System i

Siete
Služby vzdialeného prístupu: Pripojenia PPP

Verzia 6, vydanie 1

System i

Siete
Služby vzdialeného prístupu: Pripojenia PPP

Verzia 6, vydanie 1

Poznámka

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

Toto vydanie sa vzťahuje na verziu 6, vydanie 1, modifikáciu 0 produktu IBM i5/OS (číslo produktu 5761–SS1) a na všetky následné vydania a modifikácie, pokiaľ nebude v nových vydaniach uvedené inak. Táto verzia nebeží na všetkých modeloch počítačov RISC (reduced instruction set computer) a tiež nebeží na modeloch CISC.

Obsah

Služby vzdialeného prístupu: Pripojenia PPP

PPP (Point-to-Point Protocol) je internetový štandard pre prenos údajov cez sériové linky.

Medzi ISP (Internet Service Provider) je PPP najrozšírenejší protokol používaný pre pripojenia. PPP dovoľuje samostatným počítačom pristupovať do sietí. Siete zas poskytujú prístup do Internetu. Produkt System i obsahuje podporu TCP/IP PPP, ktorá je súčasťou WAN (Wide-Area Network) pripojiteľnosti.

Údaje medzi miestami si môžete vymieňať pomocou PPP pre pripojenie vzdialeného počítača k vašej platforme System i. Prostredníctvom PPP dokážu vzdialené systémy, pripojené k vášmu systému, pristupovať na prostriedky alebo iné počítače, patriace do rovnakej siete ako váš systém. Svoj systém môžete tiež nakonfigurovať, aby sa pripájal k Internetu pomocou PPP. Sprievodca System i Navigator Dial-Up Connection vás povedie procesom pripájania vášho systému k Internetu alebo k internej sieti.

Súbor PDF pre RAS (Remote Access Services)

Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

Ak si chcete zobraziť alebo stiahnuť PDF verziu tohto dokumentu, vyberte Remote Access Services: PPP connections (asi 940 KB).

Ukladanie súborov PDF

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

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

Získanie programu Adobe Reader

Aby ste si mohli tieto PDF súbory prezerať alebo tlačiť, musíte mať v systéme nainštalovaný Adobe Reader. Kópiu programu si môžete bezplatne stiahnuť z webovej stránky Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Súvisiaci odkaz

“Súvisiace informácie pre Remote Access Services” na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Koncepty PPP

PPP môžete použiť na pripojenie platformy System i k vzdialeným sieťam, klientskym PC, k ďalšej platforme System i alebo k ISP (Internet Service Provider). Aby ste mohli tento protokol naplno využívať, mali by ste porozumieť aj schopnostiam aj podpore i5/OS pre tento protokol.

Súvisiaci odkaz

“Súvisiace informácie pre Remote Access Services” na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Čo je PPP

PPP (Point-to-Point Protocol) je TCP/IP protokol, ktorý sa používa na pripojenie jedného počítačového systému k druhému. Počítače používajú PPP 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 umožňuje vzájomnú prevádzkyschopnosť medzi softvérom pre vzdialený prístup od rôznych výrobcov. Umožňuje tiež používanie tej istej fyzickej komunikačnej linky pre viac sieťových komunikačných protokolov.

PPP protokol popisujú nasledujúce štandardy RFC (Request for Comment). Bližšie informácie o RFC nájdete na webovej stránke RFC Editor  .

- RFC-1661 Point-to-Point Protocol
- RFC-1662 PPP on HDLC-like framing
- RFC-1994 PPP CHAP

Profily pripojení

Profily dvojbodových pripojení definujú sadu parametrov a prostriedkov pre špecifické PPP (Point-to-Point Protocol) pripojenia. Môžete spustiť profily, ktoré používajú tieto nastavenia parametrov na vytváranie odchádzajúcich volaní (odosielanie) alebo na načúvanie (prijímanie) PPP pripojení.

Nasledujúce dva typy profilov môžete použiť na definovanie sady charakteristík pre PPP pripojenie alebo sadu pripojení:

- *Profily pripojení odosielateľa* sú dvojbodové pripojenia, ktoré vznikajú v lokálnom systéme a prijíma ich vzdialený systém. Pomocou tohto objektu môžete konfigurovať odchádzajúce pripojenia.
- *Profily pripojení prijímateľa* sú dvojbodové pripojenia, ktoré vznikajú vo vzdialenom systéme a prijíma ich lokálny systém. Pomocou tohto objektu môžete konfigurovať prichádzajúce pripojenia.

Profil pripojenia zadáva ako bude PPP pripojenie fungovať. Informácie obsiahnuté v profile pripojenia odpovedajú na tieto otázky:

- Aký typ protokolu pripojení používate? (PPP alebo SLIP (Serial Line Internet Protocol))
- Kontaktuje váš systém iný počítač vytváraním odchádzajúceho volania (odosielateľ)? Čaká váš systém na prijatie volania z iného systému (prijímateľ)?
- Akú komunikačnú linku pripojenie používa?
- Ako by mal váš systém zistiť, ktorú IP adresu má použiť?
- Ako by mal váš systém autentifikovať iný systém? Kde by mal váš systém 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

Systém ukladá tieto konfiguračné informácie do profilu pripojenia. Tieto informácie poskytujú vášmu systému potrebný kontext pre vytvorenie PPP pripojenia s iným systémom. Profil pripojenia obsahuje tieto informácie:

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

  Typ pripojenia. Zadáva typ linky, na ktorej vaše pripojenia spočívajú a to či sú odchádzajúce (odosielateľ) alebo prichádzajúce (prijímateľ). Môžete si vybrať z týchto typov pripojenia:
  - Komutovaná linka
  - Prenajatá (vyhradená) linka
  - L2TP (Layer Two Tunneling Protocol) (virtuálna linka)
  - PPPoE (Point-to-Point Protocol over Ethernet) (virtuálna linka)

  PPPoE sa podporuje len pre profily pripojení odosielateľa.
- **Prevádzkový režim**. Možný prevádzkový režim závisí na type pripojenia.

Tabuľka 1. Dostupné prevádzkové režimy pre profily pripojenia odosielateľa

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

Tabuľka 2. Dostupné prevádzkové režimy pre profily pripojenia prijímateľa

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

  Pri všetkých ostatných typoch pripojenia (Leased, L2TP, PPPoE) bude výberom linkovej služby len jedna linka.

  Súvisiaci odkaz

  “Softvérové a hardvérové požiadavky” na strane 31
  PPP (Point-to-Point Protocol) prostredie vyžaduje, aby ste mali dva alebo viaceré počítače, ktoré podporujú PPP. Jeden z týchto počítačov, platforma System i, môže byť buď odosielateľom alebo prijímateľom.

Podpora skupinových politík

Pomocou podpory skupinových politík dokážu správcovia siete definovať skupinové politiky na báze užívateľa pre riadenie prostriedkov. Samostatným užívateľom je možné priradiť politiky riadenia prístupov, keď sa prihlásia do relácie PPP (Point-to-Point Protocol) alebo L2TP (Layer Two Tunneling Protocol).

Užívatelia sa dajú identifikovať podľa toho, do ktorej špecifickej triedy užívateľov patria. Každá trieda má svoju jedinečnú politiku, ktorá definuje limity prostriedkov (ako napríklad povolený počet liniek vo viaclinkovom zväzku), atribúty (ako napríklad IP forwarding) a identifikáciu sady pravidiel filtrovania IP paketov, ktorá sa má použiť. Napríklad pomocou podpory skupinovej politiky dokážu správcovia siete definovať skupinu Work_at_Home, ktorá umožňuje úplný prístup do siete alebo skupinu Vendor_Workers, ktorá je obmedzená na sadu služieb.

Súvisiaci odkaz

"Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE" na strane 10
Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

"Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP" na strane 23
Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

Scenár: Vzdialený prístup s použitím PPP pripojení

Tieto scenáre popisujú ako funguje PPP (Point-to-Point Protocol) a ako máte implementovať prostredie PPP v sieti. Scenáre tiež uvádzajú základné PPP koncepty, z ktorých budú profitovať aj začiatočníci aj skúsení užívatelia, skôr ako budete pokračovať v úlohách plánovania a konfigurácie.

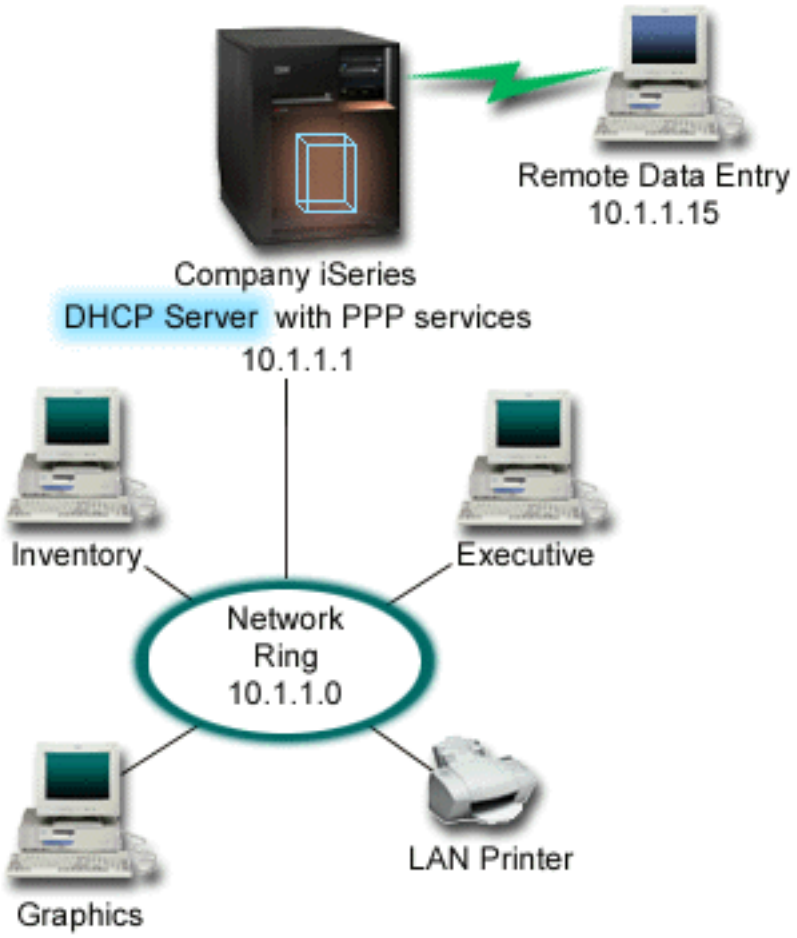
Súvisiaci odkaz

"Súvisiace informácie pre Remote Access Services" na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Príklad: PPP a DHCP na jednom System i

Tento príklad vysvetľuje ako máte nastaviť model System i ako server DHCP (Dynamic Host Configuration Protocol) pre sieť LAN a vzdialeného telefonicky pripojeného klienta.

Vzdialení klienti, napríklad klienti s telefonickým pripojením, často vyžadujú prístup do firemnej siete. Telefonicky pripojení klienti môžu získať prístup na model System i pomocou PPP (Point-to-Point Protocol) . Ak chcete pristúpiť do siete, telefonicky pripojený klient potrebuje IP informácie ako každý priamo pripojený sieťový klient. Server System i DHCP dokáže distribuovať informácie o IP adresách do PPP telefonicky pripojeného klienta ako každý iný priamo pripojený klient. Na nasledujúcom obrázku vidíte vzdialeného klienta, ktorý musí zavolať do podnikovej siete, aby mohol vykonať určitú prácu.



Obrázok 1. PPP a DHCP na jednom modeli System i

Aby sa vzdialení zamestnanci úspešne stali súčasťou podnikovej siete, model System i musí používať kombináciu RAS (Remote Access Services) a DHCP. Funkcia Remote Access Services vytvára schopnosť telefonického pripájania pre model System i. Ak je klient správne nastavený a vytvorí pripojenie prichádzajúcich volaní, PPP server oznámi serveru DHCP, aby distribuoval informácie o TCP/IP vzdialenému klientovi.

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 profilu pripojení prijímateľa nastavte metódu priradenia IP adries z Fixed na DHCP. Ak chcete umožniť telefonicky pripojeným klientom komunikovať s inými sieťovými klientmi, ako napríklad sieťová tlačiareň, musíte v TCP IP nastaveniach profilu povoliť aj IP forwarding a TCP/IP konfiguračné (zásobník) vlastnosti. Ak IP forwarding zapnete len v PPP profile, model System i nebude odovzdávať IP pakety. IP forwarding musíte nastaviť aj v profile aj v zásobníku.

Aj IP adresa lokálneho rozhrania v PPP profile musí byť IP adresou, ktorá spadá do definície podsiete v serveri DHCP. V tomto príklade musí byť IP adresa lokálneho rozhrania PPP profilu 10.1.1.1. Táto adresa musí byť tiež 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 systém aktualizácie DNS?		Nie
Podporuje systém 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 neprideľuje		10.1.1.1 (Adresa lokálneho rozhrania, zadaná v nastaveniach TCP/IP vlastností Receiver Connection Profile v System i Navigator)

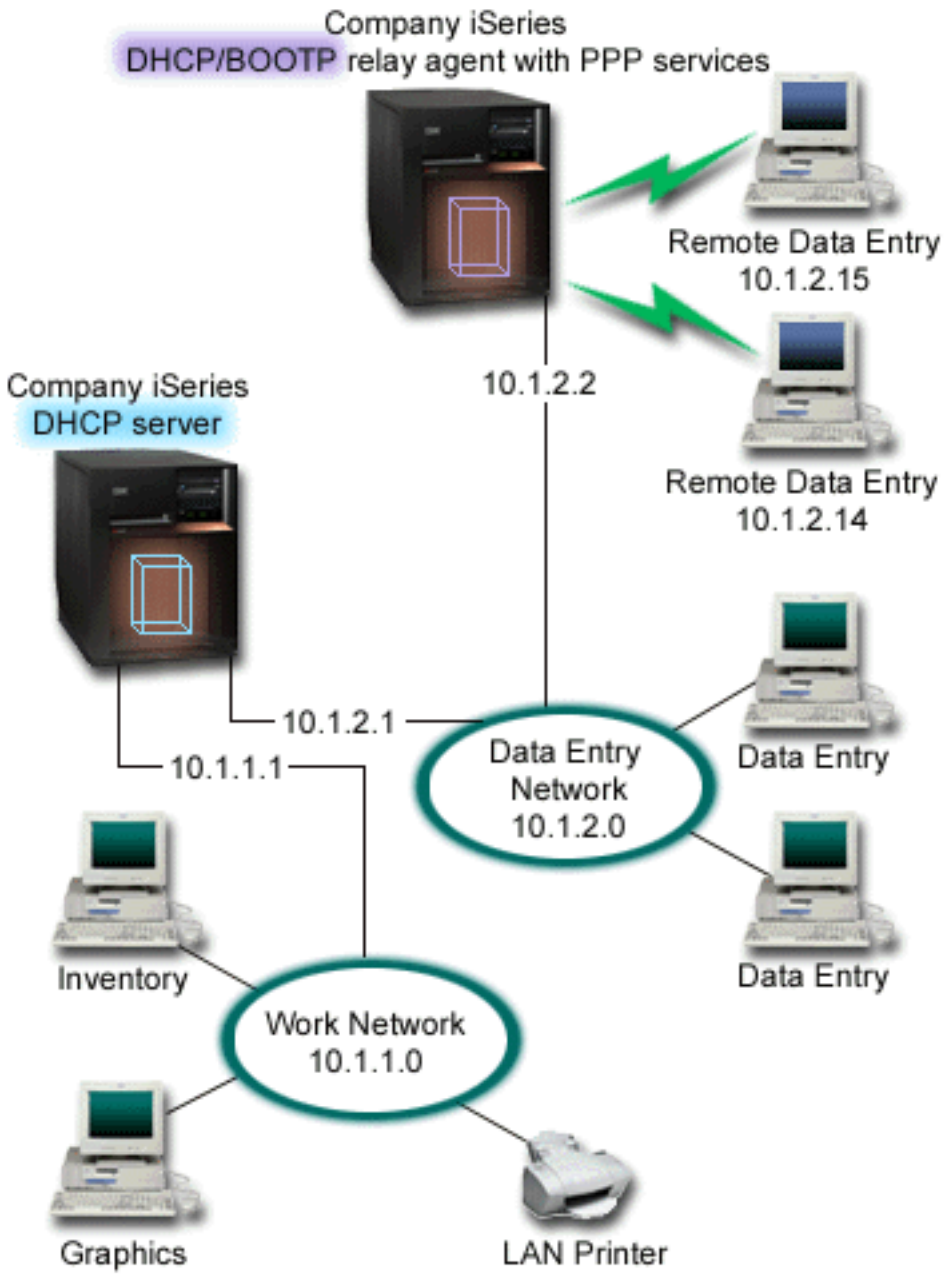
Iné nastavenie

- V profile pripojenia prijímača PPP nastavte metódu vzdialenej adresy IP na DHCP.
  1. Povoľte DHCP WAN klientske pripojenie so serverom DHCP alebo prenosové pripojenie pomocou položky ponuky **Services** pre Remote Access Services v System i Navigator.
  2. Pod TCP/IP Settings Properties profilu Receiver Connection Profile v System i Navigator vyberte pre metódu priraďovania IP adries používanie DHCP.
- Umožnite vzdialenému systému pristupovať na iné siete (IP forwarding) pod TCP/IP Settings Properties profilu Receiver Connection Profile v System i Navigator.
- Povoľte posielanie IP datagramov ďalej pod Settings Properties konfigurácie TCP/IP v System i Navigator.

Príklad: Profil DHCP a PPP na rôznych modeloch System i

Tento príklad vysvetľuje ako máte dva modely System i nastaviť ako sieťový server DHCP (Dynamic Host Configuration Protocol) a prenosového agenta BOOTP/DHCP pre dve siete LAN a vzdialených telefonicky pripojených klientov.

Príklad o PPP a DHCP na jednom modeli System i ukazuje ako máte používať PPP a DHCP na jednom systéme, aby ste povolili telefonicky pripojeným klientom prístup do siete. Ak je pre vás dôležitá fyzická štruktúra siete alebo bezpečnosť, bolo by lepšie servery PPP a DHCP oddeliť alebo mať vyhradený PPP server bez služieb DHCP. Na nasledujúcom obrázku vidíte sieť s telefonicky pripojenými klientmi ktorá má politiky PPP a DHCP na rôznych serveroch.



Obrázok 2. Profil DHCP a PPP na rôznych modeloch System i

Vzdialení klienti údajových položiek volajú do System i PPP servera. Profil PPP v tomto serveri musí mať metódu vzdialených IP adries DHCP, ako napríklad tá, ktorá bola použitá príklade PPP a DHCP na jednom modeli System i. Profil PPP a vlastnosti zásobníka TCP/IP v PPP serveri musia mať IP forwarding. Okrem toho, že tento server vystupuje ako prenosový agent DHCP, prenosový agent BOOTP/DHCP musí byť zapnutý. To umožňuje serveru System i Remote Access odovzdávať pakety DHCPDISCOVER do servera DHCP. Server DHCP potom odpovie a distribuuje informácie TCP/IP do telefonicky pripojených klientov prostredníctvom servera PPP.

Server DHCP zodpovedá za distribuovanie adries IP do sietí 10.1.1.0 a 10.1.2.0. V sieti pre zadávanie údajov server DHCP oznamuje IP adresy z rozsahu 10.1.2.10 do 10.1.2.40 buď pre telefonicky sa pripájajúcich alebo pre priamo pripojených sieťových klientov. Klienti údajových položiek potrebujú aj adresu smerovača (voľba 3) 10.1.2.1 na komunikáciu s pracovnou sieťou a server System i DHCP musí mať tiež povolené IP forwarding.

Aj IP adresa lokálneho rozhrania v PPP profile musí byť IP adresou, ktorá spadá do definície podsiete v serveri DHCP. V tomto príklade musí mať adresa lokálneho rozhrania profilu PPP hodnotu 10.1.2.2. Táto adresa musí byť tiež vylúčená z oblasti adries servera DHCP, aby nebola priradená klientovi DHCP.IP adresa lokálneho rozhrania musí byť adresou, na ktorú môže server DHCP odosielať pakety odpovedí.

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 systém aktualizácie DNS?		Nie
Podporuje systém 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 neprirađuje		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 neprirađuje		10.1.2.1 (smerovač) 10.1.2.15 (IP adresa lokálneho rozhrania klienta Remote Data Entry) 10.1.2.14 (IP adresa lokálneho rozhrania klienta Remote Data Entry)

Iné nastavenie na platforme System i, na ktorej je spustený 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 DHCP WAN klientske pripojenie so serverom DHCP alebo prenosové pripojenie pomocou položky ponuky Services pre Remote Access Services v System i Navigator
  2. Pod TCP/IP Settings Properties profilu Receiver Connection Profile v System i Navigator vyberte pre metódu priraďovania IP adries používanie DHCP

- Umožnite vzdialenému systému pristupovať na iné siete (IP forwarding) pod TCP/IP Settings Properties profilu Receiver Connection Profile v System i Navigator (aby mohli vzdialení klienti komunikovať so sieťou pre zadávanie údajov)
- Povoľte posielanie IP datagramov ďalej pod Settings Properties konfigurácie TCP/IP v System i Navigator (aby mohli vzdialení klienti komunikovať so sieťou pre zadávanie údajov)

Scenár: Ochrana nevynúteného tunela L2TP pomocou IPSec

V tomto scenári sa oboznámite so spôsobom nastavenia pripojenia medzi kancelárskym hostiteľom pobočky a centrály, ktoré používa L2TP chránené pomocou IPSec. Pobočka má dynamicky priradenú adresu IP, zatiaľ čo centrála spoločnosti má statickú, globálne smerovateľnú adresu IP.

