IBM

eserver

iSeries

Služby vzdialeného prístupu: Spojenia PPP

IBM Confidential

IBM

@server

iSeries

Služby vzdialeného prístupu: Spojenia PPP

IBM Confidential

Obsah

Časť 1. Služby vzdialeného prístupu: Spojenia PPP

Protokol point-to-point (PPP) je internetovská norma pre prenos údajov po sériových linkách. Ide o najpoužívanejší spojovací protokol u poskytovateľov služieb internetu (ISP). PPP umožňuje individuálnym počítačom pripojenie k sieťam, ktoré ďalej poskytnú prístup na internet. iSeries server obsahuje ako súčasť svojej konektivity sietí WAN (wide-area network) aj PPP podporu TCP/IP.

Údaje medzi lokalitami môžete vymieňať pomocou PPP, ktorým pripojíte vzdialený počítač k svojmu iSeries serveru. Prostredníctvom PPP môžu vzdialené systémy, ktoré sú pripojené na váš iSeries server, pristupovať k prostriedkom alebo iným počítačom, ktoré patria do rovnakej siete ako váš server. Svoj iSeries server môžete nakonfigurovať tak, aby sa pripojil na internet pomocou PPP. Sprievodca vytáčaným pripojením iSeries Navigator vás môže sprevádzať procesom pripojenia vášho servera iSeries na internet alebo na internú sieť.

- Čo je nové vo V5R2? popisuje aktualizácie Služieb vzdialeného prístupu (RAS) v tejto verzii.
- Tlač tejto témy vám umožňuje stiahnuť alebo vytlačiť PDF verziu týchto informácií.

Vysvetlenie Služieb vzdialeného prístupu: Spojenia PPP

Tieto témy vám rýchlo predstavia služby vzdialeného prístupu na vašom serveri iSeries 400. Uvedené témy vám pomôžu naplánovať prostredie PPP pre vašu sieť.

- **Scenáre PPP** sú príklady realizácií rôznych implementácií konektivity PPP. Každý príklad obsahuje pokyny a vzorové hodnoty na konfiguráciu daného spojenia PPP.
- **Koncepty PPP** poskytuje informácie o konceptoch PPP a o požiadavkách na server iSeries 400 pri pripojeniach PPP.
- **Plánovanie PPP** poskytuje informácie o konceptoch PPP a o požiadavkách na server iSeries 400 pri pripojeniach PPP.

Používanie služieb vzdialeného prístupu: Spojenia PPP

Tieto témy vám pomôžu pri konfigurácii a riadení spojení PPP na vašom serveri iSeries 400.

- **Konfigurácia PPP** určuje základné kroky pri konfigurácii pripojenia PPP.
- **Riadenie PPP** poskytuje informácie, ktoré môžete použiť ako sprievodcu pri riadení pripojení PPP.
- **Odstraňovanie problémov s PPP** opisuje základné chyby pripojení PPP a upozorňuje vás na informácie podstatné pre odstraňovanie problémov.

Ďalej tu môžete nájsť iné informácie o PPP. Táto strana obsahuje odkazy na užitočné a súvisiace informácie o iSeries serveri.

Kapitola 1. Čo je nové vo V5R2?

Vo V5R2 môže iSeries Navigator povoliť pripojenia PPP cez Ethernet (PPPoE) pochádzajúce zo servera iSeries. Táto podpora, na vytvorenie spojenia PPP s použitím adaptéra Ethernet LAN pripojeného k modemu DSL, poskytuje nový typ virtuálnej linky PPPoE, ktorá je zviazaná s fyzickou linkou Ethernet. Keď je už spojenie medzi iSeries a ISP vytvorené, môžu jednotliví užívatelia siete LAN pristupovať k ISP cez spojenie iSeries PPPoE. K tejto novej funkcii sa môžete dostať cez dialóg Profilu pôvodcu spojenia, alebo cez Univerzálneho sprievodcu spojením.

Viac informácií nájdete v časti Pripojte svoj server iSeries k prístupovej zbernici PPPoE

Niekoľko doplnkov k produktu iSeries Navigator teraz uľahčuje konfiguráciu a spravovanie pripojení PPP, vrátane:

- Konfiguračný dialóg pre DHCP-WAN teraz automaticky skontaktuje DHCP server a klientske rozhranie a určí IP adresu pre klientske rozhranie DHCP-WAN. Tento dialóg spustíte:
  - Rozviňte **Sieť > Služby vzdialeného prístupu**
  - Kliknite pravým tlačidlom myši na **Služby vzdialeného prístupu**
  - Vyberte **Služby**
  - Vyberte záložku **DHCP-WAN**
- Vylepšené dialógové okno stavu pripojenia teraz zobrazuje detaily pripojenia pre L2TP, viacskokové L2TP, viaclinkové pripojenia a pripojenia PPP cez Ethernet, vďaka čomu je spravovanie pripojení PPP jednoduchšie.
- Do zoznamu úloh bola pridaná možnosť vytvoriť profily pripojenia pôvodcu a príjemcu a skupinových politík prístupu.
- Nový sprievodca vytáčaným pripojením a Univerzálny sprievodca pripojením boli premenované a teraz sa volajú Nové internetové, alebo vytáčané ISP pripojenie a Nové univerzálne pripojenie IBM.
- Profily pôvodcu pripojenia si teraz môžu ″vypožičať″ linku PPP a modem priradený profilu príjemcu pripojenia, ktorý očakáva volanie. Keď sa spojenie ukončí, pôvodca pripojenia ″vráti″ linku PPP a modem profilu adresáta pripojenia. Túto novú funkciu povolíte, ak vyberiete možnosť **Povoliť dynamické zdieľanie prostriedkov** zo záložky Modem v konfiguračnom dialógu linky PPP. Linky PPP môžete konfigurovať v záložke Pripojenie v Profiloch pôvodcu a adresáta pripojenia.
- Ak sa oblasti vlastnosti linky práve používajú, nemôžu byť zmenené. Predchádza sa tým možným problémom s oblasťou linky.
- Podpora prevádzkových režimov Inciovanie na vyžiadanie a Vzdialené vytáčania na vyžiadanie bola z Profilov pôvodcu spojenia používajúcich spojenie L2TP vypustená.

Kapitola 2. Tlač tejto témy

Ak si chcete prezrieť alebo vytlačiť tento dokument, môžete si pozrieť alebo stiahnuť jeho PDF verziu. Na prezeranie PDF súborov potrebujete Adobe® Acrobat® Reader. Môžete si ho stiahnuť na linke Adobe  .

Ak si chcete zobraziť, alebo stiahnuť verziu vo formáte PDF, vyberte Služby vzdialeného prístupu: pripojenia PPP  (277 kB, alebo asi 58 strán).

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

1. Vo svojom prehliadači otvorte PDF (kliknite na predchádzajúci odkaz).
2. V ponuke svojho prehliadača kliknite na **Súbor**.
3. Kliknite na **Uložiť ako**.
4. Prejdite do adresára, do ktorého chcete uložiť dokument PDF.
5. Kliknite na **Uložiť**.

Kapitola 3. Scenáre PPP

Nasledujúce scenáre vám pomôžu pochopiť, ako pracuje PPP a ako môžete do vašej siete implementovať prostredie PPP. Tieto scenáre vám priblížia základné koncepty PPP, ktoré môžu byť užitočné pre začiatočníkov i skúsených používateľov pri plnení úloh plánovania a konfigurácie.

Scenár: Pripojenie vášho servera iSeries k prístupovej zbernici PPPoE

Mnohí ISP ponúkajú prístup na internet s vysokou rýchlosťou cez DSL s použitím PPPoE. Server iSeries sa môže pripojiť k týmto poskytovateľom služieb a ponúknuť pripojenie s veľkou šírkou pásma, ktoré uchováva výhody PPP.

Scenár: Pripojenie vzdialených klientov na svoj server iSeries vytáčaným pripojením

Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti, ktorí sa napájajú na sieť, môžu získať prístup na iSeries sever pomocou PPP.

Scenár: Pripojenie vašej siete modemom na internet

Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na internet. Na pripojenie iSeries servera k poskytovateľovi služieb internetu (ISP) môžu použiť modem. PC klienti, pripojení k LAN, môžu komunikovať s internetom pomocou iSeries servera ako gateway.

Scenár: Prepojenie vašich vnútropodnikových a vzdialených sietí modemom

Modem umožňuje, aby si dve vzdialené lokality (napríklad centrála a pobočka) navzájom vymieňali údaje. PPP dokáže dané dve LAN vzájomne prepojiť tak, že vytvorí prepojenie medzi iSeries serverom v centrále a ďalším iSeries serverom v pobočke.

Scenár: Overovanie vytáčaného pripojenia pomocou RADIUS NAS

Network Access Server (NAS), spustený na serveri iSeries, dokáže z klientov pripojených vytáčaním smerovať požiadavky na overenie na osobitný server RADIUS. Ak sa potvrdí ich pravosť, môže RADIUS skontrolovať aj IP adresu a porty užívateľov.

Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú skupinové politiky a filtrovanie IP

Skupinové politiky prístupu určujú pre pripojenie rozličné skupiny užívateľov a umožňujú vám na celú skupinu použiť niektoré spoločné atribúty pripojenia a nastavenia bezpečnosti. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych IP adries.

Scenár: PPP a DHCP na jednom serveri iSeries

Pripájajúci sa klienti alebo vzdialení používatelia môžu s PPP získať prístup k iSeries serveru v sieti firmy. Klient DHCP Wide Area Network (WAN) na tom istom serveri iSeries umožňuje užívateľom so vzdialeným prístupom, použitím rovnakých služieb ako pri užívateľoch LAN, získať dynamicky pridelenú IP adresu.

Scenár: Profily DHCP a PPP na rozličných serveroch iSeries

Otázky bezpečnosti či fyzické rozvrhnutie siete vedú väčšinu firiem k tomu, aby osamostatňovali sieťové služby a rozdeľovali ich na rozličné servery. Tento scenár rieši zvýšenú komplexnosť samostatných serverov pre PPP a DHCP. Podobne ako predchádzajúci scenár, toto nastavenie umožňuje vzdialeným používateľom pripojiť sa a získať prístup do siete danej firmy.

Scenár: PPP a VPN: L2TP nevynútený tunel chránený VPN

Pobočka sa môže pripojiť k centrále cez protokol L2TP (Layer 2 Tunnel Protocol). Nevynútený tunel L2TP vytvára virtuálnu linku PPP. V konečnom dôsledku L2TP rozširuje sieť centrály tak, že pobočka sa javí ako súčasť podsiete centrály. Dátovú prevádzku v tuneli L2TP chráni VPN.

Scenár: Pripojenie vášho servera iSeries k prístupovej zbernici PPPoE

Situácia: Vaše podnikanie si vyžaduje rýchlejšie pripojenie na internet, takže sa u svojho lokálneho ISP zaujímate o službu DSL. Po úvodnom prieskume zistíte, že váš ISP používa na pripájanie svojich klientov PPPoE. Radi by ste použili toto pripojenie na širokopásmové pripojenie na internet cez svoj server iSeries.

Obrázok 1. Pripojenie vášho servera iSeries k ISP pomocou PPPoE

Riešenie: Pripojenie PPPoE môžete podporiť ISP cez server iSeries. Server iSeries nachádza využitie pre nový typ virtuálnej linky PPPoE, ktorá je viazaná na fyzickú linku Ethernet nakonfigurovanú na použitie adaptéra typu 2838 Ethernet. Táto virtuálna linka podporuje protokol relácie PPP cez Ethernet LAN pripojenú k modemu DSL, ktorý poskytuje bránu k vzdialenému ISP. Toto umožňuje užívateľom v sieti LAN využívať vysokorýchlostný prístup na internet pomocou spojenia PPPoE cez server iSeries. Keď je už spojenie medzi iSeries a ISP vytvorené, môžu jednotliví užívatelia siete LAN pristupovať k ISP cez PPPoE s použitím IP adries vyhradených pre server iSeries. Pre poskytnutie vyššej bezpečnosti môžu byť pravidlá filtrovania použité na virtuálnu linku PPPoE, aby obmedzili konkrétnu prichádzajúcu internetovú komunikáciu.

Vzorová konfigurácia:

1. Nakonfigurujte pripájacie zariadenie na pripojenie k svojmu ISP.
2. Na svojom iSeries serveri nakonfigurujte profil pôvodcu spojenia.
   Nezabudnite vybrať tieto informácie:
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: PPP cez Ethernet
   - **Prevádzkový režim**: Iniciátor

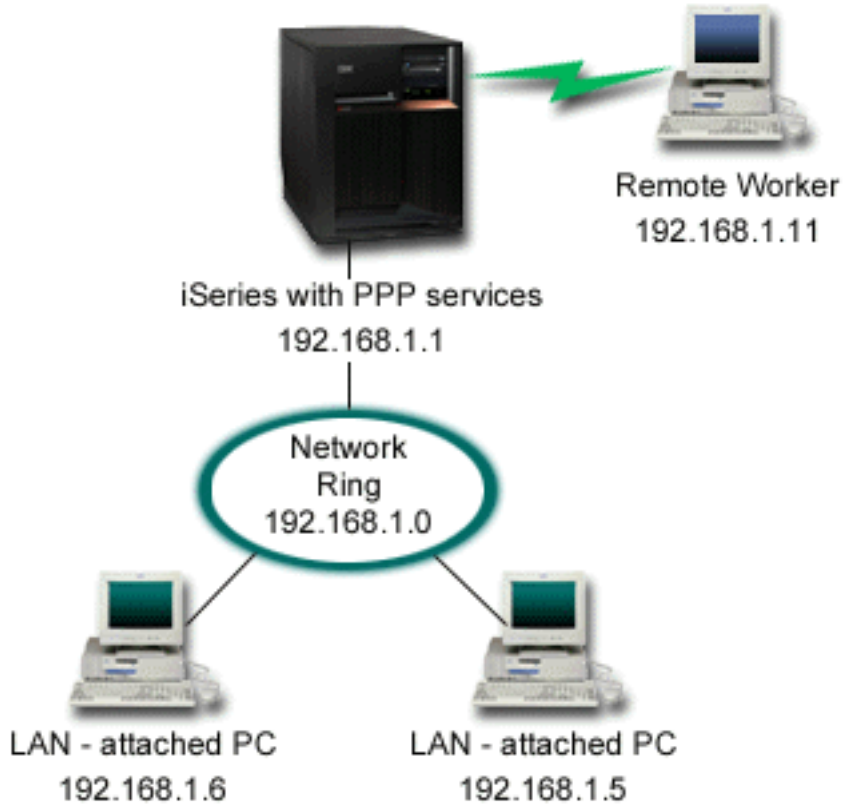
- **Konfigurácia linky**: samostatná linka

3. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a popis profilu pôvodcu. Tento názov sa bude odvolávať na profil pripojenia, aj na virtuálnu linku PPPoE.
4. Kliknite na stranu **Spojenie**. Vyberte **názov virtuálnej linky PPPoE**, ktorý sa zhoduje s názvom tohto profilu pripojenia. Keď označíte linku, zobrazí iSeries Navigator dialóg vlastností linky.
   a. Na strane **Všeobecné** zadajte zmysluplný opis virtuálnej linky PPPoE.
   b. Kliknite na stranu **Linka**. Zo zoznamu názvov fyzických liniek vyberte linku Ethernet, ktorú bude pripojenie používať a kliknite na **Otvoriť**. Ak potrebujete nadefinovať novú linku Ethernet, napíšte jej názov a kliknite na **Nová**. iSeries Navigator zobrazí dialóg vlastností linky Ethernet. **Poznámka:** Pripojenie PPPoE vyžaduje adaptér Ethernet 2838.
      1) Na strane **Všeobecné** zadajte zmysluplný opis linky Ethernet a overte si, že definícia linky používa požadované hardvérové prostriedky.
      2) Kliknite na stranu **Linka**. Zadajte vlastnosti fyzickej linky Ethernet. Viac informácií nájdete v dokumentácii k svojej karte Ethernet a v online pomoci.
      3) Kliknite na stranu **Ďalšie**. Zadajte úroveň prístupu a oprávnenia, ktoré na túto linku budú potrebovať ostatní užívatelia.
      4) Kliknutím na **OK** sa vrátite na stranu vlastností virtuálnej linky PPPoE.
   c. Po kliknutí na **Limity** nadefinujete vlastnosti overovania LCP, alebo sa kliknutím na **OK** vrátite na stranu Nový profil **pripojenia** Point-to-Point.
5. Ak váš ISP vyžaduje, aby sa server iSeries sám autentifikoval, alebo ak chcete, aby server iSeries autentifikoval vzdialený server, kliknite na stranu **Autentifikácia**. Viac informácií nájdete v časti Autentifikácia systému.
6. Kliknite na stranu **Nastavenia TCP/IP** a zadajte pre tento profil pripojenia parametre spracovávanie IP adries. Ak chcete užívateľom v sieti LAN povoliť pripojenie k ISP pomocou IP adries vyhradených pre server iSeries, označte **Schovať adresy (Plné maskovanie)**.
7. Kliknite na stranu **DNS**, zadajte IP adresu DNS servera, ktorú vám oznámil ISP.
8. Ak chcete určiť subsystém, na ktorom má byť spustená úloha pripojenia, kliknite na stranu **Ďalšie**.
9. Kliknutím na **OK** dokončite profil.

Viac informácií o obmedzení prístupu užívateľov k externým IP adresám, alebo k prostriedkom iSeries, nájdete v častiach filtrovanie IP a Skupinové politiky prístupu.

Scenár: Pripájanie vzdialených klientov na svoj server iSeries vytáčaným pripojením

Situácia: Ako správca siete vašej firmy musíte spravovať iSeries server aj sieťových klientov. Namiesto každodenného chodenia do práce, kde riešite problémy a opravujete chyby, by ste uvítali prácu zo vzdialenej lokality, napríklad z domu. Keďže vaša firma nemá pripojenie na sieť previazané s internetom, mohli by ste sa pripojiť k svojmu iSeries serveru pomocou spojenia PPP. Navyše, momentálne máte k dispozícii len svoj modem 7852-400 ECS, ktorý by ste chceli použiť pre svoje pripojenie.



Obrázok 2. Pripojenie vzdialených klientov na váš iSeries server

Riešenie: Pomocou PPP môžete pripojiť svoje domáce PC k iSeries serveru, pričom použijete svoj modem. Keďže na tento typ pripojenia PPP používate svoj modem ECS, musíte si overiť, či máte modem nakonfigurovaný na synchrónny aj asynchrónny režim. Uvedená ilustrácia zobrazuje iSeries server so službami PPP, ktorý je pripojený na LAN s dvoma PC. Diaľkový pracovník potom zavolá na iSeries server, prebehne overenie a stane sa súčasťou pracovnej siete (192.168.1.0). V tomto prípade je najjednoduchšie priradiť volajúcemu klientovi statickú IP adresu.

Na autentifikáciu so serverom iSeries využíva vzdialený užívateľ CHAP-MD5. iSeries nemôže používať MS_CHAP, preto si overte, či je váš klient PPP nastavený na použitie CHAP-MD5.

Ak chcete, aby mali vaši vzdialení pracovníci prístup do firemnej siete tak, ako sa to uvádza vyššie, musí byť prevádzanie IP nastavené v zásobníku TCP/IP aj vo vašom profile adresáta PPP a musí byť správne nakonfigurované smerovanie IP. Ak chcete obmedziť alebo zabezpečiť, aké úkony môže na vašej sieti vykonať daný vzdialený pracovník, pomocou pravidiel filtrovania môžete spracovať ich IP pakety.

Vo vyššie uvedenom príklade bol len jeden vzdialený pripájajúci sa klient, pretože modem ECS dokáže spracovať len jedno spojenie naraz. Ak vaše potreby vyžadujú, aby volalo viac klientov simultánne, zájdite do plánovacej časti, kde nájdete hardvérové a softvérové požiadavky.

Vzorová konfigurácia:

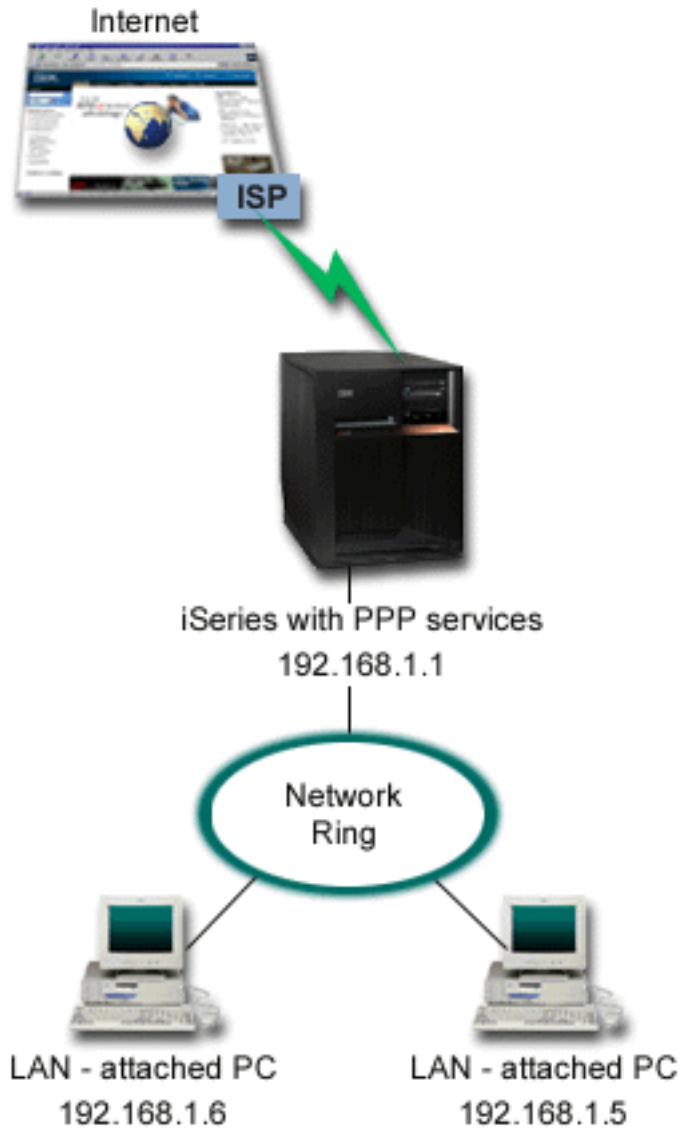
1. Nakonfigurujte Dial-up Networking a vytvorte telefonické spojenie na vzdialenom PC.
2. Nakonfigurujte Profil príjemcu spojenia na vašom iSeries serveri.
   Nezabudnite vybrať tieto informácie:
   - **Typ protokolu**: PPP

- **Typ pripojenia**: Komutovaná linka
- **Režim prevádzky**: Odpovedať
- **Konfigurácia linky**: V závislosti od prostredia to môže byť samostatná linka, alebo oblasť linky.

3. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a popis profilu príjemcu.
4. Kliknite na stranu **Spojenie**. Vyberte príslušný **Názov linky** alebo vytvorte nový názov tak, že ho napíšete a kliknete na **Nový**.
   a. Na strane **Všeobecné** vyznačte existujúce hardvérové prostriedky a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na stranu **Modem**. Zo Zoznamu názvov vyberte modem **IBM 2772**.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
5. Kliknite na stranu **Autentifikácia**.
   a. Označte **Na overenie identity vzdialeného systému požaduj tento server iSeries**.
   b. Vyberte **autentifikovať lokálne pomocou validizačného zoznamu** a do validizačného zoznamu pridajte nového vzdialeného používateľa.
   c. Vyberte **Povoliť zašifrované heslo (CHAP-MD5)**.
6. Kliknite na stranu **Nastavenia TCP/IP**.
   a. Nastavte lokálnu IP adresu na 192.168.1.1.
   b. Ako vzdialenú adresu vyberte **Pevná IP adresa** so začiatočnou adresou 192.168.1.11.
   c. Vyberte **Povoliť vzdialenému systému prístup do iných sietí**.
7. Kliknutím na **OK** dokončite profil.

Scenár: Pripojenie vašej siete LAN modemom na internet

Situácia: Vnútropodniková aplikácia, ktorú vaša firma momentálne používa, vyžaduje, aby používatelia mali prístup na internet. Keďže táto aplikácia nevyžaduje výmenu veľkých objemov dát, radi by ste na pripojenie svojho servera iSeries a klientov v sieti LAN na internet použili modem. V ďalšom popise sa uvádza príklad riešenia tejto situácie.



Obrázok 3. Pripojenie LAN na internet pomocou modemu

Riešenie: Svoj modem ECS (alebo iný kompatibilný modem) môžete použiť na pripojenie iSeries servera k svojmu poskytovateľovi služieb internetu (ISP). Na serveri musíte vytvoriť profil pôvodcu PPP, a tak vytvoriť pripojenie PPP k ISP.

Ak ste vytvorili prepojenie medzi iSeries a ISP, vaše PC zapojené do LAN môže komunikovať s internetom, pričom iSeries bude používať ako gateway. Skontrolujte, či je v profile pôvodcu zapnutá voľba Skryť adresy, aby mohli s internetom komunikovať aj klienti LAN, ktorí majú vyhradené IP adresy.

Keď máte iSeries aj sieť pripojenú na internet, musíte si byť vedomý bezpečnostných rizík, ktoré z toho vyplývajú. U svojho ISP sa poinformujte o jeho bezpečnostnej politike a uskutočnite ďalšie kroky na ochranu svojho servera a siete.

Ak na tento typ pripojenia používate modem ECS, nastavte si ho na asynchrónnu komunikáciu. Šírka pásma závisí od toho, ako používate internet. Viac sa o možnosti zvýšenia šírky pásma pripojenia naučíte v časti plánovanie.

Vzorová konfigurácia:

1. Na svojom iSeries serveri nakonfigurujte profil pôvodcu spojenia.

   Nezabudnite vybrať tieto informácie:

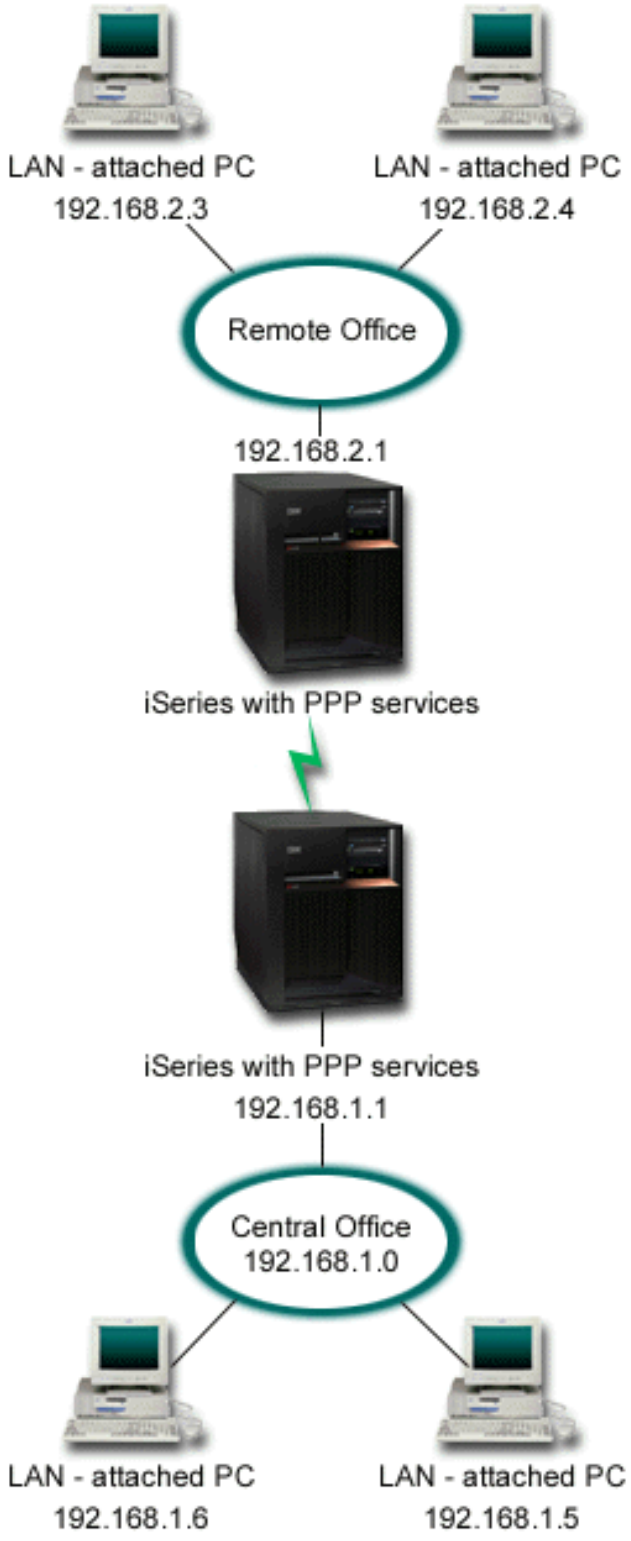
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Vytáčať
   - **Konfigurácia linky**: V závislosti od prostredia to môže byť samostatná linka, alebo oblasť linky.
2. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a popis profilu pôvodcu.
3. Kliknite na stranu **Spojenie**. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane **Všeobecné** z vlastností novej linky vyznačte existujúci hardvérový prostriedok a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na stranu **Modem**. Zo zoznamu Výber názvu vyberte modem, ktorý používate.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
4. Kliknite na **Pridať** a napíšte telefónne číslo, ktoré sa má vytočiť pri pripájaní na server ISP. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na stranu **Autentifikácia** a označte **Povoliť vzdialenému systému overenie identity tohto servera iSeries**. Zvoľte autentifikačný protokol a zadajte prípadné požadované meno používateľa alebo heslo.
6. Kliknite na stranu Nastavenia TCP/IP.
   a. Vyberte **Priradené vzdialeným systémom** pre lokálne i vzdialené IP adresy.
   b. Vyberte **Pridať vzdialený systém ako štandardnú trasu**.
   c. Začiarknite **Skryť adresy**, aby vaše interné IP adresy nepresmerovali na internet.
7. Kliknite na stranu **DNS**, zadajte IP adresu DNS servera, ktorú vám oznámil ISP.
8. Kliknutím na **OK** dokončite profil.

Ak chcete použiť profil spojenia na pripojenie na internet, pravým tlačidlom myši kliknite na profil spojenia z Operations Navigator a vyberte **Spustiť**. Spojenie je úspešné, keď sa stav zmení na **Aktívny**. Aby ste zaktualizovali obrazovku, použite obnovenie.

Poznámka: Musíte skontrolovať aj to, či majú ostatné systémy na vašej sieti zadefinované správne smerovanie, takže prevádzka TCP/IP na internet z týchto systémov sa bude posielať na iSeries server.

Scenár: Prepojenie vašej vnútropodnikovej a vzdialenej siete modemom

Situácia: Predpokladajme, že máte pobočku a centrálu na dvoch rôznych miestach. Pobočka sa musí denne spájať s centrálou a vymieňať si databázové informácie v aplikáciách zadávania dát. Množstvo vymenených dát si ešte nevyžaduje kúpu fyzického sieťového spojenia, preto ste sa rozhodli, že obe siete prepojíte pomocou modemov.



Obrázok 4. Prepojenie vašej vnútropodnikovej a vzdialenej siete modemom

Riešenie: PPP dokáže vzájomne prepojiť dve LAN tak, že zavedie prepojenie medzi každým iSeries serverom, ako to ukazuje uvedená ilustrácia. V takom prípade predpokladajme, že vzdialená kancelária iniciuje pripojenie k ústrednej kancelárii. Na vzdialenom iSeries serveri by ste mali nakonfigurovať profil pôvodcu a na serveri centrály profil príjemcu.

Ak počítače vzdialenej kancelárie potrebujú prístup k vnútropodnikovej sieti LAN (192.168.1.0), bude profil príjemcu ústredne potrebovať zapnuté postúpenie IP a pre počítače by malo byť povolené smerovanie IP adries (v tomto príklade 192.168.2, 192.168.3, 192.168.1.6 a 192.168.1.5). Tiež musí byť aktivované postúpenie IP pre zásobník TCP/IP. Táto konfigurácia umožňuje základnú komunikáciu TCP/IP medzi sieťami LAN. Mali by ste uvážiť bezpečnostné faktory a DNS na preklad názvov hostiteľov medzi LAN.

Vzorová konfigurácia:

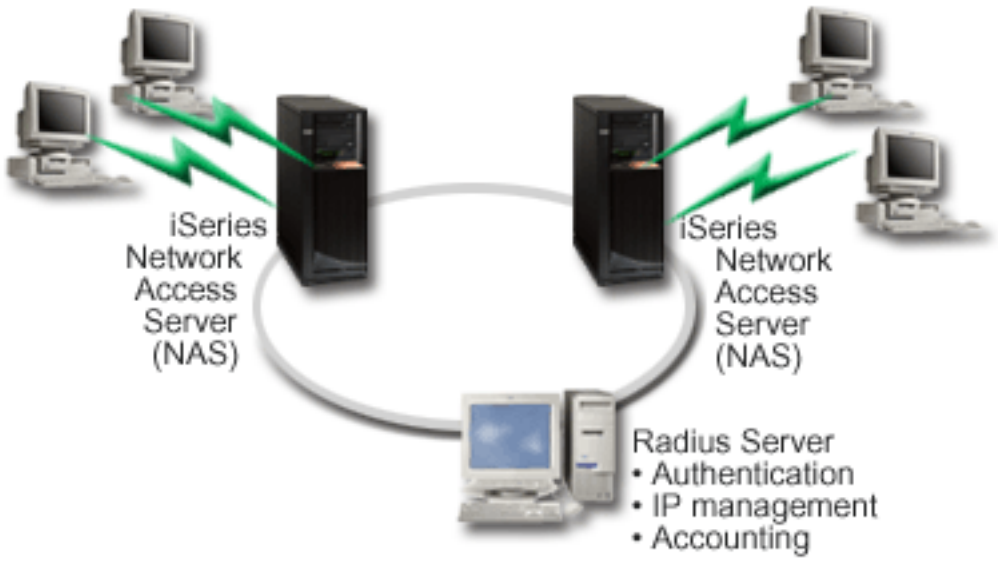
1. Nakonfigurujte profil pôvodcu spojenia na iSeries serveri vzdialenej pobočky.
   Nezabudnite vybrať tieto informácie:
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Vytáčať
   - **Konfigurácia linky**: V závislosti od prostredia to môže byť samostatná linka, alebo oblasť linky.
2. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a popis profilu pôvodcu.
3. Kliknite na stranu **Spojenie**. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane **Všeobecné** z vlastností novej linky vyznačte existujúci hardvérový prostriedok a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na stranu **Modem**. Zo zoznamu Výber názvu vyberte modem, ktorý používate.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
4. Kliknite na **Pridať** a napíšte telefónne číslo, ktoré sa má vytočiť pri pripájaní na iSeries server v centrále. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na stranu **Autentifikácia** a označte **Povoliť vzdialenému systému overiť identitu tohto servera iSeries**. Vyberte **Požadovať zašifrované heslo (CHAP-MD5)** a vložte požadované meno používateľa alebo heslo.
6. Kliknite na stranu **Nastavenia TCP/IP**.
   a. Pre lokálnu IP adresu vyberte z výberového okna **Použiť pevnú IP adresu** IP adresu rozhrania LAN vzdialenej pobočky (192.168.2.1).
   b. Pre vzdialenú IP adresu vyberte **Priradená vzdialeným systémom**.
   c. V časti pre smerovanie vyberte **Pridať vzdialený systém ako štandardnú trasu**.
   d. Kliknutím na **OK** dokončite profil pôvodcu.
7. Nakonfigurujte **Profil príjemcu spojenia** na iSeries serveri v centrále.
   Nezabudnite vybrať tieto informácie:
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Odpovedať
   - **Konfigurácia linky**: V závislosti od prostredia to môže byť samostatná linka, alebo oblasť linky.
8. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a popis profilu príjemcu.
9. Kliknite na stranu **Spojenie**. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane **Všeobecné** vyznačte existujúce hardvérové prostriedky a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na stranu **Modem**. Zo zoznamu Výber názvu vyberte modem, ktorý používate.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.

10. Kliknite na stranu **Autentifikácia**.
    a. Skontrolujte **Na overenie identity vzdialeného systému požaduj tento server iSeries**.
    b. Pridajte nového vzdialeného používateľa do validizačného zoznamu.
    c. Začiarknite autentifikáciu CHAP-MD5.
11. Kliknite na stranu **Nastavenia TCP/IP**.
    a. Pre lokálnu IP adresu vyberte z výberového okna IP adresu rozhrania centrály (192.168.1.1).
    b. Pre vzdialenú IP adresu vyberte **Založená na ID používateľa vzdialeného systému**. Objaví sa dialógové okno IP adresy definované podľa mena používateľa. Kliknite na **Pridať**. Vyplňte polia Užívateľské meno volajúceho, IP adresa a Maska podsiete. V našom prípade sa použijú tieto nastavenia:
       - Užívateľské meno volajúceho: vzdialená_strana
       - IP adresa: 192.168.2.1
       - Maska podsiete: 255.255.255.0

       Kliknite na **OK** a opätovným kliknutím na **OK** sa vrátite na stranu Nastavenia TCP/IP.
    c. Vyberte **Postupovanie IP**, čím umožníte ostatným systémom v sieti používať tento iSeries server ako gateway.
12. Kliknutím na **OK** dokončite profil príjemcu.

Scenár: Overovanie vytáčaných pripojení pomocou RADIUS NAS

Situácia: Vaša vnútropodniková sieť má vzdialených užívateľov pripájajúcich sa k vašim dvom serverom iSeries vytáčaným pripojením z distribuovanej vytáčanej siete. Chceli by ste vytvoriť spôsob centralizovania autentifikácie, služieb a spravovanie kont, povoľujúci jednému serveru spracovávať požiadavky na overenie platnosti užívateľských ID a hesiel a určovať, ktoré IP adresy im môžu byť pridelené.



Obrázok 5. Autentifikujte vytáčané pripojenia serverom RADIUS

Riešenie: Keď sa užívateľ pokúsi pripojiť, Network Access Server (NAS) spustený na serveroch iSeries postúpi autentifikačné informácie serveru RADIUS v sieti. Server RADIUS, ktorý udržiava všetky autentifikačné informácie vašej siete, spracúva autentifikačné požiadavky a odpovede. Ak je užívateľ

overený, môže byť server RADIUS nakonfigurovaný tak, aby priradil IP adresu rovnocenného počítača a aby mohol aktivovať spravovanie konta na sledovanie aktivity a použitie užívateľa. Aby ste podporili RADIUS, musíte na serveri iSeries definovať RADIUS NAS.

Vzorová konfigurácia:

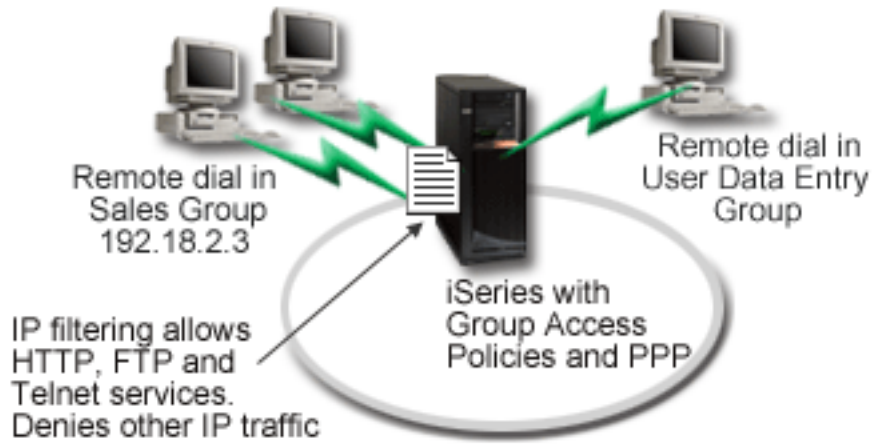
1. V produkte iSeries Navigator, rozviňte **Sieť**, kliknite pravým tlačidlom myši na **Služby vzdialeného prístupu** a označte **Služby**.
2. V záložke **RADIUS** označte **Povoliť pripojenie Network Access servera RADIUS** a **Povoliť RADIUS pre autentifikáciu**. V závislosti od riešenia RADIUS si tiež môžete vybrať, aby RADIUS spracúval priraďovanie pripojení na kontá a konfiguráciu adries TCP/IP.
3. Kliknite na tlačidlo **nastavenia RADIUS NAS**.
4. Na strane **Všeobecné** opis tohto servera.
5. Na stránkach autentifikačného servera (a prípadne kontového servera) kliknite na **Pridať** a zadajte nasledujúce informácie:
   a. Do poľa **Lokálna IP adresa** zadajte IP adresu rozhrania iSeries použitého na pripojenie k serveru RADIUS.
   b. Do poľa **IP adresa servera** zapíšte IP adresu servera RADIUS.
   c. Do poľa **Heslo** zapíšte heslo pri identifikácii servera iSeries na serveri RADIUS.
   d. Do poľa **Port** zapíšte port, ktorý je na iSeries použitý pri komunikácii so serverom RADIUS. Zadajte port 1812 pre autentifikačný server, alebo port 1813 pre kontový server.
6. Kliknite na **OK**.
7. V produkte iSeries Navigator rozviňte **Sieť > Služby vzdialeného prístupu**.
8. Označte Profil pripojenia, ktorý bude server RADIUS pri autentifikácii využívať. Na služby RADIUS môžu byť aplikované len profily adresáta pripojenia.
9. Na strane Autentifikácia označte **Na overenie identity vzdialeného systému požadujte tento server iSeries**.
10. Označte **Overiť vzdialene používaný server RADIUS**.
11. Označte autentifikačný protokol (EAP, PAP, or CHAP-MD5). Tento protokol musí byť tiež používaný aj serverom RADIUS. Viac informácií nájdete v časti Autentifikácia systému.
12. Označte **Použiť RADIUS na úpravu pripojení a prideľovanie pripojení kontám**.
13. Kliknutím na **OK** uložte zmenený profil pripojenia.

Musíte nastaviť aj server RADIUS, ako aj podporu overovacieho protokolu, užívateľských údajov, hesiel a informácií o kontách. Viac informácií si vyžiadajte u svojho predajcu systému RADIUS.

Keď sa užívateľ dovolá pomocou tohto profilu pripojenia, iSeries postúpi autentifikačné informácie zadanému serveru RADIUS. Ak je užívateľ overený, bude pripojenie povolené a budú aplikované všetky obmedzenia pripojenia určené užívateľskými informáciami na serveri RADIUS.

Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú skupinové politiky a filtrovanie IP

Situácia: Vaša sieť má niekoľko skupín distribuovaných užívateľov, z ktorých každá potrebuje prístup k rozličným prostriedkom vašej vnútropodnikovej siete LAN. Skupina užívateľov zadávajúcich údaje potrebuje prístup k údajom a niekoľkým ďalším aplikáciám, zatiaľ čo obchodní partneri potrebujú vytáčaný prístup k službám HTTP, FTP a Telnet, ale z bezpečnostných dôvodov im nesmú byť sprístupnené ďalšie služby a komunikácie TCP/IP. Určenie detailných atribútov a povolení spojenia pre každého užívateľa by znásobilo vašu prácu a vytváranie sieťových obmedzení pre všetkých užívateľov tohto profilu spojenia by vám neposkytlo dostatočnú kontrolu. Potrebovali by ste spôsob definovania nastavení spojenia a povolení pre niekoľko rozličných skupín užívateľov, ktorí sa zvyčajne pripájajú na tento server.



Obrázok 6. Aplikácia nastavenia spojenia na vytáčané pripojenie založené na nastaveniach skupinovej politiky

Riešenie: Potrebujete použiť obmedzenia filtrovania jedinečných IP adries na dve rozličné skupiny užívateľov. Aby ste to dosiahli, vytvoríte skupinové politiky prístupu a pravidlá filtrovania IP adries. Skupinové politiky prístupu sa odvolávajú na pravidlá filtrovania IP, takže musíte tieto pravidlá vytvoriť ako prvé. V tomto príklade potrebujete vytvoriť filter PPP, aby ste mohli filtračné pravidlá priradiť do skupinovej politiky prístupu ″Obchodní partneri″. Tieto filtračné pravidlá povoľujú služby HTTP, FTP a Telnet, ale obmedzujú prístup k všetkým ostatným TCP/IP službám a komunikácii cez server iSeries. Tento scenár ukazuje len filtračné pravidlá potrebné pre obchodnú skupinu; podobné filtre však môžete nastaviť aj pre skupinu ″Zadávania údajov″.

