Systémy IBM - iSeries

Práca v sieti
Služby vzdialeného prístupu: Pripojenia PPP

Verzia 5, vydanie 4

Systémy IBM - iSeries

Práca v sieti
Služby vzdialeného prístupu: Pripojenia PPP

Verzia 5, vydanie 4

Poznámka

Pred použitím týchto informácií a nimi podporovaného produktu si prečítajte informácie v časti “Poznámky”, na strane 65.

Siedme vydanie (február 2006)

Toto vydanie sa týka verzie 5, vydania 4, modifikácie 0 produktu i5/OS (číslo produktu 5722–SS1) a všetkých nasledujúcich vydaní a modifikácií, ak nie je v nových vydaniach určené 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 PPP (Point-to-Point) je internetový štandard pre prenos údajov po sériových linkách.

Je to najčastejšie používaný protokol medzi poskytovateľmi internetových služieb (ISP). PPP umožňuje individuálnym počítačom pripojenie k sieťam, ktoré ďalej poskytnú prístup na Internet. Server IBM iSeries obsahuje podporu TCP/IP PPP ako súčasť podpory rozľahlej počítačovej siete (WAN).

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. Váš server iSeries tiež môžete nakonfigurovať na pripojenie k Internetu cez PPP. Sprievodca telefonickým pripojením v Navigátore iSeries vás prevedie procesom pripojenia vášho servera iSeries k Internetu alebo internej sieti.

Novinky vo V5R4

Táto téma opisuje zmenené funkcie v službách vzdialeného prístupu: Pripojenia PPP pre V5R4.

Zmenené funkcie

- **Protokol volaní**

  Protokoly volaní sú dôležité záznamy o údajoch, ktoré tečú do alebo z modemu počas relácie PPP. Ukladajú a mažú sa na základe parametra OUTPUT (*ERROR, *PRINT alebo *NONE) príkazu STRTCPPTP (Start TCP/IP Point-to-Point).

  V predošlých vydaniach, súbory protokolov volaní v odkladacej oblasti boli nazvané call log*nnnnnn*, kde *nnnnnn* bolo číslo úlohy *nnnnnn*/QTCP/QTPPPSSN.

  Vo V5R4, všetky relácie PPP sa vykonávajú vo vlákne *nnnnnn*/QTCP/QTPPPCTL. Súbory protokolov volaní v odkladacej oblasti sú nazvané CL*mmmmmmmm*, kde *mmmmmmmm* je ID vlákna. Toto vám dovoľuje párovať správy relácie v protokole úloh QTPPPCTL (ktoré obsahujú pole Vlákno .... 00000028) so zodpovedajúcim protokolom volaní.

- **QTPPPSSN a QTPPPL2SSN**
  - Úlohy QTPPPSSN a QTPPPL2SSN (L2TP) sú úlohy relácie PPP vo vydaniach starších ako IBM i5/OS V5R4. Spúšťali a ukončovali sa príkazmi STRTCPPTP a ENDTCPPTP (End Point-to-Point TCP/IP) alebo cez QTPPPL2TP pri vytvorení alebo ukončení tunela. Dajú sa spustiť alebo ukončiť aj automaticky pri spustení alebo ukončení liniek cez protokol viacnásobnej linky.

    Od V5R4, PPP už nepoužíva úlohy QTPPPSSN a QTPPPL2SSn. Relácie sa vykonávajú ako vlákna v QTPPPCTL.
  - Vo vydaniach starších ako i5/OS V5R4, voľba 14 (Pracovať s úlohou) príkazu WRKTCPPTP (Work with Point-to-Point TCP/IP Profiles) vytvorila aktívnu úlohu relácie. Príležitostne spustí QTPPPL2TP, ak pre profil L2TP nebola žiadna aktívna relácia PPP.

    Vo V5R4, voľba 14 príkazu WRKTCPPTP spustí QTPPPCTL, ak je v danej úlohe aktívne vlákno relácie.
- **Protokol správ**

  Vo V5R4 existuje nový súbor protokolu správ v odkladacej oblasti pre správy relácie. Zhromažďuje správy z vlákna relácie, správy z úvodného vlákna, ktoré sú výsledkom práce v mene relácie, a správy zo spustených procesov do súboru v odkladacej oblasti.

  Súbor protokolu správ v odkladacej oblasti je nazvaný ML*mmmmmmmm*, kde *mmmmmmmm* je ID vlákna. Toto dovoľuje párovať protokoly volaní, protokoly správ a správy relácie v protokole úloh QTPPPCTL (ktoré majú pole Vlákno .... 00000028).
- **QTPPPCTL a QTPPPL2TP**

| Vo V5R4, úloha QTPPPCTL používa viacero systémových vlákien na vykonávanie relácií ako vlákien namiesto samostatných procesov (QTPPPSSN a QTPPPL2SSN).

| Úloha QTPPPCTL spustí vlákna sekundárnej relácie a spojenia, ktoré nahrádzajú staré úlohy relácie a spojenia QTPPPSSN a QTPPPL2SSN.

| Úloha QTPPPCTL je vrátená do aplikačných programových rozhraní (API) a GUI Navigátora iSeries pri požiadaní o úlohy relácie.

| • **Ethernetové adaptéry**

| Vo V5R4, zoznam ethernetových adaptérov s podporou PPPoE je rozšírený o ethernetové adaptéry typov 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 a 573A.

| • **PPPoE**

| Vo V5R4, PPPoE môže zdieľať rovnaký adaptér ako premávka IPv4 a IPv6.

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 časť Poznámka pre užívateľov.

Vytlačitelné PDF

Podľa týchto pokynov môžete zobraziť a vytlačiť tieto informácie vo formáte PDF

Ak chcete zobraziť alebo prevziať verziu PDF tohto dokumentu, vyberte Služby vzdialeného prístupu: Pripojenia PPP

 (približne 940 KB).

Iné informácie

Môžete tiež zobraziť alebo vytlačiť ktorúkoľvek z týchto informácií:

- Manuály:
  - Nájdite najnovšie dočasné opravy programov (PTF) a najnovšie informácie o konfigurovaní PPP a L2TP cez linku PPP na domovskej stránke TCP/IP pre server iSeries  . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a aktualizujú informácie, uvedené v tejto kolekcii tém.
- IBM Redbooks:
  - ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  opisuje služby a aplikácie TCP/IP.
  - ITSO Redbook iSeries IP Networks: Dynamic! (SG24-6718)  opisuje služby a aplikácie TCP/IP.

Ukladanie súborov PDF

Ak chcete vo svojej pracovnej stanici uložiť súbor PDF za účelom zobrazenia alebo tlače:

1. Kliknite pravým tlačidlom na PDF vo vašom prehliadači (pravým tlačidlom kliknite na odkaz hore).
2. Kliknite na voľbu, ktorá uloží súbor PDF lokálne.
3. Prejdite do adresára, kde chcete uložiť súbor PDF.
4. Kliknite na tlačidlo **Uložiť**.

Prevzatie programu Adobe Reader

Ak chcete zobraziť alebo vytlačiť tieto dokumenty PDF, vo vašom systéme musíte mať nainštalovaný program Adobe Reader. Bezplatnú kópiu tohto programu môžete prevziať z webovej lokality Adobe

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

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.

Súvisiaci odkaz

"Súvisiace informácie pre PPP" na strane 64
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Čo je PPP?

Protokol Point-to-Point (PPP) je protokol TCP/IP používaný na pripojenie jedného počítačového systému k inému. Počítače používajú **PPP** alebo **Point-to-Point Protocol** na komunikáciu cez telefónnu sieť alebo Internet.

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 dokumentoch RFC nájdete na webovej stránke RFC Editor.

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

Profily pripojení

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.

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

- **Profily pripojenia pôvodcu** 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 (Serial Line Internet Protocol))

- 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
- Vzdialené telefónne čísla a voľby vytáčania
- Autentifikácia
- Nastavenia TCP/IP: Adresy IP a 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 použitie PPP vždy, keď to je možné.
- **Výber režimu**. Typ pripojenia a prevádzkový režim pre tento profil pripojenia.

  Typ pripojenia určuje typ linky, na ktorej sa realizujú vaše pripojenia a či **vytáčajú číslo** (pôvodca) alebo **odpovedajú** (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. Pozrite si tieto tabuľky:

  V nasledujúcej tabuľke nájdete profily pripojenia pôvodcu:

Tabuľka 1. Dostupné režimy prevádzky pre profily pripojenia pôvodcu

Typ pripojenia	Dostupné režimy prevádzky
Komutovaná linka	• Vytáčanie • Vytáčať na žiadosť (len vytáčanie) • Vytáčať na žiadosť (rovnocenná strana s povoleným odpovedaním • Vytáčať na žiadosť (Povolený vzdialený rovnocenný počítač)
Prenajatá linka	Pôvodca
L2TP	• Pôvodca • Viacskokový iniciátor • Vzdialené telefonické pripojenie
PPP cez Ethernet	Pôvodca

V nasledujúcej tabuľke nájdete profily pripojenia príjemcu:

Tabuľka 2. Dostupné režimy prevádzky pre profily pripojenia príjemcu

Typ pripojenia	Dostupné režimy prevádzky
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 ostatné typy pripojení (prenajaté, L2TP, PPPoE) môžete ako službu linky vybrať len Jedna linka.

  Súvisiaci odkaz

  “Softvérové a hardvérové požiadavky” na strane 32
  Prostredie PPP vyžaduje, aby ste mali dva alebo viac počítačov, ktoré podporujú PPP. Jeden z týchto počítačov, server iSeries, môže byť buď pôvodca, alebo príjemca.

Podpora skupinových politík

Podpora skupinových politík dovoľuje administrátorom siete definovať skupinové politiky podľa užívateľov, ktoré pomáhajú manažovať prostriedky a dovoľujú priraďovanie politík riadenia prístupu k jednotlivým užívateľom pri prihlasovaní do siete cez reláciu PPP alebo L2TP.

Užívatelia môžu byť identifikovaní ako členovia špecifickej triedy užívateľov, pričom každá trieda má svoju jedinečnú 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 skupinových politík môžu administrátori siete definovať napríklad skupinu Work_at_Home, ktorá poskytuje danej triede užívateľov úplný prístup do siete, kým skupina Vendor_Workers môže byť obmedzená na limitovanú množinu služieb.

Súvisiaci odkaz

“Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE” na strane 11
Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

“Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie” na strane 24
Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Scenáre

Scenáre v tejto téme vám pomôžu porozumieť fungovaniu PPP a spôsobu implementácie prostredia PPP vo vašej sieti. Tieto scenáre vám priblížia základné koncepty PPP, ktoré môžu byť užitočné pre začiatočníkov i skúsených používateľov pri plnení úloh plánovania a konfigurácie.

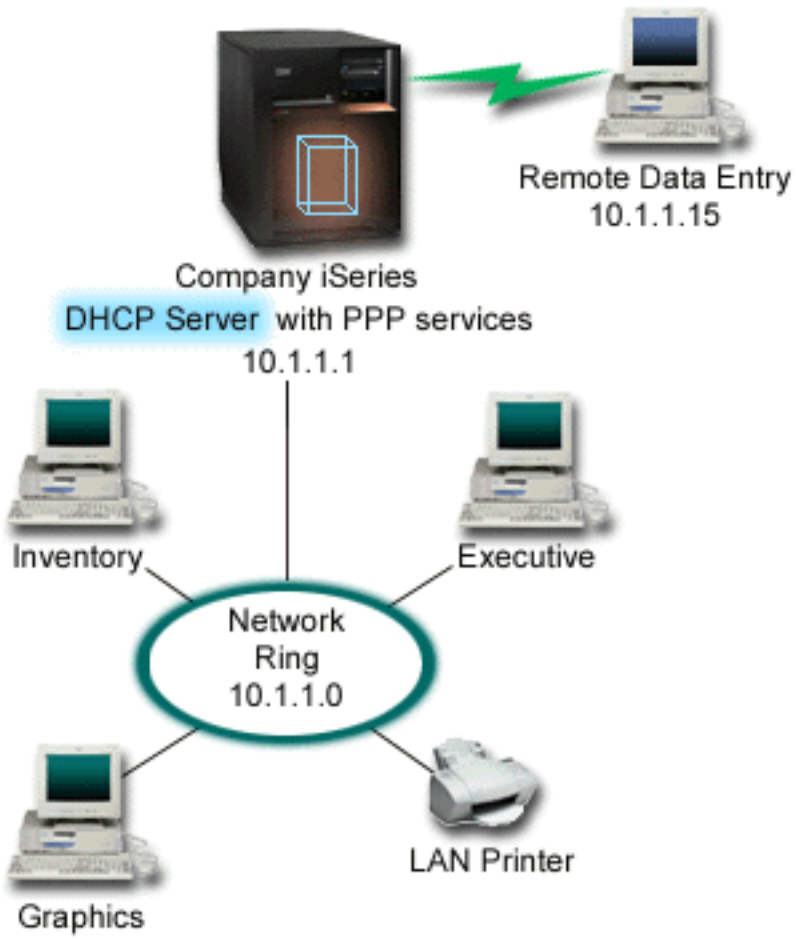
Súvisiaci odkaz

“Súvisiace informácie pre PPP” na strane 64
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Príklad: PPP a DHCP v jednom serveri iSeries

Dozviete sa tu, ako nastaviť server iSeries ako server DHCP pre LAN a vzdialených telefonicky pripájaných klientov.

Vzdialení klienti, napríklad klienti s telefonickým pripojením, často vyžadujú prístup do firemnej siete. Klienti s telefonickým pripojením často získajú prístup k serveru iSeries cez PPP. Na sprístupnenie siete bude klient s telefonickým pripojením potrebovať informácie o IP, rovnako ako priamo pripojení sieťoví klienti. Server DHCP iSeries môže distribuovať informácie o adrese IP klientovi s telefonickým pripojením PPP rovnako, ako ľubovoľnému inému priamo pripojenému klientovi. Nasledujúci obrázok znázorňuje vzdialeného zamestnanca, ktorý sa potrebuje telefonicky pripojiť k firemnej sieti a vykonať svoju prácu.



Obrázok 1. PPP a DHCP v jednom serveri iSeries

Ak sa má vzdialený zamestnanec úspešne stať súčasťou firemnej siete, server iSeries musí použiť kombináciu služieb vzdialeného prístupu a DHCP. Funkcia Služby vzdialeného prístupu vytvorí podporu pre telefonické pripojenia v serveri iSeries. Ak je správne nastavená, po vytvorení telefonického pripojenia pracovníkom, server PPP povie serveru DHCP, aby poslal pracovníkovi informácie TCP/IP.

V tomto príklade jedna politika podsiete DHCP pokrýva priamo pripojených klientov, ako aj klientov s telefonickým pripojením.

Ak chcete, aby profil PPP oneskoril oznámenie žiadosti pre DHCP o distribúciu IP, musíte to spraviť v profile PPP. V nastaveniach TCP/IP v profile pripojenia prijímača musíte nastaviť metódu priradenia vzdialenej adresy IP z Pevná na DHCP. Ak chcete povoliť klientom s telefonickým pripojením komunikovať s ostatnými klientmi siete, napríklad so

sieťovou tlačiarňou, musíte tiež povoliť postupovanie IP vo vlastnostiach TCP/IP profilu a vo vlastnostiach konfigurácie TCP/IP (zásobníka). Ak nastavíte postupovanie IP len v profile PPP, server iSeries nebude postupovať pakety IP. Postupovanie IP musíte nastaviť aj v profile, aj v zásobníku.

Okrem toho, adresa IP lokálneho rozhrania v profile PPP musí byť adresa IP, ktorá patrí do definície podsiete v serveri DHCP. V tomto príklade by mala byť adresa lokálneho rozhrania 10.1.1.1. Táto adresa by mala byť vylúčená z oblasti adries servera DHCP, aby nebola priradená klientovi DHCP.

Plánovanie nastavenia DHCP pre priamo pripojených klientov a klientov PPP

Tabuľka 3. Globálne konfiguračné voľby (týka sa všetkých klientov, ktorých obsluhuje server DHCP)

Objekt		**Hodnota**
Konfiguračné voľby	voľba 1: Maska podsiete	255.255.255.0
	voľba 6: Názvový server domén	10.1.1.1
	voľba 15: Názov domény	mycompany.com
Vykonáva server aktualizácie DNS?		Nie
Podporuje server klientov BOOTP?		Nie

Tabuľka 4. Podsieť pre priamo pripojených klientov a klientov s telefonickým pripojením

Objekt		**Hodnota**
Názov podsiete		MainNetwork
Adresy na manažovanie		10.1.1.3 - 10.1.1.150
Čas prenájmu		24 hodín (predvolené)
Konfiguračné voľby	Zdedené voľby	Voľby z globálnej konfigurácie
Adresy podsiete, ktoré server neprirađuje		10.1.1.1 (adresa lokálneho rozhrania, ktorá je zadaná v Nastaveniach TCP/IP vo vlastnostiach profilu pripojenia prijímača v Navigátore iSeries)

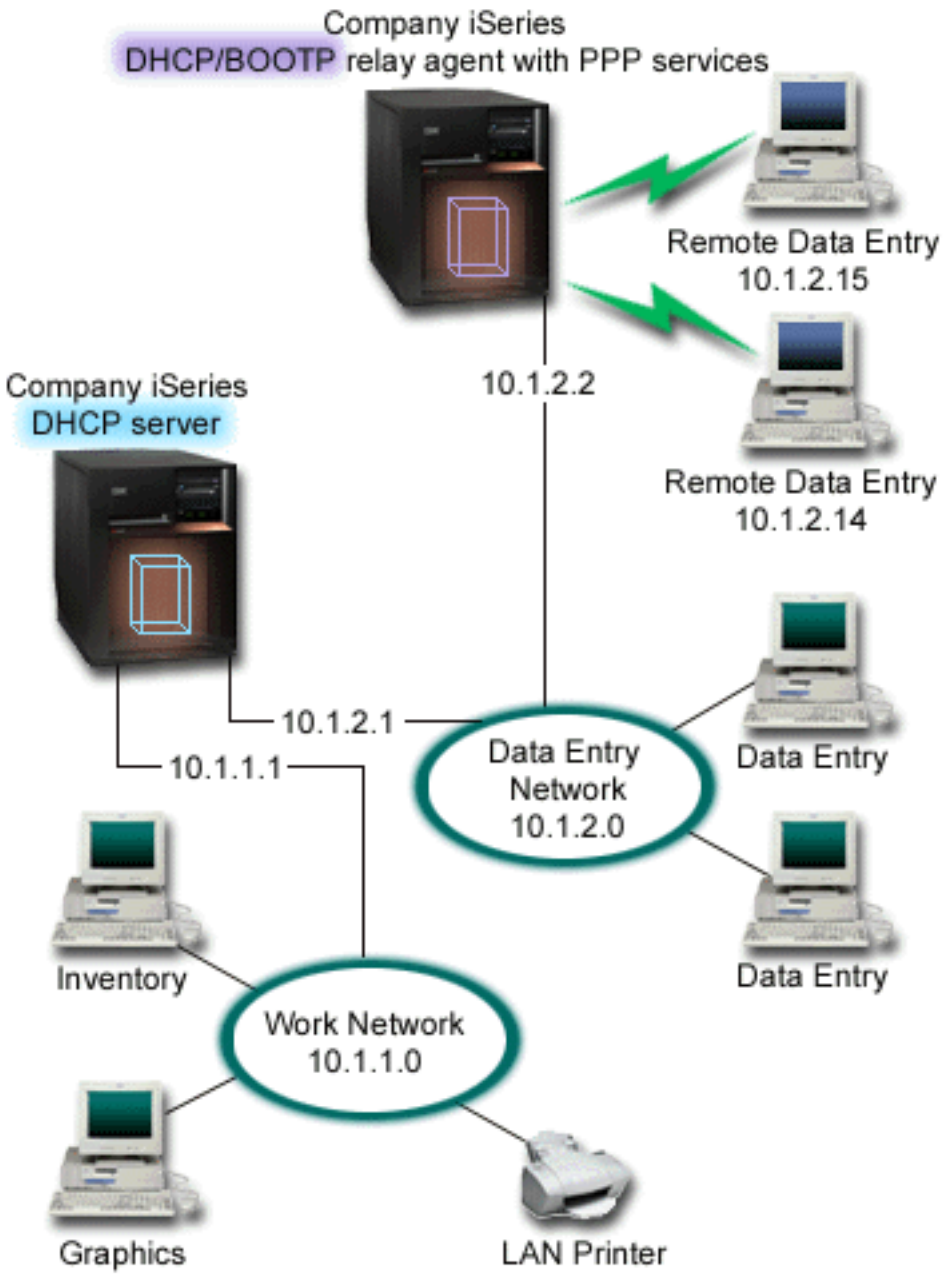
Iné nastavenie

- V profile pripojenia prijímača PPP nastavte metódu vzdialenej adresy IP na DHCP.
  1. Povoľte pripojenie klienta DHCP WAN so serverom DHCP alebo prenosovým pripojením pomocou položky ponuky Služby pre Služby vzdialeného prístupu v Navigátore iSeries.
  2. Vyberte DHCP pre metódu prideľovania adries IP pod Vlastnosti nastavení TCP/IP v Profile pripojenia prijímača v Navigátore iSeries.
- Povoľte vzdialenému systému prístup k iným sieťam (postupovanie IP) vo Vlastnostiach nastavení TCP/IP v profile pripojenia prijímača v Navigátore iSeries.
- Povoľte postupovanie datagramov IP pod Vlastnosti nastavení v Konfigurácii TCP/IP v Navigátore iSeries.