Situácia

Predpokladajme, že vaša spoločnosť má malú pobočku v inom štáte. V ktorýkoľvek pracovný deň môže pobočka vyžadovať prístup k dôverným informáciám o modeli System i v rámci vášho podnikového intranetu. Vaša spoločnosť v súčasnosti používa na zabezpečenie prístupu pobočky do podnikovej siete drahú prenajatú linku. Hoci vaša spoločnosť chce aj naďalej poskytovať bezpečný prístup k svojmu intranetu, nakoniec chcete znížiť náklady vynakladané na prenajatú linku. To môžete uskutočniť tak, že vytvoríte dobrovoľný tunel Tunelový protokol vrstvy 2 (L2TP), ktorý rozšíri vašu podnikovú sieť, takže vaša pobočka sa bude vystupovať ako súčasť vašej podnikovej podsiete. VPN ochraňuje prenos údajov cez tunel L2TP.

S dobrovoľným tunelom L2TP vytvorí vzdialená pobočka tunel priamo na sieťový server L2TP (L2TP network server, LNS) podnikovej siete. Funkčnosť koncentrátora prístupu L2TP (access concentrator L2TP, LAC) spočíva na klientovi. Tunel je pre Poskytovateľa internetových služieb (ISP) klienta transparentný, takže na podporu L2TP sa nevyžaduje ISP. Ak chcete získať viac informácií o konceptoch L2TP, pozrite si protokol L2TP (Layer 2 Tunnel Protocol).

Dôležité: Tento scenár zobrazuje bezpečnostné brány, ktoré sú priamo pripojené k Internetu. Nie je tu firewall kvôli zjednodušeniu návrhu. Neznamená to, že použitie firewallu nie je nevyhnutné. Zvážte bezpečnostné riziká, ktorým sa vystavujete pri každom pripojení na internet.

Ciele

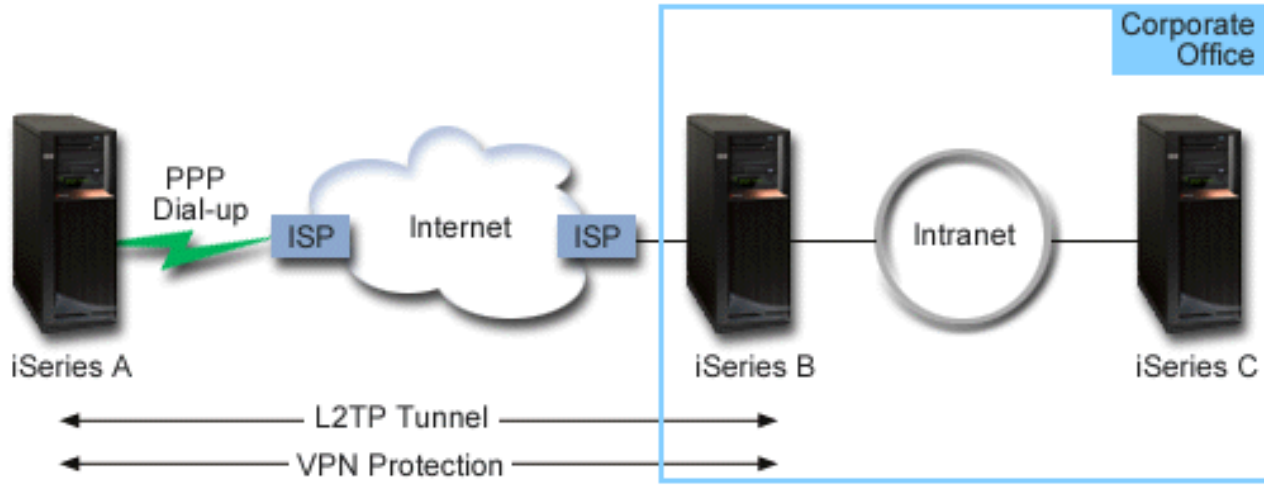
V tomto scenári sa kancelársky systém pobočky pripojí k svojej firemnej sieti cez systém brány pomocou tunela L2TP chráneného pomocou VPN.

Hlavnými cieľmi tohto návrhu sú:

- Systém pobočky vždy zahajuje pripojenie na podnikovú ústredňu.
- Systém pobočky je jediným systémom v sieti pobočky, ktorý potrebuje prístup na podnikovú sieť. Inými slovami, jeho rola v sieti pobočky je hostiteľ, nie brána.
- Podnikový systém hostiteľský počítač v sieti pobočky.

Podrobnosti

Nasledujúci obrázok ilustruje charakteristiky siete pre tento návrh.



Systém A

- Musí mať prístup k aplikáciám TCP/IP vo všetkých systémoch vo firemnej sieti.
- Prijíma dynamicky priradené adresy IP od svojho ISP.
- Musí byť nakonfigurovaný na poskytovanie podpory L2TP.

Systém B

- Musí mať prístup k TCP/IP aplikáciám na System A.
- Podsieť je 10.6.0.0 s maskou 255.255.0.0. Táto podsieť reprezentuje koncový bod údajov tunela VPN na podnikovej lokalite.
- Pripája sa na Internet s adresou IP 205.13.237.6. Toto je koncový bod pripojenia. To znamená, že System B vykoná riadenie kľúčov a použije IPSec na prichádzajúce a odchádzajúce IP datagramy. System B sa pripojí k jeho podsieti s IP adresou 10.6.11.1.

Vyjadrené terminológiou L2TP, *System A* vystupuje ako inicializátor L2TP, zatiaľ čo *System B* vystupuje ako terminátor L2TP.

Úlohy konfigurovania

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

Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE

Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

Situácia

Váš podnik si vyžaduje rýchlejšie internetové pripojenie, preto sa zaujímate o službu DSL (Digital Subscriber Line) u lokálneho ISP. Po úvodnom prieskume zistíte, že váš ISP používa na pripájanie svojich klientov PPPoE. Toto PPPoE pripojenie musíte použiť, ak chcete poskytovať širokopásmové internetové pripojenia v celom vašom systéme.

Obrázok 3. Pripájanie vášho systému k ISP pomocou PPPoE

Riešenie

Môžete podporovať PPPoE pripojenie k vášmu ISP prostredníctvom vášho systému. Systém používa nový typ PPPoE virtuálnej linky, ktorá je naviazaná na fyzickú ethernetovú linku, nakonfigurovanú aby používala typ 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A alebo ethernetový adaptér 576A. Táto virtuálna linka podporuje protokoly PPP relácie cez ethernetovú lokálnu sieť, ktorá je pripojená k DSL modemu, ktorý zabezpečuje bránu do vzdialeného ISP. Táto brána umožňuje užívateľom, pripojeným k lokálnej sieti, získať vysokorýchlostný prístup na Internet pomocou PPPoE pripojenia. Po spustení pripojenia medzi systémom a ISP môžu jednotliví užívatelia v sieti LAN pristupovať na ISP cez PPPoE s použitím IP adresy, alokovanej systému. Pre poskytnutie vyššej bezpečnosti môžu byť pravidlá filtrovania použité na virtuálnu linku PPPoE, aby obmedzili konkrétnu prichádzajúcu internetovú komunikáciu.

Vzorová konfigurácia

Ak chcete nastaviť vzorovú PPP konfiguráciu z System i Navigator, postupujte nasledovne:

1. Nakonfigurujte pripájacie zariadenie na pripojenie k svojmu ISP.
2. Vo svojom systéme nakonfigurujte profil odosielateľa pripojení.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: PPP over Ethernet
   - **Režim prevádzky**: Iniciátor
   - **Konfigurácia linky**: Jedna linka
3. Na strane General v paneli New Point-to-Point Profile Properties zadajte názov a opis profilu pôvodcu.Tento názov sa týka profilu pripojenia a virtuálnej linky PPPoE.
4. Kliknite na **Connection**, aby sa otvorila strana Connection. Vyberte **PPPoE virtual line name**, ktorý zodpovedá názvu pre tento profil pripojenia. Keď vyberiete linku System i Navigator zobrazí dialóg **Line properties**.

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

b. Kliknite na **Links**, aby sa otvorila strana Link. Z výberového zoznamu Physical Line Name vyberte ethernetovú linku, ktorú bude používať toto pripojenie a kliknite na **Open**. Ak potrebujete nadefinovať novú linku Ethernet, napíšte jej názov a kliknite na **New**. System i Navigator zobrazí dialóg **Ethernet line properties**.

   Poznámka: PPPoE vyžaduje typ 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A alebo ethernetový adaptér 576A.

   1) Na strane General zadajte zmysluplný opis pre ethernetovú linku a skontrolujte, či definícia linky používa vyžadované hardvérové prostriedky.
   2) Kliknite na **Links**, 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 **Other**, 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 **Limits**, ak chcete zadefinovať vlastnosti autentifikácie LCP, alebo kliknite na **OK**, ak sa chcete vrátiť na stranu New Point-to-Point Profile Connection.

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

5. Ak váš ISP vyžaduje, aby systém seba autentifikoval alebo, ak chcete, aby systém autentifikoval vzdialený systém, kliknite na **Authentication**, aby sa otvorila stránka Authentication a zadajte vyžadované informácie.
6. Kliknite na **TCP/IP Settings**, 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 užívateľom, ktorí sú pripojení k sieti LAN, povoliť pripojenie k ISP pomocou IP adries, alokovaných systému, vyberte **Hide addresses (Full masquerading)**.
7. Kliknite na **DNS**, aby sa otvorila strana DNS a zadajte adresu IP servera DNS, ktorú vám oznámi l ISP.
8. Kliknutím na **OK** dokončite profil.

Súvisiace koncepty

“Podpora skupinových politík” na strane 3
Pomocou podpory skupinových politík dokážu správcovia siete definovať skupinové politiky na báze užívateľa pre riadenie prostriedkov. Samostatným užívateľom je možné priradiť politiky riadenia prístupov, keď sa prihlásia do relácie PPP (Point-to-Point Protocol) alebo L2TP (Layer Two Tunneling Protocol).

Súvisiace úlohy

“Vytváranie profilu pripojenia” na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

Súvisiaci odkaz

“Konfigurácia spojenia” na strane 49
Konfigurácia linky definuje typ linkovej služby, ktorú váš profil PPP (Point-to-Point Protocol) pripojenia používa na vytvorenie pripojenia.

“Autentifikácia systému” na strane 42
PPP pripojenia k platforme System i podporujú niekoľko volieb autentifikácie pre vzdialených klientov, volajúcich do systému aj pre pripojenia k ISP alebo inému systému, do ktorého volá systém.

“Spravovanie adries IP” na strane 40
PPP (Point-to-Point Protocol) pripojenia povoľujú niekoľko rôznych sád volieb pre riadenie IP adries v závislosti od typu profilu pripojenia.

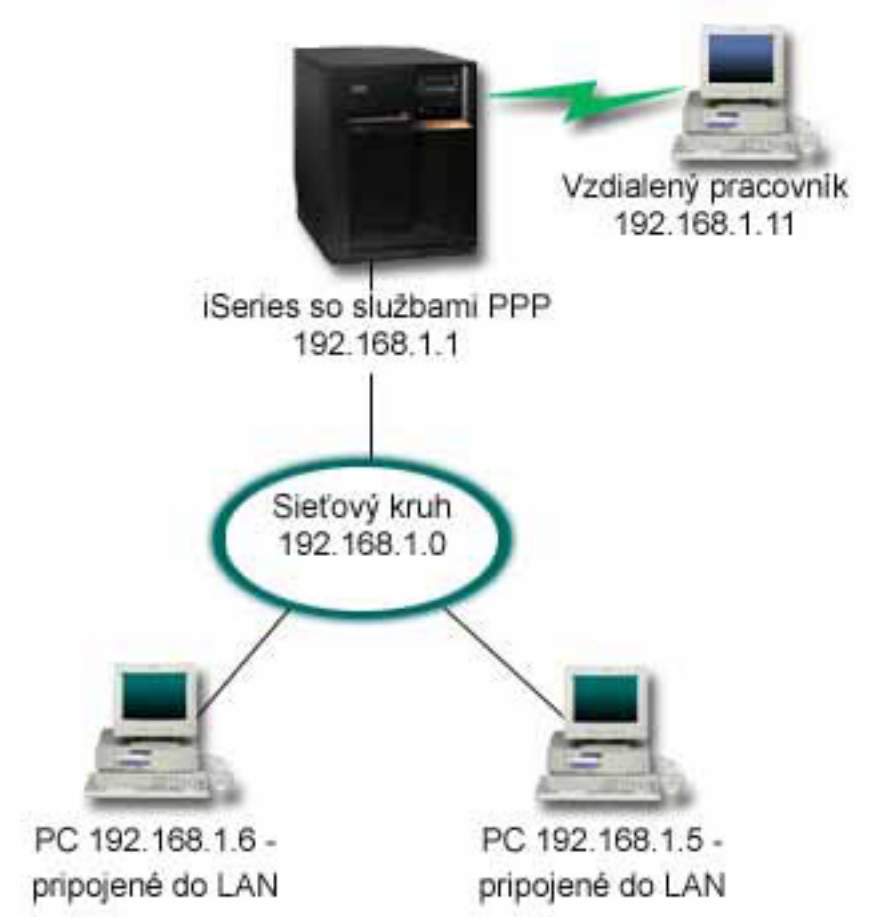
“Filtrovanie paketov IP” na strane 40
Filtrovanie IP paketov obmedzuje služby samostatným užívateľom, keď sa prihlásia do siete.

Scenár: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému

Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

Situácia

Ako správca siete vášho podniku musíte udržiavať aj svoj systém aj sieťových klientov. Namiesto toho, aby ste chodili do práce a riešili problémy, potrebujete možnosť pracovať zo vzdialeného miesta, napríklad z domu. Pretože vaša spoločnosť nemá internetové sieťové pripojenie, môžete do svojho systému volať pomocou pripojenia PPP. Okrem toho, jediný modem, ktorý máte momentálne k dispozícii, je váš modem 7852-400 elektronickej podpory zákazníkov a potrebujete ho použiť pre svoje pripojenie.



Obrázok 4. Pripájanie vzdialených klientov k vášmu systému

Riešenie

PPP môžete používať na pripojenie svojho domáceho PC k vášmu systému pomocou modemu. Pretože pre tento typ PPP pripojenia používate modem elektronickej podpory zákazníkov, musíte sa presvedčiť máte modem nakonfigurovaný aj pre synchrónny aj pre asynchrónny režim. Na obrázku vidíte systém s PPP službami, ktorý je pripojený k sieti LAN s dvomi PC. Vzdialený pracovník potom zavolá do systému. Systém sa autentifikuje a stane sa súčasťou pracovnej siete (192.168.1.0). V tomto prípade je najjednoduchšie priradiť volajúcemu klientovi statickú adresu IP.

Vzdialený pracovník používa na autentifikáciu do systému protokol CHAP-MD5 (Challenge Handshake Authentication Protocol). Systém nemôže používať MS_CHAP, preto sa musíte presvedčiť, či váš PPP klient používa 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.

Na predchádzajúcom obrázku bol len jeden vzdialený klient s telefonickým pripojením, pretože modem elektronickej podpory zákazníkov dokáže naraz spracovať len jedno pripojenie.

Vzorová konfigurácia

Ak chcete nastaviť vzorovú PPP konfiguráciu z System i Navigator, postupujte nasledovne:

1. Nakonfigurujte Dial-up Networking a vytvorte telefonické pripojenie vo vzdialenom PC.
2. Vo svojom systéme nakonfigurujte profil prijímateľa pripojení.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Odpoveď
   - **Konfigurácia linky**: V závislosti od vášho prostredia to môže byť jedna linka alebo oblasť liniek.
3. Na strane General v paneli New Point-to-Point Profile Properties zadajte názov a opis pre profil príjemcu.
4. Kliknite na **Connection**, aby sa otvorila strana Connection. Vyberte príslušný **názov linky** alebo vytvorte nový zadaním nového názvu a kliknite na **New**.
   a. Na strane General zvýraznite existujúci hardvérový prostriedok, ku ktorému je pripojený váš adaptér 7852–400 a nastavte rámcovanie na **Asynchronous**.
   b. Kliknite na **Modem**, aby sa otvorila strana Modem. Vo výberovom zozname Name vyberte **IBM 7852–400**.
   c. Kliknite na **OK**, čím sa vrátite na stranu New Point-to-Point Profile Properties.
5. Kliknite na **Authentication**, aby sa otvorila strana Authentication.
   a. Vyberte **Require this iSeries server to verify the identity of the remote system**.
   b. Vyberte **Authenticate locally using a validation list** a do validizačného zoznamu pridajte nového vzdialeného používateľa.
   c. Vyberte **Allow encrypted password (CHAP-MD5)**.
6. Kliknite na **TCP/IP Settings**, aby sa otvorila strana TCP/IP.
   a. Nastavte lokálnu IP adresu na 192.168.1.1.
   b. Pre vzdialenú IP adresu vyberte **Fixed IP address** a začiatočnú adresu IP 192.168.1.11.
   c. Vyberte **Allow remote system to access other networks**.
7. Kliknutím na **OK** dokončite profil.

Súvisiace koncepty

“Plánovanie PPP” na strane 31
Plánovanie PPP (Point-to-Point Protocol) obsahuje vytváranie a administráciu PPP pripojení.

Súvisiace úlohy

“Vytváranie profilu pripojenia” na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

Súvisiaci odkaz

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

“Konfigurácia spojenia” na strane 49
Konfigurácia linky definuje typ linkovej služby, ktorú váš profil PPP (Point-to-Point Protocol) pripojenia používa na vytvorenie pripojenia.

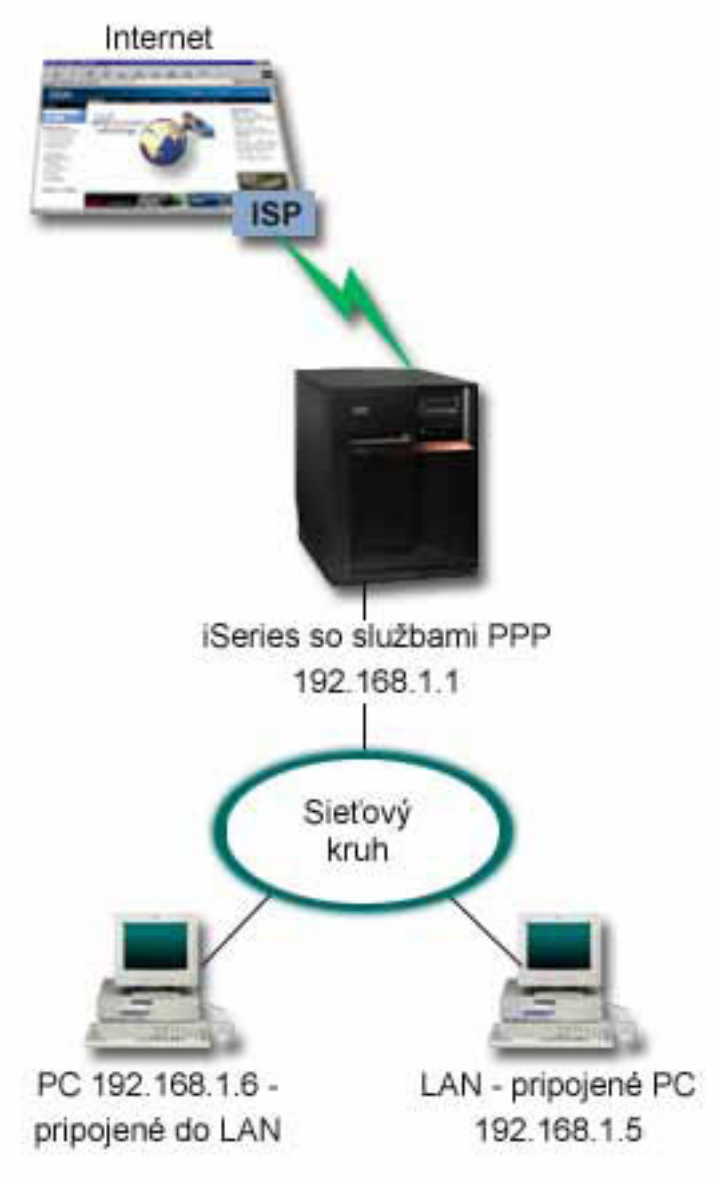
“Oblasť liniek” na strane 50
Ak chcete PPP pripojenie nastaviť, aby používalo linku zo združených liniek, vyberte túto linkovú službu. Keď sa PPP pripojenie spustí, systém zo združených liniek vyberie nepoužívanú linku. Pri profiloch dial on-demand systém nevyberie linku pokiaľ nezistí TCP/IP prevádzku pre vzdialený systém.

Scenár: Pripájanie kancelárskej siete LAN k Internetu pomocou modemu

Administrátori zvyčajne nastavujú kancelárske siete pre zamestnancov, aby mali prístup na Internet. Administrátori môžu použiť modem na pripojenie systému k ISP (Internet Service Provider). PC klienti pripojení k sieti LAN môžu komunikovať cez Internet pomocou operačného systému i5/OS v úlohe brány.

