IBM

eserver

iSeries

Služby vzdialeného prístupu: Pripojenia PPP

Verzia 5, vydanie 3

IBM

@server

iSeries

Služby vzdialeného prístupu: Pripojenia PPP

Verzia 5, vydanie 3

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si určite prečítajte informácie v časti “Poznámky”, na strane 53.

Šieste vydanie (August 2005)

Toto vydanie platí pre verziu 5, vydanie 3, modifikáciu 0 operačného systému IBM Operating System/400, 5722-SS1 a pre všetky nasledujúce vydania a modifikácie, pokiaľ sa v nových vydaniach neuvádza inak. Táto verzia nebeží na všetkých modeloch RISC (Reduced Instruction Set Computer) a nebeží ani na modeloch CISC.

Obsah

Služby vzdialeného prístupu: Pripojenia PPP

Protokol point-to-point (PPP) je internetová 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. Server iSeries obsahuje podporu PPP TCP/IP ako časť pripojiteľnosti WAN (Wide-Area Network).

Použitím PPP na pripojenie vzdialeného servera iSeries môžete vymieňať údaje medzi lokalitami. Prostredníctvom PPP môžu vzdialené systémy pripojené k vášmu serveru iSeries pristupovať na prostriedky alebo iné počítače, ktoré patria do rovnakej siete ako váš server. Server iSeries môžete tiež nakonfigurovať tak, aby sa pripájal k Internetu použitím PPP. Sprievodca iSeries Navigator Dial-Up Connection Wizard vás povedie procesom pripájania vášho servera iSeries k Internetu alebo k internej sieti.

- Novinky vo V5R3 opisuje aktualizácie Služieb vzdialeného prístupu pre toto vydanie.
- Tlač tejto témy vám umožňuje prevziať alebo vytlačiť verziu PDF týchto informácií.

Vysvetlenie Služieb vzdialeného prístupu: Pripojenia PPP

Tieto témy vás rýchlo uvedú do služieb vzdialeného prístupu, ktoré máte na vašom serveri iSeries. Uvedené témy vám pomôžu naplánovať prostredie PPP pre vašu sieť.

- **Scenáre PPP** sú príklady realizácií rôznych implementácií konektivity PPP. Každý príklad poskytuje pokyny a vzorové hodnoty pre konfiguráciu pripojenia PPP.
- **PPP concepts** poskytuje informácie o konceptoch PPP a požiadavkách servera iSeries na pripojenia PPP.
- **Plan PPP** poskytuje informácie o konceptoch PPP a požiadavkách servera iSeries na pripojenia PPP.

Používanie služieb vzdialeného prístupu: Pripojenia PPP

Tieto témy vám môžu pomôcť pri konfigurácii a riadení pripojení PPP na vašom serveri iSeries.

- **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 stránka obsahuje odkazy na užitočné a súvisiace informácie týkajúce sa servera iSeries.

Novinky vo V5R3

Tento článok opisuje nové funkcie pridané pre verziu 5, vydanie 3.

Nové funkcie

- Grafické užívateľské rozhranie (GUI) Nový profil vám umožňuje nakonfigurovať profily point-to-point, PPPoE a L2TP tak, aby sa spúšťali automaticky pri každom spustení TCP/IP.
- Podpora odchádzajúcich volaní L2TP umožňuje viacerým systémom alebo oddielom zdieľať jeden modem. Ako príklad si pozrite scenár dole.
- Na prístup k IBM vám Sprievodca univerzálnym pripojením umožňuje použiť pripojiteľnosť z iného systému alebo oddielu. Viac informácií nájdete v téme Univerzálne pripojenie: Konfigurácia univerzálneho pripojenia.
- Zrušila sa podpora integrovaných adaptérov ISDN (2750/2751). Namiesto toho môžete použiť terminálové adaptéry ISDN.
- Zrušila sa podpora 2761.

Nové informácie

- Nový scenár: Zdieľanie modemu medzi logickými oddielmi pomocou L2TP. Tento scenár ukazuje, že viac systémov alebo oddielov môže pre telefonické pripojenia zdieľať ten istý modem, takže každý systém alebo oddiel nemusí mať vlastný modem. To je možné realizovať použitím tunelov L2TP a nakonfigurovaním profilov L2TP, umožňujúcich odchádzajúce volania.

Ako zistiť, čo je nové alebo zmenené

Na identifikáciu vykonaných technických zmien tieto informácie používajú:

- Obrázok » na označenie, kde začínajú nové alebo zmenené informácie.
- Obrázok « na označenie, kde končia nové alebo zmenené informácie.

Ak chcete získať ďalšie informácie o tom, čo je v tomto vydaní nové alebo zmenené, pozrite si Poznámku pre užívateľov.

Tlač tejto témy

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

Ak chcete zobraziť alebo prevziať verziu PDF, vyberte Služby vzdialeného prístupu: Pripojenia PPP (510 KB).

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 tlačidlo **Uložiť**.

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 ku koncentrátoru prístupu PPPoE

Mnohí ISP ponúkajú prístup na Internet s vysokou rýchlosťou cez DSL s použitím PPPoE. Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

Scenár: Pripojenie vzdialených klientov, ktorí sa k vášmu serveru iSeries pripájajú telefonickým pripojením

Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo volajúci klienti môžu získať prístup k serveru iSeries pomocou PPP.

Scenár: Pripojenie vašej siete modemom na Internet

Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na Internet. Na pripojenie servera iSeries k poskytovateľovi internetových služieb (ISP) môžu použiť modem. PC klienti pripojení cez LAN môžu komunikovať s Internetom tak, že server iSeries použijú ako bránu.

Scenár: Prepojenie vašich vnútropodnikových a vzdialených sietí modemom

Modem umožňuje, aby si dve vzdialené lokality (napríklad centrála a pobočka) navzájom vymieňali údaje. PPP môže navzájom spojiť dve siete LAN vytvorením spojenia medzi serverom iSeries v centrále a iným serverom iSeries v pobočke.

Scenár: Autentifikácia telefonického pripojenia pomocou RADIUS NAS

NAS (Network Access Server), ktorý beží na serveri iSeries, môže smerovať požiadavky na autentifikáciu od volajúcich klientov na osobitný server RADIUS. Ak sa potvrdí ich pravosť, môže RADIUS skontrolovať aj adresu IP 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 adries IP.

Scenár: PPP a DHCP na jednom serveri iSeries

Volajúci klienti alebo vzdialení užívatelia môžu získať prístup k serveru iSeries v sieti spoločnosti pomocou PPP. Klient DHCP WAN (Wide Area Network) na rovnakom iSeries umožňuje vzdialeným užívateľom získať dynamicky priradenú IP adresu použitím rovnakých služieb ako užívateľom pripojeným cez LAN.

Scenár: Profil DHCP a PPP na rôznych 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: Zdieľanie modemu medzi logickými oddielmi pomocou PPP a L2TP

Medzi štyrmi virtuálnymi oddielmi máte nakonfigurovaný virtuálny Ethernet. Pomocou tohto scenára môžete povoliť zdieľanie modemu vybratými logickými oddielmi. Tieto logické oddiely budú používať zdieľaný modem na prístup k externej sieti LAN.

Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupu 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. Chceli by ste používať toto pripojenie PPPoE na poskytovanie pripojenia na Internet s vysokou šírkou pásma cez váš server iSeries.

Obrázok 1. Pripojenie vášho servera iSeries k poskytovateľovi internetových služieb (ISP) pomocou PPPoE

Riešenie: Môžete podporovať pripojenie k vášmu ISP pomocou PPPoE prostredníctvom vášho servera iSeries. Server iSeries využíva nový typ virtuálnej linky PPPoE, ktorá je pripojená k fyzickej ethernetovej linke, nakonfigurovanej na používanie ethernetového adaptéra typu 2838 alebo 2849. Táto virtuálna linka podporuje protokol relácie PPP cez Ethernet LAN pripojenú k modemu DSL, ktorý poskytuje bránu k vzdialenému ISP. Toto poskytuje užívateľom pripojeným cez LAN vysokorýchlostný prístup na Internet pomocou pripojenia serverov iSeries cez PPPoE. Po pripojení servera iSeries k poskytovateľovi internetových služieb (ISP) dostanú jednotliví užívatelia pripojení cez LAN prístup k ISP cez PPPoE použitím IP adresy, vyhradenej 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. Nakonfigurovanie profilu pôvodcu pripojenia na vašom serveri iSeries.

   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 opis profilu pôvodcu. Tento názov sa bude odvolávať na profil pripojenia, aj na virtuálnu linku PPPoE.
4. Kliknite na stranu **Pripojenie**. Vyberte **názov virtuálnej linky PPPoE**, ktorý sa zhoduje s názvom tohto profilu pripojenia. Po vybratí linky zobrazí aplikácia iSeries Navigator dialógové okno 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**. Aplikácia iSeries Navigator zobrazí dialógové okno vlastností ethernetovej linky. **Poznámka:** PPPoE vyžaduje ethernetový adaptér typu 2838 alebo 2849.

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.

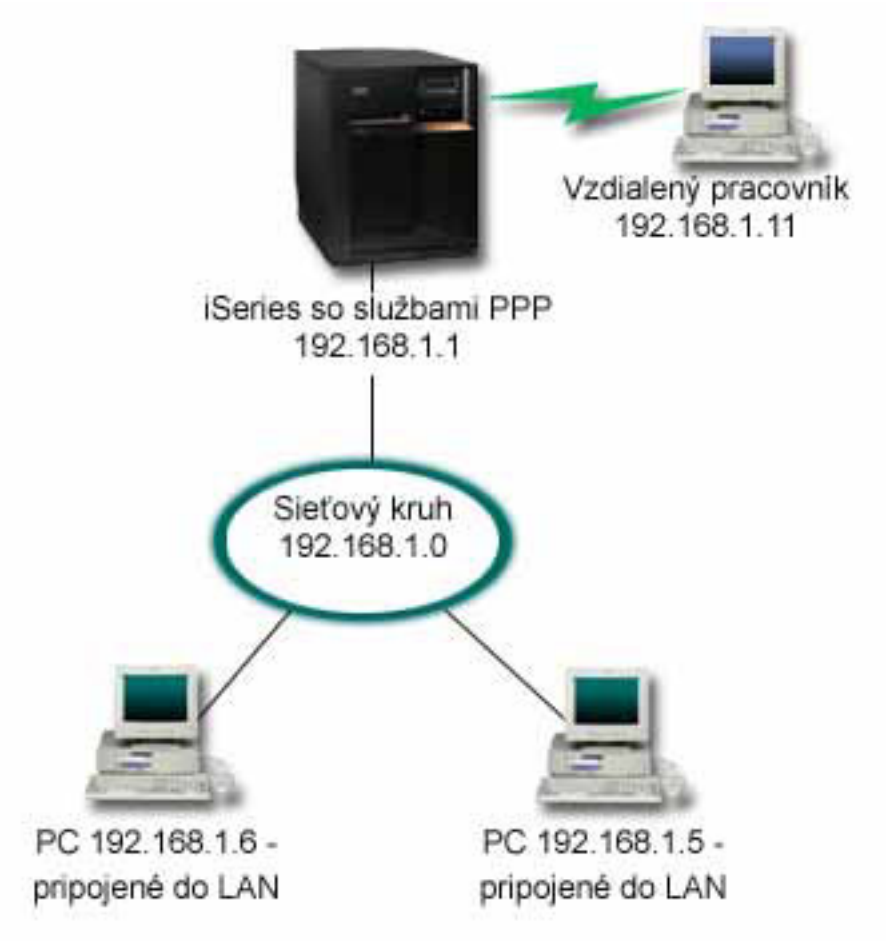
c. Po kliknutí na **Limity** nadefinujete vlastnosti overovania LCP, alebo sa kliknutím na **OK** vrátite na stranu Nový profil **pripojenia** Point-to-Point.
d. Keď sa vrátite na stránku **Pripojenie**, zadajte adresovanie servera PPPoE na základe informácií od vášho ISP.

5. Ak váš ISP vyžaduje, aby sa sever iSeries sám autentifikoval alebo ak chcete, aby iSeries autentifikoval vzdialený server, kliknite na stránku **Authentication**. Viac informácií nájdete v časti Autentifikácia systému.
6. Kliknite na stranu **Nastavenia TCP/IP** a zadajte pre tento profil pripojenia parametre spracovávanie adries IP. Potrebné nastavenie by mal poskytnúť váš ISP. Ak chcete užívateľom pripojeným cez LAN umožniť pripojenie k ISP použitím IP adries vyhradených pre server iSeries, vyberte **Hide addresses (Full masquerading)**.
7. Kliknite na stranu **DNS**, zadajte adresu IP servera DNS, ktorú vám oznámil ISP.
8. Ak chcete určiť podsystém, na ktorom má byť spustená úloha pripojenia, kliknite na stranu **Ďalšie**.
9. Kliknutím na **OK** dokončite profil.

Informácie o obmedzení prístupu užívateľov k externej IP adrese alebo k prostriedkom iSeries nájdete v časti IP filtering a v časti Group Access Policies.

Scenár: Pripojenie vzdialených klientov, ktorí sa k vášmu serveru iSeries pripájajú telefonickým pripojením

Situácia: Ako správca siete vo vašej spoločnosti musíte spravovať váš server iSeries aj sieťových klientov. Namiesto každodenného chodenia do práce, kde riešite problémy a opravujete chyby, by ste uvítali prácu zo vzdialenej lokality, napríklad z domu. Pretože vaša spoločnosť nie je pripojená k Internetu cez sieť, môžete sa telefonicky pripojiť na váš server iSeries použitím pripojenia 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 k vášmu serveru iSeries

Riešenie: Na pripojenie vášho domáceho PC k serveru iSeries pomocou svojho modemu môžete použiť PPP. Keďže na tento typ pripojenia PPP používate svoj modem ECS, musíte si overiť, či máte modem nakonfigurovaný na synchrónny aj asynchrónny režim. Na obrázku hore vidíte server iSeries so službami PPP, ktorý je pripojený k LAN pomocou dvoch PC. Vzdialený pracovník sa potom telefonicky pripojí k serveru iSeries, autentifikuje sa a stane sa súčasťou pracovnej siete (192.168.1.0). V tomto prípade je najjednoduchšie priradiť volajúcemu klientovi statickú adresu IP.