Príklad: Profil DHCP a PPP na odlišných serveroch iSeries

Dozviete sa tu, ako nastaviť dva servery iSeries ako sieťový server DHCP a prenosový agent DHCP/BOOTP pre dve siete LAN a klientov, ktorí využívajú vzdialené telefonické pripojenie.

Predošlý príklad, PPP a DHCP v jednom serveri iSeries, ukazuje spôsob použitia PPP a DHCP v jednom serveri iSeries na povolenie prístupu klientov s telefonickým pripojením do siete. Bez ohľadu na fyzickú štruktúru vašej siete a bezpečnostné aspekty, môže byť vhodnejšie mať servery PPP a DHCP oddelené alebo mať vyhradený server PPP bez služieb DHCP. Nasledujúci obrázok znázorňuje sieť, ktorá má klientov s telefonickým pripojením, ale politiky PPP a DHCP sú na rôznych serveroch.



Obrázok 2. Profil DHCP a PPP na rôznych serveroch iSeries

Klienti Remote Data Entry používajú telefonické pripojenie k serveru PPP iSeries. Profil PPP v tomto serveri musí mať ako metódu vzdialenej adresy IP nastavené DHCP, ako v predošlom príklade, a tiež nastavené postupovanie IP v profile PPP a vlastnostiach zásobníka TCP/IP. Okrem toho, tento server vystupuje ako prenosový agent DHCP, preto musí byť zapnutý server TCP/IP prenosového agenta BOOTP/DHCP. Toto dovoľuje serveru iSeries pre vzdialený prístup odovzdať pakety DHCP DISCOVER serveru DHCP. Server DHCP následne odpovie a distribuuje informácie o TCP/IP telefonicky pripojeným klientom cez server PPP.

Server DHCP zodpovedá za distribuovanie adries IP do sietí 10.1.1.0 a 10.1.2.0. V sieti Vstup údajov bude prideľovať adresy IP od 10.1.2.10 do 10.1.2.40 klientom s telefonickým pripojením alebo priamo pripojeným klientom. Klienti v sieti Vstup údajov tiež potrebujú adresu smerovača (voľba 3) 10.1.2.1, aby mohli komunikovať so sieťou a server DHCP iSeries musí mať tiež povolené postupovanie IP.

Okrem toho, adresa IP lokálneho rozhrania v profile PPP musí byť adresa IP, ktorá patrí do definície podsiete v serveri DHCP. V tomto príklade by mala byť adresa lokálneho rozhrania 10.1.2.2. Táto adresa by mala byť vylúčená z oblasti adries servera DHCP, aby nebola priradená klientovi DHCP. Adresa IP lokálneho rozhrania musí byť adresa, na ktorú môže server DHCP posielať pakety s odpoveďami.

Plánovanie nastavenia DHCP pre DHCP s prenosovým agentom DHCP

Tabuľka 5. Globálne konfiguračné voľby (týka sa všetkých klientov, ktorých obsluhuje server DHCP)

Objekt		**Hodnota**
Konfiguračné voľby	voľba 1: Maska podsiete	255.255.255.0
	voľba 6: Názvový server domén	10.1.1.1
	voľba 15: Názov domény	mycompany.com
Vykonáva server aktualizácie DNS?		Nie
Podporuje server klientov BOOTP?		Nie

Tabuľka 6. Podsieť pre Work Network

Objekt		**Hodnota**
Názov podsiete		WorkNetwork
Adresy na manažovanie		10.1.1.3 - 10.1.1.150
Čas prenájmu		24 hodín (predvolené)
Konfiguračné voľby	Zdedené voľby	Voľby z globálnej konfigurácie
Adresy podsiete, ktoré server nepriraďuje		žiadne

Tabuľka 7. Podsieť pre sieť Data Entry

Objekt		**Hodnota**
Názov podsiete		DataEntry
Adresy na manažovanie		10.1.2.10 - 10.1.2.40
Čas prenájmu		24 hodín (predvolené)
Konfiguračné voľby	voľba 3: Smerovač	10.1.2.1
	Zdedené voľby	Voľby z globálnej konfigurácie
Adresy podsiete, ktoré server nepriraďuje		10.1.2.1 (smerovač) 10.1.2.15 (Adresa IP lokálneho rozhrania Remote vzdialeného klienta Data Entry) 10.1.2.14 (Adresa IP lokálneho rozhrania Remote vzdialeného klienta Data Entry)

Iné nastavenie servera iSeries s PPP

- Nastavenie servera TCP/IP prenosového agenta BOOTP/DHCP

Objekt	**Hodnota**
Adresa rozhrania	10.1.2.2
Adresa IP pre prenos paketov do servera	10.1.2.1

- Nastavte metódu vzdialenej adresy IP na DHCP v profile pripojenia prijímača PPP
  1. Povoľte pripojenie klienta DHCP WAN so serverom DHCP alebo prenosovým pripojením pomocou položky ponuky Služby pre Služby vzdialeného prístupu v Navigátore iSeries

2. Vyberte DHCP pre metódu prideľovania adries IP pod Vlastnosti nastavení TCP/IP v Profile pripojenia prijímača v Navigátore iSeries

- Povoľte vzdialenému systému prístup k iným sieťam (postupovanie IP) pod Vlastnosti nastavení TCP/IP v Profile pripojenia prijímača v Navigátore iSeries (aby ste povolili vzdialeným klientom komunikovať so sieťou Vstup údajov)
- Povoľte postupovanie datagramov IP pod Vlastnosti nastavení v Konfigurácii TCP/IP v Navigátore iSeries (aby ste povolili vzdialeným klientom komunikovať so sieťou Vstup údajov)

Scenár: Ochrana nevynúteného tunelu L2TP pomocou IPSec

V tomto scenári sa dozviete, ako nastaviť pripojenie medzi hostiteľom v pobočke a centrálou spoločnosti, ktorá používa L2TP chránené pomocou IPSec. Pobočka má dynamicky pridelenú adresu IP a centrála spoločnosti má statickú, globálne smerovateľnú adresu IP.

Situácia

Predpokladajme, že vaša spoločnosť má malú pobočku v inom štáte. Počas bežného dňa vyžaduje pobočka prístup k dôverným informáciám o systéme iSeries vo vašom firemnom intranete. Vaša spoločnosť aktuálne používa nákladnú prenajatú linku, aby umožnila prístup pobočke k firemnej sieti. Spoločnosť chce naďalej poskytovať bezpečný prístup do vášho intranetu, ale určite chcete zredukovať náklady súvisiace s prenájmom linky. Je to možné realizovať vytvorením nevynúteného tunelu L2TP (Layer 2 Tunnel Protocol), ktorý rozšíri vašu firemnú sieť tak, že pobočka sa bude javiť ako súčasť vašej firemnej podsiete. Dátovú prevádzku v tuneli L2TP chráni VPN.

Pri nevynútenom tuneli L2TP, vzdialená pobočka vytvorí tunel priamo do sieťového servera L2TP (LNS) firemnej siete. Funkčnosť koncentrátora prístupov L2TP (LAC) je na klientovi. Tunel je pre poskytovateľa internetových služieb (ISP) vzdialeného klienta transparentný, preto sa od ISP nevyžaduje podpora pre L2TP. Ak sa chcete dozvedieť viac o konceptoch L2TP, pozrite si Layer 2 Tunnel Protocol (L2TP).

Dôležité: Tento scenár ukazuje bezpečné brány, ktoré sú pripojené priamo k Internetu. Kvôli jednoduchosti, v tomto scenári chýba firwall. Neznamená to, že použitie firewallu nie je potrebné. Zvážte bezpečnostné riziká pri každom pripojení k Internetu.

Ciele

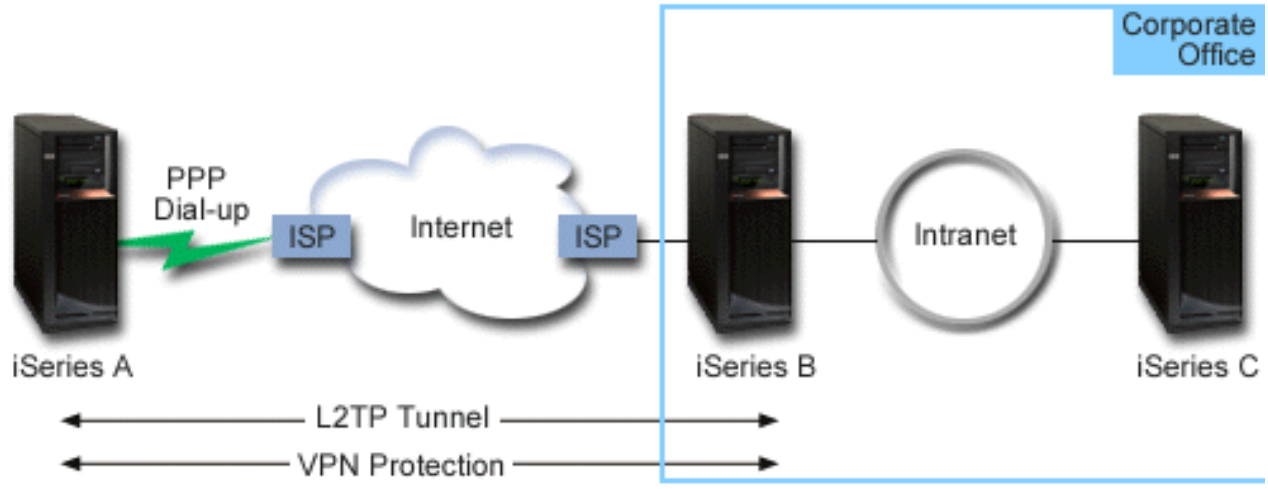
V tomto scenári sa systém v pobočke pripojí do firemnej siete cez systém brány tunelom L2TP, ktorý je chránený pomocou VPN.

Hlavné ciele tohto scenára sú:

- Systém v pobočke vždy iniciuje pripojenie k centrále spoločnosti.
- Systém v pobočke je jediný systém v sieti pobočky, ktorý potrebuje prístup do firemnej siete. Inými slovami, jeho rola v sieti pobočky je hostiteľ, nie brána.
- Systém v spoločnosti je hostiteľský počítač v sieti centrály spoločnosti.

Detaily

Tento obrázok zobrazuje charakteristiky siete pre tento scenár:



iSeries-A

- Musí mať prístup k aplikáciám TCP/IP vo všetkých systémoch v sieti spoločnosti.
- Prijíma dynamicky priradené adresy IP od jeho ISP.
- Musí byť nakonfigurovanie podpory L2TP.

iSeries-B

- Musí mať prístup k aplikáciám TCP/IP v iSeries-A.
- Podsieť je 10.6.0.0 s maskou 255.255.0.0. Táto podsieť reprezentuje koncový bod tunelu VPN na strane spoločnosti.
- Pripája sa k Internetu cez adresu IP 205.13.237.6. Toto je koncový bod pripojenia. Znamená to, že iSeries-B vykonáva manažment kľúčov a aplikuje IPSec na prichádzajúce a odchádzajúce datagramy IP. iSeries-B sa pripája do svojej podsiete adresou IP 10.6.11.1.

V terminológii L2TP, *iSeries-A* vystupuje ako iniciátor L2TP a *iSeries-B* vystupuje ako terminátor L2TP.

Úlohy konfigurovania

Za predpokladu, že už existuje a funguje konfigurácia TCP/IP, musíte vykonať nasledujúce úlohy:

Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE

Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

Situácia

Vaša spoločnosť vyžaduje rýchle pripojenie k Internetu, preto sa obrátite na lokálneho ISP so žiadosťou o službu DSL (digital subscriber line). Po úvodnom prieskume zistíte, že váš ISP používa na pripájanie svojich klientov PPPoE. Toto pripojenie PPPoE potrebujete používať na poskytnutie širokopásmových pripojení k Internetu cez váš server iSeries.

Obrázok 3. Pripojenie vášho servera iSeries k ISP s PPPoE

Riešenie

Pripojenie PPPoE k vášmu ISP môžete podporovať cez váš server iSeries. Server iSeries poskytuje nový typ virtuálnej linky PPPoE, ktorý je naviazaný na fyzickú ethernetovú linku nakonfigurovanú na používanie ethernetového adaptéra typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707 alebo 573A. Táto virtuálna linka podporuje protokoly relácie PPP cez ethernetovú lokálnu počítačovú sieť (LAN), ktorá je pripojená k modemu DSL, ktorý poskytuje bránu ku vzdialenému ISP. Toto dovoľuje užívateľom pripojeným do LAN mať vysokorýchlostný prístup k Internetu pomocou pripojenia PPPoE serverov iSeries. Po vytvorení pripojenia medzi iSeries a ISP, jednotliví užívatelia LAN môžu pristupovať k ISP cez PPPoE pomocou adresy IP, ktorá bola vyhradená 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. Nakonfigurujte profil pripojenia pôvodcu vo vašom serveri iSeries.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: PPP over Ethernet
   - **Režim prevádzky**: Iniciátor
   - **Konfigurácia linky**: Jedna linka
3. Na strane Všeobecné vo Vlastnostiach nového profilu Point-to-Point zadajte názov a opis profilu pôvodcu. Tento názov sa týka profilu pripojenia a virtuálnej linky PPPoE.
4. Kliknite na **Pripojenie**, aby sa otvorila strana Pripojenie. Vyberte **Názov virtuálnej linky PPPoE**, ktorý zodpovedá názvu pre tento profil pripojenia. Keď vyberiete linku, Navigátor iSeries zobrazí dialógové okno **Vlastnosti linky**.

   a. Na strane Všeobecné zadajte zmysluplný opis pre virtuálnu linku PPPoE.

b. Kliknite na **Linky**, aby sa otvorila strana Linka. Z výberového zoznamu Názov fyzickej linky vyberte ethernetovú linku, ktorú bude používať toto pripojenie a kliknite na **Otvoriť**. Ak potrebujete nadefinovať novú linku Ethernet, napíšte jej názov a kliknite na **Nová**. Navigátor iSeries zobrazí dialógové okno **Vlastnosti ethernetovej linky**.

| **Poznámka:** PPPoE vyžaduje ethernetový adaptér typu 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707
| alebo 573A.

1) Na strane Všeobecné zadajte zmysluplný opis pre ethernetovú linku a skontrolujte, či definícia linky používa vyžadované hardvérové prostriedky.
2) Kliknite na **Linky**, aby sa otvorila strana Linka. Zadajte vlastnosti fyzickej linky Ethernet. Viac informácií nájdete v dokumentácii k vášmu ethernetovému adaptéru a v online pomoci.
3) Kliknite na **Iné**, aby sa otvorila strana Iné. Zadajte úroveň prístupu a oprávnenia iných užívateľov, ktorí môžu používať túto linku.
4) Kliknutím na **OK** sa vrátite na stranu vlastností virtuálnej linky PPPoE.

c. Kliknite na **Limity**, ak chcete zadefinovať vlastnosti autentifikácie LCP, alebo kliknite na **OK**, ak sa chcete vrátiť na stranu Nový profil pripojenia Point-to-Point.

d. Keď sa vrátite na stranu Pripojenie, zadajte adresy servera PPPoE podľa informácií, ktoré vám poskytol váš ISP.

5. Ak váš ISP vyžaduje, aby sa server iSeries autentifikoval, alebo ak chcete autentifikovať iSeries vzdialenému serveru, kliknite na **Autentifikácia**, aby sa otvorila strana Autentifikácia.
6. Kliknite na **Nastavenia TCP/IP**, aby sa otvorila strana TCP/IP a zadajte parametre pre spracovanie adresy IP pre tento profil pripojenia. Potrebné nastavenie by mal poskytnúť váš ISP. Ak chcete povoliť, aby sa užívatelia pripojení do LAN mohli pripájať k ISP pomocou adries IP, ktoré boli priradené serveru iSeries, vyberte **Skryť adresy (úplné maskovanie)**.
7. Kliknite na **DNS**, aby sa otvorila strana DNS a zadajte adresu IP servera DNS, ktorú vám oznámi l ISP.
8. Ak chcete zadať podsystém na vykonávanie úlohy pripojenia, kliknite na **Iné**, aby sa otvorila strana Iné.
9. Kliknutím na **OK** dokončite profil.

Súvisiace koncepty

"Podpora skupinových politík" na strane 5
Podpora skupinových politík dovoľuje administrátorom siete definovať skupinové politiky podľa užívateľov, ktoré pomáhajú manažovať prostriedky a dovoľujú priraďovanie politík riadenia prístupu k jednotlivým užívateľom pri prihlasovaní do siete cez reláciu PPP alebo L2TP.

Súvisiace úlohy

"Vytvorenie profilu pripojenia" na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

Súvisiaci odkaz

"Konfigurácia spojenia" na strane 50
Konfigurácia pripojenia definuje typ linkovej služby, ktorú váš profil pripojenia PPP používa na nadviazanie pripojenia.

"Autentifikácia systému" na strane 43
Pripojenia PPP so serverom iSeries podporujú niekoľko volieb pre autentifikáciu vzdialených klientov, ktorí vytvárajú telefonické pripojenie k iSeries, ako aj pripojení k ISP a iným serverom, ku ktorým sa telefonicky pripája iSeries.

"Spravovanie adries IP" na strane 41
Pripojenia PPP poskytujú niekoľko rôznych množín volieb pre manažovanie adries IP podľa typu profilu pripojenia.