Situácia

Podniková aplikácia, ktorú používa vaša spoločnosť, vyžaduje od vašich užívateľov prístup na Internet. Pretože aplikácia nevyžaduje výmenu veľkých objemov údajov, musíte vedieť používať modem na pripojenie vášho systému a PC klientov, pripojených k sieti LAN, k Internetu. Nasledujúci obrázok popisuje príklad tohto stavu.



Obrázok 5. Pripájanie kancelárskej siete LAN k Internetu pomocou modemu

Riešenie

Svoj integrovaný (alebo iný kompatibilný) modem môžete použiť na pripojenie svojho systému k ISP. V systéme, ktorý má vytvoriť PPP pripojenie k ISP, musíte vytvoriť profil PPP (Point-to-Point Protocol) odosielateľa.

Keď vytvoríte pripojenie medzi systémom a ISP, vaše PC, pripojené k sieti LAN, môžu komunikovať cez Internet pomocou systému v úlohe brány. V profile odosielateľa sa musíte presvedčiť, či je zapnutá voľba Hide addresses, aby LAN klienti, ktorí majú súkromné IP adresy dokázali komunikovať cez Internet.

Teraz, keď je váš systém a sieť pripojená k Internetu, musíte porozumieť bezpečnostným rizikám. Spolupracujte s ISP, aby ste pochopili jeho bezpečnostné politiky a naďalej zvyšujte ochranu svojho systému a siete.

V závislosti od vášho využitia Internetu sa môže stať problémom šírka pásma.

Vzorová konfigurácia

Ak chcete nastaviť vzorovú konfiguráciu z System i Navigator, postupujte nasledovne:

1. Vo svojom systéme nakonfigurujte profil odosielateľa pripojení.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Telefonické pripojenie
   - **Konfigurácia linky**: V závislosti od vášho prostredia to môže byť jedna linka alebo oblasť liniek.
2. Na strane General v paneli New Point-to-Point Profile Properties zadajte názov a opis profilu pôvodcu.
3. Kliknite na **Connection**, aby sa otvorila strana Connection. Vyberte príslušný názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **New**.
   a. Na strane General 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 New Point-to-Point Profile Properties.
4. Kliknite na **Add** a zadajte telefónne číslo pre telefonické pripojenie k serveru ISP. Nezabudnite vložiť prípadnú požadovanú predvoľbu.
5. Kliknite na **Authentication**, aby sa otvorila strana Authentication, vyberte **Allow the remote system to verify the identity of this iSeries server**. Zvoľte autentifikačný protokol a zadajte prípadné požadované meno používateľa alebo heslo.
6. Kliknite na **TCP/IP Settings**, aby sa otvorila strana TCP/IP.
   a. Vyberte **Assigned by remote system** pre lokálne i vzdialené adresy IP.
   b. Vyberte **Add remote system as the default route**.
   c. Začiarknite **Hide addresses**, aby vaše interné adresy IP nepresmerovali na Internet.
7. Kliknite na **DNS**, aby sa otvorila stránka Domain Name System {DNS), a zadajte IP adresu DNS servera, ktorý poskytuje ISP.
8. Kliknutím na **OK** dokončite profil.

Ak chcete na pripojenie k Internetu použiť profil pripojenia, pravým tlačidlom kliknite na profil pripojenia z System i Navigator a vyberte **Start**. Pripojenie je úspešné, keď sa stav zmení na **Active**. Aby ste zaktualizovali obrazovku, použite obnovenie.

Poznámka: Ďalej sa musíte presvedčiť, či ostatné systémy vo vašej sieti majú zadefinované správne smerovanie, aby sa na Internet viazaná TCP/IP prevádzka z týchto systémov odosielala prostredníctvom systému.

Súvisiace koncepty

"Plánovanie PPP" na strane 31
Plánovanie PPP (Point-to-Point Protocol) obsahuje vytváranie a administráciu PPP pripojení.

Súvisiace úlohy

"Vytváranie profilu pripojenia" na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

Súvisiaci odkaz

"Oblasť liniek" na strane 50
Ak chcete PPP pripojenie nastaviť, aby používalo linku zo združených liniek, vyberte túto linkovú službu. Keď sa PPP pripojenie spustí, systém zo združených liniek vyberie nepoužívanú linku. Pri profiloch dial on-demand systém nevyberie linku pokiaľ nezistí TCP/IP prevádzku pre vzdialený systém.

"Konfigurácia spojenia" na strane 49
Konfigurácia linky definuje typ linkovej služby, ktorú váš profil PPP (Point-to-Point Protocol) pripojenia používa na vytvorenie pripojenia.

Scenár: Pripájanie vašich podnikových a vzdialených sietí pomocou modemu

Modem umožňuje dvom vzdialeným umiestneniam (ako napríklad ústredňa a pobočková ústredňa) vymieňať si údaje. PPP (Point-to-Point Protocol) dokáže navzájom prepojiť dve siete LAN tak, že vytvorí pripojenie medzi systémom na ústredni a druhým systémom na pobočkovej ústredni.

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. Pripájanie podnikových a vzdialených sietí pomocou modemu

Riešenie

PPP dokáže navzájom prepojiť dve siete LAN tak, že vytvorí pripojenie medzi systémami ako ho vidíte na obrázku. V takom prípade predpokladajme, že vzdialená kancelária iniciuje pripojenie k ústrednej kancelárii. Profil odosielateľa nakonfigurujte na vzdialenom systéme a profil prijímateľa v systéme ústredne.

Ak PC vzdialenej kancelárie potrebujú prístup k podnikovej sieti LAN (192.168.1.0), profil prijímateľa ústredne bude potrebovať, aby bol IP forwarding zapnutý a smerovanie IP adries by malo byť pre PC (192.168.2, 192.168.3, 192.168.1.6 a 192.168.1.5 v tomto príklade) povolené. 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

Ak chcete nastaviť vzorovú konfiguráciu z System i Navigator, postupujte nasledovne:

1. Vo vzdialenom kancelárskom systéme nakonfigurujte profil pripojení odosielateľa.

   Nezabudnite vybrať tieto informácie:

   - **Typ protokolu**: PPP
   - **Typ pripojenia**: Komutovaná linka
   - **Režim prevádzky**: Telefonické pripojenie
   - **Konfigurácia linky**: V závislosti od vášho prostredia to môže byť jedna linka alebo oblasť liniek.
2. Na strane General v paneli New Point-to-Point Profile Properties zadajte názov a opis profilu pôvodcu.
3. Kliknite na **Connection**, aby sa otvorila strana Connection. Vyberte príslušný názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **New**.
   a. Na strane General vo vlastnostiach novej linky zvýraznite existujúci hardvérový prostriedok a nastavte rámcovanie na **Asynchronous**.
   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 New Point-to-Point Profile Properties.
4. Kliknite na **Add** a zadajte telefónne číslo, na ktorom sa ozve systém ústredne. Nezabudnite vyplniť všetky požadované predvoľby.
5. Kliknite na **Authentication**, aby sa otvorila strana Authentication a vyberte **Allow the remote system to verify the identity of this iSeries server**. Vyberte **Require encrypted password (CHAP-MD5)** a zadajte požadované informácie o mene a hesle užívateľa.
6. Kliknite na **TCP/IP Settings**, aby sa otvorila strana TCP/IP Settings.
   a. Pre lokálnu adresu IP vyberte adresu IP rozhrania LAN vzdialenej pobočky (192.168.2.1) v zozname **Use fixed IP address**.
   b. Pre vzdialenú adresu IP vyberte **Assigned by remote system**.
   c. V časti pre smerovanie vyberte **Add remote system as the default route**.
   d. Kliknutím na **OK** dokončite profil pôvodcu.
7. V systéme ústredne nakonfigurujte profil pripojení prijímateľa.

   Nezabudnite vybrať tieto informácie:

   - **Protocol type**: PPP
   - **Connection type**: Switched-line
   - **Operating mode**: Answer
   - **Link configuration**: V závislosti od vášho prostredia to môže byť jedna linka alebo oblasť liniek.
8. Na strane General v paneli New Point-to-Point Profile Properties zadajte názov a opis pre profil príjemcu.
9. Kliknite na **Connection**, aby sa otvorila strana Connection. Vyberte príslušný názov linky alebo vytvorte nový názov tak, že ho napíšete a kliknete **New**.

a. Na strane General zvýraznite existujúci hardvérový prostriedok a nastavte rámcovanie na **Asynchronous**.
b. Kliknite na **Modem**, aby sa otvorila strana Modem. Zo zoznamu Name vyberte modem, ktorý používate.
c. Kliknite na **OK**, čím sa vrátite na stranu New Point-to-Point Profile Properties.

10. Kliknite na **Authentication**, aby sa otvorila strana Authentication.
    a. Označte **Require this iSeries server to verify the identity of the remote system**.
    b. Pridajte nového vzdialeného používateľa do validizačného zoznamu.
    c. Označte autentifikáciu CHAP-MD5.
11. Kliknite na **TCP/IP Settings**, aby sa otvorila strana TCP/IP Settings.
    a. Pre lokálnu IP adresu vyberte z políčka **select** IP adresu rozhrania ústredne (192.168.1.1).
    b. Pre vzdialenú adresu IP vyberte **Based on remote system's user ID**. Otvorí sa dialógové okno **IP Addresses Defined By User Name**. Kliknite na **Add**. Vyplňte polia pre užívateľské meno volajúceho, IP adresu a masku podsiete. V našom scenári bude vhodné nasledujúce:
       - Užívateľské meno volajúceho: vzdialená_strana
       - IP adresa: 192.168.2.1
       - Maska podsiete: 255.255.255.0

       Kliknite na **OK** a opätovným kliknutím na **OK** sa vrátite na stranu TCP/IP Settings.
    c. Vyberte **IP forwarding**, ak chcete ostatným systémom v sieti povoliť používanie tohto systému ako brány.
12. Kliknutím na **OK** dokončite profil príjemcu.

Súvisiace úlohy

"Vytváranie profilu pripojenia" na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

Súvisiaci odkaz

"Konfigurácia spojenia" na strane 49
Konfigurácia linky definuje typ linkovej služby, ktorú váš profil PPP (Point-to-Point Protocol) pripojenia používa na vytvorenie pripojenia.

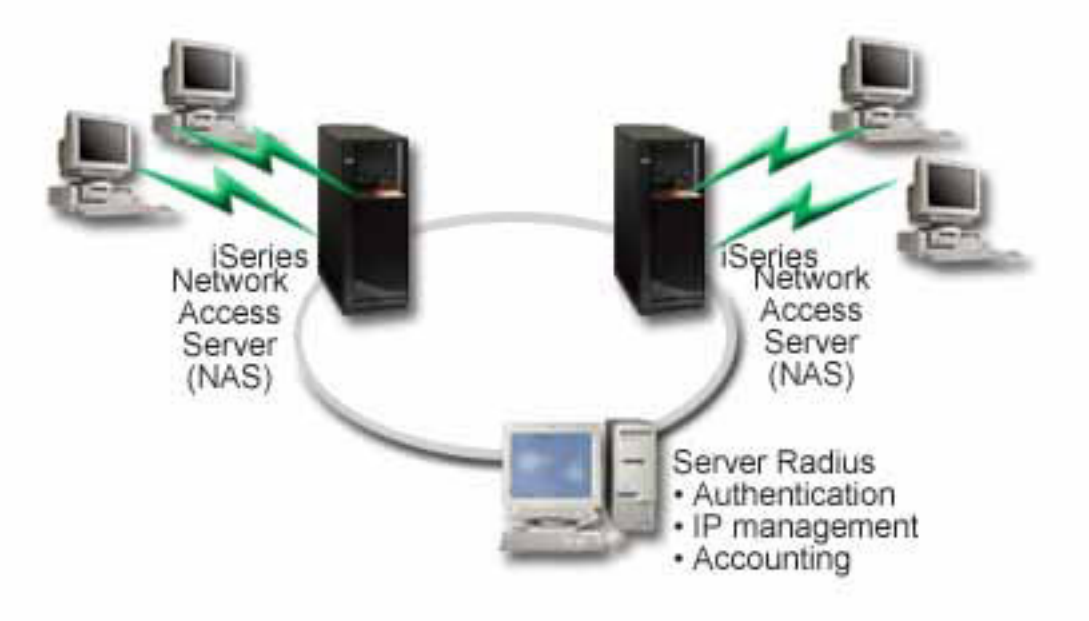
"Oblasť liniek" na strane 50
Ak chcete PPP pripojenie nastaviť, aby používalo linku zo združených liniek, vyberte túto linkovú službu. Keď sa PPP pripojenie spustí, systém zo združených liniek vyberie nepoužívanú linku. Pri profiloch dial on-demand systém nevyberie linku pokiaľ nezistí TCP/IP prevádzku pre vzdialený systém.

Scenár: Autentifikácia telefonických pripojení pomocou RADIUS NAS

V systéme spustený NAS (Network Access Server) dokáže smerovať požiadavky na autentifikáciu z telefonicky pripojených klientov na osobitný server RADIUS (Remote Authentication Dial In User Service). Ak je autentifikovaný, RADIUS dokáže riadiť aj užívateľovi priradené IP adresy.

Situácia

Vaša podniková sieť má vzdialených užívateľov, ktorí zo siete distribuovaných telefonických pripojení volajú do dvoch systémov. Autentifikáciu, servis a evidenciu musíte centralizovať, čím umožníte jednému systému, aby spracoval požiadavky na overenie platnosti ID užívateľov a hesiel a aby stanovil IP adresy, ktoré majú priradené.



Obrázok 7. Autentifikácia telefonických pripojení pomocou servera RADIUS

Riešenie

Keď sa užívatelia pokúšajú o pripojenie, NAS, spustený v systéme, pošle autentifikačné informácie ďalej do servera 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 podporovať RADIUS, musíte server RADIUS NAS zadefinovať v systéme.

Vzorová konfigurácia

Ak chcete nastaviť vzorovú konfiguráciu z System i Navigator, postupujte nasledovne:

1. V System i Navigator rozviňte **Network**, pravým tlačidlom kliknite na **Remote Access Services** a vyberte **Services**.
2. Na záložke **RADIUS** vyberte **Enable RADIUS Network Access Server connection** a **Enable RADIUS for authentication**. V závislosti od vášho riešenia RADIUS si môžete vybrať, aby RADIUS spracovával aj evidenciu pripojení a konfiguráciu TCP/IP adries.
3. Kliknite na tlačidlo **nastavenia RADIUS NAS**.
4. Na strane General zadajte opis pre tento server.
5. Na strane Authentication Server (a voliteľne na strane Accounting Server) kliknite na **Add** a zadajte nasledujúce informácie:
   a. Do políčka **Local IP address** zadajte IP adresu pre rozhranie, ktoré sa používa na pripojenie k serveru RADIUS.
   b. Do políčka **Server IP address** zadajte IP adresu pre server RADIUS.
   c. Do políčka **Password** zadajte heslo, ktoré sa používa na identifikáciu systému pre server RADIUS.
   d. Do políčka **Port** zadajte port v systéme, ktorý sa používa 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 System i Navigator rozviňte **Network → Remote Access Services**.
8. Označte Profil pripojenia, ktorý bude server RADIUS pri autentifikácii využívať. Služby RADIUS sa dajú používať len pre profily pripojení prijímateľa.

9. Vyberte **Require this iSeries server to verify the identity of the remote system**.
10. Označte **Authenticate remotely using a RADIUS server**.
11. Označte autentifikačný protokol (PAP alebo CHAP-MD5) Tento protokol tiež musí používať server RADIUS.
12. Označte **Use RADIUS for connection editing and accounting**.
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 volajú s použitím tohto profilu pripojenia, systém pošle autentifikačné informácie do zadaného servera RADIUS. Ak je platnosť užívateľa overená, pripojenie je povolené a bude používať všetky obmedzenia pripojení, ktoré sú zadané v užívateľových informáciách o serveri RADIUS.

Súvisiace úlohy

"Povolenie služieb RADIUS a DHCP pre profily pripojenia" na strane 59
Prinášame vám postup pre povolenie služieb RADIUS alebo DHCP (Dynamic Host Configuration Protocol) pre profily prijímateľa PPP pripojení.

Súvisiaci odkaz

"Autentifikácia systému" na strane 42
PPP pripojenia k platforme System i podporujú niekoľko volieb autentifikácie pre vzdialených klientov, volajúcich do systému aj pre pripojenia k ISP alebo inému systému, do ktorého volá systém.

"RADIUS (Remote Authentication Dial In User Service) - prehľad" na strane 44
RADIUS (Remote Authentication Dial In User Service) je internetový štandardný protokol, ktorý poskytuje centralizovanú autentifikáciu, evidenciu a služby riadenia IP pre užívateľov vzdialeného prístupu v sieti distribuovaných telefonických pripojení.

Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP

Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

Situácia

Vaša sieť má niekoľko skupín distribuovaných užívateľov a každá z nich potrebuje prístup k iným prostriedkom vo vašej podnikovej sieti LAN. Skupina užívateľov, ktorí zadávajú údaje potrebuje prístup k databáze a niekoľkým iným aplikáciám. Skupina osôb z iných firiem potrebuje prístup cez telefonické pripojenie k službám HTTP, FTP (File Transfer Protocol) a Telnet, ale z bezpečnostných dôvodov nesmie mať táto skupina povolený prístup k iným službám alebo prevádzke TCP/IP. Definovanie podrobných atribútov pripojenia a oprávnení pre každého užívateľa robí vašu snahu duplicitnou a poskytovanie sieťových obmedzení pre všetkých užívateľov tohto profilu pripojenia nezabezpečuje dostatočnú kontrolu. Chcete spôsob definovania nastavení pripojenia a oprávnení pre niekoľko rozdielnych skupín užívateľov, ktorí sa rutinne telefonicky pripájajú k tomuto systému.

Obrázok 8. Používanie nastavení pripojenia pre telefonické pripojenia na základe nastavení skupinových politík

Riešenie

Potrebujete aplikovať jedinečné obmedzenia filtrovania IP na dve rôzne skupiny užívateľov. Ak to chcete docieliť, vytvorte politiky skupinového prístupu a pravidlá IP filtrovania. Politiky skupinového prístupu odkazujú na pravidlá filtrovania IP, preto musíte pravidlá filtrovania vytvoriť ako prvé. V tomto príklade musíte vytvoriť PPP filter, ktorý bude obsahovať pravidlá filtrovania IP pre IBM Business Partner Group Access Policy. Tieto pravidlá filtrovania povoľujú služby HTTP, FTP a Telnet, ale obmedzujú prístup ku všetkej ostatnej prevádzke a službám TCP/IP v celom systéme. V tomto scenári uvidíte len pravidlá filtrovania potrebné pre skupinu obchodníkov; podobné filtre však môžete vytvoriť aj pre skupinu Data Entry.

Nakoniec musíte na definovanie svojej skupiny vytvoriť skupinové politiky prístupu (jednu pre každú skupinu). Politika skupinového prístupu vám povoľuje definovať spoločné atribúty pripojení pre skupinu užívateľov. Pridaním politiky skupinového prístupu na zoznam overovania platnosti v systéme môžete tieto nastavenia pripojenia použiť počas procesu autentifikácie. Politika skupinového prístupu zadáva niekoľko nastavení pre reláciu užívateľa, vrátane schopnosti použiť pravidlá filtrovania IP, ktoré obmedzujú IP adresy a služby TCP/IP, ktoré má užívateľ počas relácie k dispozícii.

Vzorová konfigurácia

Ak chcete nastaviť vzorovú konfiguráciu z System i Navigator, postupujte nasledovne:

1. Vytvorte identifikátor PPP (Point-to-Point Protocol) filtra a filtre pravidiel IP paketov, ktoré zadávajú oprávnenia a obmedzenia pre túto politiku skupinového prístupu.
   a. V System i Navigator rozviňte **Network → Remote Access Services**.
   b. Kliknite na **Receiver Connection Profiles** a vyberte Group Access Policies.
   c. Kliknite pravým tlačidlom myši na preddefinovanú skupinu v pravej časti okna a vyberte **Properies**.

      Poznámka: Ak chcete vytvoriť novú politiku skupinového prístupu, pravým tlačidlom kliknite na **Group Access Policies** a vyberte **New Group Access Policies**. Vyplňte záložku **General**. Potom vyberte záložku **TCP/IP Settings** a pokračujte krokom nižšie.

   d. Vyberte záložku **TCP/IP Settings** a kliknite **Advanced**.
   e. Označte **Use IP packet rules for this connection** a kliknite na **Edit Rules File**. Tým spustíte Editor pravidiel paketov IP a otvoríte súbor s balíčkom pravidiel filtrov PPP.
   f. Otvorte ponuku **Insert** a pre vkladanie skupiny filtrov vyberte **Filters**. Záložku **General** použite na definovanie sád filtrov a záložku **Services** použite na definovanie služieb, ktoré povoľujete, ako napríklad HTTP.

Nasledujúca skupina filtrov, ″services_rules″, povolí služby HTTP, FTP a Telnet. Filtrovacie pravidlá obsahujú implicitný príkaz predvoleného odmietnutia, čím sa obmedzia všetky služby TCP/IP alebo premávka IP, ktorá nie je špecificky povolená.