Vzdialený pracovník používa CHAP-MD5 na autentifikáciu so serverom iSeries. iSeries nemôže používať MS_CHAP, takže musíte skontrolovať, či je váš klient PPP nastavený na používanie CHAP-MD5.

Ak chcete, aby mali vaši vzdialení pracovníci prístup do firemnej siete tak, ako sa to uvádza vyššie, musí byť postupovanie IP nastavené v zásobníku TCP/IP aj vo vašom profile príjemcu 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 pakety IP.

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

Vzorová konfigurácia:

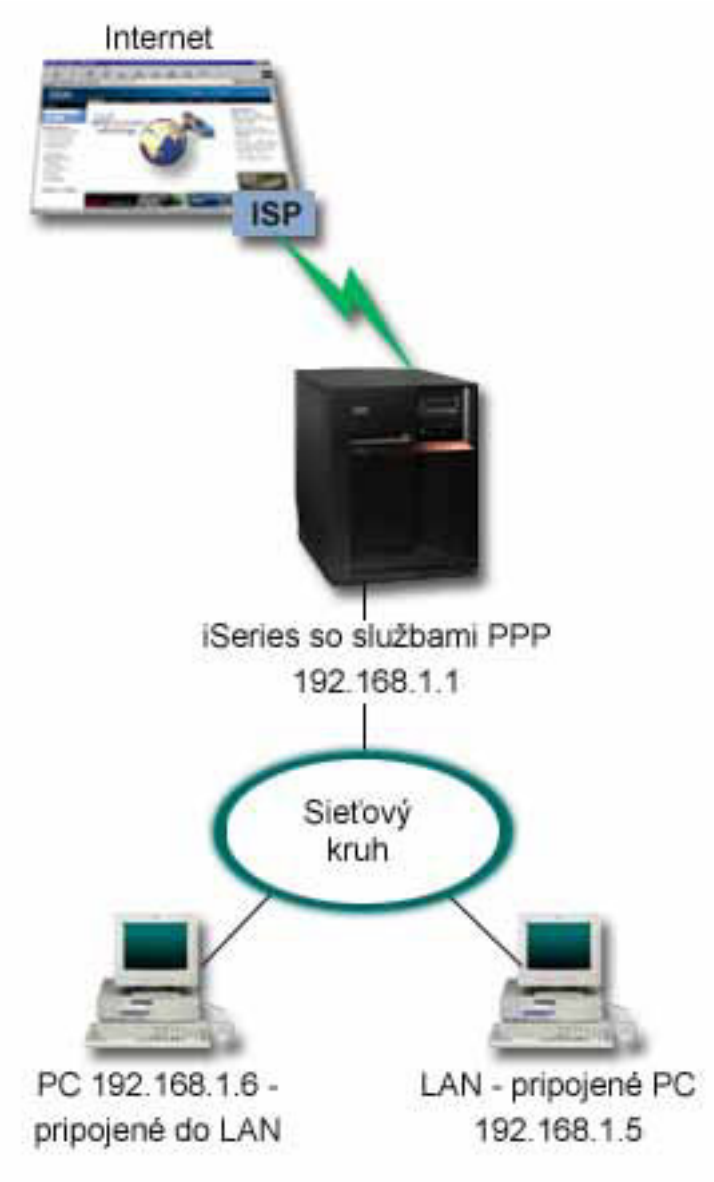
1. Nakonfigurujte Dial-up Networking a vytvorte telefonické pripojenie vo vzdialenom PC.
2. Nakonfigurovanie profilu príjemcu pripojenia na vašom serveri iSeries.
   Nezabudnite vybrať tieto informácie:

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

3. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a opis profilu príjemcu.
4. Kliknite na stranu **Pripojenie**. Vyberte príslušný **Názov linky** alebo vytvorte nový názov tak, že ho napíšete a kliknete na **Nový**.
   a. Na stránke **Všeobecné** zvýraznite existujúci hardvérový prostriedok, kde je pripojený váš adaptér 7852–400 a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na stranu **Modem**. Z výberového zoznamu Name vyberte modem **IBM 7852–400**.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
5. Kliknite na stranu **Autentifikácia**.
   a. Začiarknutím **Require this iSeries server skontrolujte identitu vzdialeného systému**.
   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 adresu IP na 192.168.1.1.
   b. Ako vzdialenú adresu vyberte **Pevná adresa IP** 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. Pretože táto aplikácia nevyžaduje výmenu veľkého množstva údajov, radi by ste na pripojenie servera iSeries aj PC klientov pripojených cez LAN k Internetu používali modem. V ďalšom opise sa uvádza príklad riešenia tejto situácie.



Obrázok 3. Pripojenie LAN na Internet pomocou modemu

Riešenie: Na pripojenie iSeries k vášmu poskytovateľovi internetových služieb (ISP) môžete použiť váš integrovaný (alebo iný kompatibilný) modem. V serveri musíte vytvoriť profil pôvodcu PPP, a tak vytvoriť pripojenie PPP k ISP.

Po vytvorení spojenia medzi iSeries a ISP môžu vaše PC pripojené cez LAN komunikovať s Internetom tak, že iSeries použijú ako bránu. V profile pôvodcu budete chcieť skontrolovať, že je zapnutá voľba Skryť adresy, takže klienti LAN so súkromnými adresami IP budú môcť komunikovať s Internetom.

Teraz, keď sú váš iSeries a sieť pripojené k Internetu, musíte vedieť aj o riziku ohrozenia bezpečnosti. Spolupracujte so svojím ISP, aby ste sa oboznámili jeho bezpečnostnou politikou a vykonajte ďalšie kroky pre zabezpečenie vášho servera a siete.

Šírka pásma závisí od toho, ako používate Internet. Viac sa o možnosti zvýšenia šírky pásma pripojenia naučíte v časti pre plánovanie.

Vzorová konfigurácia:

1. Nakonfigurovanie profilu pôvodcu pripojenia na vašom serveri iSeries.

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 liniek.

2. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a opis profilu pôvodcu.
3. Kliknite na stranu **Pripojenie**. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na stránke **Všeobecné** vo vlastnostiach novej linky zvýraznite existujúci hardvérový prostriedok. Ak vyberiete prostriedok interného modemu, automaticky sa vyberú nastavenia typu modemu a rámcovania.
   b. 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 k serveru ISP. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na stránku **Authentication** a vybratím **Allow the remote system overte identitu 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 adresy IP.
   b. Vyberte **Pridať vzdialený systém ako štandardnú trasu**.
   c. Začiarknite **Skryť adresy**, aby vaše interné adresy IP nepresmerovali na Internet.
7. Kliknite na stranu **DNS**, zadajte adresu IP servera DNS, ktorú vám oznámil ISP.
8. Kliknutím na **OK** dokončite profil.

Ak chcete profil pripojenia použiť na pripojenie k Internetu, v aplikácii iSeries Navigator kliknite pravým tlačidlom myši na profil pripojenia a vyberte **Start**. Pripojenie je úspešné, keď sa stav zmení na **Aktívny**. Aby ste zaktualizovali obrazovku, použite obnovenie.

Poznámka: Musíte tiež skontrolovať, či ostatné systémy vo vašej sieti majú zadefinované správne smerovanie, takže internetová TCP/IP premávka z týchto systémov sa bude posielať prostredníctvom servera iSeries.

Scenár: Prepojenie vašej vnútropodnikovej a vzdialenej siete modemom

Situácia: Predpokladajme, že máte pobočku a centrálu na dvoch rôznych miestach. Každý deň sa pobočka musí pripojiť k centrále, aby si vymenili informácie pre svoje aplikácie spracúvajúce údaje. Množstvo vymenených dát si ešte nevyžaduje kúpu fyzického sieťového pripojenia, preto ste sa rozhodli, že obe siete prepojíte pomocou modemov.

Obrázok 4. Prepojenie vašej vnútropodnikovej a vzdialenej siete modemom

Riešenie: PPP môže navzájom spojiť dve siete LAN vytvorením spojenia medzi jednotlivými servermi iSeries, ako vidíte na obrázku vyššie. V takom prípade predpokladajme, že vzdialená kancelária iniciuje pripojenie k ústrednej kancelárii. Na vzdialenom iSeries by ste mali nakonfigurovať profil pôvodcu a na serveri ústrednej kancelárie 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 adries IP (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. Nakonfigurovanie profilu pôvodcu pripojenia na serveri iSeries vzdialenej kancelárie.

   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 liniek.
2. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a opis profilu pôvodcu.
3. Kliknite na stranu **Pripojenie**. 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 **Add** a zadajte telefónne číslo, ktoré sa má vytočiť, aby ste sa dostali na server iSeries ústrednej kancelárie. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na stránku **Authentication** a vybratím **Allow the remote system overte 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 adresu IP vyberte z výberového okna **Použiť pevnú adresu IP** adresu IP rozhrania LAN vzdialenej pobočky (192.168.2.1).
   b. Pre vzdialenú adresu IP vyberte **Priradená vzdialeným systémom**.
   c. V časti pre smerovanie vyberte **Pridať vzdialený systém ako štandardnú trasu**.
   d. Kliknutím na **OK** dokončite profil pôvodcu.
7. Nakonfigurovanie **Profilu príjemcu pripojenia** na serveri iSeries ústrednej kancelárie.

   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 liniek.
8. Na strane **Všeobecné** z Vlastností nového profilu point-to-point zadajte názov a opis profilu príjemcu.
9. Kliknite na stranu **Pripojenie**. 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**.

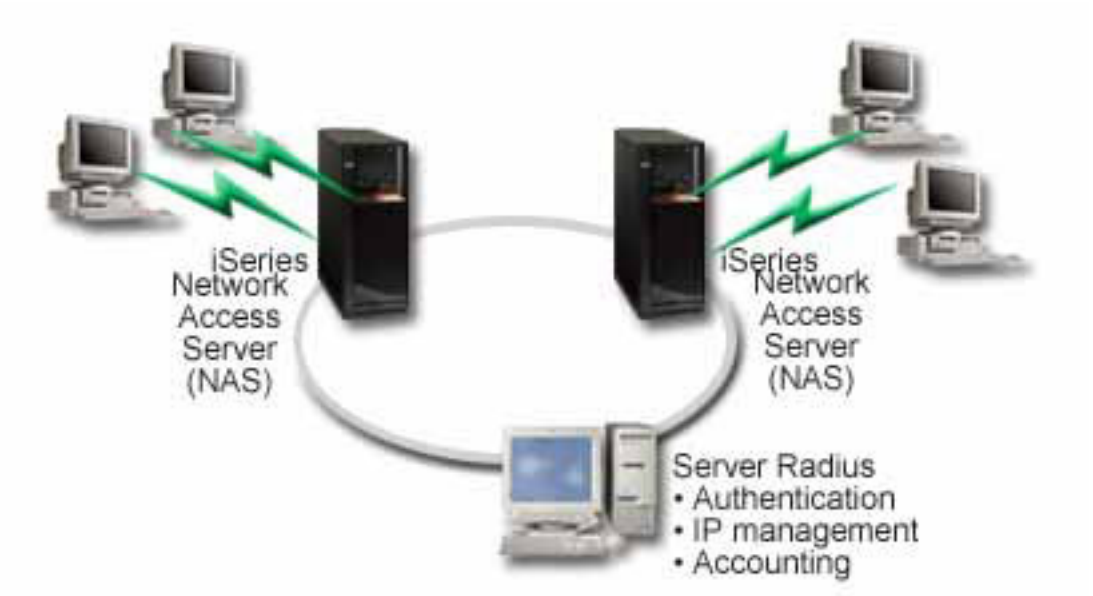
a. Začiarknutím **Require this iSeries server skontrolujte identitu vzdialeného systému**.
b. Pridajte nového vzdialeného používateľa do validizačného zoznamu.
c. Začiarknite autentifikáciu CHAP-MD5.

11. Kliknite na stranu **Nastavenia TCP/IP**.
    a. Pre lokálnu adresu IP vyberte z výberového okna adresu IP rozhrania centrály (192.168.1.1).
    b. Pre vzdialenú adresu IP vyberte **Založená na ID používateľa vzdialeného systému**. Objaví sa dialógové okno Adresy IP definované podľa mena používateľa. Kliknite na **Pridať**. Vyplňte polia Užívateľské meno volajúceho, Adresa IP a Maska podsiete. V našom prípade sa použijú tieto nastavenia:
       - Užívateľské meno volajúceho: vzdialená_strana
       - Adresa IP: 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. Vybratím **IP forwarding** povoľte ostatným systémom v sieti používať tento server iSeries ako bránu.
12. Kliknutím na **OK** dokončite profil príjemcu.

Scenár: Autentifikácia telefonického pripojenia pomocou RADIUS NAS

Situácia: Vaša vnútropodniková sieť má vzdialených užívateľov, ktorí sa telefonicky pripájajú na dva servery iSeries z distribuovanej telefonickej siete. Chceli by ste mať spôsob, ako centralizovať autentifikáciu, služby a účtovanie, čo umožní jednému serveru spracúvať požiadavky o validáciu identifikátorov a hesiel užívateľov a určiť, ktoré adresy IP sa im priraďujú.



Obrázok 5. Autentifikujte telefonické pripojenia serverom RADIUS

Riešenie: Pri pokuse užívateľov o pripojenie postúpi NAS (Network Access Server), ktorý beží na serveroch iSeries, autentifikačné informácie na server RADIUS v tejto 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 adresu IP rovnocenného počítača a aby mohol aktivovať spravovanie konta na sledovanie aktivity a použitie užívateľa. Ak chcete podporovať RADIUS, musíte zadefinovať server RADIUS NAS na serveri iSeries.

