Adresa anycast určuje skupinu rozhraní, která mohou být v různých místech a sdílejí jedinou 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 prefix ff. Jestliže je na adresu multicast poslán paket, bude kopie paketu doručena každému členovi skupiny. Server iSeries v současné době poskytuje základní podporu adresování multicast. Vytváření rozhraní multicast a aplikace nejsou v současné době podporovány.

Tunelování IPv6

Tunelování IPv6 umožňuje serveru iSeries připojovat se k uzlům IPv6 (hostitelským systémům a směrovačům) přes domény IPv4. Tunelování umožňuje, aby izolované uzly nebo sítě IPv6 spolu komunikovaly a nebylo kvůli tomu nutné měnit vlastní infrastrukturu IPv4. Tunelování umožňuje spolupráci protokolů IPv4 a IPv6, a poskytuje proto přechodný způsob implementace IPv6 při zachování připojitelnosti IPv4.

Tunel je tvořen dvěma dvouprotokolovými uzly (IPv4 a IPv6) v síti IPv4. Tyto dvouprotokolové uzly dokážou zpracovávat komunikaci IPv4 i IPv6. Jeden z krajních dvouprotokolových uzlů infrastruktury IPv6 vloží před každý přijatý paket IPv6 záhlaví IPv4 (zapouzdří jej) a odešle ho stávajícími linkami, jako by to byl normální provoz IPv4. Směrovače IPv4 pokračují ve směrování tohoto provozu. Jiný dvouprotokolový uzel na druhém konci tunelu odstraní z paketu IPv6 přidané záhlaví IPv4 (odpouzdří jej) a směruje ho na místo určení pomocí standardního protokolu IPv6.

Tunelování IPv6 probíhá u serveru iSeries přes konfigurované tunelové linky, což jsou virtuální linky. Konfigurované tunelové linky umožňují komunikaci protokolem IPv6 pro libovolný uzel se směrovatelnou adresou IPv4, který podporuje tunely IPv6. Tyto uzly mohou existovat kdekoli, tedy v lokální doméně IPv4 nebo ve vzdálené doméně.

Konfigurované tunelové spoje jsou dvoubodové. Chcete-li nakonfigurovat tento typ tunelové linky, musíte zadat lokální koncový bod tunelu (adresu IPv4), například 124.10.10.150, a lokální adresu IPv6, například 1080:0:0:0:8:800:200c:417a. Musíte také vytvořit přenosovou cestu IPv6, a umožnit tak průchod paketů tunelem. Při vytvoření přenosové cesty budete definovat jeden z koncových bodů tunelu (adresu IPv4) jako následující směrovací uzel přenosové cesty. Nakonfigurovat můžete neomezený počet koncových bodů pro neomezený počet tunelů.

Scénáře a obrázky demonstrující tunelování IPv6 najdete v částech Posílání paketů IPv6 lokální sítí IPv4 (LAN) a Posílání paketů IPv6 dálkovou sítí IPv4 (WAN).

Zjišťování sousedních uzlů

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 používají hostitelské systémy k automatickému vytvoření rozhraní typu site-local, globálních rozhraní a asociovaných 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 si přečíst dokument RFC 2461, použijte k jeho vyhledání webovou stránku editoru RFC (http://www.rfc-editor.org/rfcsearch.html) .

Bezestavová automatická konfigurace adres

Bezestavová automatická konfigurace adres je postup, který používají uzly IPv6 (hostitelské systémy nebo směrovače) k automatickému nakonfigurování adres IPv6 pro rozhraní. Uzel vytváří různé adresy IPv6 tak, že spojuje prefix adresy s adresou MAC nebo s identifikátorem rozhraní zadaným uživatelem. Prefixy zahrnují prefix typu link-local (fe80::/10) a prefixy v délce 64 oznámené lokálními směrovači IPv6 (pokud nějaké existují). Pokud je typ spoje schopen podporovat výběrové vysílání (multicast), bezestavová automatická konfigurace adres také vytvoří odpovídající rozhraní multicast.

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

IBM implementuje protokol IPv6 pro server iSeries již v několika vydáních softwaru. Protokol IPv6 je v současné době implementován na platformě pro vývoj aplikací, která slouží k vývoji a testování aplikací IPv6.

Pravděpodobně vás zajímá, čím se protokol IPv6 liší od protokolu IPv4. V následující tabulce můžete rychle projít známé atributy vztahující se k protokolu IPv4 a porovnat je s podobnými atributy protokolu IPv6. Výběrem atributu v následujícím seznamu se dostanete k porovnání odpovídajících atributů v tabulce.

• “adresa” na stránce 19

	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. Textová forma adresy IPv4 je nnn.nnn.nnn.nnn, kde 0<=nnn<=255 a každé n označuje dekadickou číslici. Úvodní nuly je možné 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. Hostitelskou částí adresy IPv6 (nebo její části) často bývá adresa MAC nebo jiný identifikátor rozhraní. Adresa IPv6 má v závislosti na prefixu podsítě složitější architekturu než adresa IPv4. Počet adres IPv6 je 10^{28} (79 228 162 514 264 337 593 543 950 336) krát větší než počet adres IPv4.Textová forma adresy IPv6 je xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx , kde každé x představuje hexadecimální číslici představující 4 bity. Úvodní nuly je možné vynechat. V textové formě adresy lze jednou použít dvě dvojtečky (::), a označit tak libovolný počet bitů 0. Například adresa ::ffff:10.120.78.40 je adresa IPv6 mapovaná na adresu IPv4. (Podrobnosti najdete v dokumentu RFC 2373. Chcete-li si přečíst dokument RFC 2373, použijte k jeho vyhledání webovou stránku editoru RFC (http://www.rfc-editor.org/rfcsearch.html).
přidělování adres	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 prefixu 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 prefixu podsítě /48.
doba trvání adresy	Toto není obecně použitelný pojem, platí pouze u adres přidělených pomocí DHCP.	Adresy IPv6 mají dvě doby trvání: preferovanou a platnou, přičemž vždy preferovaná doba trvání <= platná doba trvání. Po uplynutí preferované doby trvání nemůže být adresa použita jako zdrojová IP adresa. Po uplynutí platné doby trvání není adresa uznávána jako platná cílová IP adresa příchozích paketů. Některé adresy IPv6 mají z definice nekonečné preferované a platné doby trvání; například adresy typu link-local (viz “rozsah adresy”).
maska adresy	Používá se k určení sítě z hostitelské části.	Nepoužívá se (viz “prefix adresy”).
prefix adresy	Někdy se používá k určení sítě z hostitelské části. V prezentační formě adresy se někdy zapisuje jako přípona (suffix) /nn.	Používá se v adrese k určení prefixu podsítě. Zapisuje se jako přípona (suffix) /nnn (až 3 dekadické číslice, 0 <= nnn <= 128) za tiskovou formou. Příkladem může být adresa fe80::982:2a5c/10, kde prvních 10 bitů tvoří prefix podsítě.
ARP (Address Resolution Protocol)	Protokol ARP je používán protokolem IPv4 k vyhledání fyzické adresy (například adresy MAC nebo adresy linky) asociované s adresou IPv4.	IPv6 vkládá tyto funkce do samotného 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 adresy	Tento pojem se netýká adres unicast. Existují určené rozsahy soukromých adres a zkratovací smyčka (loopback). Adresy mimo tento rozsah jsou považovány za globální.	U IPv6 je rozsah adresy součástí architektury. Adresy unicast mají 3 definované rozsahy, včetně adres typu link-local, site-local a globálních adres. Adresy unicast mají 14 rozsahů. Rozsah je brán v úvahu při výběru předvolených zdrojových i cílových adres. Zóna rozsahu je instancí rozsahu v konkrétní síti. V důsledku toho musejí být adresy IPv6 někdy zadávány nebo asociovány s ID zóny. Syntaxe je %zid, kde zid je číslo (obvykle malé) nebo jméno. ID zóny se píše za adresou a před prefixem. Například 2ba::1:2:14e:9a9b:c%3/48.
typ adresy	Unicast, multicast nebo broadcast.	Unicast, multicast nebo anycast. Popis najdete v části Typy adres IPv6.
trasování komunikace	Nástroj určený ke shromažďování podrobných informací z trasování paketů TCP/IP (i jiných), které přicházejí na server iSeries a odcházejí z něj.	Totéž pro IPv6; podporovány jsou pakety IPv6 včetně paketů ICMPv6 a IPv6 procházejících tunelem v IPv4.
konfigurace	Dříve než může nově instalovaný systém komunikovat, musí být provedena konfigurace - musí být přiděleny IP adresy a přenosové cesty.	Konfigurace je volitelná v závislosti na požadovaných funkcích. V prostředí produktu iSeries Navigator musí být jako rozhraní IPv6 určeno odpovídající rozhraní typu Ethernet nebo tunelové rozhraní. Jakmile je to provedeno, probíhá konfigurace rozhraní IPv6 automaticky. Systém tedy dokáže komunikovat s jinými lokálními a vzdálenými systémy; v závislosti na typu sítě a na tom, zda existuje směrovač IPv6.