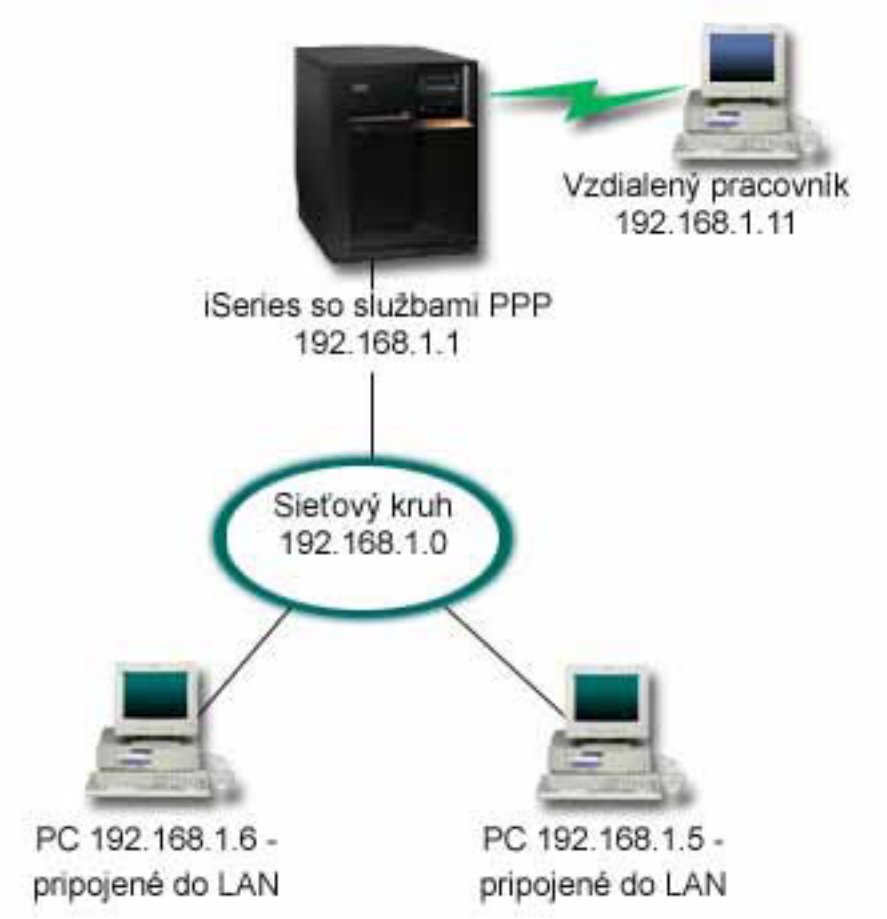
"Filtrovanie paketov IP" na strane 41
Filtrovanie paketov IP obmedzuje služby pre jednotlivých užívateľov, keď sa prihlásia do siete.

Scenár: Pripojenie vzdialených klientov s telefonickým pripojením k vášmu serveru iSeries

Vzdialení používatelia, napríklad dialĺkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

Situácia

Ako administrátor siete vašej spoločnosti musíte udržiavať server iSeries a sieťových klientov. Namiesto toho, aby ste chodili do práce a riešili problémy, potrebujete možnosť pracovať zo vzdialeného miesta, napríklad z domu. Vaša spoločnosť nemá internetové pripojenie, preto sa k vášmu serveru iSeries pripájate telefonickým pripojením využitím PPP. Okrem toho, jediný modem, ktorý aktuálne máte, je váš modem elektronickej podpory zákazníkov (ECS) 7852-400 a tento modem potrebujete pre vaše pripojenie.



Obrázok 4. Pripojenie vzdialených klientov k vášmu serveru iSeries

Riešenie

Na pripojenie vášho domáceho PC k serveru iSeries pomocou modemu môžete použiť PPP. Pre tento typ pripojenia PPP používate modem ECS, preto musíte zaručiť, že váš modem je nakonfigurovaný pre synchrónny aj asynchrónny režim. Tento obrázok znázorňuje server iSeries so službami PPP, ktorý je pripojený k LAN s dvomi osobnými počítačmi. Vzdialený pracovník sa telefonicky pripojí k serveru iSeries, autentifikuje sa a následne sa stane súčasťou 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, preto musíte vášho klienta PPP nastaviť na použitie 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 viacero simultánnych klientov s telefonickým pripojením, pozrite si časť s plánovaním hardvéru a softvéru.

Vzorová konfigurácia

1. Nakonfigurujte Dial-up Networking a vytvorte telefonické pripojenie vo vzdialenom PC.
2. Nakonfigurujte profil pripojenia prijímateľa vo vašom serveri iSeries.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Odpoveď
   - **Konfigurácia linky**: Toto môže byť jedna linka alebo oblasť liniek, podľa vášho prostredia.
3. Na strane Všeobecné z Vlastností profilu point-to-point zadajte názov a opis pre profil príjemcu.
4. Kliknite na **Pripojenie**, aby sa otvorila strana Pripojenie. Vyberte príslušný **Názo v linky** alebo vytvorte nový zadaním nového názvu a kliknite na **Nový**.
   a. Na strane Všeobecné zvýraznite existujúci hardvérový prostriedok, ku ktorému je pripojený váš adaptér 7852–400 a nastavte Rámcovanie na **Asynchrónne**.
   b. Kliknite na **Modem**, aby sa otvorila strana Modem. Vo výberovom zozname Názov vyberte modem **IBM 7852–400**.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
5. Kliknite na **Autentifikácia**, aby sa otvorila strana Autentifikácia.
   a. Vyberte **Vyžadovať od tohto servera iSeries kontrolu identity 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 **Nastavenia TCP/IP**, aby sa otvorila strana TCP/IP.
   a. Nastavte lokálnu adresu IP na 192.168.1.1.
   b. Pre vzdialenú adresu IP vyberte **Pevná adresa IP** a začiatočnú adresu IP 192.168.1.11.
   c. Vyberte **Povoliť vzdialenému systému prístup do iných sietí**.
7. Kliknutím na **OK** dokončite profil.

Súvisiace koncepty

“Plánovanie PPP” na strane 32
V tejto téme nájdete informácie o vytváraní a spravovaní pripojení PPP.

Súvisiace úlohy

“Vytvorenie profilu pripojenia” na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

Súvisiaci odkaz

“CHAP-MD5” na strane 43
Challenge Handshake Authentication Protocol (CHAP-MD5) používa algoritmus (MD-5) na vypočítanie hodnoty, ktorú pozná len autentifikačný systém a vzdialené zariadenie.

“Konfigurácia spojenia” na strane 50
Konfigurácia pripojenia definuje typ linkovej služby, ktorú váš profil pripojenia PPP používa na nadviazanie pripojenia.

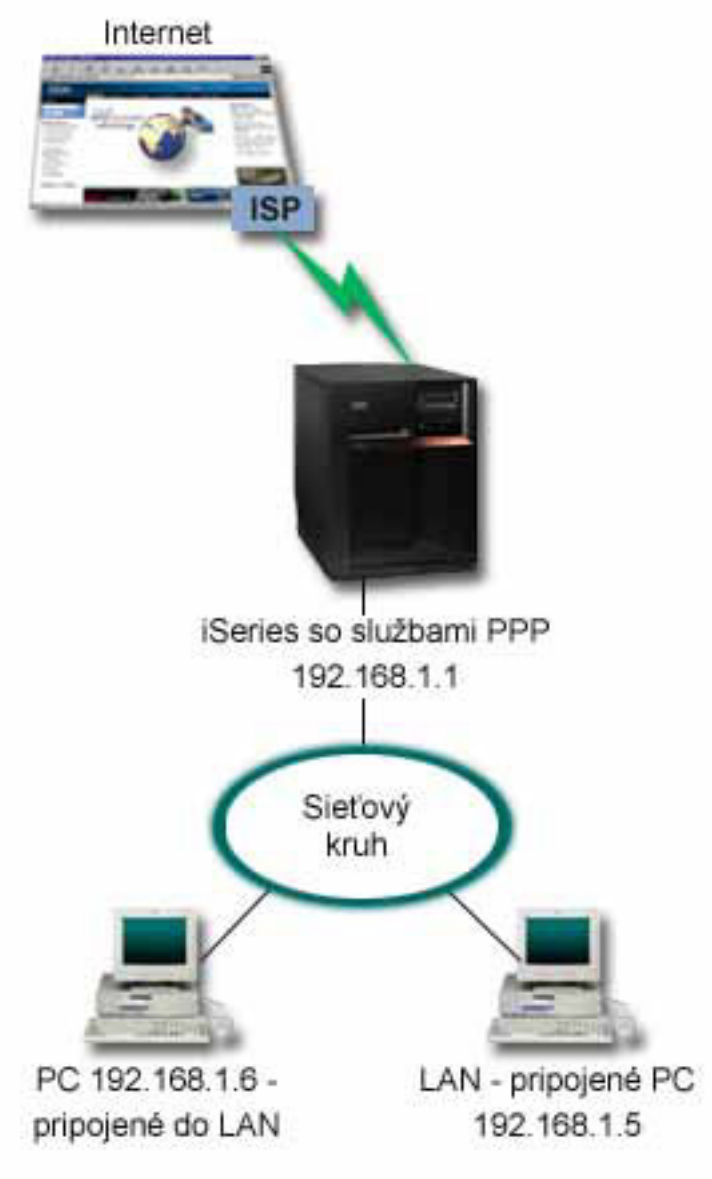
“Oblasť liniek” na strane 50
Výberom tejto linkovej služby nastavíte pripojenie PPP na používanie linky z oblasti liniek. Keď sa spustí pripojenie PPP, server iSeries vyberie nevyužitú linku z oblasti liniek. Pri profiloch telefonického pripojenia na požiadanie si server linku vyberie až vtedy, keď zistí pre vzdialený systém prevádzku TCP/IP.

Scenár: Pripojenie vašej siete LAN modemom na Internet

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

Situácia

Firemná aplikácia, ktorú používa vaša spoločnosť, vyžaduje, aby mali vaši užívatelia prístup k Internetu. Aplikácia nevyžaduje výmenu veľkého množstva údajov, preto ste schopný používať modem na pripojenie vášho servera iSeries a klientskych počítačov v LAN k Internetu. V ďalšom opise sa uvádza príklad riešenia tejto situácie.



Obrázok 5. Pripojenie kancelárskej LAN k Internetu cez modem

Riešenie

Na pripojenie vášho iSeries k vášmu 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 pripojenia medzi iSeries a ISP, počítače v LAN môžu využívať Internet využitím iSeries ako brány. 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.

V závislosti od vášho využitia Internetu sa môže stať problémom šírka pásma. Ak sa chcete dozvedieť viac, ako zvýšiť šírku pásma vášho pripojenia, pozrite si časť s plánovaním.

Vzorová konfigurácia

1. Nakonfigurujte profil pripojenia pôvodcu vo vašom serveri iSeries.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Telefonické pripojenie
   - **Konfigurácia linky**: Toto môže byť jedna linka alebo oblasť liniek, podľa vášho prostredia.

2. Na strane Všeobecné vo Vlastnostiach nového profilu Point-to-Point zadajte názov a opis profilu pôvodcu.
3. Kliknite na **Pripojenie**, aby sa otvorila strana Pripojenie. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane 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 pre telefonické pripojenie k serveru ISP. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na **Autentifikácia**, aby sa otvorila strana Autentifikácia, vyberte **Povoliť vzdialenému systému kontrolu identity tohto servera iSeries**. Zvoľte autentifikačný protokol a zadajte prípadné požadované meno používateľa alebo heslo.
6. Kliknite na **Nastavenia TCP/IP**, aby sa otvorila strana 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 **DNS**, aby sa otvorila strana DNS a zadajte adresu servera DNS, ktorú vám poskytol ISP.
8. Kliknutím na **OK** dokončite profil.

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

Poznámka: Musíte skontrolovať, či majú ostatné systémy vo vašej sieti správne definované smerovanie, aby odchádzajúca premávka TCP/IP z týchto systémov bola posielaná cez server iSeries.

Súvisiace koncepty

“Plánovanie PPP” na strane 32
V tejto téme nájdete informácie o vytváraní a spravovaní pripojení PPP.

Súvisiace úlohy

“Vytvorenie profilu pripojenia” na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

Súvisiaci odkaz

“Oblasť liniek” na strane 50
Výberom tejto linkovej služby nastavíte pripojenie PPP na používanie linky z oblasti liniek. Keď sa spustí pripojenie PPP, server iSeries vyberie nevyužitú linku z oblasti liniek. Pri profiloch telefonického pripojenia na požiadanie si server linku vyberie až vtedy, keď zistí pre vzdialený systém prevádzku TCP/IP.

“Konfigurácia spojenia” na strane 50
Konfigurácia pripojenia definuje typ linkovej služby, ktorú váš profil pripojenia PPP používa na nadviazanie pripojenia.

Scenár: Prepojenie vašich vnútropodnikových a vzdialených sietí modemom

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

Situácia

Predpokladajme, že máte sieť v pobočke a firemnú sieť 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 6. Prepojenie vašich vnútropodnikových a vzdialených sietí modemom

Riešenie

PPP môže spojiť dve siete LAN vytvorením pripojenia medzi každým serverom iSeries, ako znázorňuje obrázok hore. V takom prípade predpokladajme, že vzdialená kancelária iniciuje pripojenie k ústrednej kancelárii. Budete konfigurovať profil pôvodcu vo vzdialenom iSeries a profil príjemcu v serveri centrálnej pobočky.

Ak osobné počítače vo vzdialenej pobočke potrebujú prístup do firemnej LAN (192.168.1.0), profil príjemcu centrálnej pobočky musí mať zapnuté postupovanie IP a povolené smerovanie adries IP pre osobné počítače (v tomto príklade 192.168.2, 192.168.3, 192.168.1.6 a 192.168.1.5). Tiež musí byť aktivované postúpenie IP pre zásobník TCP/IP. Táto konfigurácia umožňuje základnú komunikáciu TCP/IP medzi sieťami LAN. Mali by ste uvážiť bezpečnostné faktory a DNS na preklad názvov hostiteľov medzi LAN.

Vzorová konfigurácia

1. Nakonfigurujte profil pripojenia pôvodcu v serveri iSeries vzdialenej pobočky.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Telefonické pripojenie
   - **Konfigurácia linky**: Toto môže byť jedna linka alebo oblasť liniek, podľa vášho prostredia.
2. Na strane Všeobecné vo Vlastnostiach nového profilu Point-to-Point zadajte názov a opis profilu pôvodcu.
3. Kliknite na **Pripojenie**, aby sa otvorila strana Pripojenie. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane Všeobecné vo vlastnostiach novej linky zvýraznite existujúci hardvérový prostriedok a nastavte rámcovanie na **Asynchrónne**.
   b. Kliknite na **Modem**, aby sa otvorila strana Modem. Zo zoznamu Výber názvu vyberte modem, ktorý používate.
   c. Kliknite na **OK**, čím sa vrátite na stranu Vlastnosti nového profilu point-to-point.
4. Kliknite na **Pridať** a napíšte telefónne číslo pre telefonické pripojenie k serveru iSeries centrálnej pobočky. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na **Autentifikácia**, aby sa otvorila strana Autentifikácia a vyberte **Povoliť vzdialenému systému kontrolu identity tohto servera iSeries**. Vyberte **Požadovať zašifrované heslo (CHAP-MD5)** a vložte požadované meno používateľa alebo heslo.
6. Kliknite na **Nastavenia TCP/IP**, aby sa otvorila strana Nastavenia TCP/IP.
   a. Pre Lokálnu adresu IP vyberte adresu IP rozhrania LAN vzdialenej pobočky (192.168.2.1) v zozname **Použiť pevnú adresu IP**.
   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**: Odpoveď
   - **Konfigurácia linky**: Toto môže byť jedna linka alebo oblasť liniek, podľa vášho prostredia.
8. Na strane Všeobecné z Vlastností profilu point-to-point zadajte názov a opis pre profil príjemcu.
9. Kliknite na **Pripojenie**, aby sa otvorila strana Pripojenie. Vyberte príslušný Názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **Nový**.
   a. Na strane Všeobecné zvýraznite existujúci hardvérový prostriedok a nastavte rámcovanie na **Asynchrónne**.

b. Kliknite na **Modem**, aby sa otvorila strana 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 **Autentifikácia**, aby sa otvorila strana Autentifikácia.
    a. Začiarknite **Vyžadovať od tohto servera iSeries kontrolu identity vzdialeného systému**.
    b. Pridajte nového vzdialeného používateľa do validizačného zoznamu.
    c. Začiarknite autentifikáciu CHAP-MD5.
11. Kliknite na **Nastavenia TCP/IP**, aby sa otvorila strana 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**. Otvorí sa dialógové okno **Adresy IP definované podľa mena užívateľa**. Kliknite na **Pridať**. Vyplňte polia Užívateľské meno volajúceho, Adresa IP a Maska podsiete. V našom scenári bude vhodné nasledujúce:
       - 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.

Súvisiace úlohy

“Vytvorenie profilu pripojenia” na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

Súvisiaci odkaz

“Konfigurácia spojenia” na strane 50
Konfigurácia pripojenia definuje typ linkovej služby, ktorú váš profil pripojenia PPP používa na nadviazanie pripojenia.

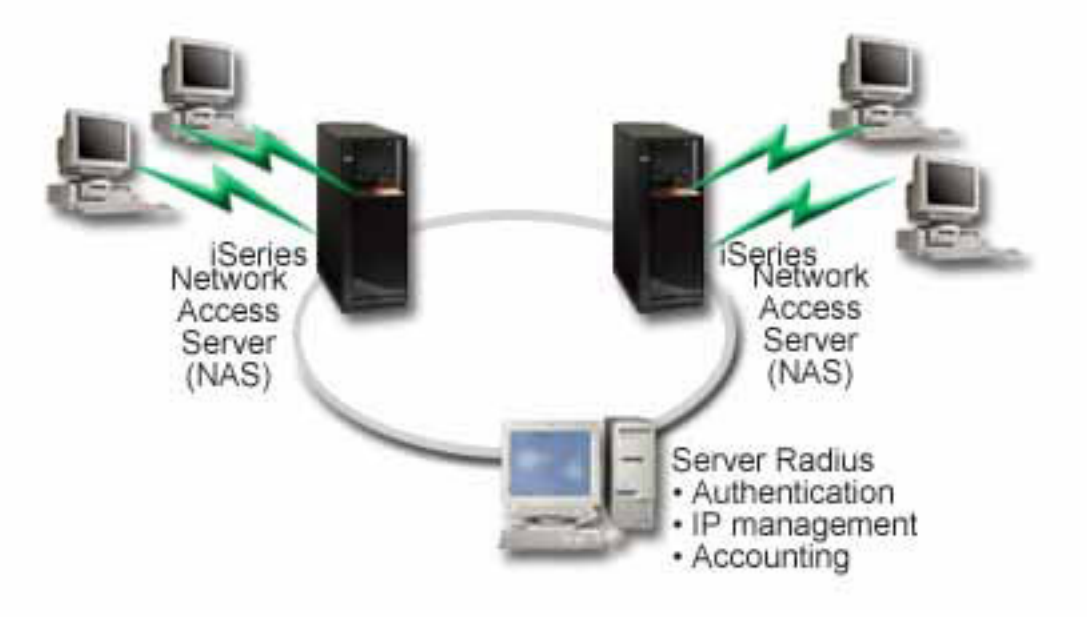
“Oblasť liniek” na strane 50
Výberom tejto linkovej služby nastavíte pripojenie PPP na používanie linky z oblasti liniek. Keď sa spustí pripojenie PPP, server iSeries vyberie nevyužitú linku z oblasti liniek. Pri profiloch telefonického pripojenia na požiadanie si server linku vyberie až vtedy, keď zistí pre vzdialený systém prevádzku TCP/IP.

Scenár: Autentifikácia telefonických pripojení cez RADIUS NAS

NAS (Network Access Server) spustený v serveri iSeries môže smerovať požiadavky o autentifikáciu od klientov s telefonickým pripojením do samostatného servera RADIUS. Ak bude autentifikácia úspešná, RADIUS tiež môže riadiť adresy IP pre užívateľa.