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

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

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

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

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

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

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

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

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

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

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

g. Otvorte ponuku **Insert** a vyberte **Filter Interface**. Použite rozhranie filtra na vytvorenie identifikátora filtra PPP s využitím skupín filtrov, ktoré ste zadefinovali.

   1) Na záložke **General** pre identifikátor PPP filtra zadajte permitted_services.

   2) Na záložke **Filter sets** vyberte sadu filtrov **services_rules** a kliknite na **Add**.

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

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

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

h. Uložte zmeny a ukončite editor. Ak budete neskôr potrebovať vrátiť tieto zmeny späť, použite znakovo orientované rozhranie na zadanie príkazu RMVTCPTBL *ALL. Tento príkaz odstráni všetky pravidlá filtrovania a NAT zo systému.

i. V dialógu **Advanced TCP/IP settings** nechajte políčko **PPP filter identifier** prázdne a kliknite na **OK**, aby ste skončili. Neskôr by ste mali použiť identifikátor filtra, ktorý ste práve vytvorili, pre politiku skupinového prístupu, nie pre tento profil pripojenia.

2. Pre túto skupinu užívateľov definujte novú politiku skupinového prístupu.

a. V System i Navigator rozviňte **Network → Remote Access Services → Receiver Connection Profiles**.
b. Pravým tlačidlom kliknite na ikonu **Group Access Policy**, a vyberte **New Group Access Policy**. System i Navigator zobrazí dialóg **New Group Access Policy definition**.
c. Na stránke General zadajte názov a popis politiky skupinového prístupu.
d. Na strane TCP/IP Settings:
   - Označte **Use IP packet rules for this connection** a označte identifikátor filtra PPP **permitted_services**.
e. Vyberte **OK**, ak chcete politiku skupinového prístupu uložiť.

3. Politiku skupinového prístupu použite pre užívateľov, ktorí sú k tejto skupine priradení.
   a. Otvorte profil pripojení prijímateľa, ktorý riadi tieto telefonické pripojenia.
   b. Na stránke Authentication profilu pripojení prijímateľa vyberte zoznam pre overovanie platnosti, ktorý obsahuje informácie o autentifikácii užívateľa a kliknite na **Open**.
   c. Vyberte užívateľa zo skupiny Sales, pre ktorého chcete použiť politiku skupinového prístupu a kliknite na **Open**.
   d. Kliknite na **Apply a Group Policy to the user** a vyberte politiku skupinového prístupu, ktorá bola definovaná v kroku 2.
   e. Toto zopakujte pre každého užívateľa skupiny Obchod.

Súvisiace koncepty

“Konfigurácia politiky skupinového prístupu” na strane 57
Zložka **Group Access Policies** pod Receiver Connection Profiles 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 3
Pomocou podpory skupinových politík dokážu správcovia siete definovať skupinové politiky na báze užívateľa pre riadenie prostriedkov. Samostatným užívateľom je možné priradiť politiky riadenia prístupov, keď sa prihlásia do relácie PPP (Point-to-Point Protocol) alebo L2TP (Layer Two Tunneling Protocol).

Súvisiace úlohy

“Vytváranie profilu pripojenia” na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

“Používanie pravidiel filtrovania IP paketov pre PPP pripojenie” na strane 59
Súbor pravidiel paketov použite na obmedzenie prístupu užívateľa alebo skupiny na IP adresy vo vašej sieti.

Súvisiaci odkaz

“Validizačný zoznam” na strane 44
Validačný zoznam sa používa na ukladanie informácií o identifikátoroch užívateľov a heslách vzdialených užívateľov.

“Autentifikácia systému” na strane 42
PPP pripojenia k platforme System i podporujú niekoľko volieb autentifikácie pre vzdialených klientov, volajúcich do systému aj pre pripojenia k ISP alebo inému systému, do ktorého volá systém.

Súvisiace informácie

IP filtering and network address translation

Scenár: Zdieľanie modemu medzi logickými oddielmi s použitím L2TP

Virtuálny ethernet ste nastavili v štyroch logických oddieloch. Chcete, aby vybraté logické oddiely zdieľali modem pre prístup k externej sieti LAN.

Situácia

Ste administrátor systému v stredne veľkom podniku. Nadišiel čas aktualizovať počítačovú techniku, ale vy chcete ešte viac; chcete zracionalizovať svoj hardvér. Proces začnete konsolidáciou práce troch starých systémov do jedného nového systému. V systéme vytvorte tri logické oddiely. Nový systém sa dodáva s interným modemom 2793. Toto je

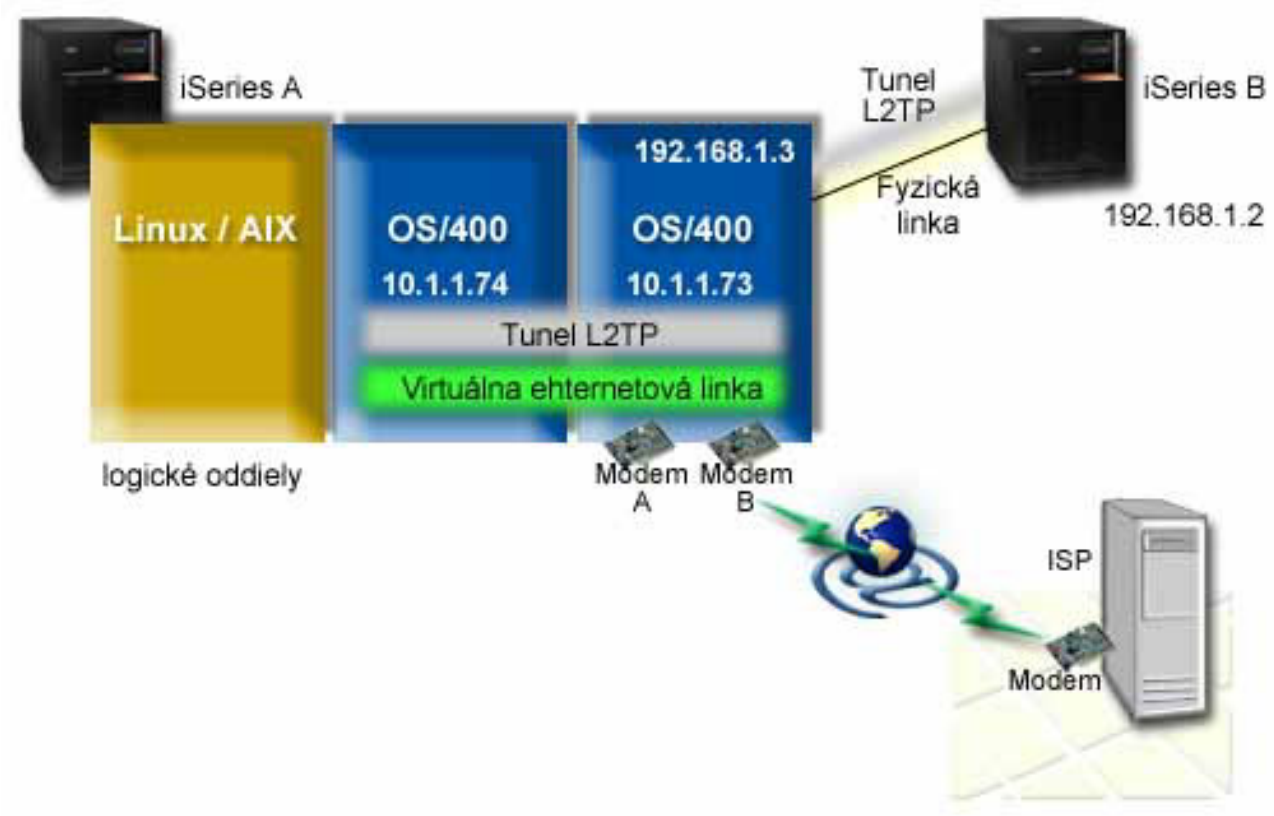
váš jediný vstupno/výstupný procesor (IOP), ktorý podporuje PPP (Point-to-Point Protocol). Máte aj starý modem 7852–400 pre elektronickú podporu zákazníkov.

Riešenie

Viac systémov alebo oddielov môže pre telefonické pripojenia zdieľať ten istý modem, takže každý systém alebo oddiel nemusí mať vlastný modem. Je to možné, ak použijete L2TP tunely a nakonfigurujete profily L2TP, ktoré umožňujú odchádzajúce volania. Vo vašej sieti budú vytvorené tunely vo virtuálnej sieti Ethernet a vo fyzickej sieti. Fyzická linka je pripojená k inému systému, ktorý zdieľa modemy vo vašej sieti.

Podrobnosti

Tento obrázok zobrazuje charakteristiky siete pre tento scenár:



Obrázok 9. Viacero systémov zdieľajúcich rovnaký modem pre telefonické pripojenia

Požiadavky a predpoklady

System A musí spĺňať nasledujúce požiadavky na nastavenie:

- V oddiele, ktorý vlastní modemy so schopnosťou ASYNC, musí byť nainštalovaný i5/OS Version 5 Release 3 alebo novší
- Hardvér, ktorý dovoľuje vytvorenie oddielov.
- System i Access for Windows a System i Navigator (Konfiguračný a servisný komponent System i Navigator), Version 5 Release 3 alebo novší,
- V systéme ste vytvorili najmenej dva logické oddiely (LPAR). Oddiel, ktorý vlastní modem, musí mať nainštalovaný i5/OS V5R3 alebo novší. Ostatné oddiely môžu mať nainštalovaný OS/400 V5R2, i5/OS V5R3, Linux alebo AIX. V tomto scenári oddiely buď používajú i5/OS alebo operačný systém Linux.

- Na komunikáciu medzi oddielmi máte vytvorený virtuálny Ethernet.

System B musí mať nainštalovaný licenčný program a relevantné komponenty System i Navigator: System i Access for Windows a System i Navigator (Konfiguračný a servisný komponent System i Navigator) V5R2 alebo novší.

Súvisiace informácie

Logické oddiely

Podrobnosti scenára: Zdieľanie modemu medzi logickými oddielmi pomocou L2TP

Keď splníte nevyhnutné podmienky, budete pripravený konfigurovať profily L2TP (Layer Two Tunneling Protocol).

Krok 1: Konfigurácia profilu terminátora L2TP pre ľubovoľné rozhranie v oddiele, ktorý vlastní modemy:

Ak chcete vytvoriť profil terminátora pre ľubovoľné rozhranie, postupujte nasledovne:

1. V System i Navigator rozviňte ***váš systém*** → **Network** → **Remote Access Services**.
2. Pravým tlačidlom myši kliknite na **Receiver Connection Profiles** a vyberte **New Profile**.
3. Na stránke Setup vyberte tieto voľby a kliknite na **OK**:
   - **Protocol type**: PPP
   - **Connection type**: L2TP (virtual line)
   - **Operating mode**: Terminator (network server)
   - **Type of line service**: Single line
4. Na záložke **New Profile - General** vyplňte tieto polia:
   - **Name**: toExternal
   - **Description**: Pripojenie príjemcu, ktoré sa bude vytáčať
   - Vyberte **Start profile with TCP**.
5. Na záložke **New Profile - Connection** vyplňte tieto polia.
   - **Local tunnel endpoint IP address**: ANY
   - **Virtual line name**: toExternal. Táto linka nemá priradené žiadne fyzické rozhrania. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Keď sa otvorí okno L2TP Line Properties, kliknite na záložku **Authentication** a zadajte názov hostiteľa vášho systému. Kliknite na **OK**, ak sa chcete vrátiť na záložku **Connection** v okne New PPP Profile Properties.
6. Kliknite na **Allow out-going call establishment**. Zobrazí sa dialógové okno **Outgoing call dial properties**.
7. Na strane Outgoing Call Dial Properties vyberte typ služby linky.
   - **Type of line service**: Line pool
   - **Name**: dialOut
   - Kliknite na **New**. Zobrazí sa dialógové okno **New Line Pool Properties**.
8. V okne New line pool properties vyberte linky a modemy, pre ktoré chcete povoliť odchádzajúce volania a kliknite na **Add**. Ak potrebujete definovať tieto linky, vyberte **New Line**. Rozhrania v oddiele, ktorý vlastní tieto modemy sa pokúsia použiť ktorúkoľvek otvorenú linku z tejto oblasti liniek. Otvorí sa okno Line Properties.
9. Na záložke **New Line Properties - General** zadajte informácie do týchto polí:
   - **Name**: line1
   - **Description**: prvá linka a prvý modem pre oblasť liniek (interný modem 2793)
   - **Hardware resource**: cmn03 (communication port)
10. Akceptujte predvolené hodnoty vo všetkých ostatných záložkách a kliknutím na **OK** sa vráťte do okna New Line Pool Properties.
11. V okne New Line Pool Properties vyberte linky a modemy, pre ktoré chcete povoliť odchádzajúce volania a kliknite na **Add**. Skontrolujte, že je pre oblasť vybratý modem 2793.
12. Znovu vyberte **New Line**, ak chcete pridať modem elektronickej podpory zákazníkov 7852–400. Otvorí sa okno Line Properties.
13. Na záložke **New Line Properties - General** zadajte informácie do týchto polí:

- **Name**: line2
- **Description**: druhá linka a druhý modem pre oblasť liniek (7852-400 externý modem elektronickej podpory zákazníkov)
- **Hardware resource**: cmn04 (V.24 port)
- **Framing**: Asynchronous

14. Na záložke **New Line Properties - Modem** vyberte externý modem (7852–400) a kliknite na **OK**, aby ste sa vrátili do okna New Line Pool Properties.
15. Vyberte všetky ostatné dostupné linky, ktoré chcete pridať do oblasti liniek a kliknite na **Add**. V tomto príklade skontrolujte, či sú dva nové modemy, ktoré ste pridali, uvedené v poli **Selected lines for pool** a kliknite na **OK**, aby ste sa vrátili do okna Outgoing Call Dial Properties.
16. V okne Outgoing Call Dial Properties zadajte Default Dial Numbers a kliknite na **OK**, aby ste sa vrátili do okna New PPP Profile Properties.

    Poznámka: Tieto čísla môžu byť niečo také ako váš ISP (Internet Service Provider), ktorého budú často volať ostatné systémy, ktoré tieto modemy používajú. Ak iné systémy použijú telefónne číslo *PRIMARY alebo *BACKUP, skutočné čísla, ktoré sa vytočia, sú tu zadané čísla. Ak iné systémy zadajú skutočné telefónne číslo, namiesto neho sa použije telefónne číslo.
17. Na záložke **TCP/IP Settings** vyberte tieto hodnoty:
    - **Local IP address**: None
    - **Remote IP address**: None

    Poznámka: Ak chcete profil použiť na ukončenie L2TP relácií, musíte vybrať lokálnu IP adresu, ktorá predstavuje systém. Pre vzdialenú IP adresu môžete vybrať oblasť adries, ktorá je v rovnakej podsieti ako váš systém. Všetky L2TP relácie získajú svoje IP adresy z tejto oblasti.
18. Na záložke **Authentication** akceptujte všetky predvolené hodnoty.

Práve ste dokončili konfiguráciu profilu L2TP terminátora v oddiele s modemami. Nasledujúcim krokom je konfigurácia vzdialeného L2TP vytáčania, profilu odosielateľa pre 10.1.1.74.

Súvisiaci odkaz

"Podpora profilov viacerých pripojení" na strane 51
Profily dvojbodového pripojenia, ktoré podporujú viaceré pripojenia vám umožňujú mať jeden profil pripojenia, ktorý bude spracovávať mnohé digitálne, analógové alebo L2TP volania.

Krok 2: Konfigurácia profilu odosielateľa L2TP na 10.1.1.74:

Tieto kroky vás povedú procesom vytvárania profilu odosielateľa L2TP (Layer Two Tunneling Protocol (L2TP):

1. V System i Navigator rozviňte **10.1.1.74 → Network → Remote Access Services**.
2. Pravým tlačidlom myši kliknite na **Originator Connection Profiles** a vyberte **New Profile**.
3. Na stránke Setup vyberte tieto voľby a kliknite na **OK**:
   - **Protocol type**: PPP
   - **Connection type**: L2TP (virtual line)
   - **Operating mode**: Remote dial
   - **Type of line service**: Single line
4. Na záložke **General** vyplňte tieto polia:
   - **Name**: toModem
   - **Description**: pripojenie pôvodcu k oddielu vlastniacemu modem
5. Na záložke **Connection** vyplňte tieto polia:

   Virtual line name: toModem. Táto linka nemá žiadne priradené fyzické rozhranie. Virtuálna linka opisuje rôzne charakteristiky tohto profilu PPP. Otvorí sa okno L2TP Line Properties.
6. Na záložke **General** zadajte opis pre virtuálnu linku.

7. Na záložke **Authentication** zadajte lokálny názov hostiteľa oddielu a kliknite na **OK**, aby ste sa vrátili na stranu Connection.
8. Do poľa **Remote telephone numbers** pridajte *PRIMARY a *BACKUP. Toto dovoľuje profilu používať rovnaké telefónne čísla ako ukončovací profil v oddiele, ktorý vlastní modemy.
9. Do poľa **Remote tunnel endpoint host name or IP address** zadajte adresu IP vzdialeného koncového bodu tunela (10.1.1.73).
10. Na záložke **Authentication** vyberte voľbu **Allow the remote system to verify the identity of this iSeries server**.
11. Pre autentifikačný protokol na použitie vyberte **Require encrypted password (CHAP-MD5)**. Predvolene je tiež vybraté **Allow extensible authentication protocol**.

    Poznámka: Protokol by sa mal zhodovať s akýmkoľvek protokolom, ktorý používa systém, do ktorého voláte.
12. Zadajte meno užívateľa a heslo.

    Poznámka: Meno užívateľa a heslo sa musí zhodovať s akýmkoľvek platným menom užívateľa a heslom v systéme, do ktorého voláte.
13. Prejdite na záložku **TCP/IP Settings** a skontrolujte vyžadované polia:
    - **Local IP address**: Assigned by remote system
    - **Remote IP address**: Assigned by remote system
    - **Routing**: No additional routing is required
14. Kliknutím na **OK** uložte profil PPP.

Krok 3: Konfigurácia profilu vzdialeného vytáčania L2TP pre 192.168.1.2:

Profil vzdialeného vytáčania L2TP (Layer Two Tunneling Protocol) môžete pre 192.168.1.2 nakonfigurovať zopakovaním Kroku 2 a zmenením koncového bodu vzdialeného tunela na 192.168.1.3 (fyzické rozhranie, ku ktorému sa pripája System B).

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

Krok 4: Testovanie pripojenia:

Keď dokončíte konfiguráciu obidvoch systémov, mali by ste otestovať pripojiteľnosť, aby ste sa presvedčili, či systémy zdieľajú modem, aby mali dosah do externých sietí.

1. Presvedčte sa, či je aktívny profil terminátora L2TP (Layer Two Tunneling Protocol).
   a. V System i Navigator rozviňte **10.1.1.73 → Network → Remote Access Services → Receiver Connection Profiles**.
   b. V pravom podokne vyhľadajte požadovaný profil (toExternal) a skontrolujte, či je v poli **Status** hodnota Active. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
2. Spustite profil vzdialeného telefonického pripojenia pre 10.1.1.74.
   a. V System i Navigator rozviňte **10.1.1.74 → Network → Remote Access Services → Originator Connection Profiles**.
   b. V pravom podokne vyhľadajte požadovaný profil (toModem) a skontrolujte, či je v poli **Status** hodnota Active. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
3. V System B spustite profil diaľkového volania.
   a. V System i Navigator rozviňte **192.168.1.2 → Network → Remote Access Services → Originator Connection Profiles**.
   b. V pravom podokne vyhľadajte vami vytvorený profil a skontrolujte, či je v poli **Status** hodnota Active. Ak nie, kliknite pravým tlačidlom myši na profil a vyberte **Spustiť**.
4. Ak je to možné, otestujte odozvu ISP (Internet Service Provider) alebo iného cieľa, do ktorého ste volali, aby ste si overili či sú obidva profily aktívne. Pokúste sa vykonať príkaz ping z adresy 10.1.1.74 aj 192.168.1.2.
5. Alternatívne môžete skontrolovať stav pripojenia.

a. V System i Navigator rozviňte **the system → Network → Remote Access Services → Originator Connection Profiles**.
b. V pravej časti okna kliknite pravým tlačidlom na profil, ktorý ste vytvorili a vyberte **Connections**. V okne Connection Status môžete vidieť, ktoré profily sú aktívne, neaktívne, pripájajú sa a podobne.

Plánovanie PPP

Plánovanie PPP (Point-to-Point Protocol) obsahuje vytváranie a administráciu PPP pripojení.

Súvisiaci odkaz

"Scenár: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému" na strane 13
Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

"Scenár: Pripájanie kancelárskej siete LAN k Internetu pomocou modemu" na strane 15
Administrátori zvyčajne nastavujú kancelárske siete pre zamestnancov, aby mali prístup na Internet. Administrátori môžu použiť modem na pripojenie systému k ISP (Internet Service Provider). PC klienti pripojení k sieti LAN môžu komunikovať cez Internet pomocou operačného systému i5/OS v úlohe brány.

"Súvisiace informácie pre Remote Access Services" na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Softvérové a hardvérové požiadavky

PPP (Point-to-Point Protocol) prostredie vyžaduje, aby ste mali dva alebo viaceré počítače, ktoré podporujú PPP. Jeden z týchto počítačov, platforma System i, môže byť buď odosielateľom alebo prijímateľom.

