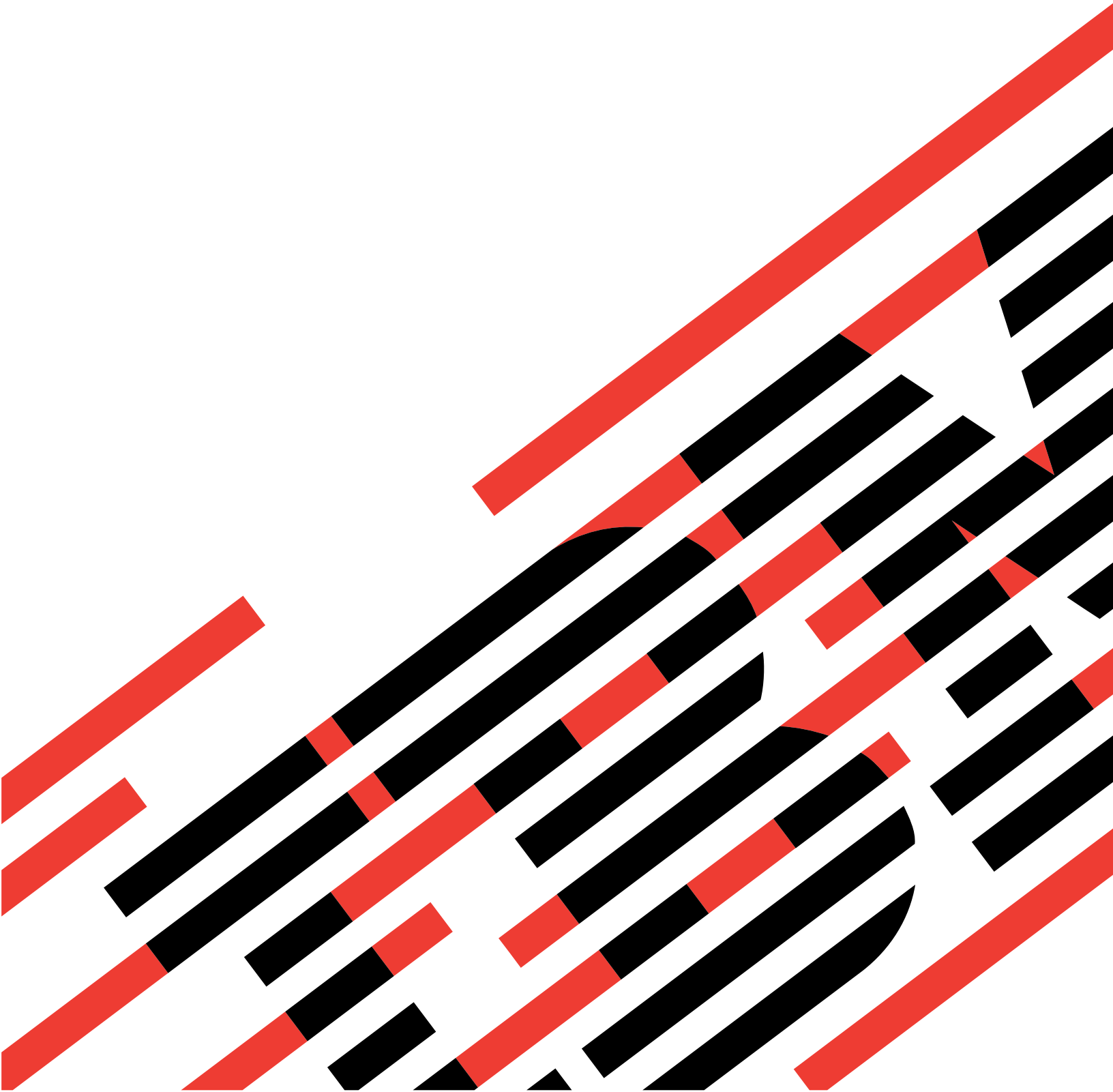
IBM

eserver

iSeries

Nastavenie TCP/IP pri tvorbe siete



IBM

@server

iSeries

Nastavenie TCP/IP pri tvorbe siete

Obsah

Časť 1. Nastavenie TCP/IP

Práve vám priviezli server iSeries a vy sa neviete dočkať, kedy spustíte jeho prevádzku. Táto časť vám prináša nástroje a procedúry pre nastavenie pripojenia a konfiguráciu TCP/IP na serveri iSeries. Po vykonaní týchto počiatočných krokov budete pripravený aplikáciami rozšíriť TCP/IP a vyhovieť tak svojim jedinečným potrebám.

Čo je nové vo V5R2?
Zistite viac o nových a zmenených funkciách TCP/IP.

Tlač tejto témy
V tejto si téme môžete vytlačiť, alebo stiahnuť dokumentáciu k nastaveniu TCP/IP vo formáte Portable Document Format (PDF).

Internetový protokol verzie 6 (IPv6)
Nový internetový protokol IPv6 hrá kľúčovú úlohu v budúcnosti internetu a môžete ho používať aj na serveri iSeries. Táto téma vám poskytuje všeobecné informácie o IPv6 a o tom, ako je protokol IPv6 implementovaný na serveri iSeries.

Plánovanie nastavenia TCP/IP
Táto téma vám pomôže pripraviť inštaláciu a konfiguráciu TCP/IP na serveri iSeries. Sú tu uvedené základné požiadavky pre inštaláciu a konfiguráciu, takže keď začnete konfigurovať TCP/IP, budete mať všetky potrebné informácie po ruke. Nájdete tu aj odkazy na podobné výrazy a koncepty.

Inštalácia TCP/IP
Nechajte sa sprevádzať inštaláciou produktov, ktoré pripravia prevádzku vášho servera iSeries.

Konfigurácia TCP/IP
Ukážeme vám, ako zapojíte svoj server iSeries a nakonfigurujete TCP/IP. Na dôvažok si prezrite aj inštrukcie o konfigurácii IPv6.

Prispôsobte si TCP/IP pomocou produktu iSeries Navigator
V tejto téme nájdete možnosti prispôsobenia pomocou produktu iSeries Navigator.

Odstraňovanie problémov s TCP/IP
Ak zaznamenáte akékoľvek problémy s pripojením, alebo prevádzkou TCP/IP, pomoc s ich riešením nájdete v časti Odstraňovanie problémov s TCP/IP. Tento sprievodca odstraňovaním problémov vám pomôže vyriešiť problémy spojené s IPv4 aj s IPv6.

Informácie, týkajúce sa nastavenia TCP/IP
Táto téma odpovedá na otázku ″Čo viac dokáže?″ Nájdete tu odkazy na služby a aplikácie, ktoré vám vylepšia výkon servera.

Kapitola 1. Čo je nové vo V5R2?

Téma o nastavení TCP/IP obsahuje vo vydaní 2 verzii 5 tieto nové položky:

- **Konfigurujte TCP/IP pomocou znakového rozhrania**
  Tu nájdete inštrukcie o nastavení TCP/IP pre zákazníkov, ktorí musia na konfiguráciu svojich serverov používať znakové rozhranie. Odporúčaná metóda nastavovania TCP/IP je metóda s pomocou Sprievodcu nastavením EZ; ak však chcete použiť iSeries Navigator z počítača, ktorý vyžaduje pred spustením produktu iSeries Navigator, bežnú konfiguráciu TCP/IP, musíte na vykonanie tejto konfigurácie použiť znakové rozhranie.
- **Internetový protokol verzie 6 (IPv6)**
  Zoznámte sa so základnými informáciami o IPv6 a zistite, ako sa implementuje na server iSeries.
- **Konfigurácia IPv6**
  Tu nájdete požiadavky na nastavenie a inštrukcie o konfigurácii servera na IPv6.
- **Prispôsobte si TCP/IP pomocou produktu iSeries Navigator**
  Táto téma bola rozšírená. Nájdete v nej nové spôsoby, ako si prispôsobiť konfiguráciu TCP/IP. Na konfiguráciu IPv6 a na vytvorenie nových rozhraní a trás použite nových sprievodcov, nových sprievodcov v produkte iSeries.

Ďalšie informácie o tom, čo je zmenené, alebo pridané v tomto vydaní, nájdete v Odkaz užívateľom .

Kapitola 2. Tlač tejto témy

Dokumentáciu vo formáte typu PDF si môžete stiahnuť, alebo prezrieť, ak kliknete na Nastavenie TCP/IP (asi 326 KB, alebo 41 strán).

Ak si chcete formát PDF uložiť na svojej pracovnej stanici s cieľom prezerania alebo tlače:

1. Vo svojom prehliadači kliknite pravým tlačidlom myši na PDF (hore uvedená linka).
2. Kliknite na **Save Target As...**.
3. Prejdite do adresára, do ktorého chcete uložiť PDF súbor.
4. Kliknite na **Save**.

Stiahnutie programu Adobe Acrobat Reader

Ak na prezeranie alebo tlač týchto PDF potrebujete Adobe Acrobat Reader, môžete si ho stiahnuť z jeho internetovej stránky (www.adobe.com/prodindex/acrobat/readstep.html)  .

Kapitola 3. Internetový protokol verzie 6 (IPv6)

Internetový protokol verzie 6 (IPv6) je aktualizovanou verziou Internetového protokolu verzie 4 (IPv4) a ako internetový štandard ho postupne nahrádza.

Zaujímate sa, ako použiť IPv6 pri vylepšení obchodov svojej firmy, alebo ste možno programátor, ktorý chce vytvoriť aplikáciu IPv6, aby mohla vaša firma používať výhody vylepšeného internetového protokolu. V týchto témach nájdete základné informácie o IPv6 a o tom, ako ho používať na serveri iSeries:

Čo je to IPv6?
Zistite, ako sa IPv6 stáva internetovým štandardom namiesto IPv4 a ako to môžete využiť vo svoj prospech.

Aké funkcie IPv6 sú dostupné?
Naučte sa, ako sa IPv6 implementuje na serveroch iSeries.

Scenáre IPv6
Pomocou príkladov spoznajte situácie, v ktorých používate IPv6 pri svojom podnikaní.

Koncepty IPv6
Spoznajte základné koncepty IPv6. Ak neviete, aké sú rozdiely medzi IPv4 a IPv6, prezrite si detailnejšie porovnanie, napríklad ako sa adresy IPv4 a IPv6 prirovnávajú jedna k druhej, alebo ako sa hlavičky paketov IPv4 líšia od hlavičiek paketov IPv6.

Konfigurácia IPv6
Zistite, aké sú hardvérové a softvérové požiadavky a inštrukcie na konfiguráciu IPv6 na svojom serveri.

Odstraňovanie problémov s IPv6
Nájdete tu riešenia problémov s IPv6.

Informácie, týkajúce sa IPv6
Linky na zdroje, ktoré vám pomôžu pochopiť IPv6.

Čo je to IPv6?

Internetový protokol verzie 6 (IPv6) je novým krokom vo vývoji internetových protokolov. Na väčšine internetu sa teraz používa IPv4, ktorý bol spoľahlivým a odolným viac než 20 rokov. Má však niekoľko obmedzení, ktoré s rozširovaním internetu spôsobujú čoraz viac problémov.

Ide najmä o rastúci nedostatok adries IPv4, ktoré sú potrebné pre všetky nové zariadenia na internete. Kľúčom k vylepšeniu IPv6 je rozšírenie IP adresy z 32 bitov na 128 bitov, a teda povolenie virtuálne neobmedzenej jedinečnej IP adresy. Nový textový formát IP adresy je:

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

kde je každé x hexadecimálnou číslicou reprezentujúcou 4 bity.

Možnosti IPv6 v rozšírenom adresovaní poskytujú riešenie problému vyčerpania IP adries. Je to dôležité najmä preto, že čoraz viac ľudí používa mobilné počítače, mobilné telefóny a vreckové počítače. Rastúci dopyt bezdrôtových užívateľov viedol k vyčerpaniu adries IPv4. Možnosť rozšírenia IP adresy v IPv6 tento problém rieši tým, že poskytne IP adresy pre rastúci počet bezdrôtových zariadení.

Na dôvažok k týmto adresným možnostiam poskytuje IPv6 nové funkcie, ktoré zjednodušujú konfiguráciu a spravovanie adries v sieti. Konfigurácia a údržba sietí je náročná práca. Automatizáciou niekoľkých úloh sieťového administrátora redukuje IPv6 časť pracovného zaťaženia.

Ak sa rozhodnete použiť IPv6, nebudete pri prechode k inému poskytovateľovi internetových služieb (ISP) musieť prečíslovať adresy svojich zariadení. Budete si môcť ponechať svoje adresy, pretože sú jedinečné v celosvetovom rozsahu.

Autokonfiguračná vlastnosť IPv6 vám automaticky nakonfiguruje adresy rozhraní a smerovačov. V autokonfigurácii bezstavovej adresy vezme IPv6 adresu MAC počítača a prefix siete, ktorý mu poskytne lokálny uzol, a kombináciou týchto dvoch adries vytvorí novú, jedinečnú adresu IPv6. Táto vlastnosť eliminuje potrebu servera DHCP, čo ušetrí čas administrátorovi a peniaze firme.

Viac zdrojov informácií o IPv6 nájdete v téme Informácie, týkajúce sa IPv6

V časti Aké funkcie IPv6 sú dostupné? nájdete informácie o IPv6 spojené konkrétne so serveromiSeries.

Aké funkcie IPv6 sú dostupné?

IBM implementuje IPv6 na serveri iSeries v rámci niekoľkých softvérových vydaní. IPv6 je momentálne implementovaný na platforme vývoja aplikácií s cieľom vývoja a testovania aplikácií IPv6. Funkcie IPv6 sú pre existujúce aplikácie TCP/IP transparentné a existujú súčasne s funkciami IPv4.

Toto sú najdôležitejšie funkcie servera iSeries ovplyvnené protokolom IPv6:

- **Konfigurácia**
  Uvedomte si, že proces konfigurácie IPv6 je odlišný, než proces konfigurácie IPv4. Ak chcete používať funkcie IPv6, musíte nakonfigurovaním linky pre IPv6 zmeniť TCP/IP konfiguráciu servera. IPv6 môžete konfigurovať na linke Ethernet, alebo tunel.