Situácia

Vaša firemná sieť má vzdialených užívateľov, ktorí sa pripájajú k dvom serverom iSeries cez telefonické pripojenie z distribuovanej telefónnej siete. Potrebujete spôsob pre centralizovanú autentifikáciu, služby a účtovanie, ktorý bude jednému serveru dovoľovať spracúvať požiadavky o validáciu identifikátorov užívateľov, ako aj určovať, ktoré adresy IP sa im priradia.



Obrázok 7. Autentifikujte telefonické pripojenia serverom RADIUS

Riešenie

Keď sa užívatelia pokúsia pripojiť, NAS v serveroch iSeries postúpi autentifikačné informácie serveru RADIUS v sieti. Server RADIUS, ktorý udržiava všetky autentifikačné informácie vašej siete, spracúva autentifikačné požiadavky a odpovede. Ak je užívateľ overený, môže byť server RADIUS nakonfigurovaný tak, aby priradil adresu IP rovnocenného počítača a aby mohol aktivovať spravovanie konta na sledovanie aktivity a použitie užívateľa. Ak chcete využívať podporu RADIUS, musíte zadefinovať server RADIUS NAS v iSeries.

Vzorová konfigurácia

1. V Navigátore iSeries rozviňte **Sieť**, kliknite pravým tlačidlom myši na **Služby vzdialeného prístupu** a vyberte **Služby**.
2. Na záložke RADIUS vyberte **Povoliť pripojenie k RADIUS Network Access Server** 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 zadajte opis pre tento server.
5. Na strane Autentifikačný server (a voliteľne na strane Účtovací server) kliknite na **Pridať** a zadajte nasledujúce informácie:
   a. Do poľa Lokálna adresa IP zadajte adresu IP pre rozhranie iSeries, ktoré sa používa na pripojenie k serveru RADIUS.
   b. Do poľa Adresa IP servera zadajte adresu IP servera RADIUS.
   c. Do poľa Heslo zadajte heslo, ktoré sa používa na identifikáciu servera iSeries pre server RADIUS.
   d. Do poľa Port zadajte port, ktorý používa iSeries 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 Navigátore iSeries rozviňte **Sieť → Služby vzdialeného prístupu**.
8. Označte Profil pripojenia, ktorý bude server RADIUS pri autentifikácii využívať. Na služby RADIUS môžu byť aplikované len profily pripojenia príjemcu.
9. Vyberte **Vyžadovať od tohto servera iSeries kontrolu identity vzdialeného systému**.
10. Označte **Overiť vzdialene používaný server RADIUS**.

11. Označte autentifikačný protokol (PAP alebo CHAP-MD5) Tento protokol tiež musí používať server RADIUS.
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 užívatelia vytvoria telefonické pripojenie pomocou tohto profilu pripojenia, iSeries postúpi autentifikačné informácie do určeného servera RADIUS. Ak bude užívateľ validovaný, povolí sa vytvorenie pripojenia a aplikujú sa všetky obmedzenia pripojenia, ktoré sú určené v informáciách užívateľa o serveri RADIUS.

Súvisiace úlohy

"Povolenie služieb RADIUS a DHCP pre profily pripojenia" na strane 60
Ak chcete povoliť služby RADIUS alebo DHCP pre profily pripojenia prijímateľa PPP, vykonajte nasledujúce kroky.

Súvisiaci odkaz

"Autentifikácia systému" na strane 43
Pripojenia PPP so serverom iSeries podporujú niekoľko volieb pre autentifikáciu vzdialených klientov, ktorí vytvárajú telefonické pripojenie k iSeries, ako aj pripojení k ISP a iným serverom, ku ktorým sa telefonicky pripája iSeries.

"RADIUS - prehľad" na strane 45
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.

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

Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Situácia

Vaša sieť má niekoľko skupín distribuovaných užívateľov a každá z nich potrebuje prístup k odlišným prostriedkom vo vašej firemnej LAN. Skupina užívateľov Data Entry potrebuje prístup k databáze a niekoľkým iným aplikáciám, kým ľudia z iných spoločností potrebujú prístup cez telefonické pripojenie k službám HTTP, FTP a Telnet, ale z bezpečnostných dôvodov nemôžu mať prístup k iným službám ani premávke TCP/IP. Definovanie detailných atribútov a povolení pripojenia pre každého užívateľa znásobí vašu vynaloženú prácu a nastavenie sieťových obmedzení pre všetkých užívateľov tohto profilu pripojenia neposkytne dostatočné riadenie. Potrebovali by ste spôsob definovania nastavení pripojenia a povolení pre niekoľko rozličných skupín užívateľov, ktorí sa zvyčajne pripájajú na tento server.

Obrázok 8. Aplikácia nastavenia pripojenia na telefonické pripojenie založené na nastaveniach skupinovej politiky

Riešenie

Potrebujete aplikovať jedinečné obmedzenia filtrovania IP na dve rôzne 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 je potrebné vytvoriť filter PPP, ktorý obsahuje filtrovacie pravidlá IP pre skupinovú politiku prístupu ″Obchodný partner IBM″. Tieto filtrovacie pravidlá povolia služby HTTP, FTP a Telnet, ale obmedzia prístup k všetkej ostatnej premávke a službám TCP/IP cez server iSeries. Tento scenár zobrazuje len filtrovacie pravidlá, ktoré sú potrebné pre skupinu Obchodníci; podobné filtre však môžete nastaviť aj pre skupinu ″Data Entry″.

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 v serveri iSeries môžete aplikovať tieto nastavenia pripojenia 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.
   a. V Navigátore iSeries rozviňte **Sieť → Služby vzdialeného prístupu**.
   b. Kliknite na **Profily pripojenia príjemcu** a vyberte Skupinové politiky prístupu.
   c. Kliknite pravým tlačidlom myši na preddefinovanú skupinu v pravej časti okna a vyberte **Vlastnosti**.

      Poznámka: Ak chcete vytvoriť novú skupinovú politiku prístupu, kliknite pravým tlačidlom myši na Skupinové politiky prístupu a vyberte **Nové skupinové politiky prístupu**. Vyplňte záložku Všeobecné. Potom vyberte záložku Nastavenia TCP/IP a pokračujte krokom e dole.
   d. Vyberte záložku Nastavenia TCP/IP a 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 zadefinujte množiny filtrov a na záložke Služby zadefinujte službu, ktorú chcete povoliť, 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) Na záložke Všeobecné zadajte permitted_services pre identifikátor filtra PPP.

   2) Na záložke Množiny filtrov vyberte množinu 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 potrebujete neskôr vrátiť späť tieto zmeny, v znakovom rozhraní zadajte príkaz: RMVTCPTBL *ALLTento príkaz odstráni všetky filtrovacie pravidlá a NAT v serveri.

i. V dialógovom okne **Rozšírené nastavenia TCP/IP** nechajte pole identifikátor filtra PPP prázdne a kliknite na **OK**, aby ste zatvorili okno. 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.

   a. V Navigátore iSeries rozviňte **Sieť → Služby vzdialeného prístupu → Profily pripojenia prijímača**.

   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. Vyberte **OK**, aby sa uložila skupinová politika prístupu.

3. Použite skupinovú politiku prístupu na užívateľov spojených s touto skupinou.
   a. Otvorte profil pripojenia prijímateľa, ktorý riadi tieto telefonické pripojenia.
   b. Na strane Autentifikácia z Profilu pripojenia prijímateľa vyberte validačný zoznam, ktorý obsahuje autentifikačné informácie pre užívateľa 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 skupinovú politiku na užívateľa** a vyberte skupinovú politiku prístupu, ktorú ste definovali v kroku 2.
   e. Toto zopakujte pre každého užívateľa skupiny Obchodníci.

Súvisiace koncepty

"Konfigurácia politiky skupinového prístupu" na strane 58
Zložka **Skupinové politiky prístupu** pod Profilmi pripojenia prijímača poskytujú voľby pre konfiguráciu parametrov pripojenia point-to-point, ktoré sa týkajú skupiny vzdialených užívateľov. Týka sa len tých pripojení point-to-point, ktoré iniciuje vzdialený systém a prijíma lokálny systém.

"Podpora skupinových politík" na strane 5
Podpora skupinových politík dovoľuje administrátorom siete definovať skupinové politiky podľa užívateľov, ktoré pomáhajú manažovať prostriedky a dovoľujú priraďovanie politík riadenia prístupu k jednotlivým užívateľom pri prihlasovaní do siete cez reláciu PPP alebo L2TP.

Súvisiace úlohy

"Vytvorenie profilu pripojenia" na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

"Použitie pravidiel filtrovania paketov IP na pripojenie PPP" na strane 59
Na obmedzenie prístupu užívateľov alebo skupín k adresám IP vo vašej sieti môžete použiť súbor pravidiel pre pakety.

Súvisiaci odkaz

"Validizačný zoznam" na strane 45
Validačný zoznam sa používa na ukladanie informácií o identifikátoroch užívateľov a heslách vzdialených užívateľov.

"Autentifikácia systému" na strane 43
Pripojenia PPP so serverom iSeries podporujú niekoľko volieb pre autentifikáciu vzdialených klientov, ktorí vytvárajú telefonické pripojenie k iSeries, ako aj pripojení k ISP a iným serverom, ku ktorým sa telefonicky pripája iSeries.

Súvisiace informácie

IP packet rules (Filtering and NAT)

Scenár: Zdieľanie modemu medzi logickými oddielmi pomocou 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.

Situácia

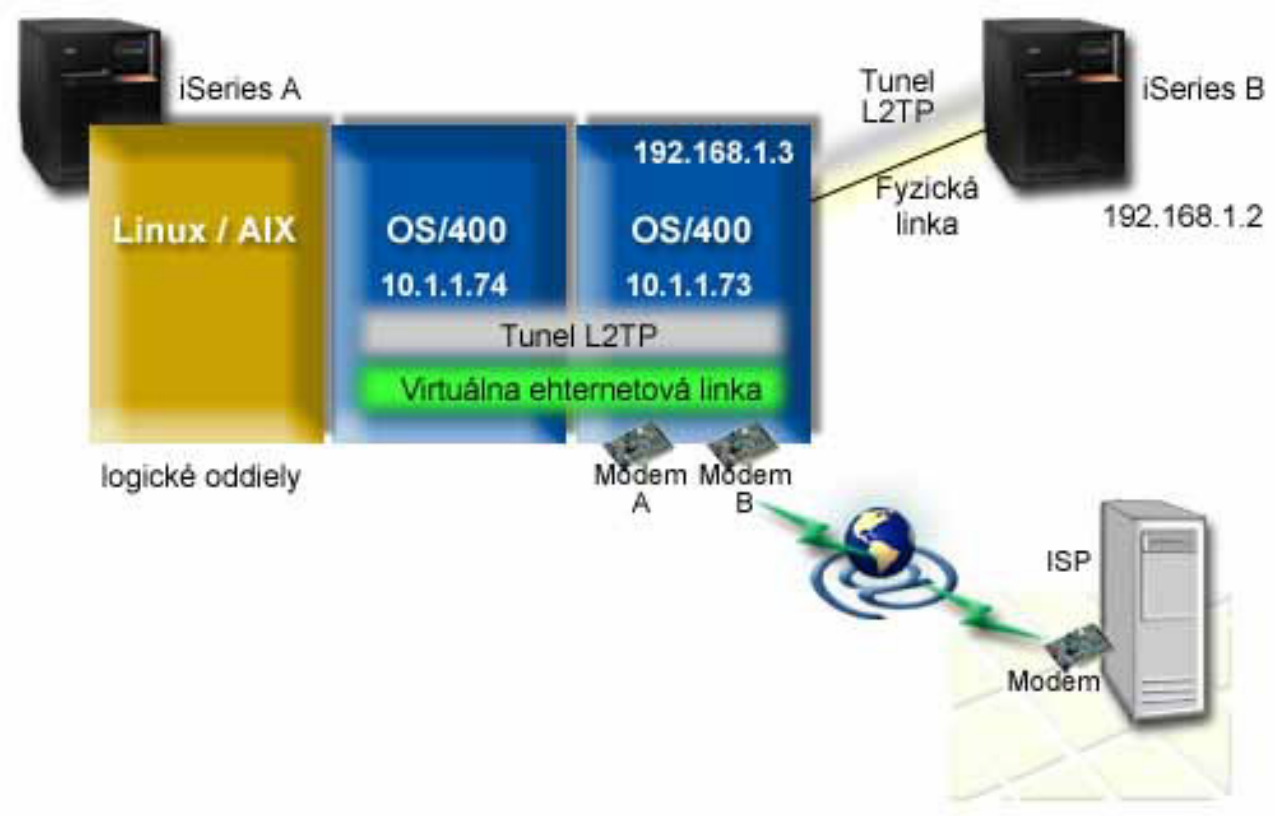
Ste administrátorom systému v stredne veľkej spoločnosti. Je čas na rozšírenie vášho počítačového vybavenia, ale radi by ste spravili viac než len to - chcete výrazne zmodernizovať váš hardvér. Začnete tým, že zlúčite prácu troch starých serverov do jedného nového servera iSeries. V serveri iSeries vytvoríte 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 elektronickej podpory zákazníkov (ECS) 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:



Obrázok 9. Viacero systémov zdieľajúcich rovnaký modem pre telefonické pripojenia

Požiadavky a predpoklady

Požiadavky pre nastavenie pre iSeries-A zahŕňajú:

- i5/OS verzia 5, vydanie 3 alebo novšie, nainštalované v oddiele, ktorý vlastní modemy s podporou ASYNC
- Hardvér, ktorý dovoľuje vytvorenie oddielov.
- iSeries Access for Windows a Navigátor iSeries (komponent Konfigurácia a servis z Navigátora iSeries Navigator), verzia 5, vydanie 3 alebo novšie
- V serveri ste vytvorili aspoň dva logické oddiely (LPAR). Oddiel, ktorý vlastní modem, musí mať nainštalované i5/OS verzia 5, vydanie 3 alebo novšie. Ostatné oddiely môžu mať nainštalované OS/400 V5R2, V5R3, Linux alebo AIX. V tomto scenári, oddiely používajú operačný systém i5/OS 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 Navigátor iSeries (komponent Konfigurácia a servis z Navigátora iSeries Navigator), verzia 5, vydanie 2 alebo novšie

Súvisiace informácie

Logické oddiely

Detaily scenára: Zdieľanie modemu medzi logickými oddielmi cez L2TP

Po splnení požiadaviek ste pripravený začať konfigurovať profily 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 Navigátore iSeries rozviňte *váš server* → **Sieť** → **Služby vzdialeného prístupu**.
2. Kliknite pravým tlačidlom myši 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 pri spustení TCP**.
5. Na záložke **Nový profil - Pripojenie** vyplňte tieto polia.
   - **Adresa IP lokálneho koncového bodu tunela**: ANY
   - **Názov virtuálnej linky**: toExternal.Táto linka nemá žiadne priradené fyzické rozhranie. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Otvorí sa okno Vlastnosti linky L2TP. Kliknite na záložku **Autentifikácia** a zadajte názov hostiteľa vášho servera. Kliknite na **OK**, aby ste sa vrátili 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 strane 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 okne Vlastnosti novej oblasti liniek vyberte linky a modemy, pre ktoré chcete povoliť 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 okne Vlastnosti novej oblasti liniek vyberte linky a modemy, pre ktoré chcete povoliť odchádzajúce volania a kliknite na **Pridať**. Skontrolujte, že je pre oblasť vybratý modem 2793.
12. Znovu vyberte **Novú linku** a pridajte modem 7852–400 ECS. 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 kliknite na **OK**, aby ste sa vrátili 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, či sú dva nové modemy, ktoré ste pridali, uvedené v poli *Vybraté linky pre oblasť* a kliknite na **OK**, aby ste sa vrátili do okna Vlastnosti vytáčania odchádzajúceho volania.
16. V okne Vlastnosti vytáčania odchádzajúceho volania zadajte Predvolené čísla na vytočenie a kliknite na **OK**, aby ste sa vrátili do okna Vlastnosti nového profilu PPP.

    Poznámka: Tieto čísla môžu byť čísla na vášho ISP, ktoré budete často vytáčať inými systémami cez tieto modemy. Ak iné systémy použijú telefónne číslo *PRIMARY alebo *BACKUP, skutočné čísla, ktoré sa vytočia, sú tu zadané čísla. Ak iné systémy používajú skutočné telefónne číslo, použije sa ich telefónne číslo namiesto týchto.
17. Na záložke **Nastavenia TCP/IP** vyberte tieto hodnoty:
    - **Lokálna adresa IP**: Žiadna
    - **Vzdialená adresa IP**: Žiadna

    Poznámka: Ak tiež používate profil na ukončenie relácií L2TP, musíte vybrať lokálnu adresu IP, ktorá reprezentuje server iSeries. Pre vzdialenú adresu IP môžete vybrať oblasť adries, ktoré sú 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: Konfigurácia profilu pôvodcu L2TP na 10.1.1.74:

Ak chcete vytvoriť profil pôvodcu L2TP, vykonajte tieto kroky:

1. V Navigátore iSeries 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: Linka toModemThis nemá priradené žiadne fyzické rozhranie. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Otvorí sa okno Vlastnosti linky L2TP.
6. Na záložke **Všeobecné** zadajte opis pre virtuálnu linku.
7. Na záložke **Autentifikácia** zadajte lokálny názov hostiteľa oddielu a kliknite na **OK**, aby ste sa vrátili na stranu Pripojenie.
8. Do poľa **Vzdialené telefónne čísla** pridajte *PRIMARY a *BACKUP. Toto dovoľuje profilu používať rovnaké telefónne čísla ako ukončovací profil v oddiele, ktorý vlastní modemy.

9. Do poľa **Názov hostiteľa alebo adresa IP vzdialeného koncového bodu tunela** zadajte adresu IP vzdialeného koncového bodu tunela (10.1.1.73).
10. Na záložke **Autentifikácia** vyberte voľbu **Povoliť vzdialenému systému overiť identitu tohto servera iSeries**.
11. Pre Autentifikačný protokol na použitie vyberte **Vyžadovať šifrované heslo (CHAP-MD5)**. Predvolene je tiež vybraté **Povoliť EAP (Extensible Authentication Protocol)**.

    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 koncovú adresu vzdialeného tunelu na 192.168.1.3 (fyzické rozhranie, ku ktorému sa pripája iSeries B).

Poznámka: Toto sú fiktívne adresy IP a slúžia len ako príklad.

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 Navigátore iSeries rozviňte **10.1.1.73 → Sieť → Služby vzdialeného prístupu → Profily pripojenia príjemcu**.
   b. V pravej časti okna nájdite požadovaný profil (toExternal) a skontrolujte, či pole **Stav** zobrazuje *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 Navigátore iSeries rozviňte **10.1.1.74 → Sieť → Služby vzdialeného prístupu → Profily pripojenia pôvodcu**.
   b. V pravej časti okna nájdite požadovaný profil (toModem) a skontrolujte, či pole **Stav** zobrazuje *Aktívny*. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
3. Spustite profil vzdialeného telefonického pripojenia v iSeries B.
   a. V Navigátore iSeries rozviňte **192.168.1.2 → Sieť → Služby vzdialeného prístupu → Profily pripojenia pôvodcu**.
   b. V pravej časti okna nájdite požadovaný profil, ktorý ste vytvorili a skontrolujte, či pole **Stav** zobrazuje *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 Navigátore iSeries rozviňte *požadovaný server (napríklad 10.1.1.73)* **→ Sieť → Služby vzdialeného prístupu → Profily pripojenia pôvodcu**.
   b. V pravej časti okna kliknite pravým tlačidlom na profil, ktorý ste vytvorili a vyberte **Pripojenia**. V okne Stav pripojenia môžete vidieť, ktoré profily sú aktívne, neaktívne, pripájajú sa a podobne.