Nakoniec musíte na definovanie svojej skupiny vytvoriť skupinové politiky prístupu (jednu pre každú skupinu). Skupinové politiky prístupu vám umožňujú definovať spoločné atribúty pripojenia pre skupinu užívateľov. Pridaním skupinovej politiky prístupu do Validizačného zoznamu na serveri iSeries môžete tieto nastavenia pripojenia použiť počas procesu autentifikácie. Skupinová politika prístupu určuje niekoľko nastavení užívateľskej relácie, vrátane schopnosti aplikovať pravidlá filtrovania IP, ktoré obmedzia IP adresy a služby TCP/IP prístupné užívateľovi počas relácie.

Vzorová konfigurácia:

1. Vytvorte identifikátor filtra PPP a filtre pravidiel paketov IP, ktoré určujú oprávnenia a obmedzenia tejto skupinovej politiky prístupu. Viac informácií o filtrovaní IP nájdete v časti Pravidlá paketov IP (Filtrovanie a NAT) .
   a. V produkte iSeries Navigator rozviňte **Sieť > Služby vzdialeného prístupu**.
   b. Kliknite na **Profily príjemcu pripojenia**, pravým tlačidlom myši kliknite na profil tohto pripojenia a vyberte **Vlastnosti**.
   c. Vyberte záložku **Nastavenia TCP/IP** kliknite na **Rozšírené**.
   d. Označte **Použiť pre toto pripojenie pravidlá paketov IP** a kliknite na **Upraviť súbor pravidiel**. Tým spustíte Editor pravidiel paketov IP a otvoríte súbor s balíčkom pravidiel filtrov PPP.
   e. Otvorte menu **Vložiť** a pre vkladanie skupiny filtrov vyberte **Filtre**. Pomocou záložky **Všeobecné** definujte skupinu filtrov a v záložke **Služby** určite služby, ktoré povoľujete, ako napríklad HTTP. Nasledujúca skupina filtrov, ″services_rules″, povolí služby HTTP, FTP a Telnet. Filtračné pravidlá obsahujú preddefinovaný zákaz obmedzujúci použitie akýchkoľvek služieb TCP/IP, alebo komunikácie IP, ktoré nie sú výslovne povolené.