  Ak nakonfigurujete linku Ethernet na prenos IPv6, zasielate sieťou IPv6 pakety IPv6. V časti Vytvorenie lokálnej siete (LAN) IPv6 nájdete scenár popisujúci situáciu, v ktorej linku Ethernet konfigurujete na IPv6.

  Ak konfigurujete tunelové linky, posielate pakety IPv6 existujúcou sieťou IPv4. Scenáre Zasielanie paketov IPv6 lokálnou sieťou (LAN) IPv4 a Zasielanie paketov IPv6 rozšírenou sieťou (WAN) IPv4 opisujú dve situácie, v ktorých by ste vytvárali tunelovú linku konfigurovanú na IPv6.

  Pozrite si v časti Konfigurácia IPv6, ako nakonfigurovať svoju sieť na IPv6.
- **Sokety**
  Vyviňte a otestujte soketové aplikácie používajúce nástroje API IPv6. IPv6 zdokonalí sokety, takže aplikácia bude môcť používať IPv6 s novou rodinou adries: AF_INET6. Tieto vylepšenia neovplyvňujú už existujúce aplikácie IPv4. Môžete vytvoriť aplikácie, ktoré súbežne podporujú prenosy IPv4 a IPv6, alebo len prenos IPv6. Viac informácií o IPv6 pre sokety nájdete v časti Použitie rodiny adries AF_INET6.
- **DNS**
  Systém názvov domén (DNS) podporuje adresy AAAA a nové domény pre spätné vyhľadávanie: IP6.ARPA. Hoci DNS získa informáciu IPv6, musí server na komunikáciu s DNS použiť IPv4.
- **Odstraňovanie problémov s TCP/IP**
  Použite štandardné nástroje na odstraňovanie problémov, ako sú PING, netstat, sledovanie trás a komunikácií pre siete a tunely IPv6. Tieto nástroje teraz podporujú adresný formát IPv6. V časti Odstraňovanie problémov s TCP/IP nájdete pomoc pri riešení problémov so sieťami IPv4 aj IPv6.

Pre prostriedky IPv6 si pozrite Informácie súvisiace s IPv6.

Scenáre: IPv6

V nasledujúcich scenároch môžete lepšie pochopiť, prečo implementovať IPv6 a ako v každej zo situácií nastaviť svoju sieť:

- Vytvorenie lokálnej siete (LAN) IPv6
- Zasielanie paketov IPv6 lokálnou sieťou (LAN) IPv4
- Zasielanie paketov IPv6 rozšírenou sieťou (WAN) IPv4

Poznámka: V týchto scenároch IP adresy 10.x.x.x reprezentujú verejné IP adresy. Všetky adresy sú v scenároch uvedené len ako príklady.

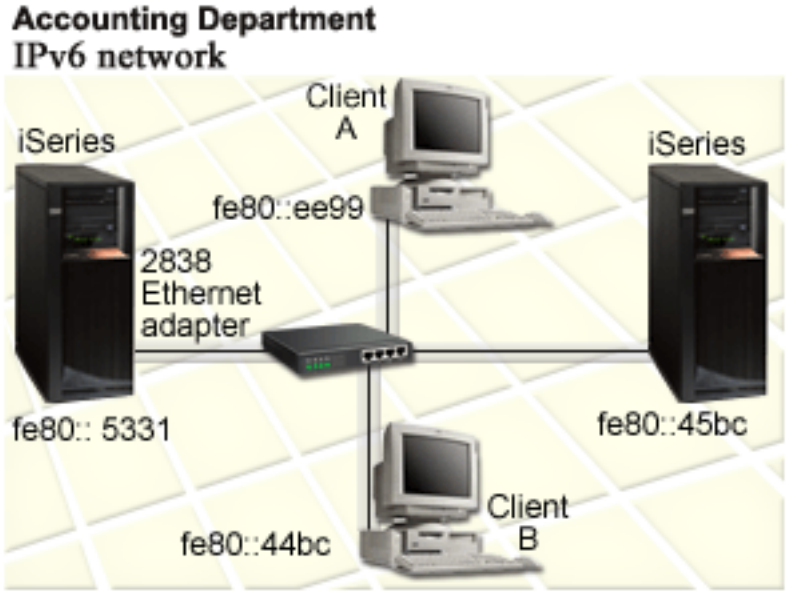
Pozrite si v časti Konfigurácia IPv6, ako nakonfigurovať svoj server na IPv6.

V časti Koncepty IPv6 nájdete definície základných konceptov IPv6.

Vytvorenie lokálnej siete (LAN) IPv6

Situácia

Internetový štandard IPv4 bude nakoniec nahradený protokolom IPv6. Preto sa vaša firma rozhodla implementovať na svoje finančné operácie IPv6 a zakúpiť si novú účtovnú aplikáciu, ktorá na pripájanie využíva IPv6. Táto aplikácia sa potrebuje pripájať k ďalšej svojej inštancii umiestnenej na inom serveri, ktorý je zapojený v lokálnej sieti (LAN) Ethernet. Vašou úlohou je nakonfigurovať server na IPv6, aby mohla vaša firma začať používať účtovnú aplikáciu. Nasledujúci obrázok popisuje nastavenie siete v tomto scenári.



Riešenie

Ak chcete vytvoriť IPv6 LAN, musíte nakonfigurovať opis linky Ethernet na IPv6. Keďže zamestnanci používajú účtovnú aplikáciu, cestujú pakety IPv6 medzi serverom iSeries a klientmi na sieti.

Požiadavky nastavenia:

- OS/400, verzia 5, vydanie 2, alebo vyššie
- Ethernet adaptéry 2838, alebo 2849, keďže toto sú zatiaľ jediné typy hardvérových prostriedkov podporované IPv6.
- iSeries Access pre Windows a iSeries Navigator (sieťový komponent produktu iSeries Navigator)
- Server musí mať osobitné fyzické rozhranie IPv4 nakonfigurované skôr, než budete konfigurovať linku Ethernet IPv6, pretože na serveri už vtedy musí byť spustené TCP/IP. Ak ste server IPv4 nekonfigurovali, pozrite si skôr, než budete konfigurovať linku pre IPv6, Prvá konfigurácia TCP/IP.

Konfigurácia

Na konfiguráciu opisu linky Ethernet pre IPv6 musíte použiť sprievodcu **Konfigurácia IPv6** v produkte iSeries Navigator. IPv6 môže byť konfigurované len z produktu iSeries Navigator a nemôže byť konfigurované zo znakového rozhrania.

Sprievodca požaduje názov hardvérového komunikačného prostriedku na serveri, na ktorom budete IPv6 konfigurovať; napríklad CMN01. Musí to byť Ethernet adaptér 2838, alebo 2849, ktorý zatiaľ nie je konfigurovaný na IPv4.

Pri použití sprievodcu **Konfigurácia IPv6**, nasledujte tieto kroky:

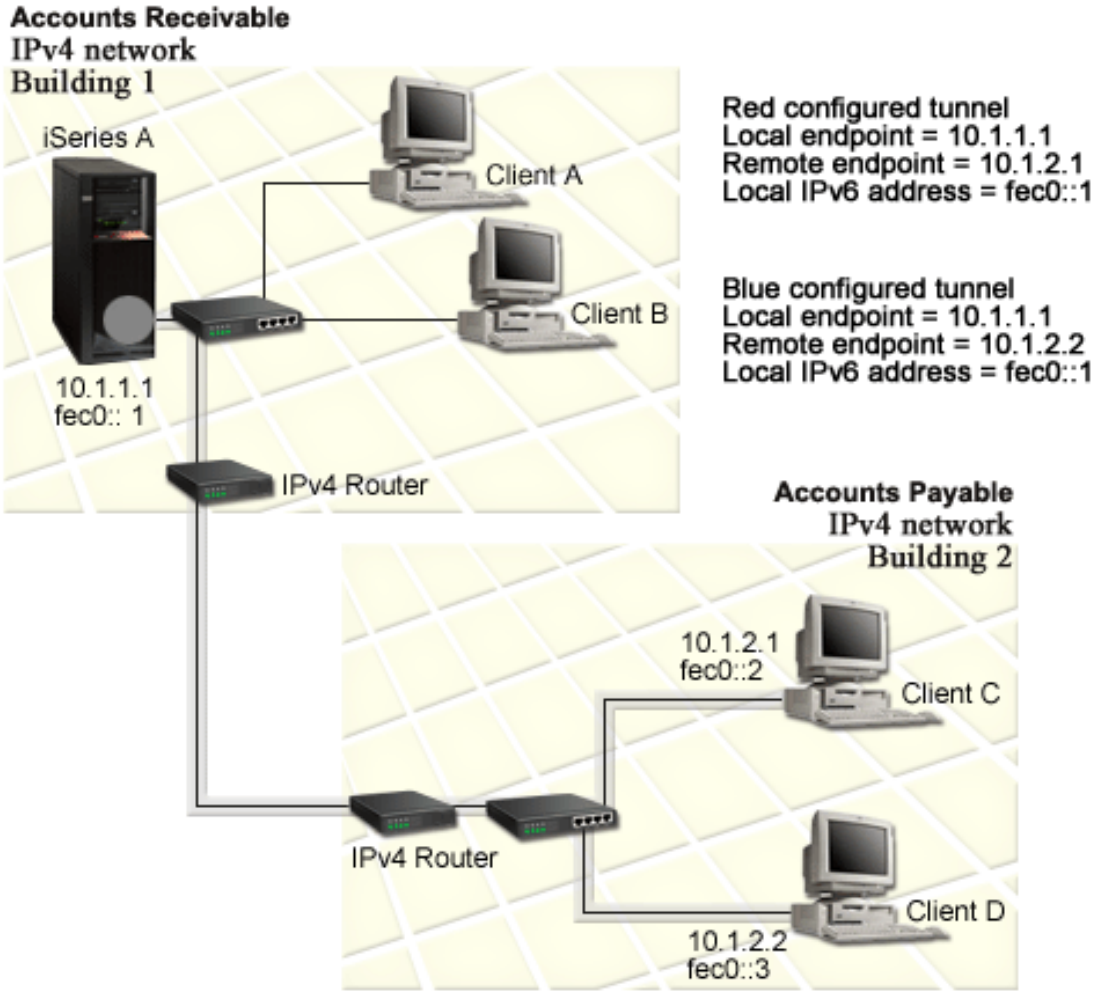
1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP**.
2. Kliknite pravým tlačidlom myši na **IPv6**, vyberte **Konfigurácia IPv6** a podľa inštrukcií sprievodcu nakonfigurujte linku Ethernet pre IPv6.

Zasielanie paketov IPv6 lokálnou sieťou (LAN) IPv4

Situácia

Vaša firma napísala novú účtovnú aplikáciu pre IPv6. Je to aplikácia typu klient-server, ktorú budete používať lokálne. Táto aplikácia komunikuje s ďalšími inštanciami umiestnenými v tej istej lokalite, ale v iných budovách a sieťach LAN. Hoci chce vaša firma pre túto aplikáciu použiť IPv6, nie je ešte pripravená zmeniť celú infraštruktúru z IPv4 na IPv6. Vašou úlohou je nakonfigurovať tunelové linky IPv6, ktoré umožňujú paketom IPv6 presúvať sa lokálnymi sieťami IPv4. Nasledujúci obrázok popisuje nastavenie siete

v tomto scenári.



Riešenie

Aby ste v týchto lokálnych sieťach IPv4 mohli používať IPv6, musíte vytvoriť dva konfigurované tunely a niekoľko prepojených trás. Pre účely tohto príkladu je jeden tunel zvýraznený červenou a druhý modrou farbou.

Najprv sa zamerajme na červený tunel:

- Červený tunel sa začína na serveri iSeries A (lokálny koncový bod 10.1.1.1) v Budove 1 a končí sa na Klientovi C (vzdialený koncový bod 10.1.2.1) v Budove 2.
- Server iSeries A zapuzdrí paket IPv6 do paketu IPv4 a zašle ho tunelom Klientovi C, ktorý ho odpuzdrí, takže sa môže pripojiť k ďalšej inštancii aplikácie IPv6.

Ďalej sa zamerajme na modrý tunel:

- Modrý tunel sa začína na serveri iSeries A (lokálny koncový bod 10.1.1.1) v Budove 1, rovnako ako červený tunel; modrý tunel sa však končí na Klientovi D (vzdialený koncový bod 10.1.2.2) v Budove 2.
- Server iSeries A zapuzdrí paket IPv6 do paketu IPv4 a zašle ho tunelom Klientovi D, ktorý ho odpuzdrí, takže sa môže pripojiť k ďalšej inštancii aplikácie IPv6.

Každé pripojenie tunelom je pripojením typu point-point, takže musíte pre každý tunel definovať vzdialený koncový bod. To dosiahnete vytvorením dvoch trás. Každá z nich je pripojená k rovnakému tunelu, ale ako ďalší skok definujú iný vzdialený koncový bod. Inými slovami, vzdialené koncové body každého tunela definujete pri vytváraní trás.

Okrem vytvorenia úvodných trás, ktoré definujú koncové body tunela a povoľujú paketom dosiahnuť klientov v Budove 2, musíte vytvoriť ešte dve trasy, aby sa pakety mohli vrátiť na server do Budovy 1.

Požiadavky nastavenia:

- OS/400 verzia 5 vydanie 2, alebo vyššie
- iSeries Access pre Windows a iSeries Navigator (sieťový komponent produktu iSeries Navigator)
- TCP/IP (s použitím IPv4) musí byť na serveri nakonfigurované skôr, než budete vytvárať konfigurovanú tunelovú linku. Ak ste server IPv4 nekonfigurovali, pozrite si skôr, než budete konfigurovať linku pre IPv6, Prvá konfigurácia TCP/IP.

Konfigurácia

Pri konfigurácii tunelovej linky musíte použiť sprievodcu **Konfigurácia IPv6** a sprievodcu **Nová trasa IPv6** v produkte iSeries Navigator. IPv6 môže byť konfigurované len z produktu iSeries Navigator a nemôže byť konfigurované zo znakového rozhrania.