Vzorová konfigurácia:

1. V aplikácii iSeries Navigator rozviňte **Network** , pravým tlačidlom myši kliknite na **Remote Access Services** a vyberte **Services** .
2. Na 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 **Local IP address** zadajte IP adresu pre rozhranie iSeries používané na spojenie so serverom RADIUS.
   b. Do poľa **Adresa IP servera** zapíšte adresu IP servera RADIUS.
   c. Do poľa **Password** zadajte heslo, používané na identifikáciu servera iSeries pre server RADIUS.
   d. Do poľa **Port** zadajte port na serveri iSeries, používaný na komunikáciu so serverom RADIUS. Predvolené hodnoty sú port 1812 pre autentifikačný server alebo port 1813 pre účtovací server.
6. Kliknite na **OK**.
7. V aplikácii iSeries Navigator rozviňte **Network > Remote Access Services** .
8. Označte Profil pripojenia, ktorý bude server RADIUS pri autentifikácii využívať. Na služby RADIUS môžu byť aplikované len profily pripojenia príjemcu.
9. Na stránke Authentication vyberte **Require this iSeries server a overte identitu vzdialeného systému.**.
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** uložíte zmeny do profilu 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 užívatelia telefonicky pripájajú použitím tohto profilu pripojenia, iSeries postúpi autentifikačné informácie na špecifikovaný server RADIUS. Ak je užívateľ overený, bude pripojenie povolené a budú aplikované všetky obmedzenia pripojenia určené užívateľskými informáciami v 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 telefonický 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 pripojenia pre každého užívateľa by znásobilo vašu prácu a vytváranie sieťových obmedzení pre všetkých užívateľov tohto profilu pripojenia by vám neposkytlo dostatočnú kontrolu. Potrebovali by ste spôsob definovania nastavení pripojenia a povolení pre niekoľko rozličných skupín užívateľov, ktorí sa zvyčajne pripájajú na tento server.

Obrázok 6. Aplikácia nastavenia pripojenia na telefonické pripojenie založené na nastaveniach skupinovej politiky

Riešenie: Potrebujete použiť obmedzenia filtrovania jedinečných adries IP na dve rozličné skupiny užívateľov. Aby ste to dosiahli, vytvoríte skupinové politiky prístupu a pravidlá filtrovania adries IP. 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 pravidlá filtrovania povolia služby HTTP, FTP a Telnet, obmedzia však prístup k všetkej ďalšej prevádzke TCP/IP a službám prostredníctvom servera 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 Validačného 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 adresy IP 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 aplikácii iSeries Navigator rozviňte **Network > Remote Access Services** .
   b. Kliknite na **Profily pripojenia príjemcu** a vyberte Skupinové politiky prístupu.
   c. Pravým tlačidlom myši kliknite na preddefinovanú skupinu, zobrazenú v pravej časti okna a vyberte **Vlastnosti**.

      Poznámka: Ak chcete vytvoriť novú skupinovú politiku prístupu, pravým tlačidlom myši kliknite na Skupinové politiky prístupu a vyberte **Nové skupinové politiky prístupu**. Vyplňte záložku Všeobecné. Potom vyberte záložku Nastavenia TCP/IP a prejdite na **krok e** dole.
   d. Vyberte záložku **Nastavenia TCP/IP** kliknite na **Rozšírené**.
   e. 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.
   f. Otvorte menu **Vložiť** a pre vkladanie skupiny filtrov vyberte **Filtre**. Pomocou záložky **Všeobecné** definujte skupinu filtrov a na záložke **Služby** určite služby, ktoré povoľujete, ako napríklad HTTP. Nasledujúca skupina filtrov, ″services_rules″, povolí služby HTTP, FTP a Telnet. Filtrovacie pravidlá obsahujú implicitný príkaz predvoleného odmietnutia, čím sa obmedzia všetky služby TCP/IP alebo premávka IP, ktorá nie je špecificky povolená.

Poznámka: Adresy IP 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

###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 = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

g. 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

      ```
      permitted_services
      ```

      ako filtračný identifikátor PPP.

   2) Na 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 profilom pripojenia PPP,
      alebo skupinovou politikou prístupu.

      FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
      ```

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

   ```
   RMVTCPTBL *ALL
   ```

   Týmto zo servera odstránite všetky filtračné pravidlá a NAT.

i. 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 aplikácii iSeries Navigator rozviňte **Network > Remote Access Services > Receiver Connection Profiles**.
   b. Kliknite pravým tlačidlom myši na ikonu Skupinová politika prístupu a vyberte Nová skupinová politika prístupu. Aplikácia iSeries Navigator zobrazí dialógové okno definície 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 telefonické 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.

Scenár: Zdieľanie modemu medzi logickými oddielmi pomocou L2TP

Situácia

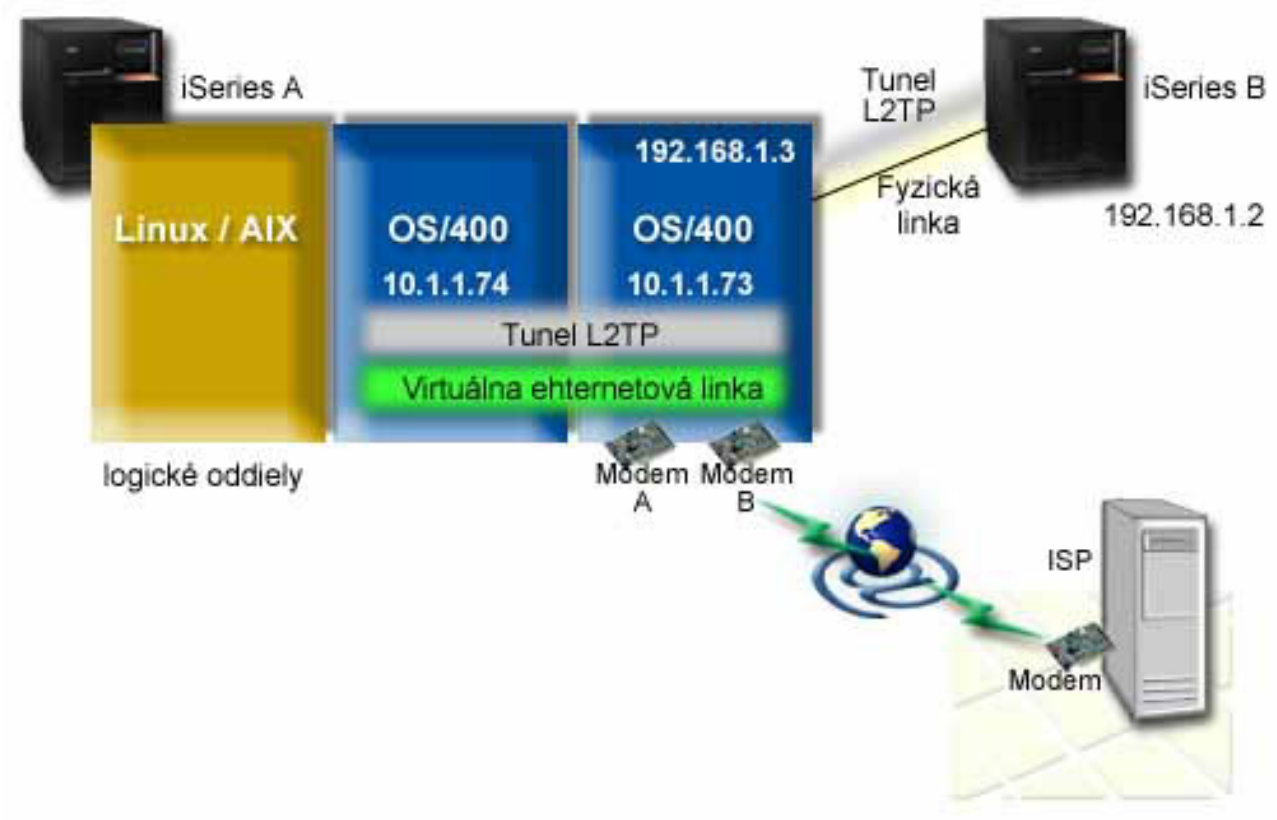
Ste administrátorom systému v stredne veľkej spoločnosti. Je čas na rozšírenie vášho počítačového vybavenia, ale radi by ste spravili viac než len to - chcete výrazne zmodernizovať váš hardvér. Začnete proces zjednotením práce troch starých serverov do jedného nového servera iSeries. V serveri iSeries vytvoríte tri logické oddiely. Nový server iSeries bol dodaný s interným modemom 2793. Máte len tento jeden vstupno/výstupný procesor (IOP) s podporu PPP. Máte tiež starý modem pre elektronickú podporu zákazníkov 7852–400.

Riešenie

Viac systémov alebo oddielov môže pre telefonické pripojenia zdieľať ten istý modem, takže každý systém alebo oddiel nemusí mať vlastný modem. To je možné realizovať použitím tunelov L2TP a nakonfigurovaním profilov L2TP, umožňujúcich odchádzajúce volania. Vo vašej sieti budú vytvorené tunely vo virtuálnej sieti Ethernet a vo fyzickej sieti. Fyzická linka pripája ďalší server vo vašej sieti, ktorý bude tiež zdieľať modem.

Detaily

Tento obrázok zobrazuje charakteristiky siete pre tento scenár:



Požiadavky a predpoklady

Požiadavky pre nastavenie pre iSeries-A zahŕňajú:

- Systém OS/400 verzia 5, vydanie 3 alebo novší, nainštalovaný v oddiele, ktorý vlastní modemy so schopnosťami ASYNC.
- Hardvér podporujúci oddiely.
- iSeries Access for Windows a iSeries Navigator (komponent Konfigurácia a servis produktu iSeries Navigator) Verzia 5, vydanie 3 alebo novšie
- V serveri ste vytvorili aspoň dva logické oddiely (LPAR). Oddiel vlastniaci modem musí mať nainštalovaný systém OS/400 verzia 5, vydanie 3 alebo novší. Ostatné oddiely môžu mať nainštalovaný systém OS/400 V5R2 alebo V5R3, Linux alebo AIX. V tomto scenári používajú systémy operačný systém OS/400 alebo Linux.
- Na komunikáciu medzi oddielmi máte vytvorený virtuálny Ethernet. Pozrite si tento scenár: Vytvorenie virtuálnej siete Ethernet pre komunikáciu medzi oddielmi.

Požiadavky pre nastavenie pre iSeries-B zahŕňajú:

- iSeries Access for Windows a iSeries Navigator (komponent Konfigurácia a servis produktu iSeries Navigator) Verzia 5, vydanie 2 alebo novšie

Kroky konfigurácie

Vykonajte tieto konfiguračné úlohy:

1. Vytvorte profil terminátora L2TP pre ľubovoľné rozhranie v oddiele, ktorý vlastní modem.
2. Vytvorte profil vzdialeného telefonického pripojenia L2TP pre 10.1.1.74
3. Vytvorte profil vzdialeného telefonického pripojenia L2TP pre 192.168.1.2
4. Otestujte pripojenie

Detaily scenára: Zdieľanie modemu medzi logickými oddielmi pomocou L2TP

Po splnení požiadaviek ste pripravený začať s konfiguráciou profilov L2TP.

Krok 1: Nakonfigurujte profil terminátora L2TP pre ľubovoľné rozhranie v oddiele, ktorý vlastní modemy.

Ak chcete vytvoriť profil terminátora pre ľubovoľné rozhranie, vykonajte tieto kroky:

1. V iSeries Navigator rozviňte váš server **--> Sieť --> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Profily pripojenia príjemcu** a vyberte **Nový profil**.
3. Na stránke Nastavenie vyberte tieto voľby a kliknite na **OK**:
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: L2TP (virtuálna linka)
   - **Režim prevádzky**: Terminátor (sieťový server)
   - **Typ služby linky**: Samostatná linka
4. Na záložke **Nový profil — Všeobecné** vyplňte tieto polia:
   - **Názov**: toExternal
   - **Opis**: Pripojenie príjemcu, ktoré sa bude vytáčať
   - Vyberte **Spustiť profil s TCP**.
5. Na záložke **Nový profil — Pripojenie** vyplňte tieto polia:
   - **Adresa IP lokálneho koncového bodu tunela**: ANY
   - **Názov virtuálnej linky**: toExternal.
     Táto linka nemá priradené žiadne fyzické rozhranie. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Otvorí sa dialógové okno Vlastnosti linky L2TP. Kliknite na záložku Autentifikácia a zadajte názov hostiteľa vášho servera. Kliknutím na **OK** sa vráťte na záložku Pripojenie v okne Vlastnosti nového profilu PPP.
6. Kliknite na **Povoliť vytvorenie odchádzajúceho volania**. Zobrazí sa dialógové okno **Vlastnosti vytáčania odchádzajúceho volania**.
7. Na stránke **Vlastnosti vytáčania odchádzajúceho volania** vyberte typ služby linky.
   - **Typ služby linky**: Oblasť liniek
   - **Názov**: dialOut
   - Kliknite na **Nová**. Zobrazí sa dialógové okno Vlastnosti novej oblasti liniek.
8. V dialógovom okne Vlastnosti novej oblasti liniek vyberte linky a modemy, ku ktorým povolíte odchádzajúce volania a kliknite na **Pridať**. Ak potrebujete definovať tieto linky, vyberte **Nová linka**. Rozhrania v oddiele, ktorý vlastní tieto modemy sa pokúsia použiť ktorúkoľvek otvorenú linku z tejto oblasti liniek. Zobrazí sa okno Vlastnosti novej linky.
9. Na záložke **Vlastnosti novej linky — Všeobecné** zadajte informácie do týchto polí:
   - **Názov**: line1
   - **Opis**: prvá linka a prvý modem pre oblasť liniek (interný modem 2793)
   - **Hardvérový prostriedok**: cmn03 (komunikačný port)
10. Akceptujte predvolené hodnoty vo všetkých ostatných záložkách a kliknutím na **OK** sa vráťte do okna Vlastnosti novej oblasti liniek.
11. V dialógovom okne Vlastnosti novej oblasti liniek vyberte linky a modemy, ku ktorým povolíte odchádzajúce volania a kliknite na **Pridať**. Skontrolujte, že je pre oblasť vybratý modem 2793.
12. Znova vyberte **Nová linka** a pridajte modem ECS 7852–400. Zobrazí sa okno Vlastnosti novej linky.
13. Na záložke **Vlastnosti novej linky — Všeobecné** zadajte informácie do týchto polí:
    - **Názov**: line2
    - **Opis**: druhá linka a druhý modem pre oblasť liniek (externý modem ECS 7852-400)
    - **Hardvérový prostriedok**: cmn04 (port V.24)
    - **Rámcovanie**: Asynchrónne

14. Na záložke **Vlastnosti novej linky — Modem** vyberte externý modem (7852–400) a kliknutím na **OK** sa vráťte do okna Vlastnosti novej oblasti liniek.
15. Vyberte všetky ostatné dostupné linky, ktoré chcete pridať do oblasti liniek a kliknite na **Pridať**. V tomto príklade skontrolujte, že dva modemy, ktoré ste predtým pridali sú zobrazené v poli *Vybraté linky pre oblasť* a kliknutím na **OK** sa vráťte do okna Vlastnosti vytáčania odchádzajúceho volania.
16. V okne Vlastnosti vytáčania odchádzajúceho volania zadajte **Predvolené čísla pre vytáčanie** a kliknutím na OK sa vráťte do okna Vlastnosti nového profilu PPP.