	IPv4	IPv6
DNS (Domain Name System)	Aplikace přijímají hostitelská jména a potom pomocí DNS získávají IP adresy - pomocí funkce rozhraní API soketů gethostbyname(). Aplikace také přijímají IP adresy a potom používají DNS k získání hostitelských jmen pomocí funkce gethostbyaddr() . U IPv4 je doménou pro zpětná vyhledávání 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. Funkce gethostbyname() rozhraní API soketů se pro IPv6 nemění. Funkce getaddrinfo() rozhraní API může být používána (podle rozhodnutí aplikace) pouze k získávání adres IPv6 nebo k získávání adres IPv4 i IPv6. U IPv6 je doménou používanou k zpětnému vyhledávání čtveřic ip6.arpa. Není-li tato doména nalezena, je použita doména ip6.int (informace najdete v popisu funkce rozhraní API getnameinfo()).
DHCP (Dynamic Host Configuration Protocol)	Tento protokol se používá k dynamickému získávání IP adres a jiných informací o konfiguraci.	DHCP v současné době nepodporuje IPv6.
FTP (File Transfer Protocol)	Tento protokol umožňuje přenášet (odesílat a přijímat) soubory v sítích.	FTP v současné době nepodporuje IPv6.
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. Rozšířené záhlaví fragmentace není v současné době podporováno.
hostitelská tabulka	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 rozpoznávání domén IPv6 nakonfigurovat záznam AAAA v DNS. DNS může probíhat 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. 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. Rozhraní mohou být spouštěna a ukončována nezávisle na sobě a nezávisle na TCP/IP pouze v prostředí produktu iSeries Navigator.
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. 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.
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 doprovázet různé 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. IPv6 v současné době nepodporuje žádná rozšířená záhlaví.
bajt protokolu záhlaví IP	Kód protokolu transportní vrstvy nebo přenosu 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 všechny funkce pro konfiguraci TCP/IP.	Produkt iSeries Navigator dovoluje úplnou volitelnou konfiguraci protokolu IPv6, včetně použití průvodce **konfigurací protokolu IPv6**.

	IPv4	IPv6
připojení k lokální síti (LAN)	Je používáno rozhraním IP k přístupu do fyzické sítě. Existuje mnoho typů; například Token-ring, Ethernet nebo PPP (dvoubodové). Někdy se používají označení jako: fyzické rozhraní, propojení, spoj, spojení nebo linka.	U IPv6 se používá stejný princip. V současné době jsou podporovány pouze karty typu Ethernet 2838 a 2849 a tunelové linky.
L2TP (Layer 2 Tunnel Protocol)	L2TP můžeme považovat za virtuální PPP (dvoubodový spoj), který funguje u všech podporovaných typů linek.	L2TP v současné době nepodporuje IPv6.
adresa typu loopback	Rozhraní s adresou 127.*.*.* (obvykle 127.0.0.1), které může uzel používat pouze k tomu, aby posílal pakety sám sobě. Fyzické rozhraní (popis linky) má jméno *LOOPBACK.	Princip je stejný jako u IPv4, jedinou adresou typu loopback je 0000:0000:0000:0000:0000:0000:0000:0001 nebo její zkrácená verze ::1. Virtuální fyzické rozhraní má jméno *LOOPBACK6.
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 k dispozici při použití produktu iSeries Navigator a 5250.	Totéž platí pro IPv6. IPv6 je podporován jak 5250, tak produktem iSeries Navigator.
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	Konfigurovatelná tabulka produktu iSeries Navigator, která asociuje jméno sítě s IP adresou bez masky. Například asociuje hostitelský systém Network14 s IP adresou 1.2.3.4.	U IPv6 se v současné době tato tabulka 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.	Filtrování paketů v současné době nepodporuje IPv6. Filtrování paketů IPv4 však může být prováděno u tunelového provozu IPv6.
směrování paketů (forwarding)	Server iSeries může být nakonfigurován tak, aby přijaté IP pakety směroval na nelokální IP adresy. Příchozí a odchozí rozhraní jsou obvykle připojena k různým lokálním sítím (LAN).	Pakety IPv6 nejsou v současné době směrovány dál.
tunelování paketů	U IPv4 se tunelování vyskytuje ve VPN pro spojení VPN fungující v tunelovém režimu (IPv4 tunelovaný v IPv4) a také v L2TP.	U IPv6 se očekává, že tunelování uvnitř paketů IPv4 bude hlavní součástí vývoje. V současné době je společností IETF definováno nejméně 5 různých typů tunelování IPv6 v IPv4. Každý typ má jiné atributy a výhody. K tomu, aby uzly IPv6 spolu mohly komunikovat přes stávající Internet typu IPv4, je podporován základní a přizpůsobivý typ tunelování IPv6 v IPv4. Nazývá se **konfigurované tunelování**. Poskytuje virtuální dvoubodové spojení mezi dvěma uzly IPv6 a používá nový typ tunelové linky s názvem *TNLCFG64.
testování spojení (příkaz PING)	Základní nástroj TCP/IP k testování dosažitelnosti. Je k dispozici při použití produktu iSeries Navigator a 5250.	Totéž platí pro IPv6. IPv6 je podporován jak 5250, tak produktem iSeries Navigator.
PPP (Point-to-Point Protocol)	Tento protokol dvoubodového připojení podporuje komutovaná rozhraní přes různé typy modemů a linek.	PPP v současné době nepodporuje IPv6.
omezení (vyhrazení) portů	Tato dialogová okna (panely) iSeries umožňují, aby zákazníci nakonfigurovali vybrané číslo portu nebo rozsahy čísel portů pro TCP nebo UDP tak, aby byly k dispozici pouze určitému profilu.	V IPv6 není podporováno. Konfigurovaná omezení se týkají pouze 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.

	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. 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. U IPv6 se používá zápis omezeného rozsahu adresy, který je součástí definice architektury (viz “rozsah adresy” na stránce 19).
tabulka protokolů	Tabulka konfigurovatelná pomocí produktu iSeries Navigator, která asociuje jméno protokolu s přiřazeným číslem protokolu; například UDP, 17. Systém je dodáván s malým počtem položek v této tabulce: IP, TCP, UDP, ICMP.	Tato tabulka podporuje IPv6 beze změny.
QoS (Quality of Service)	QoS umožňuje u aplikací TCP/IP požadovat prioritu paketů a šířku pásma.	QoS v současné době nepodporuje IPv6. Pokud je však IPv6 tunelován v IPv4, mohou být na provoz IPv4 aplikovány stávající systémové prostředky QoS iSeries, které pak budou transparentně zacházet s přenosem IPv6.
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.	Je to důležitý prvek architektury IPv6. Očekává se, že bude probíhat většinou automaticky, zvláště v rámci prefixu /48.
přenosová cesta	Tento logický pojem představuje mapování skupiny IP adres (nebo pouze 1 adresy) 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. Předvolená přenosová cesta je *DFTROUTE.	Principiálně totéž jako u IPv4. Důležitý rozdíl: Přenosové cesty IPv6 nejsou asociovány (svázány) s rozhraním, ale s fyzickým rozhraním (spojem, například *TNLCFG64 nebo ETH03). Má to různé důvody. Jeden z důvodů je, že výběr zdrojové adresy funguje u IPv6 jinak než u IPv4. Viz “výběr zdrojové adresy”. Kvůli zvýšení odolnosti jsou povoleny duplicitní přenosové cesty. Při nalezení přenosové cesty jsou však ignorovány.
RIP (Routing Information Protocol)	RIP je přenosový (směrovací) protokol podporovaný směrovacím démonem.	RIP v současné době nepodporuje IPv6. Při směrování IPv6 se používají statické přenosové cesty.
tabulka služeb	Konfigurovatelná tabulka na serveru iSeries, která asociuje jméno služby s portem a protokolem; například jméno služby FTP-control, port 21, TCP a UDP. 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.
SNMP (Simple Network Management Protocol)	SNMP je standardní protokol pro správu systémů.	SNMP v současné době nepodporuje IPv6. Při směrování IPv6 se používají statické přenosové cesty.
rozhraní API soketů	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. 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. Nová rozhraní API také podporují konverzi adres IPv6 z textové formy do binární a naopak. Další informace o vylepšeních soketů pro IPv6 najdete v tématu věnovaném používání skupiny 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 stejně jako u IPv4 určit zdrojovou IP adresu (obvykle pomocí funkce bind()). 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.

	IPv4	IPv6
spuštění a ukončení	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. Všechna rozhraní IPv6 jsou spuštěna automaticky, pokud parametr AUTOSTART = *YES (předvolba). IPv6 nelze používat nebo konfigurovat bez IPv4. IPv6 musí mít nakonfigurovanou zkratovací smyčku (loopback) IPv6 (::1).
Telnet	Telnet umožňuje přihlásit se k vzdálenému počítači a pracovat s ním, jako byste k němu byli připojeni přímo.	Telnet v současné době nepodporuje IPv6.
trasování přenosové cesty	Základní nástroj TCP/IP k určení cesty. Je k dispozici při použití produktu iSeries Navigator a 5250.	Totéž platí pro IPv6. IPv6 je podporován jak 5250, tak produktem iSeries Navigator.
transportní vrstvy	TCP, UDP, RAW. Nová transportní vrstva SCTP (Stream Control Transmission Protocol) má poskytovat nejlepší vlastnosti TCP a UDP, tedy zaručenou bezespojovou komunikaci. SCTP je v nejranější fázi používání. Serverem iSeries není podporována.	U IPv6 existují stejné tři transportní vrstvy, které jsou z funkčního hlediska nezměněné.
neuvedená 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.
VPN (Virtual Private Networking)	Technologie VPN (používající IPsec) umožňuje rozšířit zabezpečenou soukromou síť přes stávající veřejnou síť.	VPN v současné době nepodporuje IPv6. Pokud je však IPv6 tunelován v IPv4, mohou být na provoz IPv4 aplikovány stávající systémové prostředky VPN iSeries, takže přenos IPv6 pak bude probíhat transparentně.

Odstraňování problémů s IPv6

Pokud jste na serveru nakonfigurovali IPv6, můžete používat několik stejných nástrojů pro odstraňování problémů jako u IPv4. Například nástroje pro trasování přenosové cesty a testování spojení (příkaz PING) přijímají formáty adres IPv4 i IPv6; můžete je proto používat k testování spojení a přenosových cest u obou typů sítí. Kromě toho můžete pomocí funkce trasování komunikace trasovat data na obou typech komunikačních linek IPv4 i IPv6.