Pri vytváraní červenej tunelovej linky pomocou sprievodcu **Konfigurácia IPv6** nasledujte tieto kroky:

1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP**.
2. Kliknite pravým tlačidlom myši na **IPv6**, vyberte sprievodcu **Konfigurácia IPv6** a podľa inštrukcií sprievodcu nakonfigurujte tunelovú linku pre IPv6. Po skončení vás sprievodca **Konfigurácia IPv6** vyzve, aby ste pre konfigurovanú tunelovú linku vytvorili novú trasu a objaví sa dialógové okno sprievodcu **Nová trasa IPv6**. Musíte ju vytvoriť, aby ste povolili prenos paketov IPv6 červeným tunelom.
3. Sprievodcom **Nová trasa IPv6** vytvorte trasu pre červený tunel. Ako ďalší skok zadajte vzdialený koncový bod 10.1.2.1 a ako cieľovú adresu zadajte fec0::2.

Znova použite sprievodcu **Nová trasa IPv6** a vytvorte trasu pre modrý tunel. Všimnite si, že sprievodcom netreba vytvárať **Konfigurácia IPv6** aj modrý tunel. Tento sa vytvorí, keď pomocou sprievodcu **Nová trasa IPv6** zadefinujete jeho vzdialený koncový bod. Pri použití sprievodcu **Nová trasa IPv6** nasledujte tieto kroky:

1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP —> IPv6**.
2. Kliknite pravým tlačidlom myši na **Trasy**, vyberte **Nová trasa** a podľa inštrukcií sprievodcu nakonfigurujte trasu IPv6 pre modrý tunel. Ako ďalší krok zadajte vzdialený koncový bod 10.1.2.2 a ako cieľovú adresu zadajte fec0::3.

Po tom, čo ste vytvorili konfigurované tunelové linky a trasy, ktoré určujú ich koncové body, musíte vytvoriť trasu na Klienta C a trasu na Klienta D, ktoré povolia paketom presunúť sa späť na server v Budove 1. Pre každú z týchto trás by ste mali zadať 10.1.1.1 ako ďalší skok a fec0::1 ako cieľovú adresu.

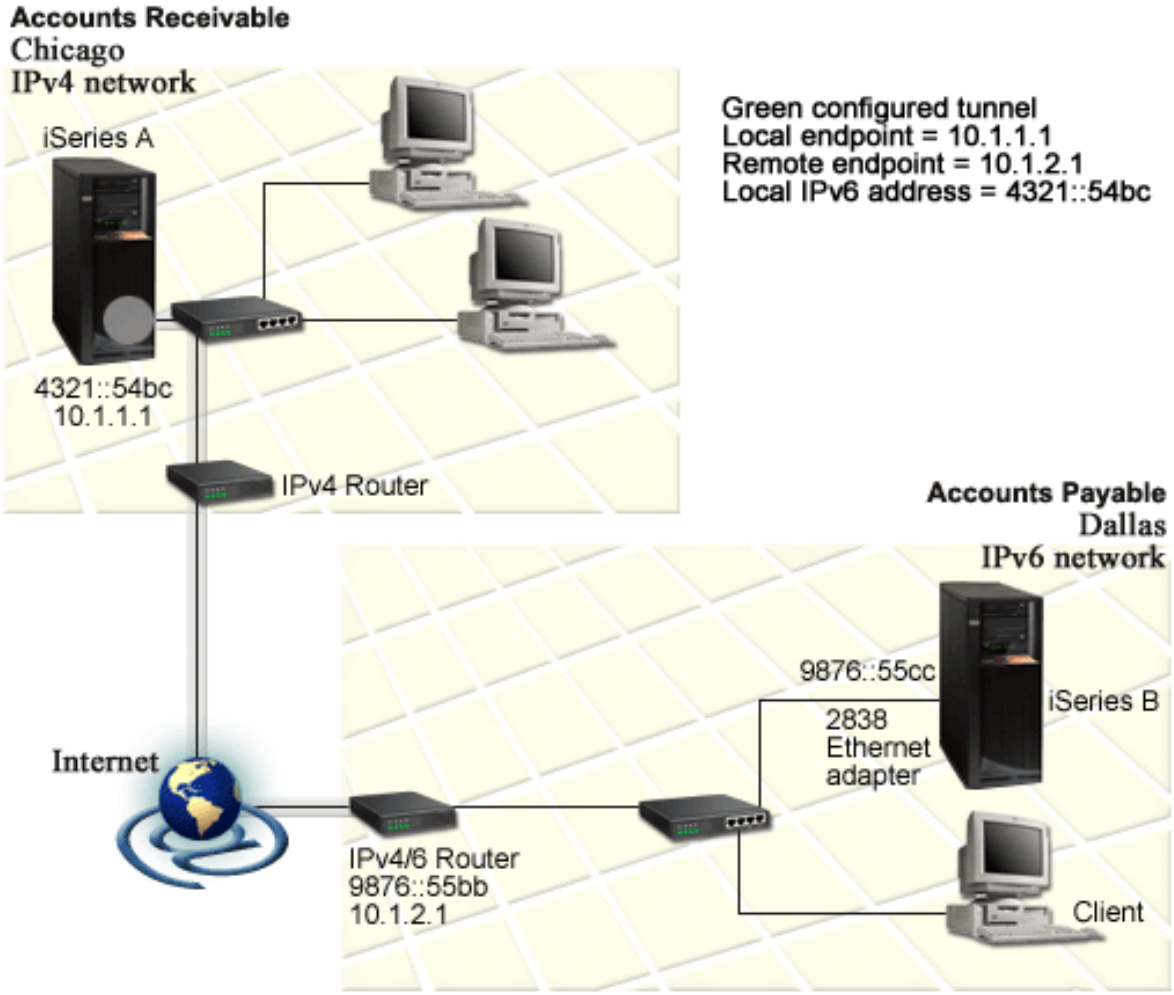
Zasielanie paketov IPv6 rozšírenou sieťou (WAN) IPv4

Situácia

Vaša firma používa pre nezaplatené účty účtovnú aplikáciu na serveri vo svojich kanceláriách v Chicagu. Túto aplikáciu potrebujete pripojiť k serveru v kanceláriách v Dallase. Na serveroch v oboch mestách používa táto aplikácia adresovanie IPv6. Keďže vám váš ISP nemôže medzi týmito dvoma miestami

poskytnúť smerovače IPv6, musíte si medzi servermi vytvoriť tunel. Pakety aplikácie sa medzi vašimi dvoma servermi presúvajú tunelom cez rozšírenú sieť (WAN) IPv4. Nasledujúci obrázok popisuje nastavenie siete v tomto scenári.

Poznámka: V tomto scenári IP adresy 10.x.x.x reprezentujú verejné IP adresy, ktoré môžu byť smerované celosvetovo. Všetky adresy sú uvedené len ako príklad.



Riešenie

Aby ste mohli IPv6 používať v rozšírenej sieti (WAN), ktorá pozostáva z infraštruktúry IPv4, musíte vytvoriť konfigurovanú tunelovú linku a niekoľko pripojených trás. Funguje to takto:

- Tunel sa začína na serveri iSeries A (lokálny koncový bod 10.1.1.1) v Chicagu a končí sa v smerovači IPv4/6 (vzdialený koncový bod 10.1.2.1) v Dallase.
- Aplikácia umiestnená na serveri iSeries A sa potrebuje pripojiť k aplikácii umiestnenej na serveri iSeries B. Server iSeries A paket IPv6 zapuzdrí do paketu IPv4 a odošle ho tunelom na smerovač IPv4/6, ktorý ho odpuzdrí a postúpi paket IPv6 na server iSeries B.
- Paket sa do Chicaga vráti použitím spätnej cesty.

Pripojenie tunelom je pripojením typu bod-bod, takže musíte zadať koncový bod tunela. Na to potrebujete vytvoriť s ním spojenú trasu. Ako ďalší skok určuje táto trasa vzdialený koncový bod (10.1.2.1). Inými

slovami, vzdialené koncové body definujete vytvorením trasy. Navyše trasa definuje cieľovú adresu ako 9876::55cc (adresa IPv6 spojená so serverom iSeries B).

Okrem vytvorenia úvodnej trasy, ktorá definuje koncový bod tunela a povoľuje presun paketu na server iSeries B v Dallase, musíte vytvoriť ešte dve trasy, aby sa mohli pakety vrátiť späť na server iSeries A v Chicagu.

Požiadavky nastavenia:

- OS/400 verzia 5 vydanie 2, alebo vyššie
- iSeries Access pre Windows a iSeries Navigator (sieťový komponent produktu iSeries Navigator)
- TCP/IP (s použitím IPv4) musí byť na serveri nakonfigurované skôr, než budete vytvárať konfigurovanú tunelovú linku. Ak ste server IPv4 nekonfigurovali, pozrite si skôr, než budete konfigurovať linku pre IPv6, Prvá konfigurácia TCP/IP.

Konfigurácia

Pri konfigurácii tunelovej linky musíte použiť sprievodcu **Konfigurácia IPv6** a sprievodcu **Nová trasa IPv6** v produkte iSeries Navigator. Konfigurované tunely môžu byť konfigurované len z produktu iSeries Navigator a nemôžu byť konfigurované zo znakového rozhrania.

Pri vytváraní tunelovej linky pomocou sprievodcu **Konfigurácia IPv6** nasledujte tieto kroky:

1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP**.
2. Kliknite pravým tlačidlom myši na **IPv6**, vyberte **Konfigurácia IPv6** a podľa inštrukcií sprievodcu nakonfigurujte tunelovú linku IPv6. Po skončení vás sprievodca **Konfigurácia IPv6** vyzve, aby ste pre konfigurovanú tunelovú linku vytvorili novú trasu a objaví sa dialógové okno sprievodcu **Nová trasa IPv6**. Musíte ju vytvoriť, aby ste povolili prenos paketov IPv6 tunelom.
3. Sprievodcom **Nová trasa IPv6** vytvorte pre tunel hostiteľskú trasu. Ako ďalší skok zadajte vzdialený koncový bod 10.1.2.1 a ako cieľovú adresu zadajte 9876::55cc.

Po vytvorení konfigurovanej tunelovej linky a trasy, ktorá definuje koncový bod tunela, musíte vytvoriť trasy na server iSeries B a na smerovač IPv4/6, ktoré povolia presun paketov späť do Chicaga. Pre trasu na server iSeries B by ste mali zadať 9876::55bb ako ďalší skok a 4321::54bc ako cieľovú adresu. Pre trasu na smerovač IPv4/6 by ste mali zadať 10.1.1.1 ako ďalší skok a 4321::54bc ako cieľovú adresu.

Poznámka: Smerovač IPv4/6 v Dallase by mal mať priamu trasu na 9876::55cc, ale keďže je táto trasa vytvorená automaticky, nie je potrebná žiadna manuálna konfigurácia.

Koncepty: IPv6

Aby ste lepšie pochopili, ako IPv6 funguje, prečítajte si popisy týchto konceptov IPv6:

Porovnanie IPv4 a IPv6
Zistite, aké je porovnanie atribútov IPv4 a atribútov IPv6. Táto tabuľka vám umožní rýchlo nájsť konkrétne funkcie a porovnať ich využitie v internetových protokoloch.

Formáty adresy IPv6
Viac informácií o veľkosti a formáte adresy IPv6.

Typy adresy IPv6
Nové typy adries v rámci IPv6.

Tunelovanie IPv6
Dozviete sa, ako tunelovanie IPv6 umožňuje paketom IPv6 presúvať sa sieťou IPv4.

Vyhľadávanie susedov
Informácie o tom, ako vyhľadávanie susedov umožňuje hostiteľom a smerovačom medzi sebou komunikovať.

Autokonfigurácia bezstavovej adresy
Zistite, ako autokonfigurácia bezstavovej adresy automatizuje niektoré administračné úlohy.

Formáty adresy IPv6

Veľkosť adresy IPv6 je 128 bitov. Uprednostňované vyjadrenie adresy IPv6 je: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, v ktorom každé x je hexadecimálna číslica zastupujúca 4 bity. Rozsah adries IPv6 je od 0000:0000:0000:0000:0000:0000:0000:0000 po ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Okrem tohto uprednostňovaného formátu môžu byť adresy IPv6 zadané v dvoch kratších formátoch:

- **Vypustenie vodiacich núl**
  Zadajte adresu IPv6 tak, že vynecháte všetky vodiace nuly. Napríklad adresa IPv6 1050:0000:0000:0000:0005:0600:300c:326b môže byť zapísaná ako 1050:0:0:0:5:600:300c:326b.
- **Dvojitá dvojbodka**
  Zadajte adresu IPv6 tak, že namiesto série núl použijete dvojité dvojbodky (::). Napríklad adresa IPv6 ff06:0:0:0:0:0:0:c3 môže byť zapísaná ako ff06::c3. Dvojité dvojbodky môžu byť v IP adrese použité len raz.

Alternatívou k týmto formátom adresy IPv6 je kombinácia dvojbodky a bodkového zápisu, takže adresa IPv4 môže byť vložená do adresy IPv6. Hexadecimálne hodnoty sú zadané pre 96 bitov na ľavej strane a desiatkové hodnoty, zadané pre 32 bitov na pravej strane, naznačujú vloženú adresu IPv4. Tento formát vám pri práci v zmiešanom sieťovom prostredí zabezpečuje súlad medzi uzlami IPv6 a IPv4.

Tieto dva typy adries IPv6 používajú tento alternatívny formát:

- **Adresa verzie IPv6 namapovaná z verzie IPv4**
  Tento typ adresy sa používa na vyjadrenie uzla IPv4 adresou IPv6. Umožňuje aplikáciám IPv6 komunikovať priamo s aplikáciami IPv4. Napríklad 0:0:0:0:0:ffff:192.1.56.10 a ::ffff:192.1.56.10/96 (skrátený formát).
- **Adresa verzie IPv6 kompatibilnej s verziou IPv4**
  Tento typ adresy sa nazýva tunelovanie. Umožňuje uzlom IPv6, aby spolu komunikovali naprieč infraštruktúrou IPv4. Napríklad 0:0:0:0:0:0:192.1.56.10 a ::192.1.56.10/96 (skrátený formát).