    Poznámka: Tieto čísla môžu byť niečo ako váš ISP a ostatné systémy ich budú pomocou týchto modemov často volať. Ak iné systémy zadajú telefónne čísla *PRIMARY alebo *BACKUP, budú sa vytáčať tu zadané čísla. Ak iné systémy zadajú konkrétne telefónne číslo, použije sa nimi zadané číslo.
17. Na záložke **Nastavenia TCP/IP** vyberte tieto hodnoty:
    - **Lokálna adresa IP**: Žiadna
    - **Vzdialená adresa IP**: Žiadna

    Poznámka: Ak používate profil aj na ukončovanie relácií L2TP, budete musieť vybrať lokálnu adresu IP, reprezentujúcu server iSeries. Pre Vzdialenú adresu IP ste mohli vybrať oblasť adries, ktorá je v rovnakej podsieti ako váš server. Všetky relácie L2TP by dostali svoje adresy IP z tejto oblasti. Ostatné úvahy nájdete v téme Podpora viacerých profilov pripojenia.
18. Na záložke **Autentifikácia** akceptujte všetky predvolené hodnoty.

Dokončili ste konfiguráciu profilu terminátora L2TP v oddiele s modemami. Ďalším krokom je konfigurácia vzdialeného telefonického pripojenia L2TP — profil pôvodcu pre 10.1.1.74.

Krok 2: Nakonfigurujte profil pôvodcu L2TP pre 10.1.1.74

Ak chcete vytvoriť profil pôvodcu L2TP, vykonajte tieto kroky:
1. V iSeries Navigator rozviňte 10.1.1.74 **--> Sieť --> Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Profily pripojenia pôvodcu** a vyberte **Nový profil**.
3. Na stránke Nastavenie vyberte tieto voľby a kliknite na **OK**:
   - **Typ protokolu**: PPP
   - **Typ pripojenia**: L2TP (virtuálna linka)
   - **Režim prevádzky**: Vzdialené telefonické pripojenie
   - **Typ služby linky**: Samostatná linka
4. Na záložke **Všeobecné** vyplňte tieto polia:
   - **Názov**: toModem
   - **Opis**: pripojenie pôvodcu k oddielu vlastniacemu modem
5. Na záložke **Pripojenie** vyplňte tieto polia:

   Názov virtuálnej linky: toModem
   Táto linka nemá žiadne priradené fyzické rozhranie. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Otvorí sa dialógové okno Vlastnosti linky L2TP.
6. Na záložke **Všeobecné** zadajte opis pre virtuálnu linku.
7. Na záložke **Autentifikácia** zadajte lokálny názov hostiteľa pre oddiel a kliknutím na **OK** sa vráťte na stránku **Pripojenie**.
8. V poli **Vzdialené telefónne čísla** pridajte *PRIMARY a *BACKUP. Toto umožňuje profilu používať rovnaké telefónne čísla ako profil terminátora v oddiele vlastniacom modemy.
9. V poli **Názov hostiteľa alebo adresa IP vzdialeného koncového bodu tunela** zadajte adresu vzdialeného koncového bodu tunela (10.1.1.73).
10. Na záložke **Autentifikácia** vyberte voľbu **Povoliť vzdialenému systému overiť identitu tohto servera iSeries**.

11. Pod autentifikačným protokolom, ktorý sa má použiť vyberte **Vyžadovať zašifrované heslo (CHAP-MD5)**. Štandardne je vybraté tiež **Povoliť rozšíriteľný autentifikačný protokol**.

    Poznámka: Protokol by mal zodpovedať protokolu, ktorý používa server, ku ktorému sa pripájate.

12. Zadajte meno užívateľa a heslo.

    Poznámka: Meno užívateľa a heslo musí zodpovedať menu užívateľa a heslu, platnému v serveri, ku ktorému sa pripájate.

13. Prejdite na záložku **Nastavenia TCP/IP** a skontrolujte vyžadované polia:
    - **Lokálna adresa IP**: Priradená vzdialeným systémom
    - **Vzdialená adresa IP**: Priradená vzdialeným systémom
    - **Smerovanie**: Nevyžaduje sa ďalšie smerovanie
14. Kliknutím na **OK** uložte profil PPP.

Krok 3: Nakonfigurujte profil vzdialeného telefonického pripojenia L2TP pre 192.168.1.2

Zopakujte krok 2. Zmeňte však adresu vzdialeného koncového bodu tunela na 192.168.1.3 (fyzické rozhranie, ku ktorému sa pripája iSeries B).

Poznámka: Toto sú fiktívne adresy IP a sú použité len na účely tohto príkladu.

Krok 4: Otestujte pripojenie

Po dokončení konfigurácie oboch serverov by ste mali otestovať pripojenie a skontrolovať, že systémy zdieľajú modem na prístup k externým sieťam. Vykonajte to podľa týchto krokov:

1. Skontrolujte, že je aktívny profil terminátora L2TP.
   a. V iSeries Navigator rozviňte 10.1.1.73 **--> Sieť --> Služby vzdialeného prístupu** --> **Profily pripojenia príjemcu**.
   b. V pravej časti okna nájdite požadovaný profil (toExternal) a skontrolujte, že v poli **Stav** je hodnota *Aktívny*. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
2. Spustite profil vzdialeného telefonického pripojenia pre 10.1.1.74.
   a. V iSeries Navigator rozviňte 10.1.1.74 **--> Sieť --> Služby vzdialeného prístupu** --> **Profily pripojenia pôvodcu**.
   b. V pravej časti okna nájdite požadovaný profil (toModem) a skontrolujte, že v poli **Stav** je hodnota *Aktívny*. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
3. Spustite profil vzdialeného telefonického pripojenia pre iSeries B.
   a. V iSeries Navigator rozviňte 192.168.1.2 **--> Sieť --> Služby vzdialeného prístupu** --> **Profily pripojenia pôvodcu**.
   b. V pravej časti okna nájdite vytvorený profil a skontrolujte, že v poli **Stav** je hodnota *Aktívny*. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
4. Ak je to možné, skontrolujte, že sú aktívne oba profily tak, že vykonáte príkaz ping pre ISP alebo iné ciele, ku ktorým ste pripojený. Pokúste sa vykonať príkaz ping z adresy 10.1.1.74 aj 192.168.1.2.
5. Prípadne môžete skontrolovať tiež Stav pripojenia.
   a. V iSeries Navigator rozviňte požadovaný server (napríklad 10.1.1.73) **--> Sieť --> Služby vzdialeného prístupu** --> **Profily pripojenia pôvodcu**.
   b. V pravej časti okna kliknite pravým tlačidlom myši na vytvorený profil a vyberte **Pripojenia**. V okne Stav pripojenia môžete vidieť, ktoré profily sú aktívne, neaktívne, pripájajú sa a podobne.

«

Koncepty PPP

PPP môžete použiť na pripojenie servera iSeries k vzdialeným sieťam, klientskym počítačom, k inému iSeries alebo k ISP. Ak chcete úplne využívať tento protokol, mali by ste sa oboznámiť so schopnosťami aj podporou iSeries tohto protokolu. 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 na komunikáciu cez telefónnu sieť alebo Internet používajú **PPP** alebo **protokol Point-to-Point**. Pripojenie PPP existuje vtedy, ak sú dva systémy fyzicky prepojené cez telefónnu linku. PPP môžete použiť na pripojenie jedného systému k druhému. Napríklad, vytvorené pripojenie PPP medzi pobočkou a centrálou im umožňuje navzájom prenášať údaje cez sieť.

PPP je internetový 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 opisujú 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 pripojení

Existujú dva typy profilov, ktoré vám umožňujú definovať skupinu charakteristík pre pripojenie alebo množinu pripojení PPP.

- **Profily pôvodcu pripojenia** sú pripojenia point-to-point, ktoré pochádzajú z lokálneho servera iSeries a prijíma ich vzdialený systém. Pomocou tohto objektu môžete konfigurovať odchádzajúce pripojenia.
- **Profily pripojenia príjemcu** sú pripojenia point-to-point, ktoré pochádzajú zo vzdialeného systému a prijíma ich lokálny server iSeries. Pomocou tohto objektu môžete konfigurovať prichádzajúce pripojenia.

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

- Aký typ protokolu pripojenia použijete? (PPP alebo SLIP)
- Kontaktuje váš server iSeries iný počítač vytáčaním (pôvodca)? Čaká váš server iSeries na prijatie volania z iného systému (príjemca)?
- Aká komunikačná linka sa použije pri pripojení?
- Ako by mal váš server iSeries zistiť, ktorá IP adresa sa má použiť ?
- Ako by mal váš server iSeries autentifikovať iný systém ? Kde by mal váš server iSeries ukladať autentifikačné informácie ?

Profil pripojenia 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: Adresy IP a ich smerovanie, filtrovanie IP.
- Riadenie prevádzky a prispôsobenie pripojenia
- Názvové servery domény

Server iSeries ukladá tieto informácie o konfigurácii do profilu pripojenia. Tieto informácie poskytujú potrebný kontext pre váš server iSeries na vytvorenie pripojenia PPP k inému počítačovému systému. Profil pripojenia obsahuje tieto informácie:

- **Typ protokolu**. Môžete si vybrať buď PPP alebo SLIP. IBM odporúča, aby ste PPP používali vždy, keď je to možné.
- **Výber režimu**. Typ pripojenia a prevádzkový režim pre tento profil pripojenia.

  Typ pripojenia určuje typ linky pre vaše pripojenia a to, či ide o **vytáčanie** alebo **odpovedanie** (resp. pôvodca alebo príjemca). Môžete si vybrať z týchto typov pripojenia:

  – 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 pre Profily 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 telefonické pripojenie
PPP cez Ethernet	Pôvodca

Prezrite si nasledujúcu tabuľku pre profily príjemcu pripojenia:

Tabuľka 2. Možné prevádzkové režimy Profilov pôvodcu pripojenia.

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

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

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

– Jednoduchá linka
– Oblasť liniek

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 do siete, 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 adries IP.

Plánovanie PPP

Vytvorenie a správa pripojení PPP vyžaduje oboznámenie sa s podporou PPP aj s alternatívami pripojenia v serveroch iSeries a tiež s mnohými plánmi týkajúcimi sa pripájania do siete a bezpečnosti, ktoré používa váš podnik. Nasledujúce témy vám pomôžu oboznámiť sa s dostupnými voľbami a požiadavkami týkajúcimi sa pripojení iSeries pomocou PPP.

Softvérové a hardvérové požiadavky
Na nakonfigurovanie pripojení PPP budete potrebovať aplikáciu iSeries Navigator. Zoznam ďalších požiadaviek nájdete v tejto téme.

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

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

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

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

Informácie o šírke pásma
iSeries podporuje pre pripojenia PPP viaclinkový protokol. To vám umožní použiť viaceré analógové telefónne linky pre jediné pripojenie, 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, server iSeries, môže byť buď pôvodcom alebo príjemcom. Server iSeries musí spĺňať nasledujúce požiadavky, aby naň mohli pristupovať vzdialené systémy.

- Aplikácia **iSeries Navigator** s podporou TCP/IP.
- Jeden z dvoch uvedených profilov pripojenia:
  – Profil pôvodcu pripojenia na spracovanie odchádzajúcich pripojení PPP
  – Profil príjemcu pripojenia na spracovanie prichádzajúcich pripojení PPP

- Konzola pracovnej stanice PC nainštalovaná s **iSeries Access for Windows (95/98/NT/Millenium/2000/XP)** s aplikáciou 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)
  - 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
  - 2838/2849: Ethernetový adaptér pre pripojenia 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 pripojenia

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 pripojenia 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 pripojenie 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 pripojení:

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

Analógové telefónne linky

Analógové pripojenie, ktoré využíva na prenos dát po prenajatých alebo komutovaných linkách modem, je najnižším typom pripojenia point-to-point. Prenajatá linka je trvalým pripojením 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 pripojenia môžu byť skrátené vďaka vylepšeniam v procese nadviazania pripojenia 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 pripojenia, 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 pripojenie. 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 pripojeniach 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 pripojenie, 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 pripojení 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 prenosová rýchlosť servera iSeries v baudoch pre asynchrónny cez RS232 je 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 synchrónny cez RS232 pri rýchlosti 128 Kbps, ale maximálna prenosová rýchlosť servera iSeries v baudoch pre synchrónny cez RS232 je 64 Kbps.

Server iSeries je schopný používať asynchrónny cez V.35 pri rýchlostiach až 230,4 Kbps, ale výrobcovia terminálových adaptérov všeobecne neponúkajú takúto konfiguráciu. Konvertory rozhrania, ktoré konvertujú RS232 na rozhranie V.35, môžu byť rozumným riešením tohto problému, tento prístup však nebol vyhodnotený pre server iSeries. 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

Pripojenie 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 pripojení 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 pripojenia dátovej linky) v rámci a na riadenie trasy alebo virtuálneho pripojenia.

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 pripojenia 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 pripojenia 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 je možné oddeliť miesto, kde sa končí protokol telefonického pripojenia a miesto, kde sa poskytuje prístup k sieti; to je dôvod, prečo sa L2TP označuje aj ako Virtuálne PPP. Protokol L2TP je dokumentovaný ako štandard RFC2661 (Request For Comment). Viac informácií o RFC nájdete na http://www.rfc-editor.org. Tunel L2TP sa môže rozšíriť cez celú reláciu PPP alebo len cez jeden segment dvoj-segmentovej relácie. To možno vyjadriť štyrmi rôznymi modelmi tunelovania:

- Nevynútený tunel
- Vynútený tunel - prichádzajúce volanie
- Vynútený tunel - vzdialené telefonické pripojenie
- Viacskokové pripojenie 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 domovskú bránu (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 pripojenie 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 pripojenie L2TP: Viacskokové pripojenie L2TP je metódou presmerovania prevádzky L2TP na klientske LAC a LNS. Viacskokové pripojenie sa nadväzuje pomocou viacskokovej brány L2TP (systému, ktorý prepája profily terminátora a iniciátora L2TP). Na vytvorenie viacskokového pripojenia bude viacskoková brána L2TP vystupovať voči sade LAC ako LNS a zároveň ako LAC voči danému LNS. Tunel sa vytvára z klientskeho LAC na viacskoková brána L2TP a ďalší tunel sa vytvára medzi viacskokovou bránou L2TP a cieľovým LNS. Prevádzku L2TP z klientskeho LAC potom viacskoková brána L2TP presmeruje na cieľový LNS a prevádzku z cieľového LNS presmeruje na klientsku LAC.