      Poznámka: IP adresy použité v nasledujúcom príklade sú všeobecne smerovateľné a uvádzajú sa len ako príklad.

```
###Nasledujúce 2 filtre povolia komunikáciu HTTP (webový prehliadač) z & do systému.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR =  %
        * DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS =  %
        NONE JRN = OFF

###Nasledujúce 4 filtre povolia komunikáciu FTP z & do vášho systému.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF
###Nasledujúce 2 filtre povolia komunikáciu Telnet z & do vášho systému.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. Otvorte menu **Vložiť** a vyberte **Rozhranie filtra**. Použite rozhranie filtra na vytvorenie identifikátora filtra PPP s využitím skupín filtrov, ktoré ste zadefinovali.

   1) Do záložky Všeobecné zadajte

      ```
      permited_services
      ```

      ako filtračný identifikátor PPP.

   2) V záložke **Skupiny filtrov** označte skupinu filtrov **services_rules** a kliknite na **Pridať**.

   3) Kliknite na OK. Do súboru pravidiel sa pridá nasledujúci riadok:

      ```
      ###Nasledujúci príkaz spája (priraďuje) skupinu filtrov 'services_rules' s
      ID filtra PPP "permitted_services." Toto ID filtra PPP môže byť použité pre fyzické rozhranie spojené s profil
      alebo skupinovou politikou prístupu.

      FILTER_INTERFACE PPP_FILTER_ID = permited_services SET = services_rules
      ```

g. Uložte zmeny a ukončite editor. Ak budete neskôr potrebovať vrátiť tieto zmeny, použite znakové rozhranie na zadanie príkazu:

   ```
   RMVTCPTBL
   ```

   Týmto zo servera odstránite všetky filtračné pravidlá a NAT.

h. V dialógu **Rozšírené nastavenia TCP/IP** nechajte prázdne pole **Identifikátor filtra PPP** a kliknutím na **OK** dialóg zavrite. Neskôr môžete práve vytvorený identifikátor filtra použiť na skupinové politiky prístupu, a nie na profil pripojenia.

2. Zadajte novú skupinovú politiku prístupu pre túto skupinu užívateľov. Detailnejší opis možností pre skupinové politiky prístupu nájdete v časti Konfigurácia skupinovej politiky prístupu.
   a. V produkte iSeries Navigator rozviňte **Sieť > Služby vzdialeného pripojenia > Profily príjemcu pripojenia**.
   b. Kliknite pravým tlačidlom myši na ikonu Skupinová politika prístupu a vyberte Nová skupinová politika prístupu. iSeries Navigator zobrazí dialóg Definícia novej skupinovej politiky prístupu.
   c. Na strane Všeobecné zadajte názov a opis skupinovej politiky prístupu.
   d. Na strane **Nastavenia TCP/IP**:
      - Označte **Použiť pre toto pripojenie pravidlá paketov IP** a označte identifikátor filtra PPP **permitted_services**.
   e. Kliknutím na **OK** uložte skupinovú politiku prístupu
3. Použite skupinovú politiku prístupu na užívateľov spojených s touto skupinou.
   a. Otvorte Profil príjemcu pripojenia, ktorý kontroluje tieto vytáčané pripojenia.
   b. Na strane **Autentifikácia** Profilu príjemcu pripojenia označte validizačný zoznam, ktorý obsahuje informácie autentifikačné informácie užívateľov a kliknite na **Otvoriť**.
   c. Označte užívateľov v skupine Obchodníci, na ktorých chcete aplikovať skupinovú politiku prístupu a kliknite na **Otvoriť**.
   d. Kliknite na **Aplikovať na užívateľa politiku skupiny** a vyberte Prístupovú politiku skupiny definovanú v kroku 2.
   e. Toto zopakujte pre každého užívateľa skupiny Obchodníci.

Viac informácií o autentifikácii užívateľov cez pripojenie PPP nájdete v časti Autentifikácia systému.

Kapitola 4. Koncepty PPP

PPP môžete použiť na pripojenie servera iSeries k vzdialeným sieťam, počítačovým klientom, iným serverom iSeries, alebo k ISP. Aby ste tento protokol plne využili, mali by ste pochopiť tak jeho možnosti, ako aj jeho podporu serverom iSeries. Viac informácií nájdete v nasledujúcej téme.

Čo je PPP?
Protokol Point-to-Point (PPP) je protokol TCP/IP používaný na pripojenie jedného počítačového systému k inému. Detailnejšie informácie nájdete v tejto téme.

Profily pripojenia
Profily pripojenia Point-to-Point definujú skupinu parametrov a prostriedkov pre konkrétne pripojenia PPP. Môžete spustiť profily, ktoré tieto nastavenia parametrov využívajú na vytočenie (vytvorenie) ALEBO na počúvanie (prijatie) pripojenia PPP.

Prístupové politiky skupiny
Tieto politiky definujú skupinu atribútov pripojenia a bezpečnostných atribútov pre skupinu užívateľov. Informácie o určení politiky vo vašom systéme nájdete v tejto téme.

Čo je PPP?

Počítače používajú **PPP** (**point-to-point protocol**) na komunikáciu cez internet prostredníctvom telefónnych liniek. Spojenie PPP existuje vtedy, ak sú dva systémy fyzicky prepojené cez telefónnu linku. PPP môžete použiť na pripojenie jedného systému k druhému. Napríklad, vytvorené spojenie PPP medzi pobočkou a centrálou im umožňuje navzájom prenášať údaje cez sieť.

PPP je internetovský štandard. Ide o najpoužívanejší spojovací protokol u poskytovateľov služieb internetu (ISP). PPP môžete využiť na pripojenie k svojmu ISP; ten vám zasa poskytne pripojenie na internet.

PPP umožňuje vzájomnú prevádzkyschopnosť medzi softvérom pre vzdialený prístup od rôznych výrobcov. Umožňuje tiež používanie tej istej fyzickej komunikačnej linky pre viac sieťových komunikačných protokolov.

Protokol PPP popisujú nasledujúce štandardy RFC (Request For Comment). Viac informácií o RFC nájdete na stránke http://www.rfc-editor.org.

- RFC1661 Point-to-Point Protocol
- RFC1662 PPP on HDLC-like framing
- RFC1994 PPP CHAP

Profily spojení

Verzia V5R2 používa dva typy profilov na to, aby ste mohli pre pripojenie PPP, alebo skupinu pripojení definovať vlastnosti.

- **Profily pôvodcu spojenia** sú spojenia point-to-point, ktoré iniciuje lokálny iSeries server a prijíma ich vzdialený systém. Pomocou tohto objektu môžete konfigurovať odchádzajúce spojenia.
- **Profily príjemcu spojenia** sú spojenia point-to-point, ktoré iniciuje vzdialený systém a prijíma ich lokálny iSeries server. Pomocou tohto objektu môžete konfigurovať prichádzajúce spojenia.

Profil spojenia konkretizuje, ako by malo prebiehať spojenie PPP. Informácie obsiahnuté v profile spojenia odpovedajú na tieto otázky:

- Aký typ protokolu pripojenia použijete? (PPP alebo SLIP)
- Kontaktuje váš iSeries server druhý počítač telefonicky (pôvodca)? Čaká váš iSeries server na prijatie volania z iného systému (príjemca)?
- Aká komunikačná linka sa použije pri spojení?
- Ako má váš iSeries server určiť, ktorú IP adresu použije?

- Ako má váš iSeries server autentifikovať iný systém? Kde by mal váš iSeries server ukladať autentifikačné informácie?

Profil spojenia je logickou reprezentáciou týchto konkrétnych informácií:

- Typ linky a profilu
- Nastavenia viacnásobnej linky
- Telefónne čísla pre vzdialený prístup a voľby vytáčania.
- Autentifikácia
- Nastavenia TCP/IP: IP adresy a ich smerovanie, filtrovanie IP.
- Riadenie prevádzky a prispôsobenie spojenia
- Názvové servery domény

iSeries server ukladá tieto konfiguračné informácie do profilu spojenia. Tieto informácie poskytujú potrebný kontext pre váš iSeries server na vytvorenie spojenia PPP s iným počítačovým systémom. Profil spojenia obsahuje tieto informácie:

- **Typ protokolu**. Môžete si vybrať buď PPP alebo SLIP. Spoločnosť IBM odporúča vždy použiť protokol PPP.
- **Výber režimu**. Typ spojenia a prevádzkový režim pre tento profil spojenia.

  Typ spojenia predstavuje typ linky, na ktorej spočívajú vaše spojenia a to, či **vytáčajú** alebo **odpovedajú** (teda či sú pôvodcom alebo príjemcom spojenia). Môžete si vybrať z týchto typov spojenia:
  - Komutovaná linka
  - Prenajatá (vyhradená) linka
  - L2TP (virtuálna linka)
  - PPPoE (virtuálna linka)

  PPPoE je podporovaná len pre Profily pôvodcu pripojenia.
- **Prevádzkový režim**. Možný prevádzkový režim závisí na type pripojenia. Prezrite si nasledujúcu tabuľku:

  Prezrite si nasledujúcu tabuľku pre Profily pôvodcu pripojenia:

Tabuľka 1. Možné prevádzkové režimy Profilov pôvodcu pripojenia.

Typ pripojenia	**Možné prevádzkové režimy**
Komutovaná linka	– Vytáčanie – Vytáčať na žiadosť (len vytáčanie) – Vytáčať na žiadosť (odpovedať povolenému rovnocennému počítaču). – Vytáčať na žiadosť (Povolený vzdialený rovnocenný počítač)
Prenajatá linka	Pôvodca
L2TP	– Pôvodca – Viacskokový iniciátor – Vzdialené vytáčanie
PPP cez Ethernet	Pôvodca

Prezrite si nasledujúcu tabuľku pre profily príjemcu pripojenia:

Tabuľka 2. Možné prevádzkové režimy pre Profily pôvodcu pripojenia.

Typ pripojenia	**Možné prevádzkové režimy**
Komutovaná linka	Odpoveď

Tabuľka 2. Možné prevádzkové režimy pre Profily pôvodcu pripojenia. (pokračovanie)

Typ pripojenia	Možné prevádzkové režimy
Prenajatá linka	Terminátor
L2TP	Terminátor (Sieťový server)

- **Konfigurácia linky**. Tu stanovíte typ linky, ktorú používa dané spojenie.

  Tieto voľby závisia od typu výberu režimu, ktorý si zvolíte. Pre komutovanú a prenajatú linku si môžete zvoliť ktorúkoľvek z uvedených volieb:

  — Jednoduchá linka
  — Linková oblasť
  — Integrovaná linka ISDN

  Pre všetky ďalšie typy pripojenia (Prenajatá, L2TP, PPPoE) je výber služby linky len Jednoduchá linka.

Podpora skupinových politík

Podpora skupinových politík umožňuje správcom siete definovať skupinové politiky založené na používateľovi, čím sa zjednoduší riadenie prostriedkov a umožní, aby jednotlivým používateľom boli priradené politiky riadenia prístupu pri prihlásení na sieť s reláciou PPP alebo L2TP. Cieľom tejto podpory je umožniť, aby používatelia mohli byť identifikovaní podľa konkrétnych skupín používateľov, pričom každá skupina bude mať vlastnú politiku. Každá jednotlivá skupinová politika umožňuje stanoviť ohraničenia zdrojov, ako napríklad počet liniek povolených pri viaclinkovom zväzku, atribúty ako napríklad postúpenie IP a určenie, akú skupinu pravidiel filtrovania paketov IP použiť. Vďaka podpore skupinovej politiky môžu správcovia siete zadefinovať napríklad skupinu Doma_pracujúci, ktorá umožní tejto triede používateľov neobmedzený prístup na sieť, alebo skupinu Pracovníci_predaja, ktorá môže využívať len obmedzený počet služieb.

Ako príklad si pozrite Scenár: Riadenie prístupu užívateľov k zdrojom s použitím Skupinových politík prístupu a filtrovania IP adries.

Kapitola 5. Plánovanie PPP

Vytváranie a administrácia spojení PPP si vyžaduje poznanie tak podpory ako možností spojenia PPP na serveroch iSeries, ako aj množstva sieťových a bezpečnostných plánov, ktoré vaše podnikanie potrebuje. Nasledujúce témy vám môžu pomôcť bližšie sa oboznámiť s možnosťami a požiadavkami spojenia PPP pri iSeries.

Softvérové a hardvérové požiadavky
iSeries Navigator, vydanie 4, verzia 4 (V4R4), alebo vyšší podporuje spojenia PPP. Zoznam ďalších požiadaviek nájdete v tejto téme.

Možnosti pre spojenia
iSeries podporuje spojenia PPP cez mnohé médiá, od analógových, alebo digitálnych telefónnych liniek, po úplné, alebo čiastočné spojenia T1. V tejto téme nájdete opis podporovaných možností pripojenia.

Spojovacie zariadenie
Servery iSeries používajú na spracovanie spojenia PPP modemy, terminálové adaptéry ISDN, adaptéry Token Ring, adaptéry Ethernet, alebo zariadenia CSU/DSU. V tejto téme nájdete informácie o podporovanom hardvéri.

Spravovanie IP adries
Spojenia PPP majú niekoľko možností ako počas pripojenia priraďovať IP adresy a filtrovať pakety IP. V tejto téme nájdete opisy týchto možností.

Autentifikácia systému
iSeries môže vytáčané pripojenia autentifikovať buď použitím validizačného zoznamu a výmeny hesiel, alebo použitím servera RADIUS. Taktiež poskytuje autentifikačné informácie systémom, ku ktorým je pripojený. V tejto téme nájdete opis autentifikačných možností.

Informácie o šírke pásma
iSeries podporuje viaclinkový protokol pre spojenia PPP. To vám umožní použiť viaceré analógové telefónne linky pre jediné spojenie, a tým zväčšiť šírku pásma. V tejto téme nájdete prehľad týchto podpôr.

Softvérové a hardvérové požiadavky

Prostredie PPP vyžaduje, aby ste mali dva alebo viac počítačov, ktoré podporujú PPP. Jeden z týchto počítačov, iSeries server, môže byť buď pôvodca, alebo príjemca. iSeries server musí spĺňať nasledujúce základné podmienky, aby naň mali prístup vzdialené systémy.

- **Operations Navigator**, vydanie 4, verzia 4 (V4R4) alebo vyššia s podporou TCP/IP
- Jeden z dvoch uvedených profilov spojenia:
  - Profil pôvodcu spojenia na spracovanie odchádzajúcich spojení PPP
  - Profil príjemcu spojenia na spracovanie prichádzajúcich spojení PPP
- Konzola pracovnej stanice s nainštalovaným softvérom **iSeries Access pre Windows (95/98/NT/Millenium/2000/XP)** s produktom iSeries Navigator.
- Nainštalovaný adaptér

  Môžete si zvoliť jeden z uvedených adaptérov:
  - 2699*: Dvojlinkový WAN IOA
  - 2720*: PCI WAN/Twinaxiálny IOA
  - 2721*: PCI dvojlinkový WAN IOA
  - 2745*: PCI dvojlinkový WAN IOA (nahrádza IOA 2721)
  - 2742*: Dvojlinkový IOA (nahrádza IOA 2745)
  - 2750: PCI ISDN V.90 Basic Rate Interface U IOA (2-drôtové rozhranie)
  - 2751: PCI ISDN V.90 Basic Rate Interface U IOA (4-drôtové rozhranie)
  - 2761: Osemportový analógový modem IOA

- 2771: Dvojportový WAN IOA s integrovaným modemom V.90 na porte 1 a štandardným komunikačným rozhraním na porte 2. Na použitie portu 2 adaptéra 2771 sa vyžaduje externý modem alebo terminálový adaptér ISDN s príslušným káblom.
- 2772: Dvojportový integrovaný modem V.90 WAN IOA
- 2838: Adaptér Ethernet pre spojenia PPPoE.
- 2793*: Dvojportový WAN IOA, s integrovaným modemom V.92 na porte 1 a štandardným komunikačným rozhraním na porte 2. Na použitie portu 2 adaptéra 2793, je požadovaný externý modem, alebo terminálový adaptér ISDN s príslušným káblom. To nahradí IOA model 2771.
- 2805 štvorportový WAN IOA s integrovaným analógovým modemom V.92. To nahradí modely 2761 a 2772.

* Tieto adaptéry vyžadujú externý modem V.90 (alebo vyšší), alebo terminálový adaptér ISDN a kábel RS232, alebo iný kompatibilný kábel.

- V závislosti od typu vášho pripojenia a linky potrebujete jedno z uvedených zariadení:
  - externý alebo interný modem, alebo CSU (channel service unit)/DSU (data service unit)
  - terminálový adaptér ISDN (Integrated Services Digital Network)
- Ak plánujete pripojenie na internet, musíte upraviť telefonické konto u ISP (Internet Service Provider). Váš ISP by vám mal poskytnúť všetky potrebné telefónne čísla a informácie pre pripojenie na internet.

Možnosti pre spojenia

PPP môže odosielať datagramy po sériových linkách point-to-point. PPP umožňuje vzájomné prepojenie zariadení viacerých predajcov a viacerých protokolov vďaka štandardizácii komunikácie point-to-point. Vrstva dátového spojenia PPP používa na zapuzdrenie datagramov cez asynchrónne aj synchrónne telekomunikačné linky point-to-point rámcovanie, podobné HDLC.

Kým PPP podporuje širokú škálu typov liniek, SLIP podporuje len asynchrónne typy liniek. SLIP sa všeobecne používa len pri analógových linkách. Lokálne telekomunikačné spoločnosti ponúkajú tradičné telekomunikačné služby v čoraz väčšej škále možností a cien. Tieto služby využívajú už vybudované zariadenia hlasovej siete medzi zákazníkom a ústredím.

Linky PPP vytvárajú fyzické spojenie medzi lokálnym a vzdialeným hostiteľom. Združené linky poskytujú vyhradenú šírku pásma. Používajú sa rôzne rýchlosti prenosu dát a protokoly. Pri linkách PPP máte na výber z týchto spojení:

- Analógové telefónne linky
- Digitálne služby a DDS
- Komutovaná-56
- ISDN
- T1/E1 a čiastočné T1
- Frame Relay
- Podpora L2TP (tunelovania) pre spojenia PPP
- Podpora PPPoE (DSL) pre spojenie PPP

Analógové telefónne linky

Analógové spojenie, ktoré využíva na prenos dát po prenajatých alebo komutovaných linkách modem, je najnižším typom spojenia point-to-point. Prenajatá linka je trvalým spojením medzi dvoma stanovenými miestami, kým komutovaná linka je normálna hlasová telefónna linka. Dnešné najrýchlejšie modemy pracujú rýchlosťou 56 kbps (nekomprimovane). Ak vezmeme do úvahy odstup signál-šum v hlasových telefónnych okruhoch, táto rýchlosť je často nedosiahnuteľná.

Rýchlosť stanovená výrobcom modemov v bitoch za sekundu (bps) sa zvyčajne odvíja od algoritmu komprimácie údajov (CCITT V.42bis), ktorý tieto modemy používajú. Hoci V.42bis má schopnosť dosiahnuť

až štvornásobnú redukciu objemu údajov, veľkosť komprimácie závisí od konkrétnych údajov a len zriedka dosahuje 50 %. Veľkosť už komprimovaných či šifrovaných údajov môže pri použití V.42bis dokonca vzrásť. X2 alebo 56Flex zvyšuje pri analógových telefónnych linkách rýchlosť prenosu údajov na 56k. Ide o hybridnú technológiu, ktorá vyžaduje, aby bol jeden koniec linky PPP digitálny a druhý koniec analógový. Rýchlosť 56 kbps sa potom dosahuje len vtedy, ak posielate údaje z digitálneho konca linky na analógový koniec. Táto technológia je vhodná najmä pre pripojenia k ISP, ktoré majú u seba digitálny koniec linky a hardvér. Zvyčajne sa môžete pripojiť na analógový modem V.24 po sériovom rozhraní RS232 s asynchrónnym protokolom s rýchlosťou prenosu až 115,2 kbps.

Štandard V.90 predstavuje riešenie problému kompatibility K 56flex/x2. Štandard V.90 je výsledkom kompromisu medzi zástancami x2 a K56flex pri modemoch. Vďaka tomu, že V.90 vníma verejnú komutovanú telefónnu sieť ako digitálnu sieť, môže táto technológia zvyšovať rýchlosť prenosu údajov z internetu na počítač až na 56 kbps. Technológia V.90 sa líši od iných štandardov tým, že údaje digitálne kóduje a nemoduluje ich, ako to robia analógové modemy. Prenos údajov je asymetrický proces, a tak prenosy proti prúdu (väčšinou príkazy z klávesnice a myši počítača na centrálnu lokalitu, ktoré si vyžadujú menšiu šírku pásma) sú aj naďalej prenášané konvenčnými rýchlosťami maximálne do 33,6 kbps. Údaje, ktoré posiela modem, sa posielajú analógovým prenosom, ktorý kopíruje štandard V.34. Len pri prenose údajov po prúde sa môže využiť výhoda vyšších prenosových rýchlostí V.90.

Štandard V.92 zdokonaľuje modem V.90 povolením kapacity odosielania až na 48 kbps. Časy spojenia môžu byť skrátené vďaka vylepšeniam v procese nadviazania spojenia a modemy, ktoré podporujú možnosť ″podržať linku″, teraz ostanú pripojené, kým telefónna linka akceptuje prichádzajúci hovor, alebo použijú čakanie na hovor.

Digitálne služby a DDS

Digitálne služby

Pri digitálnych službách údaje ″cestujú″ v digitálnej forme z počítača odosielateľa na ústredie telekomunikačnej spoločnosti, potom k vzdialenému poskytovateľovi služieb a do centrály až napokon do počítača príjemcu. Digitálny signál ponúka oveľa väčšiu šírku pásma a je spoľahlivejší ako analógový signál. Digitálny signálny systém eliminuje mnohé problémy, ktoré musia riešiť analógové modemy, napríklad šum, premenlivú kvalitu linky a útlm signálu.

DDS

Digitálne dátové služby (DDS) sú najzákladnejšími digitálnymi službami. Linky DDS sú prenajaté, trvalé spojenia, ktoré pracujú pri pevných prenosových rýchlostiach do 56 kbps. Uvedená služba je všeobecne známa aj ako DS0.

K DDS sa môžete pripojiť pomocou špeciálneho zariadenia CSU/DSU (Channel Service Unit/Data Service Unit), ktoré nahrádza modem, potrebný pre analógové spojenie. DDS má fyzické obmedzenia, ktoré sa týkajú najmä vzdialenosti medzi CSU/DSU a ústredím telekomunikačnej spoločnosti. DDS pracuje najlepšie vtedy, keď je táto vzdialenosť menšia ako 10 000 metrov. Telekomunikačné spoločnosti môžu vybaviť zariadenia používané vo väčšej vzdialenosti zosilňovačmi signálu, čo však túto službu zdražuje. DDS je najvýhodnejšia pri prepojení dvoch lokalít, ktoré obsluhuje tá istá centrála. Pri spojeniach vo väčších vzdialenostiach, ktoré zahŕňajú niekoľko rôznych centrál, je vďaka zvýšeným poplatkom vyplývajúcim z väčšej vzdialenosti DDS nepraktická. V týchto prípadoch môže byť lepším riešením linka typu komutovaná-56. Na DDS CSU/DSU sa bežne môžete pripojiť po sériovom rozhraní V.35, RS449 alebo X.21 so synchrónnym protokolom pri rýchlostiach do 56 kbps.

Komutovaná-56

Keď nepotrebujete stále spojenie, ušetríte, ak použijete komutovanú digitálnu službu, všeobecne známu ako komutovaná-56 (SW56). Linka SW56 sa podobá nastaveniu DDS v tom, že DTE sa pripája na digitálnu službu tak, ako CSU/DSU. CSU/DSU pre SW56 má však aj číselník, z ktorého zadávate telefónne číslo vzdialeného hostiteľa. SW56 vám umožní uskutočniť telefónne digitálne pripojenie k akémukoľvek inému

používateľovi linky SW56, a to nielen vnútroštátne, ale aj medzinárodne. Volanie SW56 sa prenáša po digitálnej sieti na veľké vzdialenosti podobne ako digitalizované hlasové volania. SW56 používa rovnaké telefónne čísla ako miestny telefónny systém a užívateľské poplatky sú rovnaké ako poplatky za firemné hlasové volania. Služba SW56 je možná len v sieťach Severnej Ameriky a je limitovaná jednoduchými vedeniami, ktoré prenášajú len údaje. SW56 je alternatívnou možnosťou tam, kde nie je k dispozícii ISDN. Na SW56 CSU/DSU sa obyčajne môžete pripojiť po sériovom rozhraní V.35 alebo RS 449 so synchrónnym protokolom pri rýchlostiach do 56 kbps. V prípade volacej/odpovedacej jednotky V.25bis pretekajú údaje a riadenie volania po jednom sériovom rozhraní.

ISDN

Podobne ako komutovaná-56, aj ISDN poskytuje komutovanú digitálnu konektivitu typu koniec-koniec. Na rozdiel od iných služieb však môže ISDN prenášať po jednom spojení hlas aj údaje. Existuje niekoľko rôznych druhov služieb ISDN, najbežnejšia je však Basic Rate Interface (BRI). BRI pozostáva z dvoch B-kanálov s rýchlosťou 64 kbps na prenos zákazníckych údajov a z D-kanálu na prenos signalizácie. Dva B-kanály možno združiť a získať tak celkovú prenosovú rýchlosť 128 kbps. V niektorých štátoch telekomunikačné spoločnosti obmedzujú rýchlosť jedného B-kanála na 56 kbps alebo dvoch združených B-kanálov na 112 kbps. Táto linka má aj fyzické obmedzenie: lokalita zákazníka sa musí nachádzať do 6 000 metrov od ústredne. Túto vzdialenosť však možno predĺžiť opakovačmi. Na ISDN sa môžete pripojiť pomocou terminálového adaptéra. Väčšina terminálových adaptérov má integrované sieťové ukončenie (NT1), ktoré umožňuje priame pripojenie k telefónnej zásuvke. Terminálové adaptéry sa pripájajú na váš počítač väčšinou po asynchrónnej linke RS232 a na nastavenie a ovládanie používajú sadu príkazu AT, podobne ako bežné analógové modemy. Každý výrobca má vlastné rozšírenie AT príkazov na nastavenie parametrov, ktoré sú jedinečné pre ISDN. V minulosti sa vyskytovali problémy so vzájomnou kompatibilitou medzi rôznymi značkami terminálových adaptérov ISDN. Tieto problémy boli zapríčinené najmä rozdielnymi protokolmi úpravy rýchlosti, ktoré boli v modemoch V.110 a V.120, ako aj schémami previazania pre dva B-kanály.