Všetky tieto formáty sú platnými formátmi adresy IPv6. V produkte iSeries Navigator zadajte ktorýkoľvek z týchto formátov adresy.

Typy adries IPv6

Adresy IPv6 sú rozdelené do troch základných kategórií:

Adresa typu unicast
Adresa typu unicast určuje jednotlivé rozhranie. Paket odoslaný na adresu sa presúva od jedného hostiteľa k cieľovému hostiteľovi.

Existujú tri typy adries unicast:

Adresy lokálneho spojenia
Adresy lokálneho spojenia sú vytvorené na použitie pre jedno lokálne spojenie (v lokálnej sieti). Adresy lokálneho spojenia sa automaticky konfigurujú vo všetkých rozhraniach. Prefix použitý pre adresy lokálneho spojenia je fe80::/10. Pakety, ktorých zdrojová adresa, alebo adresa určenia obsahuje adresu lokálneho spojenia, nie sú smerovačmi postúpené.

Miestne-špecifické adresy
Miestne-špecifické adresy sú vytvorené na použitie na konkrétnom mieste. Pre tieto adresy sa používa prefix fec0::/10. Ak sa miestne-špecifická cieľová adresa paketu nachádza mimo lokálnej siete, smerovač paket nepostúpi.

Globálna adresa
Globálna adresa je vytvorená tak, aby sa dala používať v akejkoľvek sieti. Jej prefix sa začína binárnym číslom 001.

Dva špeciálne typy adresy unicast obsahujú:

Neurčená adresa
Neurčená adresa je 0:0:0:0:0:0:0:0, prípadne môže byť skrátená na dve dvojbodky (::). Nezadaná adresa naznačuje absenciu adresy a nikdy nemôže byť hostiteľovi priradená. Môže byť použitá pre hostiteľa IPv6, ktorému ešte nie je priradená žiadna adresa. Ak napríklad hostiteľ zašle paket, aby vyhľadal adresu z iného uzla, používa hostiteľ nezadanú adresu ako cieľovú adresu.

Adresa slučky
Adresa je slučky 0:0:0:0:0:0:0:1, alebo jej skrátená verzia je ::1. Adresa slučky sa používa, ak uzol zasiela paket sám sebe.

Adresa ľubovoľnej siete
Adresa ľubovoľnej siete určuje skupinu rozhraní pravdepodobne na rozličných umiestneniach, ktoré zdieľajú jednu adresu. Paket, zaslaný na adresu ľubovoľnej siete, sa odošle najbližšiemu členovi tejto skupiny. Server iSeries adresy ľubovoľnej siete momentálne nepodporuje.

Viacnásobná adresa
Viacnásobná adresa určuje skupinu rozhraní, pravdepodobne vo viacerých umiestneniach. Používame pre ňu prefix ff. Ak je paket odoslaný na viacnásobnú adresu, doručí sa každému členovi skupiny. Server iSeries momentálne poskytuje viacnásobným adresám základnú podporu. Neposkytuje im podporu vytvárania viacnásobných rozhraní, ani aplikačnú podporu.

Tunelovanie IPv6

Tunelovanie IPv6 povoľuje serveru iSeries pripojiť sa na uzly IPv6 (hostitelia a smerovače) v doménach IPv4. Tunelovanie povoľuje izolovaným uzlom IPv6, alebo sieťam, komunikovať bez toho, aby bola zmenená základná infraštruktúra IPv4. Tunelovanie umožňuje spoluprácu protokolov IPv4 a IPv6 a takto poskytuje prechodný spôsob implementácie IPv6 pri ponechaní pripojiteľnosti IPv4.

Tunel pozostáva z dvoch uzlov duálnych zásobníkov (IPv4 a IPv6) na sieti IPv4. Tieto uzly sú schopné spracovať tak komunikáciu IPv4, ako aj IPv6. Jeden z týchto uzlov na okraji infraštruktúry IPv6 vloží na začiatok každého došlého paketu IPv6 hlavičku IPv4 (zapuzdrí ho) a pošle ho existujúcimi linkami, akoby to bola normálna prevádzka IPv4. Smerovače IPv4 pokračujú v postupovaní tejto prevádzky. Na druhej strane tunela ďalší uzol s duálnym zásobníkom odstraňuje hlavičku IP, ktorá je na pakete IPv6 navyše (odpuzdruje ho) a smeruje ho, s použitím štandardov IPv6, ku konečnému cieľu.

Tunelovanie IPv6 pre server iSeries beží cez konfigurované tunelové linky, ktoré sú virtuálne. Konfigurovaná tunelová linka poskytuje spojenie IPv6 s akýmkoľvek uzlom so smerovateľnou adresou IPv4, ktorý podporuje tunely IPv6. Tieto uzly môžu existovať kdekoľvek v rámci lokálnej domény IPv4, alebo v rámci vzdialenej domény.

Konfigurované tunelové pripojenia sú pripojeniami typu bod-bod. Pri konfigurácii takéhoto typu tunelovej linky musíte zadať koncový bod lokálneho tunela (adresu IPv4), ako napríklad 124.10.10.150 a lokálnu adresu IPv6, akou je 1080:0:0:0:8:800:200c:417a. Musíte tiež vytvoriť trasu IPv6 a povoliť tak prevádzke

prenos týmto tunelom. Pri vytváraní trasy nadefinujete jeden zo vzdialených koncových bodov (adresa IPv4) ako ďalší skok trasy. Môžete konfigurovať neobmedzený počet koncových bodov pre neobmedzený počet tunelov.

V častiach Zasielanie paketov IPv6 lokálnou sieťou (LAN) IPv4 a Zasielanie paketov IPv6 rozšírenou sieťou (WAN) IPv4 nájdete scenáre a zobrazenia, ktoré názorne popisujú tunelovanie IPv6.

Vyhľadávanie susedov

Funkcie vyhľadávania susedov sa používajú, ak dva uzly IPv6 (hostitelia a smerovače) zisťujú prítomnosť iných uzlov IPv6, určujú adresy uzlov vo vrstve prepojenia, hľadajú smerovače schopné postúpiť pakety IPv6 a udržiavajú cache pamäť aktívnych susedov IPv6. Uzly IPv6 používajú na komunikáciu s inými uzlami týchto päť správ Internetového protokolu riadenia správ verzia 6 (ICMPv6):

Žiadosť na smerovač
Hostiteľ zasiela tieto správy a žiada smerovače, aby vytvárali oznamy smerovača. Hostiteľ zašle úvodnú žiadosť, keď je po prvý raz prístupný na sieti.

Oznam smerovača
Smerovač zasiela tieto správy pravidelne, alebo ako odpoveď na požiadavku na smerovač. Informácie, poskytované v oznamoch smerovača, používajú hostitelia na automatické vytváranie rozhraní lokálneho umiestnenia, globálnych rozhraní a pripojených trás. Oznamy smerovača tiež obsahujú ďalšie konfiguračné informácie, ktoré hostiteľ použije, ako sú maximálna jednotka prenosu a obmedzenie skokov.

Vyžiadanie informácií o susedovi
Tieto správy posielajú uzly na určenie adresy suseda v prepojovacej vrstve, alebo na overenie, že je sused stále dosiahnuteľný.

Správa o susedovi
Tieto správy posielajú uzly ako odpoveď na vyžiadanie informácií o susedovi, alebo ako nevyžiadanú správu oznamujúcu zmenu adresy.

Presmerovanie
Tieto správy posielajú smerovače, aby informovali hostiteľov o lepšom prvom skoku k niektorému cieľu.

Viac informácií o vyhľadávaní susedov a vyhľadávaní smerovačov nájdete v RFC 2461. RFC 2461 si môžete prezrieť na stránke RFC Editor (http://www.rfc-editor.org/rfcsearch.html) .

Autokonfigurácia bezstavovej adresy

Autokonfigurácia bezstavovej adresy je proces, pri ktorom uzly IPv6 (hostitelia, alebo smerovače) používajú automatickú konfiguráciu adries IPv6 pre rozhrania. Uzol vytvorí rozličné adresy IPv6 kombináciou prefixu adresy s adresami MAC uzla, alebo s užívateľom určeným identifikátorom rozhrania. Prefixy lokálneho spojenia (fe80::/10) a prefixy s dĺžkou 64, šírené lokálnymi smerovačmi IPv6 (ak nejaké existujú). Autokonfigurácia bezstavovej adresy tiež vytvára príslušné viacnásobné rozhrania, ak typ linky viacnásobnosť povoľuje.

Skôr, než priradí adresu rozhraniu, vykoná uzol dvojité vyhľadanie adresy, aby si overil jej jedinečnosť. Zašle novej adrese požiadavku na vyžiadanie informácií o susedovi a čaká na odpoveď. Ak žiadnu odpoveď nedostane, adresa sa považuje za jedinečnú. Ak uzol dostane odpoveď vo forme správy o susedovi, znamená to, že táto adresa sa už používa. Ak uzol zistí, že jeho predbežná adresa IPv6 nie je jedinečná, autokonfigurácia sa zastaví a je potrebná manuálna konfigurácia rozhrania.

Porovnanie IPv4 a IPv6

IBM implementuje IPv6 na serveri iSeries v rámci niekoľkých softvérových vydaní. IPv6 je momentálne implementovaný na platforme vývoja aplikácií s cieľom vývoja a testovania aplikácií IPv6.

Možno vás zaujíma, ako sa líšia detaily IPv6 a IPv4. Táto tabuľka vám umožní rýchlo prezrieť známe atribúty spojené s IPv4 a porovnať ich s podobnými atribútmi IPv6. Výberom atribútu v tomto zozname sa dostanete na jeho porovnanie v tabuľke.

- “virtual private networking (VPN)” na strane 26

	IPv4	IPv6
adresa	dlhá 32 bitov (4 bajty). Adresa je vytvorená z časti siete a z hostiteľa, ktoré sú závislé od triedy adresy. Sú definované rozličné triedy adresy: A, B, C, D, alebo E, v závislosti od niekoľkých prvých bitov. Maximálny počet adries IPv4 je 4 294 967 296. Textový formát adresy IPv4 je nnn.nnn.nnn.nnn, kde 0<=nnn<=255 a každé n je desiatková číslica. Vodiace nuly môžu byť vynechané. Maximálny počet tlačených znakov je 15, nerátajúc masku.	dlhá 128 bitov (16 bajtov). Základná architektúra je 64 bitov pre číslo siete a 64 bitov pre číslo hostiteľa. Často bude hostiteľská časť adresy IPv6 (alebo časť z nej) označením adresy počítača MAC, alebo iného identifikátora rozhrania. V závislosti od prefixu podsiete má IPv6 podstatne komplikovanejšiu architektúru, než IPv4. Možný počet adries IPv6 je 10^{28} (79 228 162 514 264 337 593 543 950 336) násobne vyšší, než maximálny počet adries IPv4. Textová forma adresy IPv6 je xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, kde každé x je hexadecimálna číslica zastupujúca 4 bity. Vodiace nuly môžu byť vynechané. Dvojitá dvojbodka (::) môže byť v textovej forme adresy použitá raz, na označenie akéhokoľvek čísla s 0 bitmi. Napríklad adresa ::ffff:10.120.78.40 je zobrazenie IPv4 adresy ako adresy IPv6. (Detaily nájdete v RFC 2373. RFC si môžete prezrieť na stránke RFC Editor (http://www.rfc-editor.org/rfcsearch.html).
prideľovanie adries	Pôvodne boli adresy prideľované triedou siete. Po tom, čo boli z adresy odstránené medzery, boli pomocou Classless Inter-Domain Routing (CIDR) vykonané menšie pridelenia. Medzi krajinami a inštitúciami nebolo prideľovanie koordinované.	Prideľovanie je v skorých etapách. Internet Engineering Task Force (IETF) a Internet Architecture Board (IAB) odporúčali, aby bol v podstate každej organizácii, domácnosti, alebo jednotke pridelený prefix podsiete dĺžky48 bitov. To ponechá každej organizácii 16 bitov na očíslovanie podsiete. Medzera v adrese je dostatočne dlhá na to, aby mala každá osoba na svete svoj vlastný prefix podsiete dĺžky 48 bitov.
životnosť adresy	Vo všeobecnosti nepoužiteľný koncept, okrem pridelených pomocou DHCP.	Adresy IPv6 majú dva druhy životnosti: prednostnú a platnú, pričom prednostná životnosť je vždy <= než platná. Keď uplynie predpokladaná životnosť, adresa by sa už nemala použiť ako zdrojová IP adresa. Keď uplynie platná životnosť, nie je už adresa použitá (rozpoznaná) ako platná cieľová IP adresa pre prichádzajúce pakety. Niektoré adresy IPv6 majú, samozrejme, nekonečnú predpokladanú, aj platnú životnosť; napríklad adresy lokálneho spojenia (pozri “address scope” na strane 20).
adresa masky	Používa sa na označenie siete podľa časti hostiteľa.	Nepoužíva sa (pozri “address prefix” na strane 20).