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

Související informace k IPv6

Další informace o IPv6 najdete v těchto zdrojích informací:

IETF (Internet Engineering Task Force) (http://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.

Fórum o IPv6 (http://www.ipv6forum.com/)
Zde najdete nové články a akce poskytující informace o nejnovějším vývoji IPv6.

Kapitola 4. Plánování nastavení TCP/IP

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.

Požadavky na konfiguraci TCP/IP
Shromážděte a zapište si základní informace o konfiguraci, které budete potřebovat pro nastavení TCP/IP.

Pokyny pro zabezpečení ochrany TCP/IP
Jako nový člen sítě zvažte své požadavky na zabezpečení ochrany dat.

Požadavky na konfiguraci TCP/IP

Vytiskněte si tuto stránku a poznamenejte si údaje o konfiguraci serveru a síti TCP/IP, k níž se připojujete. Tyto informace budete později potřebovat při konfigurování TCP/IP. Pod tabulkou jsou uvedeny pokyny, podle kterých můžete zjistit hodnoty pro první dvě řádky. Jestliže nejste s těmito výrazy obeznámeni, otevřete červenou knihu IBM TCP/IP for AS/400: More Cool Things Than Ever  a prostudujte si druhou kapitolu nazvanou ″TCP/IP: Basic Installation and Configuration″.

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
Hostitelské jméno a jméno domény pro váš systém		sys400.xyz.company.com
IP adresa pro server jmen domény		199.4.191.76

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

1. Na příkazový řádek serveru napište go hardware a stiskněte klávesu **Enter**.
2. Vyberte volbu Práce s komunikačními prostředky (Volba 1). To provedete tak, že napíšete 1 a stisknete 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

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.
- **Zkraťte 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.
- **Mějte kontrolu nad tím, kdo může spouštět a měnit vaše 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.
- **Mějte kontrolu nad směrováním TCP/IP:**
  - Nepovolte přeposílání IP, aby počítačoví piráti nemohli prostřednictvím vašeho webového serveru napadnout další důvěryhodné systémy.
  - Definujte pouze jedinou předepsanou cestu k vašemu veřejnému webovému serveru: předvolenou předepsanou cestu vašeho poskytovatele služeb sítě Internet.
  - Nekonfigurujte hostitelská jména a IP adresy vašich vnitřních bezpečných systémů v hostitelské tabulce TCP/IP na vašem webovém serveru. V této tabulce uvádějte pouze jména jiných veřejných serverů, na které chcete přistupovat.
- **Mějte kontrolu nad servery TCP/IP, které slouží pro vzdálené, interaktivní přihlašování do systému.**
  Aplikace, jako například FTP a Telnet, jsou mnohem více vystaveny riziku vnějšího napadení. Podrobné informace o způsobu řízení rizika najdete v publikaci Rady a nástroje pro zabezpečení serveru iSeries v kapitole, která uvádí rady týkající se řízení interaktivního přihlašování do systému.

Další informace o zabezpečení ochrany dat a o volbách, které máte k dispozici, najdete v tématu iSeries a zabezpečení Internetu.

Kapitola 5. Instalace TCP/IP

Základní podpora TCP/IP je dodávána s operačním systémem OS/400 a umožňuje připojit server iSeries k síti. Budete-li však chtít použít nějaké aplikace 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 napište GO LICPGM a stiskněte klávesu **Enter**. Zobrazí se obrazovka Práce s licencovanými programy.
3. Na obrazovce Práce s licencovanými programy vyberte volbu **11** Instalovat licencované programy a uvidíte seznam licencovaných programů a jejich volitelných částí.
4. U položky 57*xx*TC1 (TCP/IP Connectivity Utilities for iSeries) napište do sloupce Volba volbu **1** Instalovat. Stiskněte klávesu **Enter**. Objeví se obrazovka Confirm Licensed Programs to Install, na níž jsou uvedeny licencované programy, které jste vybrali k instalaci. Stisknutím klávesy **Enter** výběr potvrďte.
5. Na obrazovce Install Options vyplňte tyto volby:

Installation device	Instalujete-li z CD-ROM, napište QOPT. 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 menu Práce s licencovanými programy, nebo obrazovka Přihlášení.
6. Vyberte volbu **50** Zobrazit protokol pro zprávy, abyste si ověřili, že je licencovaný program úspěšně nainstalován.

   Pokud se vyskytnou nějaké chyby, uvidíte v dolní části obrazovky Práce s licencovanými programy zprávu, že funkce práce s licencovanými programy se nedokončila. Vyskytne-li se problém, zkuste produkt TCP/IP Connectivity Utilities přeinstalovat. Pokud se tím problém nevyřeší, měli byste zavolat zákaznickou podporu.

Poznámka:

Mezi další licencované programy, které můžete nainstalovat, patří:

- iSeries Access for Windows 95/NT (5769–XD1 V3R1M3 nebo vyšší verze) poskytuje podporu produktu iSeries Navigator, který se používá ke konfigurování některých komponent TCP/IP.
- IBM HTTP Server for iSeries (57*xx*–DG1) poskytuje podporu webového serveru.
- Některé aplikace TCP/IP vyžadují instalaci dalších licencovaných programů. Abyste zjistili, které další programy budete potřebovat, přečtěte si pokyny pro nastavení u každé konkrétní aplikace, kterou si chcete pořídit.

Kapitola 6. Konfigurace TCP/IP

TCP/IP můžete konfigurovat poprvé nebo můžete chtít změnit stávající konfiguraci kvůli použití funkcí IPv6. Toto téma obsahuje pokyny ke konfigurování TCP/IP v obou těchto situacích. V následujících částech najdete pokyny ke konfigurování TCP/IP na serveru:

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

Konfigurace protokolu IPv6
Postupujte takto, jestliže chcete nakonfigurovat server pro IPv6. Oceníte rozšířené možnosti adresování a robustní vlastnosti tohoto protokolu Internetu. Pokud nejste s protokolem IPv6 obeznámeni, podívejte se na přehled v kapitole Protokol IP (Internet Protocol) verze 6 (IPv6). K tomu, abyste mohli nakonfigurovat protokol IPv6, musíte mít na serveru nakonfigurovaný protokol TCP/IP.

Konfigurace TCP/IP, když je operační systém ve stavu omezení
Použijte tuto metodu, pokud potřebujete spustit TCP/IP, zatímco je operační systém ve stavu omezení.

První konfigurace TCP/IP

Chcete-li na novém serveru nastavit TCP/IP, vyberte jednu z těchto metod:

Konfigurace TCP/IP pomocí průvodce EZ-Setup Wizard
Tuto preferovanou metodu použijte, je-li váš počítač vybaven pro použití průvodce EZ-Setup Wizard. Průvodce EZ-Setup Wizard je dodáván spolu se serverem iSeries.

Konfigurace TCP/IP pomocí znakově orientovaného rozhraní
Tuto metodu použijte, nemůžete-li použít průvodce EZ-Setup Wizard. Tuto metodu byste například měli použít, chcete-li používat produkt iSeries Navigator v osobním počítači vyžadujícím, aby před spuštěním produktu iSeries Navigator byla provedena základní konfigurace TCP/IP.

Konfigurace TCP/IP pomocí průvodce EZ-Setup Wizard

Produkt iSeries Navigator má grafické uživatelské rozhraní se stručnými dialogovými okny a průvodci ke konfiguraci TCP/IP. Chcete-li provést počáteční nastavení, použijte v prostředí produktu iSeries Navigator průvodce EZ-Setup k vytvoření spojení a k první konfiguraci TCP/IP. Tuto metodu práce se serverem byste měli preferovat, protože používání tohoto rozhraní je snadné. Disk CD-ROM obsahující průvodce EZ-Setup Wizard jste obdrželi spolu se serverem iSeries.

Chcete-li nakonfigurovat server, proveďte následující kroky:

1. Spusťte průvodce EZ-Setup Wizard. 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 **Server –> Síť**.
   b. Pravým tlačítkem myši klepněte na **Konfigurace TCP/IP** a vyberte **Start**. 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. Budete-li chtít přidat přenosové cesty a rozhraní, přejděte na kapitolu Přizpůsobení TCP/IP pomocí produktu iSeries Navigator. Budete-li chtít používat v síti protokol IPv6, přečtěte si část Konfigurace protokolu IPv6.

Konfigurace TCP/IP pomocí znakově orientovaného rozhraní

Jestliže nemůžete použít průvodce EZ-Setup Wizard v prostředí produktu iSeries Navigator, použijte místo toho znakově orientované rozhraní. Znakově orientované rozhraní byste měli například použít, chcete-li používat produkt iSeries Navigator v osobním počítači vyžadujícím, aby před spuštěním produktu iSeries Navigator byla provedena základní konfigurace TCP/IP.

K tomu, abyste mohli provést kroky konfigurace popisované v této části, musí mít váš uživatelský profil speciální oprávnění *IOSYSCFG. Další informace o tomto typu oprávnění najdete v publikaci iSeries Zabezpečení - referenční informace v kapitole zabývající se uživatelskými profily.

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

1. Na příkazový řádek napište příkaz GO TCPADM a stiskněte klávesu Enter. Zobrazí se obrazovka TCP/IP Administration.
2. Vyberte volbu 1 (Konfigurace TCP/IP) a stiskněte klávesu Enter. Zobrazí se menu Konfigurace TCP/IP (CFGTCP). Pomocí tohoto menu vyberte úkoly konfigurace. Dříve než začnete server konfigurovat, věnujte určitý čas prohlídce menu.

Při konfigurování TCP/IP na serveru proveďte tyto kroky:

1. Konfigurace popisu linky.
2. Zapněte postoupení datagramu pomocí IP.
3. Konfigurace rozhraní.
4. Konfigurace přenosové cesty.
5. Definice jmen lokální domény a hostitelského systému.
6. Definice hostitelské tabulky.
7. Spuštění TCP/IP.