Priemysel teraz smeruje k synchrónnemu protokolu PPP s viaclinkovým PPP na prepojenie dvoch B-kanálov. Niektorí výrobcovia integrujú do nimi vyrábaných terminálových adaptérov funkciu V.34 (analógový modem). To umožňuje zákazníkom s jednou linkou ISDN spracúvať buď volania ISDN alebo štandardné analógové volania vďaka schopnosti ISDN prenášať súčasne hlas aj údaje. Nová technológia ďalej umožňuje, aby terminálový adaptér vystupoval ako digitálny server pre klientov 56K(X2/56Flex).

Na terminálový adaptér ISDN sa bežne pripája po sériovom rozhraní RS232 pomocou asynchrónneho protokolu pri prenosových rýchlostiach do 230,4 kbps. Maximálna modulačná rýchlosť iSeries servera pre asynchrónny protokol po RS232 je však 115,2 kbps. To žiaľ obmedzuje maximálnu prenosovú rýchlosť v bajtoch na 11,5 kilobajtov/sekundu, pričom terminálový adaptér využívajúci viacnásobnú linku môže dosiahnuť rýchlosť 14/16 neskomprimovaných kilobajtov. Niektoré terminálové adaptéry podporujú synchrónne spojenie po RS232 pri 128 kbps, ale maximálna modulačná rýchlosť iSeries servera pri synchrónnom spojení po RS232 je 64 kbps.

iSeries server dokáže fungovať asynchrónne po V.35 pri rýchlostiach do 230,4 kbps, výrobcovia terminálových adaptérov však vo všeobecnosti takúto konfiguráciu nedodávajú. Konvertory rozhraní, ktoré prevádzajú RS232 na rozhranie V.35 môžu byť primeraným riešením tohto problému, v prípade iSeries servera však tento prístup nebol vyhodnotený. Ďalšou možnosťou je použitie terminálových adaptérov so synchrónnym protokolom rozhrania V.35 pri rýchlosti 128 kbps. Hoci taká trieda terminálových adaptérov existuje, len máloktorý výrobca ponúka synchrónny viaclinkový PPP.

T1/E1 a čiastočné T1

T1/E1

Spojenie T1 prepája spolu dvadsaťštyri kanálov s časovým multiplexom (TDM) a rýchlosťou 64 kbps (DS0) do 4-káblového medeného okruhu. To vytvára celkovú šírku pásma 1,544 mbps. Okruh E1 v Európe a inde vo svete spája tridsaťdva 64 kbps kanálov s celkovou šírkou pásma 2,048 mbps. Vďaka vopred vyhradeným časovým slotom umožňuje TDM viacerým používateľom zdieľať médium digitálneho prenosu. Mnoho

digitálnych pobočkových ústrední využíva T1 na importovanie viacerých volacích okruhov po jednej linke T1, takže nemusí smerovať 24 káblových párov medzi pobočkovou ústredňou a telekomunikačnou spoločnosťou. Treba si uvedomiť, že T1 možno zdieľať medzi hlas a údaje. Telefónna služba môže napríklad použiť podmnožinu 24 kanálov linky T1 a ponechať zvyšné kanály pre pripojenie na internet. Na riadenie 24 kanálov DS0 je potrebné multiplexovacie zariadenie T1, keď spojovací okruh T1 zdieľa viacero služieb. Pri jednoduchom dátovom spojení môže okruh fungovať bez vytvárania kanálov (na signáli sa nevykonáva TDM). Teda možno použiť aj jednoduchšie zariadenie CSU/DSU. Na T1/E1 CSU/DSU alebo multiplexor sa obyčajne môžete pripojiť po sériovom rozhraní V.35 alebo RS 449 so synchrónnym protokolom pri rýchlostiach násobku 64 kbps až do 1,544 mbps alebo 2,048 mbps. Časovanie v sieti zabezpečuje multiplexor alebo CSU/DSU.

Čiastočné T1

V prípade čiastočného T1 (FT1) si môže zákazník prenajať ktorýkoľvek nižší násobok 64 kbps linky T1. FT1 je výhodné vtedy, ak by náklady na nekomutované T1 znemožňovali skutočnú šírku pásma, ktorú zákazník používa. Pri FT1 platíte len za to, čo potrebujete. Navyše, FT1 obsahuje aj ďalšiu funkciu, ktorú nemá plný okruh T1: multiplexovanie kanálov DS0 v ústredni telekomunikačnej spoločnosti. Vzdialený koniec okruhu FT1 sa nachádza na ústredni Digital Access Cross-Connect Switch, ktorú spravuje telekomunikačná spoločnosť. Systémy, ktoré majú spoločnú digitálnu ústredňu, môžu prepínať kanály DS0. Táto zostava sa teší obľube u tých poskytovateľov internetu, ktorí používajú jednoduchý spojovací okruh T1 zo svojej lokality do digitálnej ústredne telekomunikačnej spoločnosti. V týchto prípadoch možno viacero klientov obslúžiť linkou FT1 súčasne. Na T1/E1 CSU/DSU alebo multiplexor sa môžete bežne pripojiť po sériovom rozhraní V.35 alebo RS 449 so synchrónnym protokolom pri prenosovej rýchlosti násobku 64 kbps. Pri FT1 dostanete vopred určenú podmnožinu z 24 kanálov. Multiplexor T1 musí byť nakonfigurovaný tak, aby zapĺňal len časové sloty, ktoré sú priradené pre vás.

Frame Relay

Frame Relay je protokol na smerovanie rámcov cez siete na základe poľa s adresou (identifikátora spojenia dátovej linky) v rámci a na riadenie trasy alebo virtuálneho spojenia.

Siete Frame Relay v USA podporujú prenosové rýchlosti pri T-1 (1,544 mbps) a T-3 (45 mbps). O službe Frame Relay môžete uvažovať aj ako o metóde, ako využiť existujúce linky T-1 a T-3, ktoré vlastní poskytovateľ služieb. Väčšina telekomunikačných spoločností teraz ponúka službu Frame Relay tým zákazníkom, ktorí požadujú spojenia s prenosovými rýchlosťami od 56 kbps po T-1. (V Európe sa prenosové rýchlosti pri službe Frame Relay pohybujú od 64 kbps do 2 mbps. V USA je služba Frame Relay pomerne obľúbená, pretože je relatívne finančne nenáročná. V niektorých oblastiach sa však nahrádza rýchlejšími technológiami, napríklad ATM.)

Podpora L2TP (tunelovania) pre spojenia PPP

L2TP (Layer 2 Tunneling Protocol) je protokol tunelovania, ktorý rozširuje PPP na podporu tunela spojovacej vrstvy medzi žiadajúcim klientom L2TP (koncentrátor prístupu L2TP alebo LAC) a cieľovým koncovým serverom L2TP (sieťový server L2TP alebo LNS). Pomocou tunelov L2TP možno izolovať miesto, na ktorom sa končí protokol pre telefonické spojenie a kde sa poskytuje prístup na sieť. L2TP sa preto nazýva aj Virtuálnym PPP. Protokol L2TP je dokumentovaný ako štandard RFC2661 (Request For Comment). Viac informácií o RFC nájdete na adrese http://www.rfc-editor.org Tunel L2TP sa môže rozšíriť na celú reláciu PPP alebo len na jeden segment v dvojsegmentovej relácii. To možno vyjadriť štyrmi rôznymi modelmi tunelovania:

- Nevynútený tunel
- Vynútený tunel - prichádzajúce volanie
- Vynútený tunel - vzdialené telefonické pripojenie
- Viacskokové spojenie L2TP.

Nevynútený tunel
Pri tomto modeli vytvára tunel používateľ, väčšinou pomocou klienta, na ktorom je umožnený L2TP. Používateľ potom bude zasielať pakety L2TP poskytovateľovi služieb internetu (ISP), ktorý ich bude ďalej zasielať na LNS. Pri nevynútenom tunelovaní nemusí ISP podporovať L2TP, pričom iniciátor tunela L2TP sa nachádza na tom istom systéme ako vzdialený klient. V tomto prípade sa tunel rozširuje na celú reláciu PPP z klienta L2TP na LNS.

Vynútený tunel - prichádzajúce volania
V prípade vynúteného tunela - prichádzajúcich volaní sa tunel vytvára bez akéhokoľvek zásahu používateľa, pričom používateľovi neposkytuje nijakú voľbu. Používateľ bude teda zasielať pakety PPP poskytovateľovi služieb internetu (ISP) na LAC, ktorý ich zapuzdrí v L2TP a pošle tunelom na LNS. Pri tomto modeli musí ISP poskytovať L2TP. Tunel sa v tomto prípade rozširuje len na segment relácie PPP, ktorý je medzi ISP a LNS.

Vynútený tunel - vzdialené telefonické pripojenie
V prípade vynúteného tunela - vzdialeného telefonického pripojenia inicializuje domovský gateway (LNS) vytvorenie tunela na LAC poskytovateľa služieb internetu a nariadi mu, aby uskutočnil miestne volanie klienta odpovede PPP. Tento model bol vytvorený pre prípad, keď má vzdialený klient odpovede PPP trvalé telefónne číslo u ISP. Použije sa vtedy, keď firma, ktorá je zavedená na internete, potrebuje vytvoriť spojenie so vzdialenou pobočkou, ktorá potrebuje telefonické pripojenie. Tunel sa v tomto prípade rozširuje len na segment relácie PPP, ktorý sa nachádza medzi LNS a ISP.

Viacskokové spojenie L2TP
Viacskokové spojenie L2TP je metódou presmerovania prevádzky L2TP na klientske LAC a LNS. Viacskokové spojenie sa nadväzuje pomocou viacskokového gateway L2TP (systému, ktorý prepája profily terminátora a iniciátora L2TP). Na vytvorenie viacskokového spojenia bude viacskokový gateway L2TP vystupovať voči sade LAC ako LNS a zároveň ako LAC voči danému LNS. Tunel sa vytvára z klientskeho LAC na viacskokový gateway L2TP a ďalší tunel sa vytvára medzi viacskokovým gateway L2TP a cieľovým LNS. Prevádzku L2TP z klientskeho LAC potom viacskokový gateway L2TP presmeruje na cieľový LNS a prevádzku z cieľového LNS presmeruje na klientsku LAC.

Podpora PPPoE (DSL) pre spojenia PPP
DSL sa odvoláva na klasickú technológiu použitú pri získavaní väčšej šírky pásma pri prepojení existujúcimi medenými telefónnymi káblami vedenými medzi komplexom zákazníka a poskytovateľom ISP. Umožňuje simultánne hlasové a vysokorýchlostné dátové služby pri prenose cez jediný pár medených telefónnych drôtov. Rýchlosť modemu sa postupne zvyšovala pomocou rôznych komprimácií a iných postupov, ale momentálne najvyššou rýchlosťou (56 kbit/s) dosahujú teoretický limit tejto technológie. Technológia DSL umožňuje dosiahnuť cez krútenú dvojlinku medzi ústredňou a domovom, školou a podnikom podstatne vyššie rýchlosti. V niektorých oblastiach možno dosiahnuť až rýchlosť 2 Mbit/s - teda 30, alebo viackrát vyššiu než dnešné najrýchlejšie modemy. PPPoE znamená Point to Point Protocol cez Ethernet. PPP sa zvyčajne používa pri sériových komunikáciách ako vytáčané modemové spojenie. Mnohí DSL poskytovatelia internetových služieb dnes používajú PPP cez Ethernet kvôli jeho schopnostiam rozširovania prihlasovacích a bezpečnostných vlastností. Čo je to modem DSL? ″Modem″ DSL je zariadenie umiestnené na konci medenej telefónnej linky, ktoré má umožniť počítaču (alebo LAN) pripojiť sa na internet cez pripojenie DSL. Na rozdiel od vytáčaného pripojenia zvyčajne nevyžaduje vyhradenú telefónnu linku (a POTS rozdeľovač umožňuje, aby bola linka zdieľaná súčasne). DSL sa považuje za novú generáciu technológie modemov. Hoci sa modemy DSL podobajú na zvyčajné analógové modemy, poskytujú podstatne vyšší výkon.

Spojovacie zariadenie
V prostredí PPP môžete používať tri druhy spojovacích zariadení:
- Modemy
- CSU/DSU
- Terminálové adaptéry ISDN
- Adaptéry typu 2838 Ethernet (pre pripojenia PPPoE).

•

Modemy

Pri spojeniach PPP môžete používať tak externé, ako aj interné modemy. Príkazová sada, ktorú modem používa, je zvyčajne opísaná v dokumentácii k modemu. Cez príkazy sa zadáva nulovanie a inicializácia modemu a vytáčanie telefónneho čísla vzdialeného systému. Každý model modemu sa musí zadefinovať skôr, než ho bude možné použiť pre profil spojenia PPP, pretože rôzne modely modemov používajú rôzne reťazce inicializačných príkazov. Ak ide o interný modem, modemové reťazce majú už zadefinované svoje použitie.

iSeries server má preddefinovaných veľa modelov modemov, no prostredníctvom Operations Navigator možno zadefinovať aj nové modely. Existujúcu definíciu možno použiť ako základ na zadefinovanie nového typu. Ak neviete, aké príkazy váš modem používa alebo ak nemáte prístup k dokumentácii k modemu, začnite generickou Hayesovou definíciou modemu. Definície, nastavené už pri dodaní, nemožno meniť. K vytvorenému inicializačnému príkazu alebo vytáčaciemu reťazcu však možno pridať ďalšie príkazy.

Na vytvorenie spojení PPP môžete použiť modem elektronickej podpory zákazníkov (ECS), ktorý sa dodáva s iSeries serverom. Pri starších systémoch bol ako modem ECS použitý externý modem IBM 7852-400. Pri novších systémoch možno ako modem ECS použiť interné modemy 2771 alebo 2772.

CSU/DSU

CSU (Channel Service Unit) je zariadenie, ktoré pripája terminál ku digitálnej linke. DSU (Data Service Unit) je zariadenie, ktoré pre telekomunikačnú linku vykonáva funkcie ochrany a diagnostiky. Obe zariadenia sa zväčša dodávajú ako jedna jednotka CSU/DSU.

CSU/DSU teda možno považovať aj za veľmi výkonný a drahý modem. Toto zariadenie požadujú oba konce spojenia T-1 alebo T-3; jednotky na oboch koncoch musia pochádzať od toho istého výrobcu.

Terminálové adaptéry ISDN

ISDN vám ponúka digitálne spojenie, ktoré vám umožní komunikovať a zároveň prenášať hlas, údaje a video, či iné multimediálne aplikácie.

Overte si, či sa váš terminálový adaptér môže použiť na iSeries serveri:

- V Odporúčaniach pre terminálový adaptér ISDN nájdete, ktorý adaptér by ste mali použiť.
- V Obmedzeniach pre terminálové adaptéry ISDN sa uvádzajú informácie a stručné vyhodnotenie rôznych terminálových adaptérov ISDN, ktoré sa skúšali s iSeries serverom.

Ak chcete nakonfigurovať svoj terminálový adaptér, postupujte podľa týchto krokov:

1. V produkte iSeries Navigator označte váš server a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. V dialógovom okne Vlastnosti nového modemu zadajte správne hodnoty do všetkých polí panelu Všeobecné. Terminálový adaptér ISDN musíte zadefinovať ako komunikačné zariadenie.
4. Vyberte panel **Parametre ISDN**.
5. Na paneli **Parametre ISDN** pridajte alebo zmeňte vlastnosti ISDN tak, aby zodpovedali vlastnostiam, ktoré vyžaduje váš terminálový adaptér.

Prezrite si príklad Konfigurovanie terminálového adaptéra ISDN, aby ste videli vzorové procedúry, ktoré používa Operations Navigator.

Odporúčania pre terminálový adaptér ISDN

Odporúčaný externý terminálový adaptér ISDN, alebo modem ISDN, je **3Com/U.S. Robotics Courier I ISDN V.Everything** . Podporuje pripojenia analógového modemu V.34, V.90 (X2), V.92 a viaclinkové pripojenie PPP cez ISDN v režime pôvodcu aj odpovedania na serveri iSeries. Pri PPP spojení ISDN

zároveň automaticky podporuje Challenge Handshake Authentication Protocol (CHAP). Tiež sú prístupné nasledujúce terminálové adaptéry ISDN: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA a ADtran ISU 2x64 Dual Port.

- **Spojenia, ktoré sú iniciované iSeries serverom.** Na výzvy CHAP, ktoré vznikajú na strane príjemcu, odpovedá terminálový adaptér Courier I, a zároveň s iSeries serverom dohoduje protokol Password Authentication Protocol (PAP). Odpovede PAP sa neobjavia na spojení ISDN.
- **Spojenia, na ktoré odpovedá iSeries server.** Courier I vyžaduje od volajúcej strany autentifikáciu CHAP vtedy, ak konfigurácia odpovede iSeries servera bude mať za následok otvorenie autentifikácie s výzvou CHAP. Ak iSeries server otvorí autentifikáciu s PAP, terminálový adaptér Courier I bude autentifikovať s PAP.

Ak používate modem Courier I vyrobený pred rokom 1999, overte, či je pripojený na váš iSeries server káblom V.35, aby ste tak dostali zo svojho spojenia ISDN ten najlepší výkon. Kábel modemu RS-232 to V.35 je dodávaný s modemom Courier I, ale staršie verzie tohto kábla majú nesprávny druh konektora V.35. Kontaktuje podporu 3Com/US Robotics, aby vám ho vymenili.

Poznámka: Podľa 3Com/US Robotics už nie je verzia V.35 tohto terminálového adaptéru dostupná, aj keď sa ešte môže nachádzať u dodávateľov. Verzia RS-232 sa stále odporúča pre iSeries server, napriek zníženému výkonu, keďže prenosové rýchlosti sú pri RS-232 obmedzené na 115,2 Kb.

Tiež si môžete zaobstarať adaptér V.35 na RS-232 od spoločnosti Black Box Corporation. Číslo dielu je FA-058.

Na iSeries serveri nezabudnite nastaviť rýchlosť linky V.35 na 230,4 kbps.

Obmedzenia pre terminálový adaptér ISDN

Nasleduje prehľad terminálových adaptérov, ktoré boli vyhodnotené. Odporúčajú sa len pre odosielanie vzdialených spojení ISDN z iSeries servera.

3Com Impact IQ ISDN:

Tento terminálový adaptér sa neodporúča pre iSeries server z týchto dôvodov:

- Terminálový adaptér nepodporuje analógové modemové spojenia V.34. Ak sa však použije externé spojenie RJ-11, môže analógové modemové spojenia V.34 podporovať.
- Terminálový adaptér aktuálne nepodporuje spojenia V.90.
- Terminálový adaptér sa nesmie pripojiť na iSeries server pri rýchlostiach vyšších ako 115200 bps.
- Terminálový adaptér nepodporuje automaticky CHAP (Challenge Handshake Authentication Protocol). Nastavenie S84=0 však umožňuje vykonanie autentifikácie CHAP na iSeries serveri.
- iSeries server nedokáže pri monitorovaní signálu Data Set Ready z terminálového adaptéra určiť, kedy sa ukončí spojenie. To môže viesť k potenciálnemu ohrozeniu bezpečnosti systému.

Motorola BitSurfr Pro ISDN:

Tento terminálový adaptér sa neodporúča pre iSeries server z týchto dôvodov:

- Terminálový adaptér nepodporuje analógové modemové spojenia V.34. Ak sa však použije externé spojenie RJ-11, môže analógové modemové spojenia V.34 podporovať.
- Terminálový adaptér aktuálne nepodporuje spojenia V.90.
- Terminálový adaptér sa nesmie pripojiť na iSeries server pri rýchlostiach vyšších ako 115200 bps.
- Terminálový adaptér nepodporuje automaticky autentifikáciu CHAP. Nastavenie S84=0 však umožňuje vykonanie autentifikácie CHAP na serveri iSeries.
- Terminálový adaptér nepovoľuje automaticky odpovedanie na jednolinkové a viaclinkové PPP hovory. Vzdialený terminálový adaptér pôvodcu musí byť nastavený na rovnaký protokol (jedno, alebo viaclinkový) ako odpovedajúci terminálový adaptér.

- Mechanizmus hardvérového riadenia toku iSeries servera pri tomto terminálovom adaptéri nefunguje správne. To spôsobuje zníženie výkonu, keď server iSeries odosiela údaje viaclinkovým pripojením PPP.

Spravovanie IP adries

Pripojenia PPP umožňujú niekoľko rozličných skupín nastavení spravovania IP adries, v závislosti od typu profilu pripojenia, ktorý umožňuje spravovaniu IP adries pre prepojenie PPP jednoliato pracovať s vašou už existujúcou architektúrou siete. Informácie o definovaní schémy IP adries pre vašu sieť nájdete v nasledujúcich témach:

- DHCP

  DHCP môže vo vašej sieti centrálne spravovať prideľovanie IP adries. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby DHCP.
- DNS

  DNS vám môže pomôcť spravovať hostiteľské mená a im priradené IP adresy. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby DNS.
- BOOTP

  BOOTP sa používa na spojenie klientskych pracovných staníc so serverom iSeries a na priraďovanie ich IP adries. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby BOOTP.
- Filtrovanie IP paketov

  Vytvorením súboru s pravidlami filtrovania IP obmedzte prístup užívateľov a skupín ku konkrétnym IP adresám. Naučte sa viac o podpore filtrovania IP a o tom, ako túto možnosť implementovať vo vašej sieti.

Pred tým, než budete konfigurovať profil pripojenia PPP, mali by ste byť dobre oboznámený so stratégiou spravovania IP adries vo svojej sieti. Táto stratégia ovplyvní mnohé vaše rozhodnutia v priebehu konfiguračného procesu, vrátane vašej stratégie autentifikácie, zvažovania bezpečnosti a nastavenia TCP/IP.

Profily pôvodcu spojenia

V normálnom prípade budú lokálne a vzdialené IP adresy, definované pre profil pôvodcu, zadefinované ako **Priradené vzdialeným systémom**. To umožňuje správcom na vzdialenom systéme spravovať IP adresy, ktoré budú použité pri danom spojení. Takto bude definovaná väčšina všetkých pripojení k poskytovateľom služieb internet (ISP), hoci mnohí ISP ponúkajú pevné IP adresy za dodatočný poplatok.

Ak definujete pevné IP adresy pre lokálnu alebo vzdialenú IP adresu, musíte zaistiť, aby bol vzdialený systém zadefinovaný tak, aby tieto adresy prijal. Bežný postup je taký, že zadefinujete svoju lokálnu adresu ako pevnú IP adresu a vzdialenú ako priradenú vzdialeným systémom. Systém, ktorý kontaktujete, môže byť zadefinovaný rovnako, takže keď sa pripojíte, oba systémy si vzájomne vymenia adresy, aby sa tak dozvedeli adresu vzdialeného systému. Uvedený postup má výhodu, keď jedna pobočka volá druhú, aby získala dočasné pripojenie.

Iným prípadom je, ak chcete umožniť maskovanie IP adries. Napríklad, ak sa iSeries server pripája na internet prostredníctvom ISP, môže to umožniť pripojenej sieti za týmto iSeries serverom mať tiež prístup na internet. iSeries server v podstate ″skryje″ IP adresy systémov na sieti za lokálnu IP adresu, priradenú ISP, vďaka čomu sa bude celá IP prevádzka javiť ako prevádzka z iSeries servera. Existujú však aj iné podmienky smerovania, ktoré platia pre oba systémy v LAN (aby sa zabezpečilo, že ich internetová prevádzka sa posiela na iSeries server.) ako aj pre iSeries server, kde musíte aktivovať políčko 'pridať vzdialený systém ako štandardnú trasu'.

Profily príjemcu spojenia:

Profily príjemcu spojenia obsahujú podstatne viac zvažovania a možností IP adries, než Profil pôvodcu spojenia. To, ako konfigurujete IP adresy, záleží na plánovaní spravovania IP adries vo vašej sieti, na konkrétnych požiadavkách na výkon a funkčnosť tohto pripojenia a na pláne bezpečnosti.

Lokálne IP adresy

Pre samostatný Profil príjemcu spojenia môžete definovať jedinečnú IP adresu, alebo použiť už existujúcu lokálnu IP adresu na vašom serveri iSeries. Tá sa stane adresou, ktorá bude identifikovať druhý koniec spojenia PPP na strane iSeries servera. Pre profily príjemcu spojenia definovaných na podporu viacnásobných pripojení v tom istom čase musíte použiť už existujúcu IP adresu. Ak práve neexistuje žiadna lokálna IP adresa, môžete s týmto cieľom vytvoriť Virtuálnu IP adresu.

Vzdialené IP adresy

Je mnoho možností, ako klientom PPP prideliť vzdialené IP adresy. Nasledujúce možnosti môžu byť definované v profile príjemcu spojenia na strane **TCP/IP**.

Poznámka: Ak chcete, aby bol vzdialený systém považovaný za časť siete LAN, mali by ste nakonfigurovať smerovanie IP adries, zadať IP adresu z rozsahu adries systémov v sieti LAN a overiť si, že bolo povolené postúpenie IP pre tento profil pripojeniam aj pre systém iSeries.