	IPv4	IPv6
prefix adresy	Niekedy sa používa na označenie siete podľa časti hostiteľa. Niekedy zapísaný ako /nn prípona v presentation form adresy.	Je použitý na označenie prefixu podsiete adresy. Zapísaný ako prípona /nnn (do 3 desiatkových číslic, 0 <= nnn <= 128) po tlačovej forme. Príkladom je fe80::982:2a5c/10, kde prvých 10 bitov zahŕňa prefix podsiete.
Protokol rozpoznania adresy (ARP)	Protokol rozpoznania adresy používa IPv4 na nájdenie fyzickej adresy, ako napríklad adresy MAC, alebo linky, spojených s adresou IPv4.	IPv6 zakotvuje tieto funkcie v samotnom IP ako časť algoritmu pri bezstavovej autokonfigurácii a vyhľadávaní susedov s použitím Internetového protokolu riadenia správ verzia 6 (ICMPv6). Preto tu neexistuje nič také, ako ARP6.
rozsah adresy	Tento koncept sa nepoužíva na adresy unicast. Sú určené súkromné rozsahy adries slučka. Okrem tohto sa adresa považuje za globálnu.	Vo verzii IPv6 je rozsah adresy súčasťou architektúry. Adresy unicast majú 3 určené rozsahy, obsahujúce lokálne spojenia, lokálne a globálne umiestnenie; viacnásobné adresy majú 14 rozsahov. Štandardný výber adresy pre zdroj, aj cieľ, berie rozsah do úvahy. Zóna rozsahu je inštancia rozsahu v príslušnej sieti. Preto musia byť niekedy adresy IPv6 zadané aj s im priradeným ID zóny. Syntax je %zid kde zid je číslo (zvyčajne malé), alebo názov. ID zóny sa píše po adrese, ale pred prefixom. Napríklad 2ba::1:2:14e:9a9b:c%3/48.
typy adries	Unicast, multicast a broadcast.	Unicast, multicast a anycast.Opisy nájdete v časti Typy adries IPv6.
sledovanie komunikácií	Nástroj na zbieranie údajov o sledovaní podrobností paketov TCP/IP (a iných), ktoré prichádzajú a odchádzajú zo servera iSeries.	Rovnako je podporovaný IPv6, vrátane paketov ICMPv6 a IPv6 tunelovaných vo formáte IPv4.
konfigurácia	Konfigurácia musí prebehnúť na novoinštalovanom systéme skôr, než môže komunikovať; to znamená, že musia byť priradené IP adresy a trasy.	Konfigurácia je, v závislosti od požadovaných funkcií, voliteľná. Patričné rozhranie Ethernet, alebo tunelové rozhranie, musí byť, pomocou produktu iSeries Navigator, určené ako rozhranie IPv6. Keď je toto hotové, konfigurujú sa rozhrania IPv6 samy. Takže systém bude schopný komunikovať s inými lokálnymi, aj vzdialenými systémami IPv6, v závislosti od typu siete a od toho, či existuje smerovač IPv6.

	IPv4	IPv6
Systém názvov domén (DNS)	Aplikácie akceptujú hostiteľské názvy a potom sa pomocou DNS snažia, s použitím soketu API gethostbyname(), získať IP adresu. Aplikácie tiež akceptujú IP adresy a potom sa pomocou DNS snažia, s použitím gethostbyaddr(), získať názov hostiteľa. Pre IPv4, doménou na spätné hľadania je in-addr.arpa.	Rovnako pre IPv6. Podpora pre IPv6 existuje s použitím typu záznamu AAAA (štvorica A) a spätného vyhľadávania (IP-to-name). Aplikácia si môže zvoliť, či od DNS akceptuje (alebo neakceptuje) adresy IPv6 a či potom na spojenie použije (alebo nepoužije) IPv6. Soket API gethostbyname() je pre IPv6 nezmenené a getaddrinfo() API môže byť (podľa voľby aplikácie) použité na získanie len adries IPv6, alebo adries IPv4 a IPv6. Doména použitá pri spätnom nibble vyhľadávaní pre IPv6 je ip6.arpa a ak nie je nájdená, je to ip6.int (pozri API getnameinfo()).
Protokol dynamickej konfigurácie hostiteľov (DHCP)	Používa sa na dynamické prideľovanie IP adries a iných konfiguračných informácií.	DHCP momentálne nepodporuje IPv6.
Protokol prenosu súborov (FTP)	Protokol prenosu súborov vám umožňuje odosielať a prijímať súbory naprieč sieťou.	FTP momentálne nepodporuje IPv6.
fragmenty	Ak je paket pre ďalšiu linku, ktorou sa má presúvať, príliš veľký, môže byť odosielateľom (hostiteľom, alebo smerovačom) rozdrobený (fragmentovaný).	Pre IPv6 môže ku fragmentácii dôjsť len v zdrojovom uzle a ku znovuzostaveniu len v cieľovom uzle. Hlavička fragmentačnej prípony momentálne nie je podporovaná.
hostiteľská tabuľka	Je to konfigurovateľná tabuľka v produkte iSeries Navigator, ktorá priraďujte Internetovej názov hostiteľa; napríklad 127.0.0.1, slučka. Túto tabuľku používa rozpoznávač názvov soketov, buď pred vyhľadaním DNS, alebo po tom, čo vyhľadanie DNS zlyhá (to je určené prioritou vyhľadania názvu hostiteľa).	Táto tabuľka zatiaľ IPv6 nepodporuje. Zákazníci si musia záznam AAAA nakonfigurovať v DNS pre rozpoznávanie domén IPv6. DNS môžete mať spustený lokálne na tom istom systéme, ako rozpoznávač, alebo ho môžete spustiť na inom systéme.
rozhranie	Koncepčná, alebo logická jednotka, ktorú používa TCP/IP na zasielanie a prijímanie paketov, je vždy úzko spojená s adresou IPv4, alebo je ňou aj pomenovaná. Niekedy sa na túto jednotku odkazuje ako na logické rozhranie. Každé z nich môže byť nezávisle spustené a vypnuté a nezávisle od TCP/IP môžu používať príkazy STRTCPIFC a ENDTCPIFC a produkt iSeries Navigator.	Rovnaký koncept ako IPv4. Môžu byť nezávisle spustené a vypnuté a nezávisle od TCP/IP môžu používať produkt iSeries Navigator.

	IPv4	IPv6
Internetový protokol riadenia správ (ICMP)	IPv4 používa ICMP na komunikáciu sieťových informácií.	Podobne ho používa aj IPv6; Internetový protokol riadenia správ verzia 6 (ICMPv6) však prináša niekoľko nových atribútov. Základné typy chýb ostávajú, ako napríklad nezastihnuteľný cieľ, ozvena požiadavky a odpovede. Na podporu vyhľadávania susedov a s tým spojených funkcií pribudli nové typy chýb a ich kódy.
Internetový protokol spravovania skupín (IGMP)	IGMP používajú smerovače IPv4 na hľadanie hostiteľov, ktorí chcú prevádzku pre konkrétnu viacnásobnú skupinu a tiež ho používajú hostitelia IPv4, aby mohli smerovače IPv4 informovať o načúvačoch viacnásobných skupín (na hostiteľovi).	Je nahradený protokolom MLD (nachádzanie načúvačov viacnásobných skupín) pre IPv6. Robí presne to, čo IGMP pre IPv4, ale pridaním niekoľkých hodnôt typu vlastných pre MLD, používa ICMPv6.
hlavička IP	V závislosti od aktuálnych volieb IP je dĺžka premennej 20-60 bajtov.	Pevná dĺžka 40 bajtov. Pre hlavičku IP nie sú žiadne voľby. Vo všeobecnosti je hlavička IPv6 jednoduchšia než hlavička IPv4.
voľby hlavičky IP	Rôzne možnosti, ktoré môžu hlavičku IP sprevádzať (pred akoukoľvek hlavičkou presunu).	Hlavička IPv6 nemá žiadne voľby. Namiesto toho IPv6 pridáva dodatočné (voliteľné) rozšírené hlavičky. Rozšírené hlavičky sú AH a ESP (rovnaké ako pre IPv4), skok-za-skokom, smerovanie, fragment a cieľ. Momentálne IPv6 nepodporuje žiadne rozšírené hlavičky.
bajt protokolu hlavičky IP	Kód protokolu transportnej vrstvy, alebo užitočné zaťaženie paketu; napríklad ICMP.	Typ hlavičky, ktorá nasleduje priamo za hlavičkou IPv6. Používa rovnaké hodnoty, ako pole protokolu IPv4. Efekt architektúry je ale povolenie aktuálne definovaného rozsah ďalších hlavičiek a jeho jednoduché rozšírenie. Ďalšie hlavičky sú transportná hlavička, rozšírená hlavička, alebo ICMPv6.
bajt hlavičky IP Typ služby	Používané QoS and rozlíšenými službami na určenie triedy prevádzky.	Podobne ako pre IPv4, určuje triedu prevádzky IPv6. Používa rozličné kódy. IPv6 momentálne nepodporuje TOS.
podpora produktu iSeries Navigator	Produkt iSeries Navigator poskytuje pre TCP/IP plnú konfiguračnú funkčnosť.	Voliteľná konfigurácia pre IPv6 je produktom iSeries Navigator plne poskytovaná, vrátane sprievodcu **Konfigurácia IPv6**.
pripojenie LAN	Používané rozhraním IP pri dosahovaní fyzickej siete. Existuje veľa typov; napríklad token ring, Ethernet a PPP. Niekedy je spomínané ako fyzické rozhranie, spojenie, alebo linka.	IPv6 má rovnaký koncept. Momentálne sú podporované len karty Ethernet 2838 a 2849 a tunelové linky.
Layer 2 Tunnel Protocol (L2TP)	L2TP môže byť považovaný za virtuálny PPP a funguje na akomkoľvek podporovanom type linky.	L2TP momentálne nepodporuje IPv6.
adresa miestnej slučky	Rozhranie s adresou 127.*.*.* (zvyčajne 127.0.0.1), ktoré môže byť používané uzlom len zasielanie paketov samému sebe. Fyzické rozhranie (opis linky) je pomenované *LOOPBACK.	Koncept je rovnaký ako pre IPv4 a samostatná adresa miestnej slučky je 0000:0000:0000:0000:0000:0000:0000:0001, alebo ::1 (skrátená verzia). Virtuálne fyzické rozhranie je pomenované *LOOPBACK6.

	IPv4	IPv6
Maximálna jednotka prenosu (MTU)	Maximálna jednotka prenosu linky je číslo určujúce maximálny počet bajtov, ktorý podporuje konkrétny typ linky, napríklad Ethernet, alebo modem. Pre IPv4 je typické maximum 576.	IPv6 má štandardne navrhnutú dolnú hranicu v MTU na 1280 bajtov. To znamená, že IPv6 nefragmentuje pakety pod touto hranicou. Pri zasielaní IPv6 cez linku s MTU nižším než 1280 musí prepájacia vrstva transparentne fragmentovať a defragmentovať pakety IPv6.
netstat	Nástroj na prezeranie stavu pripojení TCP/IP, rozhraní, alebo trás. Je dostupný pri použití produktu iSeries Navigator a 5250.	Rovnako je to pre IPv6; IPv6 je podporované oboma, 5250 aj produktom iSeries Navigator.
Network Address Translation (NAT)	Základné funkcie firewallu integrované do TCP/IP, konfigurované pomocou produktu iSeries Navigator.	NAT momentálne nepodporuje IPv6. Všeobecne IPv6 nevyžaduje NAT. Rozšírený priestor adresy IPv6 eliminuje problém s krátkou adresou a umožňuje jednoduchšie prečíslovanie.
sieťová tabuľka	Je to konfigurovateľná tabuľka v produkte iSeries Navigator, ktorá priraďuje sieťový názov k IP adrese bez masky. Napríklad hostiteľ Network14 a IP adresa 1.2.3.4.	Momentálne nie sú pre IPv6 v tejto tabuľke urobené žiadne zmeny.
požiadavka na informácie o uzle	Neexistuje.	Jednoduchý a pohodlný sieťový nástroj, ktorý by mal, až na obsah, fungovať ako testovanie odozvy: uzol IPv6 môže požiadať iný uzol IPv6 o DNS názov cieľa, unicast adresu IPv6, alebo adresu IPv4. Momentálne nie je podporovaný.
filtrovanie paketov	Základné funkcie firewalu integrované do TCP/IP, konfigurované pomocou produktu iSeries Navigator.	Filtrovanie paketov momentálne nepodporuje Pv6. Filtrovanie IPv4 však môže byť použité na tunelovú prevádzku IPv6.
postúpenie paketov	Server iSeries môže byť konfigurovaný na postupovanie prijatých paketov IP, na adresy IP, ktoré nie sú lokálne. Rozhrania pre prijímanie a pre odosielanie sú bežne pripojené k rozličným sieťam LAN.	Pakety IPv6 sa momentálne nepostupujú.
tunelovanie paketov	V IPv4 sa tunelovanie objavuje v pripojeniach VPN ako tunelový režim (tunelovanie IPv4 v IPv4) a v L2TP.	Pokiaľ ide o IPv6, tunelovanie v paketoch IPv4 by malo byť najväčšou časťou rozvoja IPv6. Momentálne IETF definuje minimálne 5 rôznych typov tunelovania 6-v-4, každý s inými atribútmi a výhodami. Základný a prispôsobivý typ tunelovania IPv6-v-IPv4 je podporovaný, aby umožnil uzlom IPv6 komunikovať naprieč existujúcim internetom IPv4. Nazýva sa **konfigurované tunelovanie** a poskytuje virtuálne spojenie typu bod-bod medzi dvoma uzlami IPv6 a používa nový typ tunelu, nazvaný *TNLCFG64.
PING	Základný nástroj TCP/IP na testovanie dostupnosti. Je dostupný pri použití produktu iSeries Navigator a 5250.	Rovnako je to pre IPv6; IPv6 je podporované oboma, 5250 aj produktom iSeries Navigator.
Protokol bod-bod (PPP)	PPP podporuje rozhranie vytáčané cez rozličné modemy a typy liniek.	PPP momentálne nepodporuje IPv6.