Konfigurace popisu linky (Ethernet)

Tyto pokyny se týkají konfigurace TCP/IP přes komunikační adaptér typu Ethernet. Používáte-li jiný typ adaptéru, například Token-ring, vyhledejte příkaz určený pro váš adaptér v publikaci TCP/IP Configuration and Reference, *Appendix A*.

Chcete-li nakonfigurovat popis linky, proveďte následující kroky:

1. Na příkazový řádek napište příkaz CRTLINETH a stiskněte klávesu Enter. Zobrazí se menu Vytvoření popisu linky (Ethernet) (CRTLINETH).
2. Zadejte název linky a stiskněte klávesu Enter. (Použijte libovolné jméno.)
3. Zadejte název prostředku (resource) a stiskněte klávesu Enter.

Další krok:
Zapněte postoupení datagramu pomocí IP.

Zapněte postoupení datagramu pomocí IP.

Zapněte postoupení datagramu pomocí IP, takže pakety budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, použijte tento postup:

1. Na příkazový řádek napište CHGTCPA a stiskněte klávesu F4.
2. Na náznak *Postoupení datagramu IP* zadejte *YES.

Další krok:
Konfigurace rozhraní

Konfigurace rozhraní

Chcete-li nakonfigurovat rozhraní, proveďte následující kroky:

1. Na příkazový řádek napište příkaz CFGTCP a stiskněte klávesu Enter. Zobrazí se menu Konfigurace TCP/IP.
2. V menu Konfigurace TCP/IP vyberte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
3. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Zobrazí se obrazovka Přidání TCP/IP rozhraní.
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 (Start) a stiskněte klávesu Enter.

Další krok:
Konfigurace přenosové cesty

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 nakonfigurovat předvolenou přenosovou cestu, proveďte následující kroky:

1. V menu Konfigurace TCP/IP vyberte volbu 2 (Práce se směry TCP/IP) a stiskněte klávesu Enter.
2. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Zobrazí se obrazovka Přidání směru TCP/IP (ADDTCPRTE).
3. Zadejte jako cíl přenosové cesty hodnotu *DFTROUTE, zadejte jako masku podsítě hodnotu *NONE, zadejte IP adresu následujícího směrovacího uzlu a stiskněte klávesu Enter.

Další krok:
Definice jmen lokální domény a hostitelského systému

Definice jmen lokální domény a hostitelského systému

Chcete-li definovat jména lokální domény a hostitelského systému, proveďte následující kroky:

1. V menu Konfigurace TCP/IP vyberte volbu 12 (Změna domény TCP/IP) a 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.

Další krok:
Definice hostitelské tabulky

Definice hostitelské tabulky

Chcete-li definovat hostitelskou tabulku, proveďte následující kroky:

1. V menu Konfigurace TCP/IP vyberte volbu 10 (Práce se záznamy tabulky hostitelů) a stiskněte klávesu Enter.
2. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Tak přejdete k obrazovce Přidání záznamu hostitelské tabulky TCP/IP.
3. Zadejte IP adresu, přidružené jméno lokálního hostitelského systému a plně kvalifikované hostitelské jméno a potom stiskněte klávesu Enter.
4. Pokud je to nezbytné, zadejte znaménko plus (+). Tak uvolníte dostupný prostor pro více než jedno hostitelské jméno.
5. Opakujte tyto kroky pro každý z dalších hostitelských systémů v síti, s nimiž chcete komunikovat podle jména, a pro každý z nich přidejte položku.

Další krok:
Spuštění TCP/IP

Spuštění TCP/IP

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

Chcete-li spustit TCP/IP, napište na příkazový řádek příkaz STRTCP.

Příkaz STRTCP (Spuštění TCP/IP) inicializuje a aktivuje zpracování TCP/IP, spustí TCP/IP rozhraní a úlohy serveru. Příkazem STRTCP budou spuštěna pouze rozhraní a servery, pro které má parametr AUTOSTART hodnotu *YES.

Postup konfigurace TCP/IP na serveru je ukončen. Bude-li třeba konfiguraci sítě změnit, použijte produkt iSeries Navigator. Budete-li chtít přidat přenosové cesty a rozhraní, přejděte na kapitolu Přizpůsobení TCP/IP pomocí produktu iSeries Navigator. Budete-li chtít používat v síti protokol IPv6, přečtěte si část Konfigurace protokolu IPv6.

Konfigurace protokolu IPv6

Nyní jste připraveni využívat Internet nové generace - tím, že budete ve své síti používat protokol IPv6. Chcete-li používat funkce protokolu IPv6, musíte změnit konfiguraci TCP/IP tím, že nakonfigurujete linku vyhrazenou pro protokol IPv6. Nakonfigurovat musíte buď linku na adaptéru 2838 nebo 2849 typu Ethernet, nebo konfigurovanou tunelovou linku (virtuální linku). Pokyny ke konfigurování IPv6 obsahují tato témata:

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

Konfigurace protokolu IPv6 pomocí průvodce konfigurací protokolu IPv6
Zde najdete pokyny k použití průvodce **konfigurací protokolu IPv6** ke konfiguraci protokolu IPv6 na serveru.

Požadavky na konfiguraci

Určete, který z následujících dvou typů konfigurace IPv6 odpovídá vaší situaci. Nevíte-li jistě, který typ zvolit, podívejte se na příklady uvedené v části Scénáře IPv6.

Chcete-li umožnit fungování IPv6 na serveru, musíte splnit tyto požadavky:

Požadavky na konfiguraci linky typu Ethernet pro IPv6:

- Operační systém OS/400 (verze 5 vydání 2 nebo novější).
- iSeries Access for Windows a iSeries Navigator
  - Síťová komponenta produktu iSeries Navigator.
- Adaptér 2838 nebo 2849 typu Ethernet vyhrazený pro IPv6.
- Směrovač podporující IPv6 je požadován pouze tehdy, chcete-li odesílat provoz IPv6 za hranice nejbližší sítě (LAN).
- Protože na serveru musí být spuštěn TCP/IP, musíte na samostatném fyzickém adaptéru nakonfigurovat TCP/IP (používající IPv4). Pokud jste nenakonfigurovali server pro IPv4, přejděte před konfigurováním linky pro IPv4 na část První konfigurace TCP/IP.

Požadavky na vytvoření konfigurované tunelové linky (TNLCFG64):

- Operační systém OS/400 (verze 5 vydání 2 nebo novější).
- iSeries Access for Windows a iSeries Navigator
  - Síťová komponenta produktu iSeries Navigator.
- Dříve než budete konfigurovat tunelovou linku, musíte na serveru nakonfigurovat TCP/IP (používající IPv4). Pokud jste nenakonfigurovali server pro IPv4, přečtěte si část První konfigurace TCP/IP.

V části Konfigurace protokolu IPv6 pomocí průvodce konfigurací protokolu IPv6 najdete pokyny k práci s průvodcem.

Konfigurace protokolu IPv6 pomocí průvodce konfigurací protokolu IPv6

Chcete-li na serveru nakonfigurovat IPv6, musíte změnit konfiguraci serveru pomocí průvodce **konfigurací protokolu IPv6** v prostředí produktu iSeries Navigator. IPv6 je možné nakonfigurovat pouze v prostředí produktu iSeries Navigator - nelze použít znakově orientované rozhraní.

Poznámka: Popis linky typu Ethernet můžete pro IPv6 nakonfigurovat v znakově orientovaném rozhraní pomocí příkazu CRTLINETH (Vytvoření popisu linky - Ethernet); musíte však zadat hexadecimální adresu skupiny multicast 333300000001. Potom musíte dokončit konfiguraci protokolu IPv6 pomocí průvodce **konfigurací protokolu IPv6**.

Průvodce bude požadovat zadání následujících údajů:

Požadavky na konfiguraci linky typu Ethernet pro IPv6:
Tato konfigurace umožňuje posílání paketů IPv6 lokální sítí IPv6 (LAN). Průvodce požaduje jméno hardwarového komunikačního prostředku na serveru, na kterém chcete IPV6 nakonfigurovat; například CMN01. Musí to být adaptér 2838 nebo 2849 typu Ethernet, který není v současné době nakonfigurován pro IPv4. Scénář popisující situaci, kdy byste mohli nakonfigurovat linku Ethernet pro IPv6, najdete v části Vytvoření lokální sítě IPv6 (LAN).

Požadavky na vytvoření konfigurované tunelové linky (TNLCFG64):
Tato konfigurace umožňuje posílání paketů IPv6 sítěmi IPv4. Průvodce požaduje zadání adresy IPv4 lokálního koncového bodu a adresy IPv6 lokálního rozhraní asociovaného s tunelem. Scénáře popisující dvě situace, kdy byste mohli vytvořit konfigurované tunelové linky pro IPv6, najdete v částech Posílání paketů IPv6 lokální sítí IPv4 (LAN) a Posílání paketů IPv6 dálkovou sítí IPv4 (WAN).

Chcete-li použít průvodce **konfigurací protokolu IPv6**, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator rozbalte **Server —> Síť —> Konfigurace TCP/IP**.
2. Klepněte pravým tlačítkem myši na **IPv6** a vyberte **Konfigurace protokolu IPv6**.
3. Při konfiguraci protokolu IPv6 na serveru postupujte podle pokynů průvodce.

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

Situace

Jako síťový administrátor budete potřebovat obdržet zprávu o stavu zálohování na vašem 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 TCP/IP síťového zařízení). PDA využívá aplikaci podporující sokety, která vyžaduje ke komunikaci aktivní TCP/IP rozhraní. Tuto komunikaci umožníte tak, že spustíte TCP/IP se speciálními parametry. Poté, co spustíte TCP/IP, budete muset spustit specifické TCP/IP rozhraní, abyste povolili přístup k systému. Níže uvedené informace vám poskytnou detailnější popis.