Systém musí spĺňať nasledujúce nevyhnutné podmienky, aby mohli vzdialené systémy naň pristupovať.

- System i Navigator s podporou TCP/IP.
- Jeden z dvoch profilov pripojenia:
  - Profil pripojení odosielateľa pre spracovanie odchádzajúcich PPP pripojení.
  - Profil pripojení prijímateľa pre spracovanie prichádzajúcich PPP pripojení.
- Konzola pracovnej stanice PC, na ktorej je nainštalovaný System i Access for Windows 95 alebo novší s System i Navigator.
- Nainštalovaný adaptér.

  Môžete si zvoliť jeden z uvedených adaptérov:
  - 2699*: Dvojlinkový WAN vstupno/výstupný adaptér (IOA).
  - 2720*: PCI WAN/Twinaxial IOA.
  - 2721*: PCI dvojlinkový WAN IOA.
  - 2745*: PCI dvojlinkový WAN IOA (nahrádza IOA 2721).
  - 2742*: Dvojlinkový IOA (nahrádza IOA 2745).
  - 2771: Dvojportový WAN IOA s integrovaným modemom V.90 na porte 1 a štandardným komunikačným rozhraním na porte 2. Na použitie portu 2 adaptéra 2771 sa vyžaduje externý modem alebo terminálový adaptér ISDN s príslušným káblom.
  - 2772: Dvojportový V.90 integrovaný modem WAN IOA.
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: Ethernetový adaptér pre PPPoE pripojenia.
  - 2793/576C: Dvojportový WAN IOA, s integrovaným modemom V.92 na porte 1 a štandardným komunikačným rozhraním na porte 2. Ak chcete používať port 2, vyžaduje sa externý modem alebo ISDN terminálový adaptér s príslušným káblom.
  - 2805 Štvorportový WAN IOA s integrovaným analógovým modemom V.92. To nahradí modely 2761 a 2772.

***** Tieto adaptéry vyžadujú externý modem V.90 (alebo novší) alebo ISDN (Integrated Services Digital Network) terminálový adaptér a RS-232 (EIA 232) alebo kompatibilný kábel.

- V závislosti od typu vášho pripojenia a linky potrebujete jedno z uvedených zariadení:
  - externý alebo interný modem alebo CSU/DSU (Channel Service Unit/Data Service Unit).
  - ISDN (Integrated Services Digital Network) terminálový adaptér.
- 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 2
Profily dvojbodových pripojení definujú sadu parametrov a prostriedkov pre špecifické PPP (Point-to-Point Protocol) pripojenia. Môžete spustiť profily, ktoré používajú tieto nastavenia parametrov na vytváranie odchádzajúcich volaní (odosielanie) alebo na načúvanie (prijímanie) PPP pripojení.

"Modemy" na strane 38
Aj externé aj interné modemy sa dajú použiť pre PPP (Point-to-Point Protocol) pripojenia.

"CSU/DSU" na strane 38
CSU (Channel Service Unit) je zariadenie, ktoré pripája terminál k digitálnej linke. DSU (Data Service Unit) je zariadenie, ktoré vykonáva ochranné a diagnostické funkcie pre telekomunikačnú linku. Obe zariadenia sa zväčša dodávajú ako jedna jednotka CSU/DSU.

"Terminálové adaptéry ISDN" na strane 38
ISDN (Integrated Services Digital Network) vám poskytuje digitálne pripojenie, ktoré vám umožní komunikovať s použitím ľubovoľnej kombinácie hlasu, údajov a videa a mnohých iných multimediálnych aplikácií.

Alternatívy pripojenia

PPP (Point-to-Point Protocol) dokáže prenášať datagramy cez sériové dvojbodové linky.

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.

PPP podporuje veľkú škálu typov liniek, ale SLIP (Serial Line Internet Protocol) podporuje len typy asynchrónnych 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 používajú medzi zákazníkom a ústredňou existujúcich zariadení hlasových sietí telefónnych spoločností.

Linky PPP vytvárajú fyzické pripojenie medzi lokálnym a vzdialeným hostiteľom. Oblasť liniek poskytuje 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. Najrýchlejšie modemy dnes pracujú nekomprimovanou rýchlosťou 56 kbps. 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 %. Údaje, ktoré už boli skomprimované alebo zašifrované, sa môžu pri použití V.42bis dokonca zvýšiť. X2 alebo 56Flex rozširuje rýchlosť bps 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 sa 56 kbps používa len vtedy keď presúvate údaje z digitálneho konca

na analógový koniec linky. Táto technológia je vhodná najmä pre pripojenia k ISP, ktoré majú u seba digitálny koniec linky a hardvér. Zvyčajne sa pripájate k analógovému modemu V.24 cez sériové rozhranie RS-232 pomocou asynchrónneho protokolu 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. Pretože technológia V.90 nazerá na verejnú komutovanú telefónnu sieť ako na digitálnu sieť, dokáže zrýchliť údaje z Internetu do počítača rýchlosťami až 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 (väčšinou cez klávesnicu a myš zadávané príkazy z počítača do centrálnej lokality, ktoré vyžadujú menšiu šírku pásma) pokračujú konvenčnými rýchlosťami 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 tak, že umožňuje prenášať údaje proti prúdu rýchlosťami do 48 kbps. Okrem toho sa skrátia časy pripojenia vďaka zlepšeniam v procese dotaz-odpoveď a modemom, ktoré podporujú funkciu podržania, a preto zostanú pripojené, zatiaľ čo telefónna linka akceptuje prichádzajúci hovor alebo používa čakajúce volanie.

Digitálny servis a DDS (Digital Data Services)

Digitálny servis a DDS (Digital Data Services) môžete používať s PPP (Point-to-Point Protocol).

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 prenajaté, trvalé pripojenia s pevne stanovenými prenosovými rýchlosťami do 56 kbps. Uvedená služba je všeobecne známa aj ako DS0.

K DDS sa môžete pripojiť pomocou špeciálnej krabičky s názvom *CSU/DSU (Channel Service Unit/Data Service Unit)*, ktorá v analógovom scenári nahrádza modem. DDS má fyzické obmedzenia, ktoré súvisia hlavne so vzdialenosťou medzi CSU/DSU a ústredňou telefónnej spoločnosti. DDS funguje najlepšie do vzdialenosti 9000 m (30000 stôp). Telefónne spoločnosti dokážu dlhšie vzdialenosti kompenzovať zosilňovačmi signálov, ale táto služba je drahšia. DDS najlepšie vyhovuje pre pripojenie dvoch lokalít, ktoré obsluhuje rovnaká ústredňa. Pri medzimestských pripojeniach medzi rôznymi ústredňami, vzdialenostné poplatky rýchlo urobia z DDS nepraktické riešenie. V takýchto prípadoch môže byť lepším riešením Komutované-56. K DDS CSU/DSU sa bežne pripájate cez sériové rozhranie V.35, RS449 alebo X.21 so synchrónnym protokolom rýchlosťami maximálne 56 kbps.

Súvisiaci odkaz

“CSU/DSU” na strane 38
CSU (Channel Service Unit) je zariadenie, ktoré pripája terminál k digitálnej linke. DSU (Data Service Unit) je zariadenie, ktoré vykonáva ochranné a diagnostické funkcie pre telekomunikačnú linku. 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.

Linka SW56 sa na nastavenie DDS (Digital Data Services) podobá v tom, že zariadenie údajového terminálu (DTE) sa pripája k digitálnej službe prostredníctvom SCU/DSU (Channel Service Unit/Data Service Unit). SW56 CSU/DSU,

však obsahuje číselník, z ktorého zadávate telefónne číslo vzdialeného hostiteľa. SW56 môžete použiť na vytváranie telefonických digitálnych pripojení k ľubovoľnému účastníkovi SW56 kdekoľvek v regióne alebo za medzinárodnými hranicami.

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.

Bežne sa môžete k SW56 CSU/DSU pripojiť cez V.35 alebo cez sériové rozhranie RS 449 so synchrónnym protokolom rýchlosťami až do 56 kbps. V prípade volacej/odpovedacej jednotky V.25bis pretekajú údaje a riadenie volania po jednom sériovom rozhraní.

Súvisiaci odkaz

"Digitálny servis a DDS (Digital Data Services)" na strane 33
Digitálny servis a DDS (Digital Data Services) môžete používať s PPP (Point-to-Point Protocol).

"Digitálna sieť s integrovanými službami (ISDN)"
ISDN (Integrated Services Digital Network) poskytuje komutovanú digitálnu pripojiteľnosť z jedného konca na druhý. ISDN dokáže prenášať hlas aj údaje cez rovnaké pripojenie.

Digitálna sieť s integrovanými službami (ISDN)

ISDN (Integrated Services Digital Network) poskytuje komutovanú digitálnu pripojiteľnosť z jedného konca na druhý. ISDN dokáže prenášať hlas aj údaje cez rovnaké pripojenie.

Existuje niekoľko rôznych druhov služieb ISDN, najbežnejšia je však Basic Rate Interface (BRI). BRI sa skladá z dvoch 64 kbps B kanálov na prenos zákaznických údajov a D kanála na prenos signalizačných údajov. Dva B kanále sadajú navzájom prepojiť, aby poskytovali kombinovanú rýchlosť 128 kbps. V niektorých oblastiach môže telefónna spoločnosť obmedziť každý B kanál buď na 56 kbps alebo na kombinovaných 112 kbps. 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.

Odvetvie sa teraz skonvergovalo na synchrónny PPP protokol s PPP multilink pre prepojenie dvoch B kanálov. Niektorí výrobcovia integrujú do nimi vyrábaných terminálových adaptérov funkciu V.34 (analógový modem). Táto schopnosť umožňuje zákazníkom s jednou ISDN linkou spracovávať buď ISDN alebo konvenčné analógové volania a využívať pritom výhodu súčasných hlasových/údajových schopností služieb ISDN. Pomocou tejto technológie dokáže terminálový adaptér pracovať aj ako strana digitálneho systému pre klientov V.92.

Bežne sa musíte k ISDN terminálovému adaptéru pripojiť cez sériové rozhranie RS-232 s použitím asynchrónneho protokolu rýchlosťami do 230.4 kbps. Avšak maximálna systémová prenosová rýchlosť v baudoch pre asynchrónny protokol cez RS-232 je 115.2 kbps. Bohužiaľ to obmedzuje maximálnu prenosovú rýchlosť v bajtoch na 11.5 kbps, zatiaľ čo terminálový adaptér s viacerými linkami môže poskytovať nekomprimovaných 14 alebo 16 KB. Niektoré terminálové adaptéry podporujú synchrónny protokol cez RS-232 pri 128 kbps, ale maximálna systémová prenosová rýchlosť v baudoch pre synchrónny protokol cez RS-232 je 64 kbps.

Systém dokáže spúšťať asynchrónny protokol cez V.35 rýchlosťami až do 230.4 kbps, ale výrobcovia terminálových adaptérov bežne takúto konfiguráciu neponúkajú. Prevodníky rozhraní, ktoré prevádzajú rozhranie RS-232 na rozhranie V.35 môžu byť rozumným riešením problému, ale tento prístup nebol ešte pre systém posúdený. Ďalšou možnosťou je

použiť terminálové adaptéry so synchrónnym protokolom rozhrania V.35 pri rýchlosti 128 kbps. Hoci táto trieda terminálových adaptérov existuje, nezdá sa, že by mnohé ponúkali synchrónny viaclinkový PPP.

Súvisiaci odkaz

"Komutovaná-56" na strane 33
Ak nepotrebujete non-stop pripojenie, používaním komutovanej digitálnej služby, ktorá sa nazýva *Komutovaná-56 (SW56)* môžete ušetriť.

"Terminálové adaptéry ISDN" na strane 38
ISDN (Integrated Services Digital Network) vám poskytuje digitálne pripojenie, ktoré vám umožní komunikovať s použitím ľubovoľnej kombinácie hlasu, údajov a videa a mnohých iných multimediálnych aplikácií.

T1/E1 a čiastočné pripojenia T1

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

T1/E1

V pripojení T1 je navzájom previazaných 24 64-kbps (DS0) TDM (Time-Division Multiplexed) kanálov cez 4 vodičový medený okruh. To vytvára celkovú šírku pásma 1.544 mbps. V obvode E1 v Európe a iných častiach sveta je navzájom previazaných 32 64-kbps kanálov, ktoré tvoria celkovú šírku pásma 2.048 mbps. Vďaka vopred vyhradeným časovým slotom umožňuje TDM viacerým používateľom zdieľať médium digitálneho prenosu. Mnohé digitálne pobočkové ústredne (PBX) využívajú službu T1 na importovanie viacerých hovorových okruhov cez jednu T1 linku namiesto 24 dvojíc vodičov, natiahnutých medzi PBX a telefónnou spoločnosťou.

Treba si uvedomiť, že T1 možno zdieľať medzi hlas a údaje. Telefonické služby môžu prechádzať cez podmnožinu 24 kanálov T1 linky, napríklad zostávajúce kanály budú ponechané pre pripojenia 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). V dôsledku toho je možné použiť jednoduchšie zariadenie CSU/DSU (Channel Service Unit/Data Service Unit). Bežne sa k T1/E1 CSU/DSU alebo k multiplexeru môžete pripojiť cez V.35 alebo cez sériové rozhranie RS 449 pomocou synchrónneho protokolu rýchlosťami násobkov od 64 kbps do 1.544 mbps alebo 2.048 mbps. Časovanie v sieti zabezpečuje multiplexor alebo CSU/DSU.

Čiastočné T1

Pomocou FT1 (Fractional T1) si môže zákazník prenajať ľubovoľnú alikvotnú časť 64-kbps T1 linky. FT1 je užitočné vždy, keď náklady na vyhradenú T1 sú pre zákazníka nedostupné pri skutočnej šírke pásma, ktorú využíva. 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. Toto riešenie je veľmi rozšírené medzi ISP (Internet Service Provider), ktorý používajú jedno T1 diaľkové vedenie zo svojej prevádzky do digitálneho prepínača telefónnej spoločnosti. V týchto prípadoch možno viacero klientov obslúžiť linkou FT1 súčasne. Bežne sa môžete k T1/E1 CSU/DSU alebo multiplexeru pripojiť cez V.35 alebo cez sériové rozhranie RS 449 so synchrónnym protokolom určitým násobkom 64 kbps. Pri FT1 máte vopred alokovanú 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 podporujú v USA 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 spoločností teraz poskytuje službu Frame Relay pre zákazníkov, ktorí chcú pripojenia od rýchlosti 56 kbps do rýchlosti T1. (V Európe rýchlosť Frame Relay kolíše od 64 kbps do 2 mbps. V USA je Frame Relay dosť rozšírená, pretože je relatívne lacná. V niektorých oblastiach sa však nahrádza rýchlejšími technológiami, napríklad asynchrónny režim prenosu (ATM).

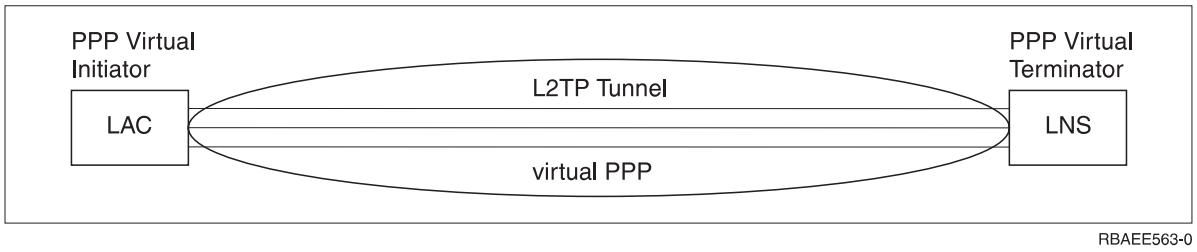
Podpora L2TP (tunelovania) pre pripojenia PPP

L2TP (Layer 2 Tunneling Protocol) je tunelovací protokol, ktorý rozširuje PPP (Point-to-Point Protocol) aby podporoval a tunel vrstvy liniek medzi žiadajúcim L2TP klientom (L2TP Access Concentrator alebo LAC) a cieľovým koncovým bodom L2TP servera (L2TP Network Server alebo LNS).

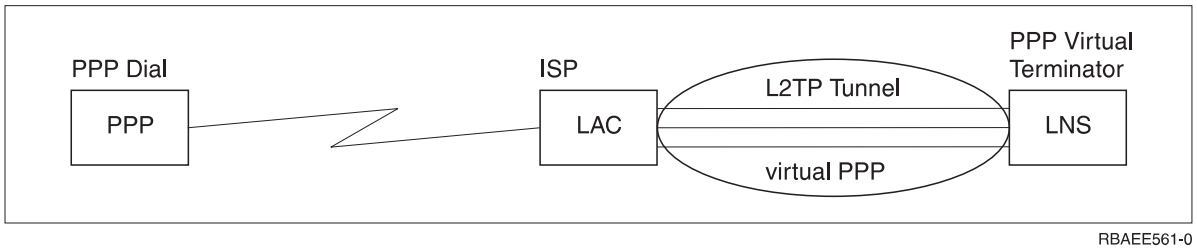
Layer Two Tunneling Protocol

Používaním L2TP (Layer Two Tunneling Protocol) tunelov je možné oddeliť miesto, v ktorom sa končí protokol telefonického pripojenia a v ktorom sa poskytuje prístup do siete. Z tohto dôvodu sa L2TP nazýva aj *virtuálne PPP*.

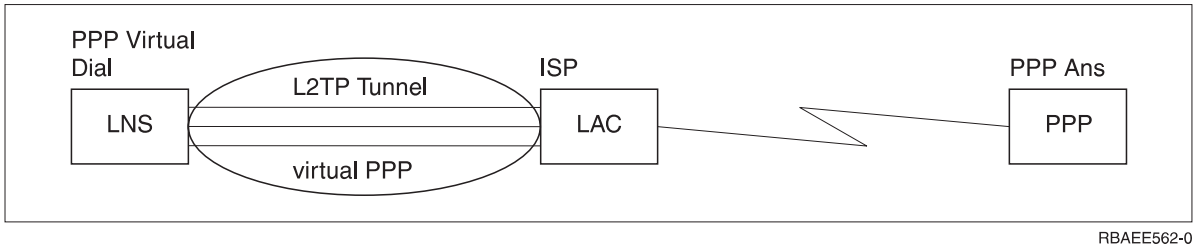
Tieto obrázky ilustrujú tri rozdielne implementácie tunelovania L2TP.



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 RCF (Request for Comment), RFC-2661. Tunel L2TP môže pokrývať celú reláciu PPP alebo len jeden segment dvojsegmentovej relácie. Je to možné dosiahnuť štyrmi rôznymi modelmi tunelovania.

Súvisiace informácie

Scenár: Ochrana nevynúteného tunela L2TP pomocou IPSec

Editor RFC

Nevynútený tunel:

V modeli nevynúteného tunelu užívateľ vytvorí tunel, zvyčajne s použitím klienta, ktorý má povolený protokol L2TP (Layer Two Tunneling Protocol).

Výsledkom je, že užívateľ odošle pakety L2TP do ISP (Internet Service Provider), ktorý ich pošle ďalej do LNS (L2TP Network Server). Pri nevynútenom tunelovaní ISP nemusí podporovať L2TP a inicializátor L2TP tunela je na rovnakom systéme ako vzdialený klient. V tomto modeli sa tunel tiahne celou PPP (Point-to-Point Protocol) reláciou z klienta L2TP do 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 odošle pakety PPP (Point-to-Point Protocol) do ISP (Internet Service Provider) LAC (L2TP (Layer Two Tunneling Protocol (L2TP) Access Concentrator)). ISP zapuzdrí pakety do L2TP a odošle ich tunelom do LNS (L2TP Network Server). V prípade povinného odosielania cez tunel musí mať ISP schopnosť L2TP. V tomto modeli sa tunel tiahne len cez segment PPP relácie medzi ISP a LNS.

Vynútený tunel - vzdialené telefonické pripojenie:

V modeli s povinným tunelom - vzdialené telefonické pripojenie, domovská brána (LNS (L2TP Network Server)) inicializuje tunel k ISP (Internet Service Provider) LAC a dáva pokyny ISP, aby vložil miestne volanie do PPP (Point-to-Point Protocol) odpovedacieho klienta.

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:

L2TP (Layer Two Tunneling Protocol) pripojenie s viacerými skokmi je spôsob presmerovania L2TP prevádzky v mene klientskych LAC (L2TP Access Concentrators) a LNS (L2TP Network Servers).

Pripojenie s viacerými skokmi sa vytvorí pomocou L2TP viacúsekovej brány (systém, ktorý vzájomne prepája profily L2TP Terminator a L2TP Initiator). 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) označuje triedu technológie, ktorá sa používa na získavanie širšieho pásma cez existujúce medené telefónne vedenia, natiahnuté medzi pozemkom zákazníka a ISP (Internet Service Provider).