	IPv4	IPv6
obmedzenia portov	Tieto panely iSeries umožňujú zákazníkovi konfigurovať vybrané čísla portov, alebo rozsahy čísel portov pre TCP, alebo UDP, takže sú dostupné len konkrétnym profilom.	Nepodporuje IPv6. Konfigurované obmedzenia sú aplikované len na IPv4.
porty	Protokoly TCP a UDP majú rozličné porty, každý z nich je identifikovaný číslom v rozsahu 1-65535.	Pre IPv6 pracujú porty rovnako ako pre IPv4. Keďže porty sú teraz v novej rodine adries, tak existujú štyri osobitné umiestnenia portov. Sú napríklad dve umiestnenia TCP portu 80, na ktoré sa môže viazať aplikácia, jeden v AF_INET a jeden v AF_INET6.
súkromné a verejné adresy	Všetky adresy IPv4 sú verejné, okrem troch rozsahov adries, ktoré boli IETF RFC 1918 určené ako súkromné: 10.*.*.* (10/8), 172.16.0.0 cez 172.31.255.255 (172.16/12) a 192.168.*.* (192.168/16). Domény súkromných adries sú v rámci organizácií bežne využívané. Súkromné adresy nemôžu byť smerované naprieč internetom.	IPv6 má podobný koncept, ale s dôležitými rozdielmi. Adresy sú verejné, alebo dočasné, predtým označené ako anonymné. Pozri RFC 3041. Na rozdiel od súkromných adries IPv4, dočasné adresy môžu byť všeobecne smerovateľné. Aj motivácia je odlišná; dočasné adresy IPv6 majú pri začatí komunikácie ochrániť identitu klienta (záležitosť súkromia). Dočasná adresa má obmedzenú životnosť a neobsahuje identifikátor rozhrania, ktorý je adresou linky (MAC). Všeobecne sú nerozpoznateľné od verejných adries. IPv6 pracuje s novým platným rozsahom adries, pričom používa vlastné štandardne nastavené označenia rozsahu (see “address scope” na strane 20).
tabuľka protokolu	Je to konfigurovateľná tabuľka v protokole iSeries Navigator, ktorá priraďuje názov protokolu s číslom protokolu; napríklad UDP, 17. Systém je distribuovaný len s malým počtom záznamov: IP, TCP, UDP, ICMP.	Tabuľka podporuje IPv6 bez zmien.
Kvalita služieb (QoS)	Kvalita služieb vám umožňuje požadovať pre aplikácie TCP/IP prioritu paketov a šírku pásma.	QoS momentálne nepodporuje IPv6. Ak je však IPv6 tunelovaný v IPv4, existujúce možnosti QoS v systéme iSeries môžu byť aplikované na prevádzku IPv4c, ktorá potom transparentne spracuje užitočné zaťaženie IPv6.
prečíslovanie	Sa vykonáva manuálnou rekonfiguráciou, možnou výnimkou je DHCP. Všeobecne je to pre organizáciu náročný a problematický proces, ktorému sa, ak je to možné, treba vyhnúť.	Je to dôležitou súčasťou architektúry IPv6 a malo by byť prevažne automatické, najmä pre prefix /48.

	IPv4	IPv6
trasa	Logicky je to mapovanie skupiny IP adries (môže to byť jedna) na fyzické rozhranie a jeden ďalší skok k IP adrese. Pakety IP, ktorých cieľová adresa je definovaná ako časť skupiny, sú pomocou linky postúpené k ďalšiemu skoku. Trasy IPv4 sú prepojené s rozhraním IPv4, a teda aj adresou IPv4. Štandardná trasa je *DFTROUTE.	Rovnaký koncept ako IPv4. Je tu jeden dôležitý rozdiel: trasy IPv6 sú skôr priradené (zviazané) fyzickému rozhraniu (spojenie, ako napríklad *TNLCFG64, alebo ETH03), než k rozhraniu. Sú na to rozličné dôvody. Jedným z nich je, že výber zdrojovej adresy funguje pre IPv6 inak než pre IPv4. Pozrite si “source address selection”. Duplikátne trasy sú povolené, aby podporili priamosť siete, ale počas prehľadávania trás sú ignorované.
Protokol smerovania informácií (RIP)	RIP je smerovací protokol podporovaný smerovaným démonom.	RIP momentálne nepodporuje IPv6. Smerovanie IPv6 používa stále trasy.
tabuľka služieb	Konfigurovateľná tabuľka na serveri iSeries server, ktorá priraďuje názov služby k portu a protokolu; napríklad názov služby riadenie FTP, port 21, TCP a UDP. V tabuľke služieb je uvedené veľké množstvo známych služieb. Pri procese rozhodovania, aký port použiť, túto tabuľku využívajú mnohé aplikácie.	Pre IPv6 v tejto tabuľke nie sú urobené žiadne zmeny.
Protokol jednoduchého spravovania siete (SNMP)	SNMP je protokol pre spravovanie systému.	SNMP momentálne nepodporuje IPv6. Smerovanie IPv6 používa stále trasy.
API sokety	Tieto API sú spôsob, akým aplikácie používajú TCP/IP. Aplikácie, ktoré nepotrebujú IPv6, nie sú ovplyvnené zmenami soketov na podporu IPv6.	IPv6 zdokonalí sokety, takže aplikácia bude môcť používať IPv6 s novou rodinou adries: AF_INET6. Vylepšenia boli navrhnuté tak, aby existujúce aplikácie IPv4 neboli vôbec ovplyvnené zmenami IPv6 a API. Aplikácie, ktoré chcú podporovať prevádzku IPv4 aj IPv6, alebo len prevádzku IPv6, sa jednoducho prispôsobia použitím formátu IPv4 adresy IPv6 v tvare ::ffff:a.b.c.d, kde a.b.c.d je klientska adresa IPv4. Nová API tiež obsahuje podporu konvertovania adresy IPv6 z textovej na a z binárnej na textovú. Viac informácií o IPv6 pre sokety nájdete v časti Použitie rodiny adries AF_INET6.
výber zdrojovej adresy	Aplikácia môže určiť zdrojovú IP adresu (zvyčajne použitím soketov bind()). Ak sa zviaže s INADDR_ANY, je zdrojový IP určený na základe trasy.	Ako pri IPv4, môže aplikácia určiť zdrojovú adresu IPv6 (zvyčajne použitím soketov bind()). Rovnako ako pri IPv4, môže nechať systém, aby použitím in6addr_any vybral zdrojovú adresu IPv6. Keďže ale linky IPv6 obsahujú mnoho adries IPv6, je spôsob výberu zdrojovej IP adresy odlišný.

	IPv4	IPv6
spúšťanie a zastavovanie	na spustenie a zastavenie TCP/IP používa príkazy STRTCP a ENDTCP.	Rovnaké ako IPv4. IPv4 a IPv6 nie sú spustené, alebo zastavené nezávisle jeden od druhého, alebo nezávisle od TCP/IP. To znamená, že spúšťate, alebo zastavujete celý TCP/IP, nielen IPv4, alebo IPv6. Akékoľvek rozhrania IPv6 sú spustené automaticky, ak je hodnota parametra AUTOSTART nastavená na *YES (predvolené). IPv6 nemôže byť používaný, ani konfigurovaný bez IPv4, a IPv6 musí mať nakonfigurovanú miestnu slučku IPv6 (::1).
Telnet	Telnet vám umožňuje prihlásiť sa k vzdialenému počítaču a používať ho, akoby ste k nemu boli pripojení priamo.	Telnet momentálne nepodporuje IPv6.
sledovanie trás	Základný nástroj TCP/IP na určovanie cesty. Je dostupný pri použití produktu iSeries Navigator a 5250.	Platí to rovnako pre IPv6; IPv6 je podporované oboma, 5250 aj produktom iSeries Navigator.
transportné vrstvy	TCP, UDP, RAW. Nový transportný protokol SCTP sa snaží ponúknuť najlepšie vlastnosti TCP a UDP, teda zaručenú komunikáciu bez pripojenia. SCTP je v jednom z prvých štádií použitia a podporujú ho servery iSeries.	Rovnaké tri transporty existujú a ich funkčnosť je nezmenená aj pre IPv6.
neurčená adresa	Zjavne nie je ako taká definovaná. Programovanie soketov používa 0.0.0.0 ako INADDR_ANY.	Je definovaná ako ::/128 (128 0 bitov). Je použitá ako zdrojová IP adresa v niektorých paketoch vyhľadávania susedov a v rozličných ďalších konceptoch, ako napríklad v soketoch. Programovanie soketov používa ::/128 ako in6addr_any.
vytváranie súkromnej virtuálnej siete (VPN)	Vytváranie virtuálnej súkromnej siete (s použitím IPsec) vám umožňuje natiahnuť vo verejnej sieti bezpečnú súkromnú sieť.	VPN momentálne nepodporuje IPv6. Keď je však IPv6 tunelovaný v IPv4, existujúce možnosti VPN v systéme iSeries môžu byť aplikované na prevádzku IPv4c, ktorá potom transparentne spracuje užitočné zaťaženie IPv6.

Informácie, týkajúce sa IPv6

V týchto zdrojoch informácií nájdete viac informácií o IPv6:

The Internet Engineering Task Force (IETF) (http://www.ietf.cnri.reston.va.us/)
Dozviete sa o skupine ľudí, ktorí vyvinuli Internetový protokol, vrátane IPv6.

IP Version 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html)
Dozviete sa o aktuálnych špecifikáciách IPv6 a nájdete odkazy na ďalšie zdroje informácií o IPv6.

IPv6 Forum (http://www.ipv6forum.com/)
Prečítajte si články s novinkami a prípady, ktoré vás oboznámia s najnovším vývojom v IPv6.

Kapitola 4. Plánovanie nastavenia TCP/IP

Skôr, než prikročíte k inštalácii a konfigurácii svojho servera iSeries, obetujte pár chvíľ na prípravu operácie. Pri plánovaní návodu si pozrite dole uvedené témy. Tento naplánovaný návod patrí k základnému nastaveniu TCP/IP s použitím IPv4. Ak trváte na konfigurácii IPv6, nájdete v časti Konfigurácia IPv6 požiadavky na nastavenie a konfiguračné inštrukcie.

Požiadavky pre nastavenie TCP/IP
Získať a zaznačiť základné konfiguračné informácie, ktoré sa vyžadujú pre nastavenie TCP/IP.

Úvahy o bezpečnosti TCP/IP
Zvážiť svoje bezpečnostné potreby, ktoré sa vás týkajú ako nového člena siete.

Požiadavky pre nastavenie TCP/IP

Vytlačte si túto stranu a zaznačte si konfiguračné informácie o svojom serveri a TCP/IP sieti, ku ktorej sa pripájate. Tieto informácie budete potrebovať neskôr počas konfigurovania TCP/IP. Dodržiavajte inštrukcie a pomocou tabuľky určite hodnoty pre prvé dva riadky. Ak je vám ktorýkoľvek z týchto výrazov neznámy,

prezrite si IBM redbook TCP/IP pre AS/400: More Cool Things Than Ever  , a zamerajte sa na Kapitolu dva, ″TCP/IP: Základná inštalácia a konfigurácia.″

Požadované informácie	Pre váš systém	Príklad
Typ komunikačného adaptéra, nainštalovaného vo svojom systéme (pozrite si inštrukcie dole)		Ethernet
Názov prostriedku		CMN01
IP adresa vášho servera iSeries		199.5.83.158
Maska podsiete vášho servera iSeries		255.255.255.0
Adresa brány		199.5.83.129
Názov hostiteľa a názov domény pre svoj systém		sys400.xyz.company.com
IP adresa pre názvový server domény		199.4.191.76

Informácie o svojom komunikačnom adaptéri nájdete vykonaním týchto krokov:

1. V príkazovom riadku servera zadajte go hardware a stlačte **Enter**.
2. Ak napíšete 1 a stlačíte **Enter**, zobrazí sa vám Práca s komunikačnými prostriedkami (Voľba 1).
   Zobrazí sa zoznam vašich komunikačných prostriedkov, usporiadaný podľa názvu prostriedku. Ak chcete pracovať so svojimi adaptérmi alebo chcete zobraziť viac detailov, postupujte podľa inštrukcií na obrazovke.

Ďalší postup:
Inštalácia TCP/IP

Úvahy o bezpečnosti TCP/IP

Pri plánovaní svojej konfigurácie TCP/IP by ste mali zvážiť svoje bezpečnostné potreby. Možnú hrozbu, ktorá je spojená s používaním TCP/IP, vám pomôžu obmedziť nasledujúce stratégie:

- **Spúšťajte len tie TCP/IP aplikácie, ktoré potrebujete.**
  Každá TCP/IP aplikácia má svoje vlastné jedinečné bezpečnostné riziká. Pri odmietnutí požiadaviek na

konkrétne aplikácie sa nespoliehajte len na smerovač. Druhé bezpečnostné opatrenie, nepotrebným aplikáciám nastavte hodnotu automatického spúšťania na NO.

- **Obmedzte hodiny, počas ktorých sa vykonávajú TCP/IP aplikácie.**
  Znížte možné riziká zredukovaním hodín, v ktorých sú spustené servery. Ak je to možné, mimo pracovných hodín zastavte TCP/IP servery, ako sú FTP a Telnet.
- **Riaďte, kto môže spustiť a zmeniť svoje TCP/IP aplikácie.**
  Na zmenu konfiguračných nastavení sa štandardne vyžaduje oprávnenie *IOSYSCFG. Používateľ bez oprávnenia *IOSYSCFG potrebuje oprávnenie *ALLOBJ alebo explicitné oprávnenie na spúšťanie TCP/IP príkazov. Keď dáte používateľom špeciálne oprávnenie, predstavuje to bezpečnostné riziko. Prehodnoťte potrebu špeciálnych oprávnení pre každého používateľa a snažte sa ich prideľovať čo najmenej. Uchovajte si záznamy o tom, ktorí používatelia majú špeciálne oprávnenia a pravidelne prehodnocujte ich požiadavky. Týmto postupom tiež znižujete možnosť prístupu na server mimo pracovných hodín.
- **Riaďte smerovanie svojho TCP/IP:**
  - Zakážte postupovanie IP, aby hackeri nemohli používať váš webový server na útoky na iné dôveryhodné systémy.
  - Definujte len jednu trasu na svoj verejný webový server: štandardne je nastavené smerovanie na svojho poskytovateľa internetových služieb (ISP).
  - V tabuľke TCP/IP hostiteľov svojho webového servera nekonfigurujte názvy hostiteľov a IP adresy interných bezpečných systémov. Do tejto tabuľky umiestnite len názvy iných verejných serverov, s ktorými sa potrebujete spojiť.
- **Riaďte TCP/IP servery, určené na vzdialené interaktívne prihlasovanie.**
  Aplikácie ako FTP a Telnet sú vo väčšej miere vystavené vonkajším útokom. Detaily o tom, ako riadiť vaše vystavenie, nájdete v kapitole o tipoch pri riadení interaktívneho prihlasovania sa, Tipy a nástroje zabezpečenia servera iSeries  .

Viac informácií o bezpečnosti a vám prístupných možnostiach, nájdete v časti IBM Secureway: iSeries a Internet.