Předpoklady

Váš server iSeries musí být server provozovaný pod operačním systémem OS/400(R) V5R2 nebo vyšší verze.

Omezení

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

- Nelze spustit servery TCP/IP (příkaz STRTCPSRV CL), protože tyto 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 iSeries ve stavu omezení, zadejte tento příkaz z prostředí příkazového řádku: STRTCP STRSVR(*NO) STRIFC(*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 specifické TCP/IP rozhraní

   Poté, co spustíte TCP/IP ve stavu omezení, můžete spustit specifické rozhraní potřebné pro aplikace povolující použití SSL.

   a. Ověřte, že rozhraní, které chcete spustit, používá popis linky typu *ELAN, *TRLAN nebo *DDI.

      Typ linky vašeho rozhraní zjistíte tak, že na příkazovém řádku zadáte příkaz CFGTCP a vyberete volbu 1 - Práce s TCP/IP rozhraními.

   b. Ověřte, že rozhraní není připojeno k NWID nebo NWSD. Na jakékoliv jiné pokusy bude systém reagovat chybovou zprávou.

      To, zda rozhraní je nebo není připojeno k NWID nebo NWSD, zjistíte zadáním příkazu DSPLIND abc na příkazovém řádku (kde abc je název popisu linky). Ověřte, zda jméno prostředku (resource name) není *NWID or *NWSD.

      Poznámka: Pokud je rozhraní připojeno k NWID nebo NWSD, doporučujeme použít jiné rozhraní.

   c. Nakonec spusťte rozhraní. Na příkazový řádek zadejte: STRTCPIFC INTNETADR('a.b.c.d'). Místo a.b.c.d zadejte IP adresu vašeho rozhraní.

      Poznámka: Ověřte, že není zadáno STRTCPIFC INTNETADR(*AUTOSTART).

3. Ověřte, že je rozhraní aktivní.

   Proveďte testování spojení specifického rozhraní vaší aplikace. Existuje pouze velmi málo obslužných programů TCP/IP, které mohou být provozovány ve stavu omezení. Avšak příkazy Ping a Netstat lze použít. Více informací o použití příkazů ping a netstat najdete v tématu Nástroje k ověření síťové struktury pod heslem Odstraňování problémů s TCP/IP.

Kapitola 7. Přizpůsobení TCP/IP 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 přizpůsobit konfiguraci pomocí produktu iSeries Navigator, vyberte některé z témat uvedených níže. Tato témata jsou výchozím bodem při správě konfigurace TCP/IP pomocí produktu iSeries Navigator.

Změna nastavení TCP/IP

Konfigurace protokolu IPv6

Přidání rozhraní IPv4

Přidání rozhraní IPv6

Přidání přenosových cest IPv4

Přidání přenosových cest IPv6

Změna nastavení TCP/IP

Nastavení TCP/IP můžete zobrazit a změnit pomocí produktu iSeries Navigator. Například můžete změnit vlastnosti pro jméno hostitele nebo domény, server jmen, položky hostitelské tabulky, atributy systému, omezení portů, servery nebo připojení klientů. Měnit můžete obecné vlastnosti i vlastnosti specifické pro IPv4 nebo IPv6, například transportní vrstvy.

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

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Vlastnosti**. Tím otevřete dialog **Vlastnosti TCP/IP**.
3. Zde si můžete vybírat jednotlivé karty a prohlížet nebo editovat informace o TCP/IP.

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

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť**.
2. Klepněte pravým tlačítkem myši na **Konfigurace TCP/IP** a vyberte **Hostitelská tabulka**. Tím otevřete dialog **Hostitelská tabulka**.
3. Použijte dialog **Hostitelská tabulka** k přidávání, úpravám a odstraňování položek hostitelské tabulky.

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

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť**.
2. Klepněte pravým tlačítkem myši na **IPv4** a vyberte **Vlastnosti**. Tím otevřete dialog **Vlastnosti IPv4**.
3. Zde si můžete vybírat jednotlivé karty a prohlížet nebo editovat nastavení vlastností IPv4.

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

1. V prostředí produktu iSeries Navigator vyberte **Server —> Síť**.
2. Klepněte pravým tlačítkem myši na **IPv6** a vyberte **Vlastnosti**. Tím otevřete dialog **Vlastnosti IPv6**.
3. Zde si můžete vybírat jednotlivé karty a prohlížet nebo editovat nastavení vlastností IPv6.

Konfigurace protokolu IPv6

Pokud nejste s protokolem IPv6 obeznámeni, podívejte se na přehled v kapitole Protokol IP (Internet Protocol) verze 6 (IPv6).

Chcete-li nakonfigurovat protokol IPv6, musíte změnit konfiguraci serveru pomocí průvodce **konfigurací protokolu IPv6**. Před spuštěním průvodce si v části Konfigurace protokolu IPv6 přečtěte pokyny a speciální požadavky.

Přidání rozhraní IPv4

Chcete-li vytvořit nové rozhraní IPv4, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **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

Chcete-li vytvořit nové rozhraní IPv6, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **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

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

Chcete-li nakonfigurovat novou přenosovou cestu IPv4, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **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

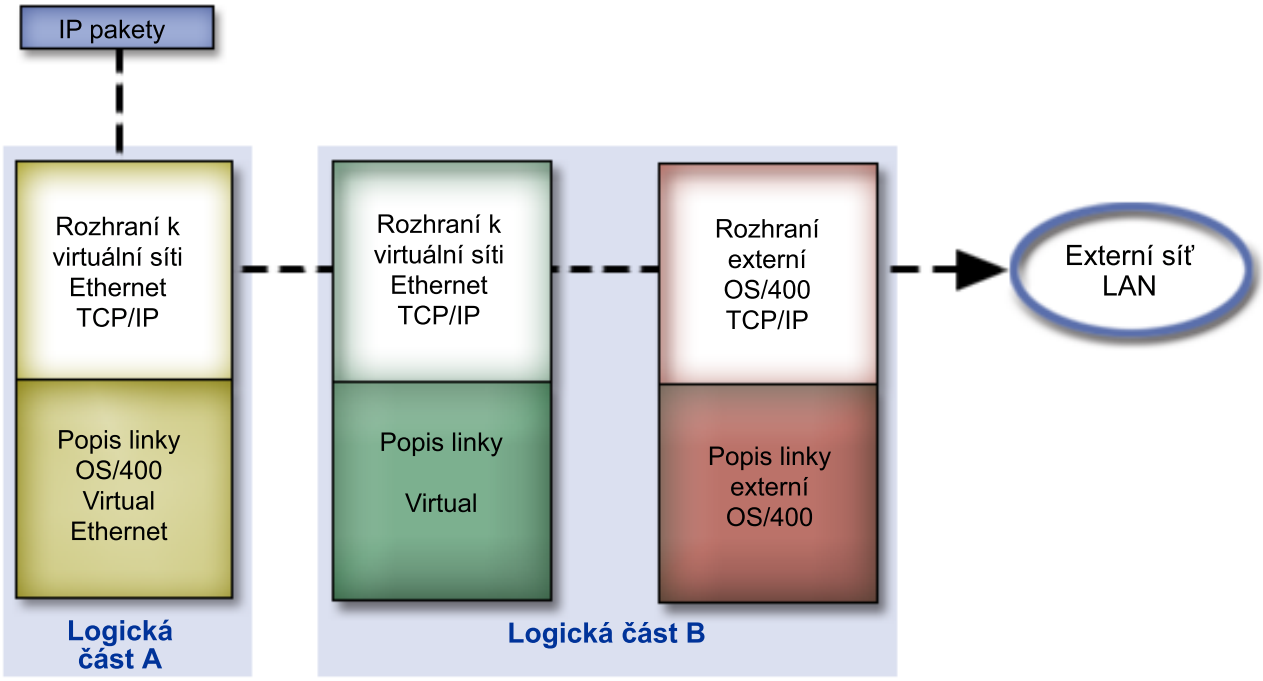
Jakékoliv změny, které provedete v informacích o přenosové cestě, začnou platit okamžitě.

Chcete-li nakonfigurovat novou přenosovou cestu IPv6, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator vyberte **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.

Kapitola 8. TCP/IP metody propojení virtuální sítě Ethernet s externími sítěmi LAN

Pokud používáte virtuální síť typu Ethernet, aby jednotlivé logické části mezi sebou komunikovaly, budete možná potřebovat rozšířit tuto komunikaci 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:

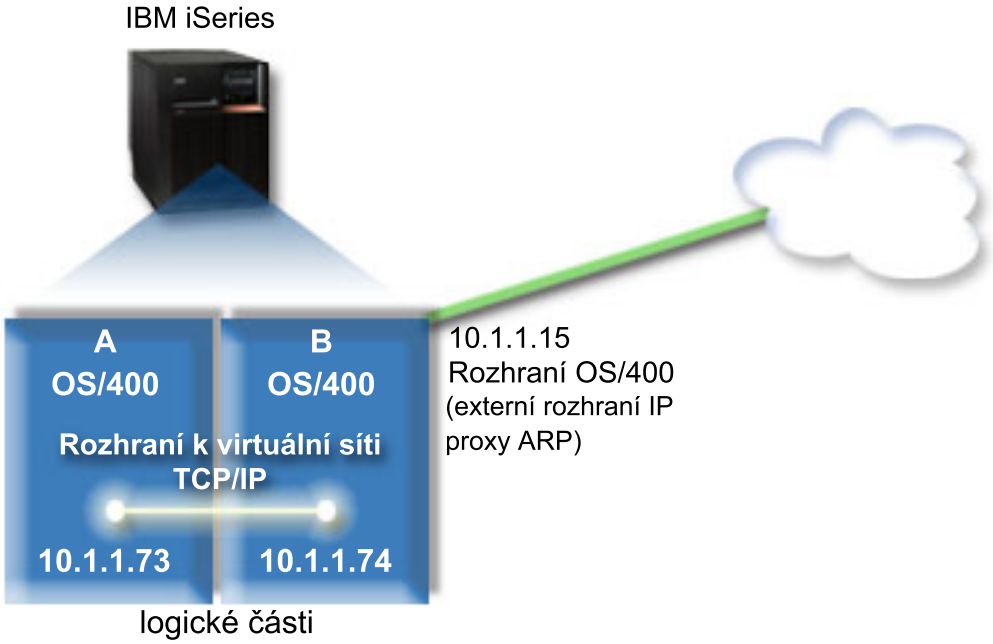
- **Proxy ARP**
  Tato metoda využívá transparentní vytváření podsítí k tomu, aby asociovala virtuální rozhraní logické části s externím rozhraním. Funkce proxy ARP je vestavěna v balíku TCP/IP. Pokud znáte potřebné IP adresy, doporučujeme vám použít tuto metodu.
- **NAT (převod síťové adresy)**
  Pro směrování provozu mezi logickou částí a vnější sítí můžete použít filtr paketu operačního systému OS/400.
- **Směrování TCP/IP**
  Standardní směrování TCP/IP se používá ke směrování provozu do virtuální sítě typu Ethernet stejným způsobem, jako byste definovali směrování do jakékoliv jiné sítě typu LAN. Toto vyžaduje aktualizaci informací o přenosové cestě vaší sítí.

Metoda proxy ARP

Metoda proxy ARP používá techniky všeobecně známé jako *transparentní vytváření podsítí*. Více informací o technice transparentního vytváření podsítí se dozvíte zde:

- Červená kniha V4 TCP/IP for AS/400: More Cool Things Than Ever
  Tato červená kniha obsahuje ukázkové scénáře znázorňující běžná řešení a příklady konfigurací. Pomůže vám také naplánovat, instalovat, uzpůsobit, nakonfigurovat a odstranit závady TCP/IP na vašem serveru iSeries.
- Směrování TCP/IP a vyvažování zatížení
  Toto téma pojednává o technikách a pokynech směrování a vyvažování zatížení.

Pokud se rozhodnete použít metodu proxy ARP, musíte mít dobré znalosti 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). Poněvadž se jedná o blok čtyř IP adres, je maska podsítě těchto adres 255.255.255.252. Každému virtuálnímu TCP/IP rozhraní 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. Vzhledem k tomu, že rozhraní 10.1.1.74 je asociováno s externím rozhraním ARP 10.1.1.15, pokračují pakety dále z virtuální sítě typu Ethernet prostřednictvím rozhraní proxy ARP.

Ke konfiguraci virtuální sítě typu Ethernet tak, aby používala metodu propojení proxy ARP, postupujte takto:

1. Povolte logickým částem stát se součástí virtuální sítě typu Ethernet.
2. Vytvořte popis linky sítě Ethernet.
3. Zapněte postoupení datagramu pomocí IP.
4. Vytvořte rozhraní, které povolí proxy ARP.
5. Vytvořte virtuální TCP/IP rozhraní v logické části A.
6. Vytvořte virtuální TCP/IP rozhraní v logické části B.
7. Vytvořte přenosovou cestu.
8. Ověřte síťové komunikace.

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

Poznámka: Pokud používáte servery jiné než servery modelu 270 nebo 8 *xx*, musíte provést tento krok s pomocí HMC (Hardware Management Console for eServer) namísto použití primární logické části. Podrobnosti najdete v tématu Virtuální síť typu Ethernet.

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

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a stiskněte klávesu Enter.
2. Zadejte vaše ID uživatele servisních nástrojů a heslo.
3. Na obrazovce SST (System Service Tools) vyberte volbu 5 (Práce s logickými částmi systému).
4. Na obrazovce Práce s logickými částmi systému vyberte volbu 3 (Práce s konfigurací logické části).
5. Stiskněte klávesu F10 (Práce s virtuální sítí typu 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.

Další krok

Vytvořte popis linky sítě Ethernet.

Krok 2: Vytvořte popis linky sítě 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 vašeho serveru.

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

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) 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 logickou částí zde bude jeden.
3. Na obrazovce Display Resource Detail 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 obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration descriptions) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* 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 asociované sítě typu Ethernet stejný název, můžete snadno sledovat konfiguraci virtuální sítě typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.
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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) vedle příslušného portu virtuální sítě typu Ethernet.

   Porty typu Ethernet označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet zde bude jeden. Každý port označený jako 268C má asociovaný kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).
3. Na obrazovce Display Resource Detail posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro virtuální síť typu Ethernet.
4. Na obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* zadejte VETH0. Pokud použijete pro popisy linek a asociované sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace vašich virtuálních sítí typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.
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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

Krok 3: Zapněte postoupení datagramu pomocí IP.

Zapněte postoupení datagramu pomocí IP, takže pakety budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, použijte tento postup:

1. Na příkazový řádek logické části A zadejte CHGTCPA a stiskněte klávesu F4.
2. Na náznak *Postoupení datagramu IP* zadejte *YES.

Další krok

Vytvořte rozhraní, které povolí proxy ARP.

Krok 4: Vytvořte rozhraní, které povolí proxy ARP.

Při vytváření TCP/IP rozhraní, které povolí proxy ARP, 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 TCP/IP rozhraní 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 TCP/IP rozhraní operačního systému OS/400 pro logickou část B. Toto rozhraní je externím rozhraním, rozhraním proxy ARP IP. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.

Další krok

Vytvořte virtuální TCP/IP rozhraní v logické části A.

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

Při vytváření virtuálního rozhraní postupujte takto:

1. Na příkazový řádek logické části A zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
2. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
3. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
4. Na náznak *Internetová adresa* zadejte '10.1.1.73'.
5. Na náznak *Popis linky* zadejte název popisu linky, například ETHLINE.
6. Na náznak *Maska podsítě* zadejte '255.255.255.252'.
7. Spusťte rozhraní. Na obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.

Další krok

Vytvořte virtuální TCP/IP rozhraní v logické části B.

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

Při vytváření virtuálního rozhraní postupujte takto:

1. Na příkazový řádek logické části B zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
2. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
3. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
4. Na náznak *Internetová adresa* zadejte '10.1.1.74'.
5. Na náznak *Popis linky* zadejte název popisu linky, například ETHLINE.
6. Na náznak *Maska podsítě* zadejte '255.255.255.252'.
7. Na náznak *Související lokální rozhraní* zadejte '10.1.1.15'. To přiřadí virtuální rozhraní k externímu rozhraní a povolí proxy ARP doručovat pakety mezi virtuálním rozhraním 10.1.1.74 a externím rozhraním 10.1.1.15.
8. Spusťte rozhraní. Na obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.

Další krok

Vytvořte přenosovou cestu.

Krok 7: Vytvořte přenosovou cestu.

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

1. Na příkazový řádek logické části A zadejte CFGTCP a stiskněte klávesu Enter.
2. Zadejte volbu 2 (Práce se směry TCP/IP) a stiskněte klávesu Enter.
3. Zadejte volbu 1 (Přidat)a stiskněte klávesu Enter.
4. Na náznak *Určení směru* zadejte *DFTROUTE.
5. Na náznak *Maska podsítě* zadejte *NONE.
6. Na náznak *Adresa dalšího přechodu* zadejte '10.1.1.74'.

   Pakety z logické části A jsou přenášeny přes virtuální síť typu Ethernet do rozhraní 10.1.1.74 pomocí této předvolené přenosové cesty. Protože je 10.1.1.74 asociováno s externím rozhraním proxy ARP 10.1.1.15, pokračují pakety dále z virtuální sítě typu Ethernet pomocí rozhraní proxy ARP.

Další krok

Ověřte síťové komunikace.

Krok 8: Ověřte síťové komunikace

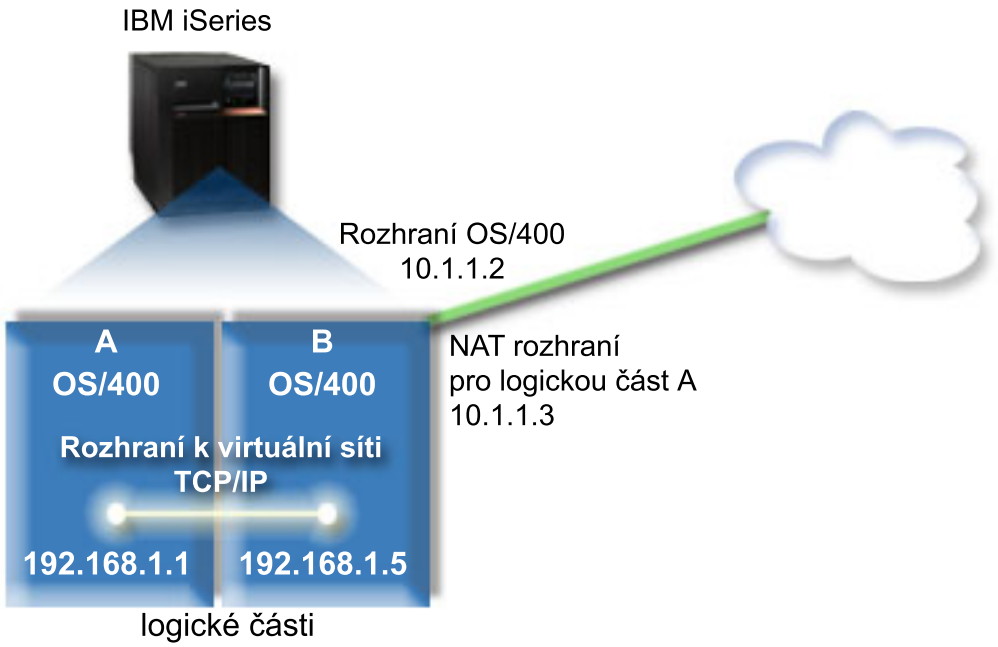
Ověřte funkčnost vaší síťové komunikace příkazem testování spojení (ping):

- Pomocí příkazu ping v logické části A otestujte spojení virtuálního rozhraní sítě Ethernet 10.1.1.74 a externího hostitelského systému.
- Z externího hostitelského systému OS/400 otestujte příkazem ping virtuální rozhraní Ethernet 10.1.1.73 a 10.1.1.74.