DSL dovoľuje simultánne používanie hlasových a vysokorýchlostných dátových služieb cez jeden pár medených telefónnych vodičov. Modemové rýchlosti sa postupne zvýšili vďaka použitiu rôznych komprimačných a iných techník, ale pri dnešných najrýchlejších (56 kbps) sa približujú teoretickému limitu pre túto technológiu. Technológia DSL povoľuje oveľa vyššie rýchlosti cez krútenú dvojlinku z ústredne domov, do školy alebo do práce. V niektorých oblastiach je možné dosahovať rýchlosti do 2 Mbps. PPP sa typicky používa na sériových komunikačných linkách, ako sú telefonické pripojenia modemov. Mnohí poskytovatelia DSL internetových služieb teraz používajú PPPoE (PPP over Ethernet) kvôli jeho pridaným prihlasovacím a bezpečnostným funkciám.

DSL modem je zariadenie, ktoré sa umiestni na ľubovoľný koniec medenej telefónnej linky, aby počítaču (alebo sieti LAN) umožnil pripojiť sa k Internetu prostredníctvom DSL pripojenia. Na rozdiel od telefonického pripojenia, zvyčajne nevyžaduje vyhradenú telefónnu linku (rozdeľovač POTS dovoľuje simultánne zdieľanie linky). Hoci sa DSL modemy podobajú na bežné analógové modemy, poskytujú oveľa väčšiu priepustnosť.

Zariadenia pre pripojenia

Systém používa na spracovanie PPP (Point-to-Point Protocol) pripojení modemy, ISDN (Integrated Services Digital Network) terminálové adaptéry, adaptéry kruhových sietí so známkou, ethernetové adaptéry alebo zariadenia CSU/DSU (Channel Service Unit/Data Service Unit).

Vo svojom PPP prostredí môžete používať nasledujúce štyri druhy komunikačných zariadení:

- Modemy
- CSU/DSU
- Terminálové adaptéry ISDN
- Ethernetové adaptéry (pre pripojenia PPPoE)

Modemy

Aj externé aj interné modemy sa dajú použiť pre PPP (Point-to-Point Protocol) pripojenia.

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 sa jedná o interný modem, reťazce modemu už boli zadefinované na použitie.

V systéme je zadefinovaných mnoho modelov modemov, ale nové modely môžete definovať prostredníctvom System i Navigator. Existujúcu definíciu možno použiť ako základ na zadefinovanie nového typu. Ak neviete, aké príkazy váš modem používa alebo ak nemáte prístup k dokumentácii k modemu, začnite generickou Hayesovou definíciou modemu. Preddefinované definície sa nemôžu meniť. K vytvorenému inicializačnému príkazu alebo vytáčaciemu reťazcu však možno pridať ďalšie príkazy.

Modem elektronickej zákazníckej podpory, ktorý je súčasťou systému, môžete použiť na vytvorenie PPP pripojení. V starších systémoch bol modem elektronickej zákazníckej podpory externým modemom IBM 7852-400. Tento modem bol nahradený modemom MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. V novších systémoch môžete ako modem elektronickej zákazníckej podpory používať 2771, 2793 alebo nejaký iný podporovaný interný modem.

Súvisiaci odkaz

“Softvérové a hardvérové požiadavky” na strane 31
PPP (Point-to-Point Protocol) prostredie vyžaduje, aby ste mali dva alebo viaceré počítače, ktoré podporujú PPP. Jeden z týchto počítačov, platforma System i, môže byť buď odosielateľom alebo prijímateľom.

CSU/DSU

CSU (Channel Service Unit) je zariadenie, ktoré pripája terminál k digitálnej linke. DSU (Data Service Unit) je zariadenie, ktoré vykonáva ochranné a diagnostické funkcie pre telekomunikačnú linku. 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 31
PPP (Point-to-Point Protocol) prostredie vyžaduje, aby ste mali dva alebo viaceré počítače, ktoré podporujú PPP. Jeden z týchto počítačov, platforma System i, môže byť buď odosielateľom alebo prijímateľom.

“Digitálny servis a DDS (Digital Data Services)” na strane 33
Digitálny servis a DDS (Digital Data Services) môžete používať s PPP (Point-to-Point Protocol).

Terminálové adaptéry ISDN

ISDN (Integrated Services Digital Network) vám poskytuje digitálne pripojenie, ktoré vám umožní komunikovať s použitím ľubovoľnej kombinácie hlasu, údajov a videa a mnohých iných multimediálnych aplikácií.

Musíte si skontrolovať, či je váš terminálový adaptér dimenzovaný pre použitie v systéme.

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

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Pravým tlačidlom myši kliknite na **Modems** a vyberte **New Modem**.
3. Do dialógového okna **New Modem Properties** zadajte správne hodnoty do všetkých políčok **field** na záložke **General**. Terminálový adaptér ISDN musíte zadefinovať ako komunikačné zariadenie.
4. Vyberte panel **ISDN Parameters**.
5. Na paneli **ISDN Parameters** pridajte alebo zmeňte vlastnosti ISDN tak, aby zodpovedali vlastnostiam, ktoré vyžaduje váš terminálový adaptér.

Súvisiace úlohy

"Príklad: Konfigurácia ISDN terminálového adaptéra" na strane 55
Príklad demonštruje ako máte nakonfigurovať ISDN (Integrated Services Digital Network) terminálový adaptér.

Súvisiaci odkaz

"Softvérové a hardvérové požiadavky" na strane 31
PPP (Point-to-Point Protocol) prostredie vyžaduje, aby ste mali dva alebo viaceré počítače, ktoré podporujú PPP. Jeden z týchto počítačov, platforma System i, môže byť buď odosielateľom alebo prijímateľom.

"Digitálna sieť s integrovanými službami (ISDN)" na strane 34
ISDN (Integrated Services Digital Network) poskytuje komutovanú digitálnu pripojiteľnosť z jedného konca na druhý. ISDN dokáže prenášať hlas aj údaje cez rovnaké pripojenie.

Odporúčania pre terminálový ISDN adaptér:

Existuje niekoľko rôznych terminálových adaptérov, ktoré môžete používať.

Odporúčaný externý terminálový ISDN (Integrated Services Digital Network) adaptér alebo ISDN modem je **3Com/U.S. Robotics Courier I ISDN V.Everything**. Podporuje analógové modemové pripojenia V.34, V.90 (X2), V.92 a viaclinkové PPP cez ISDN aj v režime vzniku aj odpovedania v systéme. 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 vznikajú v systéme.** Na výzvy CHAP, ktoré pochádzajú zo strany prijímania, odpovedá terminálový adaptér Courier I zatiaľ čo vyjednáva autentifikáciu PAP (Password Authentication Protocol) so systémom. Odpovede PAP sa neobjavia na pripojení ISDN.
- **Pripojenia, na ktoré systém odpovedá.** Courier I vyžaduje autentifikáciu CHAP zo strany volajúceho, ak konfigurácia odpovedania spôsobí, že systém otvorí autentifikáciu pomocou výzvy CHAP. Ak systém otvorí autentifikáciu pomocou PAP, terminálový adaptér Courier I bude autentifikovať pomocou PAP.

Ak používate modem Courier I spred roku 1999, skontrolujte, či je modem Courier I pripojený k vášmu systému káblom V.35 pre dosiahnutie najlepšej výkonnosti 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 spoločnosti 3Com/US Robotics verziu V.35 tohto terminálového adaptéra už viac nedodávajú tretie strany hoci niektoré verzie V.35 môžu ešte pochádzať od dodávateľov tretích strán. Verzia RS-232 sa stále odporúča pri trochu zníženom výkone v systéme, pretože pripojenia RS-232 sú obmedzené na 115,2 KB.

V systéme nezabudnite nastaviť rýchlosť linky V.35 na 230.4 kbps.

Obmedzenia pre terminálový adaptér ISDN:

V tejto téme sú vyhodnotené terminálové adaptéry. Odporúčajú sa len pri vytváraní vzdialených pripojení ISDN (Integrated Services Digital Network) zo systému.

3Com Impact IQ ISDN:

Tento terminálový adaptér sa neodporúča pre platformu System i, z nasledujúcich dôvodov:

- Terminálový adaptér nepodporuje analógové modemové pripojenia V.34. Môže však analógové modemové pripojenia V.34 podporovať pomocou externého pripojenia RJ-11.
- Terminálový adaptér aktuálne nepodporuje pripojenia V.90.
- Terminálový adaptér nesmie byť k systému pripojený pri rýchlostiach prevyšujúcich 115 200 bps.
- Terminálový adaptér nepodporuje automaticky CHAP (Challenge Handshake Authentication Protocol). Ak S84 nastavíte na 0, vykoná sa autentifikácia CHAP.
- Systém nedokáže zistiť čas ukončenia pripojenia, keď monitoruje signál Data Set Ready z terminálového adaptéra. Spôsobuje to potenciálne oslabenie bezpečnosti systému.

Motorola BitSurfr Pro ISDN:

Tento terminálový adaptér sa neodporúča pre platformu System i, z nasledujúcich dôvodov:

- Terminálový adaptér nepodporuje analógové modemové pripojenia V.34. Môže však analógové modemové pripojenia V.34 podporovať pomocou externého pripojenia RJ-11.
- Terminálový adaptér aktuálne nepodporuje pripojenia V.90.
- Terminálový adaptér nesmie byť k systému pripojený pri rýchlostiach prevyšujúcich 115 200 bps.
- Terminálový adaptér nepodporuje automaticky autentifikáciu CHAP. Avšak nastavenie @M2=C umožňuje vykonanie autentifikácie CHAP.
- Terminálový adaptér nepovoľuje automatické odpovedanie aj na jedno linkové aj na viaclinkové PPP volania. Vzdialený počiatočný terminálový adaptér musí byť nastavený na rovnaký protokol (jednolinkový alebo viaclinkový) ako odpovedací terminálový adaptér.
- Tokový riadiaci mechanizmus hardvéru nefunguje spoľahlivo s týmto terminálovým adaptérom. Následkom je znižovanie výkonu, keď systém odosiela údaje cez viaclinkové PPP pripojenie.

Spravovanie adries IP

PPP (Point-to-Point Protocol) pripojenia povoľujú niekoľko rôznych sád volieb pre riadenie IP adries v závislosti od typu profilu pripojenia.

- DHCP môže vo vašej sieti centrálne spravovať prideľovanie adries IP. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby DHCP. Pozrite si DHCP (Dynamic Host Configuration Protocol)
- DNS vám môže pomôcť spravovať hostiteľské mená a im priradené adresy IP. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby DNS. Pozrite si DNS (Domain Name System)
- BOOTP sa používa na priradenie klientskych pracovných staníc k vášmu systému a na priradenie ich IP adries. Naučte sa, ako vo svojej sieti nastaviť a spravovať služby BOOTP. Pozrite si Bootstrap Protocol

Súvisiaci odkaz

“Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE” na strane 10
Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

Filtrovanie paketov IP

Filtrovanie IP paketov obmedzuje služby samostatným užívateľom, keď sa prihlásia do siete.

Filtrovanie paketov môže povoliť alebo zakázať prístup podľa cieľa adresy IP, portov alebo oboje. Rozličné politiky sa vynucujú definovaním viacerých sád pravidiel filtrovania paketov, pričom každá má svoj vlastný jedinečný identifikátor PPP filtra. Pravidlá filtrovania paketov môžete priradiť konkrétnemu profilu pripojení prijímateľa alebo ich môžete priradiť s použitím skupinovej politiky, ktorá použije pravidlá filtrovania pre túto kategóriu užívateľa. Samotné pravidlá filtrovania paketov nie sú definované v PPP, ale sú definované pod IP Packet Rules v System i Navigator.

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

Súvisiaci odkaz

“Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE” na strane 10
Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

Súvisiace informácie

IP filtering and network address translation

VPN (Virtual Private Networking)

Stratégia manažmentu adries IP

Predtým ako nakonfigurujete profil PPP pripojení by ste sa mali oboznámiť so stratégiou riadenia sieťových IP adries. Táto stratégia ovplyvňuje mnohé rozhodnutia počas konfiguračného procesu, vrátane vašich autentifikačných stratégií, bezpečnostných hľadísk a nastavení TCP/IP.

Profily pripojení odosielateľa

V normálnom prípade budú lokálne a vzdialené adresy IP, definované pre profil pôvodcu, zadefinované ako *Priradené vzdialeným systémom*. To administrátorom na vzdialenom systéme povoľuje získať riadenie nad IP adresami, ktoré sa na pripojenie použijú. Takto bude definovaná väčšina všetkých pripojení k poskytovateľom služieb Internet (ISP), hoci mnohí ISP ponúkajú pevné adresy IP za dodatočný poplatok.

Ak zadefinujete trvalé IP adresy buď pre lokálnu alebo vzdialenú IP adresu, musíte mať istotu, že vzdialený systém je definovaný, aby akceptoval vami zadefinované IP adresy. 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.

Ďalším hľadiskom je, či chcete povoliť maskovanie IP adresy. Napríklad, ak sa systém pripojí k Internetu prostredníctvom ISP, za systémom pripojenej sieti to umožní pristupovať na Internet. Systém vlastne skrýva IP adresy systémov v sieti za lokálne IP adresy, ktoré priradil ISP, a tým vytvára dojem, že všetka IP prevádzka pochádza zo systému. Existujú aj ďalšie hľadiská smerovania aj pri systémoch v sieti LAN (aby sa zabezpečilo, že ich internetová prevádzka sa bude odosielať do systému) aj pri systéme, v ktorom musíte povoliť políčko **add remote system as the default route**.

Profily pripojení prijímateľa

Profily pripojení prijímateľa majú oveľa viac hľadísk a volieb IP adries ako má Profil pripojení odosielateľa. 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

Pri jednom profile prijímateľa môžete definovať jedinečnú IP adresu alebo môžete použiť existujúcu lokálnu IP adresu z vášho systému, aby ste identifikovali koniec PPP pripojenia. Pre profily príjemcu pripojenia definovaných na podporu viacnásobných pripojení v tom istom čase musíte použiť už existujúcu adresu IP. Ak nie sú k dispozícii žiadne existujúce lokálne IP adresy, pre tento účel môžete vytvoriť virtuálnu IP adresu.

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 sa vzdialený systém považoval za súčasť siete LAN, mali by ste nakonfigurovať smerovanie IP adries, zadať IP adresu v rámci rozsahu IP adries pre systémy pripojené k sieti LAN a skontrolovať, či bol IP Forwarding povolený aj pre tento profil pripojenia aj pre systém.

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). To tiež umožňuje pre každé z týchto ID užívateľa definovať ďalšie trasy, aby ste mohli prostredie prispôsobiť na mieru známeho vzdialeného užívateľa. Na správnu činnosť tejto funkcie musí byť zapnutá autentifikácia.
Určite dodatočné adresy IP založené na užívateľskom ID vzdialeného systému	Táto voľba vám 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 systému, prebehne vyhľadávanie, ktoré zistí, či je vzdialená IP adresa definovaná konkrétne pre tohto užívateľa. Ak je, pre pripojenie sa použije daná adresa IP, maska a množina možných trás. Ak užívateľ nie je definovaný, IP adresa bude predvolene nastavená ako definovaná adresa Fixed IP alebo nasledujúca adresa Address Pool IP.
Povoľte vzdialenému systému určovať vlastné adresy IP	Táto voľba umožní vzdialenému používateľovi zadefinovať si vlastnú adresu IP, ak o to prejaví záujem. Ak si nevyjednajú, že budú používať svoju vlastnú IP adresu, vzdialená IP adresa bude určená pomocou metódy priraďovania definovanej vzdialenej IP adresy. Táto voľba nie je pôvodne nastavená. Pred jej nastavením treba uvážiť všetky aspekty.
Smerovanie adries IP	Klient telefonického pripojenia a systém musia mať smerovanie IP adries správne nakonfigurované, ak klient potrebuje prístup k ľubovoľným IP adresám v sieti LAN, do ktorej systém patrí.

Autentifikácia systému

PPP pripojenia k platforme System i podporujú niekoľko volieb autentifikácie pre vzdialených klientov, volajúcich do systému aj pre pripojenia k ISP alebo inému systému, do ktorého volá systém.

Systém podporuje niekoľko metód udržiavania autentifikačných informácií. K týmto metódam patrí zoznamy jednoduchého overenia platnosti v systéme, ktorý obsahuje zoznamy autorizovaných užívateľov a ich heslá pre podporu serverov RADIUS (Remote Authentication Dial In User Service). Servery RADIUS udržiavajú podrobné informácie pre užívateľov siete. Systém podporuje aj niekoľko volieb pre šifrovanie informácií o ID užívateľov a heslách, jednoduchou výmenou hesiel počínajúc a podporou protokolu CHAP-MD5 (Challenge Handshake Authentication

Protocol) končiac. Svoje preferencie pre autentifikáciu systému, vrátane ID užívateľa a hesla pre overenie platnosti systému, keď uskutočňuje odchádzajúce volanie, môžete zadávať na záložke **Authentication** profilu pripojenia v System i Navigator.

Súvisiaci odkaz

"Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE" na strane 10
Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

"Scenár: Autentifikácia telefonických pripojení pomocou RADIUS NAS" na strane 21
V systéme spustený NAS (Network Access Server) dokáže smerovať požiadavky na autentifikáciu z telefonicky pripojených klientov na osobitný server RADIUS (Remote Authentication Dial In User Service). Ak je autentifikovaný, RADIUS dokáže riadiť aj užívateľovi priradené IP adresy.

"Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP" na strane 23
Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

CHAP-MD5 (Challenge Handshake Authentication Protocol with MD5)

CHAP-MD5 (Challenge Handshake Authentication Protocol) používa algoritmus (MD-5) na výpočet 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: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému" na strane 13
Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

"PAP (Password Authentication Protocol)" na strane 44
PAP (Password Authentication Protocol) používa obojsmernú vzájomnú dohodu, aby partnerskému systému poskytol jednoduchú metódu na vytvorenie jeho identity.

EAP (Extensible Authentication Protocol)

EAP (Extensible Authentication Protocol) povoľuje autentifikačné moduly tretích strán pre interakciu s PPP implementáciou.

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 systémom vyjednať potrebnú autentifikáciu predtým ako dôjde prijatiu alebo odovzdaniu nejakých informácií.

Systém priamo nepodporuje EAP. Môžete však použiť vzdialenú autentifikáciu pre server RADIUS (Remote Authentication Dial In User Service), ktorá môže podporovať niektoré ďalšie už skôr popísané schémy autentifikácie.

PAP (Password Authentication Protocol)

PAP (Password Authentication Protocol) používa obojsmernú vzájomnú dohodu, aby partnerskému systému poskytol jednoduchú metódu na vytvorenie jeho 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 sa ID užívateľa a heslo nikdy nešifrujú, a preto sa dajú sledovať, čo ich robí zraniteľnými voči útoku počítačových pirátov. Z tohto dôvodu by ste mali vždy ak je to možné používať CHAP (Challenge Handshake Authentication Protocol).

Súvisiaci odkaz

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

RADIUS (Remote Authentication Dial In User Service) - prehľad

RADIUS (Remote Authentication Dial In User Service) je internetový štandardný protokol, ktorý poskytuje centralizovanú autentifikáciu, evidenciu a služby riadenia IP pre užívateľov vzdialeného prístupu v sieti distribuovaných telefonických pripojení.

Model klient-server protokolu RADIUS má server Network Access Server (NAS), ktorý pracuje ako klient pre server RADIUS. Systém, ktorý vystupuje ako NAS, odosiela informácie o užívateľovi a o pripojení do označeného servera RADIUS a používa pri tom štandardný RADIUS protokol, definovaný v RFC 2865.

Servery RADIUS jednajú podľa prijatých požiadaviek na užívateľské pripojenia autentifikovaním užívateľa, a potom vrátia všetky potrebné konfiguračné informácie do NAS, aby NAS (systém) mohol poskytovať autorizované služby autentifikovaným doň volajúcim užívateľom.

Ak server RADIUS nie je v dosahu, systém dokáže smerovať autentifikačné požiadavky na alternatívny server. To umožňuje globálne pôsobiacim podnikom ponúknuť svojim užívateľom službu prichádzajúcich hovorov s jedinečným prihlasovacím ID užívateľa pre celopodnikový prístup, bez ohľadu na to ktorý prístupový bod použijú.

Keď server RADIUS prijme požiadavku na autentifikáciu, platnosť požiadavky sa overí; potom server RADIUS dešifruje paket údajov, aby získal prístup k menu užívateľa a heslu. Informácie sa dostanú do príslušného bezpečnostného systému, ktorý je podporovaný. Môžu to byť súbory hesiel UNIX, Kerberos, komerčný zabezpečovací systém alebo zákazníkom vytvorený bezpečnostný systém. Server RADIUS pošle naspäť do systému všetky služby, ktoré je autentifikovaný užívateľ oprávnený používať, ako napríklad IP adresa. Požiadavky o účtovanie RADIUS sú spracúvané podobne. Informácie o kontách vzdialeného používateľa môžu byť zaslané na vybraný určený RADIUS server. Štandardný protokol evidencie 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 pomocou RADIUS NAS" na strane 21
V systéme spustený NAS (Network Access Server) dokáže smerovať požiadavky na autentifikáciu z telefonicky pripojených klientov na osobitný server RADIUS (Remote Authentication Dial In User Service). Ak je autentifikovaný, RADIUS dokáže riadiť aj užívateľovi priradené IP adresy.

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. Môže byť **šifrované - CHAP-MD5/EAP** alebo **nešifrované - PAP**.

Bližšie informácie nájdete v online pomoci.

Súvisiaci odkaz

"Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP" na strane 23
Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

Hľadiská šírky pásma pri viacerých linkách

Ďalšia šírka pásma sa často vyžaduje pre dokončenie určitých úloh, ale nie je vždy povinná.