Podpora PPPoE (DSL) pre pripojenia 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 telefonické modemové pripojenie. 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 telefonického 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
- Ethernetové adaptéry typu 2838 alebo 2849 (pre pripojenia PPPoE).

Modemy

Pri pripojeniach 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 pripojenia PPP, pretože rôzne modely modemov používajú rôzne reťazce inicializačných príkazov. Ak ide o interný modem, modemové reťazce majú už zadefinované svoje použitie.

Server iSeries má preddefinovaných veľa modelov modemov, nové modely však možno zadefinovať prostredníctvom aplikácie iSeries Navigator. 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.

Môžete používať modem ECS (electronic customer support), ktorý sa dodáva so serverom iSeries na vytvorenie pripojení PPP. V starších systémoch bol modemom ECS externý modem IBM 7852-400. V novších systémoch sa môže ako modem ECS použiť typ 2771, 2793 alebo ľubovoľný iný podporovaný interný modem.

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 pripojenia T-1 alebo T-3; jednotky na oboch koncoch musia pochádzať od toho istého výrobcu.

Terminálové adaptéry ISDN

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

Skontrolujte, či je váš terminálový adaptér odporúčaný pre používanie na serveri iSeries:

- V Odporúčaniach pre terminálový adaptér ISDN nájdete, ktorý adaptér by ste mali použiť.
- V Obmedzeniach pre terminálové adaptéry ISDN nájdete informácie a stručné vyhodnotenia rôznych terminálových adaptérov ISDN, ktoré boli testované serverom iSeries.

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

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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.

Pozrite si príklad Konfigurácia terminálového adaptéra ISDN, kde nájdete vzorové procedúry, ktoré používajú aplikáciu iSeries 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 PPP cez ISDN v režimoch vzniku aj odpovede na serveri iSeries. Pri PPP pripojení 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.

- **Pripojenia, ktoré pochádzajú zo servera iSeries.** Na výzvy CHAP, ktoré pochádzajú z prijímajúcej strany, odpovedá terminálový adaptér Courier I pri dohodovaní autentifikácie PAP (Password Authentication Protocol) so serverom iSeries. Odpovede PAP sa neobjavia na pripojení ISDN.
- **Pripojenia, na ktoré odpovedá server iSeries.** Courier I vyžaduje od volajúcej strany autentifikáciu CHAP, ak konfigurácia odpovedí servera iSeries spôsobí, že server iSeries otvorí autentifikáciu pomocou výzvy CHAP. Ak server iSeries otvorí autentifikáciu pomocou PAP, terminálový adaptér Courier I autentifikuje pomocou PAP.

Ak používate modem Courier I starší ako z r. 1999, skontrolujte, či je modem Courier I pripojený k vášmu serveru iSeries káblom V.35, aby ste z vášho pripojenia ISDN dostali čo 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 ešte stále odporúča pri trocha zníženom výkone na serveri iSeries, pretože pripojenia RS-232 sú 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.

Rýchlosť linky V.35 musíte na serveri iSeries nastaviť na 230,4 Kbps.

Obmedzenia pre terminálový adaptér ISDN: Nasleduje prehľad terminálových adaptérov, ktoré boli vyhodnotené. Odporúčajú sa len pre vytvorenie vzdialených pripojení ISDN zo servera iSeries.

3Com Impact IQ ISDN:

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

- Terminálový adaptér nepodporuje analógové modemové pripojenia V.34. Ak sa však použije externé pripojenie RJ-11, môže analógové modemové pripojenia V.34 podporovať.
- Terminálový adaptér aktuálne nepodporuje pripojenia V.90.
- Terminálový adaptér sa nesmie pripojiť k serveru iSeries pri rýchlostiach vyšších ako 115200 bps.
- Terminálový adaptér nepodporuje automaticky CHAP (Challenge Handshake Authentication Protocol). Nastavenie S84=0 však umožňuje serveru iSeries vykonávať autentifikáciu CHAP.
- Server iSeries nie je pri monitorovaní signálu Data Set Ready z terminálového adaptéra schopný určiť, kedy pripojenie skončí. To môže viesť k potenciálnemu ohrozeniu bezpečnosti systému.

Motorola BitSurfr Pro ISDN:

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

- Terminálový adaptér nepodporuje analógové modemové pripojenia V.34. Ak sa však použije externé pripojenie RJ-11, môže analógové modemové pripojenia V.34 podporovať.
- Terminálový adaptér aktuálne nepodporuje pripojenia V.90.
- Terminálový adaptér sa nesmie pripojiť k serveru iSeries pri rýchlostiach vyšších ako 115200 bps.
- Terminálový adaptér nepodporuje automaticky autentifikáciu CHAP. Nastavenie @M2=C však umožňuje serveru iSeries vykonávať autentifikáciu CHAP.
- 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 servera iSeries nespolupracuje dobre s týmto terminálovým adaptérom. Toto má za následok znížený výkon, keď server iSeries posiela údaje na viaclinkovom pripojení PPP.

Spravovanie adries IP

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

- DHCP

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

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

  BOOTP sa používa na spojenie klientskych pracovných staníc s vaším serverom iSeries a na priradenie IP adries týmto pracovným staniciam. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby BOOTP.
- Filtrovanie paketov IP

  Vytvorením súboru s pravidlami filtrovania IP obmedzte prístup užívateľov a skupín ku konkrétnym adresám IP. 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 adries IP 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 pripojenia

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

Ak definujete pevné adresy IP pre lokálnu alebo vzdialenú adresu IP, musíte zaistiť, aby bol vzdialený systém zadefinovaný tak, aby tieto adresy prijal. Bežný postup je taký, že zadefinujete svoju lokálnu adresu ako pevnú adresu IP 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 adries IP. Napríklad, ak sa server iSeries pripojí k Internetu cez ISP, toto môže umožniť aj pripojenej sieti za serverom iSeries prístup na Internet. Jednoducho, server iSeries 'skryje' IP adresy systémov v tejto sieti za lokálne IP adresy, priradené poskytovateľom internetových služieb, takže sa zdá, že celá prevádzka IP je zo servera iSeries. Existujú aj ďalšie úvahy o smerovaní pre systémy v sieti LAN (aby sa zabezpečilo odoslanie ich internetového prenosu na server iSeries), ako aj pre server iSeries, kde budete musieť aktivovať políčko 'add remote system as the default route'.

Profily príjemcu pripojenia:

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

Lokálne adresy IP

Pre jeden profil príjemcu môžete zadefinovať jedinečnú IP adresu alebo použiť existujúcu lokálnu IP adresu na vašom serveri iSeries. Táto sa stane adresou, ktorá bude identifikovať ukončenie pripojenia PPP servera iSeries. Pre profily príjemcu pripojenia definovaných na podporu viacnásobných pripojení v tom istom čase musíte použiť už existujúcu adresu IP. Ak práve neexistuje žiadna lokálna adresa IP, môžete s týmto cieľom vytvoriť Virtuálnu adresu IP.

Vzdialené adresy IP

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

Poznámka: Ak chcete, aby bol vzdialený systém považovaný za súčasť LAN, mali by ste nakonfigurovať smerovanie IP adresy, špecifikovať IP adresu v rámci rozsahu adries pre systémy pripojené cez LAN a overiť, či postúpenie IP bolo aktivované pre tento profil pripojenia aj pre systém iSeries.

Tabuľka 3. Možnosti priraďovania adries IP pre profil príjemcu pripojení

Voľba	Opis
Pevná adresa IP	Definujete jednu adresu IP, ktorá sa poskytne vzdialeným používateľom pri telefonickom pripájaní. Táto adresa IP je len hostiteľská (maska podsiete je 255.255.255.255) a je len pre jednotlivé profily príjemcov pripojenia.
Oblasti adries	Definujete počiatočnú adresu IP a potom rozsah, koľko ďalších adries IP sa má definovať. Každý užívateľ, ktorý sa pripája získa jedinečnú adresu z definovaného rozsahu. Je to len hostiteľská adresa IP (Maska podsiete je 255.255.255.255) a je len pre viacnásobné profily príjemcu pripojenia.

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

Voľba	Opis
RADIUS	Vzdialenú adresu IP 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 adresovanie IP. • V profile príjemcu pripojenia je aktivovaná autentifikácia a je definovaná tak, že ju autentifikuje vzdialene Radius.
DHCP	Vzdialená adresa IP 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 adresu IP (maska podsiete je 255.255.255.255).
V závislosti od ID užívateľa vzdialeného systému	Vzdialená adresa IP určuje id užívateľa určeného pre vzdialený systém pri autentifikácii. To umožňuje, aby správca prideľoval používateľovi, ktorý sa telefonicky pripája, rôzne vzdialené adresy IP (a s nimi spojené masky podsiete). Toto umožňuje tiež definovanie ďalších trás pre každý z týchto identifikátorov užívateľov, takže môžete prispôsobiť prostredie pre známeho vzdialeného užívateľa. Na správnu činnosť tejto funkcie musí byť zapnutá autentifikácia.
Určite dodatočné adresy IP 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 adries IP určená ako **Založená na užívateľskom id vzdialeného systému**. Táto metóda je povolená aj pri priraďovaní pevnej adresy IP a oblasti adries. Keď sa k serveru iSeries pripojí vzdialený užívateľ, prebehne vyhľadávanie, aby sa zistilo, či je vzdialená IP adresa zadefinovaná konkrétne pre tohto užívateľa. Ak to je potom táto adresa, pri pripojení sa použije maska a množina možných trás. Ak nie je užívateľ určený, bude štandardne pridelená určená Pevná adresa IP, alebo ďalšia adresa z Oblasti adries IP.
Povoľte vzdialenému systému určovať vlastné adresy IP	Táto voľba umožní vzdialenému používateľovi zadefinovať si vlastnú adresu IP, ak o to prejaví záujem. Ak o to záujem neprejavia, bude vzdialená adresa IP určená pomocou nastavenej metódy prideľovania vzdialených adries IP. Táto voľba nie je pôvodne nastavená. Pred jej nastavením treba uvážiť všetky aspekty.
Smerovanie adries IP	Klient telefonického pripojenia a iSeries musia mať správne nakonfigurované smerovanie IP adries, ak tento klient potrebuje prístup k všetkým IP adresám v sieti LAN, do ktorej patrí tento server iSeries.

Filtrovanie paketov IP

Filtrovanie paketov IP 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 adresy IP 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 pripojenia, alebo môžu byť pridelené pomocou skupinovej politiky, ktorá použije pravidlá filtrovania na kategóriu užívateľa. Samotné pravidlá filtrovania paketov nie sú zadefinované v PPP, sú však zadefinované pod pravidlami paketov IP v aplikácii iSeries Navigator. Viac informácií nájdete v Informačnom centre v časti Pravidlá paketov IP.

Pre pripojenia L2TP by sa na ochranu sieťovej prevádzky malo použiť VPN s filtrovaním IPSec. Viac informácií nájdete v Informačnom centre v časti VPN.

Autentifikácia systému

Pripojenia PPP so serverom iSeries podporujú rôzne voľby pre autentifikáciu vzdialených klientov, ktorí sa telefonicky pripájajú k iSeries aj pripojení k ISP alebo k inému serveru, ku ktorému sa telefonicky pripája iSeries. iSeries podporuje rôzne metódy spravovania autentifikačných informácií, od jednoduchých validačných zoznamov na iSeries, ktoré obsahujú zoznamy autorizovaných užívateľov a priradených hesiel, až po podporu serverov RADIUS, ktoré spravujú podrobné autentifikačné informácie o vašich sieťových užívateľoch. Sever iSeries podporuje aj rôzne voľby šifrovania informácií o ID užívateľa a hesle, od jednoduchej výmeny hesla až po podporu macerácie pomocou CHAP-MD5. Na záložke **Authentication** profilu pripojenia v aplikácii iSeries Navigator môžete špecifikovať vaše preferencie pre autentifikáciu systému, vrátane ID užívateľa a hesla, používaných na overenie platnosti iSeries pri vytáčaní.

Viac informácií o udržiavaní informácií na validáciu 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 pripojenia 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 pripojenie 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.

Server iSeries momentálne podporuje len verziu EAP, ktorá je prakticky rovnocenná 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 pripojenia. Po vytvorení pripojenia vzdialené zariadenie odošle dvojicu ID a heslo užívateľa autentifikujúcemu systému. V závislosti od správnosti tejto dvojice autentifikujúci systém buď pokračuje v pripojení, alebo ho ukončí.

Autentifikácia PAP vyžaduje, aby bolo meno používateľa a heslo zaslané do vzdialeného systému 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 internetový 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. Server iSeries, ktorý vystupuje ako NAS, odosiela informácie o užívateľovi a pripojení na označený server RADIUS použitím štandardného protokolu RADIUS, zadefinovaného v RFC 2865.

Servery RADIUS pracujú na prijatých požiadavkách na pripojenie užívateľa autentifikovaním tohto užívateľa a následne vrátia všetky potrebné informácie o konfigurácii na NAS, takže NAS (server iSeries) môže poskytnúť autorizované služby autentifikovanému volajúcemu užívateľovi.

Ak je server RADIUS nedosiahnuteľný, server iSeries môže smerovať požiadavky na autentifikáciu na náhradný 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. Môžu to byť súbory hesiel UNIX, Kerberos, komerčný bezpečnostný systém alebo aj vlastný vyvinutý bezpečnostný systém. Server RADIUS odošle späť na server iSeries všetky služby, ktoré je autentifikovaný užívateľ oprávnený používať, napríklad IP adresu. Požiadavky na účtovanie RADIUS sa spracovávajú podobným spôsobom. 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 v 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 pripojenia. 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 pripojenie sa dá vytvoriť len vtedy, ak oba konce pripojenia 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 pripojenia 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).