Tabuľka 3. Možnosti priraďovania IP adries pre profil príjemcu spojení

Voľba	Popis
Pevná IP adresa	Definujete jednu IP adresu, ktorá sa poskytne vzdialeným používateľom pri telefonickom pripájaní. Táto IP adresa je len hostiteľská (maska podsiete je 255.255.255.255) a je len pre jednotlivé profily príjemcov pripojenia.
Oblasti adries	Definujete počiatočnú IP adresu a potom rozsah, koľko ďalších IP adries sa má definovať. Každý používateľ, ktorý sa pripojí, potom dostane jedinečnú adresu z tohto zadefinovaného rozsahu. Je to len hostiteľská IP adresa (Maska podsiete je 255.255.255.255) a je len pre viacnásobné profily príjemcu pripojenia.
RADIUS	Vzdialenú IP adresu a jej masku podsiete určí RADIUS server. Toto platí, len ak je určené: • Z konfigurácie služieb servera vzdialeného prístupu bola aktivovaná podpora Radius pre autentifikáciu a IP adresovanie. • V profile príjemcu spojenia je aktivovaná autentifikácia a je definovaná tak, že ju autentifikuje vzdialene Radius.
DHCP	Vzdialená IP adresa je určená priamo serverom DHCP, alebo nepriamo cez relé DHCP. Toto platí, len ak bola podpora DHCP povolená v konfigurácii služieb Servera vzdialeného prístupu. Ide o výlučne hostiteľskú IP adresu (maska podsiete je 255.255.255.255).
V závislosti od ID užívateľa vzdialeného systému	Vzdialená IP adresu určuje id užívateľa určeného pre vzdialený systém pri autentifikácii. To umožňuje, aby správca prideľoval používateľovi, ktorý sa telefonicky pripája, rôzne vzdialené IP adresy (a s nimi spojené masky podsiete). To tiež umožňuje určiť pre každé z týchto užívateľských ID dodatočné trasy, takže môžete každému známemu vzdialenému užívateľovi prispôsobiť prostredie. Na správnu činnosť tejto funkcie musí byť zapnutá autentifikácia.
Určite dodatočné IP adresy založené na užívateľskom ID vzdialeného systému	Táto voľba vám umožní zadefinovať adresy na základe ID používateľa vzdialeného systému. Táto možnosť je automaticky vybraná (a musí sa použiť), ak je metóda prideľovania vzdialených IP adries určená ako **Založená na užívateľskom id vzdialeného systému**. Táto metóda je povolená aj pri priraďovaní pevnej IP adresy a oblasti adries. Keď sa vzdialený používateľ pripája na iSeries server, spustí sa hľadanie, ktoré zisťuje, či je pre tohto konkrétneho používateľa zadefinovaná nejaká vzdialená IP adresa. Ak to je potom táto adresa, pri spojení sa použije maska a množina možných trás. Ak nie je užívateľ určený, bude štandardne pridelená určená Pevná IP adresa, alebo ďalšia adresa z Oblasti IP adries.
Povoľte vzdialenému systému určovať vlastné IP adresy	Táto voľba umožní vzdialenému používateľovi zadefinovať si vlastnú IP adresu, ak o to prejaví záujem. Ak o to záujem neprejavia, bude vzdialená IP adresa určená pomocou nastavenej metódy prideľovania vzdialených IP adries. Táto voľba nie je pôvodne nastavená. Pred jej nastavením treba uvážiť všetky aspekty.

Tabuľka 3. Možnosti priraďovania IP adries pre profil príjemcu spojení (pokračovanie)

Voľba	Popis
Smerovanie IP adries	Ak potrebuje klient prístup k akýmkoľvek IP adresám v sieti LAN, do ktorej iSeries patrí, musia mať volajúci klient aj server iSeries poriadne nakonfigurované smerovanie IP adries.

Filtrovanie IP paketov

Filtrovanie IP paketov je mechanizmus, ktorý môže po prihlásení do siete obmedziť služby pre jednotlivých užívateľov. Filtrovanie paketov môže prístup ″povoliť″ alebo ″zamietnuť″, podľa toho, aké sú cieľové IP adresy a/alebo porty. Rozličné politiky sa implementujú definovaním viacerých sád pravidiel filtrovania paketov, pričom každá sada má vlastný identifikátor filtrovania PPP. Pravidlá filtrovania paketov môžu byť pridelené konkrétnemu Profilu príjemcu spojenia, alebo môžu byť pridelené pomocou skupinovej politiky, ktorá použije pravidlá filtrovania na kategóriu užívateľa. Samotné pravidlá filtrovania paketov nie sú určené v PPP, ale sú definované pod Pravidlami paketov IP v produkte iSeries Navigator. Viac informácií nájdete v Informačnom centre v časti Pravidlá IP paketov.

Pre pripojenia L2TP musí byť na ochranu komunikácie na sieti použité VPN s filtrovaním IP SEc. Viac informácií nájdete v Informačnom centre v časti VPN.

Autentifikácia systému

Spojenie PPP so serverom iSeries podporuje niekoľko možností overovania tak klienta volajúceho na server iSeries, ako aj pripojenia k ISP, alebo inému serveru volanému serverom iSeries. iSeries podporuje niekoľko spôsobov udržiavania autentifikačných informácií, od jednoduchého validizačného zoznamu na iSeries, ktorý obsahuje zoznam oprávnených užívateľov a im priradených hesiel, až po podporu serverov RADIUS, ktoré udržiavajú detailné autentifikačné informácie sieťových užívateľov. iSeries tiež podporuje niekoľko možností šifrovania informácií o užívateľskom ID a hesle, od jednoduchej výmeny hesiel, po podporu CHAP-MD5. Svoje voľby pre systémovú autentifikáciu, vrátane užívateľského ID a hesla použitého na overenie platnosti volajúceho servera iSeries, môžete zadať v záložke **Autentifikácia** profilu pripojenia produktu iSeries Navigator.

Viac informácií o udržiavaní informácií na overovanie platnosti a autentifikáciu nájdete v:

- Remote Authentication Dial In User Service (RADIUS)
- Validizačný zoznam

Viac informácií o podporovaných autentifikačných protokoloch nájdete v:

- Challenge Handshake Authentication Protocol (CHAP-MD5)
- Password Authentication Protocol (PAP)
- Extensible Authentication Protocol (EAP)

CHAP-MD5

Challenge Handshake Authentication Protocol (CHAP-MD5) používa algoritmus (MD-5) na vypočítanie hodnoty, ktorú pozná len autentifikačný systém a vzdialené zariadenie. S CHAP je užívateľské IDa heslo stále zašifrované, takže je to bezpečnejší protokol, než PAP. Tento protokol je efektívny voči pokusom prehrávania a pokusom získať prístup metódou pokus-omyl. Autentifikácia CHAP sa môže počas spojenia vyskytnúť viac ako raz.

Autentifikujúci systém posiela výzvu vzdialenému zariadeniu, ktoré sa snaží o pripojenie k sieti. Vzdialené zariadenie odpovedá s hodnotou, ktorá je vypočítaná spoločným algoritmom (MD-5), ktorý používajú obe zariadenia. Autentifikujúci systém porovná odpoveď so svojím vlastným výpočtom. Autentifikácia je uznaná, keď sa hodnoty zhodujú, v opačnom prípade sa spojenie ukončí.

EAP

Extensible Authentication Protocol (EAP) umožňuje, aby autentifikačné moduly tretích strán komunikovali s implementáciou PPP. EAP rozširuje PPP, keďže poskytuje štandardný mechanizmus podpory pre autentifikačné systémy, napríklad token (smart) card, Kerberos, Public Key a S/Key. EAP reaguje na čoraz častejšiu požiadavku, aby autentifikácia RAS bola doplnená o bezpečnostné zariadenia tretích strán. EAP chráni bezpečné VPN pred hackermi, ktorí útočia na adresáre a heslá. EAP vylepšuje PAP a CHAP.

Pri EAP nie sú autentifikačné informácie zahrnuté v danej informácii, prichádzajú už skôr spolu s informáciou. To umožňuje vzdialeným serverom získať potrebnú autentifikáciu skôr, ako získajú alebo odovzdajú akúkoľvek informáciu.

iSeries server v súčasnosti podporuje len tú verziu EAP, ktorá je v základe ekvivalentná s CHAP-MD5. Môžete však použiť vzdialenú autentifikáciu pomocou RADIUS servera, ktorý môže podporovať niektoré z vyššie uvedených dodatočných autentifikačných systémov.

PAP

Password Authentication Protocol (PAP) používa dvojsmerné dohodnutie, a tak poskytuje rovnocennému systému jednoduchú metódu vytvorenia vlastnej identity. Vzájomná dohoda (handshake) sa vykonáva pri nadväzovaní spojenia. Keď sa spojenie vytvorí, zašle vzdialené zariadenie autentifikačnému systému užívateľské IDa heslo. V závislosti od správnosti tejto dvojice autentifikujúci systém buď pokračuje v spojení, alebo ho ukončí.

Autentifikácia PAP vyžaduje, aby bolo meno používateľa a heslo zaslané na vzdialený systém v čistej textovej forme. Pri PAP sa ID používateľa a heslo nikdy nešifrujú, teda možno ich vystopovať a nie sú odolné voči útokom hackerov. Z týchto dôvodov by ste mali vždy, ak je to možné, používať protokol CHAP.

RADIUS - prehľad

RADIUS (Remote Authentication Dial In User Service) je internetovský štandardný protokol, ktorý poskytuje služby centralizovanej autentifikácie, autorizácie a riadenia IP pre používateľov vzdialeného prístupu v distribuovanej telefónnej sieti.

Model klient-server protokolu RADIUS má server Network Access Server (NAS), ktorý pracuje ako klient pre server RADIUS. iSeries server, ktorý vystupuje ako NAS, posiela informácie o používateľovi a spojení na určený RADIUS server pomocou štandardného protokolu RADIUS, ktorý je definovaný v RFC 2865.

RADIUS servery pracujú na základe prijatých žiadostí používateľov o spojenie tak, že jednotlivých používateľov autentifikujú a potom vrátia všetky potrebné konfiguračné informácie na NAS, takže NAS (iSeries server) môže autentifikovanému telefonickému používateľovi poskytnúť autorizované služby.

Ak sa nedá skontaktovať s RADIUS serverom, iSeries server môže smerovať žiadosti o autentifikáciu na alternatívny server. Vďaka tomu môžu globálne spoločnosti ponúknuť svojim používateľom telefonické pripojenie s jedinečným prihlasovacím ID používateľa na prístup do celej vnútropodnikovej siete bez ohľadu na to, aký prístupový bod použijú.

Keď RADIUS server prijme žiadosť o autentifikáciu, vyhodnotí ju a dešifruje dátový paket, aby získal informácie o mene používateľa a hesle. Tieto informácie ďalej posunie príslušný podporovaný bezpečnostný systém. Toto môžu byť súbory hesiel systému UNIX, protokol Kerberos, komerčný bezpečnostný systém, alebo dokonca vyvinutý bezpečnostný systém. Server RADIUS zašle naspäť serveru iSeries akékoľvek služby, ktoré je autentifikovaný užívateľ oprávnený používať, ako napríklad IP adresy. Požiadavky RADIUS na prideľovanie kont sú spracované podobne. Informácie o kontách vzdialeného používateľa môžu byť zaslané na vybraný určený RADIUS server. Štandardný autorizačný protokol RADIUS je definovaný v RFC 2866. Autorizačný RADIUS server spracúva prijaté žiadosti o kontá protokolovaním informácií zo žiadosti o konto RADIUS. Príklad konfigurácie servera RADIUS nájdete v scenári Autentifikácia volajúcich užívateľov na serveri RADIUS.

Validizačný zoznam

Validizačný zoznam sa používa na ukladanie informácií o užívateľských id a heslách vzdialených užívateľov. Môžete používať už vytvorené validizačné zoznamy alebo si vytvoriť vlastný na autentifikačnej strane Profilu príjemcu spojenia. Záznamy vo validizačnom zozname tiež vyžadujú, aby ste identifikovali typ autentifikačného protokolu, ktorý má byť pridelený užívateľskému id a heslu. To môže byť **zašifrované - CHAP-MD5**/**EAP** alebo **nezašifrované - PAP**.

Viac informácií nájdete v online pomoci.

Informácie o šírke pásma - viacnásobná linka

Často pri vykonávaní určitých úloh požadujete dodatočnú šírku pásma, ktorú však nepotrebujete vždy. Pre tieto prípady je zbytočné kupovať špecializovaný hardvér a drahé komunikačné linky. Viaclinkový protokol PPP Protocol (MP) zoskupuje viaceré linky PPP do formy jednotlivej virtuálnej linky, alebo ″zväzku″. Nazhromaždenie viacerých liniek zvyšuje celkovú výkonnú šírku pásma medzi dvoma systémami pri použití štandardných modemov a telefónnych liniek. Do zväzku MP môžete zlúčiť až šesť liniek. Viaclinkové spojenie sa dá vytvoriť len vtedy, ak oba konce spojenia PPP podporujú viaclinkový protokol. Viaclinkový protokol je dokumentovaný ako štandard RFC1990 (Request For Comment). Viac informácií o RFC nájdete na http://www.rfc-editor.org.

Šírka pásma na požiadanie:

Schopnosť dynamicky pridávať a odstraňovať fyzické spojenia umožňuje systému, aby bol nakonfigurovaný tak, že bude podporovať šírku pásma len vtedy, keď je potrebná. Tento prístup je všeobecne známy ako ″Šírka pásma na vyžiadanie″ a umožní vám platiť za dodatočnú šírku pásma, len ak ju naozaj používate. Aby ste mohli využiť výhody ″Šírky pásma na vyžiadanie″, musí byť aspoň jeden rovnocenný počítač schopný využiť sledovanie aktuálnej celkovej šírky pásma v zväzku MP. Linky potom možno pridávať alebo odoberať zo zväzku, keď využitie šírky pásma presiahne hodnoty definované v konfigurácii. Protokol o pridelení šírky pásma umožňuje, aby sa rovnocenné systémy dohodli na pridávaní a odoberaní liniek do a zo zväzku MP. RFC2125 dokumentuje PPP BAP (Bandwidth Allocation Protocol) a BACP (Bandwidth Allocation Control Protocol).

Kapitola 6. Konfigurácia PPP

Najskôr si musíte nakonfigurovať prostredie PPP a až potom môžete použiť PPP na vytvorenie spojenia point-to-point. V týchto častiach získate konfiguračné informácie pre prostredia PPP:

- Vytvorenie profilu spojenia
- Konfigurácia vášho modemu
- Konfigurácia vzdialeného počítača
- Konfigurácia prístupu na internet cez Všeobecnú sieť AT&T
- Sprievodcovia pripojením
- Konfigurácia skupinovej politiky prístupu
- Aplikácia pravidiel filtrovania IP paketov pri spojení PPP
- Povolenie služieb RADIUS a DHCP pre profily príjemcu spojenia PPP

Vytvorenie profilu spojenia

Prvým krokom pri konfigurovaní spojenia PPP medzi systémami bude vytvorenie profilu spojenia na iSeries serveri. Profil spojenia je logickou reprezentáciou týchto konkrétnych informácií:

- Typ linky a profilu
- Nastavenia viacnásobnej linky
- Telefónne čísla pre vzdialený prístup a voľby vytáčania
- Autentifikácia
- Nastavenia TCP/IP: IP adresy a smerovanie
- Riadenie prevádzky a prispôsobenie spojenia
- Názvové servery domény

Služby vzdialeného prístupu v adresári Podsieť obsahujú tieto objekty:

- **Profily pôvodcu spojenia** sú odchádzajúce spojenia point-to-point, ktoré iniciuje iSeries server (lokálny systém). Tieto spojenia PPP prijíma vzdialený systém.
- **Profily príjemcu spojenia** sú prichádzajúce spojenia point-to-point, ktoré iniciuje vzdialený systém. Tieto spojenia PPP prijíma iSeries server (lokálny systém).
- **Modemy**

Ak chcete vytvoriť profil spojenia, postupujte podľa týchto krokov:

1. V produkte iSeries Navigator označte svoj systém a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Vyberte jednu z týchto volieb:
   - Kliknutím pravého tlačidla myši na **Profily pôvodcu pripojenia** nastavte server iSeries ako server, ktorý iniciuje pripojenie.
   - Pravým tlačidlom myši kliknite na **Profily príjemcu spojenia**, čím nastavíte iSeries server ako server, ktorý umožní pripojenia prichádzajúce od vzdialených systémov a používateľov.
3. Vyberte **Nový profil**.
4. Na strane **Nastavenie nového profilu spojenia point-to-point** vyberte typ protokolu.
5. Zadajte výber režimu.
6. Vyberte konfiguráciu linky.
7. Kliknite na **OK**.

   Zobrazí sa strana **Vlastnosti nového profilu point-to-point**. Môžete nastaviť ostatné hodnoty, špecifické pre vašu sieť. Viac konkrétnych informácií nájdete v online pomoci.

Typ protokolu: PPP alebo SLIP

Aký typ protokolu by ste si mali vybrať na vytvorenie spojenia point-to-point?

PPP je štandardné internetovské spojenie. PPP umožňuje vzájomnú prevádzkyschopnosť medzi softvérom pre vzdialený prístup od rôznych výrobcov. PPP tiež umožňuje používanie tej istej fyzickej komunikačnej linky pre viac sieťových komunikačných protokolov.

PPP nahrádza SLIP ako protokol pre spojenia point-to-point. Request For Comment (RFC) pre SLIP sa nikdy nestal internetovským štandardom, pretože má uvedené nedostatky:

- SLIP nemá štandardný spôsob, akým definuje IP adresovanie medzi dvoma hostiteľmi. To znamená, že nemožno použiť neočíslovanú sieť.
- SLIP nemá žiadnu podporu pre zisťovanie alebo potláčanie chýb. Zisťovanie a potláčanie chýb sa implementuje v PPP.
- SLIP nemá žiadnu podporu pre autentifikáciu systému, PPP však má dvojsmernú autentifikáciu.

SLIP sa dnes stále používa a iSeries server ho podporuje. Spoločnosť IBM vám však pri nastavovaní konektivity point-to-point odporúča použiť PPP. SLIP neposkytuje žiadnu podporu viaclinkových spojení. PPP má v porovnaní so SLIP lepšiu autentifikáciu. PPP dosahuje lepší výkon kvôli možnosti komprimácie.

Poznámka: V tomto vydaní sa už nepodporujú profily spojení SLIP, ktoré sú definované s typmi liniek ASYNC. Ak máte také profily spojení, musíte ich presunúť, a to buď do profilu SLIP alebo do profilu PPP, ktorý používa typ linky PPP.

Výber režimu

Výber režimu pre profil spojenia PPP pozostáva z výberu **typu spojenia** a výberu **režimu prevádzky**. Výberom režimu určíte, ako bude server používať nové spojenie PPP.

Ak chcete zadať svoje voľby režimu, postupujte podľa týchto krokov:

1. Vyberte jeden z uvedených typov spojenia:
   - Komutovaná linka
   - Prenajatá linka
   - L2TP (virtuálna linka)
   - Linka PPPoE
2. Vyberte vhodný režim prevádzky pre nové spojenie PPP.
3. Zaznamenajte si typ spojenia a režim prevádzky, ktorý ste vybrali. Tieto informácie budete potrebovať, keď začnete s konfiguráciou svojho spojenia PPP.

Komutovaná linka

Vyberte tento typ spojenia, ak na spojenie po telefónnej linke používate niektoré z uvedených zariadení:

- Modem (interný alebo externý)
- Interný adaptér ISDN pre Basic Rate Interface
- Externý terminálový adaptér ISDN

Typ spojenia komutovanou linkou rozoznáva tieto režimy prevádzky:

- **Odpovedať**

  Výberom tohto typu režimu prevádzky umožníte vzdialenému systému telefonicky sa pripojiť k iSeries serveru.
- **Vytáčať**

  Týmto režimom prevádzky umožníte iSeries serveru telefonicky sa pripojiť k vzdialenému systému.
- **Vytáčať na požiadanie (len vytáčanie)**

Výberom tohto režimu prevádzky umožníte iSeries serveru automatické telefonické pripojenie k vzdialenému systému, keď na ňom zistí prevádzku TCP/IP. Pripojenie sa ukončí, keď je prenos údajov ukončený a po stanovený čas sa nevyskytne žiadna prevádzka TCP/IP.

- **Vytáčať na požiadanie (rovnocenný systém s povoleným odpovedaním)**

  Výberom tohto režimu prevádzky umožníte iSeries serveru odpovedať na volania zo vzdialeného systému. iSeries server bude môcť zavolať vzdialený systém, ak zistí prevádzku TCP/IP pre daný vzdialený systém. Ak sú oba systémy iSeries servery a ak oba používajú tento režim prevádzky, prevádzka TCP/IP tečie medzi nimi na požiadanie a nepotrebujú trvalé fyzické spojenie. Tento režim prevádzky vyžaduje vyhradený prostriedok. Ak má režim správne fungovať, vzdialený rovnocenný systém musí realizovať telefonické volanie.
- **Vytáčať na požiadanie (povolený vzdialený rovnocenný systém)**

  V tomto režime prevádzky umožníte telefonické pripojenie k vzdialenému systému alebo odpoveď naň. Pri spracúvaní prichádzajúcich volaní sa musíte odvolať na existujúci profil odpovede z toho profilu spojenia PPP, v ktorom sa zadal tento prevádzkový režim. To umožní, aby jeden profil odpovede spracúval všetky prichádzajúce volania z jedného alebo viacerých vzdialených rovnocenných systémov a iný profil vytáčania na požiadanie spracúval každé odchádzajúce volanie. Tento prevádzkový režim nevyžaduje na spracúvanie prichádzajúcich volaní zo vzdialených rovnocenných systémov vyhradený prostriedok.

Prenajatá linka

Tento typ spojenia vyberte vtedy, ak máte komutovanú linku medzi lokálnym iSeries serverom a vzdialeným systémom. Ak máte prenajatú linku, nepotrebujete na prepojenie týchto dvoch systémov modem ani terminálový adaptér ISDN.

Spojenie prenajatou linkou medzi dvoma systémami sa považuje za trvalú alebo nekomutovanú linku. Toto spojenie je stále otvorené. Jeden koniec spojenia prenajatou linkou sa konfiguruje ako iniciátor spojenia, druhý koniec ako terminátor.

Typ spojenia prenajatou (nekomutovanou) linkou rozoznáva tieto režimy prevádzky:

- **Terminátor**

  Výberom tohto typu režimu prevádzky umožníte vzdialenému systému pristupovať na iSeries server po nekomutovanej linke. Tento režim prevádzky sa odvoláva na profil odpovede pri prenajatej linke.
- **Iniciátor**

  Výberom tohto režimu prevádzky umožníte iSeries serveru pristúpiť ku vzdialenému systému po nekomutovanej linke. Tento režim prevádzky sa odvoláva na profil vytáčania pri prenajatej linke.

L2TP (virtuálna linka)

V tomto type spojenia umožníte spojenie medzi systémami, ktoré používajú L2TP - Layer Two Tunneling Protocol.

Keď sa vytvorí tunel L2TP, nadviaže sa virtuálne spojenie PPP medzi vaším iSeries serverom a vzdialeným systémom. Použitím tunelovania L2TP v spojení s bezpečnosťou IP (IP-SEC) môžete posielať, smerovať a prijímať bezpečné údaje prostredníctvom internetu.

Typ spojenia L2TP (virtuálna linka) rozoznáva tieto režimy prevádzky:

- **Terminátor**

  Výberom tohto typu režimu prevádzky umožníte vzdialenému systému pripojiť sa k iSeries serveru cez tunel L2TP.
- **Iniciátor**

  Výberom tohto režimu prevádzky umožníte iSeries serveru pripojenie k vzdialenému systému cez tunel L2TP.
- **Vzdialené telefonické pripojenie**

  Výberom tohto režimu prevádzky umožníte iSeries serveru pripojenie k ISP cez tunel L2TP a vydáte pokyn pre ISP, aby sa telefonicky spojil so vzdialeným klientom PPP.

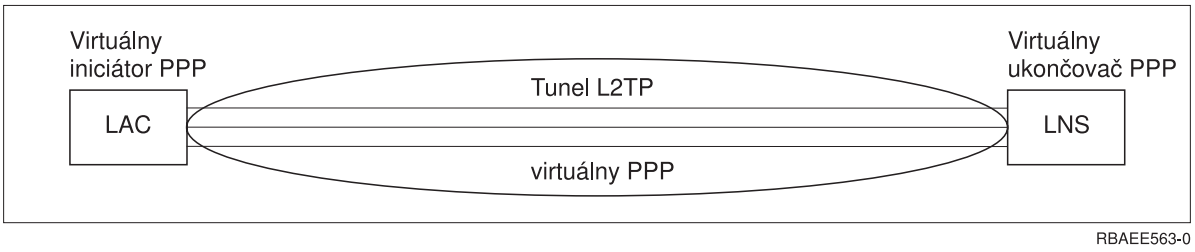
- **Viacskokový iniciátor**
  Výberom tohto režimu prevádzky umožníte iSeries serveru nadviazať viacskokové spojenie.

  Poznámka: Profil Terminátor L2TP, s ktorým je tento viacskokový iniciátor spojený, musí mať začiarknuté políčko ″Umožniť viacskokové spojenie″ a mať vo validizačnom zozname PPP položku, ktorá spája meno používateľa PPP s profilom viacskokového iniciátora.

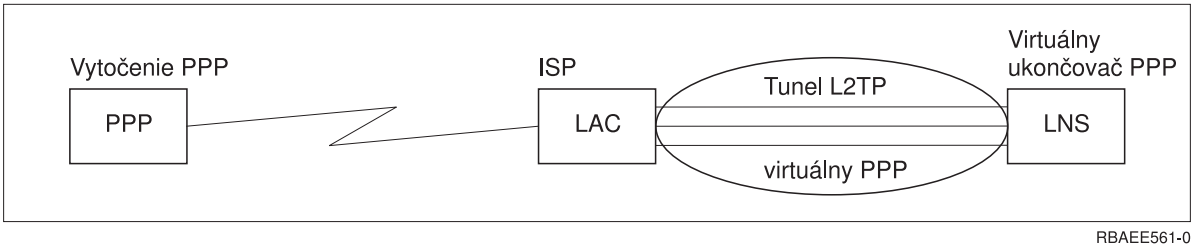
L2TP - Layer 2 Tunneling Protocol: L2TP rozširuje PPP tak, aby podporovala tunel spojovacej vrstvy medzi žiadajúcim klientom L2TP a cieľovým koncovým bodom, serverom L2TP. Pomocou tunelov L2TP možno oddeliť miesto, na ktorom sa končí protokol telefonického pripojenia od miesta, na ktorom sa poskytuje prístup na sieť.

Poskytovateľ služieb internetu (ISP) používa na prevádzku Virtual Private Networks (VPN) režim virtuálnej linky. Pozrite si Konfigurovanie spojenia L2TP, chráneného VPN, aby ste lepšie rozumeli tomu, ako pracuje VPN s L2TP.