Nákup špecializovaného hardvéru a drahých komunikačných liniek nemusí byť opodstatnený. PPP MP (Multilink Protocol) zoskupuje viaceré PPP linky, aby vytvorili jednu virtuálnu linku alebo zväzok. Agregácia viacerých liniek zvýši celkovú efektívnu šírku pásma medzi dvomi systémami, ktoré používajú štandardné modemy a telefónne linky. Do zväzku MP môžete zaradiť až šesť liniek. Ak chcete vytvoriť viaclinkové pripojenie, obidva konce PPP linky musia podporovať MP (Multilink Protocol). MP (Multilink Protocol) je zdokumentovaný ako štandard RFC (Request for Comment) RFC-1990.

Bandwidth On Demand

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 sa bežne označuje ako Bandwidth on Demand a umožňuje vám platiť za ďalšiu šírku pásma len vtedy, keď ju naozaj využívate. Aby ste spoznali výhody Bandwidth on Demand, aspoň jeden partnerský počítač musí mať schopnosť monitorovať momentálne využívanie celkovej šírky pásma vo zväzku MP. Linky môžete do zväzku pridávať alebo ich z neho odstraňovať, keď využitie šírky pásma prekročí hodnoty, definované v konfigurácii. Bandwidth Allocation Protocol umožňuje partnerským počítačom vyjednávať pridávanie a odstraňovanie liniek v zväzku MP. RFC-2125 dokumentuje aj PPP BAP (Bandwidth Allocation Protocol) aj BACP (Bandwidth Allocation Control Protocol).

Súvisiace informácie

Editor RFC

Konfigurácia PPP

Predtým ako budete môcť PPP použiť na nastavenie dvojbodového pripojenia musíte nakonfigurovať PPP prostredie.

Súvisiaci odkaz

"Súvisiace informácie pre Remote Access Services" na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Vytváranie profilu pripojenia

Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

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 pripojení odosielateľa
- Profily pripojení prijímateľa
- **Modemy**

Ak chcete vytvoriť profil pripojenia, postupujte podľa týchto krokov:
1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Vyberte jednu z týchto volieb:
   - Pravým tlačidlom kliknite na **Originator Connection Profiles**, aby ste nastavili inicializáciu systému.
   - Pravým tlačidlom kliknite na **Receiver Connection Profiles**, ak chcete systém nastaviť, aby povoľoval pripojenia prichádzajúce zo vzdialených systémov a užívateľov.
3. Vyberte **New Profile**.
4. Na strane New Point-to-Point Connection Profile Setup vyberte typ protokolu.
5. Určite výbery režimov.
6. Vyberte konfiguráciu linky.
7. Kliknite na **OK**.

   Zobrazí sa strana New Point-to-Point Profile Properties. Môžete nastaviť ostatné hodnoty, špecifické pre vašu sieť. Špecifické informácie nájdete v online pomoci.

   Súvisiace úlohy

   “Priradenie modemu k popisu linky” na strane 55
   Téma predstavuje kroky pre priradenie modemu k popisu linky.

   Súvisiaci odkaz

   “Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE” na strane 10
   Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

   “Scenár: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému” na strane 13
   Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

   “Scenár: Pripájanie kancelárskej siete LAN k Internetu pomocou modemu” na strane 15
   Administrátori zvyčajne nastavujú kancelárske siete pre zamestnancov, aby mali prístup na Internet. Administrátori môžu použiť modem na pripojenie systému k ISP (Internet Service Provider). PC klienti pripojení k sieti LAN môžu komunikovať cez Internet pomocou operačného systému i5/OS v úlohe brány.

   “Scenár: Pripájanie vašich podnikových a vzdialených sietí pomocou modemu” na strane 18
   Modem umožňuje dvom vzdialeným umiestneniam (ako napríklad ústredňa a pobočková ústredňa) vymieňať si údaje. PPP (Point-to-Point Protocol) dokáže navzájom prepojiť dve siete LAN tak, že vytvorí pripojenie medzi systémom na ústredni a druhým systémom na pobočkovej ústredni.

   “Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP” na strane 23
   Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

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

PPP nahrádza SLIP (Serial Line Internet Protocol) ako výberový protokol pre dvojbodové pripojenia.

PPP umožňuje vzájomnú spoluprácu medzi softvérom pre vzdialený prístup od rôznych výrobcov. PPP tiež umožňuje, aby viaceré sieťové komunikačné protokoly používali rovnakú fyzickú komunikačnú linku.

SLIP RFC (Request for Comment) sa nikdy nestane internetovým štandardom kvôli nasledujúcim nedostatkom:

- 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 v dnešnej dobe naďalej používa a je podporovaný v operačnom systéme i5/OS. IBM však odporúča, aby ste pri nastavovaní pripojení point-to-point používali PPP. SLIP neposkytuje podporu pre viaclinkové pripojenia. 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

Výbery režimu pre profil PPP (Point-to-Point Protocol) pripojení obsahuje výbery pre typ pripojenia a prevádzkový režim. Vaše výbery režimu zadávajú ako bude váš systém používať nové PPP pripojenie.

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

1. Vyberte jeden z uvedených typov pripojenia:
   - Komutovaná linka
   - Prenajatá linka
   - L2TP (Layer Two Tunneling Protocol) (virtuálna linka)
   - Linka PPPoE (Point-to-Point Protocol over Ethernet)
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:

Keď na pripojenie cez telefónnu linku používate modem (interný alebo externý) alebo externý ISDN (Integrated Services Digital Network) terminálový adaptér, vyberte pripojenie komutovanou linkou.

Typ pripojenia komutovanou linkou rozoznáva tieto režimy prevádzky:

Odpoveď

Vyberte tento prevádzkový režim, ak chcete povoliť vzdialenému systému volať do systému.

Vytáčanie

Vyberte tento prevádzkový režim, ak chcete povoliť systému volať do vzdialeného systému.

Vytáčať na žiadosť (len vytáčanie)

Vyberte si tento prevádzkový režim, ak chcete povoliť systému automaticky volať do vzdialeného systém, keď bola v systéme zistená TCP/IP prevádzka vzdialeného systému. 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)

Vyberte si tento prevádzkový režim, ak chcete povoliť systému, aby odpovedal na volania z vyhradeného vzdialeného systému. Tento prevádzkový režim systému tiež umožňuje volať vzdialený systém vtedy, keď bola zistená TCP/IP prevádzka pre vzdialený systém. Ak obidva systémy používajú operačný systém i5/OS a

používajú tento prevádzkový režim, TCP/IP prevádzka prebieha medzi týmito dvomi systémami na vyžiadanie 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. Ak chcete spracovávať prichádzajúce volania, ste odkázaný na existujúci odpovedací profil z profilu PPP (Point-to-Point Protocol) pripojení, ktorý tento prevádzkový režim špecifikuje. 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:

Ak máte medzi lokálnym systémom a vzdialeným systémom vyčlenenú linku, vyberte pripojenie prenajatej linky. Ak máte prenajatú linku, na pripojenie k týmto dvom systémom nepotrebujete modem ani ISDN (Integrated Services Digital Network) terminálový adaptér.

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

Vyberte tento prevádzkový režim, ak chcete povoliť vzdialenému systému prístup do systému cez vyčlenenú linku. Tento režim prevádzky sa odvoláva na profil odpovede pri prenajatej linke.

Pôvodca

Vyberte tento prevádzkový režim, ak chcete povoliť systému prístup do vzdialeného systému cez vyčlenenú linku. Tento režim prevádzky sa odvoláva na profil vytáčania pri prenajatej linke.

L2TP (virtuálna linka):

Ak chcete poskytovať pripojenie medzi systémami, ktoré používajú L2TP (Layer Two Tunneling Protocol), vyberte pripojenie L2TP.

Po vytvorení tunelu L2TP sa medzi vašim systémom a vzdialeným systémom vytvorí virtuálne PPP (Point-to-Point) pripojenie. 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

Vyberte si tento prevádzkový režim, ak chcete povoliť vzdialenému systému pripojiť sa k systému cez L2TP tunel.

Pôvodca

Vyberte si tento prevádzkový režim, ak chcete povoliť systému pripojiť sa k vzdialenému systému cez L2TP tunel.

Vzdialené telefonické pripojenie

Vyberte si tento prevádzkový režim, ak chcete povoliť systému pripojiť sa k inému systému alebo k ISP (Internet Service Provider) cez L2TP tunel a nariadiť ISP, aby zavolal vzdialeného PPP klienta.

Viacskokový iniciátor

Vyberte si tento prevádzkový režim, ak chcete systému povoliť vytvorenie pripojenia s viacerými skokmi.

Poznámka: Profil L2TP Terminator, ktorému je tento inicializátor viacnásobného skoku priradený, musí mať označené políčko **Allow multi-hop connection** a musí mať položku zoznamu overovania PPP platnosti, ktorá prepája meno užívateľa PPP s profilom inicializátora viacnásobného skoku.

Linka PPPoE:

PPPoE (Point-to-Point Protocol over Ethernet) pripojenia používajú virtuálnu linku na odosielanie PPP údajov (prostredníctvom ethernetového adaptéra) do DSL (Digital Subscriber Line) modemu, ktorý poskytuje váš ISP (Internet Service Provider). Modem je tiež pripojený k sieti LAN na báze ethernetu.

To užívateľom siete LAN umožňuje vysokorýchlostný internetový prístup prostredníctvom PPP relácií v operačnom systéme i5/OS. Po spustení pripojenia medzi systémom a ISP môžu jednotliví užívatelia v sieti LAN spustiť jedinečné relácie s ISP cez PPPoE.

PPPoE pripojenia používajú len profily pripojení odosielateľa. Pripojenia naznačujú prevádzkový režim Initiator a používajú len jednu linku.

Konfigurácia spojenia

Konfigurácia linky definuje typ linkovej služby, ktorú váš profil PPP (Point-to-Point Protocol) pripojenia používa na vytvorenie pripojenia.

Typy linkovej služby závisia od typu pripojenia, ktoré zadáte.

Súvisiaci odkaz

"Scenár: Pripájanie vášho systému ku koncentrátoru prístupu PPPoE" na strane 10
Mnohí ISP (Internet Service Provider) poskytujú vysokorýchlostný prístup na Internet cez DSL (Digital Subscriber Line) s použitím PPPoE (Point-to-Point Protocol over Ethernet). Svoj systém môžete pripojiť k týmto ISP, aby mu poskytli širokopásmové pripojenia, ktoré zachovávajú prínosy PPP (Point-to-Point Protocol).

"Scenár: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému" na strane 13
Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

"Scenár: Pripájanie kancelárskej siete LAN k Internetu pomocou modemu" na strane 15
Administrátori zvyčajne nastavujú kancelárske siete pre zamestnancov, aby mali prístup na Internet. Administrátori môžu použiť modem na pripojenie systému k ISP (Internet Service Provider). PC klienti pripojení k sieti LAN môžu komunikovať cez Internet pomocou operačného systému i5/OS v úlohe brány.

"Scenár: Pripájanie vašich podnikových a vzdialených sietí pomocou modemu" na strane 18
Modem umožňuje dvom vzdialeným umiestneniam (ako napríklad ústredňa a pobočková ústredňa) vymieňať si údaje. PPP (Point-to-Point Protocol) dokáže navzájom prepojiť dve siete LAN tak, že vytvorí pripojenie medzi systémom na ústredni a druhým systémom na pobočkovej ústredni.

Jednoduchá linka:

Ak chcete definovať PPP (Point-to-Point Protocol) linku, ktorá je priradená k analógovému modemu, vyberte túto linkovú službu. Táto voľba sa tiež používa pre prenajaté linky, kde sa nevyžaduje modem. Profil PPP pripojení vždy používa rovnaký prostriedok komunikačného portu i5/OS.

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 popis komutovanej linky a vyberte **Enable Dynamic Resource Sharing**.

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:

Ak chcete PPP pripojenie nastaviť, aby používalo linku zo združených liniek, vyberte túto linkovú službu. Keď sa PPP pripojenie spustí, systém zo združených liniek vyberie nepoužívanú linku. Pri profiloch dial on-demand systém nevyberie linku pokiaľ nezistí TCP/IP prevádzku pre vzdialený systém.

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. Môžete ho nastaviť na záložke **Connections** dialógu **New Point-to-Point Profile Properties** pri konfigurácii vášho profilu 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.

  Systém vyberie linku z oblasti liniek len vtedy, keď používa pripojenie dial-on-demand. 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 System i Navigator vyberte svoj systém a rozviňte **Networking → Remote Access Services**.
2. Vytvorte profil pripojenia pre vytáčanie alebo prijímanie volaní. Vyberte jednu z týchto volieb:
   - Pravým tlačidlom kliknite na **Originator Connection Profiles**, aby ste systém nastavili pre inicializáciu pripojenia k vzdialenému systému.
   - Pravým tlačidlom kliknite na **Receiver Connection Profiles**, ak chcete systém nastaviť, aby povoľoval pripojenia prichádzajúce zo vzdialených systémov a užívateľov.
3. Vyberte **New profile**.
4. Pre profil pôvodcu (vytáčanie) vyberte: PPP, Komutovaná linka a Režim prevádzky (typicky telefonické pripojenie). Pre konfiguráciu spojenia vyberte **Line pool**. Kliknite na **OK** a System i Navigator otvorí okno vlastností pre tento profil pripojenia.

   Poznámka: Keď vytvárate profily pripojení prijímateľa, môžete vybrať aj oblasť liniek. Voľba oblasti liniek môže, ale nemusí byť uvedená. Závisí to od nasledujúcich hodnôt polí: protocol type, connection type a operating mode.
5. Na strane General pomenujte profil a zadajte opis.
6. Na strane Connection zadajte názov pre oblasť liniek a kliknite na **New**. Zobrazí sa dialógové okno **New Line Pool Properties**, 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 **New line** 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 prechádza zoznam dostupných liniek (v rámci oblasti) kým nenájde dostupný prostriedok a túto linku použije na pripojenie. Viac užitočných informácií nájdete v pomoci System i Navigator.

Súvisiaci odkaz

"Scenár: Pripájanie vzdialených klientov s telefonickým pripojením k vášmu systému" na strane 13
Vzdialení užívatelia, ako napríklad z domova pracujúci zamestnanci alebo mobilní klienti často vyžadujú prístup k podnikovej sieti. Títo klienti s telefonickým pripojením môžu získať prístup k systému pomocou PPP (Point-to-Point Protocol).

"Scenár: Pripájanie kancelárskej siete LAN k Internetu pomocou modemu" na strane 15
Administrátori zvyčajne nastavujú kancelárske siete pre zamestnancov, aby mali prístup na Internet. Administrátori môžu použiť modem na pripojenie systému k ISP (Internet Service Provider). PC klienti pripojení k sieti LAN môžu komunikovať cez Internet pomocou operačného systému i5/OS v úlohe brány.

"Scenár: Pripájanie vašich podnikových a vzdialených sietí pomocou modemu" na strane 18
Modem umožňuje dvom vzdialeným umiestneniam (ako napríklad ústredňa a pobočková ústredňa) vymieňať si údaje. PPP (Point-to-Point Protocol) dokáže navzájom prepojiť dve siete LAN tak, že vytvorí pripojenie medzi systémom na ústredni a druhým systémom na pobočkovej ústredni.

Podpora profilov viacerých pripojení:

Profily dvojbodového pripojenia, ktoré podporujú viaceré pripojenia vám umožňujú mať jeden profil pripojenia, ktorý bude spracovávať mnohé digitálne, analógové alebo L2TP volania.

Je to užitočné, keď chcete aby sa k vášmu systému pripojili mnohí užívatelia, ale nechcete zadať osobitný profil dvojbodových pripojení, ktorý má spracovávať každú PPP linku. Táto funkcia užitočná hlavne pri 4 portovom integrovanom modeme 2805, v ktorom môžete z jedného adaptéra použiť štyri linky.

Pre analógové linky s podporou profilu pre viacnásobné pripojenia sa používajú všetky linky v špecifikovanej oblasti liniek až po maximálny počet spojení. Vlastne sa pre každú linku, ktorá je definovaná v oblasti liniek, spustí osobitné vlákno profilu pripojenia. Všetky vlákna profilu pripojenia čakajú na prichádzajúce volanie na svojich príslušných linkách.

Lokálny IP adresa pre profily viacnásobných pripojení

Môžete použiť lokálnu IP adresu s profilmi viacnásobných pripojení, ale musí to byť existujúca IP adresa, ktorá je definovaná vo vašom systéme. Na výber existujúcej IP adresy môžete použiť roletový zoznam lokálnych IP adries. Vzdialení užívatelia môžu pristupovať na prostriedky, ktoré sú vo vašej lokálnej sieti, ak si vyberiete lokálnu IP adresu ako lokálnu IP adresu pre váš PPP profil. Tiež musíte definovať adresy IP, ktoré sú vo vzdialenej spoločnej oblasti adries IP, aby boli v rovnakej sieti ako lokálne adresy IP.

Ak nemáte lokálnu IP adresu alebo nechcete, aby vzdialení užívatelia pristupovali na LAN, musíte pre svoj systém zadefinovať virtuálnu IP adresu. Virtuálna IP adresa je známa aj ako bezobvodové rozhranie. Vaše profily point-to-point môžu používať túto adresu IP ako ich lokálnu adresu IP. Pretože táto IP adresa nie je naviazaná na fyzickú sieť, nebude automaticky posielať prevádzku ďalej do iných sietí, ktoré sú k vášmu systému pripojené.

Na vytvorenie virtuálnej adresy IP vykonajte tieto kroky:

1. V System i Navigator rozviňte svoj systém a pristúpte na **Network → TCP/IP configuration → IPV4 → Interfaces**.
2. Kliknite pravým tlačidlom myši na **Interfaces** a vyberte **New Interface → Virtual IP**.
3. Postupujte podľa inštrukcií sprievodcu rozhrania, aby ste vytvorili vaše virtuálne IP rozhranie. Vaše profily dvojbodových pripojení môžu používať virtuálnu IP adresu hneď ako bude vytvorená. Ak chcete vo svojom profile používať IP adresu, použite roletový zoznam v poli **Local IP address**, ktorý sa nachádza na stránke TCP/IP Settings.

   Poznámka: Virtuálna IP adresa musí byť aktívna ešte 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 IP adries pre profily viacnásobných 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 oblastí 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.

  Súvisiace úlohy

  “Krok 1: Konfigurácia profilu terminátora L2TP pre ľubovoľné rozhranie v oddiele, ktorý vlastní modemy” na strane 28
  Ak chcete vytvoriť profil terminátora pre ľubovoľné rozhranie, postupujte nasledovne:

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.

Sem patrí L2TP (Layer Two Tunneling Protocol) a oblasti liniek s maximálnym počtom pripojení, ktorý je väčší ako jedno. Táto funkcia povoľuje systému, aby každému prichádzajúcemu pripojeniu priradil jedinečnú vzdialenú IP adresu.

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 **Authentication**, 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 **Define additional IP addresses based on remote system's user ID** a kliknutím na **IP addresses defined by User Name**.

  Keď je k systému pripojený vzdialený užívateľ, systém zistí, či je pre tohto užívateľa definovaná špecifická IP adresa. V takomto prípade sa vzdialenému systému pridelí adresa IP, inak dostane adresu IP z oblasti vzdialených adries IP.

Konfigurácia modemu pre PPP

Modem vám poskytuje schopnosti analógového pripojenia (prenajaté a komutované linky). Pre svoje analógové PPP (Point-to-Point Protocol) pripojenia môžete použiť externý modem, interný modem alebo ISDN (Integrated Services Digital Network) terminálový adaptér.

Súvisiaci odkaz

"Odstraňovanie problémov PPP" na strane 62
Ak ste zaznamenali problémy s pripojením PPP (Point-to-Point Protocol), na zhromaždenie informácií o chybách použite kontrolný zoznam. Tento kontrolný zoznam vám pomôže identifikovať symptómy chýb a vyriešiť problémy s pripojením PPP.

Konfigurácia nového modemu

Nový modem môžete nakonfigurovať pomocou existujúceho popisu modemu alebo môžete popis modemu založiť na predchádzajúcom popise modemu.

Ak chcete nakonfigurovať nový modem, vykonajte nasledujúce kroky.

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Pravým tlačidlom myši kliknite na **Modems** a vyberte **New Modem**.
3. Na záložke **General** zadajte správne hodnoty do všetkých políčok field.
4. Voliteľné: Kliknite na záložku **Additional Parameters**, na ktorej môžete pridať všetky potrebné inicializačné príkazy pre váš modem.
5. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu New Modem Properties.

Použitie existujúceho popisu modemu

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

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Vyberte **Modems**.
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 **Properties**, 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 popisu modemu na základe predchádzajúceho popisu modemu

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

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Vyberte **Modems**.
3. V zozname modemov kliknite pravým tlačidlom myši na **Generic hayes** a vyberte **New modem based on**.
4. V dialógovom okne **New Modem** zmeňte príkazové reťazce, aby sa zhodovali s informáciami, ktoré vyžaduje váš modem.