Konfigurácia PPP

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

- Vytvorenie profilu pripojenia
- Konfigurácia vášho modemu
- Konfigurácia vzdialeného počítača

- Konfigurácia prístupu na Internet prostredníctvom AT&T Global Network
- Sprievodcovia pripojením
- Konfigurácia skupinovej politiky prístupu
- Aplikácia pravidiel filtrovania paketov IP pri pripojení PPP
- Povolenie služieb RADIUS a DHCP pre profily príjemcu pripojenia PPP

Vytvorenie profilu pripojenia

Prvým krokom pri konfigurácii pripojenia PPP medzi systémami je vytvorenie profilu pripojenia na serveri iSeries. Profil pripojenia 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: Adresy IP a smerovanie
- Riadenie prevádzky a prispôsobenie pripojenia
- Názvové servery domény

Služby vzdialeného prístupu v adresári Podsieť obsahujú tieto objekty:

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

Ak chcete vytvoriť profil pripojenia, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator vyberte svoj systém a rozviňte **Network –> Remote Access Services**.
2. Vyberte jednu z týchto volieb:
   - Pravým tlačidlom myši kliknite na **Originator Connection Profiles**, čím nastavíte server iSeries ako server, ktorý iniciuje pripojenia.
   - Pravým tlačidlom myši kliknite na **Receiver Connection Profiles**, čím nastavíte server iSeries ako server, ktorý umožňuje prichádzajúce pripojenia zo vzdialených systémov a od vzdialených užívateľov.
3. Vyberte **Nový profil**.
4. Na strane **Nastavenie nového profilu pripojenia 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 pripojenia point-to-point?

PPP je štandardné internetové pripojenie. 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 pripojenia point-to-point. Request For Comment (RFC) pre SLIP sa nikdy nestal internetovým štandardom, pretože má uvedené nedostatky:

- SLIP nemá štandardný spôsob, akým definuje adresovanie IP 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 ešte stále používa a na serveri iSeries je ešte stále podporovaný.IBM však odporúča, aby ste pri nastavovaní pripojiteľnosti point-to-point použili PPP. SLIP neposkytuje žiadnu podporu viaclinkových pripojení. PPP má v porovnaní so SLIP lepšiu autentifikáciu. PPP dosahuje lepší výkon kvôli možnosti komprimácie.

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

Výber režimu

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

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

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

Komutovaná linka: Vyberte tento typ pripojenia, ak na pripojenie po telefónnej linke používate niektoré z uvedených zariadení:

- Modem (interný alebo externý)
- Externý terminálový adaptér ISDN

Typ pripojenia komutovanou linkou rozoznáva tieto režimy prevádzky:

- **Odpovedať**

  Tento režim prevádzky vyberte v prípade, ak chcete umožniť vzdialenému systému telefonicky sa pripojiť na server iSeries.

- **Vytáčať**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť pripojiť sa telefonicky k vzdialenému systému.

- **Vytáčať na požiadanie (len vytáčanie)**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť automaticky sa telefonicky pripojiť k vzdialenému systému, keď sa na tomto systéme zistí prevádzka 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)**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť odpovedať na volania z vyhradeného vzdialeného systému. Tento režim prevádzky tiež umožňuje serveru iSeries volať vzdialený systém, keď sa na vzdialenom systéme zistí prevádzka TCP/IP. Ak sú oba systémy servery iSeries a ak oba používajú tento režim prevádzky, prevádzka TCP/IP sa prenáša medzi týmito dvoma systémami na požiadanie a bez potreby trvalého fyzického pripojenia. 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 pripojenia 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 pripojenia vyberte v prípade, ak máte medzi lokálnym serverom iSeries a vzdialeným systémom vyhradenú linku. Ak máte prenajatú linku, nepotrebujete na prepojenie týchto dvoch systémov modem ani terminálový adaptér ISDN.

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

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

- **Terminátor**

  Tento režim prevádzky vyberte v prípade, ak chcete umožniť vzdialenému systému prístup na server iSeries cez vyhradenú linku. Tento režim prevádzky sa odvoláva na profil odpovede pri prenajatej linke.
- **Iniciátor**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť prístup na vzdialený systém cez vyhradenú linku. Tento režim prevádzky sa odvoláva na profil vytáčania pri prenajatej linke.

L2TP (virtuálna linka): V tomto type pripojenia umožníte pripojenie medzi systémami, ktoré používajú L2TP - Layer Two Tunneling Protocol.

Po vytvorení tunela L2TP sa medzi serverom iSeries a vzdialeným systémom vytvorí virtuálne pripojenie PPP. Použitím tunelovania L2TP v spojení s bezpečnosťou IP (IP-SEC) môžete posielať, smerovať a prijímať bezpečné údaje prostredníctvom Internetu.

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

- **Terminátor**

  Tento režim prevádzky vyberte v prípade, ak chcete umožniť vzdialenému systému pripojiť sa k serveru iSeries cez tunel L2TP.
- **Iniciátor**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť pripojiť sa k vzdialenému systému cez tunel L2TP.
- **Vzdialené telefonické pripojenie**

  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť pripojiť sa k ISP cez tunel L2TP a ISP nasmerovať na volanie vzdialeného klienta PPP.
- **Viacskokový iniciátor**

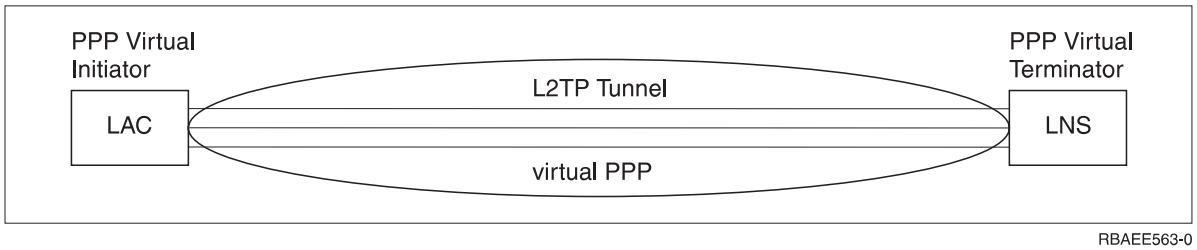
  Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť vytvorenie viacskokového pripojenia.

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

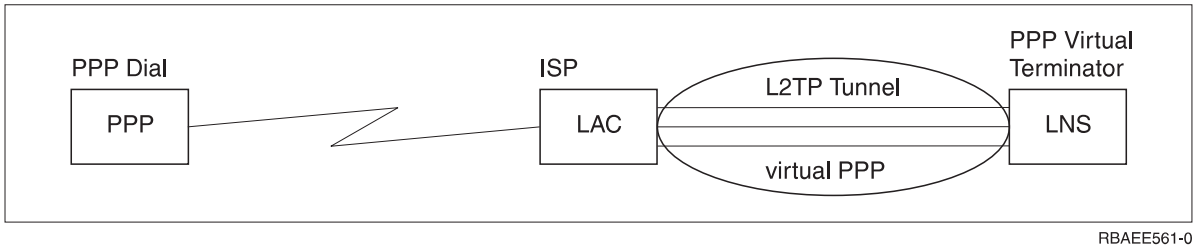
L2TP - Layer 2 Tunneling Protocol: L2TP rozširuje PPP tak, aby podporovala tunel spojovacej vrstvy medzi žiadajúcim klientom L2TP a cieľovým koncovým bodom, serverom L2TP. Pomocou tunelov L2TP možno oddeliť miesto, na ktorom sa končí protokol telefonického pripojenia od miesta, na ktorom sa poskytuje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

Poskytovateľ služieb Internetu (ISP) používa na prevádzku Virtual Private Networks (VPN) režim virtuálnej linky. Ak chcete vedieť viac o tom, ako pracuje IPSec s L2TP, pozrite si Konfigurovanie pripojenia L2TP, chráneného pomocou VPN.

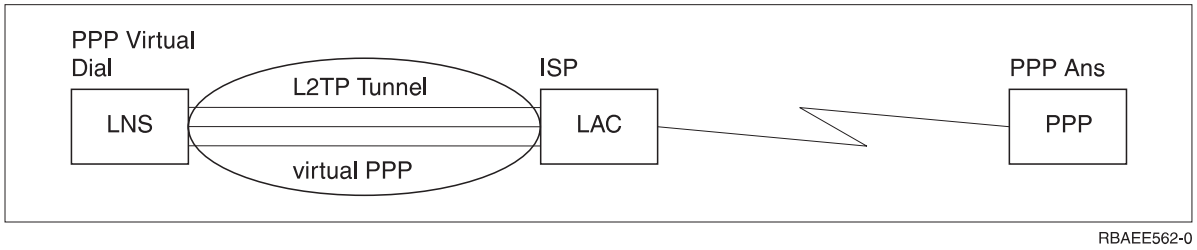
Nasledujúce obrázky ilustrujú tri rôzne realizácie tunelovania L2TP:



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: Pripojenia PPPoE používajú virtuálnu linku na odosielanie údajov PPP (cez vyhradený Ethernetový adaptér 2838 alebo 2849) modemu DSL poskytnutému vaším ISP, ktorý je tiež pripojený k sieti LAN, založenej na systéme Ethernet. Toto umožňuje vysokorýchlostný prístup na Internet pre užívateľov v sieti LAN cez relácie PPP prostredníctvom servera iSeries. Po pripojení servera iSeries k poskytovateľovi internetových služieb (ISP) môžu jednotliví užívatelia v sieti LAN spustiť jedinečné relácie s poskytovateľom internetových služieb cez PPPoE.

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

Konfigurácia pripojenia

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

- Jednoduchá linka
- Oblasť liniek

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. Profil pripojenia PPP používa vždy rovnaký prostriedok komunikačného portu servera iSeries.

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. Predpokladá sa, 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 telefonické pripojenie, odpovedajúci profil si vyžiada linku a spustí sa. V druhom prípade počká spustený odpovedajúci profil na prichádzajúce pripojenie. Kým nie je vykonané prichádzajúce pripojenie, 'požičia' si volajúce pripojenie, ktoré bolo spustené ako druhé, linku od odpovedajúceho profilu, ktorý mu linku 'požičia'. Potom sa vytvorí odchádzajúce pripojenie. Keď je pripojenie ukončené, volajúci profil vráti linku odpovedajúcemu profilu, ktorý bude znova schopný akceptovať prichádzajúce pripojenia. Funkciu zdieľania povolíme kliknutím na opis prepnutej linky na 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 pripojenia L2TP (virtuálna linka) sa nepoužíva na jednoduchú linku žiadny hardvérový prostriedok komunikačného portu. Jednoduchá linka použitá pripojením 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.

Oblasť liniek: Výberom tejto linkovej služby nastavíte pripojenie PPP na používanie linky z oblasti liniek. Server iSeries vyberie po spustení pripojenia PPP z oblasti liniek nepoužívanú linku. Pri profiloch telefonického pripojenia na požiadanie si server linku vyberie až vtedy, keď zistí pre vzdialený systém prevádzku TCP/IP.

Oblasť liniek môžete použiť namiesto definovania určitého opisu linky pre profil pripojenia. V oblasti liniek môžete špecifikovať jeden alebo viac opisov linky.

Oblasť liniek ďalej umožňuje, aby jeden profil pripojenia spracúval buď viacnásobné prichádzajúce analógové volania alebo jedno odchádzajúce analógové volanie. Linka sa po ukončení pripojenia PPP vracia do oblasti liniek.

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

Výhody používania oblastí liniek:

- Prostriedok linky viažete na pripojenie 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 oblasti liniek, 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 pripojenia dosiahnutá dodatočná dostupnosť prostriedkov.
- Aby ste prostriedky využívali efektívnejšie, môžete použiť profily telefonického pripojenia na požiadanie (dial-on-demand) s oblasťami liniek.

  Server iSeries vyberie z oblasti liniek linku len v prípade, ak používa telefonické pripojenie na požiadanie. Ostatné pripojenia môžu tú istú linku použiť inokedy.
- Môžete spustiť viac pripojení PPP s menším počtom prostriedkov na ich podporu.

Ak napríklad vaše prostredie potrebuje štyri jedinečné typy pripojení, ale vám stačia naraz maximálne dve linky, na spustenie tohto prostredia môžete použiť oblasť liniek. Vytvoríte štyri profily telefonického pripojenia na požiadanie a každý profil odkážete na oblasť liniek, ktorá obsahuje opisy dvoch liniek. Každá z liniek by mohla byť použitá všetkými štyrmi profilmi a tak dvom pripojeniam umožňuje byť aktívnymi kedykoľvek. Použitím spoločnej oblasti liniek nemusíte mať štyri samostatné linky.

Ak je vaše prostredie kombináciou klienta PPP a servera PPP, linky sa môžu tiež zdieľať (povoľte dynamické zdieľanie prostriedkov), keď sa používajú ako 'samostatné linky' alebo sú umiestnené v 'oblasti liniek'. Profil, ktorý bol spustený ako prvý, nezapojí prostriedok, kým nie je pripojenie aktívne. Napríklad, ak je spustený Server PPP a očakáva prichádzajúce pripojenia, 'požičia' používanú linku Klientovi PPP, ktorý sa spustil a 'požičiava' si od Servera PPP túto zdieľanú linku.

Konfigurovanie oblastí liniek

Oblasti liniek sa definujú v profile pripojenia. Základnú konfiguráciu oblasti liniek vykonajte pomocou týchto krokov:

1. V aplikácii iSeries Navigator vyberte svoj systém a rozviňte **Networking —>Remote Access Services**.
2. Vytvorte profil pripojenia pre vytáčanie alebo prijímanie volaní. Vyberte jednu z týchto volieb:
   - Pravým tlačidlom myši kliknite na Originator Connection Profiles, čím nastavíte server iSeries ako server, ktorý iniciuje pripojenia.
   - Pravým tlačidlom myši kliknite na Receiver Connection Profiles, čím nastavíte server iSeries ako server, ktorý umožňuje prichádzajúce pripojenia zo vzdialených systémov a od vzdialených užívateľov.
3. Vyberte **Nový profil**.
4. Pre profil pôvodcu (vytáčanie) vyberte: PPP, Komutovaná linka a Režim prevádzky (typicky telefonické pripojenie). Pre konfiguráciu spojenia vyberte **Oblasť liniek**. Kliknutín na **OK** otvorí aplikácia iSeries Navigator dialógové okno vlastností tohto profilu pripojenia.