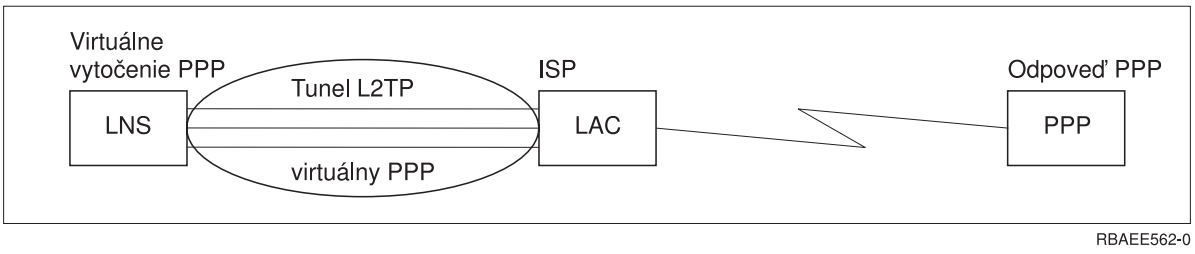
Nasledujúce obrázky ilustrujú tri rôzne realizácie tunelovania L2TP:



Obrázok 7. Virtuálny iniciátor PPP alebo virtuálny terminátor PPP



Obrázok 8. Telefonický iniciátor PPP alebo virtuálny terminátor PPP



Obrázok 9. Virtuálne vytáčanie PPP alebo virtuálne odpovedanie PPP

Linka PPPoE

Pripojenie PPPoE používa virtuálnu linku na odosielanie údajov PPP cez adaptér typu Ethernet 2838 k modemu DSL, poskytnutému vaším ISP, ktorý je tiež pripojený do Ethernetovej siete LAN. Toto umožňuje

užívateľom siete LAN vysokorýchlostný prístup na internet cez reláciu PPP na serveri iSeries. Keď je už spojenie medzi iSeries a ISP spustené, môžu jednotliví užívatelia siete LAN začať s IPS jedinečné relácie cez PPPoE.

Pripojenia PPPoE sú používané len profilom pôvodcu spojenia, naznačujú prevádzkový režim Iniciátora a používajú len samostatnú linku.

Konfigurácia spojenia

Konfigurácia spojenia definuje typ linkovej služby, ktorú váš profil spojenia PPP používa na nadviazanie spojenia. Typy linkovej služby závisia od typu spojenia, ktoré zadáte.

- Jednoduchá linka
- Linková oblasť
- Integrovaná linka ISDN

Jednoduchá linka

Túto linkovú službu vyberte na zadefinovanie linky PPP, ktorá je napojená na analógový modem. Táto voľba sa tiež používa pre prenajaté linky, kde sa nevyžaduje modem. Tento typ spojenia PPP vždy používa rovnaký prostriedok komunikačného portu na iSeries serveri.

Ak je to žiaduce, môže byť samostatná analógová linka nakonfigurovaná ako 'zdieľaná' medzi volajúcim a odpovedajúcim profilom. Dynamické zdieľanie prostriedkov je nová funkcia navrhnutá na zvýšenie ich použiteľnosti. Pred vydaním 2, verziou 5 (V5R2), boli prostriedky modemu viazané ihneď po spustení profilu, ktorý ich používal. To obmedzovalo užívateľa na jeden prostriedok v rámci relácie, aj keď bol tento prostriedok v pasívnom stave čakania. Teraz sú pri prístupe ku konkrétnemu prostriedku použité nové pravidlá zdieľania. Sú dve možnosti: Po prvé, volajúci profil bol spustený skôr, než odpovedajúci. Po druhé, odpovedajúci profil bol spustený skôr, než volajúci. Podmienkou je, že je povolené zdieľanie prostriedkov. V prvom prípade sa spustený volajúci profil úspešne pripojí. Odpovedajúci profil, ktorý bol spustený ako druhý, počká, kým bude linka prístupná. Keď sa ukončí vytáčané pripojenie, odpovedajúci profil si vyžiada linku a spustí sa. V druhom prípade počká spustený odpovedajúci profil na prichádzajúce spojenie. Kým nie je vykonané prichádzajúce spojenie, 'požičia' si volajúce spojenie, ktoré bolo spustené ako druhé, linku od odpovedajúceho profilu, ktorý mu linku 'požičia'. Potom bude vytvorené odchádzajúce spojenie. Keď je spojenie ukončené, volajúci profil vráti linku odpovedajúcemu profilu, ktorý bude znova schopný akceptovať prichádzajúce spojenia. Funkciu zdieľania povolíme kliknutím na opis prepnutej linky v záložke Modem a výberom 'Povoliť dynamické zdieľanie prostriedkov'.

Služba samostatnej linky je tiež použitá pre typy pripojenia L2TP (virtuálna linka) a PPPoE (virtuálna linka). Pri typoch spojenia L2TP (virtuálna linka) sa nepoužíva na jednoduchú linku žiadny hardvérový prostriedok komunikačného portu. Jednoduchá linka použitá spojením L2TP je skôr *virtuálna* v tom, že na vytvorenie tunela nie je požadovaný žiaden fyzický hardvér PPP. Jednoduchá linka použitá na vytvorenie pripojenia PPPoE je tiež virtuálna, a tak umožňuje mechanizmus, vďaka ktorému sa môžeme k fyzickému Ethernetu správať, akoby to bola linka PPP, ktorá podporuje vzdialené pripojenie. Virtuálna linka PPP je pripojená k linke fyzického Ethernetu a používa sa na podporu prenosu údajov z pripojenia LAN Ethernet k modemu DSL.

Linková oblasť

Výberom tejto linkovej služby nastavíte spojenie PPP na používanie linky z linkovej oblasti. Keď sa spojenie PPP spustí, iSeries server si vyberie z linkovej oblasti nepoužívanú linku. Pri profiloch telefonického pripojenia na požiadanie si server linku vyberie až vtedy, keď zistí pre vzdialený systém prevádzku TCP/IP.

Linkovú oblasť môžete použiť namiesto definovania určitého popisu linky pre profil spojenia. V linkovej oblasti môžete špecifikovať jeden alebo viac popisov linky.

Linková oblasť ďalej umožňuje, aby jeden profil spojenia spracúval buď viacnásobné prichádzajúce analógové volania alebo jedno odchádzajúce analógové volanie. Linka sa po ukončení spojenia PPP vracia do linkovej oblasti.

Ak používate linkovú oblasť na spracúvanie viacnásobných prichádzajúcich analógových volaní súčasne, musíte stanoviť maximálny počet prichádzajúcich volaní. Ten môžete nastaviť v paneli Spojenia v dialógovom okne **Vlastnosti nového profilu point-to-point** pri konfigurácii profilu vášho spojenia. Použite viaclinkové nastavenia, pomocou ktorých môžete linkové oblasti použiť na samostatné pripojenie so zväčšenou šírkou pásma.

Výhody používania linkových oblastí:

- Prostriedok linky viažete na spojenie PPP až pri jeho spustení.

  Pri pripojení PPP, ktoré využíva konkrétnu linku, sa pripojenie ukončí, ak nie je linka prístupná, ak nie je povolené dynamické zdieľanie prostriedkov. Pre pripojenia, ktoré používajú linkové oblasti, musí byť pri spustení spojenia dostupná aspoň jedna linka oblasti.

  Navyše, ak boli prostriedky nakonfigurované ako zdieľané (s povoleným dynamickým zdieľaním prostriedkov) je najmä pre odchádzajúce spojenia dosiahnutá dodatočná dostupnosť prostriedkov.
- Aby ste prostriedky využívali efektívnejšie, môžete použiť profily telefonického pripojenia na požiadanie (dial-on-demand) s linkovými oblasťami.

  iSeries server si vyberie linku z linkovej oblasti len vtedy, keď používa spojenie typu dial-on-demand. Ostatné spojenia môžu tú istú linku použiť inokedy.
- Môžete spustiť viac spojení PPP s menším počtom prostriedkov na ich podporu.

  Ak napríklad vaše prostredie potrebuje štyri jedinečné typy spojení, ale vám stačia naraz maximálne dve linky, na spustenie tohto prostredia môžete použiť linkovú oblasť. Vytvoríte štyri profily spojenia typu dial-on-demand a každý profil odkážete na linkovú oblasť, ktorá obsahuje popisy dvoch liniek. Každá z liniek by mohla byť použitá všetkými štyrmi profilmi a tak dvom pripojeniam umožňuje byť aktívnymi kedykoľvek. Použitím spoločnej linkovej oblasti nemusíte mať štyri samostatné linky.

  Taktiež, ak je vaše prostredie kombináciou medzi Klientom PPP a Serverom PPP, môžu byť linky zdieľané (s povoleným dynamickým zdieľaním zdrojov) nezávisle od toho, či sú použité ako 'samostatné linky', alebo umiestnené v 'linkovej oblasti'. Profil, ktorý bol spustený ako prvý, nezapojí prostriedok, kým nie je spojenie aktívne. Napríklad, ak je spustený Server PPP a očakáva prichádzajúce spojenia, 'požičia' používanú linku Klientovi PPP, ktorý sa spustil a 'požičiava' si od Servera PPP túto zdieľanú linku.

Podpora profilu viacnásobného spojenia

Profily spojenia point-to-point, ktoré podporujú viaceré spojenia, vám umožňujú mať jeden profil spojenia, ktorý obsluhuje viacero digitálnych, analógových volaní alebo volaní L2TP. Túto možnosť využijete vtedy, keď chcete, aby sa na váš iSeries server pripojilo viac používateľov, ale nechcete na spracovanie každej linky PPP definovať osobitný profil spojenia point-to-point. Táto vlastnosť je mimoriadne užitočná pri integrovanom štvorportovom modeme 2805l, pri ktorom sú štyri linky využívané jedným adaptérom, alebo pri adaptéroch 2750 a 2751, ktoré podporujú osem osobitných pripojení ISDN B-kanálov.

Pre analógové linky s podporou profilu pre viacnásobné spojenia sa používajú všetky linky v špecifikovanej linkovej oblasti až po maximálny počet spojení. V podstate sa spustí samostatná úloha profilu spojenia pre každú linku, ktorá je definovaná v spoločnej linkovej oblasti. Všetky úlohy profilu spojenia čakajú na prichádzajúce volania na príslušných linkách.

Lokálna IP adresa pre profily viacnásobných spojení:

Lokálnu IP adresu môžete použiť pri profiloch viacnásobných spojení, musí však ísť o existujúcu IP adresu, ktorá je definovaná na vašom iSeries serveri. Môžete použiť sťahovací zoznam lokálnych IP adries, aby ste vybrali existujúcu adresu. Vzdialení používatelia môžu pristupovať k prostriedkom, ktoré sa nachádzajú na vašej lokálnej sieti, ak si zvolíte IP adresu lokálneho iSeries servera ako lokálnu IP adresu pre svoj profil PPP. Tiež musíte definovať IP adresy, ktoré sú vo vzdialenej spoločnej oblasti IP adries, aby boli v rovnakej sieti ako lokálne IP adresy.

Ak nemáte IP adresu lokálneho iSeries servera alebo ak nechcete, aby vzdialení používatelia mali prístup na LAN, musíte zadefinovať pre svoj iSeries server virtuálnu IP adresu. Virtuálna IP adresa je tiež známa

ako bezokruhové rozhranie. Vaše profily point-to-point môžu používať túto IP adresu ako ich lokálnu IP adresu. Keďže táto adresa sa neviaže na fyzickú sieť, nebude automaticky presmerúvať prevádzku na iné siete, ktoré sú pripojené k vášmu iSeries serveru.

Na vytvorenie virtuálnej IP adresy vykonajte tieto kroky:

1. V produkte iSeries Navigator rozviňte svoj server a pristúpte na **Sieť –> Konfigurácia TCP/IP > IPV4 > Rozhrania**.
2. Kliknite pravým tlačidlom myši **Rozhrania** a vyberte **Nové rozhranie—>Virtuálna IP.**
3. Postupujte podľa inštrukcií sprievodcu rozhrania, aby ste vytvorili vaše virtuálne IP rozhranie. Keď sa vytvorí Virtuálna IP adresa, vaše profily spojenia point-to-point ju môžu používať. Ak chcete so svojím profilom použiť adresu, môžete použiť sťahovací zoznam z poľa Lokálna IP adresa, ktorý je na stránke Nastavenia TCP/IP.

   Poznámka: Virtuálna IP adresa musí byť aktívna pred spustením vášho profilu viacnásobných spojení, inak sa profil nespustí. Na aktiváciu adresy po vytvorení rozhrania počas používania sprievodcu rozhraním vybrať voľbu na spustenie adresy.

Spoločná oblasť vzdialených IP adries pre profily viacnásobných spojení:

S profilmi viacnásobných spojení môžete tiež použiť spoločné oblasti vzdialených IP adries. Len typický profil jedného spojenia point-to-point vám umožňuje určiť jednu vzdialenú IP adresu, ktorá je daná volajúcemu systému, keď sa vytvorí spojenie. Keďže viacerí volajúci sa teraz môžu pripájať simultánne, spoločná oblasť vzdialených IP adries sa používa na definovanie počiatočnej vzdialenej IP adresy a tiež ako rozsah dodatočných IP adries, ktoré sú pridelené volajúcemu systému.

Obmedzenia linkovej oblasti:

Tieto obmedzenia platia pri používaní linkových oblastí pre viacnásobné spojenia:

- Určitá linka môže existovať len v jednej spoločnej oblasti v určitom čase. Ak odstránite linku zo spoločnej oblasti, môže sa použiť v inej spoločnej oblasti.
- Pri spúšťaní profilu viacnásobného spojenia, ktorý používa linkovú oblasť, sa použijú všetky linky v linkovej oblasti až po maximálny počet spojení, ktorý je zadefinovaný v tomto profile. Ak nie sú dostupné žiadne linky, zlyhajú všetky nové spojenia. Taktiež, ak je spustený ďalší profil, ale nie sú dostupné žiadne linky v linkovej oblasti, bude tento profil ukončený.
- Keď spustíte profil jedného spojenia, ktorý má linkovú oblasť, systém používa len jednu linku zo spoločnej oblasti. Ak spustíte profil viacnásobného pripojenia, ktorý používa rovnakú linkovú oblasť, použijú sa akékoľvek dostupné linky linkovej oblasti.

Spoločné oblasti vzdialených IP adries: Systém môže používať spoločné oblasti vzdialených IP adries na odpovedanie alebo ukončovanie profilu spojenia PPP, ktorý sa používa s viacerými prichádzajúcimi spojeniami. Toto zahŕňa L2TP, pôvodný ISDN a linkové oblasti s maximálnym počtom spojení väčším ako jeden. Táto funkcia dovoľuje systému priraďovať jedinečné vzdialené IP adresy každému prichádzajúcemu spojeniu.

Prvý systém na pripojenie dostane IP adresu definovanú v poli Počiatočná IP adresa. Ak je už táto adresa použitá, je pridelená nasledujúca IP adresa z rozsahu Počtu adries. Predpokladajme, napríklad, že Počiatočná adresa je 10.1.1.1 a Počet adries je určený ako 5. Adresy oblasti vzdialených IP adries budú 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 a 10.1.1.5. Maska podsiete, definovaná pre adresy spoločnej oblasti vzdialených IP adries, bude vždy 255.255.255.255.

Keď používate spoločné oblasti vzdialených IP adries, platia tieto obmedzenia:

- Viac ako jeden profil spojenia môže špecifikovať rovnakú oblasť adries. Ak sa však používajú všetky adresy v oblasti, každá nasledujúca požiadavka na spojenie bude odmietnutá, pokiaľ sa neskončí nejaké iné spojenie a neuvoľní adresu.

- Ak chcete priradiť špecifické adresy niektorým vzdialeným systémom a iným prichádzajúcim systémom povoliť používanie adresy zo spoločnej oblasti, postupujte podľa týchto krokov:
  1. Umožnite Autentifikáciu vzdialeného systému zo záložky **Autentifikácia**, aby sa dal zistiť názov používateľa vzdialeného systému.
  2. Definujte oblasť vzdialených IP adries pre všetky prichádzajúce požiadavky spojenia, ktoré nevyžadujú špecifickú IP adresu.
  3. Definujte vzdialené IP adresy pre konkrétnych používateľov začiarknutím **Definovať dodatočné IP adresy na základe ID používateľa vzdialeného systému** a kliknutím na **IP adresy definované podľa mena používateľa**.

  Keď sa pripojí daný vzdialený používateľ, iSeries server zistí, či je preňho definovaná konkrétna IP adresa. V tomto prípade je systému daná IP adresa, inak sa vráti adresa zo spoločnej oblasti vzdialených adries.

ISDN
Vyberte túto linkovú službu na definovanie linky PPP, ktorá je spojená so sieťovým spojením ISDN.

Výhody použitia ISDN:
- ISDN ponúka nerušenú komunikáciu pri vyšších rýchlostiach.
- Účelom ISDN je poskytovať univerzálnu konektivitu pri použití jediného rozhrania a vysokorýchlostnej digitálnej siete na prenos všetkých druhov údajov.
- ISDN má aj výhodu rýchlych spojovacích časov v prípade komutovaných spojení. Pripojenie analógového modemu môže trvať 30 sekúnd alebo viac, kým pripojenie ISDN trvá len niekoľko sekúnd.

Konfigurácia vášho modemu pre PPP

Na svoje analógové pripojenia PPP môžete použiť externý modem, interný modem, alebo terminálový adaptér ISDN. Modem vám poskytuje schopnosti analógového spojenia (nekomutované a komutované linky). Pre iSeries server boli zadefinované popisy najpoužívanejších modemov.

Môžete vykonať tieto úlohy konfigurácie modemu:
- Konfigurácia nového modemu
- Priradenie modemu k opisu linky
- Nastaviť príkazové reťazce modemu

Konfigurácia nového modemu

1. V produkte iSeries Navigator označte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. Na paneli Všeobecné zadajte správne hodnoty do všetkých políčok.
4. **Voliteľné:** Kliknite na panel Dodatočné parametre a pridajte akékoľvek potrebné inicializačné príkazy pre svoj modem.
5. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu Vlastnosti nového modemu.

Ak chcete určiť, či môžete použiť už existujúci popis modemu, vykonajte tieto kroky:
1. V produkte iSeries Navigator označte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Vyberte **Modemy**.
3. Prezrite si zoznam modemov a nájdite výrobcu, model a značku svojho modemu.

   Poznámka: Ak sa váš modem nachádza na tomto zozname, nemusíte vykonať žiadne ďalšie kroky.
4. Kliknite pravým tlačidlom myši na popis modemu, ktorý sa približne zhoduje s vaším modemom a vyberte **Vlastnosti**, aby ste si prezreli príkazové reťazce.

5. Konkrétne príkazové reťazce pre váš modem nájdete v jeho dokumentácii.

   Použite vopred nastavené vlastnosti modemu, ak tieto príkazové reťazce zodpovedajú požiadavkám vášho modemu. V opačnom prípade musíte pre svoj modem vytvoriť jeho popis a pridať ho do zoznamu modemov.

Ak chcete vytvoriť popis modemu, postupujte podľa týchto krokov:

1. V Operations Navigator vyberte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Vyberte **Modemy**.
3. Na zozname modemov kliknite pravým tlačidlom na **$generic hayes** a vyberte **Nový modem založený na**.
4. V dialógovom okne **Nový modem** zmeňte príkazové reťazce tak, aby zodpovedali informáciám, ktoré váš modem vyžaduje.

Nastaviť príkazové reťazce modemu

Dole uvedená tabuľka uvádza zoznam minimálnej sady príkazových reťazcov, ktoré používajú modemy zadefinované na iSeries serveri. Ekvivalentný príkazový reťazec pre svoj modem nájdete v užívateľskej príručke. V popise modemu použite výrobcom odporúčané nastavenie.

Vlastnosť modemu	**Správny príkazový reťazec pre väčšinu modemov**
Resetovanie modemu na štandardné nastavenie z továrne	AT&F alebo AT&Z
Inicializácia modemu:	
Kódy Display Verbal Results	Q0 a V1
Normálne režimy CD a DTR	&C1 a &D2
Vypnutie režimu Echo	E0
DSR (Data Set Ready) podľa Carrier Detect	&S1
Umožniť hardvérové riadenie toku (RTS/CTS)	
Umožniť opravu chýb a voliteľne i kompresiu (V.42/V.42 bis)	
Skontrolujte, či je rýchlosť linky DTE-DCE nastavená na pevnú hodnotu 115,2 kbps (alebo maximálnu hodnotu, ktorú modem umožňuje)	
(Voliteľné) Umožniť čas nečinnosti, ak modem podporuje túto funkciu	
Režim odpovedania modemu:	
Odpovedať po *n* zvoneniach	S0=*n*, kde n = 1 alebo 2
Odpojiť, ak nie je spojenie po *m* sekundách	S7=*m*
Typ vytáčania modemu	ATDT pre tónovú voľbu alebo ATDP pre impulzovú voľbu

Príklad: Konfigurácia terminálového adaptéra ISDN

1. V Operations Navigator vyberte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. Na paneli Všeobecné zadajte správne hodnoty do všetkých políčok.
4. **Voliteľné:** Kliknite na panel Parametre ISDN a pridajte akékoľvek potrebné inicializačné príkazy pre svoj modem.

   Pre terminálové adaptéry ISDN sú príkazy a parametre v tomto zozname odoslané na terminálový adaptér len pri splnení nasledujúcich podmienok:

   - Príkazy alebo parametre v zozname sú buď zmenené, alebo pridané
   - iSeries server vykonal isté úkony obnovovania po chybe

Následne by mali tieto príkazy zahŕňať a mali by byť obmedzené na nasledujúce:

- Nastavenie komutovaného typu ISDN a verzie, ktorú poskytuje miestna telekomunikačná spoločnosť
- Nastavenie čísel adresára a SPID (Service Profile Identifiers), ktoré poskytuje miestna telekomunikačná spoločnosť
- Nastavenie TEI (Terminal Entry ID), ktoré môže poskytovať miestna telekomunikačná spoločnosť
- Nastavenie protokolu B-kanála (asynchrónne na synchrónne PPP)
- Iné nastavenia modemu, ktoré má parametre s premenlivou dĺžkou, ktoré si vyžadujú na označenie dĺžky parametra CR
- Uloženie a aktivácia nových nastavení tak, aby boli obnovené po vynulovaní alebo vypnutí systému.
- Príkaz skúšky aktívneho stavu rozhrania *U* (ATD*x*), ktorý umožňuje iSeries serveru určiť, kedy bola dosiahnutá synchronizácia s centrálnou ústredňou. *x* môže byť akákoľvek číslica povolená pre telefónne číslo, vrátane # a *.

5. Kliknite na **Pridať** k dodatočným príkazom pre modem. Tieto príkazy môžu byť uvedené s alebo bez priradeného parametra a krátkeho popisu na zoznam príkazov. Ku ktorémukoľvek príkazu, ktorý určíte bez priradeného parametra, môže byť priradený parameter po tom, ako sa modemu priradí popis linky.
6. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu Vlastnosti nového modemu.

Priradenie modemu k opisu linky

1. V produkte iSeries Navigator označte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu –> Profily pôvodcu spojenia**, alebo **Profily príjemcu spojenia**.
2. Vyberte jednu z uvedených možností:
   - Ak chcete pracovať s už vytvoreným profilom spojenia, pravým tlačidlom myši kliknite na profil spojenia a vyberte **Vlastnosti**.
   - Ak chcete pracovať s novým profilom spojenia, vytvorte ho.
3. Zo strany Vlastnosti nového profilu point-to-point vyberte panel **Spojenie** a kliknite na **Nové**.
   - Zadajte názov konfigurácie spojenia.
   - Kliknite na **Nová**, čím otvoríte dialógové pole Vlastnosti novej linky.
4. V dialógovom okne Vlastnosti novej linky kliknite na panel **Modem** a zo zoznamu vyberte modem. Vybraný modem bude priradený k popisu tejto linky. Pri internom modeme by už mala byť patričná definícia modemu označená. Viac informácií nájdete v online pomoci.

Vo verzii V5R2 si profily pôvodcu pripojenia môžu ″vypožičať″ linku PPP a modem priradený profilu príjemcu pripojenia, ktorý očakáva volanie. Keď sa spojenie ukončí, pôvodca pripojenia ″vráti″ linku PPP a modem profilu adresáta pripojenia. Túto novú funkciu povolíte, ak vyberiete možnosť **Povoliť dynamické zdieľanie prostriedkov** zo záložky Modem v konfiguračnom dialógu linky PPP. Linky PPP môžete konfigurovať v záložke Pripojenie v Profiloch pôvodcu a adresáta pripojenia.

Konfigurácia vzdialeného počítača

Ak sa chcete pripojiť k iSeries serveru z počítača, na ktorom je spustený akýkoľvek 32-bitový operačný systém Windows, overte, či je na tomto počítači nainštalovaný a správne nakonfigurovaný modem a skontrolujte, či ste na počítač nainštalovali TCP/IP a Dial-Up Networking.

Informácie o konfigurovaní Dial-Up Networking na svoj počítač nájdete v dokumentácii k Microsoft Windows. Nezabudnite špecifikovať alebo zadať tieto informácie:

- Typ telefonického spojenia by mal byť **PPP**.
- Ak používate šifrované heslá, skontrolujte, či používate MD-5 CHAP (MS-CHAP iSeries server NEPODPORUJE). Niektoré verzie Windows nepodporujú MD-5 CHAP priamo, ale s pomocou Microsoftu ich môžete nakonfigurovať.
- Ak používate nezašifrované (alebo nezabezpečené) heslá, automaticky sa použije PAP. Iný typ nezabezpečeného protokolu iSeries server nepodporuje.

- IP adresovanie zvyčajne definuje daný vzdialený systém alebo v tomto prípade iSeries server. Ak chcete použiť iné metódy IP adresovania (napríklad definovanie vlastných IP adries), skontrolujte, či je váš iSeries server nakonfigurovaný na prijatie tejto metódy adresovania.
- Pridajte IP adresu DNS, ak sa to týka vášho prostredia.

Konfigurácia prístupu na internet cez Všeobecnú sieť AT&T