Plánovanie PPP

V tejto téme nájdete informácie o vytváraní a spravovaní pripojení PPP.

Súvisiaci odkaz

"Scenár: Pripojenie vzdialených klientov s telefonickým pripojením k vášmu serveru iSeries" na strane 14
Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

"Scenár: Pripojenie vašej siete LAN modemom na Internet" na strane 16
Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na Internet. Na pripojenie servera iSeries k ISP môžu použiť modem. PC klienti pripojení cez LAN môžu komunikovať s Internetom tak, že server iSeries použijú ako bránu.

"Súvisiace informácie pre PPP" na strane 64
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

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 pôvodca, alebo príjemca.

Server iSeries musí spĺňať nasledujúce požiadavky, aby naň mohli pristupovať vzdialené systémy.

- Navigátor iSeries s podporou TCP/IP.
- Jeden z dvoch profilov pripojenia:
  - Profil pôvodcu pripojenia na spracovanie odchádzajúcich pripojení PPP
  - Profil príjemcu pripojenia na spracovanie prichádzajúcich pripojení PPP
- Konzola pracovnej stanice musí mať nainštalované iSeries Access for Windows 95 alebo novší s Navigátorom iSeries.
- Nainštalovaný adaptér

  Môžete si zvoliť jeden z uvedených adaptérov:
  - 2699*: Dvojlinkový WAN vstupno/výstupný adaptér (IOA)
  - 2720*: PCI WAN/Twinaxiálny IOA
  - 2721*: PCI dvojlinkový WAN IOA
  - 2745*: PCI dvojlinkový WAN IOA (nahrádza IOA 2721)
  - 2742*: Dvojlinkové 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 WAN IOA V.90
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A: 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 sa vyžaduje 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 lepší) alebo terminálový adaptér ISDN a kábel RS-232 (EIA 232) alebo kompatibilný.
- V závislosti od typu vášho pripojenia a linky potrebujete jedno z uvedených zariadení:
  - externý alebo interný modem alebo jednotka kanálových služieb (CSU)/jednotka dátových služieb (DSU)
  - terminálový adaptér digitálnej siete s integrovanými službami (ISDN)
- Ak plánujete pripojenie na Internet, musíte upraviť telefonické konto u ISP (Internet Service Provider). Váš ISP by vám mal dať potrebné telefónne čísla a informácie pre internetové pripojenie.

Súvisiaci odkaz

“Profily pripojení” na strane 3
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.

“Modemy” na strane 38
Pri pripojeniach PPP môžete používať tak externé, ako aj interné modemy.

“CSU/DSU” na strane 39
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.

“Terminálové adaptéry ISDN” na strane 39
ISDN vám ponúka digitálne pripojenie, ktoré vám umožní komunikovať a zároveň prenášať hlas, údaje a video, či iné multimediálne aplikácie.

Alternatívy 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 spojenia PPP používa rámcovanie podobné HDLC (High-level Data Link Control) na uzatváranie datagramov na asynchrónnych a synchrónnych komunikačných linkách point-to-point.

Kým PPP podporuje široký rozsah typov liniek, SLIP (Serial-Line Internet Protocol) 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

Analógové pripojenie, ktoré využíva na prenos dát po prenajatých alebo komutovaných linkách modem, je najnižším typom pripojenia point-to-point.

Prenajaté linky sú non-stop pripojenia medzi dvomi určenými mestami, kým komutované linky sú normálne hlasové telefónne linky. Dnešné najrýchlejšie modemy pracujú na rýchlosti 56 Kbps bez komprimácie. Ak vezmeme do úvahy odstup signál-šum v hlasových telefónnych okruhoch, táto rýchlosť je často nedosiahnuteľná.

Vyššie bitové rýchlosti, ktoré uvádza výrobca modemov, sú dosiahnuté vďaka algoritmu komprimácie údajov (CCITT V.42bis), ktorý používajú jeho modemy. 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 rozširuje bitovú rýchlosť na 56 Kbps pre analógové telefónne linky. Ide o hybridnú technológiu, ktorá vyžaduje, aby bol jeden koniec linky PPP digitálny a druhý koniec analógový. Okrem toho, 56 Kbps platí len pri prenose údajov z digitálneho konca do analógového konca pripojenia. Táto technológia je vhodná najmä pre pripojenia k ISP, ktoré majú u seba digitálny koniec linky a hardvér. K analógovému modemu V.24 cez sériové rozhranie RS-232 s asynchrónnym protokolom sa môžete pripojiť rýchlosťami do 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. Pri pohľade na verejnú komutovanú telefónnu sieť ako na digitálnu sieť, technológia V.90 môže akcelerovať prenos údajov z Internetu do počítača rýchlosťami do 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 asymetrická metóda, preto prenosy proti prúdu údajov (stlačenia klávesov a príkazy myši z počítača do

centrálneho miesta, ktoré vyžadujú menšiu šírku pásma) používajú tradičné rýchlosti do 33,6 Kbps. Údaje, ktoré posiela modem, sa posielajú analógovým prenosom, ktorý kopíruje štandard V.34. Výhody vysokej rýchlosti V.90 využívajú len prenosy údajov po prúde.

Štandard V.92 vylepšuje V.90 zvýšením rýchlosti proti prúdu do 48 Kbps. Okrem toho, časy vytvárania pripojení môžu byť menšie vďaka vylepšeniam procesu dohodovania a modemy, ktoré podporujú funkciu ″hold″, môžu zostať pripojené, kým telefónna linka prijíma prichádzajúci hovor alebo čaká na hovor.

Digitálne služby a DDS

S PPP môžete používať digitálne služby a DDS (Digital Data Services).

Digitálna služba

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.

Digitálne dátové služby

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 funguje najlepšie do vzdialenosti 9000 m (30000 stôp). 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 takých prípadoch môže byť vhodnejším riešením Komutované-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.

Súvisiaci odkaz

“CSU/DSU” na strane 39
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.

“Komutovaná-56”
Ak nepotrebujete non-stop pripojenie, používaním komutovanej digitálnej služby, ktorá sa nazýva *Komutovaná-56 (SW56)* môžete ušetriť.

Komutovaná-56

Ak nepotrebujete non-stop pripojenie, používaním komutovanej digitálnej služby, ktorá sa nazýva *Komutovaná-56 (SW56)* môžete ušetriť.

Pripojenie SW56 je podobné nastaveniu službám digitálnych údajov (DDS) v tom, že koncové dátové zariadenie (DTE) sa pripája k digitálnej službe cez CSU/DSU. SW56 CSU/DSU, však obsahuje 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 lokálny telefónny systém a poplatky za používanie sú rovnaké ako za hlasové hovory vašej spoločnosti. 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.

Súvisiaci odkaz

"Digitálne služby a DDS" na strane 34
S PPP môžete používať digitálne služby a DDS (Digital Data Services).

"Digitálna sieť s integrovanými službami (ISDN)"
ISDN (Integrated Services Digital Network) poskytuje komutované digitálne prepojenie dvoch koncov. Na rozdiel od iných služieb však môže ISDN prenášať po jednom pripojení hlas aj údaje.

Digitálna sieť s integrovanými službami (ISDN)

ISDN (Integrated Services Digital Network) poskytuje komutované digitálne prepojenie dvoch koncov. 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 používa dva 64 Kbps kanály B na prenos zákazníckych údajov a kanál D na prenos signalizácie. Dva kanály B je možné zlúčiť a získať rýchlosť 128 Kbps. V niektorých oblastiach môže telefónna spoločnosť obmedziť každý kanál B na 56 Kbps alebo 112 Kbps pri ich zlúčení. Existuje tiež fyzické obmedzenie - zákazník sa musí nachádzať do 5400 m (18000 stôp) od ústredne. Túto vzdialenosť však možno predĺžiť opakovačmi. Do ISDN sa môžete pripojiť zariadením nazvaným terminálový adaptér. Väčšina terminálových adaptérov má integrované sieťové ukončenie (NT1), ktoré umožňuje priame pripojenie k telefónnej zásuvke. Terminálové adaptéry sa zvyčajne pripájajú k vášmu PC cez asynchrónnu linku RS-232 a na nastavovanie a riadenie používajú množinu príkazov AT, podobne ako tradičné 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).

Zvyčajne je potrebné pripojiť sa k terminálovému adaptéru ISDN cez sériové rozhranie RS-232 pomocou asynchrónneho protokolu s rýchlosťou do 230,4 Kbps. Maximálna baudová rýchlosť servera iSeries pre synchrónnu komunikáciu cez RS-232 je však 115,2 Kbps. To žiaľ obmedzuje maximálnu prenosovú rýchlosť v bajtoch na 11,5 kilobajtov/sekundu, pričom terminálový adaptér využívajúci viacnásobnú linku môže dosiahnuť rýchlosť 14/16 neskomprimovaných kilobajtov. Niektoré terminálové adaptéry podporujú synchrónnu komunikáciu cez RS-232 rýchlosťou 128 Kbps, ale maximálna baudová rýchlosť servera iSeries pre synchrónnu komunikáciu cez RS-232 je 64 Kbps.

Server iSeries podporuje asynchrónnu komunikáciu cez V.35 s rýchlosťami do 230,4 Kbps, ale výrobcovia terminálových adaptérov zvyčajne neposkytujú takúto konfiguráciu. Problém je možné vyriešiť konvertormi rozhrania, ktoré konvertujú RS-232 na rozhranie V.35, ale tento prístup nebol testovaný pre server iSeries. Inou možnosťou je použiť terminálové adaptéry s rozhraním V.35, synchrónnou komunikáciou s rýchlosťou 128 Kbps. Hoci taká trieda terminálových adaptérov existuje, len máloktorý výrobca ponúka synchrónny viaclinkový PPP.

Súvisiaci odkaz

"Komutovaná-56" na strane 34
Ak nepotrebujete non-stop pripojenie, používaním komutovanej digitálnej služby, ktorá sa nazýva *Komutovaná-56 (SW56)* môžete ušetriť.

"Terminálové adaptéry ISDN" na strane 39
ISDN vám ponúka digitálne pripojenie, ktoré vám umožní komunikovať a zároveň prenášať hlas, údaje a video, či iné multimediálne aplikácie.

T1/E1 a čiastočné T1

T1/E1 a čiastočné T1 sú dva druhy platných alternatív pripojenia.

T1/E1

Pripojenie T1 zlučuje dokopy 24 64 Kbps (DS0) kanálov s časovým multiplexom (TDM) na 4-žilovom medenom okruhu. Výsledná šírka pásma je 1,544 Mbps. Okruh E1 v Európe a iných častiach sveta zlučuje dokopy 32 64 Kbps kanálov a výsledkom je 2,048 Mbps. Vďaka vopred vyhradeným časovým slotom umožňuje TDM viacerým používateľom zdieľať médium digitálneho prenosu. Veľa digitálnych súkromných pobočkových ústrední (PBX) využíva službu T1 na import viacerých volacích okruhov na jednej linke T1 namiesto vedenia 24 párov vodičov medzi PBX a telefónnou spoločnosťou. Treba si uvedomiť, že T1 možno zdieľať medzi hlas a údaje. Telefónna služba môže využívať podmnožinu z 24 kanálov pripojenia T1 a zvyšné kanály môžu slúžiť na pripojenie k Internetu. 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. K T1/E1 CSU/DSU alebo multiplexoru po sériovom rozhraní V.35 alebo RS 449 sa môžete zvyčajne pripojiť synchrónnym protokolom s rýchlosťami, ktoré sú násobkami 64 Kbps, do 1,544 Mbps alebo 2,048 Mbps. Časovanie v sieti zabezpečuje multiplexor alebo CSU/DSU.

Čiastočné T1

Pri čiastočnom T1 (FT1) si môže zákazník prenajať ľubovoľný násobok 64 Kbps linky T1. FT1 je užitočné tam, kde náklady na vyhradené T1 limitujú skutočnú šírku pásma, ktorú bude používať zákazník. 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. K T1/E1 CSU/DSU alebo multiplexoru po sériovom rozhraní V.35 alebo RS 449 sa môžete zvyčajne pripojiť synchrónnym protokolom s rýchlosťou, ktorá je násobkom 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 pre smerovanie rámcov cez sieť na základe poľa s adresou IP (identifikátor dátového spojenia) v rámci a pre manažovanie trasy alebo virtuálneho pripojenia.

Siete frame-relay v USA podporujú rýchlosti prenosu údajov T1 (1,544 Mbps) a T3 (45 Mbps). Na frame relay sa môžete pozerať ako na spôsob využitia existujúcich liniek T1 a T3, ktoré vlastní poskytovateľ služieb. Väčšina telefónnych spoločnosti teraz poskytuje službu Frame Relay zákazníkom, ktorí požadujú rýchlosti od 56 Kbps do T1. (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 asynchrónny režim prenosu (ATM).

Podpora L2TP (tunelovania) pre pripojenia PPP

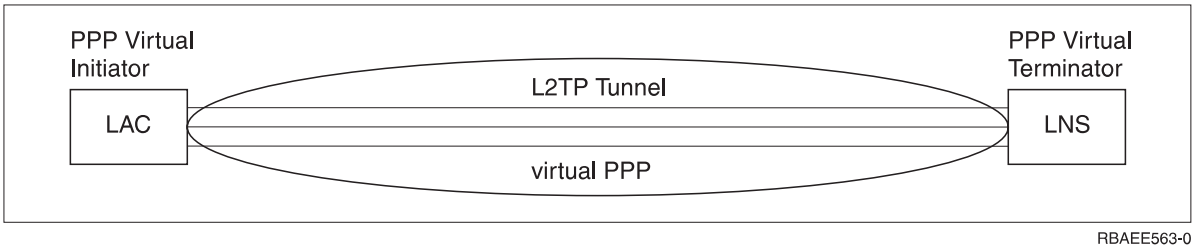
L2TP (Layer 2 Tunneling Protocol) je protokol tunelovania, ktorý rozširuje PPP na podporu tunela spojovacej vrstvy medzi žiadajúcim klientom L2TP (koncentrátor prístupu L2TP alebo LAC) a cieľovým koncovým serverom L2TP (sieťový server L2TP alebo LNS).

Layer 2 Tunneling Protocol

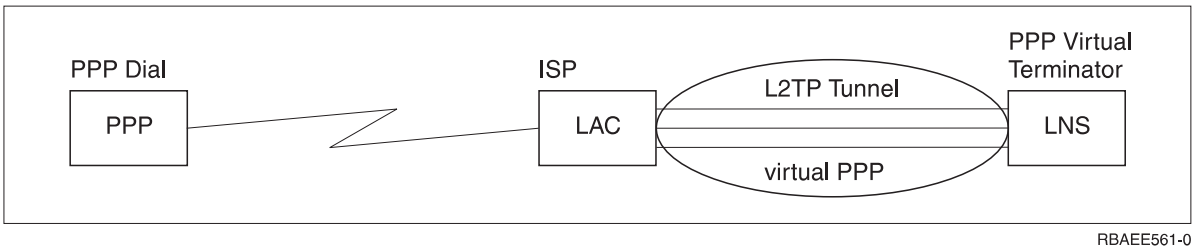
Pomocou tunelov L2TP (Layer 2 Tunneling Protocol) je možné oddeliť miesto, kde končí protokol telefonického pripojenia od miesta, kde je poskytnutý prístup do siete. Z tohto dôvodu sa L2TP nazýva aj *virtuálne PPP*.

Poskytovateľ internetový služieb (ISP) používa režim virtuálnej linky na prevádzkovanie virtuálnych súkromných sietí (VPN). Pozrite si tému Konfigurácia pripojenia L2TP, chráneného VPN, kde nájdete viac informácií o fungovaní IPSec s L2TP.

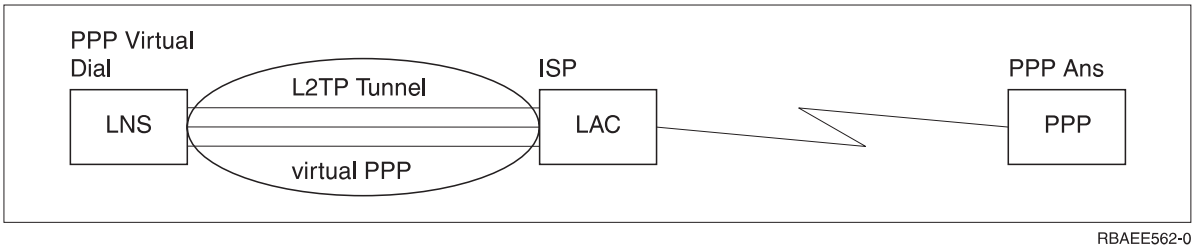
Tieto obrázky ilustrujú tri rozdielne implementácie tunelovania L2TP.



Obrázok 10. Virtuálny iniciátor PPP alebo virtuálny terminátor PPP



Obrázok 11. Iniciátor telefonického pripojenia PPP alebo virtuálny terminátor PPP



Obrázok 12. Virtuálne telefonické pripojenie PPP alebo virtuálne odpovedanie PPP

Protokol L2TP je zdokumentovaný ako štandard Request For Comment, RFC2661. Viac informácií o dokumentoch RFC nájdete na webovej stránke RFC Editor. Tunel L2TP môže pokrývať celú reláciu PPP alebo len jeden segment dvojsegmentovej relácie. To možno vyjadriť štyrmi rôznymi modelmi tunelovania:

Nevynútený tunel:

V modeli nevynúteného tunelu, tunel vytvorí užívateľ, zvyčajne pomocou klienta s podporou L2TP.

Výsledkom je, že klient posiela pakety L2TP do ISP, ktorý ich postupuje do LNS. Pri nevynútenom tunelovaní, ISP nemusí podporovať L2TP a iniciátor tunela L2TP je v skutočnosti v rovnakom systéme ako vzdialený klient. V tomto modeli pokrýva tunel celú reláciu PPP, od klienta L2TP po LNS.

Vynútený tunel - prichádzajúce volania:

V modeli vynúteného tunelu - prichádzajúce volanie, tunel je vytvorený bez zásahu užívateľa a neposkytuje užívateľovi žiadne voľby.

Výsledkom je, že užívateľ posiela pakety PPP do ISP (LAC), ktorý ich uzatvára do L2TP a posiela cez tunel do LNS. Pri tomto modeli musí ISP poskytovať L2TP. V tomto modeli pokrýva tunel len segment relácie PPP medzi ISP a LNS.

Vynútený tunel - vzdialené telefonické pripojenie:

V modeli vynúteného tunelu - vzdialené telefonické pripojenie, domáca brána (LNS) iniciuje tunel k ISP (LAC) a povie ISP, aby vytvoril lokálne volanie klienta PPP, ktorý odpovedá.

Tento model je určený pre prípady, kedy má odpovedajúci vzdialený klient PPP trvalo vytvorené telefónne číslo u ISP. Použije sa vtedy, keď firma, ktorá je zavedená na Internete, potrebuje vytvoriť pripojenie so vzdialenou pobočkou, ktorá potrebuje telefonické pripojenie. V tomto modeli pokrýva tunel len segment relácie PPP medzi LNS a ISP.

Viacskokové pripojenie L2TP:

Viacskokové pripojenie L2TP je spôsob presmerovania premávky L2TP v mene LAC a LNS klienta.

Viacskokové pripojenie sa vytvorí pomocou viacskokovej brány L2TP (systém, ktorý obsahuje profily terminátora a iniciátora L2TP zároveň). Ak chcete vytvoriť viacskokové pripojenie, viacskoková brána L2TP musí vystupovať ako LNS pre množinu LAC a zároveň vystupovať ako LAC pre dané LNS. Od klienta LAC k viacskokovej bráne L2TP sa vytvorí tunel a ďalší tunel sa vytvorí medzi viacskokovou bránou L2TP a cieľovým LNS. Premávka L2TP z LAC klienta je presmerovaná viacskokovou bránou L2TP do cieľového LNS a premávka z cieľového LNS je presmerovaná do LAC klienta.