   Poznámka: Oblasť liniek môžete vybrať aj pri vytváraní profilov pripojenia príjemcu. Voľba oblasti liniek môže alebo nemusí byť zobrazená, v závislosti od hodnôt týchto polí: typ protokolu, typ pripojenia a režim prevádzky.
5. Na stránke **Všeobecné** zadajte názov a opis profilu.
6. Na stránke **Pripojenie** zadajte názov pre oblasť liniek a kliknite na **Nová**. Toto otvorí dialógové okno Vlastnosti novej oblasti liniek, kde sa zobrazia všetky dostupné linky a modemy pre tento systém.
7. Vyberte linky, ktoré chcete použiť a pridajte ich do oblasti. Môžete tiež kliknúť na **Nová linka** a definovať novú linku.
8. Kliknutím na **OK** uložíte túto oblasť liniek a vrátite sa do vlastností nového profilu point-to-point.
9. Vyplňte všetky potrebné informácie na ostatných stránkach (napríklad Nastavenie TCP/IP a Autentifikácia).
10. Profil pripojenia bude postupne prehľadávať zoznam dostupných liniek (v oblasti), kým nenájde dostupný prostriedok a túto linku použije pre pripojenie. Ďalšiu pomoc nájdete v pomoci pre aplikáciu iSeries Navigator.

Profil viacnásobných pripojení: Profily pripojenia point-to-point, ktoré podporujú viaceré spojenia, vám umožňujú mať jeden profil pripojenia, ktorý obsluhuje viacero digitálnych, analógových volaní alebo volaní L2TP. Je to užitočné v prípade, ak chcete, aby sa k vášmu serveru iSeries pripojilo viac užívateľov, ale na spravovanie jednotlivých liniek PPP nechcete špecifikovať osobitný profil pripojenia point-to-point. Táto vlastnosť je dôležitá hlavne pre 4-portový integrovaný modem 2805, kde sa používajú 4 linky z jedného adaptéra.

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

Lokálna adresa IP pre profily viacnásobných pripojení:

Lokálnu IP adresu môžete používať s profilmi viacnásobných pripojení, musí to však byť existujúca IP adresa, ktorá je zadefinovaná na vašom serveri iSeries. Môžete použiť sťahovací zoznam lokálnych adries IP, aby ste vybrali existujúcu

adresu. Vzdialení užívatelia môžu pristupovať na prostriedky vo vašej lokálnej sieti, ak lokálnu IP adresu servera iSeries vyberiete ako lokálnu IP adresu pre váš profil PPP. Tiež musíte definovať adresy IP, ktoré sú vo vzdialenej spoločnej oblasti adries IP, aby boli v rovnakej sieti ako lokálne adresy IP.

Ak nemáte lokálnu IP adresu servera iSeries alebo ak nechcete, aby vzdialení užívatelia pristupovali na LAN, musíte pre svoj server iSeries zadefinovať virtuálnu IP adresu. Virtuálna adresa IP je tiež známa ako bezokruhové rozhranie. Vaše profily point-to-point môžu používať túto adresu IP ako ich lokálnu adresu IP. Pretože táto adresa nie je viazaná na fyzickú sieť, nebude automaticky postupovať prenos do iných sietí, ktoré sú pripojené k vášmu serveru iSeries.

Na vytvorenie virtuálnej adresy IP vykonajte tieto kroky:

1. V aplikácii iSeries Navigator rozviňte svoj server a prejdite na **Network –> TCP/IP configuration > IPV4 > Interfaces**.
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 adresa IP, vaše profily pripojenia point-to-point ju môžu používať. Ak chcete so svojím profilom použiť adresu, môžete použiť sťahovací zoznam z poľa Lokálna adresa IP, ktorý je na stránke Nastavenia TCP/IP.

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

Oblasť vzdialených adries IP pre profily viacnásobných pripojení:

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

Obmedzenia oblasti liniek:

Tieto obmedzenia platia pri používaní oblastí liniek pre viacnásobné pripojenia:

- 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 pripojenia, ktorý používa oblasť liniek, sa použijú všetky linky v oblasti liniek až po maximálny počet spojení, ktorý je zadefinovaný v tomto profile. Ak nie sú dostupné žiadne linky, zlyhajú všetky nové pripojenia. Taktiež, ak je spustený ďalší profil, ale nie sú dostupné žiadne linky v oblasti liniek, bude tento profil ukončený.
- Keď spustíte profil jedného pripojenia, ktorý má oblasť liniek, systém používa len jednu linku zo spoločnej oblasti. Ak spustíte profil viacnásobného pripojenia, ktorý používa rovnakú oblasť liniek, použijú sa akékoľvek dostupné linky oblasti liniek.

Spoločné oblasti vzdialených adries IP: Systém môže používať spoločné oblasti vzdialených adries IP na odpovedanie alebo ukončovanie profilu pripojenia PPP, ktorý sa používa s viacerými prichádzajúcimi spojeniami. Toto zahŕňa L2TP a oblasti liniek s maximálnym počtom pripojení väčším ako jedno. Táto funkcia dovoľuje systému priraďovať jedinečné vzdialené adresy IP každému prichádzajúcemu pripojeniu.

Prvý systém na pripojenie dostane adresu IP definovanú v poli Počiatočná adresa IP. Ak sa táto adresa už používa, priradí sa ďalšia adresa IP z rozsahu. Predpokladajme, napríklad, že Počiatočná adresa je 10.1.1.1 a Počet adries je určený ako 5. Adresy oblasti vzdialených adries IP 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 adries IP, bude vždy 255.255.255.255.

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

- Viac ako jeden profil pripojenia môže špecifikovať rovnakú oblasť adries. Keď sú však použité všetky adresy v oblasti, všetky nasledujúce požiadavky o pripojenie sa odmietnu, kým sa neukončí iné pripojenie a adresa sa neuvoľní.
- 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 adries IP pre všetky prichádzajúce požiadavky o pripojenia, ktoré nevyžadujú špecifickú adresu IP.
  3. Definujte vzdialené adresy IP pre konkrétnych používateľov začiarknutím **Definovať dodatočné adresy IP na základe ID používateľa vzdialeného systému** a kliknutím na **Adresy IP definované podľa mena používateľa**.

  Keď sa pripojí vzdialený užívateľ, server iSeries zistí, či je pre tohto užívateľa zadefinovaná konkrétna IP adresa. V tomto prípade je systému daná adresa IP, inak sa vráti adresa zo spoločnej oblasti vzdialených adries.

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 pripojenia (nekomutované a komutované linky). Pre server iSeries boli zadefinované opisy najobľúbenejších modemov.

Môžete vykonať tieto úlohy konfigurácie modemu:

- Konfigurácia nového modemu
- Priradenie modemu k opisu linky
- Nastaviť príkazové reťazce modemu

Konfigurácia nového modemu

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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 opis modemu, vykonajte tieto kroky:

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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 opis 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 opis a pridať ho do zoznamu modemov.

Ak chcete vytvoriť opis modemu na základe predošlého opisu modemu, vykonajte tieto kroky:

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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 minimálnu skupinu príkazových reťazcov používaných modemami, ktoré sú zadefinované na serveri iSeries. Ekvivalentný príkazový reťazec pre svoj modem nájdete v užívateľskej príručke. V opise 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 pripojenie po *m* sekundách	S7=*m*
Typ vytáčania modemu	ATDT pre tónovú voľbu alebo ATDP pre impulzovú voľbu

Príklad: Konfigurácia terminálového adaptéra ISDN

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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
   - Ako výsledok určitých akcií obnovy po chybe, ktoré môže vykonávať server iSeries

   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 na otestovanie aktívneho stavu rozhrania *U* (ATD*x*), ktorý umožňuje serveru iSeries určiť, kedy sa dosiahla synchronizácia s ústredňou ISDN. *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 opisu na zoznam príkazov. Ku ktorémukoľvek príkazu, ktorý určíte bez priradeného parametra, môže byť priradený parameter po tom, ako sa modemu priradí opis linky.
6. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu Vlastnosti nového modemu.

Priradenie modemu k opisu linky

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services –> Originator Connection Profiles** alebo **Receiver Connection Profiles**.
2. Vyberte jednu z uvedených možností:
   - Ak chcete pracovať s už vytvoreným profilom pripojenia, pravým tlačidlom myši kliknite na profil pripojenia a vyberte **Vlastnosti**.
   - Ak chcete pracovať s novým profilom pripojenia, vytvorte ho.
3. Zo strany Vlastnosti nového profilu point-to-point vyberte panel **Pripojenie** 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 opisu tejto linky. Pri internom modeme by už mala byť patričná definícia modemu označená. Viac informácií nájdete v online pomoci.

Môžete nakonfigurovať profily pripojenia pôvodcu, aby si ″požičiavali″ linku PPP a modem priradený k profilu pripojenia príjemcu, ktorý čaká na prichádzajúce volanie. Keď sa spojenie ukončí, pôvodca pripojenia ″vráti″ linku PPP a modem profilu pripojenia príjemcu. Túto novú funkciu povolíte, ak vyberiete možnosť **Povoliť dynamické zdieľanie prostriedkov** zo záložky Modem v konfiguračnom dialógu linky PPP. Linky PPP môžete konfigurovať na záložke Pripojenie v Profiloch pôvodcu a príjemcu pripojenia.

Konfigurácia vzdialeného počítača

Ak sa chcete pripojiť k serveru iSeries z osobného počítača používajúceho ktorékoľvek 32-bitové operačné systémy Windows, overte si, či je modem správne nainštalovaný a nakonfigurovaný a skontrolujte, či ste na tento osobný počítač nainštalovali TCP/IP a Dial-Up Networking.

Informácie o konfigurovaní Dial-up Networking v PC nájdete v dokumentácii k Microsoft Windows. Nezabudnite špecifikovať alebo zadať tieto informácie:

- Typ telefonického pripojenia by mal byť **PPP**.
- Ak používate zašifrované heslá, skontrolujte, či používate MD-5 CHAP (server iSeries NEPODPORUJE MS-CHAP). Niektoré verzie systému Windows nepodporujú MD-5 priamo, ale s ďalšou pomocou od spoločnosti Microsoft je ho možné nakonfigurovať.
- Ak používate nezašifrované (alebo nezabezpečené) heslá, automaticky sa použije PAP. Server iSeries nebude podporovať žiadny ďalší typ nezabezpečeného protokolu.
- Adresovanie IP je zvyčajne zadefinované vzdialeným systémom, alebo v tomto prípade serverom iSeries. Ak máte v úmysle používať alternatívne metódy adresovania IP (napríklad chcete zadefinovať vaše vlastné adresy IP), skontrolujte, či je server iSeries nakonfigurovaný aj na akceptovanie vašej metódy adresovania.
- Pridajte adresu IP DNS, ak sa to týka vášho prostredia.

Konfigurácia prístupu na Internet cez Všeobecnú sieť AT&T

Pri komunikácii s AT&T Global Network sa vyžadujú špeciálne profily. Na prístup k tejto službe môžete použiť Sprievodcu telefonickým pripojením do AT&T Global Network, ktorý vám pomôže nakonfigurovať profil komutovaného telefonického pripojenia 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**: Umožňuje vám pravidelne načítavať poštu z jedného konta AT&T Global Network a odosielať ju na váš server iSeries, ktorý ju rozdistribuuje vašim užívateľom Lotus Mail alebo užívateľom SMTP (Simple Mail Transfer Protocol).
- **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 pripojení 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)
- 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.
- Adresy IP poštového servera a názvového servera domény pre aplikáciu výmeny pošty.
- Názov modemu, ktorý sa použije pre pripojenia jednou linkou.

Ak chcete spustiť Sprievodcu telefonickým pripojením do AT&T Global Network, postupujte podľa týchto krokov:

1. V aplikácii iSeries Navigator rozviňte svoj server a prejdite na **Network –> Remote Access Services**.
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.

IBM Universal Connection Wizard

Tento sprievodca vás povedie krokmi konfigurácie profilu, ktorý môže použiť softvér Electronic Customer Support na pripojenie k IBM. Podpora elektronickej služby poskytuje monitorovanie prostredia vášho jedinečného systému servera iSeries a dáva vám odporúčania na personalizované opravy pre váš systém a situáciu. Viac informácií o dokončení tohto sprievodcu nájdete v časti Konfigurácia univerzálneho pripojenia.

Konfigurácia skupinovej politiky prístupu

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

Ak chcete nakonfigurovať novú skupinovú politiku prístupu:

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services –> Receiver Connection Profiles**.
2. Pravým tlačidlom myši kliknite na **Skupinové politiky prístupu** a vyberte **Nová skupinová politika prístupu**.
3. Na paneli **Všeobecné** zadajte názov a opis 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 spojení vo zväzku môže byť 1 až 6. Keďže pred uskutočnením pripojenia 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 pripojenie 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. V prípade jej vybratia v podstate umožňujete serveru iSeries správať sa ako smerovač pre toto pripojenie. Toto umožňuje datagramom IP (Internet Protocol), ktoré nie sú určené pre tento iSeries, prejsť cez tento systém na pripojenú sieť. Ak toto necháte prázdne, IP (Internet Protocol) vymaže zo vzdialeného systému tie datagramy, ktoré nie sú určené pre žiadne adresy, lokálne pre tento server iSeries.

     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 systém môžete zobraziť zo záložky Všeobecné na stránke Vlastnosti IPv4.
   - Vyžadovať komprimáciu záhlavia TCP/IP (VJ)

     Táto voľba určí, či bude Internet Protocol (IP) komprimovať informáciu záhlavia potom, ako nadviaže pripojenie. 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 pripojenia. Ak opačný koniec spojenia nepodporuje komprimáciu VJ, server iSeries vytvorí spojenie, ktoré nepoužíva komprimáciu.
   - Použiť pravidlá pre pakety IP pri tomto pripojení

     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 paketov IP 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 pripojenia point-to-point pre nový **Profil príjemcu pripojenia**.

Ak chcete použiť skupinovú politiku pre používateľa vzdialeného prístupu:

1. Kliknite na stranu **Autentifikácia**.
2. Začiarknutím **Require this iSeries server skontrolujte identitu vzdialeného systému**.
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 pripojenia point-to-point.