Kapitola 5. Inštalácia TCP/IP

Základná podpora TCP/IP prichádza s OS/400 a umožňuje vám pripojiť server iSeries k sieti. Ak však chcete používať nejaké TCP/IP aplikácie, ako sú Telnet, FTP a SMTP, musíte tiež nainštalovať TCP/IP Connectivity Utilities. Ide o samostatne inštalovateľný licenčný program, ktorý sa dodáva s vaším operačným systémom.

TCP/IP Connectivity Utilities nainštalujete na svoj server iSeries nasledujúcim spôsobom:

1. Vložte do svojho servera inštalačné médium pre TCP/IP. Ak je vaším inštalačným médiom CD-ROM, vložte ho do svojho optického zariadenia. Ak je vaším inštalačným médiom páska, vložte ju do svojho páskového zariadenia.
2. V príkazovom riadku napíšte GO LICPGM a stlačte **Enter**, aby sa zobrazila obrazovka Práca s licenčnými programami.
3. Na obrazovke Práca s licenčnými programami vyberte voľbu **11** (Inštalovať licencované programy), aby sa zobrazil zoznam licenčných programov a voliteľných častí licenčných programov.
4. Napíšte **1** (Install) do stĺpca Voľby vedľa 57*xx*TC1 (TCP/IP Connectivity Utilities pre iSeries). Stlačte **Enter**. Zobrazí sa obrazovka Potvrďte inštaláciu licenčných programov, ktorá zobrazuje vami vybratý program na inštaláciu. Stlačením **Enter** ju potvrďte.
5. Na obrazovke Install Options vyplňte nižšie uvedené:

Installation device	Ak inštalujete z CD-ROM zariadenia, napíšte QOPT. Ak inštalujete z páskovej jednotky, napíšte TAP01.
Objects to install	Táto voľba vám umožňuje nainštalovať programy aj jazykové objekty, len programy alebo len jazykové objekty.
Automatický reštart	Táto voľba určuje, či sa systém po úspešnom dokončení inštalačného procesu automaticky spustí.

   Po úspešnom nainštalovaní TCP/IP Connectivity Utilities sa zobrazí ponuka Práca s licenčnými programami alebo sa zobrazí prihlasovacia obrazovka.
6. Či sa licenčný program nainštaloval úspešne, zistíte vybratím voľby **50** (Display log for messages).

   Ak došlo k chybe, naspodu obrazovky Práca s licenčnými programami bude zobrazená správa Práca s licenčnými programami nie je ukončená. Aby sa predišlo problémom, skúste preinštalovať TCP/IP Connectivity Utilities. Ak sa tým problém nevyrieši, možno budete musieť kontaktovať podporu.

Poznámka:

K iným licenčným programom, ktoré možno budete chcieť nainštalovať, patria:

- iSeries Access pre Windows 95/NT (5769–XD1 V3R1M3 alebo vyššia) poskytuje produktu iSeries Navigator podporu, ktorú potrebuje pri konfigurácii niektorých komponentov TCP/IP.
- IBM HTTP Server pre iSeries (57*xx*–DG1) poskytuje podporu webového servera.
- Niektoré TCP/IP aplikácie požadujú inštaláciu dodatočných licenčných programov. Aby ste našli požadované programy, pozrite si inštrukcie k nastaveniu konkrétnej aplikácie.

Kapitola 6. Konfigurácia TCP/IP

Možno konfigurujete TCP/IP po prvý raz, alebo meníte jeho aktuálne nastavenia, aby ste mohli využívať funkcie IPv6. Táto téma vám poskytne informácie o konfigurácii TCP/IP v oboch prípadoch. Prezrite si nižšie uvedené možnosti s inštrukciami o tom, ako na svojom serveri konfigurovať TCP/IP:

Prvá konfigurácia TCP/IP
Tieto inštrukcie využite, ak nastavujete nový server. Po prvý raz vytvoríte spojenie a nakonfigurujete TCP/IP.

Konfigurácia IPv6
Tieto inštrukcie využijete, ak konfigurujete svoj server na využívanie funkcií IPv6. Využijete výhody vylepšených možností adresovania a silných vlastností Internetového protokolu. Ak IPv6 ešte nepoznáte, nájdete jeho prehľad v časti Internetový protokol verzie 6 (IPv6). Skôr než ho však začnete konfigurovať, na serveri už musíte mať konfigurované TCP/IP.

Prvá konfigurácia TCP/IP

Vyberte si jeden z nasledujúcich spôsobov nastavenia TCP/IP na vašom serveri:

Konfigurácia TCP/IP pomocou Sprievodcu nastavením EZ
Túto možnosť použite, ak je váš počítač na použitie Sprievodcu nastavením EZ pripravený. Sprievodca nastavením EZ je pribalený k vášmu serveru iSeries.

Konfigurujte TCP/IP pomocou znakového rozhrania
Tento spôsob použite, ak nemôžete použiť Sprievodcu nastavením EZ. Ak napríklad chcete použiť iSeries Navigator na počítači, ktorý pred spustením produktu iSeries Navigator vyžaduje základné nastavenie TCP/IP, mali by ste použiť tento spôsob.

Konfigurácia TCP/IP pomocou Sprievodcu nastavením EZ

Produkt iSeries Navigator je grafické užívateľské rozhranie, ktoré poskytuje stručné dialógové okná a sprievodcov nastavením TCP/IP. Pri úvodnom nastavení použite Sprievodcu nastavením EZ v produkte iSeries Navigator, vytvorte pripojenie a po prvý raz nakonfigurujte TCP/IP. Toto je uprednostňovaný spôsob práce s vaším serverom, pretože rozhranie sa jednoducho používa. CD-ROM, na ktorom je Sprievodca nastavením EZ, je pribalené k vášmu serveru iSeries.

Pri konfigurácii servera dodržte tieto kroky:

1. Použite Sprievodcu nastavením EZ. Sprievodcu nájdete na disku CD-ROM, ktorý bol pribalený k vášmu serveru. Pri konfigurácii TCP/IP nasledujte inštrukcie sprievodcu.
2. Spustite TCP/IP
   a. V produkte iSeries Navigator vyberte **server —> Sieť**.
   b. Kliknite pravým tlačidlom myši na **Konfigurácia TCP/IP** a vyberte **Spustiť**. Spustia sa všetky rozhrania a servery, ktoré sa mali spustiť automaticky pri spustení TCP/IP.

Dokončili ste konfiguráciu TCP/IP na vašom serveri. Pomocou produktu iSeries Navigator upravte konfiguráciu tak, ako si to vyžaduje vytváranie vašej siete. V časti Prispôsobenie TCP/IP s produktom iSeries Navigator nájdete informácie o pridávaní trás a rozhraní, alebo v časti Konfigurácia IPv6 zistíte viac o použití Internetového protokolu verzia 6 vo vašej sieti.

Konfigurujte TCP/IP pomocou znakového rozhrania

Ak nemôžete použiť Sprievodcu nastavením EZ v produkte iSeries Navigator, použite namiesto neho znakové rozhranie. Ak napríklad chcete použiť iSeries Navigator na počítači, ktorý pred spustením produktu iSeries Navigator vyžaduje základnú konfiguráciu TCP/IP, mali by ste pri vykonaní tejto základnej konfigurácie použiť znakové rozhranie.

Aby ste mohli vykonať jednotlivé konfiguračné kroky, spomenuté v tejto časti, musí mať váš užívateľský profil mimoriadne oprávnenie *IOSYSCFG. Viac informácií o tomto type oprávnenia nájdete v kapitole o užívateľských profiloch iSeries Security Reference .

Konfiguráciu TCP/IP pomocou znakového rozhrania vykonáte takto:

1. Do príkazového riadku napíšte GO TCPADM, a keď sa vám zobrazí ponuka Administrácia TCP/IP, stlačte Enter.
2. zadaním voľby 1 (Konfigurácia TCP/IP) zobrazte ponuku Konfigurácia TCP/IP (CFGTCP) a stlačte Enter. V tomto menu vyberte konfiguračné úlohy. Skôr než pristúpite ku konfigurácii svojho servera, venujte pár chvíľ prehľadu tejto ponuky.

Vykonaním nasledujúcich krokov nakonfigurujte TCP/IP na svojom serveri.

1. Konfigurácia opisu linky
2. Konfigurácia rozhrania
3. Konfigurácia trasy
4. Definovanie lokálnych názvov domény a hostiteľov
5. Definovanie hostiteľskej tabuľky
6. Spustenie TCP/IP

Konfigurácia opisu linky (Ethernet)

Tieto inštrukcie patria ku konfigurácii TCP/IP cez komunikačný adaptér Ethernet. Ak však používate iný typ adaptéra, ako napríklad token-ring, nájdite si v časti Konfigurácia a odkazy TCP/IP, *Dodatok A*, príkazy určené pre adaptér.

Opis linky nakonfigurujete takto:

1. Do príkazového riadku napíšte CRTLINETH, a keď sa vám zobrazí ponuka Vytvorenie opisu linky (Ethernet) (CRTLINETH), stlačte Enter.
2. Zadajte názov linky a stlačte Enter. (Použite akýkoľvek názov.)
3. Zadajte názov prostriedku a stlačte Enter.

Ďalší postup:
Konfigurácia rozhrania

Konfigurácia rozhrania

Pri konfigurácii rozhrania dodržte tieto kroky:

1. Do príkazového riadku napíšte CFGTCP, a keď sa vám zobrazí ponuka Konfigurácia TCP/IP, stlačte Enter.
2. V menu Konfigurácia TCP/IP označte voľbu 1 (Práca s rozhraniami TCP/IP) a stlačte Enter.
3. Výberom voľby 1 (Pridať) zobrazte displej Pridať rozhranie TCP/IP a stlačte Enter.
4. Zadajte hodnotu adresy, ktorá má zastupovať váš server iSeries, adresu masky podsiete a názov opisu linky, ktorý ste zadali pred chvíľou, a stlačte Enter.

Rozhranie spustíte, ak pre rozhranie, ktoré ste konfigurovali, zadáte voľbu 9 (Spustiť) a stlačíte Enter.

Ďalší postup:
Konfigurácia trasy

Konfigurácia trasy

Na dosiahnutie vzdialenej siete musíte mať zadaný aspoň jeden záznam smerovania. Ak žiadne záznamy smerovania nie sú manuálne pridané, server nemôže dosiahnuť na systémy, ktoré nie sú v tej istej sieti, ku ktorej je pripojený on. Záznamy smerovania musíte pridať aj preto, aby mohli správne fungovať aj vaši klienti TCP/IP, ktorí sa snažia dosiahnuť váš server zo vzdialenej siete.

Definovanie tabuľky smerovania by ste si mali plánovať tak, aby v nej bol vždy minimálne jeden štandardný záznam (*DFTROUTE). Ak sa nenájde zhoda so žiadnym iným záznamom v tabuľke smerovania, sú údaje odoslané na smerovač IP zadaný v prvom dostupnom štandardnom zázname trasy.

Pri konfigurácii štandardnej trasy dodržte tieto kroky:

1. V ponuke Konfigurácia TCP/IP označte voľbu 2 (Práca s trasami TCP/IP) a stlačte Enter.
2. Zadaním voľby 1 (Pridať) zobrazte displej Pridať trasu TCP/IP (ADDTCPRTE) display a stlačte Enter.
3. Zadajte *DFTROUTE ako cieľ trasy, *NONE ako masku podsiete, IP adresu nasledujúceho skoku a stlačte Enter.

Ďalší postup:
Definovanie lokálnych názvov domény a hostiteľov

Definovanie lokálnych názvov domény a hostiteľov

Pri definovaní lokálnych názvov domény a hostiteľov nasledujte tieto kroky:

1. V ponuke Konfigurácia TCP/IP označte voľbu 12 (Zmena domény TCP/IP) a stlačte Enter.
2. Zadajte názvy, ktoré ste si vybrali ako názvy lokálnych hostiteľov a lokálnej domény, ostatné parametre ponechajte, ako boli predvolené a stlačte Enter.

Ďalší postup:
Definovanie hostiteľskej tabuľky

Definovanie hostiteľskej tabuľky

Hostiteľskú tabuľku nadefinujete takto:

1. V ponuke Konfigurácia TCP/IP označte voľbu 10 (Práca so záznamami v hostiteľskej tabuľke TCP/IP) a stlačte Enter.
2. Zadaním voľby 1 (Pridať) zobrazte displej Pridať záznam do hostiteľskej tabuľky TCP/IP a stlačte Enter.
3. Zadajte IP adresu, názov lokálneho hostiteľa a jeho plný názov a stlačte Enter.
4. Ak je to potrebné, zadaním znamenia plus (+) vyhraďte priestor pre viac, než jeden názov hostiteľa.
5. Tieto kroky zopakujte pre každého z hostiteľov v sieti, s ktorými chcete komunikovať podľa názvu a pre každého z nich pridajte nový záznam.

Ďalší postup:
Spustenie TCP/IP

Spustenie TCP/IP

Kým nespustíte TCP/IP, nebudú služby TCP/IP k dispozícii.

TCP/IP spustíte napísaním STRTCP do príkazového riadku.

Príkaz Start TCP/IP (STRTCP) inicializuje a aktivuje proces TCP/IP, spúšťa rozhrania TCP/IP a spúšťa serverové úlohy. Príkazom STRTCP sú spustené len tie TCP/IP rozhrania a servery, ktorých hodnota parametra AUTOSTART je *YES.

Dokončili ste konfiguráciu TCP/IP na svojom serveri. Pomocou produktu iSeries Navigator upravte konfiguráciu tak, ako si to vyžaduje vytváranie vašej siete. V časti Prispôsobenie TCP/IP s produktom iSeries Navigator nájdete informácie o pridávaní trás a rozhraní, alebo v časti Konfigurácia IPv6 zistíte viac o použití Internetového protokolu verzie 6 vo svojej sieti.

Konfigurácia IPv6

Už ste pripravení použiť na svojej sieti IPv6, a začať tak využívať výhody novej generácie internetu. Aby ste mohli využívať funkcie IPv6, musíte konfigurovaním linky určenej pre IPv6 zmeniť konfiguráciu svojho TCP/IP. Konfigurovaná linka musí byť na buď adaptéri Ethernet 2838, alebo 2849, alebo na konfigurovanej tunelovej linke (virtuálnej linke). V týchto témach si prečítate inštrukcie ku konfigurovaniu IPv6:

Požiadavky nastavenia
V tejto téme je vymenovaný zoznam hardvérových a softvérových požiadaviek nevyhnutných pri konfigurácii servera pre IPv6.