Podpora PPPoE (DSL) pre pripojenia PPP

DSL (Digital subscriber line) je pomenovanie triedy technológií, ktoré sa používajú na získanie väčšej šírky pásma na existujúcich medených telefónnych rozvodoch, ktoré sú medzi zákazníkom a poskytovateľom ISP.

DSL dovoľuje simultánne používanie hlasových a vysokorýchlostných dátových služieb cez jeden pár medených telefónnych vodičov. 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 poskytuje vysokorýchlostný prenos údajov po linkách z krútených párov z hlavnej pobočky do domácnosti, školy alebo firmy. V niektorých oblastiach sú k dispozícii rýchlosti do 2 Mbps. PPPoE znamená Point to Point Protocol cez Ethernet. PPP sa typicky používa na sériových komunikačných linkách, ako sú telefonické pripojenia modemov. 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, ktoré sa nachádza na oboch koncoch medenej telefónnej linky a dovoľuje pripojenie počítača (alebo LAN) do Internetu cez pripojenie DSL. Na rozdiel od telefonického pripojenia, zvyčajne nevyžaduje vyhradenú telefónnu linku (rozdeľovač POTS dovoľuje simultánne zdieľanie linky). Hoci sa modemy DSL podobajú tradičným analógovým modemom, poskytujú oveľa vyššiu priepustnosť.

Zariadenia pre pripojenia

Servery iSeries používajú pre pripojenia PPP modemy, terminálové adaptéry ISDN, token-ringové adaptéry, ethernetové adaptéry alebo zariadenia CSU/DSU.

V prostredí PPP môžete používať tri druhy spojovacích zariadení:

- Modemy
- CSU/DSU
- Terminálové adaptéry ISDN
- Ethernetové adaptéry (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. Príkazy sa používajú na vynulovanie a inicializovanie modemu a na prikázanie modemu, aby vytočil telefónne číslo 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, ale nové modely je možné definovať cez Navigátor iSeries. 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.

Súvisiaci odkaz

"Softvérové a hardvérové požiadavky" na strane 32
Prostredie PPP vyžaduje, aby ste mali dva alebo viac počítačov, ktoré podporujú PPP. Jeden z týchto počítačov, server iSeries, môže byť buď pôvodca, alebo príjemca.

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.

Súvisiaci odkaz

"Softvérové a hardvérové požiadavky" na strane 32
Prostredie PPP vyžaduje, aby ste mali dva alebo viac počítačov, ktoré podporujú PPP. Jeden z týchto počítačov, server iSeries, môže byť buď pôvodca, alebo príjemca.

"Digitálne služby a DDS" na strane 34
S PPP môžete používať digitálne služby a DDS (Digital Data Services).

Terminálové adaptéry ISDN

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

Bude potrebné, aby ste skontrolovali, či je váš terminálový adaptér určený pre používanie vo vašom serveri iSeries.

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

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. V dialógovom okne **Vlastnosti nového modemu** zadajte správne hodnoty do všetkých polí na záložke 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.

Súvisiace úlohy

"Príklad: Konfigurácia terminálových adaptérov ISDN" na strane 55

Súvisiaci odkaz

"Softvérové a hardvérové požiadavky" na strane 32
Prostredie PPP vyžaduje, aby ste mali dva alebo viac počítačov, ktoré podporujú PPP. Jeden z týchto počítačov, server iSeries, môže byť buď pôvodca, alebo príjemca.

"Digitálna sieť s integrovanými službami (ISDN)" na strane 35
ISDN (Integrated Services Digital Network) poskytuje komutované digitálne prepojenie dvoch koncov. Na rozdiel od iných služieb však môže ISDN prenášať po jednom pripojení hlas aj údaje.

Odporúčania pre terminálový adaptér ISDN:

Existuje niekoľko rôznych terminálových adaptérov, ktoré môžete používať.

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 autentifikáciu CHAP na volajúcej strane, ak konfigurácia odpovedania servera iSeries spôsobí, že server iSeries otvorí autentifikáciu pomocou CHAP. Ak server iSeries otvorí autentifikáciu pomocou PAP, terminálový adaptér Courier I autentifikuje pomocou PAP.

Ak máte modem Courier I spred roku 1999, skontrolujte, či je modem Courier I pripojený k vášmu serveru iSeries káblom V.35, aby ste získali maximálny výkon z vášho pripojenia ISDN. 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 je odporúčaná, hoci má trochu znížený výkon pre iSeries, pretože pripojenia RS-232 sú limitované 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:

V tejto téme sú vyhodnotené terminálové adaptéry. Sú odporúčané pre vytváranie vzdialených pripojení ISDN zo servera iSeries.

3Com Impact IQ ISDN:

Tento terminálový adaptér neodporúčame pre server iSeries z týchto 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 nemusí pripojiť k serveru iSeries pri rýchlostiach vyšších ako 115 200 bps.
- Terminálový adaptér nepodporuje automaticky CHAP (Challenge Handshake Authentication Protocol). Nastavenie S84=0 však dovolí serveru iSeries vykonať 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 neodporúčame pre server iSeries z týchto 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 nemusí pripojiť k serveru iSeries pri rýchlostiach vyšších ako 115 200 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. Vedie to k zníženému výkonu, keď server iSeries posiela údaje na pripojení PPP na viacnásobnej linke.

Spravovanie adries IP

Pripojenia PPP poskytujú niekoľko rôznych množín volieb pre manažovanie adries IP podľa typu profilu pripojenia.

Súvisiaci odkaz

"Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE" na strane 11
Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

Filtrovanie paketov IP

Filtrovanie paketov IP obmedzuje služby pre jednotlivých užívateľov, keď sa prihlásia do siete.

Filtrovanie paketov môže povoliť alebo zakázať prístup podľa cieľa adresy IP, portov alebo oboje. Rozličné politiky sa implementujú definovaním viacerých sád pravidiel filtrovania paketov, pričom každá sada má vlastný identifikátor filtrovania PPP. Pravidlá filtrovania paketov je možné priradiť konkrétnemu profilu pripojenia príjemcu alebo ich priradiť pomocou skupinovej politiky, ktorá aplikuje filtrovacie pravidlá pre kategóriu daného užívateľa. Samotné pravidlá filtrovania paketov nie sú definované v PPP, ale sú definované v pravidlách pre pakety IP v Navigátore iSeries.

Pre pripojenia L2TP by sa na ochranu sieťovej prevádzky malo použiť VPN s filtrovaním IPSec.

Súvisiaci odkaz

"Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE" na strane 11
Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

Súvisiace informácie

Pravidlá pre pakety IP

VPN

Stratégia manažmentu adries IP

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 pripojenia pôvodcu:

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 ste definovali pevné adresy IP pre lokálnu alebo vzdialenú adresu IP, musíte sa presvedčiť, či je vzdialený systém definovaný na akceptovanie vami definovaných adries IP. Typickou aplikáciou je zadefinovať vašu lokálnu adresu IP ako pevnú adresu IP a vzdialenú adresu nechať prideľovať vzdialeným systémom. Systému, ku ktorému sa pripájate, môže byť zadefinovaný rovnakým spôsobom a keď sa pripojíte, tieto dva systémy si vymenia vzájomne adresy IP a získajú tak adresu vzdialeného systému. Toto môže byť užitočné pri dočasných pripojeniach, keď jedna pobočka volá druhú pobočku.

Iným prípadom je, ak chcete umožniť maskovanie adries IP. Napríklad, sa server iSeries pripojí k Internetu cez ISP, dovoľuje to pripojenej sieti za serverom iSeries tiež sa pripojiť k Internetu. Server iSeries v zásade skrýva adresy IP systémov v sieti za lokálnu adresu IP, ktorú mu priradil ISP a zdá sa, že všetka premávka IP pochádza zo servera iSeries. Existujú tiež dodatočné aspekty pre systémy v LAN (zaručenie, že sa ich internetová premávka posiela do servera iSeries) ako aj pre server iSeries, kde musíte začiarknuť políčko 'pridať vzdialený systém ako predvolenú trasu'.

Profily pripojenia prijímača:

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. Stane sa adresou IP, ktorá bude identifikovať koniec pripojenia PPP so serverom 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. Na strane TCP/IP profilu pripojenia príjemcu je možné zadať nasledujúce voľby.

Poznámka: Ak chcete, aby bol vzdialený systém považovaný za súčasť LAN, mali by ste nakonfigurovať smerovanie adresy IP, zadať adresu IP z rozsahu adries IP pre systémy pripojené do LAN a skontrolovať, že pre tento profil pripojenia aj systém iSeries bolo povolené postupovanie IP.

Tabuľka 8. 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 pripojí, dostane jedinečnú adresu IP z definovaného rozsahu. Je to len hostiteľská adresa IP (Maska podsiete je 255.255.255.255) a je len pre viacnásobné profily príjemcu pripojenia.
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 sa určí podľa ID užívateľa, ktoré je definované pre vzdialený systém, keď sa autentifikuje. 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.

Tabuľka 8. Možnosti priraďovania adries IP pre profil príjemcu pripojení (pokračovanie)

Voľba	Opis
Určite dodatočné adresy IP založené na užívateľskom ID vzdialeného systému	Táto voľba vám dovoľuje definovať adresy IP podľa ID užívateľa vzdialeného systému. Táto voľba sa automaticky vyberie (a musí použiť), ak metóda pridelenia vzdialenej adresy je definovaná ako **Podľa ID užívateľa vzdialeného systému**. Táto voľba je tiež dovolená pre metódy priradenia adresy IP Pevná adresa IP a Oblasť adries. Keď sa vzdialený užívateľ pripojí k serveru iSeries, hľadaním sa určí, či je pre tohto užívateľa špecificky definovaná vzdialená adresa IP. Ak je, pre pripojenie sa použije daná adresa IP, maska a množina možných trás. Ak užívateľ nie je definovaný, adresa IP sa nastaví na definovanú pevnú adresu IP alebo ďalšiu adresu IP z oblasti adries.
Povoľte vzdialenému systému určovať vlastné adresy IP	Táto voľba umožní vzdialenému používateľovi zadefinovať si vlastnú adresu IP, ak o to prejaví záujem. Ak sa nedohodnú na použití vlastnej adresy IP, vzdialená adresa IP sa určí definovanou metódou priradenia vzdialenej adresy IP. Táto voľba nie je pôvodne nastavená. Pred jej nastavením treba uvážiť všetky aspekty.
Smerovanie adries IP	Klient s telefonickým pripojením a iSeries musia mať správne nakonfigurované smerovanie adries IP, aby mohol klient pristupovať k ľubovoľným adresám v LAN, do ktorej patrí iSeries.

Autentifikácia systému

Pripojenia PPP so serverom iSeries podporujú niekoľko volieb pre autentifikáciu vzdialených klientov, ktorí vytvárajú telefonické pripojenie k iSeries, ako aj pripojení k ISP a iným serverom, ku ktorým 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 **Autenfikácia** v profile pripojenia v Navigátore iSeries, môžete zadať vaše preferencie pre autentifikáciu systému, vrátane ID užívateľa a hesla na validovanie iSeries pri vytváraní telefonického pripojenia smerom von.

Súvisiaci odkaz

“Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE” na strane 11
Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). Server iSeries sa môže pripojiť k týmto poskytovateľom služieb, aby poskytol pripojenia s vysokou šírkou pásma, ktoré zachovávajú možnosti využitia PPP.

“Scenár: Autentifikácia telefonických pripojení cez RADIUS NAS” na strane 22
NAS (Network Access Server) spustený v serveri iSeries môže smerovať požiadavky o autentifikáciu od klientov s telefonickým pripojením do samostatného servera RADIUS. Ak bude autentifikácia úspešná, RADIUS tiež môže riadiť adresy IP pre užívateľa.

“Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie” na strane 24
Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

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, ID užívateľa a heslo sa vždy šifrujú, preto to je bezpečnejší protokol ako PAP (Password Authentication Protocol). 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.

Súvisiaci odkaz

"Scenár: Pripojenie vzdialených klientov s telefonickým pripojením k vášmu serveru iSeries" na strane 14
Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

"PAP"
Password Authentication Protocol (PAP) používa dvojsmerné dohodnutie, a tak poskytuje rovnocennému systému jednoduchú metódu vytvorenia vlastnej identity.

"EAP"
Extensible Authentication Protocol (EAP) umožňuje, aby autentifikačné moduly tretích strán komunikovali s implementáciou PPP.

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 je odpoveďou na zvýšený dopyt na rozšírenie autentifikácie s bezpečnostnými zariadeniami tretích strán. EAP chráni virtuálne súkromné siete (VPN) pred hackermi, ktorí používajú slovníkové útoky a hádanie hesiel. EAP vylepšuje PAP (Password Authentication Protocol) a CHAP (Challenge Handshake Authentication Protocol).

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 nepodporuje priamo EAP. Môžete však používať vzdialenú autentifikáciu so serverom RADIUS, ktorá môže podporovať niektoré z dodatočných autentifikačných schém opísaných hore.

Súvisiaci odkaz

"PAP"
Password Authentication Protocol (PAP) používa dvojsmerné dohodnutie, a tak poskytuje rovnocennému systému jednoduchú metódu vytvorenia vlastnej identity.

"CHAP-MD5" na strane 43
Challenge Handshake Authentication Protocol (CHAP-MD5) používa algoritmus (MD-5) na vypočítanie hodnoty, ktorú pozná len autentifikačný systém a vzdialené zariadenie.

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 pošle pár ID užívateľa a heslo do autentifikujúceho 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, ID užívateľa a heslo sa nikdy nešifrujú, preto existuje riziko ich odhalenia pri útokoch hackerov. Z tohto dôvodu by ste mali vždy používať CHAP, ak to je možné.

Súvisiaci odkaz

"CHAP-MD5" na strane 43
Challenge Handshake Authentication Protocol (CHAP-MD5) používa algoritmus (MD-5) na vypočítanie hodnoty, ktorú pozná len autentifikačný systém a vzdialené zariadenie.

"EAP" na strane 44
Extensible Authentication Protocol (EAP) umožňuje, aby autentifikačné moduly tretích strán komunikovali s implementáciou PPP.

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, posiela informácie o užívateľovi a pripojení do určeného servera RADIUS pomocou štandardného protokolu RADIUS, ktorý je definovaný v RFC 2865.

Servery RADIUS sa podieľajú na prijatých požiadavkách o pripojenie autentifikovaním užívateľa a následným vrátením všetkých potrebných konfiguračných informácií do NAS a NAS (server iSeries) môže poskytovať autorizované služby autentifikovanému užívateľovi s telefonickým pripojením.

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 zabezpečovací systém alebo zákazníkom vytvorený bezpečnostný systém. Server RADIUS pošle späť serveru iSeries všetky služby, ktoré je autentifikovaný užívateľ autorizovaný používať, napríklad adresu IP. Požiadavky o účtovanie RADIUS sú spracúvané podobne. Informácie o kontách vzdialeného používateľa môžu byť zaslané na vybraný určený RADIUS server. Štandardný autorizačný protokol RADIUS je definovaný v RFC 2866. Autorizačný RADIUS server spracúva prijaté žiadosti o kontá protokolovaním informácií zo žiadosti o konto RADIUS.

Súvisiaci odkaz

"Scenár: Autentifikácia telefonických pripojení cez RADIUS NAS" na strane 22
NAS (Network Access Server) spustený v serveri iSeries môže smerovať požiadavky o autentifikáciu od klientov s telefonickým pripojením do samostatného servera RADIUS. Ak bude autentifikácia úspešná, RADIUS tiež môže riadiť adresy IP pre užívateľa.

Validizačný zoznam

Validačný zoznam sa používa na ukladanie informácií o identifikátoroch užívateľov a heslách vzdialených užívateľov.

Môžete používať už vytvorené validizačné zoznamy alebo si vytvoriť vlastný na autentifikačnej strane Profilu príjemcu pripojenia. Položky validačného zoznamu tiež vyžadujú, aby ste identifikovali typ autentifikačného protokolu, ktorý je spojený s ID užívateľa a heslom. To môže byť **zašifrované - CHAP-MD5/EAP** alebo **nezašifrované - PAP**.

Viac informácií nájdete v online pomoci.

Súvisiaci odkaz

"Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie" na strane 24
Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Informácie o šírke pásma - viacnásobná linka

Často pri vykonávaní určitých úloh požadujete dodatočnú šírku pásma, ktorú však nepotrebujete vždy.

V týchto prípadoch nemusí pomôcť zakúpenie špecializovaného hardvéru a drahých komunikačných liniek. Viaclinkový protokol PPP Protocol (MP) zoskupuje viaceré linky PPP do formy jednotlivej virtuálnej linky, alebo

″zväzku″. Agregácia viacerých liniek zvýši celkovú efektívnu šírku pásma medzi dvomi systémami, ktoré používajú štandardné modemy a telefónne linky. Do zväzku MP môžete zahrnúť najviac 6 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 dokumentoch RFC nájdete na webovej stránke RFC Editor.

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 je možné pridávať alebo odoberať zo zväzku, keď využitie šírky pásma prekročí hodnoty definované konfiguráciou. 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.

Súvisiaci odkaz

“Súvisiace informácie pre PPP” na strane 64
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Vytvorenie profilu pripojenia

Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

Profil pripojenia je logickou reprezentáciou týchto konkrétnych informácií:

- Typ linky a profilu
- Nastavenia viacnásobnej linky
- Vzdialené telefónne čísla 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 Navigátore iSeries vyberte váš systém a rozviňte **Sieť → Služby vzdialeného prístupu**.
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 profilu pripojenia point-to-point vyberte typ protokolu.
5. Určite výbery režimov.
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.

   Súvisiace úlohy

   "Priradenie modemu k opisu linky" na strane 56

   Súvisiaci odkaz

   "Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE" na strane 11
   Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). 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 s telefonickým pripojením k vášmu serveru iSeries" na strane 14
   Vzdialení používatelia, napríklad dialŕkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

   "Scenár: Pripojenie vašej siete LAN modemom na Internet" na strane 16
   Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na Internet. Na pripojenie servera iSeries k 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" na strane 19
   Modem umožňuje, aby si dve vzdialené lokality (napríklad centrála a pobočka) navzájom vymieňali údaje. PPP môže spojiť dve siete LAN vytvorením pripojenia medzi serverom iSeries v centrálnej pobočke a iným serverom iSeries v pobočke.

   "Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie" na strane 24
   Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Typ protokolu: PPP alebo SLIP (Serial Line Internet Protocol)

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 (Serial Line Internet Protocol) ako protokol na výber 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 stále používa a je stále podporovaný v serveri iSeries. IBM však odporúča, aby ste pri nastavovaní pripojení point-to-point používali 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 používate jedno z nasledujúceho na pripojenie cez telefónnu linku: modem (interný alebo externý) alebo externý terminálový adaptér ISDN.

Typ pripojenia komutovanou linkou rozoznáva tieto režimy prevádzky:

Odpoveď

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

Vytáčanie

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

Vytáčať na žiadosť (len vytáčanie)

Tento režim prevádzky vyberte v prípade, ak chcete serveru iSeries umožniť automaticky vytvoriť telefonické pripojenie k vzdialenému systému, ak sa v systéme zistí premávka TCP/IP. Pripojenie sa ukončí, keď je prenos údajov ukončený a po stanovený čas sa nevyskytne žiadna prevádzka TCP/IP.

Vytáčať na žiadosť (rovnocenná strana 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 žiadosť (povolená vzdialená strana)

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:

Vyberte tento typ pripojenia, ak máte vyhradenú linku medzi lokálnym serverom iSeries a vzdialeným systémom. 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.