Použitie pravidiel filtrovania paketov IP na pripojenie PPP

Téma Filtrovanie paketov IP a pravidlá NAT v Informačnom centre rozoberá, ako vytvoriť pravidlá paketov IP, na ktoré sa môžete odvolať z profilu pripojenia PPP. Na obmedzenie prístupu užívateľov alebo skupín k adresám IP vo vašej sieti môžete použiť súbor pravidiel pre pakety. 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 paketov IP sa môžete odkázať dvojako:

- Úroveň profilu pripojenia
  1. Keď vyplníte **Vlastnosti point-to-point** pre **Profil pripojenia príjemcu**, vyberte stranu Nastavenia TCP/IP a kliknite na **Rozšírené**.
  2. Kliknite na **Použiť pravidlá pre pakety IP pri tomto pripojení** a zo sťahovacieho zoznamu vyberte identifikátor filtra PPP.
  3. Kliknutím na **OK** aplikujete filter PPP na profil pripojenia.
- 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 pakety IP pri tomto pripojení** 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 povoliť služby RADIUS alebo DHCP pre profily pripojenia príjemcu PPP:

1. V aplikácii iSeries Navigator vyberte svoj server a rozviňte **Network –> Remote Access Services**.
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 vráťte do aplikácie iSeries Navigator.

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

Spravovanie PPP

Uvádzame úlohy riadenia PPP, ktoré môžete vykonávať na serveri iSeries:

- Nastavenie vlastností profilov pripojenia
- Monitorovanie aktivity PPP

Nastavenie vlastností profilov pripojenia PPP

Pri vytváraní profilu pripojenia si väčšinou v dialógovom okne Nastavenie profilu pripojenia 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 pripojenia. Voľby, ktoré zadáte v dialógovom okne Nastavenie profilu pripojenia point-to-point určujú obsah stránky vlastností profilu pripojenia a zoradenie panelov na nej. Stránka vlastností je iná pre profily pôvodcu a iná pre profily príjemcu pripojenia.

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 pripojenia, ktoré konfigurujete. V online pomoci pre aplikáciu iSeries Navigator nájdete opis každej voľby, ktorá sa zobrazí v dialógovom okne. Viac informácií nájdete aj v príkladoch a postupoch pre PPP.

Monitorovanie aktivity PPP

Táto stránka vysvetľuje, ako sa použitím aplikácie iSeries Navigator prezerá profil pripojenia a protokol relácie.

Informácie o úlohách pripojenia PPP:

- Existujú dve kontrolné úlohy PPP, ktoré sa používajú na riadenie individuálnych úloh pripojení PPP. Tieto úlohy sa vykonávajú v podsystéme QSYSWRK:
  - QTPPPCTL - hlavná kontrolná úloha PPP. Táto úloha riadi každú úlohu pripojenia PPP.
  - QTPPPL2TP - L2TP server. Táto úloha spravuje založenie tunela L2TP a spúšťa sa, len ak je práve spustený profil L2TP.
- Úlohy pripojenia PPP sa vykonávajú pod užívateľským profilom QTCP a používajú sa na spracovanie každého jednotlivého pripojenia 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 pripojenia PPP:
  - QTPPPSSN - táto úloha sa používa na spracovanie všetkých pripojení PPP okrem spojení typu L2TP.
  - QTPPPL2SSN - táto úloha sa používa na spracovanie virtuálnych údajov PPP potom, ako QTPPPL2TP úspešne dohodne vytvorenie tunela L2TP.
- Úlohy pripojenia 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 pripojení:

1. V aplikácii iSeries Navigator rozviňte svoj server a prejdite na **Network –> Remote Access Services**. Vyberte **Profil pripojenia pôvodcu** alebo **Profil pripojenia príjemcu**.
2. V stĺpci Profil kliknite pravým tlačidlom myši na názov profilu pripojenia a vyberte jednu z nasledujúcich volieb:

- **Úlohy** - otvorí protokol úloh pre úloh QTPP*xxx*.
- **Pripojenia** - otvorí dialógové okno, zobrazujúce informácie o všetkých spojeniach priradených danému profilu. Môže ísť o údaje o aktuálnom pripojení, predchádzajúcich pripojeniach alebo o aktuálnych aj predchádzajúcich pripojeniach. Sú dostupné voľby pre zobrazenie výstupu úlohy alebo detailov o pripojení pre každé pripojenie.
- **Vlastnosti** - otvorí strany Vlastností na zobrazenie aktuálnych vlastností pre pripojenie.

Prezeranie informácií o pripojení:

1. V aplikácii iSeries Navigator rozviňte svoj server a prejdite na **Network –> Remote Access Services**. Vyberte **Profil pripojenia pôvodcu** alebo **Profil pripojenia príjemcu**.
2. V stĺpci Profil kliknite pravým tlačidlom na názov profilu pripojenia, ktorý nemá stav Neaktívny a vyberte **Pripojenia**, aby ste si mohli prezrieť informácie o pripojení.

   Zobrazí sa každé pripojenie pre tento profil (aktuálne aj predchádzajúce). Stavové pole označuje aktuálny stav pripojenia. V závislosti od stavu každej úlohy PPP možno zobraziť aj dodatočné informácie, napríklad ID používateľa pripojeného používateľa, lokálnu a vzdialenú adresu IP a názov úlohy PPP.
3. Ak si chcete prezerať výstup úlohy alebo podrobnosti o pripojení, pravým tlačidlom myši kliknite na pripojenie 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 pripojenia a protokolov úloh (pri ukončených reláciách).
5. Ak si chcete prezrieť podrobnosti o pripojení, kliknite na **Podrobnosti**. Možno zobraziť len podrobnosti o aktuálne aktívnych pripojeniach. Dialógové okno Podrobnosti vám umožní prezerať si dodatočné informácie o pripojení pre konkrétne pripojenie.

Práca s výstupom PPP zo servera iSeries:

Ak chcete pracovať s výstupom PPP, v príkazovom riadku servera iSeries zadajte 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 pripojenia, vyberte pri tomto profile **voľbu 8** (Práca s výstupom).
- Ak chcete tlačiť konfiguráciu profilu PPP, vyberte pri tomto profile **voľbu 6** (Tlač). Potom pomocou príkazu WRKSPLF pristúpte k vytlačenému výstupu.

Stav pripojenia:

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 Pripojenia.

Primárny opis stavu	**Vysvetlenie**
Čaká sa na požiadavky na pripojenie	Profil príjemcu je pripravený na pripojenie
Čaká sa na prichádzajúce volanie	Server je pripravený na pripojenie
Spája sa	Prebieha proces spájania so vzdialeným systémom
Aktívne/Aktívne pripojenia	Pripojenie sa vytvorilo a úloha sa úspešne vykonáva
Neaktívne	Pre tento profil pripojenia 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 telefonického 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	Pripojenie 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 adresy IP	pre problémy pri získavaní adresy IP 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

Odstraňovanie problémov s PPP

Aktuálne a relevantné informácie o PTF (program temporary fixes) a odstraňovaní problémov sú zdokumentované na domovskej stránke TCP/IP servera iSeries . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a aktualizujú informácie, uvedené v tejto téme.

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

1. Požadovaný podporný materiál:
   - Typ vzdialeného hostiteľa, operačný systém a úroveň
   - Úroveň operačného systému hostiteľa servera iSeries
   - Protokol úloh neúspešnej relácie a protokol telefonického pripojenia

     Protokoly úloh a výstup dialógového okna pripojenia sa ukladá do OUTQ s rovnakým názvom ako profil.
   - Skript pripojenia, ak sa používa vo vašom prostredí.
   - Stav profilu pripojenia pred a po zlyhaní spojenia
2. Odporúčaný podporný materiál:
   - Opis linky
   - Profil pripojenia

     Voľba 6 z WRKTCPPTP vytlačí nastavenia profilu.
   - Typ modemu a model
   - Príkazové reťazce modemu
   - Sledovanie komunikácií

V ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) nájdete množstvo informácií o nasledujúcich problémoch 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 používať, nie je v preddefinovanom zozname modemov v aplikácii iSeries Navigator.	Vytvorte nový modem.
Používatelia a heslá PPP Keď sa pokúšate nadviazať pripojenie 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 pripojenia Identifikované linky PPP používajú rovnaký hardvérový prostriedok.	Nezabudnite vypnúť ostatné linky, používajúce ten istý hardvérový prostriedok.
Protokol PPP Chyby pri pripojení 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.

Ďalšie informácie o PPP

Iné zdroje informácií o PPP:

- Najnovšie PTF (program temporary fixes) a najnovšie konfiguračné informácie pre PPP a L2TP nájdete cez odkaz PPP na domovskej stránke TCP/IP servera iSeries  . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a nahrádzajú informácie uvedené v téme **Služby vzdialeného prístupu: Pripojenia PPP**.
- V ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  nájdete množstvo informácií o službách a aplikáciách TCP/IP.
- ITSO Redbook iSeries IP Networks: Dynamic! (SG24-6718)  obšírne opisuje služby a aplikácie TCP/IP.

Príloha. Poznámky

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Informácie o produktoch a službách aktuálne dostupných vo vašej krajine získate od lokálneho zástupcu spoločnosti IBM. Žiadne odkazy na produkt, program alebo službu spoločnosti IBM neznamenajú, ani z nich nevyplýva, že musí byť použitý len tento produkt, program alebo služba spoločnosti IBM. Namiesto nich môže byť použitý akýkoľvek funkčne ekvivalentný produkt, program alebo služba, ktoré neporušujú právo na duševné vlastníctvo spoločnosti IBM. Za zhodnotenie a overenie činnosti akéhokoľvek produktu, programu alebo služby, ktoré nie sú od spoločnosti IBM, je však zodpovedný užívateľ.

Spoločnosť IBM môže mať patenty alebo nevybavené žiadosti o patenty týkajúce sa predmetných záležitostí opísaných v tomto dokumente. Poskytnutie tohto dokumentu vám neudeľuje žiadne licencie na tieto patenty. Žiadosti o licencie môžete zasielať písomne na:

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

Požiadavky na licencie, týkajúce sa dvojbajtových znakových sád (DBCS), posielajte oddeleniu duševného vlastníctva spoločnosti IBM vo vašej krajine, alebo pošlite písomné požiadavky na adresu:

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

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s lokálnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE" BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK NEPOŠKODENIA, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nedovoľujú zriecť sa vyjadrených alebo implikovaných záruk v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie môžu obsahovať technické nepresnosti alebo typografické chyby. Tu uvádzané informácie sa periodicky menia; tieto zmeny budú začleňované do nových vydaní publikácie. V produktoch a/alebo v programoch opísaných v tejto publikácii môže spoločnosť IBM bez upozornenia kedykoľvek vykonať vylepšenia a/alebo zmeny.

Všetky odkazy v týchto informáciách na webové lokality iné ako od IBM sú poskytnuté len pre pohodlie a v žiadnom prípade neslúžia ako potvrdenie obsahu týchto webových lokalít. Materiály na týchto webových stránkach nie sú súčasťou materiálov pre tento produkt IBM a tieto webové stránky používate na vaše vlastné riziko.

Spoločnosť IBM môže ktorúkoľvek z vami poskytnutých informácií použiť alebo distribuovať spôsobom, ktorý považuje za správny, bez toho, aby jej voči vám z toho vyplynul akýkoľvek záväzok.

Vlastníci licencií na tento program, ktorí chcú o ňom získať informácie za účelom povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto) a (ii) vzájomného použitia vymieňaných informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť dostupné, môžu byť predmetom príslušných pojmov a podmienok a v niektorých prípadoch sú dostupné za poplatok.

Licenčný program opísaný v týchto informáciách a všetok licenčný materiál, ktorý je preň dostupný, poskytla spoločnosť IBM za podmienok Zákazníckej zmluvy IBM, Medzinárodnej dohody o licenčných programoch IBM, Licenčnej dohody o počítačovom kóde IBM alebo inej ekvivalentnej dohody medzi nami.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

Ochranné známky

Nasledujúce pojmy sú ochranné známky spoločnosti International Business Machines v USA, v iných krajinách alebo v oboch:

AT
e (logo)Server
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro sú ochrannými známkami spoločností International Business Machines Corporation a Lotus Development Corporation v USA, iných krajinách alebo v oboch.

Microsoft, Windows, Windows NT, Windows NT a logo Windows sú ochrannými známkami spoločnosti Microsoft Corporation v USA, iných krajinách alebo v oboch.

Java a všetky ochranné známky založené na Java sú ochranné známky spoločnosti Sun Microsystems v USA, v iných krajinách alebo v oboch.

UNIX je registrovaná ochranná známka spoločnosti The Open Group v USA a iných krajinách.

Ostatné názvy spoločnosti, produktov alebo služieb môžu byť ochranné známky alebo značky služieb iných.

Pojmy a podmienky pre preberanie a tlač publikácií

Povolenia na používanie informácií, ktoré ste si vybrali na stiahnutie, sa udeľujú v závislosti od vášho akceptovania nasledujúcich podmienok.

Osobné použitie: Tieto informácie smiete reprodukovať pre vaše osobné, nekomerčné používanie za podmienky, že budú zachované všetky oznamy týkajúce sa vlastníctva. Bez súhlasu spoločnosti IBM nesmiete tieto informácie distribuovať, zobrazovať alebo vyrábať z nich alebo z ich častí odvodeniny.

Komerčné použitie: Tieto informácie smiete reprodukovať, distribuovať a zobrazovať výlučne v rámci vášho podniku za podmienky, že budú zachované všetky oznamy týkajúce sa vlastníctva. Bez súhlasu spoločnosti IBM nesmiete vyrábať z týchto informácií odvodeniny alebo tieto informácie alebo ich časti reprodukovať, distribuovať alebo zobrazovať mimo vášho podniku.

Okrem toho, čo je výslovne udelené v tomto povolení, sa neudeľujú žiadne ďalšie povolenia, licencie alebo práva, buď vyjadrené alebo implikované, na informácie ani žiadne údaje, softvér alebo ďalšie intelektuálne vlastníctvo v nich obsiahnuté.

Spoločnosť IBM si vyhradzuje právo podľa vlastného uváženia kedykoľvek odobrať tu uvedené povolenia, ak použitie týchto informácií škodí jej záujmom alebo ako stanovuje IBM, hore uvedené inštrukcie sa nedodržujú správne.

| Tieto informácie nemôžete prevziať ani exportovať okrem prípadu, ak to dovoľujú všetky aplikovateľné zákony a
| regulácie, vrátane všetkých zákonov a regulácií USA pre export. IBM NEDÁVA ZÁRUKU NA OBSAH TÝCHTO
| INFORMÁCIÍ. TIETO INFORMÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ A BEZ ZÁRUKY AKÉHOKOĽVEK
| DRUHU, BUĎ VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE)
| IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA ALEBO VHODNOSTI NA KONKRÉTNY
| ÚČEL.

| Pri sťahovaní alebo tlači informácií z tejto lokality ste uviedli, že súhlasíte týmito podmienkami.

Vytlačené v USA