Spoločnosť IBM poskytuje prístup na internet prostredníctvom svojej AT&T Global Network. Na prístup k tejto službe môžete použiť Sprievodcu telefonickým pripojením do AT&T Global Network, ktorý vám pomôže nakonfigurovať profil komutovaného telefonického spojenia PPP na prístup ku AT&T Global Network. Sprievodca vás prevedie cez osem panelov a celé to trvá asi desať minút. Sprievodcu môžete kedykoľvek zrušiť a žiadne existujúce údaje sa neuložia.

Toto pripojenie ku AT&T Global Network môžu používať dva typy aplikácií:
- **Mail Exchange**: Umožní vám pravidelne odoberať poštu z jedného konta AT&T Global Network a posielať ju na svoj iSeries server, ktorý ju distribuuje vaším užívateľom Lotus Mail alebo Simple Mail Transfer Protocol (SMTP).
- **Dial-up Networking**: pre AT&T Global Network použite iné aplikácie telefonického prístupu na sieť, napríklad štandardný prístup na internet.

Profily pripojenia ku AT&T Global Network spravujete rovnako, ako iné profily spojení PPP.

Na to, aby ste mohli použiť Sprievodcu telefonickým pripojením do AT&T Global Network, potrebujete jeden z uvedených adaptérov:
- 2699: Dvojlinkový WAN IOA
- 2720: PCI WAN/Twinaxiálny IOA
- 2721: PCI dvojlinkový WAN IOA
- 2745: PCI dvojlinkový WAN IOA (nahrádza IOA 2721)
- 2761: Osemportový analógový modem IOA
- 2771: Dvojportový WAN IOA s integrovaným modemom V.90 na porte 1 a štandardným komunikačným rozhraním na porte 2. Na použitie portu 2 adaptéra 2771 sa vyžaduje externý modem alebo terminálový adaptér ISDN s príslušným káblom.
- 2772: Dvojportový integrovaný modem V.90 WAN IOA
- 2793 Dvojportový WAN IOA s integrovaným modemom V.92 na porte 1 a štandardným komunikačným rozhraním na porte 2. To nahradí model 2771.
- 2805 Štvorportový WAN IOA s integrovaným modemom V.92. To nahradí modely 2761 a 2772.

Skôr ako spustíte Sprievodcu telefonickým pripojením do AT&T Global Network, musíte získať tieto informácie o svojom prostredí:
- Informácie o konte v AT&T Global Network (číslo konta, ID používateľa a heslo) pre aplikáciu elektronickej pošty alebo telefonického pripojenia k sieti.
- IP adresy poštového servera a názvového servera domény pre aplikáciu výmeny pošty.
- Názov modemu, ktorý sa použije pre spojenia jednou linkou.

Ak chcete spustiť Sprievodcu telefonickým pripojením do AT&T Global Network, postupujte podľa týchto krokov:
1. V produkte iSeries Navigator rozviňte svoj server a pristúpte na **Sieť –> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Profil pôvodcu spojenia** a vyberte **Nové telefonické pripojenie do AT&T Global Network**.
3. Keď sa spustí Sprievodca telefonickým pripojením do AT&T Global Network, kliknite na **Pomoc**, kde nájdete informácie o vyplnení panelu.

Sprievodcovia pripojením

Sprievodca novým telefonickým pripojením

Tento sprievodca vás prevedie krokmi na konfiguráciu profilu telefonického pripojenia k vášmu poskytovateľovi služieb internetu (ISP) alebo priamo na internet. Kvôli ukončeniu sprievodcu budete možno musieť poznať niektoré informácie od svojho sieťového administrátora alebo od poskytovateľa internetových služieb (ISP). Viac informácií o vyplnení tohto sprievodcu nájdete v online pomoci.

Sprievodca univerzálnym pripojením

Tento sprievodca vás prevedie krokmi na konfiguráciu profilu, ktorý môže používať softvér elektronickej podpory zákazníkov na pripojenie k IBM. Elektronická podpora zabezpečuje monitorovanie vášho jedinečného prostredia iSeries servera, aby vám mohli byť poskytnuté konkrétne odporúčania pre opravu vášho konkrétneho systému a situácií. Viac informácií o vyplnení tohto sprievodcu nájdete v online pomoci.

Konfigurácia skupinovej politiky prístupu

Zložka **Skupinové politiky prístupu** pod **Profilmi spojenia príjemcu** poskytuje možnosti na konfiguráciu parametrov spojenia point-to-point, ktoré sa týkajú skupiny vzdialených používateľov. Týka sa len tých spojení point-to-point, ktoré iniciuje vzdialený systém a prijíma lokálny systém.

Ak chcete nakonfigurovať novú skupinovú politiku prístupu:

1. V Operations Navigator vyberte svoj server a rozviňte **Sieť –> Služby vzdialeného prístupu –> Profily pôvodcu spojenia**.
2. Pravým tlačidlom myši kliknite na **Skupinové politiky prístupu** a vyberte **Nová skupinová politika prístupu**.
3. Na paneli **Všeobecné** zadajte názov a popis novej skupinovej politiky prístupu.
4. Kliknite na záložku **Viaclinkové** a nastavte viaclinkovú konfiguráciu.

   Viaclinková konfigurácia určuje, že chcete mať viac fyzických liniek spojených do jedného zväzku. Maximálny počet liniek v jednom zväzku môže byť od 1 do 16. Keďže pred uskutočnením spojenia nepoznáte typ nastavenia linky, je štandardná hodnota zvyčajne 1. Na zvýšenie, alebo limitovanie možností viaclinkového protokolu pre konkrétneho užívateľa sa môže použiť skupinová politika.

   - **Maximálny počet liniek vo zväzku** stanovuje maximálny počet spojení (alebo liniek), z ktorých chcete vytvoriť jednu logickú linku. Keď je táto skupinová politika použitá na reláciu profilu PPP, nemôže byť maximálny počet liniek vyšší, než počet voľných liniek.
   - Skontrolujte voľbu **Vyžadovať protokol na vyhradenie šírky pásma**, ak chcete zadefinovať, že spojenie sa nadviaže len vtedy, ak vzdialený systém podporuje Bandwidth Allocation Protocol (BACP). Ak nemôže byť použitý BACP, je povolená len samostatná linka.
5. Kliknite na panel **Nastavenia TCP/IP**, na ktorom sa nachádzajú tieto voľby:
   - Umožniť vzdialenému systému prístup do iných sietí (postupovanie IP)

     Táto voľba určuje, či chcete definovať postupovanie IP. Jej výberom v podstate umožníte, aby iSeries server vystupoval pri tomto spojení ako smerovač. Tým umožníte IP (Internet Protocol) datagramom, ktoré nie sú určené pre tento iSeries server, aby prešli cez systém do pripojenej siete. Ak túto voľbu necháte prázdnu, Internet Protocol (IP) vymaže všetky datagramy zo vzdialeného systému, ktoré nie sú určené pre žiadnu adresu, ktorá je pre tento iSeries server lokálnou.

     Možno z bezpečnostných dôvodov nechcete umožniť postupovanie IP. Poskytovateľ služieb internetu (ISP) však takmer vždy poskytuje postupovanie IP. Všimnite si, že táto voľba je platná len vtedy, ak umožníte postupovanie datagramov IP pre celý systém, v opačnom prípade bude táto voľba ignorovaná, a to aj vtedy, ak ste ju začiarkli. Postupovanie datagramov IP pre celý systém možno zobraziť z panelu Nastavenia na strane Vlastnosti TCP/IP.
   - Vyžadovať komprimáciu záhlavia TCP/IP (VJ)

Táto voľba určí, či bude Internet Protocol (IP) komprimovať informáciu záhlavia potom, ako nadviaže spojenie. Komprimácia obyčajne zvyšuje výkon, najmä pri interaktívnej prevádzke či pomalých sériových linkách. Komprimácia záhlavia sa vykonáva podľa Van Jacobsonovej (VJ) metódy, ktorá je definovaná v RFC 1332. Pri PPP sa komprimácia stanovuje pri nadviazaní spojenia. Ak druhý koniec spojenia nepodporuje VJ komprimáciu, iSeries server nadviaže spojenie, ktoré ju nepoužíva.

- Použiť pravidlá pre IP pakety pri tomto spojení

  Táto voľba určuje, či chcete pre danú skupinovú politiku aplikovať pravidlo filtrovania. Pravidlá filtrovania vám umožnia riadiť prevádzku IP na svojej sieti. Tento komponent pre filtrovanie IP paketov môžete použiť na ochranu svojho systému. Daný komponent ochraňuje váš systém, keďže filtruje pakety podľa vami zadaných pravidiel. Tie sa odvíjajú od informácií v záhlaví paketu.

  Viac informácií o pravidlách pre pakety IP nájdete v téme Filtrovanie paketov IP a NAT v Information Center.

Ako príklad si pozrite Riadenie prístupu užívateľov k prostriedkom s použitím Skupinových politík prístupu a Filtrovania IP.

Aplikovanie skupinovej politiky pre používateľa vzdialeného prístupu:

Skupinovú politiku môžete použiť pre používateľa vzdialeného prístupu, keď vyplníte Vlastnosti spojenia point-to-point pre nový **Profil príjemcu spojenia**.

Ak chcete použiť skupinovú politiku pre používateľa vzdialeného prístupu:

1. Kliknite na stranu **Autentifikácia**.
2. Skontrolujte **Na overenie identity vzdialeného systému požaduj tento server iSeries**.
3. Vyberte **Autentifikovať lokálne pomocou validizačného zoznamu**.
4. Ak už je validizačný zoznam vytvorený, vyberiete ho zo sťahovacieho zoznamu a kliknite na **Otvoriť**. Ak ho vytvárate po prvýkrát, zadajte názov nového validizačného zoznamu a kliknite na **Nový**.
5. Kliknutím na **Pridať** pridáte nového používateľa do validizačného zoznamu.
6. V dialógovom okne Pridať používateľa vykonajte tieto kroky:
   - Vyberte autentifikačný protokol, pre ktorý je definované dané meno používateľa.
   - Zadajte meno používateľa a heslo.

     Poznámka: Z bezpečnostných dôvodov sa odporúča, aby ste nepoužili pre používateľa rovnaké heslo ako to, ktoré je definované v Challenge Handshake Authentication Protocol22314 (CHAP), Extensible Authentication Protocol (EAP) a Password Authentication Protocol (PAP).
   - Začiarknite **Aplikovať skupinovú politiku pre používateľa**, vyberte skupinovú politiku zo sťahovacieho zoznamu a kliknite na **Otvoriť**.

     Vlastnosti skupinovej politiky môžete meniť alebo môžete pracovať s existujúcim nastavením. Kliknutím na **OK** dokončíte konfiguráciu a vrátite sa na stranu Vlastnosti spojenia point-to-point.

Použitie pravidiel filtrovania IP paketov na pripojenie PPP

Téma Filtrovanie IP paketov a pravidlá NAT v Informačnom centre rozoberá, ako vytvoriť pravidlá IP paketov, na ktoré sa môžete odvolať z profilu pripojenia PPP. Súbor pravidiel paketov môžete použiť na obmedzenie prístupu užívateľov a skupín k IP adresám vo vašej sieti. Príklad použitia súboru filtračných pravidiel na pripojenie PPP nájdete v časti Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom s použitím skupinových politík a filtrovania IP.

Na existujúce pravidlá filtrovania IP paketov sa môžete odkázať dvojako:

- Úroveň profilu spojenia

1. Keď vyplníte **Vlastnosti point-to-point** pre **Profil spojenia príjemcu**, vyberte stranu Nastavenia TCP/IP a kliknite na **Rozšírené**.
2. Kliknite na **Použiť pravidlá pre IP pakety pri tomto spojení** a zo sťahovacieho zoznamu vyberte identifikátor filtra PPP.
3. Kliknutím na **OK** aplikujete filter PPP na profil spojenia.

- Úroveň používateľa
  1. Otvorte existujúcu skupinovú politiku prístupu, alebo vytvorte novú skupinovú politiku prístupu.
  2. Kliknite na stranu Nastavenia TCP/IP.
  3. Kliknite na **Použiť pravidlá pre IP pakety pri tomto spojení** a zo sťahovacieho zoznamu vyberte identifikátor filtra PPP.
  4. Kliknutím na **OK** sa aplikuje filter PPP.

Povolenie služieb RADIUS a DHCP pre profily pripojenia

Ak chcete aktivovať služby RADIUS a DHCP pre profily príjemcu spojení:

1. V Operations Navigator vyberte svoj server a rozviňte **Sieť —> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Služby vzdialeného prístupu** a vyberte **Služby**.
3. Kliknite na záložku **DHCP-WAN**. Tým automaticky povolíte DHCP a určíte, ktorý server DHCP a prenesení agenti (ak nejakí sú) sú v systéme spustené.
4. Služby RADIUS povolíte kliknutím na záložku **RADIUS**.
   a. Označte **Povoliť pripojenie Servera sieťového prístupu RADIUS**
   b. Označte **Povoliť RADIUS pre autentifikáciu**.
   c. V závislosti od riešenia RADIUS sa tiež môžete rozhodnúť povoliť RADIUS prideľovanie kont a konfiguráciu adries TCP/IP.
5. Kliknite na tlačidlo **Nastavenia RADIUS NAS** a nakonfigurujte pripojenie k serveru RADIUS.
6. Kliknutím na OK sa vrátite do produktu iSeries Navigator.

Príklad konfigurácie servera RADIUS nájdete v scenári Autentifikácia volajúcich užívateľov na serveri RADIUS.

Kapitola 7. Spravovanie PPP

Na iSeries serveri môžete vykonať tieto úlohy riadenia PPP:

- Nastavenie vlastností profilov pripojenia
- Monitorovanie aktivity PPP

Nastavenie vlastností profilov pripojenia PPP

Pri vytváraní profilu spojenia si väčšinou v dialógovom okne Nastavenie profilu spojenia point-to-point vyberáte protokol, typ spojenia a režim prevádzky pre nový typ spojenia. Po zadaní vašich volieb v tomto okne sa zobrazí stránka s vlastnosťami profilu spojenia. Voľby, ktoré zadáte v dialógovom okne Nastavenie profilu spojenia point-to-point určujú obsah stránky vlastností profilu spojenia a zoradenie panelov na nej. Stránka vlastností je iná pre profily pôvodcu a iná pre profily príjemcu spojenia.

Tieto návody môžete použiť pri vypĺňaní každej strany v dialógovom okne **Vlastností nového profilu point-to-point**. Nastavenia, ktoré vyberiete na každej strane, závisia od vášho prostredia a typu spojenia, ktoré konfigurujete. Online pomoc produktu iSeries Navigator opisuje každú z možností, ktoré sa objavia v dialógovom okne. Viac informácií nájdete aj v príkladoch a postupoch pre PPP.

Monitorovanie aktivity PPP

Táto strana vysvetľuje, ako si môžete pozrieť profil spojenia a protokol relácie pomocou Operations Navigator.

Informácie o úlohách spojenia PPP:

- Existujú dve kontrolné úlohy PPP, ktoré sa používajú na riadenie individuálnych úloh spojení PPP. Tieto úlohy sa vykonávajú v podsystéme QSYSWRK:
  - QTPPPCTL - hlavná kontrolná úloha PPP. Táto úloha riadi každú úlohu spojenia PPP.
  - QTPPPL2TP - L2TP server. Táto úloha spravuje založenie tunela L2TP a spúšťa sa, len ak je práve spustený profil L2TP.
- Úlohy spojenia PPP sa vykonávajú pod užívateľským profilom QTCP a používajú sa na spracovanie každého jednotlivého spojenia PPP. Tieto úlohy sa štandardne vykonávajú v podsystéme QUSRWRK, možno ich však nakonfigurovať tak, aby sa spúšťali v iných podsystémoch. Používajú sa dva názvy úloh spojenia PPP:
  - QTPPPSSN - táto úloha sa používa na spracovanie všetkých spojení PPP okrem spojení typu L2TP.
  - QTPPPL2SSN - táto úloha sa používa na spracovanie virtuálnych údajov PPP potom, ako QTPPPL2TP úspešne dohodne vytvorenie tunela L2TP.
- Spojovacie úlohy SLIP sa vykonávajú v podsystéme QSYSWRK pod užívateľským menom QTCP. Rozoznávame dva typy názvov úloh SLIP:
  - QTPPDIAL*nn* sú úlohy dial-out, kde *nn* je ľubovoľné číslo od 1 do 99.
  - QTPPANS*nn* sú úlohy dial-in, kde *nn* je ľubovoľné číslo od 1 do 99.

Práca s profilmi spojení:

1. V produkte iSeries Navigator rozviňte svoj server a pristúpte na **Sieť –> Služby vzdialeného prístupu**.Vyberte **Profil spojenia pôvodcu** alebo **Profil spojenia príjemcu**.
2. V stĺpci Profil kliknite pravým tlačidlom myši na názov profilu spojenia a vyberte jednu z nasledujúcich volieb:
   - **Úlohy** - otvorí protokol úloh pre úloh QTPP*xxx*.

- **Spojenia** - otvorí dialógové okno, zobrazujúce informácie o všetkých spojeniach priradených danému profilu. Môže ísť o údaje o aktuálnom spojení, predchádzajúcich spojeniach alebo o aktuálnych aj predchádzajúcich spojeniach. Pri každom spojení je dostupná voľba na prezretie výstupu úlohy alebo podrobností o spojení.
- **Vlastnosti** - otvorí strany Vlastností na zobrazenie aktuálnych vlastností pre spojenie.

Prezeranie informácií o spojení:

1. V produkte iSeries Navigator rozviňte svoj server a pristúpte na **Sieť –> Služby vzdialeného prístupu**.Vyberte **Profil spojenia pôvodcu** alebo **Profil spojenia príjemcu**.
2. V stĺpci Profil kliknite pravým tlačidlom na názov profilu spojenia, ktorý nemá stav Neaktívny a vyberte **Spojenia**, aby ste si mohli prezrieť informácie o spojení.

   Zobrazí sa každé spojenie pre tento profil (aktuálne aj predchádzajúce). Stavové pole označuje aktuálny stav spojenia. V závislosti od stavu každej úlohy PPP možno zobraziť aj dodatočné informácie, napríklad ID používateľa pripojeného používateľa, lokálnu a vzdialenú IP adresu a názov úlohy PPP.
3. Ak si chcete prezerať výstup úlohy alebo podrobnosti o spojení, pravým tlačidlom myši kliknite na spojenie a tlačidlá budú aktivované.
4. Ak si chcete prezrieť výstup úlohy, kliknite na **Úlohy**. V protokole úloh kliknite pravým tlačidlom myši na názov úlohy a vyberte **Výstup tlačiarne**. Potom možno zobraziť obsah protokolov relácie spojenia a protokolov úloh (pri ukončených reláciách).
5. Ak si chcete prezrieť podrobnosti o spojení, kliknite na **Podrobnosti**. Možno zobraziť len podrobnosti o aktuálne aktívnych spojeniach. Dialógové okno Podrobnosti vám umožní prezerať si dodatočné informácie o spojení pre konkrétne spojenie.

Práca s výstupom PPP z iSeries servera:

Ak chcete pracovať s výstupom PPP, napíšte do príkazového riadka iSeries servera WRKTCPPTP:

- Ak chcete pracovať so VŠETKÝMI aktívnymi úlohami PPP (vrátane úloh QTPPPCTL a QTPPPL2TP), stlačte **F14** (Práca s aktívnymi úlohami).
- Ak chcete pracovať s celým výstupom pre konkrétny profil spojenia, vyberte pri tomto profile **voľbu 8** (Práca s výstupom).
- Ak chcete tlačiť konfiguráciu profilu PPP, vyberte pri tomto profile **voľbu 6** (Tlač). Použitím príkazu WRKSPLF sa dostanete k tlačovému výstupu.

Stav spojenia:

Stav profilu pripojenia je pre každý profil zobrazený v poli **Stav** v zozname profilov pripojenia pod **Sieť > Služby vzdialeného prístupu** po označení profilu pôvodcu, alebo príjemcu. Stav individuálneho spojenia zobrazíte pomocou dialógového okna Spojenia.

Primárny opis stavu	Vysvetlenie
Čaká sa na požiadavky na spojenie	Profil príjemcu je pripravený na spojenie
Čaká sa na prichádzajúce volanie	Server je pripravený na spojenie
Spája sa	Prebieha proces spájania so vzdialeným systémom
Aktívne/Aktívne spojenia	Spojenie sa uskutočnilo a úloha sa úspešne vykonáva
Neaktívne	Pre tento profil spojenia momentálne nebežia žiadne úlohy
Ukončený	Sú k dispozícii informácie
Viacskokový terminátor spúšťa viacskokový iniciátor	Prebieha viacskokové pripojenie
Aktívne viacskokové pripojenie	Úspešne ukončené viacskokové pripojenie

Sekundárny opis stavu	Vysvetlenie

Inicializácia modemu	inicializácia modemu na začiatku vytáčaného pripojenia
Čakanie na pripojenie modemu	server PPP je v stave načúvania
VYTÁČANIE xxx-xxxx	číslo vytáčané volajúcim klientom
Zistené prichádzajúce volanie	server PPP zistil prichádzajúce modemové volanie
Modem pripojený	úspešne ukončené PPP nadviazanie sojenia
V prevádzke	pripojenie PPP je aktívne
Linka ukončená	Spojenie ukončené rovnocenným počítačom
Zastavené	profil, alebo úloha je skončená
Zlyhanie autentifikácie	pre zlyhanie autentifikácie nebolo vytvorené pripojenie PPP
Uplynul čas vyhradený na pripojenie	pre dlhú neaktivitu nebolo vytvorené pripojenie PPP
Získavanie IP adresy	pre problémy pri získavaní IP adresy bolo ukončené pripojenie PPP
Vzdialený modem neodpovedal	pripojenie PPP nebolo vytvorené, pretože druhá strana neodpovedala
Zamietnutie protokolu	pre problémy pri dohadovaní NCP zlyhalo vytvorenie pripojenia PPP
Zlyhanie nových pokusov	pripojenie PPP nebolo vytvorené, pretože bol presiahnutý povolený počet opakovaní
Prijaté potvrdenie relácie PPPoE od rovnocenného počítača	Dohadovanie PPPoE je úspešne ukončené
Vytvorené volanie L2TP	Správa o vytváraní tunelu L2TP

Kapitola 8. Odstraňovanie problémov s PPP

Aktuálne a platné informácie o dočasných opravách programu (PTF) a o odstraňovaní problémov sú zdokumentované na stránke TCP/IP servera iSeries . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a aktualizujú informácie, uvedené v tejto téme.

Ak sa vyskytnú problémy so spojením PPP, môžete pomocou tohto kontrolného zoznamu získať informácie o chybe. Tento kontrolný zoznam vám pomôže identifikovať príznaky chyby a vyriešiť problémy so spojením PPP.

1. Požadovaný podporný materiál:
   - Typ vzdialeného hostiteľa, operačný systém a úroveň
   - Úroveň hostiteľského operačného systému iSeries servera
   - Protokol úloh neúspešnej relácie a protokol telefonického spojenia
     Vo verzii V5R1 sa protokoly úloh a telefonického spojenia ukladajú v OUTQ pod názvom profilu.
   - Skript spojenia, ak sa používa vo vašom prostredí
   - Stav profilu spojenia pred a po zlyhaní spojenia
2. Odporúčaný podporný materiál:
   - Popis linky
   - Profil spojenia
     Voľba 6 z WRKTCPPTP vytlačí nastavenia profilu.
   - Typ modemu a model
   - Príkazové reťazce modemu
   - Sledovanie komunikácií

The ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) široko pokrýva nasledujúce problémy s PPP. Poskytuje aj podrobné informácie o riešení problémov.

Problém	Riešenie
Hardvérová konfigurácia modemu Nesprávna konfigurácia prepínačov a iných hardvérových nastavení	Skontrolujte, či je modem nakonfigurovaný na správny typ rámcovania. Môže byť buď *asynchrónny* alebo *synchrónny*. Viac informácií nájdete v príručke k modemu.
Modemové príkazy AT Modem, ktorý sa pokúšate použiť, sa nenachádza v preddefinovanom zozname modemov v Operations Navigator.	Vytvorte nový modem.
Používatelia a heslá PPP Keď sa pokúšate nadviazať spojenie PPP, objavia sa chyby súvisiace s menom a heslom používateľa.	• Prekontrolujte, či ste ID používateľa a heslo zadali správne (malé a veľké písmená). • Skontrolujte, či oba komunikujúce systémy používajú rovnaký autentifikačný protokol. • Ak je jedna strana nakonfigurovaná ako CHAP, na druhej strane nepoužívajte PAP.
Linky PPP pre spustenie profilu spojenia Identifikované linky PPP používajú rovnaký hardvérový prostriedok.	Nezabudnite vypnúť ostatné linky, používajúce ten istý hardvérový prostriedok.

Problém	Riešenie
Protokol PPP Chyby pri spojení sa môžu vyskytnúť aj z dôvodu nesprávnej konfigurácie protokolu PPP.	V niektorých situáciách, keď komunikujúce systémy nemôžu navzájom komunikovať kvôli chybnej konfigurácii, je potrebné preskúmanie nižších úrovní protokolu PPP. Ak protokol PPP alebo protokol úlohy PPP nezobrazuje žiadnu indikáciu problému, môžete ho preskúmať pomocou funkcie sledovania priebehu komunikácie.

Kapitola 9. Ďalšie informácie o PPP

Iné zdroje informácií o PPP:

- Kliknutím na linku PPP na úvodnej stránke TCP/IP servera iSeries nájdite najnovšie dočasné programové opravy (PTF) a najnovšie informácie o konfigurácii PPP a L2TP  . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a nahrádzajú informácie uvedené v téme **Služby vzdialeného prístupu: Spojenia PPP**.
- The ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  široko pokrýva služby a aplikácie TCP/IP.

IBM Confidential
Vytlačené v USA