Konfigurácia IPv6 pomocou sprievodcu Konfigurácia IPv6
Prezrite si inštrukcie na použitie sprievodcu **Konfigurácia IPv6** pri konfigurácii IPv6 na vašom serveri.

Požiadavky nastavenia

Určite, ktorý z týchto dvoch typov konfigurácie IPv6 je vhodný vo vašej situácii. Ak neviete, ktorý typ si vybrať, preštudujte si ako príklady Scenáre IPv6.

Aby ste na svojom serveri mohli povoliť IPv6, splňte tieto požiadavky:

Pri konfigurácii linky Ethernet pre IPv6:

- OS/400 verzia 5 vydanie 2, alebo vyššie
- iSeries Access pre Windows a iSeries Navigator
  - Sieťový komponent produktu iSeries Navigator
- Adaptér Ethernet 2838, alebo 2849, určený pre IPv6.
- Smerovač umožňujúci IPv6 je nevyhnutný, len ak chcete posielať prevádzku IPv6 mimo aktuálnej siete LAN.
- Protokol TCP/IP (s použitím IPv4) musí byť nakonfigurovaný na osobitnom fyzickom adaptéri, pretože TCP/IP musí byť spustený na serveri. Ak ste svoj server ešte na IPv4 nekonfigurovali, tak si skôr, než budete konfigurovať linku pre IPv4, prezrite si časť Prvá konfigurácia TCP/IP.

Pri vytváraní konfigurovanej tunelovej linky (TNLCFG64):

- OS/400, verzia 5, vydanie 2, alebo vyššie
- iSeries Access pre Windows a iSeries Navigator
  - Sieťový komponent produktu iSeries Navigator
- Skôr, než budete konfigurovať tunelovú linku pre IPv6, musí byť na serveri nakonfigurované TCP/IP (s použitím IPv4). Ak ste svoj server ešte nekonfigurovali na IPv4, pozrite si časť Prvá konfigurácia TCP/IP.

V časti Konfigurácia IPv6 pomocou sprievodcu Konfigurácia IPv6 nájdete pokyny na používanie tohto sprievodcu.

Konfigurácia IPv6 pomocou sprievodcu Konfigurácia IPv6

Aby ste mohli na serveri nakonfigurovať IPv6, musíte pomocou sprievodcu **Konfigurácia IPv6** v produkte iSeries Navigator, zmeniť konfiguráciu servera. IPv6 môže byť konfigurované len z produktu iSeries Navigator a nemôže byť konfigurované zo znakového rozhrania.

Poznámka: Opis linky Ethernet pre IPv6 môžete konfigurovať v znakovom rozhraní pomocou príkazu Create Line Desc (Ethernet) CRTLINETH; musíte ale zadať hexadecimálnu viacnásobnú skupinovú adresu 333300000001. Potom musíte konfiguráciu IPv6 dokončiť pomocou sprievodcu **Konfigurácia IPv6**.

Sprievodca bude vyžadovať nasledujúce vstupy:

Pri konfigurácii linky Ethernet pre IPv6:
Táto konfigurácia vám umožňuje posielať pakety IPv6 lokálnou sieťou (LAN) IPv6. Sprievodca požaduje názov hardvérového komunikačného prostriedku na serveri, na ktorom budete IPv6 konfigurovať; napríklad CMN01. Musí to byť Ethernet adaptér 2838, alebo 2849, ktorý zatiaľ nie je konfigurovaný na IPv4. V časti Vytvorenie lokálnej siete (LAN) IPv6 nájdete scenár popisujúci situáciu, v ktorej by ste linku Ethernet konfigurovali pre IPv6.

Pri vytváraní konfigurovanej tunelovej linky (TNLCFG64):
Táto konfigurácia vám umožňuje posielať pakety IPv6 lokálnou sieťou (LAN) IPv4. Sprievodca vyžaduje pre lokálny koncový bod adresu IPv4 a pre lokálne rozhranie prepojené s tunelom adresu IPv6. Scenáre Zasielanie paketov IPv6 lokálnou sieťou (LAN) IPv4 a Zasielanie paketov IPv6 rozšírenou sieťou (WAN) IPv4 opisujú dve situácie, v ktorých by ste vytvárali konfigurovanú tunelovú linku pre IPv6.

Pri použití sprievodcu **Konfigurácia IPv6**, nasledujte tieto kroky:

1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP**.
2. Kliknite pravým tlačidlom myši na **IPv6** a vyberte **Konfigurácia IPv6**.
3. Pri konfigurácii IPv6 na svojom serveri nasledujte inštrukcie sprievodcu.

Kapitola 7. Prispôsobte si TCP/IP pomocou produktu iSeries Navigator

Keď ste nakonfigurovali TCP/IP, môžete sa rozhodnúť upraviť svoju konfiguráciu. Keďže vaša sieť stále rastie, budete možno potrebovať zmeniť jej vlastnosti, pridať na svoj server rozhrania, alebo trasy. Budete možno potrebovať konfigurovať server na IPv6 (Internetový protokol verzie 6), aby ste mohli používať aplikácie IPv6. Pomocou sprievodcov v produkte iSeries Navigator rýchlo vykonáte väčšinu týchto úloh.

Vyberte si niektorú z tém a prispôsobte svoju konfiguráciu pomocou produktu iSeries Navigator. Tieto témy vám poskytnú počiatočný bod pre spravovanie vašej konfigurácie TCP/IP pomocou produktu iSeries Navigator.

- Zmena nastavení TCP/IP
- Konfigurácia IPv6
- Pridanie rozhrania IPv4
- Pridanie rozhrania IPv6
- Pridanie trás IPv4
- Pridanie trás IPv6

Zmena nastavení TCP/IP

Pomocou produktu iSeries Navigator môžete prezerať a meniť svoje nastavenia TCP/IP. Napríklad, môžete zmeniť vlastnosti pre názov hostiteľa alebo domény, názvový server, záznamy tabuľky hostiteľov, systémové atribúty, obmedzenia portov, servery alebo spojenia klientov. Môžete meniť všeobecné vlastnosti, alebo vlastnosti, ktoré sú vlastné buď IPv4, alebo IPv6, ako napríklad prenosy.

Na všeobecné stránky TCP/IP sa dostanete takto:

1. V produkte iSeries Navigator vyberte **server —> Sieť**.
2. Pravým tlačidlom kliknite na **Konfigurácia TCP/IP** a vyberte **Vlastnosti**, aby sa otvorilo dialógové okno **Vlastnosti TCP/IP**.
3. Ak si chcete zobraziť alebo upraviť informácie o TCP/IP, použite záložky navrchu tohto dialógového okna.

Položky hostiteľskej tabuľky môžete pridávať a meniť takto:

1. V produkte iSeries Navigator vyberte **server —> Sieť**.
2. Kliknite pravým tlačidlom myši na **Konfigurácia TCP/IP** a výberom položky **Hostiteľská tabuľka** otvorte dialóg **Hostiteľská tabuľka**.
3. Pomocou dialógu **Hostiteľská tabuľka** pridávajte, upravujte a odstraňujte položky hostiteľskej tabuľky.

Na stránky s vlastnosťami špecifickými pre IPv4 sa dostanete takto:

1. V produkte iSeries Navigator vyberte **server —> Sieť**.
2. Kliknite pravým tlačidlom myši na **IPv4** a výberom položky **Vlastnosti** otvorte dialóg **Vlastnosti IPv4**.
3. Označením záložiek v hornej časti dialógového okna môžete prezerať a editovať nastavenia vlastností IPv4.

Na stránky s vlastnosťami špecifickými pre IPv6 sa dostanete takto:

1. V produkte iSeries Navigator vyberte **server —> Sieť**.
2. Kliknite pravým tlačidlom myši na **IPv6** a výberom položky **Vlastnosti** otvorte dialóg **Vlastnosti IPv6**.
3. Označením záložiek v hornej časti dialógového okna môžete prezerať a editovať nastavenia vlastností IPv6.

| **Konfigurácia IPv6**

| Ak IPv6 ešte nepoznáte, nájdete jeho prehľad v časti Internetový protokol verzie 6 (IPv6).

| Aby ste mohli konfigurovať IPv6, musíte pomocou sprievodcu **Konfigurácia IPv6** zmeniť konfiguráciu
| servera. Pred použitím sprievodcu si v časti Konfigurácia IPv6 nájdite inštrukcie a špeciálne požiadavky.

| **Pridanie rozhrania IPv4**

| Nové rozhranie IPv4 vytvoríte takto:
| 1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP —> IPv4**.
| 2. Kliknite pravým tlačidlom myši na **Rozhrania** označte **Nové rozhranie** a výberom **Lokálna sieť**,
| **Rozšírená sieť**, alebo **Virtuálny IP** vytvorte správny typ rozhrania IPv4.
| 3. Nasledujte inštrukcie sprievodcu a vytvorte nové rozhranie IPv4.

| **Pridanie rozhrania IPv6**

| Nové rozhranie IPv6 vytvoríte takto:
| 1. V produkte iSeries Navigator, vyberte **server —> Sieť —> Konfigurácia TCP/IP —> IPv6**.
| 2. Pravým tlačidlom kliknite na **Rozhrania** a vyberte **Nové rozhranie**.
| 3. Nasledujte inštrukcie sprievodcu a vytvorte nové rozhranie IPv6.

| **Pridanie trás IPv4**

| Všetky vami vykonané zmeny v smerovacích informáciách sa okamžite prejavia.

| Pri konfigurácii novej trasy IPv4 dodržte tieto kroky:
| 1. V produkte iSeries Navigator vyberte **server —> Sieť —> Konfigurácia TCP/IP —> IPv4**.
| 2. Pravým tlačidlom myši kliknite na **Trasy** a vyberte **Nová trasa**.
| 3. Pri konfigurácii novej trasy IPv4 nasledujte inštrukcie sprievodcu.

| **Pridanie trás IPv6**

| Všetky vami vykonané zmeny v smerovacích informáciách sa okamžite prejavia.

| Pri konfigurácii novej trasy IPv6 dodržte tieto kroky:
| 1. V produkte iSeries Navigator, vyberte **server —> Sieť —> Konfigurácia TCP/IP —> IPv6**.
| 2. Pravým tlačidlom myši kliknite na **Trasy** a vyberte **Nová trasa**.
| 3. Nasledujte inštrukcie sprievodcu a vytvorte novú trasu IPv6.

Kapitola 8. Odstraňovanie problémov s IPv6

Ak máte na serveri nakonfigurovaný IPv6, môžete používať niekoľko rovnakých nástrojov na odstraňovanie problémov ako pri IPv4. Napríklad nástroje ako sledovanie trasy a príkaz PING akceptujú adresné formáty tak IPv4, ako aj IPv6, takže ich môžete použiť na testovanie pripojenia a trás v oboch typoch sietí. Na dôvažok môžete použiť funkciu sledovanie komunikácií na oba typy liniek, IPv4 aj IPv6.

V časti Odstraňovanie problémov s TCP/IP nájdete všeobecného sprievodcu odstraňovaním problémov, ktorý vám ponúka spôsoby riešenia problémov spojené s IPv4 a IPv6.

Kapitola 9. Informácie, týkajúce sa nastavenia TCP/IP

Teraz, keď máte server spustený a funkčný, môžete sa spýtať sám seba: Čo viac môžem urobiť pre svoj server? Nižšie sú uvedené manuály a Redbooks IBM (vo formáte PDF) a téma Informačné centrum, ktorá obsahuje odkazy na témy o nastavení TCP/IP. Dokumenty PDF si môžete prezerať, alebo vytlačiť. Pomocou nasledujúcich odkazov nastavíte na svojom serveri iSeries väčšinu TCP/IP:

Manuály

- **Konfigurácia TCP/IP a odkazy** (približne 100 strán)
  Táto kniha prináša informácie o konfigurácii Transmission Control Protocol/Internet Protocol (TCP/IP) a o fungovaní a spravovaní vašej siete.

- **Tipy a nástroje na zabezpečenie servera iSeries** (približne 254 strán)
  Táto kniha poskytuje základné odporúčania pre používanie bezpečnostných vlastností servera iSeries pri ochrane servera a s tým súvisiacich funkcií.

Redbooks

- **Výučbový program a technický prehľad TCP/IP**
  Táto redbook prináša základy TCP/IP.

- **TCP/IP pre AS/400: More Cool Things Than Ever**
  V tomto redbook nájdete rozsiahly zoznam bežných aplikácií a služieb TCP/IP.

IPv6

- **The Internet Engineering Task Force (IETF)** (http://www.ietf.cnri.reston.va.us/)
  Dozviete sa o skupine ľudí, ktorí vyvinuli Internetový protokol, vrátane IPv6.

- **IP Version 6 (IPv6)** (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  Dozviete sa o aktuálnych špecifikáciách IPv6 a nájdete odkazy na ďalšie zdroje informácií o IPv6.

- **Fórum IPv6**(http://www.ipv6forum.com/)
  Prečítajte si články s novinkami a prípady, ktoré vás oboznámia s najnovším vývojom v IPv6.

Ostatné informácie

- **TCP/IP**
  Táto téma obsahuje informácie o TCP/IP aplikáciách a službách, ktoré sa už netýkajú konfigurácie.

Ak si chcete dokument typu PDF uložiť na svojej pracovnej stanici s cieľom prezerania alebo tlače:

1. Vo svojom prehliadači kliknite pravým tlačidlom myši na PDF (hore uvedená linka).
2. Kliknite na **Save Target As...**.
3. Prejdite do adresára, do ktorého chcete uložiť tento PDF súbor.
4. Kliknite na **Save**.

Ak na prezeranie alebo tlač týchto PDF potrebujete Adobe Acrobat Reader, môžete si ho stiahnuť z internetovej stránky (www.adobe.com/prodindex/acrobat/readstep.html) .

Vytlačené v USA