   Súvisiaci odkaz

   “Odstraňovanie problémov PPP” na strane 62
   Ak ste zaznamenali problémy s pripojením PPP (Point-to-Point Protocol), na zhromaždenie informácií o chybách použite kontrolný zoznam. Tento kontrolný zoznam vám pomôže identifikovať symptómy chýb 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. V systéme definované modemy and 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)	
Presvedčte sa, či je povolená rýchlosť linky DTE-DCE pre spúšťanie konštantnou rýchlosťou 115.2 kbps (alebo maximálnou rýchlosťou, ktorú povoľuje modem)	
(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*

Tabuľka 9. V systéme definované modemy and príkazové reťazce (pokračovanie)

Vlastnosť modemu	Správny príkazový reťazec pre väčšinu modemov
Typ vytáčania modemu	ATDT pre tónovú voľbu alebo ATDP pre impulzovú voľbu

Príklad: Konfigurácia ISDN terminálového adaptéra

Príklad demonštruje ako máte nakonfigurovať ISDN (Integrated Services Digital Network) terminálový adaptér.

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Pravým tlačidlom myši kliknite na **Modems** a vyberte **New Modem**.
3. Na záložke **General** zadajte do všetkých políčok **field** správne hodnoty.
4. Voliteľný: Kliknite na záložku **ISDN Parameters**, aby ste mohli pridať 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 vykonal systém

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

   - Nastavenie typu ISDN prepínača a verzie, ktorú poskytuje lokálna telefónna spoločnosť.
   - Nastavenie telefónnych čísiel z telefónneho zoznamu a SPID (Service Profile Identifiers), ktoré poskytuje lokálna telefónna spoločnosť.
   - Nastavenie TEI (Terminal Entry ID), ktoré môže poskytovať lokálna telefónna spoločnosť.
   - Nastavenie protokolu B kanála (asynchrónny-pre-synchrónny PPP).
   - Ostatné nastavenia modemu, ktoré majú parametre s premenlivou dĺžkou, ktoré na označenie dĺžky parametra vyžadujú návrat vozíka.
   - Uloženie a aktivácia nových nastavení tak, aby boli obnovené po vynulovaní alebo vypnutí systému.
   - Príkaz sondy stavu aktivity *U* rozhrania (ATD*x*), ktorý umožňuje systému zistiť, kedy bola dosiahnutá synchronizácia s prepínačom ISDN ústredne. Znak *x* môže byť ľubovoľná číslica, ktorá je dovolená pre telefónne číslo, vrátane # a *.
5. Kliknite na **Add** k dodatočným príkazom pre modem. Tieto príkazy môžu byť uvedené s alebo bez priradeného parametra a krátkeho opisu na zoznam príkazov. Všetkým príkazom, ktoré zadáte bez priradeného parametra, môže byť parameter priradený, keď je modem priradený k popisu linky.
6. Kliknutím na **OK** vaše položky uložíte a zatvoríte stranu New Modem Properties.

Súvisiaci odkaz

"Terminálové adaptéry ISDN" na strane 38
ISDN (Integrated Services Digital Network) vám poskytuje digitálne pripojenie, ktoré vám umožní komunikovať s použitím ľubovoľnej kombinácie hlasu, údajov a videa a mnohých iných multimediálnych aplikácií.

Priradenie modemu k popisu linky

Téma predstavuje kroky pre priradenie modemu k popisu linky.

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services → Originator Connection Profiles alebo Receiver Connection Profiles**.
2. Vyberte jednu z uvedených možností:
   - Ak chcete pracovať s existujúcim profilom pripojenia, kliknite pravým tlačidlom myši na profil pripojenia a vyberte **Properties**.
   - Ak chcete pracovať s novým profilom pripojenia, vytvorte nové pripojenie.
3. Zo strany New Point-to-Point Profile Properties vyberte panel **Connection** a kliknite na **New**.
   - Zadajte názov konfigurácie spojenia.

- Kliknite na **New**, aby sa otvorilo okno New Line Properties.

4. V okne New Line Properties kliknite na záložku **Modem** a vyberte modem zo zoznamu. Vybraný modem bude priradený k opisu tejto linky. Pri interných modemoch by už mala byť vybratá príslušná definícia modemu. Bližšie informácie nájdete v online pomoci.

Profily odosielateľa pripojení môžete nakonfigurovať tak, že si budú požičiavať PPP linku a modem, priradený profilu prijímateľa pripojení, ktorý čaká prichádzajúce volanie. Pripojenie odosielateľa vráti PPP linku a modem do profilu prijímateľa pripojení, keď sa pripojenie ukončí. Ak chcete túto funkciu povoliť, v okne konfigurácie PPP linky vyberte na záložke **Modem** voľbu **Enable dynamic resource sharing**. PPP linky môžete nakonfigurovať na záložke **Connection** stránky Receiver Connection Profile a Originator Connection Profile.

Súvisiace úlohy

"Vytváranie profilu pripojenia" na strane 45
Prvým krokom pri konfigurácii PPP pripojenia medzi systémami je vytvorenie profilu pripojenia v systéme.

Konfigurácia vzdialeného PC

Ak sa chcete pripojiť k platforme System i z osobného počítača (PC), na ktorom sú spustené ľubovoľné 32 bitové operačné programy Windows, mali by ste si overiť, či je nainštalovaný a správne nakonfigurovaný modem a či ste na PC nainštalovali TCP/IP a Dial-Up Networking.

Informácie o konfigurácii Dial-up Networking na PC nájdete vo svojej dokumentácii Microsoft Windows. Nezabudnite špecifikovať alebo zadať tieto informácie:

- Typom telefonického pripojenia by malo byť **PPP**.
- Ak používate šifrované heslá, presvedčte sa, či používate CHAP-MD5 (MS-CHAP nie je podporovaný operačným systémom i5/OS). 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). Systém nepodporuje žiadny iný typ nezabezpečeného protokolu.
- IP adresovanie bežne definuje vzdialený systém alebo operačný systém i5/OS. Ak plánujete používať alternatívne metódy IP adresovania (ako napríklad definovanie vašich vlastných IP adries), presvedčte sa, či je systém nakonfigurovaný, aby akceptoval vašu metódu adresovania.
- Pridajte adresu IP DNS, ak sa to týka vášho prostredia.

Nakonfigurovanie prístupu na Internet prostredníctvom AT&T Global Network

Ak chcete komunikovať s AT&T Global Network, musíte nakonfigurovať 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 AT&T Global Network môžu používať nasledujúce typy aplikácií:

- **Poštová výmena**: Umožňuje vám pravidelne opakovane získavať poštu z jedného konta AT&T Global Network a odosielať ju do vášho systému za účelom distribúcie vašim užívateľom Lotus Mail alebo vašim 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.

Niektorý z týchto adaptérov musí používať sprievodcu AT&T Global Network Dial Connection:

- 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
- 2793/576C: Dvojportový WAN IOA s integrovaným modemom V.92 na porte 1 a štandardným komunikačným rozhraním na porte 2. 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 System i Navigator rozviňte svoj systém a pristúpte na **Network → Remote Access Services**.
2. Kliknite pravým tlačidlom myši na **Originator Connection Profiles** a vyberte **New AT&T Global Network Dial Connection**.
3. Po spustení sprievodcu pripojením k AT&T Global Network kliknite na **Help**, aby sa zobrazili informácie k práci s panelom.

Sprievodcovia pripojením

Sprievodcovia pripojením vás prevedú cez konfiguráciu profilu pripojenia.

Sprievodca novým telefonickým pripojením

Tento sprievodca popisuje kroky pre konfiguráciu profilu telefonického pripojenia pre prístup k vášmu ISP alebo intranetu. Aby ste mohli sprievodcu dokončiť, musíte určité informácie získať od svojho správcu siete alebo od ISP. Bližšie informácie o dokončení tohto sprievodcu nájdete v online pomoci.

Sprievodca univerzálnym pripojením IBM

Tento sprievodca popisuje kroky pre konfiguráciu profilu, ktorý môže softvér Electronic Customer Support používať na pripojenie sa k IBM. Elektronická servisná podpora zabezpečuje monitorovanie vášho jedinečného prostredia i5/OS, aby vám poskytla odporúčania personalizovaných opráv pre váš systém a momentálny stav.

Súvisiace informácie

Univerzálne pripojenie

Konfigurácia politiky skupinového prístupu

Zložka **Group Access Policies** pod Receiver Connection Profiles 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 politiku skupinového prístupu, postupujte nasledovne:

1. V System i vyberte svoj systém a rozviňte **Network → Remote Access Services → Receiver Connection Profiles**.
2. Kliknite pravým tlačidlom myši na **Group Access Policies** a vyberte **New Group Access Policy**.

3. Na paneli **General** zadajte názov a opis novej skupinovej politiky prístupu.
4. Kliknite na záložku **Multilink** 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 **TCP/IP Settings**, ak chcete povoliť ľubovoľné z týchto nastavení:

   Allow remote system to access other networks (IP forwarding). Táto voľba určuje, či chcete definovať postupovanie IP. Ak vyberiete túto voľbu, v podstate povolíte systému, aby pri tomto pripojení vystupoval ako smerovač. To umožňuje IP datagramom, ktoré nie sú určené pre tento systém, aby prechádzali cez tento systém do pripojenej siete. Ak necháte túto voľbu prázdnu, IP zruší tieto datagramy zo vzdialeného systému, ktoré nie sú určené pre žiadne lokálne adresy tohto systému.

   Nepovolenie postupovania IP môže mať bezpečnostné dôvody. Opakom sú ISP, ktorí vo všeobecnosti poskytujú postupovanie IP. Nezabúdajte, že sa to prejaví len vtedy, ak je povolený celosystémový IP datagram; v opačnom prípade sa bude ignorovať, aj keď bude označená. Postupovanie datagramov IP je možné zobraziť na záložke **General** na strane IPv4 Properties.

   Request TCP/IP header compression (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, systém vytvorí pripojenie, ktoré nepoužíva komprimáciu.

   Use IP packet rules for this connection. Táto voľba určuje, či chcete pre danú skupinovú politiku aplikovať pravidlo filtrovania. Pravidlá filtrovania riadia IP prevádzku vo vašej sieti. Tento komponent filtrovania IP paketov môžete použiť na ochranu svojho systému pomocou filtrovania paketov 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 **Authentication**, aby sa otvorila strana Authentication.
2. Kliknite na **Require this iSeries server to verify the identity of the remote system**.
3. Vyberte **Authenticate locally using a validation list**.
4. Ak neexistuje validačný zoznam, vyberte ho zo zoznamu a kliknite na **Open**. Ak ho vytvárate po prvýkrát, zadajte názov nového validizačného zoznamu a kliknite na **New**.
5. Kliknutím na **Add** 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 **Apply a group policy to the user**, vyberte skupinovú politiku zo zoznamu a kliknite na **Open**.

Môžete zmeniť vlastnosti skupinovej politiky alebo pracovať s existujúcim nastavením.

7. Kliknutím na **OK** dokončíte konfiguráciu a vrátite sa na stranu Point-to-Point Properties.

Súvisiaci odkaz

“Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP” na strane 23
Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

Súvisiace informácie

IP filtering and network address translation

Používanie pravidiel filtrovania IP paketov pre PPP pripojenie

Súbor pravidiel paketov použite na obmedzenie prístupu užívateľa alebo skupiny na IP adresy vo vašej sieti.

Téma Filtrovanie IP a preklad sieťových adries v informačnom centre pojednáva o pravidlách IP paketov, na ktoré môžete odkazovať pri profile PPP pripojenia.

Existujúce pravidlá filtrovania IP paketov si môžete pozrieť dvomi spôsobmi:

- Úroveň profilu pripojenia
  1. Keď vyplníte **Point-to-Point Properties** pre **Receiver Connection Profile**, vyberte stranu TCP/IP Settings a kliknite na **Advanced**.
  2. Začiarknite **Use IP packet rules for this connection** 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 TCP/IP Settings.
  3. Začiarknite **Use IP packet rules for this connection** a vyberte identifikátor filtra PPP zo zoznamu.
  4. Kliknutím na **OK** sa aplikuje filter PPP.

Súvisiaci odkaz

“Scenár: Riadenie prístupu vzdialených užívateľov k prostriedkom pomocou skupinových politík a filtrovania IP” na strane 23
Politiky skupinového prístupu identifikujú rôzne skupiny užívateľov pre pripojenie a umožňujú vám použiť bežné atribúty pripojenia a bezpečnostné nastavenia pre celú skupinu. Skupinové politiky spolu s filtrovaním IP môžete použiť na povolenie a zakázanie prístupu k špecifickým IP adresám vo vašej sieti.

Povolenie služieb RADIUS a DHCP pre profily pripojenia

Prinášame vám postup pre povolenie služieb RADIUS alebo DHCP (Dynamic Host Configuration Protocol) pre profily prijímateľa PPP pripojení.

1. V System i Navigator vyberte svoj systém a rozviňte **Network → Remote Access Services**.
2. Kliknite pravým tlačidlom myši na **Remote Access Services** a vyberte **Services**.
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 **Enable RADIUS Network Access Server connection**
   b. Označte **Enable RADIUS for authentication**.
   c. Ak je to použiteľné vo vašom riešení RADIUS, povoľte aj evidenciu RADIUS a konfiguráciu TCP/IP adries.
5. Kliknite na tlačidlo **RADIUS NAS settings** a nakonfigurujte pripojenie k serveru RADIUS.
6. Kliknite na **OK**, ak sa chcete vrátiť do System i Navigator.

Súvisiaci odkaz

"Scenár: Autentifikácia telefonických pripojení pomocou RADIUS NAS" na strane 21
V systéme spustený NAS (Network Access Server) dokáže smerovať požiadavky na autentifikáciu z telefonicky pripojených klientov na osobitný server RADIUS (Remote Authentication Dial In User Service). Ak je autentifikovaný, RADIUS dokáže riadiť aj užívateľovi priradené IP adresy.

Riadenie PPP

Táto téma obsahuje informácie o úlohách riadenia PPP, ktoré môžete vykonávať v systéme.

Súvisiaci odkaz

"Súvisiace informácie pre Remote Access Services" na strane 63
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Nastavenie vlastností pre profily PPP pripojení

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.

Tento návod môžete použiť pri vyplňovaní stránok v okne New Point-to-Point Profile Properties. Nastavenia, ktoré vyberiete na každej strane, závisia od vášho prostredia a typu pripojenia, ktoré konfigurujete. Online pomoc System i Navigator popisuje každú voľbu, ktorá sa zobrazí v okne. Bližšie informácie nájdete aj v príkladoch a procedúrach PPP.

Monitorovanie činnosti PPP

Pomocou System i Navigator si môžete zobraziť profil pripojenia a protokol relácie.

Informácie o úlohách pripojení PPP

- Existujú dve PPP riadiace úlohy, ktoré sa používajú na riadenie jednotlivých vláken pripojenia PPP. Tieto úlohy sa vykonávajú v podsystéme QSYSWRK:
  - QTPPPCTL - hlavná kontrolná úloha PPP. Táto úloha riadi všetky vlákna 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*nnn* sú úlohy dial-in, pričom *nnn* predstavuje ľubovoľné číslo od 1 do 999.

Práca s profilmi pripojenia:

1. V System i Navigator rozviňte svoj systém a pristúpte na **Network → Remote Access Services**. Vyberte **Originator Connection Profile** alebo **Receiver Connection Profile**.
2. V stĺpci Profile kliknite pravým tlačidlom myši na názov profilu pripojenia a vyberte jednu z nasledujúcich volieb:
   - **Connection** 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.
   - **Properties** - otvorí strany vlastností na zobrazenie aktuálnych vlastností pre pripojenie.

Zobrazovanie informácií o pripojení:

1. V System i Navigator rozviňte svoj systém a pristúpte na **Network → Remote Access Services**. Vyberte **Profil pripojenia pôvodcu** alebo **Profil pripojenia prijímača**.
2. V stĺpci Profile kliknite pravým tlačidlom na názov profilu pripojenia, ktorý nemá stav Inactive a vyberte **Connections**, 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 **Jobs**. V okne pripojení kliknite pravým tlačidlom myši na názov úlohy a vyberte **Printer Output** alebo **Job Log**, aby sa zobrazili informácie o všetkých vláknach, ktoré sú priradené k QTPPPCTL.
5. Ak si chcete prezrieť podrobnosti o pripojení, kliknite na **Details**. 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 **Call Log**.
7. Ak chcete zobraziť protokoly správ, kliknite na **Message Log**.

Práca s výstupom PPP zo systému:

Ak chcete pracovať s výstupom PPP, do systémového príkazového riadku 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 **Status** pre každý profil v zozname profilov pripojení pod **Network → Remote Access Services** po vybratí profilov pôvodcu alebo prijímača. Stav pre jednotlivé pripojenia sa zobrazí pomocou okna Connections.

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	Systém 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

Tabuľka 11. Opis sekundárneho stavu (pokračovanie)

Opis sekundárneho stavu	Vysvetlenie
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 PPP

Ak ste zaznamenali problémy s pripojením PPP (Point-to-Point Protocol), na zhromaždenie informácií o chybách použite kontrolný zoznam. Tento kontrolný zoznam vám pomôže identifikovať symptómy chýb a vyriešiť problémy s pripojením PPP.

Aktuálne a relevantné informácie o dočasných opravách programov (PTF) a o odstraňovaní problémov sú zdokumentované na webovej stránke TCP/IP for i5/OS  . Táto webová stránka poskytuje najnovšie informácie, ktoré dopĺňajú a rušia informácie obsiahnuté v tejto téme.

1. Požadovaný podporný materiál:
   - Typ vzdialeného hostiteľa, operačný systém a úroveň
   - Úroveň operačného systému hostiteľa i5/OS
   - 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, ktorý 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

Publikácia ITSO Redbook V4 TCP/IP for AS/400: More Cool Things Than Ever  pokrýva nasledujúce PPP problémy. Poskytuje aj podrobné informácie o riešení problémov.

Ak chcete identifikovať problémy a nájsť ich riešenia, pozrite si kontrolný zoznam v nasledujúcej tabuľke.

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 na preddefinovanom zozname modemov v System i Navigator.	Vytvorte nový modem.
Používatelia a heslá PPP Keď sa pokúšate nadviazať pripojenie PPP, objavia sa chyby súvisiace s menom a heslom používateľa.	• Prekontrolujte, či ste ID používateľa a heslo zadali správne (malé a veľké písmená). • Skontrolujte, či oba komunikujúce systémy používajú rovnaký autentifikačný protokol. • Ak je jedna strana nakonfigurovaná ako CHAP, na druhej strane nepoužívajte PAP.
Linky PPP pre spustenie profilu pripojenia Identifikované linky PPP používajú rovnaký hardvérový prostriedok.	Nezabudnite vypnúť ostatné linky, používajúce ten istý hardvérový prostriedok.
Protokol PPP Chyby pri pripojení sa môžu vyskytnúť aj z dôvodu nesprávnej konfigurácie protokolu PPP.	Preskúmanie nižších úrovní PPP protokolu môže byť v niektorých situáciách nevyhnutné, keď partnerské počítače nedokážu navzájom komunikovať kvôli chybe v konfigurácii. Ak protokol PPP alebo protokol úlohy PPP nezobrazuje žiadnu indikáciu problému, môžete ho preskúmať pomocou funkcie sledovania priebehu komunikácie.

Súvisiace koncepty

“Konfigurácia modemu pre PPP” na strane 53
Modem vám poskytuje schopnosti analógového pripojenia (prenajaté a komutované linky). Pre svoje analógové PPP (Point-to-Point Protocol) pripojenia môžete použiť externý modem, interný modem alebo ISDN (Integrated Services Digital Network) terminálový adaptér.

“Konfigurácia nového modemu” na strane 53
Nový modem môžete nakonfigurovať pomocou existujúceho popisu modemu alebo môžete popis modemu založiť na predchádzajúcom popise modemu.

Súvisiaci odkaz

“Súvisiace informácie pre Remote Access Services”
Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

Súvisiace informácie pre Remote Access Services

Publikácie IBM Redbooks a webové stránky obsahujú informácie, ktoré súvisia s kolekciou tém Remote Access Services. Ľubovoľný z týchto súborov PDF môžete zobraziť alebo vytlačiť.

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic!
- V4 TCP/IP for AS/400: More Cool Things Than Ever

Webové lokality

Najnovšie dočasné opravy programov (PTF) a najnovšie konfiguračné informácie pre PPP a L2TP nájdete prostredníctvom PPP odkazu na webovú stránku TCP/IP for i5/OS  . Táto webová stránka poskytuje najnovšie informácie, ktoré dopĺňajú a rušia informácie, obsiahnuté v tejto kolekcii tém.

Súvisiaci odkaz

“Súbor PDF pre RAS (Remote Access Services)” na strane 1
Môžete zobraziť alebo vytlačiť súbor PDF týchto informácií.

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, popísaný v tomto dokumente a všetok licenčný materiál, preň dostupný, dodáva spoločnosť IBM podľa podmienok uvedených v zmluve IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code alebo v nejakej inej rovnocennej zmluve, ktorá medzi nami existuje.

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. _uveďte rok alebo roky_. Všetky práva vyhradené.

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

Informácie o programovacom 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
AS/400
eServer
i5/OS

IBM
IBM (logo)
iSeries
Lotus
OS/400
Redbooks
System i

Adobe, logo Adobe, PostScript a logo PostScript sú buď registrované ochranné známky alebo ochranné známky spoločnosti Adobe Systems Incorporated v USA a/alebo v iných krajinách.

Linux je registrovaná ochranná známka spoločnosti Linus Torvalds v USA, v iných krajinách alebo v obidvoch.

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.

SPOLOČNOSŤ 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