Pôvodca

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):

Vyberte tento typ pripojenia, ak chcete 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 sa chcete pripojiť k serveru iSeries cez tunel L2TP.

Pôvodca

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 vytvoriť viacskokové pripojenie.

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.

Linka PPPoE:

Pripojenia PPPoE (Point-to-Point over Ethernet) používajú virtuálnu linku na posielanie údajov PPP (cez ethernetový adaptér) do modemu DSL (Digital Subscriber Line), ktorý vám dodal váš poskytovateľ internetových služieb (ISP). Tento modem je tiež pripojený do ethernetovej LAN.

Toto dovoľuje vysokorýchlostný prístup k Internetu pre užívateľov LAN cez relácie PPP cez server iSeries. Po vytvorení pripojenia medzi iSeries a ISP, jednotliví užívatelia v LAN môžu vytvoriť jedinečné relácie s ISP cez PPPoE.

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

Konfigurácia spojenia

Konfigurácia pripojenia definuje typ linkovej služby, ktorú váš profil pripojenia PPP používa na nadviazanie pripojenia.

Typy linkovej služby závisia od typu pripojenia, ktoré zadáte.

Súvisiaci odkaz

“Scenár: Pripojenie vášho servera iSeries ku koncentrátoru prístupov PPPoE” na strane 11
Veľa poskytovateľov ISP ponúka vysokorýchlostný prístup k Internetu cez DSL pomocou PPPoE (Point-to-Point Protocol over Ethernet). 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 s telefonickým pripojením k vášmu serveru iSeries” na strane 14
Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

“Scenár: Pripojenie vašej siete LAN modemom na Internet” na strane 16
Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na Internet. Na pripojenie servera iSeries k 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” na strane 19
Modem umožňuje, aby si dve vzdialené lokality (napríklad centrála a pobočka) navzájom vymieňali údaje. PPP môže spojiť dve siete LAN vytvorením pripojenia medzi serverom iSeries v centrálnej pobočke a iným serverom iSeries v pobočke.

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 vždy používa rovnaký prostriedok komunikačného portu servera iSeries.

Ak to je potrebné, samostatnú analógovú linku je možné nakonfigurovať ako zdieľanú medzi profilom na odpovedanie a profilom na vytáčanie. Dynamické zdieľanie prostriedkov je nová funkcia navrhnutá na zvýšenie ich použiteľnosti. Do V5R2, prostriedky modemu boli priradené hneď po začatí používania profilu. 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. Existujú dva prípady: prvý, profil vytvorenia pripojenia bol spustený pred profilom na odpovedanie; druhý, profil na odpovedanie bol spustený pred profilom vytvorenia pripojenia. 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. Po ukončení profilu vytvorenia pripojenia, profil na odpovedanie požiada o linku a spustí sa. V druhom prípade počká spustený odpovedajúci profil na prichádzajúce pripojenie. Kým sa nespustí prichádzajúce pripojenie, profil vytvorenia pripojenia, ktorý bol spustený ako druhý, si ″požičia″ linku od profilu na odpovedanie, ktorý ″prepožičia″ linku. Potom sa vytvorí odchádzajúce pripojenie. Po ukončení pripojenia, profil vytvorenia pripojenia vráti linku profilu na odpovedanie, ktorý bude znovu schopný prijímať prichádzajúce pripojenia. Ak chcete povoliť funkciu zdieľania, kliknite na záložku Modem pre opis komutovanej linky a vyberte **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. Keď sa spustí pripojenie PPP, server iSeries vyberie nevyužitú linku z oblasti liniek. 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.

  Okrem toho, ak sú prostriedky nakonfigurované ako zdieľané (povoľte dynamické zdieľanie prostriedkov), hlavne pre odchádzajúce pripojenia je väčšia dostupnosť dodatočných 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 bude určená na použitie všetkými štyrmi profilmi pripojenia, preto môžu byť naraz aktívne dve pripojenia. 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.

Konfigurácia oblastí liniek

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

1. V Navigátore iSeries vyberte váš systém a rozviňte **Sieť → Služby vzdialeného prístupu**.
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**. Kliknite na **OK** a Navigátor iSeries otvorí okno s vlastnosťami pre tento profil 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 strane Všeobecné pomenujte profil a zadajte opis.
6. Na strane Pripojenie zadajte názov pre oblasť liniek a kliknite na **Nová**. Zobrazí sa dialógové okno **Vlastnosti novej oblasti liniek**, kde budú zobrazené 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. Zadajte potrebné informácie na iných stranách (napríklad Nastavenia 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.

Súvisiaci odkaz

"Scenár: Pripojenie vzdialených klientov s telefonickým pripojením k vášmu serveru iSeries" na strane 14
Vzdialení používatelia, napríklad diaľkoví pracovníci alebo mobilní klienti často požadujú prístup do siete firmy. Títo klienti s telefonickým prístupom môžu získať prístup k serveru iSeries s PPP.

"Scenár: Pripojenie vašej siete LAN modemom na Internet" na strane 16
Správcovia obyčajne nastavujú kancelárske siete tak, aby umožnili zamestnancom prístup na Internet. Na pripojenie servera iSeries k 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" na strane 19
Modem umožňuje, aby si dve vzdialené lokality (napríklad centrála a pobočka) navzájom vymieňali údaje. PPP môže spojiť dve siete LAN vytvorením pripojenia medzi serverom iSeries v centrálnej pobočke a iným serverom iSeries v pobočke.

Podpora profilov viacerých 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, ak chcete, aby sa k vášmu serveru iSeries pripájalo viac užívateľov, ale nechcete zadávať samostatný profil pripojenia point-to-point pre obsluhu každej linky PPP. 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 viacerých pripojení:

Pre profily viacerých pripojení môžete použiť lokálnu adresu IP, ale musí to byť existujúca adresa IP, ktorá je definovaná vo vašom serveri iSeries. Na výber existujúcej adresy IP môžete použiť sťahovaciu ponuku Lokálna adresa IP. Vzdialení užívatelia môžu pristupovať k prostriedkom, ktoré sú vo vašej lokálnej sieti, ak ako lokálnu adresu IP pre váš profil PPP vyberiete adresu lokálnu IP servera iSeries. 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 adresu IP servera iSeries alebo nechcete, aby vzdialení užívatelia mali prístup do LAN, musíte zadefinovať virtuálnu adresu IP pre server iSeries. Virtuálna adresa IP je tiež známa ako bezokruhové rozhranie. Vaše profily point-to-point môžu používať túto adresu IP ako ich lokálnu adresu IP. Táto adresa nie je naviazaná na fyzickú sieť, preto nebude automaticky postupovať premávku do iných sietí, ktoré sú pripojené k vášmu serveru iSeries.

Na vytvorenie virtuálnej adresy IP vykonajte tieto kroky:

1. V Navigátore iSeries rozviňte váš server a kliknite na **Sieť → Konfigurácia TCP/IP → IPV4 → Rozhrania**.
2. Kliknite pravým tlačidlom myši na **Rozhrania** a vyberte **Nové rozhranie → Virtuálne 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. Na použitie adresy IP s vašim profilom môžete použiť sťahovaciu ponuku z poľa Lokálna adresa IP, ktoré je na strane Nastavenia TCP/IP.

   Poznámka: Virtuálna adresa IP musí byť aktívna pred spustením vášho profilu viacnásobných pripojení, inak sa profil nespustí. Ak chcete aktivovať adresu IP po vytvorení rozhrania, vyberte voľbu na spustenie adresy IP pomocou sprievodcu rozhraním.

Oblasti vzdialených adries IP pre profily viacerých pripojení:

Oblasti vzdialených adries IP tiež môžete používať s profilmi viacerých pripojení. Len typický profil jedného pripojenia point-to-point vám umožňuje určiť jednu vzdialenú adresu IP, ktorá je daná volajúcemu systému, keď sa vytvorí spojenie. Viacerí volajúci sa môžu pripojiť súčasne, preto sa oblasť vzdialených adries IP používa na definovanie začiatočnej vzdialenej adresy IP, ako aj rozsahu ďalších adries IP, ktoré sú dané 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 oblasti vzdialených adries IP pre odpovedanie alebo zastavenie profilu pripojenia point-to-point, ktoré sa používa viacerými prichádzajúcimi pripojeniami.

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 IP už používa, použije sa ďalšia adresa IP z rozsahu. Napríklad predpokladajme, že Začiatočná adresa IP je 10.1.1.1 a Počet adries IP je definovaný ako 5. Adresy IP v 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 sa však použijú všetky adresy IP z oblasti, ďalšie požiadavky o pripojenie budú odmietnuté, kým sa neuvoľní niektorá adresa IP.
- Ak chcete vyhradiť špecifické adresy IP niektorým vzdialeným systémom a ostatným pripájajúcim sa systémom prideľovať adresy IP z oblasti, vykonajte tieto kroky:
  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 určí, či je pre tohto užívateľa definovaná špecifická adresa IP. V takomto prípade sa vzdialenému systému pridelí adresa IP, inak dostane adresu IP z oblasti vzdialených adries IP.

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). Opisy modemov pre bežne používané modemy boli definované pre server iSeries.

Súvisiaci odkaz

"Odstraňovanie problémov s PPP" na strane 62
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.

Konfigurácia nového modemu

Dozviete sa tu, ako nakonfigurovať nový modem.

Ak chcete nakonfigurovať nový modem, vykonajte nasledujúce kroky.

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. Na paneli Všeobecné zadajte správne hodnoty do všetkých políčok.
4. Voliteľné: Kliknite na záložku **Dodatočné parametre**, na ktorej môžete pridať všetky potrebné inicializačné príkazy pre váš modem.
5. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu Vlastnosti nového modemu.

Použitie existujúceho opisu modemu

Ak chcete určiť, či môžete použiť existujúci opis modemu, vykonajte tieto kroky:

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Vyberte **Modemy**.
3. Prezrite si zoznam modemov a nájdite výrobcu, model a značku svojho modemu.

   Poznámka: Ak sa váš modem nachádza na tomto zozname, nemusíte vykonať žiadne ďalšie kroky.
4. Kliknite pravým tlačidlom na opis modemu, ktorý sa najviac podobá na váš modem a vyberte **Vlastnosti**, aby sa zobrazili 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. Inak musíte vytvoriť modem opisu pre váš modem a pridať ho do zoznamu modemov.

Vytvorenie opisu modemu na základne predošlého opisu modemu

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

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Vyberte **Modemy**.
3. V zozname modemov kliknite pravým tlačidlom myši na **Generický hayes** a vyberte **Nový modem podľa**.
4. V dialógovom okne **Nový modem** zmeňte príkazové reťazce, aby sa zhodovali s informáciami, ktoré vyžaduje váš modem.

Súvisiaci odkaz

"Nastavenie príkazových reťazcov modemu" na strane 55

"Odstraňovanie problémov s PPP" na strane 62
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.

Nastavenie príkazových reťazcov modemu

Ekvivalentný príkazový reťazec pre svoj modem nájdete v užívateľskej príručke. V opise modemu použite výrobcom odporúčané nastavenie.

Tabuľka 9. Modemy definované v serveri iSeries a príkazové reťazce

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

Súvisiace koncepty

"Konfigurácia nového modemu" na strane 54
Dozviete sa tu, ako nakonfigurovať nový modem.

Príklad: Konfigurácia terminálových adaptérov ISDN

Nasledujúci príklad opisuje konfiguráciu terminálového adaptéru ISDN.

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Pravým tlačidlom myši kliknite na **Modemy** a vyberte **Nový modem**.
3. Na paneli Všeobecné zadajte správne hodnoty do všetkých políčok.
4. **Voliteľný:** Kliknite na záložku Parametre ISDN a pridajte všetky potrebné inicializačné príkazy pre váš 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 vykonať server iSeries

   Následne, tieto príkazy by mali obsahovať a byť limitované na tieto nastavenia:

   - 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 zistenie stavu aktivity rozhrania *U* (ATD*x*), ktorý dovoľuje serveru iSeries určiť, kedy bola získaná synchronizácia s prepínačom ISDN centrálnej pobočky. Znak *x* môže byť ľubovoľná číslica, ktorá je dovolená 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.

Súvisiaci odkaz

"Terminálové adaptéry ISDN" na strane 39
ISDN vám ponúka digitálne pripojenie, ktoré vám umožní komunikovať a zároveň prenášať hlas, údaje a video, či iné multimediálne aplikácie.

Priradenie modemu k opisu linky

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu → Profily pripojenia pôvodcu alebo Profily pripojenia prijímača**.
2. Vyberte jednu z uvedených možností:
   - Ak chcete pracovať s existujúcim profilom pripojenia, kliknite pravým tlačidlom myši na profil pripojenia a vyberte **Vlastnosti**.
   - Ak chcete pracovať s novým profilom pripojenia, vytvorte nové pripojenie.
3. Zo strany Vlastnosti nového profilu point-to-point vyberte panel **Pripojenie** a kliknite na **Nové**.
   - Zadajte názov konfigurácie spojenia.
   - Kliknite na **Nové**, aby sa otvorilo okno Vlastnosti novej linky
4. V okne Vlastnosti novej linky kliknite na záložku **Modem** a vyberte modem zo zoznamu. 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. Ak chcete povoliť túto funkciu, vyberte voľbu **Povoliť dynamické zdieľanie prostriedkov** na záložke Modem v okne na konfiguráciu linky PPP. Linky PPP môžete konfigurovať na záložke Pripojenie v Profiloch pôvodcu a príjemcu pripojenia.

Súvisiace úlohy

"Vytvorenie profilu pripojenia" na strane 46
Prvý krok pri konfigurovaní pripojenia PPP medzi systémami je vytvorenie profilu pripojenia v serveri iSeries.

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.

Pozrite si dokumentáciu k Microsoft Windows, kde nájdete informácie o konfigurovaní telefonického pripojenia v PC. Nezabudnite špecifikovať alebo zadať tieto informácie:

- Typ telefonického pripojenia by mal byť **PPP**.
- Ak nepoužívate šifrované heslá, skontrolujte, či používate MD-5 CHAP (MS-CHAP nie je podporované serverom iSeries). Niektoré verzie Windows nepodporujú priamo MD-5 CHAP, ale dajú sa nakonfigurovať podľa dodatočných informácií od spoločnosti Microsoft.
- Ak používate nezašifrované (alebo nezabezpečené) heslá, automaticky sa použije PAP (Password Authentication Protocol). Server iSeries nebude podporovať žiadny iný typ nezabezpečeného protokolu.

- Adresovanie IP je zvyčajne zadefinované vzdialeným systémom, alebo v tomto prípade serverom iSeries. Ak plánujete používať alternatívne metódy adresovania IP (napríklad definovanie vlastných adries IP), skontrolujte, či je server iSeries nakonfigurovaný na akceptovanie vašej metódy adresovania.
- Pridajte adresu IP DNS, ak sa to týka vášho prostredia.

Konfigurácia prístupu na Internet cez AT&T Global Network

Pri komunikácii s AT&T Global Network sú vyžadované špeciálne profily.

Ak chcete pristupovať k tejto službe, môžete použiť Sprievodcu telefonickým pripojením AT&T Global Network, ktorý vám pomôže nakonfigurovať profil komutovaného pripojenia PPP k 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.

Pripojenie k AT&T Global Network môžu používať dva typy aplikácií:

- **Výmena pošty**: Dovoľuje vám pravidelne prijímať poštu z jedného konta AT&T Global Network a posielať ju do vášho servera iSeries na distribúciu vašim užívateľom Lotus alebo užívateľom SMTP (Simple Mail Transfer Protocol).
- **Telefonické pripojenie siete**: Použite ostatné aplikácie využívajúce telefonické pripojenie k AT&T Global Network, ako je štandardný prístup k Internetu.

Profily pripojení AT&T Global Network môžete udržiavať rovnako ako ostatné profily pripojení PPP.

Na použitie sprievodcu pripojením k AT&T Global Network sa vyžaduje jeden z týchto 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 WAN IOA V.90
- 2793 Dvojportový WAN IOA, s integrovaným modemom V.92 na porte 1 a štandardným komunikačným rozhraním na porte 2. Tento model nahrádza model 2771.
- 2805 Štvorportový WAN IOA s integrovaným modemom V.92. To nahradí modely 2761 a 2772.

Pred spustením sprievodcu pripojením k AT&T Global Network musíte zhromaždiť nasledujúce informácie o vašom prostredí:

- Informácie o konte AT&T Global Network (číslo konta, ID užívateľa a heslo) pre aplikáciu na výmenu pošty alebo aplikáciu využívajúcu telefonické pripojenie siete.
- 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 pripojením AT&T Global Network, vykonajte tieto kroky:

1. V Navigátore iSeries rozviňte váš server a sprístupnite **Sieť → Služby vzdialeného prístupu**.
2. Kliknite pravým tlačidlom myši na **Profily pripojenia pôvodcu** a vyberte **Nové telefonické pripojenie k AT&T Global Network**.
3. Po spustení sprievodcu pripojením k AT&T Global Network kliknite na **Pomoc**, aby sa zobrazili informácie k práci s panelom.

Sprievodcovia pripojením

Sprievodcovia pripojením vás prevedú cez konfiguráciu profilu pripojenia.

Sprievodca novým telefonickým pripojením

Tento sprievodca vás prevedie krokmi na konfiguráciu profilu telefonického pripojenia na prístup k vášmu ISP alebo intranetu. Dokončenie sprievodcu môže vyžadovať získanie niektorých informácií od vášho administrátora siete alebo ISP. Viac informácií o používaní tohto sprievodcu nájdete v online pomoci.

Sprievodca univerzálnym pripojením IBM

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.

Súvisiace informácie

Konfigurácia univerzálneho pripojenia

Konfigurácia politiky skupinového prístupu

Zložka **Skupinové politiky prístupu** pod Profilmi pripojenia prijímača poskytujú voľby pre konfiguráciu parametrov pripojenia point-to-point, ktoré sa týkajú skupiny vzdialených užívateľov. 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 Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu → Profily pripojenia prijímača**.
2. Kliknite pravým tlačidlom myši 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 **Viac liniek** a nastavte konfiguráciu viacnásobnej linky.

   Konfigurácia viacnásobnej linky určuje, že chcete spojiť viacero fyzických liniek do zväzku. Maximálny počet liniek vo zväzku je 6. Typ nastavenia linky je známy až po vytvorení pripojenia, preto je predvolená hodnota vždy 1. Skupinová politika sa môže použiť na rozšírenie alebo obmedzenie schopností protokolu pre viacnásobné linky.

   Maximálny počet liniek vo zväzku stanovuje maximálny počet spojení (alebo liniek), z ktorých chcete vytvoriť jednu logickú linku. Maximálny počet liniek nemôže byť väčší ako počet voľných liniek, ak je táto skupinová politika aplikovaná na reláciu pre profil PPP.

   Ak chcete určiť, že pripojenie sa vytvorí len v prípade, ak vzdialený systém podporuje BACP (Bandwidth Allocation Protocol), začiarknite **Vyžadovať protokol pre vyhradenie šírky pásma)**. Ak nemôže byť použitý BACP, je povolená len samostatná linka.
5. Kliknite na záložku **Nastavenia TCP/IP**, ak chcete povoliť ľubovoľné z týchto nastavení:

   Povoliť vzdialenému systému pristupovať k iným sieťam (postupovanie IP). Táto voľba určuje, či chcete definovať postupovanie IP. Ak vyberiete túto voľbu, povolíte serveru iSeries vystupovať ako smerovač pre toto pripojenie. Datagramy, ktoré nie sú určené pre tento server iSeries, majú dovolené prejsť cez tento systém do pripojenej siete. Ak túto voľbu necháte prázdnu, IP zničí všetky datagramy zo zdrojového systému, ktoré nie sú určené pre žiadnu z adries, ktoré sú lokálne pre tento server iSeries.