Metoda NAT (převod síťové adresy)

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. Jiné formy NAT, jako např. masquerade NAT je také možné použít za předpokladu, že vaše virtuální síť typu Ethernet nevyžaduje, aby byl přijímaný provoz iniciován externími klienty. Stejně jako u metod směrování TCP/IP a proxy ARP můžete využít vašeho existujícího síťového spojení OS/400. Protože budete používat pravidla paketu IP, musíte pro vytvoření a provedení těchto pravidel použít 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 a síť 192.168.1.*x* představuje virtuální síť typu Ethernet.



V tomto příkladu postupuje přes rozhraní 10.1.1.2 veškerý existující TCP/IP provoz serveru. Protože toto je scénář statické mapy, je příchozí provoz veden z rozhraní 10.1.1.3 do rozhraní 192.168.1.5. Odchozí provoz je veden z rozhraní 192.168.1.5 do externího rozhraní 10.1.1.3. Logická části A a logická část B používají ke komunikaci mezi sebou svá vlastní příslušná virtuální rozhraní 192.168.1.1 a 192.168.1.5.

Chcete-li zprovoznit statický NAT, musíte nejprve instalovat komunikace OS/400 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:

1. Povolte logickým částem stát se součástí virtuální sítě typu Ethernet.
2. Vytvořte popis linky sítě Ethernet.
3. Zapněte postoupení datagramu pomocí IP.
4. Vytvořte rozhraní.
5. Ověřte síťové komunikace.
6. Vytvořte pravidla paketu.
7. Ověřte síťové komunikace.

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

Poznámka: Pokud používáte servery jiné než servery modelu 270 nebo 8 *xx*, musíte provést tento krok s pomocí HMC (Hardware Management Console for eServer) namísto použití primární logické části. Podrobnosti najdete v tématu Virtuální síť typu Ethernet.

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

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a stiskněte klávesu Enter.
2. Zadejte vaše ID uživatele servisních nástrojů a heslo.
3. Na obrazovce SST (System Service Tools) vyberte volbu 5 (Práce s logickými částmi systému).
4. Na obrazovce Práce s logickými částmi systému vyberte volbu 3 (Práce s konfigurací logické části).
5. Stiskněte klávesu F10 (Práce s virtuální sítí typu 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.

Další krok

Vytvořte popis linky sítě Ethernet.

Krok 2: Vytvořte popis linky sítě 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 vašeho serveru.

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

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) 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 logickou částí zde bude jeden.
3. Na obrazovce Display Resource Detail 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 obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration descriptions) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* 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 asociované sítě typu Ethernet stejný název, můžete snadno sledovat konfiguraci virtuální sítě typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.
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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) vedle příslušného portu virtuální sítě typu Ethernet.

Porty typu Ethernet označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet zde bude jeden. Každý port označený jako 268C má asociovaný kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).

3. Na obrazovce Display Resource Detail posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro virtuální síť typu Ethernet.
4. Na obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* zadejte VETH0. Pokud použijete pro popisy linek a asociované sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace vašich virtuálních sítí typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.
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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

Krok 3: Zapněte postoupení datagramu pomocí IP.

Zapněte postoupení datagramu pomocí IP, takže pakety budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, použijte tento postup:

1. Na příkazový řádek logické části A zadejte CHGTCPA a stiskněte klávesu F4.
2. Na náznak *Postoupení datagramu IP* zadejte *YES.

Další krok

Vytvořte rozhraní.

Krok 4: Vytvořte rozhraní.

Při vytváření TCP/IP rozhraní postupujte takto:

1. V logické části B vytvořte a spusťte TCP/IP rozhraní operačního systému OS/400 pro příchozí a odchozí hlavní komunikaci serveru. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.

2. Vytvořte a spusťte další TCP/IP rozhraní, které naváže spojení s externí sítí. Mělo by použít stejný popis linky jako existující externí TCP/IP rozhraní. Toto rozhraní posléze provede převod adres logických částí. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.
3. V logické části A vytvořte a spusťte TCP/IP rozhraní operačního systému OS/400 pro virtuální síť typu Ethernet. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části A zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.
4. V logické části B vytvořte a spusťte TCP/IP rozhraní operačního systému OS/400 pro virtuální síť typu Ethernet. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části B zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.

Další krok

Ověřte síťové komunikace.

Krok 5: Ověřte síťové komunikace

Ověřte funkčnost vaší síťové komunikace příkazem testování spojení (ping):

- Z logické části A otestujte spojení rozhraní virtuální sítě typu Ethernet 192.168.1.5 a externího hostitele.
- Z externího hostitele OS/400 otestujte spojení rozhraní virtuální sítě typu Ethernet 192.168.1.1 a 192.168.1.5.

Další krok

Vytvořte pravidla paketu.

Krok 6: Vytvořte pravidla paketu.

Chcete-li vytvořit pravidla paketu mapující soukromou adresu umístěnou v logické části A na veřejnou adresu umístěnou 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 **iSeries server –> Síť–> Metody pro práci s IP**.
2. Klepněte pravým tlačítkem na položku **Pravidla paketu** a vyberte **Editor pravidel**.
3. Vyberte **Převod adresy** z menu **průvodce**.
4. Při vytváření pravidel paketu postupujte podle pokynů průvodce. Tato procedura zahrnuje výběr těchto položek:
   - Vyberte **Mapovat převod adresy.**
   - Zadejte soukromou IP 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** z menu **Soubor**.

Další krok

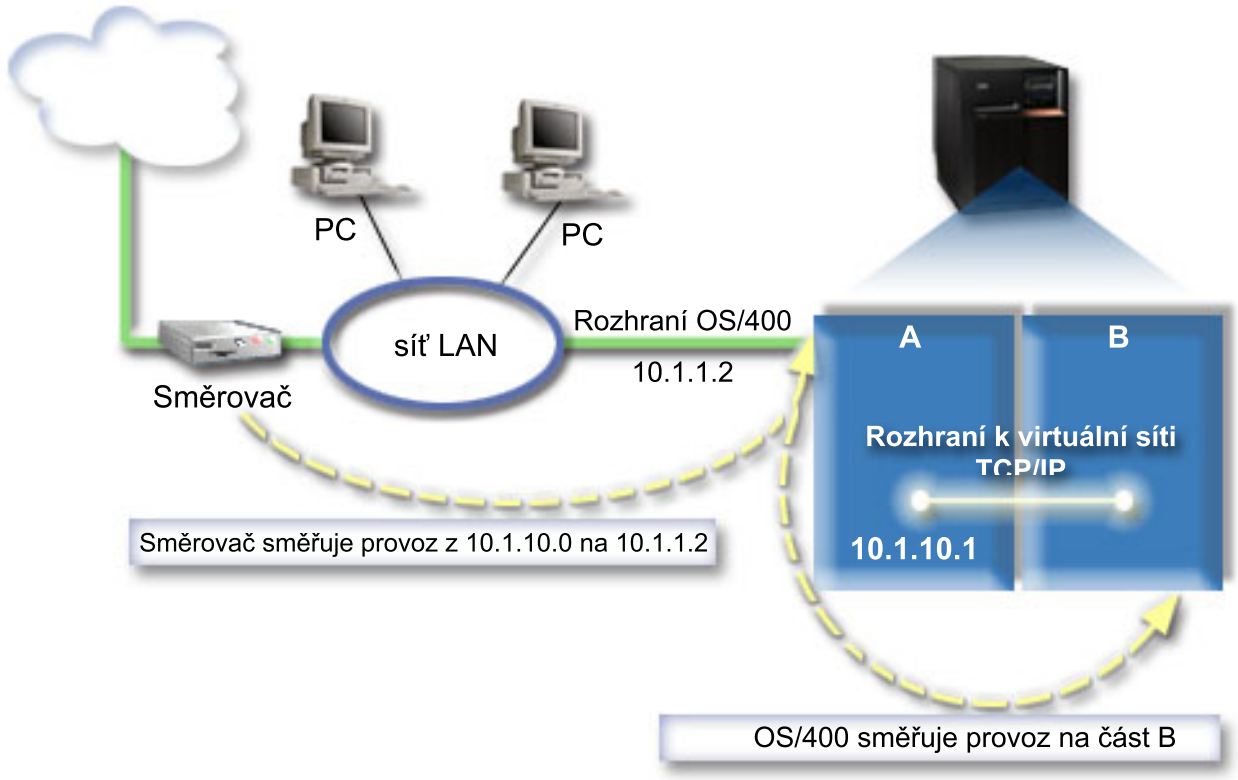
Ověřte síťové komunikace.

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

Přenosy můžete také směrovat na logické části různými způsoby přes server iSeries. Toto řešení není obtížné z hlediska konfigurace,ale jeho implementace nemusí být vhodná vzhledem k topologii vaší sítě. Prohlédněte si tento obrázek.



Existující TCP/IP rozhraní (10.1.1.2) naváže spojení se sítí LAN. Síť LAN je spojena se vzdálenou sítí pomocí směrovače. Virtuální TCP/IP rozhraní 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. Pokud v operačním systému OS/400 zapnete postoupení datagramu pomocí IP, bude operační systém OS/400 směrovat IP pakety na logickou část B a z logické části B. Když definujete spojení TCP/IP pro logickou část B, musí být adresa směrovače 10.1.10.1.