   Nepovolenie postupovania IP môže mať bezpečnostné dôvody. Opakom sú ISP, ktorí vo všeobecnosti poskytujú postupovanie IP. Toto nastavenie má vplyv len v prípade, ak je povolené postupovanie datagramov IP pre celý systém, inak bude ignorované, aj keď ho aktivujete. Postupovanie datagramov IP je možné zobraziť na záložke **Všeobecné** na strane Vlastnosti IPv4.

   Požadovať komprimáciu hlavičky TCP/IP (VJ). Táto voľba určuje, či má IP komprimovať informácie hlavičky po vytvorení pripojenia. Komprimácia zvyčajne zvyšuje výkon, hlavne pre interaktívnu premávku alebo pomalé sériové linky. Komprimácia záhlavia sa vykonáva podľa Van Jacobsonovej (VJ) metódy, ktorá je definovaná v RFC 1332. Pri PPP sa komprimácia stanovuje pri nadviazaní pripojenia. Ak druhý koniec pripojenia nepodporuje komprimáciu VJ, server iSeries vytvorí pripojenie, ktoré nepoužíva komprimáciu.

   Použiť pre toto pripojenie pravidlá paketov IP. 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.

Aplikovanie skupinovej politiky na užívateľa so vzdialeným prístupom

Skupinovú politiku môžete aplikovať na užívateľa so vzdialeným prístupom, keď nastavujete vlastnosti point-to-point pre nový profil pripojenia prijímateľa.

Ak chcete aplikovať skupinovú politiku na užívateľa so vzdialeným prístupom, vykonajte tieto kroky:

1. Kliknite na **Autentifikácia**, aby sa otvorila strana Autentifikácia.
2. Kliknite na **Vyžadovať od tohto servera iSeries kontrolu identity vzdialeného systému**.
3. Vyberte **Autentifikovať lokálne pomocou validizačného zoznamu**.
4. Ak neexistuje validačný zoznam, vyberte ho zo 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 okne Pridanie užívateľa zadajte tieto informácie:
   a. Vyberte autentifikačný protokol, pre ktorý je definované dané meno používateľa.
   b. Zadajte meno používateľa a heslo.

      Poznámka: Kvôli bezpečnosti odporúčame, aby ste nepoužili rovnaké heslo pre užívateľa definovaného pre CHAP (Challenge Handshake Authentication Protocol 22314), EAP (Extensible Authentication Protocol) a PAP (Password Authentication Protocol).

   c. Začiarknite **Aplikovať skupinovú politiku na užívateľa**, vyberte skupinovú politiku zo zoznamu a kliknite na **Otvoriť**.

   Môžete zmeniť vlastnosti skupinovej politiky alebo pracovať s existujúcim nastavením.
7. Kliknutím na **OK** dokončíte konfiguráciu a vrátite sa na stranu Vlastnosti pripojenia point-to-point.

Súvisiaci odkaz

“Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie” na strane 24
Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Súvisiace informácie

Filtrovanie IP a preklad sieťových adries (NAT)

Použitie pravidiel filtrovania paketov IP na pripojenie PPP

Na obmedzenie prístupu užívateľov alebo skupín k adresám IP vo vašej sieti môžete použiť súbor pravidiel pre pakety.

Téma Filtrovanie paketov IP a pravidlá NAT v Informačnom centre opisuje, ako vytvoriť pravidlá pre pakety IP, ktoré môžete použiť pre profil pripojenia PPP.

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. Začiarknite **Použiť pre toto pripojenie pravidlá pre pakety IP** a vyberte identifikátor filtra PPP zo zoznamu.
  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. Začiarknite **Použiť pre toto pripojenie pravidlá pre pakety IP** a vyberte identifikátor filtra PPP zo zoznamu.
4. Kliknutím na **OK** sa aplikuje filter PPP.

Súvisiaci odkaz

"Scenár: Riadenie prístupu vzdialených užívateľov k zdrojom, ktoré používajú Skupinové politiky a IP filtrovanie" na strane 24
Skupinové politiky prístupu identifikujú presné skupiny užívateľov pre pripojenie a dovoľujú vám aplikovať spoločné atribúty pripojenia a nastavenia bezpečnosti pre celú skupinu. V kombinácii s filtrovaním IP vám toto umožňuje vo vašej sieti povoliť a zakázať prístup konkrétnych adries IP.

Povolenie služieb RADIUS a DHCP pre profily pripojenia

Ak chcete povoliť služby RADIUS alebo DHCP pre profily pripojenia prijímateľa PPP, vykonajte nasledujúce kroky.

1. V Navigátore iSeries vyberte váš server a rozviňte **Sieť → Služby vzdialeného prístupu**.
2. Kliknite pravým tlačidlom myši 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. Vyberte **Povoliť pripojenie k RADIUS Network Access Server**
   b. Označte **Povoliť RADIUS pre autentifikáciu**.
   c. Ak to je aplikovateľné na vaše riešenie RADIUS, môžete tiež povoliť účtovanie RADIUS a konfiguráciu adresy TCP/IP.
5. Kliknite na tlačidlo **Nastavenia RADIUS NAS** a nakonfigurujte pripojenie k serveru RADIUS.
6. Kliknite na **OK**, aby ste sa vrátili do Navigátora iSeries.

Súvisiaci odkaz

"Scenár: Autentifikácia telefonických pripojení cez RADIUS NAS" na strane 22
NAS (Network Access Server) spustený v serveri iSeries môže smerovať požiadavky o autentifikáciu od klientov s telefonickým pripojením do samostatného servera RADIUS. Ak bude autentifikácia úspešná, RADIUS tiež môže riadiť adresy IP pre užívateľa.

Manažovanie PPP

Dozviete sa tu o úlohách manažovania PPP, ktoré môžete vykonať v serveri iSeries.

Súvisiaci odkaz

"Súvisiace informácie pre PPP" na strane 64
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Nastavenie vlastností profilov pripojenia PPP

Keď vytvárate profil pripojenia, zvyčajne vyberáte protokol, typ pripojenia a režim prevádzky pre nový profil pripojenia v okne Nastavenie profilu pripojenia point-to-point.

Po zadaní vašich výberov v tomto okne sa zobrazí list vlastností pripojenia. Výbery, ktoré zadáte v okne Nastavenie profilu pripojenia point-to-point určujú strany a poradie záložiek listu vlastností profilu pripojenia. Stránka vlastností je iná pre profily pôvodcu a iná pre profily príjemcu pripojenia.

Tieto pokyny môžete použiť na vyplnenie každej strany okna **Vlastnosti nového pripojenia profil point-to-point**. Nastavenia, ktoré vyberiete na každej strane, závisia od vášho prostredia a typu pripojenia, ktoré konfigurujete. Online pomoc Navigátora iSeries opisuje každú voľbu, ktorá je zobrazená v okne. Viac informácií nájdete aj v príkladoch a postupoch pre PPP.

Monitorovanie aktivity PPP

Na zobrazenie profilu pripojenia a protokolu relácie môžete použiť Navigátora iSeries.

Informácie o úlohách pripojení 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.
- Vlákno pripojenia PPP v QTPPPCTL sa vykonáva pod menom užívateľa QTCP.
- 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 Navigátore iSeries rozviňte váš server a sprístupnite **Sieť → Služby vzdialeného prístupu**. 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:
   - **Pripojenia** otvorí okno na zobrazenie informácií o všetkých pripojeniach, ktoré sú priradené k profilu. Môže ísť o údaje o aktuálnom pripojení, predchádzajúcich pripojeniach alebo o aktuálnych aj predchádzajúcich pripojeniach. Sú k dispozícii voľby na zobrazenie výstupu úlohy, detailov pripojenia, protokolov volaní alebo protokolov správ pre každé pripojenie.
   - **Vlastnosti** - otvorí strany Vlastností na zobrazenie aktuálnych vlastností pre pripojenie.

Zobrazenie informácií o pripojení:

1. V Navigátore iSeries rozviňte váš server a sprístupnite **Sieť → Služby vzdialeného prístupu**. Vyberte **Profil pripojenia pôvodcu** alebo **Profil pripojenia prijímača**.
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 a predošlé). Stavové pole označuje aktuálny stav pripojenia. Môžu sa zobraziť dodatočné informácie ako ID užívateľa použitého užívateľa, ID vlákna, lokálna a vzdialená adresa IP a názov úlohy PPP, v závislosti od stavu každej úlohy PPP.
3. Ak chcete zobraziť výstup úloh, detaily pre pripojenie, protokoly volania alebo protokoly správ, kliknite pravým tlačidlom myši na pripojenie, aby ste povolili tlačidlá.
4. Ak chcete zobraziť QTPPPCTL, kliknite na **Úlohy**. V okne pripojení kliknite pravým tlačidlom myši na názov úlohy a vyberte **Výstup pre tlačiareň** alebo **Protokol úloh**, aby sa zobrazili informácie o všetkých vláknach, ktoré sú priradené k QTPPPCTL.
5. Ak si chcete prezrieť podrobnosti o pripojení, kliknite na **Podrobnosti**. Možno zobraziť len podrobnosti o aktuálne aktívnych pripojeniach. Okno s detailmi zobrazuje dodatočné informácie o pripojení pre toto konkrétne pripojenie.
6. Ak chcete zobraziť protokoly volaní, kliknite na **Protokol volaní**.
7. Ak chcete zobraziť protokoly správ, kliknite na **Protokol správ**.

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 **voľbu 8** (práca s výstupom) pre daný profil.

- Ak chcete tlačiť konfiguráciu profilu PPP, vyberte pri tomto profile **voľbu 6** (Tlač). Potom príkazom WRKSPLF sprístupnite vytlačený výstup.

Stav pripojenia:

Stav profilu pripojenia je zobrazený v poli **Stav** pre každý profil v zozname profilov pripojení pod **Sieť → Služby vzdialeného prístupu** po vybratí profilov pôvodcu alebo prijímača. Stav pre jednotlivé pripojenia sa zobrazí pomocou okna Pripojenia.

Tabuľka 10. Opis primárneho stavu

Opis primárneho 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 pripojené viacskokové pripojenie

Tabuľka 11. Opis sekundárneho stavu

Opis sekundárneho 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 dokončené vzájomné dohodnutie PPP
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	Úspešne dokončené dohodovanie PPPoE
Vytvorené volanie L2TP	Správa o vytváraní tunelu L2TP

Odstraňovanie problémov s PPP

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.

Aktuálne a súvisiace informácie o dočasných opravách programov (PTF) a odstraňovaní problémov nájdete na domovskej stránke servera iSeries pre TCP/IP . Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a aktualizujú informácie, uvedené v tejto téme.

1. Požadovaný podporný materiál:
   - Typ vzdialeného hostiteľa, operačný systém a úroveň
   - Úroveň operačného systému hostiteľa servera iSeries
   - Všetky výstupné súbory, ktoré sú uložené vo výstupnom fronte s rovnakým názvom ako profil
   - Protokoly úloh pre QTPPPCTL a QTPPPL2TP (ak sa jedná o profil L2TP)
   - 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

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

Tabuľka 12. Problémy s PPP z dokumentu ITSO Redbook

Problém	Riešenie
Hardvérová konfigurácia modemu Nesprávna konfigurácia prepínačov a iných hardvérových nastavení	Skontrolujte, či je modem nakonfigurovaný pre správny typ rámcovania. Môže byť buď *asynchrónny* alebo *synchrónny*. Viac informácií nájdete v príručke k modemu.
Modemové príkazy AT Modem, ktorý sa pokúšate použiť, nie je v preddefinovanom zozname modemov v Navigátore iSeries.	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.

Súvisiace koncepty

“Konfigurácia vášho modemu pre PPP” na strane 54
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). Opisy modemov pre bežne používané modemy boli definované pre server iSeries.

“Konfigurácia nového modemu” na strane 54
Dozviete sa tu, ako nakonfigurovať nový modem.

Súvisiaci odkaz

“Súvisiace informácie pre PPP”
V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Súvisiace informácie pre PPP

V tejto téme sú uvedené dokumenty IBM Redbooks (vo formáte PDF) a webové lokality, ktoré sa týkajú témy PPP. Každý z týchto súborov PDF môžete zobraziť alebo vytlačiť.

IBM Redbooks

- TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)
- iSeries IP Networks: Dynamic! (SG24-6718)

Webové lokality

Nájdite najnovšie dočasné opravy programov (PTF) a najnovšie informácie o konfigurovaní PPP a L2TP cez linku PPP na domovskej stránke TCP/IP pre server iSeries™. Tento odkaz vám poskytne najnovšie informácie, ktoré dopĺňajú a aktualizujú informácie, uvedené v tejto kolekcii tém.

Ukladanie súborov PDF

Ak chcete uložiť PDF vo vašej pracovnej stanici za účelom prezerania alebo tlače:

1. Kliknite pravým tlačidlom na PDF vo vašom prehliadači (kliknite pravým tlačidlom na vyššie uvedený odkaz).
2. Kliknite na možnosť, ktorá uloží súbor PDF lokálne.
3. Prejdite do adresára, kde chcete uložiť súbor PDF.
4. Kliknite na tlačidlo **Uložiť**.

Prevzatie programu Adobe Reader

Na zobrazenie alebo tlač týchto súborov PDF musíte mať vo vašom systéme nainštalovaný program Adobe Reader. Jeho kópiu môžete zdarma prevziať z webovej lokality spoločnosti Adobe (www.adobe.com/products/acrobat/readstep.html) .

Príloha. Poznámky

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

IBM nemusí ponúkať produkty, služby alebo vlastnosti opisované v tomto dokumente v iných krajinách. Ak chcete získať informácie o produktoch a službách, ktoré sú aktuálne dostupné vo vašej oblasti, kontaktujte lokálneho zástupcu spoločnosti IBM. Akékoľvek odkazy na produkt, program alebo službu IBM nemajú byť chápané ako výslovná či mlčky predpokladaná povinnosť použiť jedine tento produkt, program alebo službu. Môžete použiť ľubovoľný funkčne ekvivalentný produkt, program alebo službu, ktoré neporušujú práva duševného vlastníctva IBM. Za zhodnotenie a overenie činnosti akéhokoľvek produktu, programu alebo služby, ktoré nie sú od spoločnosti IBM, je však zodpovedný užívateľ.

IBM môže vlastniť patenty alebo mať podané žiadosti o patenty, týkajúce sa predmetnej veci popísanej 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.

Otázky, týkajúce sa dvojbajtových informácií (DBCS), predložte Oddeleniu IBM pre intelektuálne vlastníctvo vo vašej krajine alebo ich písomne zašlite 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. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných v tejto publikácii.

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 lokalitách nie sú súčasťou materiálov pre tento produkt IBM a použitie týchto webových lokalít je na vlastné riziko.

IBM môže použiť alebo distribuovať všetky vami poskytnuté informácie ľubovoľným spôsobom bez toho, aby voči vám vznikli akékoľvek záväzky.

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 YBWA
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 všetky licenčné materiály, ktoré sú preň dostupné, poskytuje IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, alebo inej ekvivalentnej zmluvy medzi nami.

Všetky údaje o výkone, uvádzané v tomto dokumente boli získané v riadenom prostredí. Výsledky získané v iných prevádzkových prostrediach sa môžu podstatne odlišovať. Niektoré merania boli vykonané v systémoch vývojovej úrovne a nie je žiadna záruka, že tieto merania budú rovnaké vo všeobecne dostupných systémoch. Okrem toho, niektoré výsledky boli odhadnuté extrapoláciou. Skutočné výsledky sa môžu odlišovať. Užívatelia tohto dokumentu by si mali overiť použiteľnosť týchto údajov pre svoje špecifické prostredie.

Informácie o produktoch iných dodávateľov ako IBM boli získané od dodávateľov týchto produktov z ich uverejnených oznámení alebo z iných, verejne prístupných zdrojov. IBM netestovala tieto produkty a nemôže potvrdiť presnosť ich výkonu, kompatibilitu alebo akékoľvek iné tvrdenie, týkajúce sa produktov, ktoré nepochádzajú od IBM. Otázky o schopnostiach produktov nepochádzajúcich od IBM adresujte dodávateľom týchto produktov.

Tieto informácie obsahujú príklady dát a výpisov používaných v bežných podnikových operáciách. Kvôli ich čo najlepšej ilustrácii obsahujú tieto príklady mená osôb, názvy spoločností, pobočiek a produktov. Všetky tieto mená sú fiktívne a každá podobnosť s menami a adresami, ktoré používajú skutočné podniky, je celkom náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom kóde, ktoré ilustrujú programovacie techniky v rôznych platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez poplatku pre IBM, za účelom vývoja, používania, predaja alebo distribúcie aplikačných programov, vyhovujúcich aplikačnému programovému rozhraniu pre operačnú platformu, pre ktorú sú tieto programy napísané. Tieto príklady neboli dôkladne testované vo všetkých podmienkach. Z tohto dôvodu spoločnosť IBM nemôže zaručiť alebo predpokladať spoľahlivosť, prevádzkyschopnosť alebo funkciu týchto programov.

Každá kópia alebo časť týchto vzorových programov alebo odvodená práca musí obsahovať túto poznámku o autorských právach:

© (názov vašej spoločnosti) (rok). Časti tohto kódu sú odvodené od vzorových programov spoločnosti IBM. © Copyright IBM Corp. _zadajte rok, alebo roky_. Všetky práva vyhradené.

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

Informácie o programovom rozhraní

Dokumenty tejto publikácie, Služby vzdialeného prístupu: Pripojenia PPP, používali programové rozhrania, ktoré dovoľujú zákazníkovi písať programy na získanie služieb systémov IBM i5/OS.

Ochranné známky

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

AIX
i5/OS
IBM
iSeries

| Lotus
| OS/400
| Redbooks

Linux je ochranná známka Linusa Torvaldsa v USA alebo iných krajinách.

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

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

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

Pojmy a podmienky

Oprávnenia na používanie týchto publikácií sú predmetom nasledujúcich pojmov a podmienok.

Osobné použitie: Tieto publikácie môžete reprodukovať pre svoje osobné, nekomerčné použitie za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia autora ich nemôžete distribuovať, zobrazovať ani odvádzať práce z týchto publikácií ani žiadnej ich časti.

Komerčné použitie: Tieto publikácie môžete reprodukovať, distribuovať a zobrazovať výlučne vo vašej spoločnosti za podmienky zachovania všetkých informácií o autorských právach. Bez výslovného povolenia od autora nemôžete odvádzať práce z týchto publikácií ani reprodukovať, distribuovať a zobrazovať tieto publikácie ani žiadne ich časti.

S výnimkou ako je uvedené v týchto podmienkach, na publikácie ľubovoľné informácie, údaje, softvér alebo iné tu obsiahnuté intelektuálne vlastníctvo nemáte žiadne oprávnenia, licencie ani práva, vyjadrené ani implikované.

Spoločnosť IBM si vyhradzuje právo odobrať tu uvedené oprávnenia vždy, podľa vlastného uváženia, keď použitie týchto publikácií škodí autorovi, alebo ak spoločnosť IBM, že pokyny hore nie sú striktne dodržiavané.

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 NERUČÍ ZA OBSAH TÝCHTO PUBLIKÁCIÍ. PUBLIKÁCIE SÚ POSKYTNUTÉ ″TAK AKO SÚ″ BEZ ZÁRUKY AKÉHOKOĽVEK DRUHU, VYJADRENEJ ALEBO IMPLIKOVANEJ, VRÁTANE (ALE NEOBMEDZENE) IMPLIKOVANÝCH ZÁRUK PREDAJNOSTI, NEPOŠKODENIA A VHODNOSTI NA KONKRÉTNY ÚČEL.

Vytlačené v USA