Úskalí tohoto typu směrování spočívá v doručení IP paketů na server iSeries. V tomto scénáři by bylo možné definovat přenosovou cestu na směrovači tak, že by byly pakety určené pro síť 10.1.10.0 posílány do rozhraní 10.1.1.2. Toto je možné u vzdálených síťových klientů. Také by to bylo možné u klientů lokální sítě typu LAN (klientů spojených se stejnou sítí LAN jako server iSeries) pokud by rozpoznaly stejný směrovač jako svůj následující směrovací uzel. Pokud jej nerozpoznají, musí mít každý klient přenosovou cestu směrující provoz 10.1.10.0 na rozhraní operačního systému OS/400 10.1.1.2. V tom spočívá nepraktičnost této metody. Pokud máte klientů LAN mnoho, musíte definovat mnoho přenosových cest.

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

1. Povolte logickým částem stát se součástí virtuální sítě typu Ethernet.
2. Vytvořte popis linky sítě Ethernet.
3. Zapněte postoupení datagramu pomocí IP.
4. Vytvořte rozhraní.

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

Poznámka: Pokud používáte servery jiné než servery modelu 270 nebo 8 *xx*, musíte provést tento krok s pomocí HMC (Hardware Management Console for eServer) namísto použití primární logické části. Podrobnosti najdete v tématu Virtuální síť typu Ethernet.

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

1. Na příkazový řádek primární logické části (logická část A) zadejte STRSST a stiskněte klávesu Enter.
2. Zadejte vaše ID uživatele servisních nástrojů a heslo.
3. Na obrazovce SST (System Service Tools) vyberte volbu 5 (Práce s logickými částmi systému).
4. Na obrazovce Práce s logickými částmi systému vyberte volbu 3 (Práce s konfigurací logické části).
5. Stiskněte klávesu F10 (Práce s virtuální sítí typu 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.

Další krok

Vytvořte popis linky sítě Ethernet.

Krok 2: Vytvořte popis linky sítě 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 vašeho serveru.

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

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) 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 logickou částí zde bude jeden.
3. Na obrazovce Display Resource Detail 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 obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration descriptions) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* 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 asociované sítě typu Ethernet stejný název, můžete snadno sledovat konfiguraci virtuální sítě typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.

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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

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

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

1. Na příkazový řádek logické části A zadejte WRKHDWRSC *CMN a stiskněte klávesu Enter.
2. Na obrazovce Work with Communication Resources vyberte volbu 7 (Display resource detail) vedle příslušného portu virtuální sítě typu Ethernet.

   Porty typu Ethernet označené jako 268C jsou prostředky virtuální sítě typu Ethernet. Pro každý adaptér typu Ethernet zde bude jeden. Každý port označený jako 268C má asociovaný kód umístění, který je vytvořen při vytvoření virtuálního adaptéru typu Ethernet pomocí konzole HMC (Krok 1).
3. Na obrazovce Display Resource Detail posuňte kurzor svisle tak, aby se zobrazil prostředek 268C, který je přiřazený ke specifickému kódu umístění vytvořenému pro virtuální síť typu Ethernet.
4. Na obrazovce Work with Communication Resources vyberte volbu 5 (Work with configuration) vedle příslušného portu virtuální sítě typu Ethernet a stiskněte klávesu Enter.
5. Na obrazovce Work with Configuration Descriptions vyberte volbu 1 (Create) a stiskněte klávesu Enter. Objeví se obrazovka CRTLNIETH (Create Line Description Ethernet).
   a. Na náznak *Line description* zadejte VETH0. Pokud použijete pro popisy linek a asociované sítě typu Ethernet stejný název, jako například VETHO, můžete snadno sledovat konfigurace vašich virtuálních sítí typu Ethernet.
   b. Na náznak *Line speed* zadejte 1G.
   c. Na náznak *Duplex* zadejte *FULL a stiskněte klávesu Enter.
   d. Na náznak *Maximum frame size* zadejte 8996 a 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 vyberte volbu 1 (Vary on) pro VETH0.
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 mohou být názvy popisu linek libovolné, je užitečné používat stejné názvy pro všechny popisy linek asociovaných s virtuální sítí typu Ethernet. V tomto scénáři jsou všechny popisy linek pojmenovány VETHO.

Další krok

Zapněte postoupení datagramu pomocí IP.

Krok 3: Zapněte postoupení datagramu pomocí IP.

Zapněte postoupení datagramu pomocí IP, takže pakety budou moci být doručovány mezi různými podsítěmi.

Chcete-li zapnout volbu postoupení datagramu pomocí IP, použijte tento postup:

1. Na příkazový řádek logické části A zadejte CHGTCPA a stiskněte klávesu F4.
2. Na náznak *Postoupení datagramu IP* zadejte *YES.

Další krok

Vytvořte rozhraní.

Krok 4: Vytvořte rozhraní.

Při vytváření TCP/IP rozhraní postupujte takto:

1. Vytvořte TCP/IP rozhraní operačního systému OS/400 v logické části A. Při vytváření rozhraní postupujte takto:
   a. Na příkazový řádek logické části A zadejte CFGTCP a stiskněte klávesu Enter. Objeví se obrazovka Konfigurace TCP/IP.
   b. Zadejte volbu 1 (Práce s TCP/IP rozhraními) a stiskněte klávesu Enter.
   c. Zadejte volbu 1 (Přidat) a stiskněte klávesu Enter. Objeví se obrazovka ADDTCPIFC (Přidání TCP/IP rozhraní).
   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 obrazovce Práce s TCP/IP rozhraními vyberte volbu 9 (Start) vedle příslušného rozhraní.
3. Opakujte kroky 2 a 3, kterými vytvoříte a spustíte TCP/IP rozhraní 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 pro 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. To vám umožní vytvořit vysokorychlostní komunikaci mezi logickými částmi bez nutnosti koupě dalšího hardwaru. 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 Mbps a 100 Mbps 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 vlastnost je obzvláště potřebná, pokud používáte logické části s operačním systémem Linux jako hostitelský systém pro aplikace ochranné bariéry.
- 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, jestli jsou logické části provozovány pod operačním systémem OS/400 nebo Linux, mohou být všechny připojeny do stejné virtuální sítě 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.

«

Kapitola 9. Související informace k nastavení TCP/IP

Nyní, když je server nastaven a v provozu, se možná budete ptát: ″Co dalšího bych mohl se serverem udělat?″ Níže jsou uvedeny příručky a červené knihy IBM (ve formátu PDF) a témata v aplikaci Information Center, která souvisejí s tématem Nastavení TCP/IP. Soubory PDF můžete prohlížet nebo tisknout. Chcete-li využít všech výhod TCP/IP na serveru iSeries, prostudujte si následující odkazy:

Manuály

- **TCP/IP Configuration and Reference** (zhruba 592 KB)
  Tato publikace nabízí informace o konfigurování TCP/IP (Transmission Control Protocol/Internet Protocol) a o provozu a správě sítě.

- **Rady a nástroje pro zabezpečení serveru iSeries** (asi 1 MB)
  Tato publikace obsahuje základní doporučení k používání funkcí zabezpečení dat serveru iSeries k ochraně serveru a k provádění souvisejících činností.

Červené knihy

- **TCP/IP Tutorial and Technical Overview** (zhruba 7 MB)
  Tato červená kniha obsahuje informace o základech TCP/IP.

- **TCP/IP for AS/400: More Cool Things Than Ever** (zhruba 9 MB)
  Tato červená kniha obsahuje rozsáhlý seznam běžných aplikací a služeb TCP/IP.

IPv6

- **IETF (Internet Engineering Task Force)** (http://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.

- **Fórum o IPv6**(http://www.ipv6forum.com/)
  Zde najdete nové články a akce poskytující informace o nejnovějším vývoji IPv6.

Jiné informace

- **TCP/IP**
  Toto téma obsahuje informace o aplikacích a službách TCP/IP, které jsou za hranicemi rozsahu poskytovaného konfigurací.

K uložení PDF souboru na svou pracovní stanici za účelem prohlížení a tisku použijte tento postup:

1. Klepněte pravým tlačítkem myši v prohlížeči na odkaz na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na **Save Target As... (Uložit cíl jako...)**.
3. Vyhledejte adresář, do kterého chcete PDF soubor uložit.
4. Klepněte na **Save** (Uložit).

K prohlížení nebo tisku těchto souborů ve formátu PDF potřebujete program Adobe Acrobat Reader. Jeho kopii si můžete stáhnout webových stránek společnosti Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Část 2. Dodatky

Dodatek. Upozornění

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 49XA
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.

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

Ochranné známky

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

AS/400
e(logo)server
eServer
IBM
iSeries
OS/400
Redbooks

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation 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 pro stahování a tisk publikací

Oprávnění k používání informací, které jste se rozhodli stáhnout, závisí na níže uvedených ustanoveních a podmínkách a na vašem potvrzení, že je akceptujete.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto informace kopírovat pro své osobní nekomerční použití. Tyto informace 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 informace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto informací 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 informace a veškerá data, software a další duševní vlastnictví obsažené v těchto informacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání informací poškozuje její zájmy, nebo když zjistí, 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 NEPŘEBÍRÁ ŽÁDNÉ ZÁRUKY OHLEDNĚ OBSAHU TĚCHTO INFORMACÍ. INFORMACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS) A BEZ JAKÝCHKOLI ZÁRUK VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL.

Stažením nebo vytištěním informací z tohoto serveru vyjadřujete svůj souhlas s těmito ustanoveními a podmínkami.

Vytištěno v Dánsku společností IBM Danmark A/S.